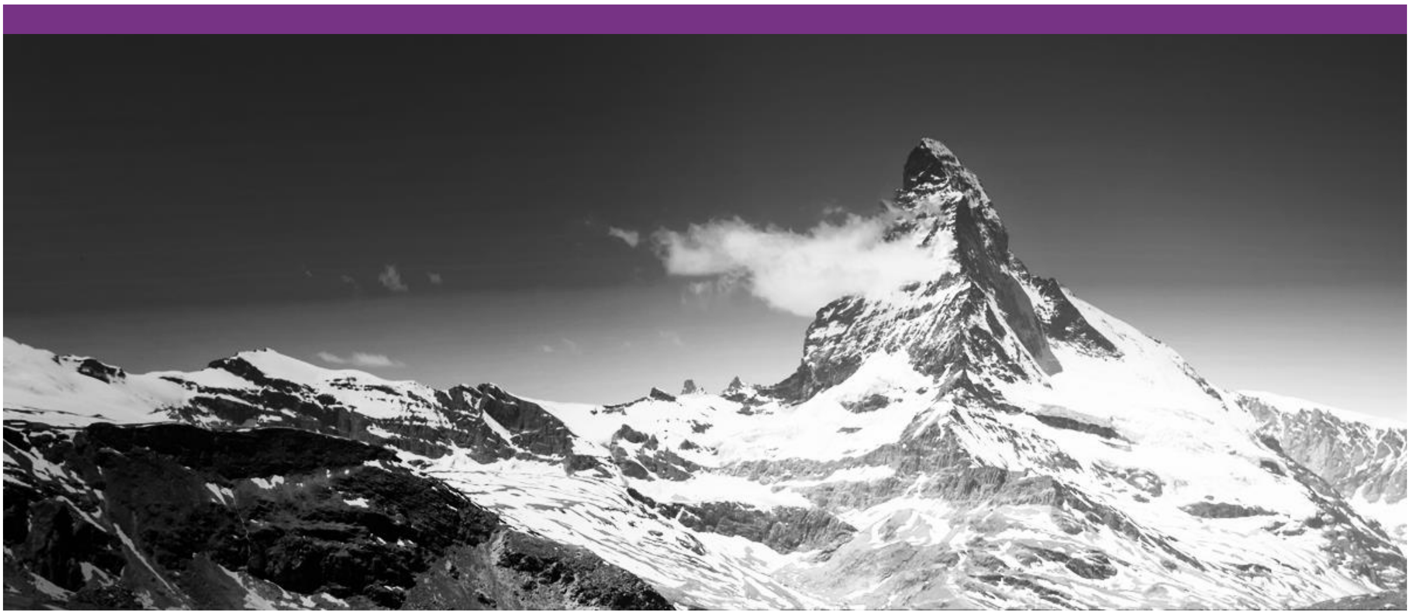

VIVAS Executive Summary Report

Verification and Validation of Autonomous Systems

Submitted by:

Solenix Engineering GmbH
Project Ref.: SLXENGDE/VIVAS/2021
Doc. Ref.: SLXENGDE-VIVAS-ESR

Title:	VIVAS Executive Summary Report		
Volume:	Verification and Validation of Autonomous Systems		
Customer:	ESTEC		
Customer Reference:	4000137021/21/NL/MGu		
Project Reference:	SLXENGDE/VIVAS/2021		
Document Reference:	SLXENGDE-VIVAS-ESR		
Date:	13/07/2023		
Version:	01.01		
Document Responsible:	Simone Fratini		
Author(s):	Consortium Team		
Approved:	Technical Officer		
Company:	Solenix Engineering GmbH Spreestrasse 3 64295 Darmstadt Germany	Phone: E-Mail: Internet:	+49 6151 870 91 0 info@solenix.de www.solenix.de

Document Log

Revision	Date	Responsible	Comment
00.01	24/05/2023	Simone Fratini	First Issue
01.00	28/06/2023	Simone Fratini	Final version
01.01	13/07/2023	Simone Fratini	General Review after AR. Updated Figure 1 and Section 4.

Distribution List

Name	Organisation
Quirien Wijnands	European Space Agency
VIVAS Consortium	Solenix – Fondaztione Bruno Kessler – Trasys

Table of Content

1 Introduction

1.1 Scope and Purpose

The current document represents the deliverable “VIVAS Executive Summary Report” for the study “Verification and Validation of Autonomous Systems”. This document summarizes the work done by the consortium led by Solenix, with FBK and TRASYS under ESA Contract “4000137021/21/NL/MGu”.

