

Software Challenges in Aviation Systems

John C. Knight

Department of Computer Science
University of Virginia
151, Engineer's Way, P.O. Box 400740
Charlottesville, VA 22904-4740, USA
knight@cs.virginia.edu

Abstract. The role of computers in aviation is extensive and growing. Many crucial systems, both on board and on the ground, rely for their correct operation on sophisticated computer systems. This dependence is increasing as more and more functionality is implemented using computers and as entirely new systems are developed. Several new concepts are being developed specifically to address current safety issues in aviation such as runway incursions. This paper summarizes some of the system issues and the resulting challenges to the safety and software engineering research communities.

1 Introduction

The operation of modern commercial air transports depends on digital systems for a number of services. Some of these services, e.g., autopilots, operate on board, and others, e.g., current air-traffic management systems, operate on the ground. In many cases, the systems interact with each other via data links of one form or another, e.g., ground system interrogation of on-board transponders, and aircraft broadcast of position and other status information [1]. This dependence on digital systems includes general aviation aircraft in a significant way also.

In most cases, digital systems in aviation are safety-critical. Some systems, such as a primary flight-control system [2], are essential for normal aircraft operation. Others, such as some displays and communications systems, are important but only crucial under specific circumstances or at specific times.

Any complex digital system will be software intensive, and so the correct operation of many aviation systems relies upon the correct operation of the associated software. The stated requirement for the reliability of a flight-crucial system on a commercial air transport is 10^{-10} failures per hour where a failure could lead to loss of the aircraft [2, 3]. This is a system requirement, not a software requirement, and so it is not the case that software must meet this goal—software must exceed it because hardware components of the system will not be perfect.

The development of digital aviation systems present many complex technical challenges because the dependability requirements are so high. Some of the difficulties encountered are summarized in this paper. In the next section, aviation systems are reviewed from the perspectives of enhanced functionality and enhanced safety, and the characteristics of such systems are discussed. In section 3, some of the challenges that arise in software engineering are presented.

2 Aviation Systems

2.1 Enhanced Functionality

The trend of reduced digital hardware costs and the coincident reduction in hardware size and power consumption has led to an increasing use of digital systems in aviation. In some cases, digital implementations have replaced older analog-based designs. In other cases, entirely new concepts become possible thanks to digital systems. An example of the former is autopilots. Autopilots used to be based on analog electronics but now are almost entirely digital. The basic ideas behind the operation of an autopilot have remained the same through this transition, but modern digital autopilots are characterized by greater functionality and flexibility. Examples of entirely new concepts are modern full-authority, digital engine controllers (FADECs) and envelope protection systems. FADECs manage large aircraft engines and monitor their performance with sophistication that would be essentially impossible in anything but a digital implementation. Similarly, comprehensive envelope protection is only possible using a digital implementation.

Functionality enhancement is taking place in both on-board and ground-based systems. Flight deck automation is very extensive, and this has led to the use of the term “glass cockpit” since most information displays are now computer displays [4, 5]. Ground based automation is extensive and growing. Much of the development that is taking place is designed to support Free Flight [6] and the Wide Area Augmentation System (WAAS) [7], a GPS-based precision guidance system for aircraft navigation and landing. Both Free Flight and WAAS depend heavily on computing and digital communications.

It is difficult to obtain accurate estimates of the number of processing units, the precise communications architecture, and the amount of software in an aviation system for many reasons. It is sometimes not clear what constitutes “a processor”, for example, because so much specialized electronics is involved. Similarly, software is sometimes in read-only memories and called “firmware” rather than software. In addition, digital systems are often used for non-safety-related functions and so are not of interest. Finally, many of the details of digital systems in aviation applications are considered proprietary and are not made available.

Although some details are not available, it is clear that there are many safety-critical digital systems in present aviation applications. It is also clear that these systems are extremely complex in many cases. Both aircraft on-board systems and ground-based systems are often sophisticated computer networks, and these systems also interact. In some cases, such as WAAS, the architecture is a wide-area network with very high dependability and real-time performance requirements. Given the continuing technological trends, it is to be expected that there will be many more such systems in the future.

2.2 Enhanced Safety

The stimulus for developing new and enhanced digital systems is evolving. While the change from analog to digital implementation of major systems will no doubt continue, there are major programs underway to develop techniques that will address safety issues explicitly [8].

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 occurs when a perfectly serviceable aircraft under control of its pilots impacts the ground, usually because the crew was distracted. CFIT was involved in 37% of 76 approach and landing accidents or serious incidents from 1984-97 [9, 10, 11], and CFIT incidents continue to occur [12]. The prevention of collisions on the ground is a major goal of the Federal Aviation Administration [13].

