

An Overview of the V&V of Flight-Critical Systems Effort at NASA

2011-01-2560

Published
10/18/2011Guillaume Brat
NASA

Copyright © 2011 SAE International

doi:[10.4271/2011-01-2560](https://doi.org/10.4271/2011-01-2560)

ABSTRACT

As the US is getting ready for the Next Generation (NextGen) of Air Traffic System, there is a growing concern that the current techniques for verification and validation will not be adequate for the changes to come. The JPDO (in charge of implementing NextGen) has given NASA a mandate to address the problem and it resulted in the formulation of the V&V of Flight-Critical Systems effort. This research effort is divided into four themes: argument-based safety assurance, distributed systems, authority and autonomy, and, software intensive systems. This paper presents an overview of the technologies that will address the problem.

INTRODUCTION

These past few years, the US has started modernizing its air transportation system through an effort, known as the Next Generation Air Transportation System (NextGen). NextGen has been mandated by the US Congress with the goals [1] of retaining U.S. leadership in global aviation, expanding capacity, ensuring safety, and protecting the environment, through a cost beneficial implementation. To coordinate development and implementation of the Next Generation Air Transportation System by 2025, the US Congress created the Joint Planning and Development Office (JPDO), a multi-agency public/private initiative.

NextGen will require innovative changes to concepts of operation, demanding the implementation of complex software systems coupled with advanced hardware and communications capabilities. The validation and verification of these complex operational and technological developments has been identified by the JPDO as a critical gap for the implementation of NextGen [1]. Thus, The Research & Development activity R-1440, entitled “Applied Research on

Complex Systems Validation and Verification”, states this need as follows:

“Applied research on the methods and algorithms to support the validation and verification of complex systems. Complex systems provide multiple functions that support many different operating models, environments and technologies and therefore require more advanced and integrated validation and verification methods and algorithms beyond those used for less complex systems. This research will support the development of complex systems, their risk assessment and eventual certification decisions.”

The JPDO also listed a corresponding enabler, called EN-3050 Advanced Complex System Validation and Verification Methods, which states the following:

“Advanced tools and processes are developed to improve the verification and validation of complex systems and software. Improvements will focus on reducing the time and resources needed to conduct validation and verification as well as improving the quality of the results.”

At the request of the JPDO, and as a member of the JPDO, the National Aeronautics and Space Administration (NASA) has been charged to address this critical gap in V&V of complex systems. Thus, the NASA Aeronautics' Aviation Safety Program has examined the research required to develop transformative safety validation and verification methods required to rigorously assure the safety of Next Generation Air Transportation System developments in a time- and cost-effective manner.

This article summarizes its findings and describes the resulting execution plan. We first motivate the need for better V&V for complex systems by describing how the increase in

system complexity and the V&V cost drivers led us to divide the research into four important themes: argument-based safety assurance, distributed systems, autonomy & authority, and software intensive systems. The bulk of the paper is a description of each of these themes. It borrows heavily from the VVFCs study report, called Validation and Verification of Flight Critical Systems: Assessment of Critical Research Activities.

OVERVIEW

Current flight-critical systems are already so complex that they pose significant challenges to safety assurance; [Table 1](#) shows the increase in software size (and complexity) for some well-known aerospace systems. For example, it is impossible to fully demonstrate safety in all possible operating conditions. Furthermore, the cost and time required by traditional V&V methods are prohibitive, and in many cases, they prevent the introduction of new technologies such as the use of adaptive algorithms in control. Yet, the operational improvements proposed under NextGen plans will increase the complexity of flight-critical systems and therefore reduce the current safety margins. Therefore, NextGen forces us to expand the traditional V&V strategy based on testing.

Table 1. Estimation of software complexity for some aerospace systems.

Mars Reconnaissance Orbiter	0.5 MLOC
Orion Primary Flight System	1.2 MLOC
F-22 Raptor	1.7 MLOC
Boeing 777	4 MLOC
Boeing 787	6 MLOC
F-35 JSF	>10 MLOC

The NASA study identified four general factors, which are outlined here:

- *The safety levels demanded of flight-critical systems are unique and unprecedented.*
- *Flight-critical systems span a range of design elements, including air, ground, and space. They involve human-human, human-automation, and automation-automation interactions with varying authority and autonomy constructs.*
- *Flight-critical systems are increasingly distributed (i.e., functions are delegated to individual components) and integrated (i.e., disparate components are providing information and functions to, and acting upon information and functions from, other components).*
- *Flight-critical systems are increasingly software-based, and that software is increasing in complexity.*

Besides the specific needs of complex systems, we are currently limited in our ability to perform V&V of flight-

critical systems. For example, the current cost of V&V is enormous, especially given the requirements imposed by the certification process. Informal discussions with the FAA reveal that the verification cost to meet the DO-178B standards for level-A software (i.e., systems for which failures can have catastrophic consequences) can represent as much as seven times the development cost. Furthermore, V&V is not incorporated into the earliest stages of design, system development, during which V&V is actually less costly than in other stages, as shown in [2] by Barry Boehm and confirmed by industry during our study. Finally, V&V is often cited as an obstacle to innovation [3]. The cost and programmatic risk inherent to V&V can provide a business case against implementing new capabilities such as adaptive control, software with stochastic elements, or for novel air traffic concepts of operation that are highly distributed and interactive.

The VVFCs capabilities will advance safety assurance for flight-critical systems over their life cycle, to foster innovation within the air transportation system. The following four critical challenge areas have been identified:

- **Argument-based Safety Assurance:** ensuring safety in NextGen requires a comprehensive safety assurance framework applicable to NextGen operational concepts and to all its components and their interactions, wherever they reside - in the air, on the ground, or in space. Such a framework must address the increased complexity of NextGen and provide a consistent approach to safety assurance across all scales from specific components to airspace operational concepts.
- **Distributed Systems:** Critical aircraft system functions increasingly integrate (and are distributed across) multiple aircraft systems. Likewise, important airspace system functions increasingly integrate across multiple air and ground elements. This distributed nature can provide robustness, but can also be fragile when component interactions result in unintended consequences. Thus, capabilities to ensure the safety-critical properties of distributed systems need to be enhanced.
- **Authority and Autonomy:** tools are needed to assess whether advanced operational constructs properly assign authority and autonomy between automation and humans and whether such assignments are safe.
- **Software Intensive Systems:** The dependence on and complexity of software in the air and ground based components of the system will increase substantially with NextGen. There is a need to improve the effectiveness (and lower the cost) of assessing whether software meets safety objectives.

As mentioned above, new V&V methods should permit their application starting in the earliest stages of the design process and continuing throughout the remainder of the system's life