1.2 Document Structure

The document is organized as it follows.

Chapter 1	This chapter. Provides the purpose and scope of the activity together with applicable and reference documents
Chapter 2	Provides the background of the activity
Chapter 3	Lists the different activities performed in this study
Chapter 4	Contains the final Conclusions and Achievements of the activity

1.3 Applicable Documents

Ref.	Document Title	Reference
AD-01	Statement of Work	ESA-TDE-TECSWT-SOW-023541, 1.0, 17/02/2021
AD-02	VIVAS Technical Proposal	SLXENGDE-VERVAL-PRP-02-TP, 01.00, 27/10/2021
AD-03	Space Engineering – Software Tailoring for Ground Segment Systems (TT4), QMS-EIMO-GUID-CKL-9500-OPS, v 1.0. July 2009	ECSS-E-ST-40C
AD-04	VIVAS Management Proposal	SLXENGDE-VIVAS-ESR, 01.00, 27/10/2021

1.4 Reference Documents

Ref.	Document Title	Reference
RD-01	VIVAS D1 - Analysis Report on Verification and Validation of AI using Simulators	SLXENGDE-VIVAS-TN-01

RD-02	VIVAS D2 - Identification and definition of the Use-Case	SLXENGDE-VIVAS-TN-02
RD-03	VIVAS D3 - Architectural design of the Verification and Validation framework	SLXENGDE-VIVAS-TN-03
RD-04	VIVAS D4 – PoC Detailed Design	SLXENGDE-VIVAS-TN-04
RD-05	VIVAS D5 – PoC Test Report	SLXENGDE-VIVAS-TN-05

1.5 Acronyms and Abbreviations

Acronym	Description
AI	Artificial Intelligence
AR	AR: Acceptance Review
ESA	European Space Agency
ESOC	European Space Operation Centre
ESTEC	European Space Research and Technology Centre
FBK	Fondazione Bruno Kessler
KOM	Kick-off Meeting
ML	Machine Learning
MLOps	Machine Learning Operations
P&S	Planning and Scheduling
POC	Proof of Concept
SoW	Statement of Work
SSF	System-level Simulation Facility
V&V	Verification and Validation
XAI	Explainable AI

2 Background

The objective of the Verification and Validation of Autonomous Systems (VIVAS) activity is to propose and demonstrate a generic Verification and Validation methodology based on the usage of the System-level Simulation Facilities, specifically targeted at autonomous systems using AI-models.

Growing usage of AI/ML technologies in autonomous systems poses new challenges because the approach is very effective in implementing specific functionalities, but it comes with inherent uncertainty, and thus may be not suitable “as-is” for mission-critical systems. The validation and verification of autonomous systems using AI/ML components or integrating AI/ML components with control-based planning and scheduling systems, is therefore of paramount importance for future missions.

The overall concept of VIVAS is to provide a V&V framework that makes use of symbolic models to generate test cases to be executed on a system-level simulator, encompassing the AI/ML models “under test, to obtain execution traces which are in turn analysed by a monitor that is automatically generated.

The outcome of the proposed approach is a V&V methodology that provides the coverage statistics of the executed traces with respect to the symbolic models and quantitative and qualitative information for each executed test case.

The proposed approach has been demonstrated by implementing a Proof of Concept based on a state-of-the-art simulator of a planetary robotic asset making use of on-board ML models.

The outcomes of the project were:

- A V&V methodology based on model checking and simulation for autonomous systems
- The VIVAS Framework, a general, domain independent, software implementation of the proposed methodology
- A proof of concept, full instantiation of the VIVAS Framework for the 3DROV robotic simulator
- An image recognition ML model trained for the proof of concept and integrated in the simulator
- Two test cases to demonstrate usage and advantages of the VIVAS Framework

Assessment and lessons learned have been collected, recommendations and guidelines for possible extensions and future application of the framework proposed have been synthesized and reported at the end of the project.

3 Executive Summary

Between May 2022 and June 2023, the consortium has analysed the state-of-the-art of V&V processes of AI-models, defined and implemented a generic V&V architecture, adapted an autonomous system based on the 3DROV simulator, trained an image recognition ML model, and tested the V&V architecture on two significant test cases on a realistic robotic scenario.

The activities have been broken into four main tasks. These are synthesized in the following sections.