During the decade of the 1990's, 16 separate accident categories (including "unknown") were identified in the world-wide commercial jet fleet [14]. The category that was responsible for the most fatalities (2,111) was CFIT. An analysis of these categories by Miller has suggested that nine of the categories (responsible for 79% of the accidents) might be addressable by automation [15]. Thus, there is a very strong incentive to develop new technologies to address safety explicitly, and this, together with the rapidly rising volume of commercial air traffic, is the motivation for the various aviation safety programs [8].

These new programs are expected to yield entirely new systems that will enhance the safe operation of aircraft. 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 [16]. The ACAMS system operates with on-board components that diagnose problems and ground-based components that inform maintenance and other personnel.

Another important new direction in aviation safety is in structural health monitoring. The concept is to develop systems that will perform detailed observation of aircraft structures in real time during operation. They are expected to provide major benefits by warning of structural problems such as cracks while they are of insignificant size. The approach being followed is to develop sensors that can be installed in critical components of the airframe and to use computers to acquire and analyze the data returned by the sensors. For an example of such a system, see the work of Munns et al [17].

A significant innovation in ground-based systems is automatic alerts of potential runway incursions. In modern airports, the level of ground traffic is so high that various forms of traffic entering runways being used for flight operations are difficult to prevent. The worst accident in aviation history, with 583 fatalities, occurred in Tenerife, Canary Islands in March 1977, and was the result of a runway incursion. Research is underway to develop systems that will warn pilots of possible incursions so that collisions can be avoided [18].

2.3 Characteristics of Enhanced System

Inevitably, new aviation systems, whether for enhanced functionality or enhanced safety, will be complex—even more so than current systems. Considerable hardware will be required for the computation, storage and communication that will be required, and extensive hardware replication will be present to address dependability goals.

Replication will, in most cases, have to go beyond simple duplication or triplica-

tion because the reliability requirements cannot be met with these architectures. Replication will obviously extend also into power and sensor subsystems.

The functional complexity of the systems being designed is such that they will certainly be software intensive. But functionality is not the only requirement that will be addressed by software. Among other things, it will be necessary to develop extensive amounts of software to manage redundant components, to undertake error detection in subsystems such as sensors and communications, and to carry out routine health monitoring and logging.

The inevitable conclusion of a brief study of the expected system structures is that very large amounts of ultra-dependable software will be at the heart of future aviation systems. It is impossible to estimate the total volume of software that might be expected in a future commercial transport, but it is certain that the number of lines will be measured in hundreds of millions. Not all of that software will be flight crucial, but much of it will be.

3 Software Challenges

The development of software for future aviation applications will require that many technical challenges be addressed. Most of these challenges 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.

In this section six of the most prominent challenges are reviewed. These six challenges are:

- *Requirements Specification*
Erroneous specification is a major source of defects and subsequent failures of safety-critical systems. Many failures occur in systems using software that is perfect, it is just not the software that is needed because the specification is defective. Vast amounts of research has been conducted in specification technology but errors in specifications continue to occur. It is clear that the formal languages which have been developed offer tremendous advantages, yet they are rarely used even for the development of safety-critical software.
- *Verification*
Verification is a complex process. Testing remains the dominant approach to verification, but testing is able to provide assurance only in the very simplest of systems. It has been shown that it is impossible to assess ultra-high dependability using testing in a manner reminiscent of statistical sampling, a process known as life testing [19, 20]. The only viable alternative is to use formal verification, and case studies in the use of formal verification have been quite successful. However, presently formal verification has many 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-crucial software system is extremely high because large amounts of human effort is employed. Far better synthesis and analysis tools and techniques are required that provide the ability to develop safety-critical software having the requisite dependability with far less effort.
- Commercial Off The Shelf Components*

The use of commercial-off-the-shelf (COTS) components as a means of reducing costs is attractive in all software systems. COTS components are used routinely in many application domains, and the result is a wide variety of inexpensive components with impressive functionality including operating systems, compilers, graphics systems and network services. In aviation systems, COTS components could be used in a variety of ways but for the issue of dependability.

If an aviation system is to meet the required dependability goals, it is necessary to base any dependability argument on extensive knowledge of everything used in building the system. This knowledge must include knowledge of the system itself as well as all components in the environment that are used to produce the final binary form of the software.

COTS components, no matter what their source, are built for a mass market. As such they are not built to meet the requirements of ultra-dependable applications, they are built to meet the requirements of the mass market. Making the situation worse is that COTS components are sold in binary form only. The source code and details of the development process used in creating a COTS component are rarely available. Even if they are available, they usually reflect a development process that does not have the rigor necessary for ultra-dependable applications.

