Validation & Verification for Emerging Avionic Systems

Gregory S. Tallant, James M. Buffington, Walter A. Storm, Peter O. Stanfill
Lockheed Martin Aeronautics Company
Fort Worth, Texas
{greg.s.tallant|james.m.buffington|walter.a.storm|peter.o.stanfill}@lmco.com

Bruce H. Krogh
Carnegie Mellon University
Pittsburgh, Pennsylvania
krogh@ece.cmu.edu

1. INTRODUCTION

This position paper reports findings from the project Verification & Validation of Intelligent and Adaptive Control Systems (VVIACS) [1]. Flight-safety-critical system software is any software that controls or monitors hardware whose reliability, location, or performance directly impacts the areas of (1) probability of loss of control (PLOC), (2) survivability, (3) aircraft performance, and (4) crew safety. Testing of flight-critical software is oriented to the verification of these four high-level requirements, and any software errors that remain after testing are not considered flight critical.

For current systems, control law, software implementation, and test comprise over 60% of total development costs. This percentage will be even higher using current verification and validation (V&V) strategies on emerging autonomous control systems. Although traditional certification practices have historically produced sufficiently safe and reliable aircraft control systems, they will not be cost effective for next-generation autonomous control systems due to inherent size and complexity increases from added functionality.

As emerging safety-critical systems become more complex, system certification costs will increase exponentially due to a projected increase in required testing resources. Planned test automation improvements will certainly reduce testing hours but may not sufficiently reduce them for emerging control system requirements. Rigorous verification of the PLOC requirement may not be cost effective in the presence of these system enhancements.

The VVIACS study was undertaken with the following technical objectives:

- Classify emerging safety-critical control systems by their inherent fundamental characteristics that challenge traditional certification practices;
- Develop and demonstrate preliminary V&V strategies that focus on critical schedule and cost points within flight certification;
- Identify critical, high-payoff V&V process, tool, and method technologies for further development.

The primary benefit of achieving these objectives is enabling cost-effective, rapid development of safe and reliable autonomous safety-critical systems.

2. APPROACH

Our approach centered on exploiting key interactions between V&V and flight certification of safety-critical autonomous control systems. Feasible V&V strategies that improve flight safety while reducing software development and life-cycle costs (LCC) were developed. We also developed representative system models and software implementations that captured critical attributes of advanced safety-critical systems to be used in the evaluation of the V&V methods.

V&V process, tool, method, and technology that impacted all phases of system development we considered. Early development phase activities focused on the initial translation of requirements into concrete design artifacts such as model-based design environments, formal specification techniques [2], and advanced V&V-aware design techniques [3], [4]. Mid-phase development activities included the expression of a design into executable software and preliminary testing and verification such as control analysis [5], [6], software implementation [7], and formal V&V [8]-[11]. Late development phase activities focused on test and review for certification and may be impacted by improvements to automated test [12] and process-based certification.

We completed technology roadmaps for promising V&V technologies based on well-established methodologies and fundamental principles and approaches in the literature [13]. We completed a technology maturation plan for each of the emerging technologies identified during the program. We also provided detailed information and roadmaps for the continued investment and development of the innovative V&V technologies for the purpose of making the technologies ready for the certification of emerging advanced control systems.

The critical path schedule includes approximately 100 tasks that span the development cycle and define the starting and ending days, duration, and dependencies of each task. For the refined cost model, we categorized costs using the following functional disciplines: system (SYS), stability and control (S&C), control laws (CLAW), software (SW), simulation (SIM), test tool development (TTD), test (TEST), hardware procurement and analysis (HWPA), hardware (HW), and other (OTHER). The total system development cost was then allocated to each functional discipline using percentages based on data from the industry team members (Figure 1).

Fundamental properties which were considered to be included in the baseline system development model were categorized as baseline fundamental properties (BFPs). All remaining fundamental properties were categorized as emerging fundamental properties (EFPs).

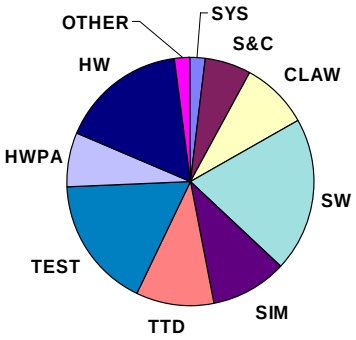

Figure 1 – Percentage Development Cost by Functional Discipline

We identified opportunities to improve the existing development process by reducing iterations, combining steps, and implementing a reliability growth (*i.e.*, build a little/test a little) philosophy. In general, our approach was to make the current process more cost-effective from a development and maintenance perspective by: (1) eliminating, reducing, and/or combining tasks where reasonable (*e.g.*, through automation); (2) early detection of defects; (3) minimizing the dependence of methodology requirements on specific technologies; and (4) implementing acquisition reform principles with subcontractors.

