2nd ESA BLAST Workshop

List of V&V techniques

T1. Deterministic and stochastic mu analysis

Mu analysis is a powerful framework for robust control design and analysis. Deterministic mu analysis assesses the robustness of a system against bounded uncertainties, such as parameter variations and external disturbances. Stochastic mu analysis extends this framework to address uncertainties with probabilistic characteristics. By considering the statistical properties of uncertainties, stochastic mu analysis enables less conservative assessments at the expense of more computationally demanding algorithms.

T2. Sampling-based worst-case analysis

Sampling-based worst-case analysis involves systematically exploring a system's parameter space through high-fidelity simulations. By systematically varying key parameters such as environmental conditions, actuator limitations, and initial conditions, the simulation can identify combinations of factors that lead to the most critical performance degradations. The main challenge of this type of approach is to concurrently minimise the potential for missing critical scenarios and the computational cost of running too many simulations.

T3. IQC and LMI-based analysis

By formulating system properties, such as stability and performance, as Linear Matrix Inequalities (LMIs), efficient convex optimisation techniques can be used to find solutions or to prove infeasibility. This approach enables rigorous analysis of complex systems but requires a very advanced expertise of the underlying theoretical concepts. A particular application of LMI-based analysis is the use of Integral Quadratic Constraints (IQCs), which provide a modular way to represent various types of nonlinearities and time-varying uncertainties.

T4. Nonlinear techniques (CLFs, CBFs, etc.)

Nonlinear techniques move beyond the limitations of linear analysis by directly addressing the inherent nonlinearities of the system dynamics. As an example, Lyapunov theory provides rigorous proofs of stability by constructing energy-like functions that decrease along system trajectories. Control barrier functions can be used to enforce safety constraints, such as preventing actuator saturation or exceeding flight envelope limits. Describing functions enable the analysis of systems with harmonic inputs, providing insights into limit cycle oscillations.

T5. Surrogate modelling

While accounting for dynamical effects such as fuel sloshing and aerothermal plume interactions may be critical for launcher V&V, the complexity and uncertainty of these phenomena render high-fidelity simulation impractical and the derivation of analytical models impossible. In this case, surrogate modelling techniques can be employed to create reduced-order models that capture the essential dynamics and quantify the associated uncertainties. Examples of these techniques include polynomial chaos expansion and Gaussian process regression.

T6. Reachability analysis

Reachability analysis is a formal verification technique that determines the set of all possible states a system can reach under a given set of inputs and initial conditions. In the context of launchers, this translates to analysing whether the vehicle remains within predefined flight corridors or satisfies specific constraints during different flight phases. Reachability analysis is particularly valuable for complex systems where exhaustive testing is often impractical and can identify potential failures and safety violations early in the design process.

T7. Data-driven methods for V&V

Data-driven techniques offer powerful new avenues for GNC V&V. These techniques can analyse vast amounts of simulation outputs, test results and flight data to identify complex patterns and anomalies that traditional methods might miss. Machine learning algorithms can be trained to detect subtle deviations from the expected behaviour. AI-powered tools and anomaly detection algorithms can also be used to automate V&V tasks, freeing engineers for higher-level work and increasing the efficiency and effectiveness of the V&V process.

T8. From autocoding to rapid PIL and HIL testing

Autocoding translates high-level models into production-quality code, in some cases with formal proofs, eliminating manual coding errors and ensuring consistency between design and implementation. The generated code can then be deployed onto a target processor within a simulated hardware environment and onto prototypes in actual flight. An efficient framework to go from autocoding to PIL and HIL allows for rapid and iterative testing of the GNC software against a high-fidelity plant model, enabling early detection of software defects and performance issues.

List of advanced V&V applications

A1. Systems with adaptive elements

V&V of systems with adaptive elements presents unique challenges. It is inherently difficult to guarantee that the adaptive element will never adapt incorrectly and cause harm to the vehicle, and it is even harder to prove that, in case of a failure in adaptation, the controller is still able to recover and ensure stability. As traditional V&V approaches are often insufficient in this case, it may be required to use formal methods for verifying specific properties of the adaptation logic and potentially real-time monitoring to ensure safe and predictable behaviour during flight.

A2. Systems with neural networks

Neural networks represent an important type of adaptive elements due to their strong ability to learn complex, nonlinear relationships from data. However, their inherent "black-box" nature presents challenges for traditional V&V methods, and specialised techniques are required for reachability and robustness analysis. One promising approach is IQC analysis, which allows to characterise the input-output behaviour of the neural network, even in the presence of uncertainties, using frequency-domain inequalities that can be efficiently solved.

A3. Systems with optimisation-in-the-loop

Optimisation-in-the-loop (e.g. real-time optimised guidance) poses additional difficulties due to the dynamic interplay between the system and the optimisation process. In this case, V&V must address the convergence and robustness of the optimisation algorithm, as well as its impact on the overall system behaviour. This includes verifying that the optimiser converges to valid solutions within acceptable constraints and timeframes, and that the inner control loop(s) can cope with a wide range of solutions stemming from distinct initial conditions and model parameters.

A4. Systems with hybrid navigation

V&V of systems with hybrid navigation algorithms using inputs from onboard cameras or LIDARs presents unique challenges as the algorithm’s performance might be severely impacted by the dynamic nature of the environment. These challenges are further compounded by the difficulty of accurately simulating real-world environmental conditions. It is therefore crucial to augment the V&V activities with rigorous testing using synthetic and/or real-world datasets featuring varying atmospheric conditions, sensor noise models and terrain representations.