3.1 Quality Model and Verification and Validation Philosophy

The goal of the first preparatory activity was twofold. First it aimed at establishing a clear overview of the state of the art of verification and validation process of AI-models, and on the usage of simulators for that purpose. Second, it aimed at supporting the definition of the V&V philosophy proposed, specifically targeting the V&V of autonomous systems. This analysis drove the identification of appropriate use cases and the architectural design of the VIVAS Framework (in Task 2), as well as the detailed design and implementation of the Proof of Concept (in Task 3).

Main activities carried on during Task 1 were:

- Analysis of current common practices of testing, verification and validation of autonomous systems based on AI-models and Identification of software frameworks for supporting the development, verification, and validation of AI models.
- Analysis of the state of the art of system-level simulators for the verification and validation purposes of AI-models.
- Review of the current practice for supporting the life cycle and Quality Model for AI/ML modelling.

Results and findings of this preparatory activity have been reported in the deliverable “Analysis Report on Verification and Validation of AI using Simulators” [RD-01].

3.2 Use-Case Identification and V&V Architectural Design

The second task related to the definition of the architectural design of the VIVAS Framework and to the identification, analysis, selection, and validation of appropriate use cases to validate the VIVAS Framework.

The high-level conceptual architecture adopted for the system-level verification is depicted in Figure 1. The V&V workflow is made of 4 main steps:

- Abstract Scenario Generation. The scenario generation is the first step of the approach. The starting point is a formal, symbolic model of the system, which provides an abstract view of both the environment and the components under test (including AI/ML parts). Abstract test scenarios are generated from the formal system model using symbolic model checking techniques by the abstract scenario generator. The main task of this step is generating a set of formal properties, with the goal of stimulating interesting behaviours of the abstract system. For each property defined by the abstract scenario generator, a model checker will be executed on the system model, with the goal of producing execution traces witnessing the violation of the property itself. The properties here are then used to explore the system behaviour (i.e., to satisfy some coverage conditions); then the different set of properties are specified to check whether the result of a test case is pass or fail.

- Concrete Scenario Generation. Each of the traces produced by the model checker is then refined into a (set of) concrete scenarios that can be used to drive the system-level (concrete) simulator. Ensuring an adequate level of coverage is one of the primary goals of a good set of tests. Although the specific criteria usually depend on the actual use-case application, VIVAS defines some general coverage criteria at abstract level, including coverage of the abstract scenarios with respect to the set of properties, coverage of the properties with respect to the abstract model and coverage with respect to a domain-specific notion of "interesting situations".
- Simulation. The objective of the system level simulator is to run a simulation of the target asset under the requested conditions and, at completion, to provide the execution trace. To this end, the models of all the subsystems are initialised at the provided state and the environment models are set at the given initial conditions from the concrete scenarios generated by VIVAS.
- Execution Monitor. Each concrete scenario produced is executed by the simulator, which generates a corresponding concrete execution trace. This trace is then used to determine whether the concrete system satisfies the formal property, by formally evaluating the trace with a run-time monitor that is automatically generated from the formal specification of the property and the abstract system model. The formal properties are evaluated both qualitatively and quantitatively to see if the trace correctness is robust to minor variation of the inputs. Moreover, the monitor also measures the coverage to check that the concrete execution matches the abstract scenario constraints.

