# SOFTWARE DEVELOPMENT ISSUES IN AIRCRAFT SAFETY

**Marina George**[1*], **Jula Nicolae**[2]
Military Technical Academy, 81-83 G. Cosbuc Blvd, Sector 5, Bucharest, Romania

**Cepisca Costin**[3]
Polytechnic University, Bucharest, Romania

**Abstract:** There is no doubt on the importance of onboard computers in nowadays aerospace safety and security. Many crucial aircraft systems rely for their correct operation on complex computer systems. A series of new concepts are being developed specifically to address safety issues in aviation such as controlled flight into terrain, mid-air collisions, or runway incursions. This paper presents from the safety point-of-view some of the software issues that are to be closely regarded and observed for the next generation of aircraft systems.

***Keywords:*** *software, aircraft, safety*

## 1 INTRODUCTION

Any complex digital system is software intensive, and so the correct operation of many aviation systems relies upon the correct operation of the associated software. For any given system reliability requirement software must exceed it because hardware components of the system will not be perfect. The developments of digital aviation systems present many complex technical challenges due the high dependability requirements. After focusing on enhanced functionality versus enhanced safety of such systems we will present some of the issues that arise in aircraft related software development.

## 2. ENHANCED SAFETY VERSUS ENHANCED FUNCTIONALITY

Based on the increasing use of digital systems in aviation, functionality enhancement is taking place in both onboard and ground-based systems. Flight deck automation is very extensive, and this has lead to the use of the term "glass cockpit" since most information displays are now computer displays. Ground based automation is extensive and growing. Much of the development that is taking place is designed to support Free Flight and the Wide Area Augmentation System (WAAS), a GPS-based precision guidance system for aircraft navigation and landing. Both Free Flight and WAAS depend heavily on computing and digital communications.

In many aircraft safety-critical complex digital systems the architecture is a wide-area network with very high dependability and real-time performance requirements.

Three of the major concerns in aviation safety are: (1) accidents caused by Controlled Flight Into Terrain (CFIT); (2) collisions during ground operations, take off, or landing; and (3) mechanical degradation or failure. CFIT was involved in 37% of 76 approach and landing accidents or serious incidents from 1984-97 and CFIT incidents continue to occur. An analysis of the accident causes has suggested that more than two thirds of them might be addressable by automation. Thus, there is a very strong incentive to develop new technologies to address safety explicitly, expressed by various aviation safety programs. The Aircraft Condition Analysis and Management System (ACAMS), for example, is designed to diagnose and predict faults in various aircraft subsystems so as to assess the flight integrity and airworthiness of those aircraft subsystems.

Another important new direction in aviation safety is in structural health monitoring, performing detailed observation of aircraft structures in real time. In future systems, extensive hardware replication will be present to address safety and dependability goals. The software will manage redundant components, to undertake error detection in subsystems such as sensors and communications, and to carry out routine health monitoring and logging. Thus, the fact that large amount of ultra-dependable software will be at the heart of future aviation systems.

## 3 SOFTWARE DESIGN ISSUES

The development of software for future aerospace applications will require that many technical issues be addressed. These issues derive from the required dependability goal and approaches that might be used to meet it. An important aspect of the goal is assurance that the goal is met. We will discuss in this section the most prominent issues.

- *Requirements Specification*

Erroneous specification is a major source of defects and subsequent failures of safety-critical systems. Many failures occur in systems using perfect operating software, meaning that it is just not the software that is needed because the specification is defective.

- *Verification*

Testing remains the dominant approach to verification, but testing is able to provide assurance only in simple systems. A viable alternative to statistical sampling is to use formal verification. However, presently formal verification has limitations, such as floating-point arithmetic and concurrent systems, that preclude its comprehensive and routine use in aviation systems. In addition, formal verification is usually applied to a relatively high level representation of the program, such as a high-level programming language. Thus it depends upon a comprehensive formal semantic definition of the representation and an independent verification of the process that translates the high-level representation to the final binary form.

• *Application Scale*

Building the number of ultra-dependable systems that will be required in future aviation systems will not be possible with present levels of productivity. The cost of development of a flight-critical software system is extremely high. Better synthesis and analysis tools and techniques are required that provide the ability to develop safety-critical software having the requisite dependability with less effort.

• *Commercial off the Shelf Components*

Commercial-off-the-shelf (COTS) components are used routinely in many application domains, with impressive functionality including operating systems, compilers, graphics systems and network services. Unfortunately, COTS components are built for a mass market not for ultra-dependable applications. Furthermore, the source code and details of the development process used in creating a COTS component are rarely available. If COTS components are to be useful in safety-critical aviation applications, it will be necessary to develop techniques to permit complete assurance that defects in the COTS components cannot affect safety.

• *Development Cost and Schedule Management*

Managing the development of major software systems and estimating the cost of that development have always been difficult, but they appear to be especially difficult for aviation systems. Most of the major multi-annual safety – related aerospace programs initiated in the mid '90s exceeded the initially allocated financial and time budgets, transforming this issue in the most critical factor in reaching the desired objectives.

• *System Security*

The future aviation systems will be faced with the possibility of external threats. Present critical networks are notoriously lacking in security. This problem must be dealt with for aviation systems. Even something as simple as a denial-of-service attack effected by swamping data links or by jamming radio links could have serious consequences if the target was a component of the air-traffic network. Far worse is the prospect of intelligent tampering with the network so as to disrupt service. Dealing with tampering requires effective authentication and this issue must be dealt with if aviation systems are to be trustworthy.

## 4. CONCLUSION

The computer – based aircraft systems are dominant and the application scale for future systems is increasing rapidly. If the requisite productivity and dependability goals for these systems are to be met, significant new technology will be required to address the software design issues starting from specifications till validation and qualification.

## REFERENCES

1. ARINC Engineering Services LLC: Aircraft Condition Analysis and Management System. http://avsp.larc.nasa.gov/images_saap_ACAMSdemo.html
2. Federal Aviation Administration: Wide Area Augmentation System. http://gps.faa.gov/Programs/WAAS/waas.htm
3. Honeywell Int'l Inc.: Enhanced Ground Proximity Warning Systems. http://www.egpws.com/
4. Inside The Glass Cockpit: http://www.spectrum.ieee.org/publicaccess/0995ckpt.html.
5. Knight, J.C.: Software Challenges in Aviation Systems, Department of Computer Science, University of Virginia, 2001
6. Marina, G.: Contributions on the Architecture of Aircraft Distributed Data Networks, Ph.D. Thesis, Bucharest 2003.
7. NASA Aviation Safety Reporting System, http://asrs.arc.nasa.gov/
8. National Transportation Safety Board, http://www.ntsb.gov
9. Rockwell Collins Incorporated. http://www.rockwellcollins.com
10. RTCA Incorporated: Software Considerations in Airborne Systems and Equipment Certification. RTCA document number RTCA/DO-178B (1992)
11. U.S. Department of Transportation, memorandum from the Inspector General to various addresses: Status of Federal Aviation Administration's Major Acquisitions. (February 22, 2002) http://www.oig.dot.gov/show_pdf.php?id=701