Verification and Validation for ISHM

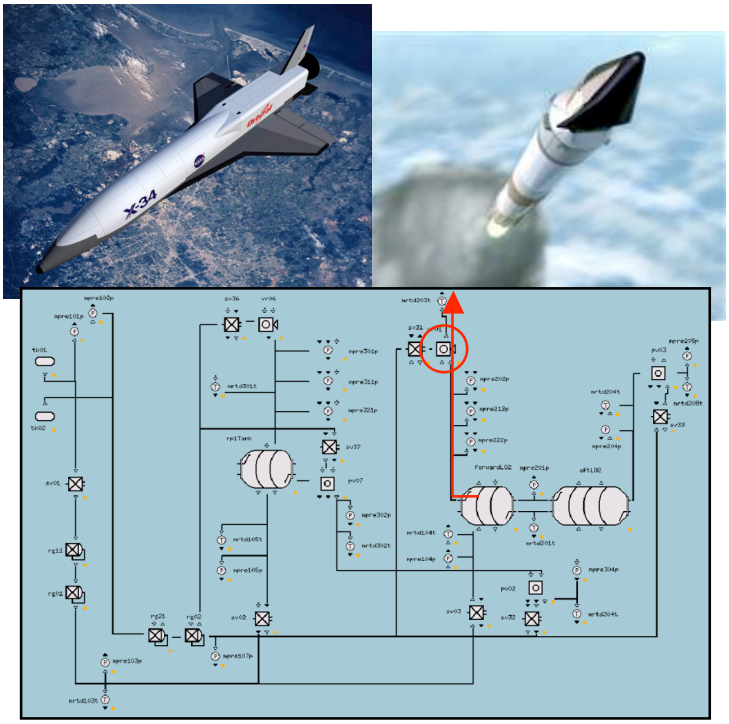
The Automated Software Engineering Group at NASA Ames is developing a comprehensive integrated portfolio of V&V techniques and tools for ISHM systems. This capability is critical to be able to deliver, at competitive cost, a validated V&V process with tool support that can handle the large increase in complexity that results from new ISHM architectures applicable to large systems and broad ranges of operating scenarios.

Background

New ISHM technologies can be applied to systems at a larger scale, can handle a broader range of unforeseen circumstances, and can dramatically reduce the need for human oversight. As the size and complexity of these systems increases, however, the task of software V&V gets more and more complex, to the point that it overwhelms traditional test-based techniques. Several factors contribute to this situation:

- New ISHM systems will cover a wider range of faults, in a wider range of operational contexts, over longer periods. This increases the space of configurations to be verified by orders of magnitude.
- ISHM will substitute for human supervision in some instances, therefore very strong reliability guarantees are needed.
- Innovative ISHM technologies will require adaptation of current development and V&V practices. For example, model-based approaches condense most of the application-specific development in models rather than in the generic programs that interpret or compile them, so the V&V approach needs to be accordingly shifted from the programs to the models.

Very costly final verification can be mitigated by a more formal development process that carries requirements down to the implementation, in a verifiable fashion, supported by appropriate tools. Core V&V technologies are readily available for maturation and integration within the ISHM lifecycle. ISHM and V&V processes and technologies need to be defined and selected in concert, to ensure that V&V is driven by the needs of ISHM applications, and that V&V considerations are infused early on into the ISHM process.



Research Overview

The Automated Software Engineering Group brings together a team of twenty experts in advanced software engineering techniques, with an outstanding scientific track record and covering a broad spectrum of approaches and technologies, from synthesis to verification.

In the area of ISHM systems, we have developed and matured techniques and tools for analyzing and verifying model-based fault protection systems such as the Livingstone system from Ames.

(see reverse)

Verification and Validation for ISHM

Livingstone PathFinder (LPF) is an automated testing/simulation framework for HM subsystems, that expands conventional testing with model checking concepts:

- Increased automation reduces test suite development costs.
- Optimized execution (backtracking) reduces test execution times.
- Modularity allows easy configuration to adjust fidelity, coverage, speed, focus, …

Livingstone Model Verifier (LMV) allows a full formal verification for HM models:

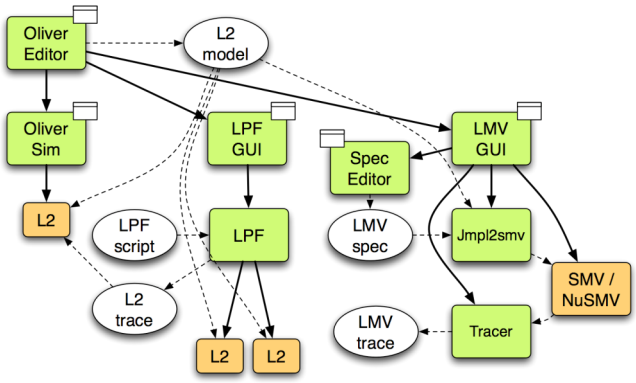
- Feeds HM models to automated, powerful Verifiers (symbolic model checking).
- Can detect and eliminate modeling errors or flaws that might lead to improper diagnosis.
- Symbolic reasoning allows exhaustive analysis of very large state spaces (10^{50+}).
- Front-end hides away details of the Verifier.

Diagnosability Verification verifies that faults are detectable/identifiable from available observable data:

- Based on model-based verification using symbolic model checking.
- Application in FTA analysis, sensor placement, model-based diagnosis.

These tools feature a user-friendly graphical front-end, have been integrated with other HM design tools and have been demonstrated on real-size HM applications such as an In-Situ Propellant Production system from KSC and the X-34 propulsion feed sub-system.

We have also developed a tool, techniques, and a software process to perform design-time analysis, verification and validation, and dynamic monitoring of adaptive controllers. This monitoring (providing a measure about its current performance) is vital for reliable and safe operation in unknown and changing environments. Our approach has been successfully demonstrated on adaptive flight control systems for the F-15 aircraft.



More broadly, our V&V solutions for ISHM can build on on a comprehensive portfolio of software engineering expertise and technologies available within the ASE group, including:

- Model Checking (Java PathFinder),
- Compositional Verification (automated assume-guarantee reasoning),
- Static Analysis (C Global Surveyor),
- Runtime Monitoring (Java Path Explorer, Eagle),
- Program Synthesis (AutoBayes, AutoFilter).

Relevance to Exploration Systems

ISHM is Innovative V&V is a key enabling technology to the sustainable deployment of advanced ISHM, which is a major technology area for the CEV and other exploration vehicles and robots.

H&RT Program Elements:

This research capability supports the following H&RT program /elements:

- ASTP/ASCT (Technology-Systems V&V)
- ASTP/SISM (Software Stds, Tools and Envs)
- TMP/SPST (ISHM)

Points of Contact:

Dr. Michael Lowry (NASA)
650-604-3369; lowry@email.arc.nasa.gov

Dr. Allen Goldberg (Kestrel Technologies)
650-604-4858; goldberg@email.arc.nasa.gov

Dr. Charles Pecheur (RIACS)
650-604-3588; pecheur@email.arc.nasa.gov
http://ase.arc.nasa.gov/pecheur

Ames Research Center

NASA