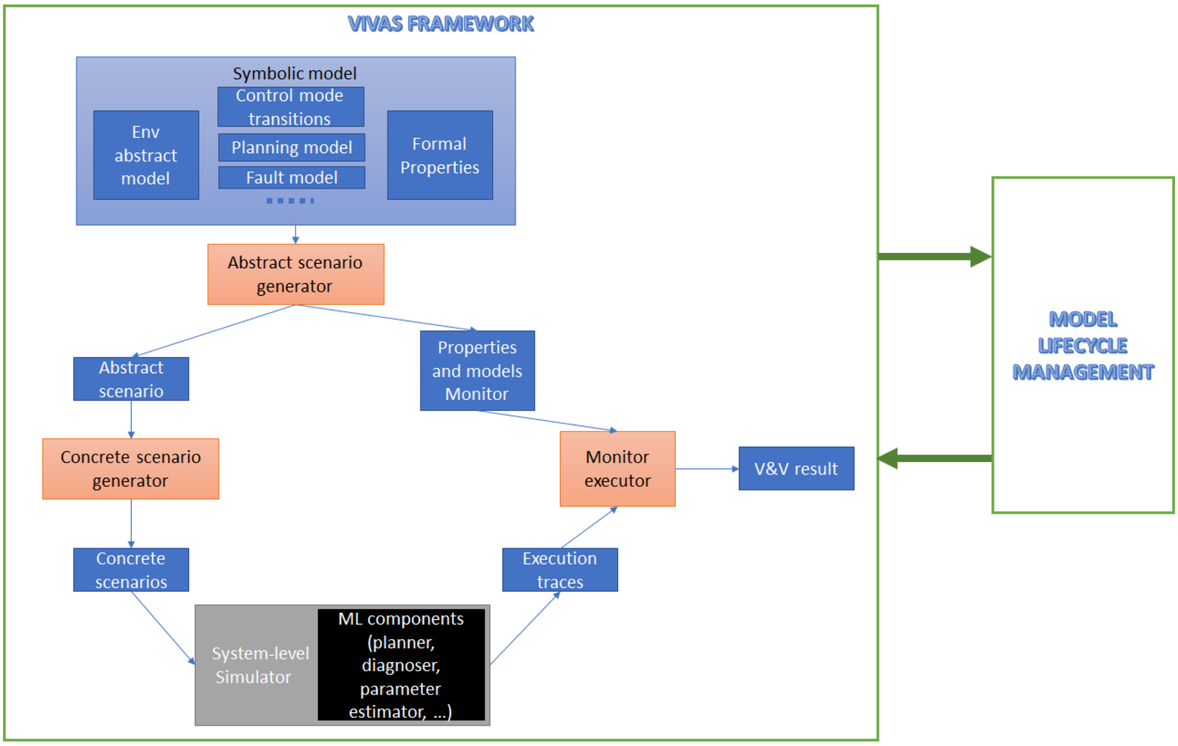

Figure 1 - VIVAS Framework Conceptual Architecture

The architectural design sketched above has been reported in the deliverable "Architectural design of the Verification and Validation framework" [RD-03].

Regarding the use cases definition, it was of preeminent importance to select a challenging scenario in terms of autonomous capabilities and usage of AI/ML models and to define the adaptation of the simulator to support the implementation of the use cases.

We chose to work on a planetary robotic asset as, by its nature, lend itself well to the integration of different on-board ML models since it is characterized by various degrees of uncertainty from its strong interaction with the environment in which it operates via impact, contact and sensing. We considered a typical scenario prepared for a 'sol' execution from the ExoMars planetary exploration mission: the 'Drilling site approach and surface sample acquisition'. In this scenario the rover moves over a grid to execute activities that shall be performed autonomously under the constraints of the available power and temporal constraints. The 3DROV simulator has been used to implement 2 test cases:

- The first use case, namely the "Resource Allocation Estimation", relates to the validation of execution of activities subject to uncertain duration and resource production/consumption estimated via an ML model.
- The second use case, namely the "Novelty Detection in Images for Opportunistic Science" relates to the validation of a rover equipped with an ML model to detect interesting objects in the environment. The rover, while moving over a grid to perform science operations, acquires images and analyse them to identify novel objects, to possibly support opportunistic science.

The ML model to detect objects in the environment has been designed and trained specifically for this activity.

A detailed definition of the use cases and the ML models used have been reported in the deliverable "Identification and definition of the Use-Cases" [RD-02].

3.3 Proof of Concept, Implementation and Demonstration

The Proof-of-Concept implementation task led to the delivery of:

- The VIVAS Framework, a general, domain independent, software implementation of the conceptual architecture in Figure 1. The implemented software architecture is depicted in Figure 2.
- An instantiation of the 3DROV simulator for the proposed use cases.
- An instantiation of the VIVAS Framework for the adapted 3DROV robotic simulator. The instantiation provides:
    - A symbolic model, to represent the interesting features for the proposed test cases
    - A concrete scenario generator, to translate the symbolic scenarios into proper inputs for the specific 3DROV simulator
    - A monitor, to translate the executed traces from the specific 3DROV simulator to check the properties of interest for the proposed test cases
- An image recognition ML model, trained with the 3DROV simulator, subsequently integrated into the adapted simulator

The instantiated framework has been validated on tests cases, implementing test procedures to validate the framework itself and providing examples of testing campaigns for the two test cases.

A detailed description of the implementation and customization of the VIVAS Framework have been reported in the deliverable “PoC Detailed Design” [RD-03]. Tests and validation in the deliverable “PoC Test Report” [RD-05].