Once the process improvement opportunities had been identified we developed a list of the V&V technologies required to realize these process improvements. This technology list was based on tools and methods previously identified by team members and included existing commercially available tools, research tools and/or methods currently under development, and proposed tools and/or methods with low maturity levels. Each V&V technology was then classified as either a near-term technology (mature in 1 to 3 years), a mid-term technology (mature in 4 to 6 years), or a far-term technology (mature in 7-9 years).

3. RESULTS

Based on our analysis, EFPs are projected to significantly increase V&V costs (Figure 2). From Figure 2, we see that V&V costs for the single-vehicle emerging control systems (ECS) are projected to increase approximately 2 times and for the multi-vehicle ECS approximately 3 times. The largest increases are in the software (200%) and test (250%) functional disciplines for the multi-vehicle ECS. Cost grows approximately exponentially as complexity increases within these functional disciplines.

As expected, our analysis confirms that as the complexity of the emerging control systems increases the cost, schedule, and risk impacts will also increase. Cost, schedule, and risk will grow at a faster and faster rate (possibly exponentially) as complexity increases.

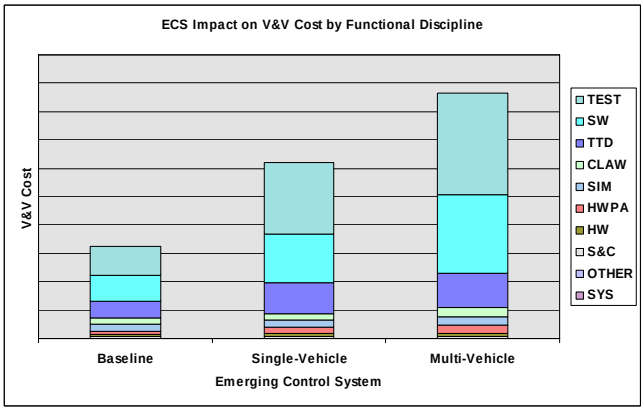

Figure 2 – Emerging Control System Impact on V&V Costs by Functional Discipline.

The greatest impact on V&V occurs in the software (SW), test (TEST), and test tool development (TTD) functional disciplines. Efforts to reduce impact in other functional disciplines will have very little significant impact on overall system development. This does not mean that the other functional disciplines can be ignored. It simply means that the percentage of the tasks in the other functional disciplines that are V&V related is not significant. Tool, method, or process research and development in functional disciplines other than SW, TEST, and TTD will only have a significant positive impact on development if they reduce the cost and/or schedule duration of the tasks in the SW, TEST, and TTD functional disciplines.

The following 15 V&V technologies were identified as having the potential to impact the development cycle:

Near-term (1-3 yrs.):

- Auto-code
- Auto-test
- Rapid prototyping
- System model-based development
- Automated verification management
- Simulation-based design

Mid-term (4-6 yrs.):

- Formal requirements specifications
- Requirements and traceability analysis
- Formal methods
- Computer-aided system engineering

Far-term (7-9 yrs.):

- V&V run-time design
- Rigorous analysis for test reduction
- Requirements and design abstraction
- Probabilistic/statistical test
- Testing metrics

Based on our analysis, the V&V technologies will significantly reduce both the growth and rate of growth in system development costs (Figure 3). Referring to Figure 3, we see that use of the advanced V&V technologies will reduce system development costs for the baseline system by 25%, the single-vehicle ECS by 33%, and the multi-vehicle ECS by 35% when compared to the current process. Even though the cost continues to grow with increasing complexity, the rate at which both cost and schedule grow is reduced significantly when advanced V&V technologies are used.

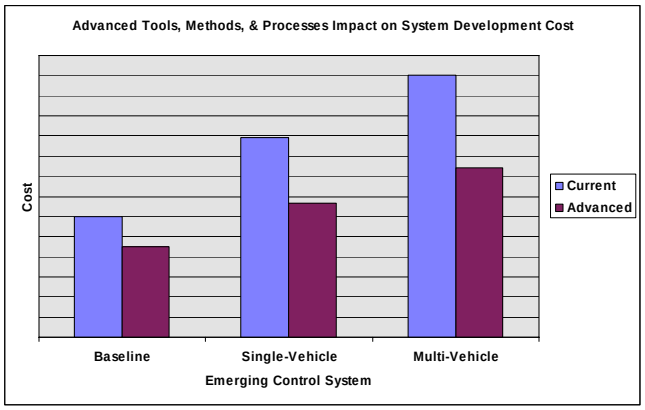

Figure 3 – V&V Technologies Impact on System Development Cost

For the existing development process, 80% of the composite V&V impact occurred in the software and test functional disciplines for both the single- and multi-vehicle ECS projects. When advanced V&V technologies are used as a part of the development process, 80% of the composite V&V impact now occurs in the test, control law, and test tool development functional disciplines. In addition, a redistribution across functional disciplines occurs through a reduction in the number of design iterations, combining steps in the design process, and use of the reliability growth approach (build a little/test a little) to shift the emphasis on V&V to earlier stages of the development process

In summary, use of advanced V&V tools, methods, and processes that are focused on the V&V tasks associated with the high impact functional disciplines (*i.e.*, SW, TEST, & TTD) will significantly reduce the V&V cost and effort required to develop advanced safety-critical emerging control systems. The resulting reductions in V&V cost and V&V effort will result in significant reductions in overall system development costs and schedule.

