Verification, Validation, and Certification of Aerospace Control Systems

Today's Control Systems

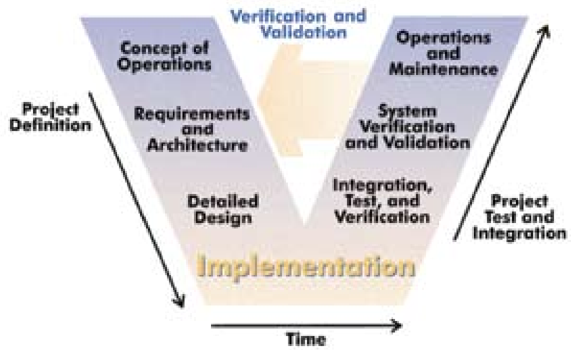
The development of control systems from concept to validation is a complex, multidisciplinary activity. For applications where certification is required prior to operation, specifically aerospace systems, the control laws must go through a rigorous verification and validation process. This process subjects the control laws to a wide variety of analysis and tests to ensure that they will function properly under both nominal and failure conditions. The development process, characterized by numerous iterative design and analysis activities, is lengthy and costly.

Today's safety-critical flight control systems, control laws, software implementation, and tests account for over 60% of the total development cost. (Source: Lockheed Martin Aeronautics Company)

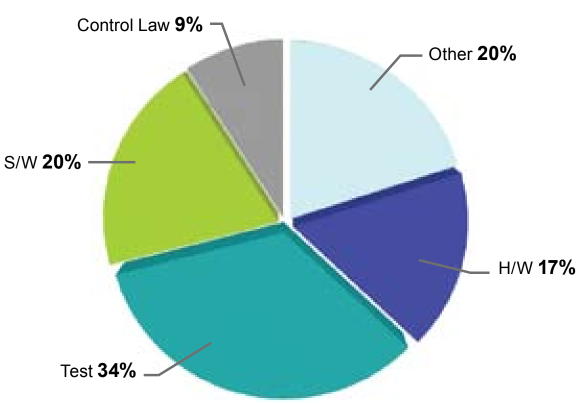
Future Control Systems . . .

For future aeronautics and space applications, the design of the control systems is predicted to include autonomous features such as automated mission planning, target selection and mission replanning, multivehicle cooperative control, situation awareness and automatic collision avoidance, and adaptative and reconfigurable control with diagnostic and prognostic health functionalities.

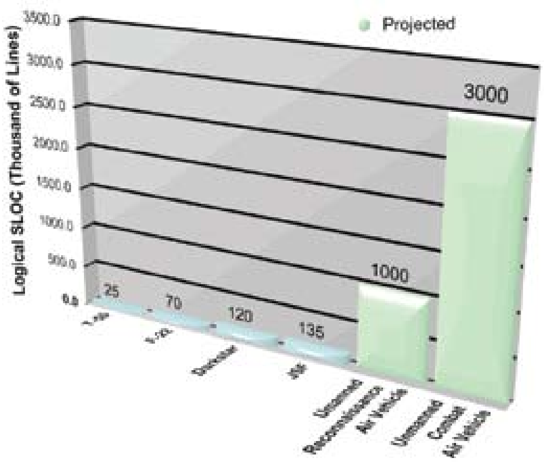
Although the traditional verification, validation, and certification process is producing sufficiently safe and reliable control systems today, it will not be technically adequate and cost-effective for managing the design complexity and safety requirements of future aerospace control systems and for certifying their embedded software. The cost, schedule, and risk impacts are likely to increase exponentially.



A common view of the development timeline
Source: NASA Aviation Safety Program



Typical development cost breakdown for safety-critical flight control systems



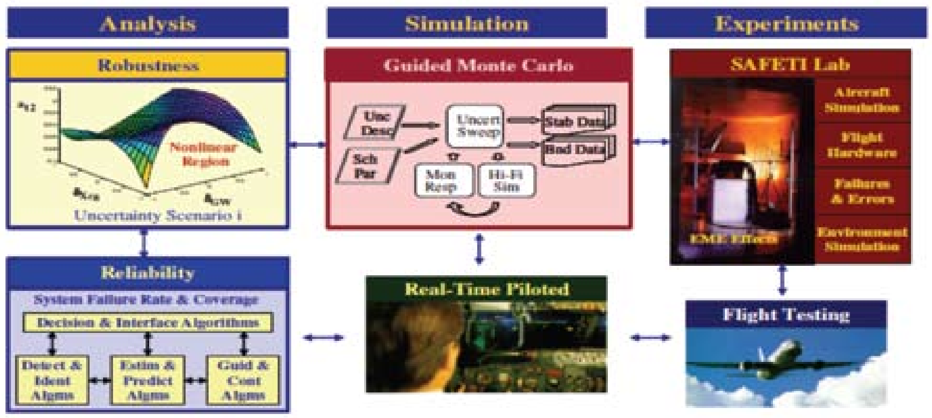
Complexity growth, as measured by logical software lines of code, of future safety-critical flight control systems (autonomy)
Source: Lockheed Martin Aeronautics Company

Contributor: Christian Philippe, European Space Agency, The Netherlands

Closing the Gap Between Future Needs and Certification

The need for engineering tools, methods, and techniques that make V&V cost- and time-effective while applicable to a broad range of aerospace vehicle and airspace systems is widely recognized. An integrated validation process involving analytical, simulation-based, and experimental methods appears to be the most promising approach for coping with the complexity of future control systems. In this process, the analysis results (for example, robustness, worst-case analysis) are used in guided Monte Carlo simulation evaluations and in defining test scenarios for closed-loop real-time simulation with hardware-in-the-loop and flight tests whenever possible.

With regard to worst-case analysis, the use of mixed global/local optimization techniques such as the differential approach augmented with local optimization methods could significantly improve the reliability and efficiency of the current flight clearance process. The use of randomized algorithms and probabilistic methods for robustness design and analysis of control systems affected by random uncertainty could also contribute to the improvement of the traditional V&V process. For the verification and validation of intelligent and autonomous control systems, NASA has proposed a method based on mixing local linear analytical techniques with global random search algorithms.



Integration of analytical and simulation methods for validating vehicle health management and control upset prevention and recovery technologies. Source: NASA

Challenges and Benefits

Control will play an important role in the successful deployment of advanced verification and validation technologies in the aerospace industries. Numerous challenging (and potentially rewarding) problems will need to be addressed by control scientists and engineers.

The main industrial benefits for advanced verification and validation technologies (including theory, methods, and engineering tools) are a reduction of the time-to-market and associated development cost while achieving sufficiently reliable results. Alternatively, V&V technologies could provide increased reliability of the analysis results for reasonable additional effort.