SOFTWARE V & V TOOLS – AN ASSESSMENT PROGRAM

Dr. Pio V. de Feo
NASA Ames Research Center
Moffett Field, CA 94035

ABSTRACT

Significant progress has been made in recent years in the area of software verification tools. However, their utilization in the verification of Digital Avionics Systems has been very limited. The primary reason for this is the lack of data proving the cost effectiveness of these tools.

NASA has started a program to fully and quantitatively assess the impact of including advanced software verification and validation (V & V) tools in the verification of Digital Flight Control Systems (DFCS) software for commercial applications; the technical capabilities as well as the financial implications of these tools will be analyzed. An outline of the program and of its primary motivators is presented.

BACKGROUND

A significant shift from analog to Digital Flight Controls is occurring in recent civil aircraft developments due to improvements in life cycle cost and the ability to perform complex functions. These systems have great potential for improving aircraft performance and cost of operation; however, the reliability requirements can be very high for systems which perform critical functions such as low visibility landings, and relaxed static stability, etc. The reliability requirements are established by the ceritification agencies based upon:

1. The probability that the loss of the system will induce a catastrophe (loss of life);
2. The exposure time of the system.

As an example, the reliability required for critical autoland systems, which have an exposure time of less than one (1) minute per flight, is significantly less than the reliability requirements for flight critical systems, like advanced relaxed static stability, which is 10^{-9} failures/hour. These reliability requirements are satisfied by configuring the hardware in redundant configurations; however, although not explicitly stated, the software is assumed to be free of errors and is handled as a component with a zero failure rate; as a result, the software in most redundant configurations is the primary source of single point failures. The verification of the software of flight critical DFCS is therefore an extremely challenging task; the challenges are further increased by the need to keep the verification cost within reasonable limits.

The present V & V technology for DFCS is primarily based upon extensively exercising the systems in closed-loop, real-time simulations where the actual operational environment is simulated to a degree of fidelity which reflects the objectives of the test. The technique is very comprehensive; in fact, it is capable of detecting any type of errors, from specification errors to coding errors. The avionics and airframe companies have significant experience in the use of this technique and practically every digital system which has been flown was verified primarily using this technique; however, the technique is not perfect and errors which were undetected during the verification were

later found during the operation of those systems. The technique cannot guarantee consistent results; and, actually, the quality of the test is in large part dependent on the intelligence and dedication of the analysts who performed the tests. The actual test coverage is not quantifiable; and, in fact, much time can be spent in testing over and over again the same programs, routines, or logic paths while others have never been executed. Finally, the technique is expensive; sophisticated iron-bird simulations are costly to develop and operate and their use should be limited to very specific and well planned test objectives.

PROGRAM OBJECTIVES

In recent years significant progress has been made towards a better understanding of the entire software development process and the challenges involved in each phase of this process. It is generally agreed that the early phases of the process, the specification, the requirement, and the design phase have the greatest impact on the quality and the correctness of the final product. However, the most significant progress has been made in the area of the software verification tools which can be applied only after code generation; these tools are generally classified as static tools, which do not require the flight software to be executed, and dynamic tools which do require it. The theoretical feasibility of many software verification tools has been demonstrated, several have already been developed, and some have also been applied to software programs of medium size. In spite of this obvious progress, the airframe and avionics companies show very little enthusiasm for the new technology and are reluctant to include it in the verification process. The primary reasons for this are: The tools are poorly understood; very limited quantitative data are presently available relative to their error detection capabilities and their operating cost; the poor level of development of most tools; the poorly designed operational environment.

The primary purpose of this program is to perform a quantitative assessment of the operating cost and of the technical capabilities of these tools within the context of Digital Flight Control Systems.

THE PROGRAM PLAN

To meet the program objectives, an analysis must be performed to clearly understand the technical capabilities and limitations and the cost of the present verification technology. The same analysis must then be performed relative to the advanced software verification tools. At the end, the relative advantages and disadvantages of each technique will be defined and an integrated methodology, which includes conventional and advanced techniques, will be proposed.

The program is structured in three phases:

Phase 1: During this phase a quantitative assessment of the present development and verification technology of Digital Avionics Systems will be made. Data will be gathered exclusively from the analysis of recent development programs of Digital Avionics Systems. Specifically, the following will be determined:

P. deFeo
NASA/AMES
2 of 4

(a) The type and frequency of software errors most likely to be present;

(b) The cost to detect, correct, and document these errors and the procedures and techniques used;

(c) The errors most likely to escape detection.

These data will provide a meaningful benchmark, representative of the present technology, against which the capabilities and cost effectiveness of the advanced techniques will be rated

Phase 2: During this phase, a quantitative assessment of the error detection capabilities of the software verification tools will be made. The following is an outline of the activities required to accomplish this objective:

(a) A Digital Avionics System, representative of the near term technology for critical commercial applications, has been procured. The system will be used as a test bed for the software tools.

(b) An initial integrated set of software V & V tools, compatible with the test bed system, is currently under procurement.

(c) The flight software of the test bed system will be randomly seeded with errors consistent, in type and frequency, with the results of the analysis performed during Phase 1.

(d) The error detection capabilities of each tool will then be determined by applying the tools to the seeded software; the percentage of detected errors will be a quantitative measure of the test coverage achievable by each tool. Enhancements will be made, whenever feasible, to increase the original test coverage of each tool.

At the end of this phase, the technical limits and capabilities of the V & V tools will be quantitatively assessed. A technical recommendation for the inclusion of selected tools in the verification process of DFCS can also be made based upon:

(1) The types of errors which each tool is capable of detecting and how thoroughly and consistently each tool performs.

(2) The level of complementarity of coverage and synergism with the conventional verification techniques.

Phase 3: A quantitative assessment of the error detection capabilities of advanced software V & V tools will be performed during Phase 2. The technical capabilities must be the prime consideration for the inclusion of selected tools in the verification process of critical DFCS. However, the willingness or reluctance of the avionics and airframe companies to actually include advanced software V & V tools in their verification programs will be strongly influenced by the economical impact of the tools to the already high cost of verification. The activities in this Phase of the program will aim at a quantitative assessment of the economics of operating the tools. Major cost factors which will be analyzed are: The initial cost of procuring the tools, the cost of adapting existing tools to new environments, the number of systems over which these costs can be amortized, the cost of operating the tools, etc.

P. deFeo
NASA/AMES
3 of 4

The use of the verification tools will result in software programs which have fewer errors at the start of the system testing phase. This could appreciably decrease the efforts needed in the area of closed-loop, iron-bird simulation analysis. These simulations are very expensive to build and even more expensive to run due to the high personnel support they need. A more efficient use of these facilities could be a major cost savings factor induced by the utilization of the tools. Additional savings should be realizable because the tools promote error detection at a very early phase of the coding process; this minimizes the economical impact of the errors and their documentation process. If the errors were detected later, the process would be significantly more expensive because the configuration would be more formally controlled.

All these economic factors will be quantified at the end of this phase.

CONCLUSION

The objective of this program is to fully and quantitatively assess the impact of software V & V tools to the verification of Digital Flight Control Systems for critical applications. The intrinsic complementarity of the tools and their synergism with conventional verification techniques should make feasible and attractive the development of an integrated verification package so that high quality software can be generated at a reasonable cost. An effort will be made, within the scope of this program to specify that package.

P. deFeo
NASA/AMES
4 of 4