We prioritized our list of V&V technology needs (Table 1) by developing a technology maturation plan for each technology identified during the strategy development task. We then performed a cost-benefit analysis on the technologies using the results obtained from the proof of concept task (net benefit) and data contained in the maturation plans (technology development cost). Note that the only near-term technology included in the final prioritized list is Automated Verification Management. The other near-term technologies were removed from the ranking process because these technologies are relatively mature (moderate technical risk) and significant industry investment in these technologies is ongoing and is expected to continue for the next 5-10 years.

Table 1 – Prioritized V&V Technologies

PRIORITY	V&V TECHNOLOGY
1	Automated Verification Management
2	Formal Requirements Specifications
3	Requirements and Traceability Analysis
4	Formal Methods
5	Probabilistic/Statistical Test
6	Requirements and Design Abstraction
7	V&V Run-Time Design
8	Testing Metrics
9	Rigorous Analysis for Test Reduction
10	Computer-Aided System Engineering

5. CONCLUSIONS

We have identified and prioritized a set of V&V technologies that significantly reduce the development cost and compress the development schedule of emerging safety-critical flight control systems. Our approach was based on a comprehensive system development and operational perspective and sound system engineering principles. We have compiled a database from which the industry at large may draw upon and identified a set of representative emerging control systems which were utilized for V&V technology development and technology maturation planning. Details are available in [1].

ACKNOWLEDGMENTS

The VVIACS project was funded by the Control Sciences Division in the Air Vehicles Directorate at the Air Force Research Laboratory under contract F33615-02-C-3206. The Program Manager was V.W. Crum. The authors also acknowledge the contributions of the VVIACS team members: R.A. Hull, Lockheed Martin Missiles & Fire Control; P. Bose, Lockheed Martin Missiles, and Space; T. Johnson, General Electric Global Research Center; and R. Prasanth, Scientific Systems Company, Inc.

REFERENCES

[1] Tallant, G.S., Buffington, J.M., and Krogh, B.H. Validation & Verification of Intelligent and Adaptive Control Systems, Final Project Report, Lockheed Martin Aeronautics Company, Fort Worth, TX, December 2005.

[2] Gluch D. and Weinstock, C., "Model-Based Verification: A Technology for Dependable System Upgrade," CMU/SEI-98-TR-009, ADA 354756.

[3] Seto D., Krogh B., Sha L., Cury J., Chutinan A., and Biswas A., “Safe Online Control Upgrades with the Simplex Architecture – A Hybrid System,” Hybrid Systems and Autonomous Control Workshop.

[4] Prasanth R. K., , Boskovic J. D., and Mehra R. K., “Development of Assurance Techniques for High-Confidence Flight Software Design for Autonomous Unmanned Air Vehicles,” DARPA Phase I SBIR final report, SSCI Report No:1311, 2001.

[5] Boskovic J. D. and Mehra R. K., “Computer Simulation Analysis for Reconfigurable Flight Control Design,” 2002 AIAA Modeling and Simulation Conference and Exhibit, Monterey, California, August 2002, AIAA-2002-4787.

[6] Davis M. H. A., *Markov Models and Optimization, Monographs on Statistics and Applied Probability*, Vol. 49, Chapman and Hill, New York, 1993.

[7] Rimvall C.M., Spang H.A. III, Farrell, J.A., Radecki M., and Idelchik M., “An open architecture for automatic code generation using the BEACON CACE environment,” IEEE/IFAC Joint Symposium on Computer-Aided Control System Design, p. 315-320, 1994.

[8] Henzinger T.A.; Pei-Hsin Ho; Wong-Toi, “HYTECH: a model checker for hybrid systems,” *International Journal on Software Tools for Technology Transfer*, vol.1, no.1-2 p. 110-22, Dec. 1997.

[9] McMillan, “Symbolic model checking: an approach to the state space explosion problem,” Carnegie Mellon University, School of Computer Science, Ph. D. Thesis, 1992.

[10] Silva I. and Krogh B., “Formal verification of hybrid systems using CheckMate: a case study,” 2000 American Control Conference, Chicago, June 2000.

[11] Prasanth R. K., , Boskovic J. D., and Mehra R. K., “Mixed integer/LMI approach to low level path planning,” Proceedings of the American Control Conference, May 2002.

[12] Blackburn M., Busser R., Nauman A., “Removing Requirement Defects and Automating Test,” 2001 Software Productivity Consortium.

[13] Garcia M. L and Bray O. H., “Fundamentals of Technology Roadmapping,” Sandia National Laboratories Unlimited Release Document, SAND97-066