

Software and Digital Systems Safety

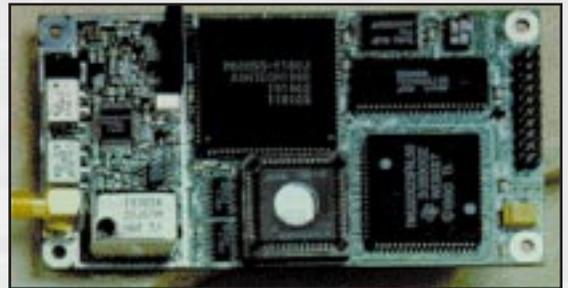
To ensure aircraft safety, the FAA is proactively addressing the increasing complexity of aircraft software and digital hardware.

Civil aircraft are becoming more and more dependent on digital avionics and flight control systems. This is due to new aircraft and avionics designs that incorporate digital computers in systems that are flight critical. If a flight critical system should fail, it may result in the loss of the aircraft. For this reason, the FAA is very concerned about the safety of aircraft using this technology.

The Software and Digital Systems Safety (SDSS) Program addresses this issue by conducting research on constantly emerging complex software and advanced digital hardware technology. The data and results of the research are used to write policy and guidance for certification of new aircraft and systems using this technology. Currently, much of this advanced technology is not directly addressed in FAA regulations. The desired outcome is increased aircraft safety. The SDSS Program is conducting research in the following areas.

Complex Electronic Hardware

The SDSS Program is currently addressing the safety and certification issues concerning highly complex avionics hardware that is being proposed for use in future aircraft and avionics systems designs. The project objective is to conduct a case study using the DO-254 standard developed by RTCA Special Committee #180. This standard provides guidance for design assurance and verification of complex electronic hardware such as application specific integrated circuits (ASICs), erasable programmable logic devices (EPLDs), field programmable gate arrays (FPGAs), etc. These devices have millions of gates and are very difficult to fully test.



Circuit Using Complex Electronic Hardware
(Reprinted with permission from ASHTECH, Inc.)

Commercial-Off-The-Shelf (COTS)

The FAA is conducting a study to develop guidelines, verification methods, and assessment and acceptance criteria for COTS software and hardware. There is substantial concern in the aerospace industry for investigating whether methods are available or could be found for determining the safety of COTS software and hardware for use in airborne systems. COTS software and hardware offer significant cost savings for aircraft manufacturers. There is the potential for increased aircraft safety if lower cost systems could be shown to be safe and serve as a replacement for older, less capable systems.

Software Service History

The aircraft and avionics industry, as well as certification authorities, have expressed a need to expand guidance on what and how much service history data is required for certification credit for previously approved software. Currently, there is limited guidance for either the industry or the certification authorities as to the acceptable duration of the service period, number of hours of service, and definition of normal operation time. The SDSS Program is conducting a software service history study to develop guidelines on the use of such data in aircraft certification.

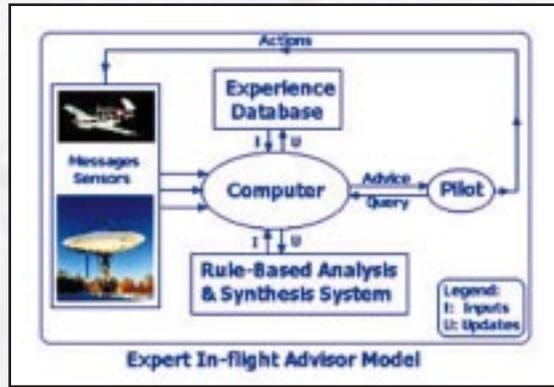
Object-Oriented Technology (OOT)

The FAA and other certification authorities have concerns about the use of object-oriented languages on aviation projects, especially for safety-critical applications. Many companies are beginning to use this OOT.





System Efficiency



The FAA is conducting research to develop policy and guidance for the use of OOT – particularly in the area of verification techniques. The study will document the issues, develop a tutorial or report, and develop criteria for certification authorities to use in evaluating airborne systems manufacturer's use of OOT in developing airborne systems software.

Modified Condition/Decision Coverage (MC/DC) Tutorial

Over the past years, the FAA has conducted research in the area of MC/DC. MC/DC is a verification technique that helps assure that software does not have unintended functionality. The FAA and NASA are using past research, industry experiences, and certification authority experiences to develop a tutorial to encourage accurate application

and evaluation of MC/DC.

In-Flight Advisor

The FAA has conducted a feasibility study to assess the use of artificial intelligence (AI) in alerting the crew of potential emergency situations before they actually occur. The objectives of the In-Flight Advisor project were to specifically determine the feasibility of applying AI methodologies to reduce information overload on the pilot; monitor data from selected components of an aircraft in flight; inform the pilot of potentially critical events occurring or materializing; and advise the pilot of specific actions to be taken in order to delay or avoid potential mishaps. To find out more about the Software and Digital Systems Safety Program, contact:

Airport and Aircraft Safety
Research and Development Division
Aircraft Safety
Research and Development Branch
Flight Safety Research Section

Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405
Phone: (609) 485-6235
Fax: (609) 485-4005
<http://www.tc.faa.gov>