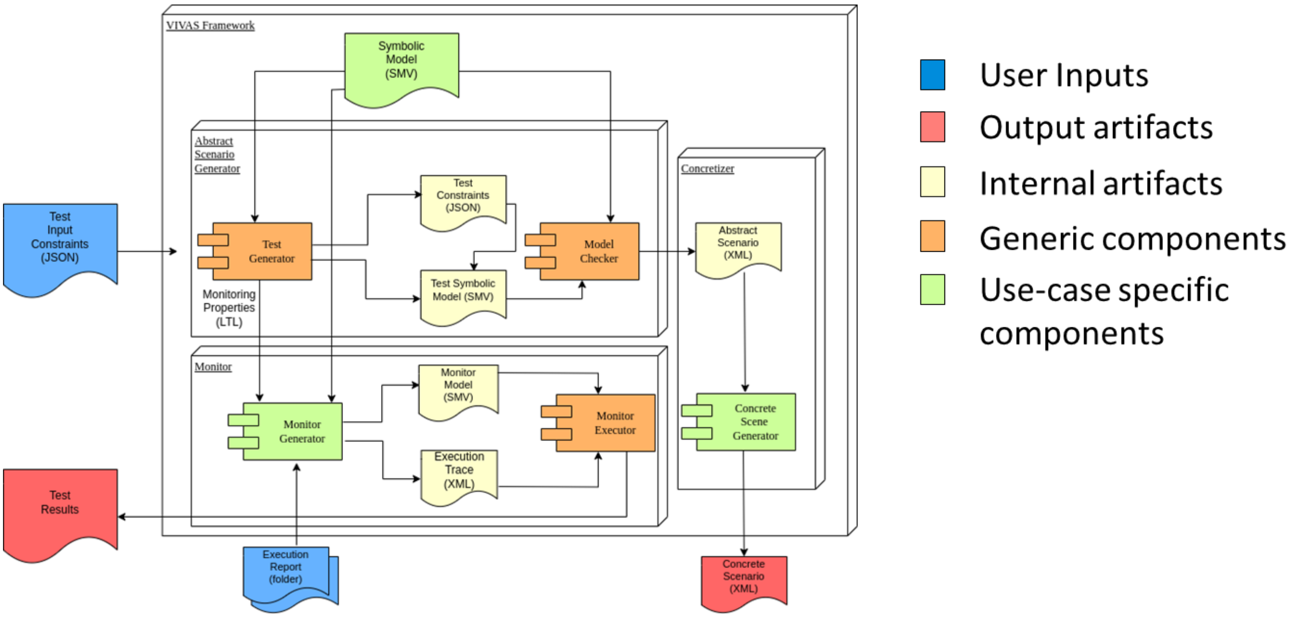

Figure 2 - VIVAS Framework Implementation

3.4 Delivery and Acceptance

The conclusions of this study include recommendations for future work and improvements, as well as considerations for adaptability of the VIVAS Framework on other scenarios. In this task such an analysis has been done, together with the preparation of all the study final deliverables.

4 Conclusions & Achievements

The outcomes of the project can be summarized by the following points:

- An analysis of the state of the art in (1) common practices of testing, V&V of autonomous systems; (2) AI-model life cycle and Quality Model for AI-models and (3) System-level simulators for the verification and validation purposes of AI-models
- A generic Verification and Validation methodology based on the usage of the System-level Simulation Facilities, specifically targeted at autonomous systems using AI-models.
- The VIVAS Framework, a general, domain independent, software implementation of the proposed methodology
- A proof of concept, full instantiation of the VIVAS Framework for the 3DROV robotic simulator
- An image recognition ML model trained for the proof of concept and integrated in the simulator
- Two test cases to demonstrate usage and advantages of the VIVAS Framework. The test cases have been deployed using 3DROV and a planning technology to implement a state-of-the-art autonomous planetary robotic asset.

In conclusion the project demonstrated **the feasibility of a model-based approach to system-level validation and verification of autonomous systems integrating AI/ML components**. This approach complements the validation of the AI/ML model done when the model is designed/trained, supporting the **qualification of AI/ML in operation**. In fact, with VIVAS the model can be tested considering interaction with other subsystems and the disturbances induced by such an integration, as well as the capability of the model to support system-level behaviours, **leveraging the rigorousness provided by the model checking approach**.

As part of future deployments, considering the growing usage of AI/ML technologies in autonomous systems and the paramount importance of operational validation of these technologies, we suggest the Agency (1) to consider a follow-up activity to integrate VIVAS in an MLOps loops for AI/ML models qualification; (2) to investigate the customization of VIVAS in different scenarios; (3) to consider the possible integration of VIVAS into wider future deployments where the V&V can be a building block, like the DT (digital twin) infrastructure for Exomars or the Exomars ground rover control infrastructure.