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. Development of the WAAS system, for example, was originally estimated to cost \$892.4M but the current program cost estimate is \$2,900M. The original deployment schedule for WAAS was expected to begin in 1998 and finish in 2001. The current deployment schedule is to start in 2003 and no date for completion has been projected. WAAS is not an isolated example [21].

The need to develop many systems of the complexity of WAAS indicates that success will depend on vastly improved cost estimation and project management.
- System Security*

Many future aviation systems will be faced with the possibility of external threats. Unless a system is entirely self contained, any external digital interface represents an opportunity for an adversary to attack the system. It is not necessary for an adversary to have physical access. Of necessity many systems will communicate

by radio, and digital radio links present significant opportunities for unauthorized access.

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. Again, this is not a solved problem, and must be dealt with if aviation systems are to be trustworthy.

4 Summary

The application of computers in aviation systems is increasing, and the range of applications being developed is increasing. If the requisite productivity and dependability goals for these systems are to be met, significant new technology will be required.

Further details can be found about many aspects of aviation in general and safety in particular from many sources including the Federal Aviation Administration [22], the National Transportation Safety Board [23], NASA's Aviation Safety program [8], NASA's Aviation Safety Reporting System [24], Honeywell International, Inc. [25], and Rockwell Collins, Inc. [26].

Acknowledgments

It is a pleasure to thank Ms. Kelly Hayhurst of NASA's Langley Research Center for her suggestions for the content of this paper. This work was supported in part by NASA under grant number NAG-1-2290.

References

1. Automatic Dependant Surveillance - Broadcast (ADS-B) System. <http://www.ads-b.com>
2. Yeh, Y.C.: Design Considerations in Boeing 777 Fly-By-Wire Computers. 3rd. IEEE International High-Assurance Systems Engineering Symposium (1998)
3. RTCA Incorporated: Software Considerations in Airborne Systems and Equipment Certification. RTCA document number RTCA/DO-178B (1992)
4. Swenson, E.H.: Into The Glass Cockpit. Navy Aviation News (May-June, 1998) <http://www.history.navy.mil/nan/1998/0598/cockpit.pdf>
5. Inside The Glass Cockpit: IEEE Spectrum. <http://www.spectrum.ieee.org/publicaccess/0995ckpt.html>
6. Federal Aviation Administration: Welcome to Free Flight. <http://ffp1.faa.gov/home/home.asp>
7. Federal Aviation Administration: Wide Area Augmentation System. <http://gps.faa.gov/Programs/WAAS/waas.htm>
8. NASA Aviation Safety Program, <http://avsp.larc.nasa.gov/>
9. Aviation Week and Space Technology, Industry Outlook (January 15, 2001)
10. Aviation Week and Space Technology, Industry Outlook (November 27, 2000)
11. Aviation Week and Space Technology, Industry Outlook (July 17, 2000)
12. Bateman, Donald: CFIT Accident Statistics. Honeywell International Incorporated,

- http://www.egpws.com/general_information/cfitstats.htm
13. Aviation Week and Space Technology, Industry Outlook (June 26, 2000)
 14. Aviation Week and Space Technology (July 2001)
 15. Miller, S., personal communication (2002)
 16. ARINC Engineering Services LLC: Aircraft Condition Analysis and Management System. http://avsp.larc.nasa.gov/images_saap_ACAMSdemo.html
 17. Munns, T.E. et al.: Health Monitoring for Airframe Structural Characterization. NASA Contractor Report 2002-211428, February 2002.
 18. Young, S.D., Jones, D.R.: Runway Incursion Prevention: A Technology Solution. Flight Safety Foundation's 54th Annual International Air Safety Seminar, the International Federation of Airworthiness' 31st International Conference, Athens, Greece (November 2001)
 19. Finelli, G.B., Butler, R.W.: The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software. IEEE Transactions on Software Engineering, pp. 3-12 (January 1993)
 20. Ammann, P.A., Brilliant, S.S., Knight, J.C.: The Effect of Imperfect Error Detection on Reliability Assessment via Life Testing. IEEE Transactions on Software Engineering pp. 142-148 (February 1994)
 21. 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
 22. Federal Aviation Administration, <http://www.faa.gov>
 23. National Transportation Safety Board, <http://www.nts.gov>
 24. NASA Aviation Safety Reporting System, <http://asrs.arc.nasa.gov/>
 25. Honeywell International Incorporated: Enhanced Ground Proximity Warning Systems. <http://www.egpws.com/>
 26. Rockwell Collins Incorporated. <http://www.rockwellcollins.com>