On the Achievement of a Highly Dependable and Fault-Tolerant Air Traffic Control System

Algirdas Avižienis
University of California, Los Angeles
Danforth E. Ball, MITRE Corporation

Can we trust the new AAS to deliver highly dependable air traffic control services until the year 2000? Yes, systematic application of fault tolerance offers a solid promise of success.

The Advanced Automation System, or AAS, will provide automation services to both en-route and terminal air traffic controllers throughout the United States. Although controllers are able to maintain separation between aircraft during periods of interruption of the automatic services, the transition to backup modes of operation is potentially hazardous. The increased controller workload resulting from interruption of the services provided to controllers limits the traffic handling capability of the Air Traffic Control System, which can result in major delays during periods of heavy traffic. As the level of automation services provided to controllers increases, interruption of computer services to the controllers will become even more critical. Accordingly, extremely high reliability and availability of the services provided by the AAS will be required on a continuous basis, 24 hours a day, seven days a week.

Reliability of the present system

The 9020 system. The system currently in use in the air route traffic control centers, or ARTCCs, is the IBM 9020 System, a modified configuration of IBM System 360 computers.[1] This system contains fault-isolation and recovery features that were state-of-the-art when the system was developed in the mid-sixties. However, the system design is mainly oriented toward tolerance of hardware faults, and the 9020's highly centralized architecture and pooled memory design remained vulnerable to software faults. Over the past 20 years, the software has stabilized and changes have been judiciously introduced and verified through testing and maintenance. A failure of the 9020 system results in the interruption of computer services at all controller operating positions. In this event, the ATC system relies on the independent backup capabilities of the direct access radar channel, or DARC, controller-pilot voice communications, and flight data strips, as discussed below.

Although the computer complex is often referred to as an automation system, the services provided by it are far more than automation services; other than voice communication, it is the controller's primary contact with the airspace being controlled. After interrupting air traffic control processing, the 9020 attempts to isolate the failure, reconfigure the system if necessary, and restart ATC processing. If automatic recovery is successful, ATC processing is interrupted for 20 to 60

0018-9162/87/0200-0084$01.00 © 1987 IEEE

seconds. If automatic recovery is not successful, an unscheduled outage occurs. The mean time to restore service following an unscheduled outage is approximately 20 minutes, while the mean time between failures is about 600 hours.

Broadband backup. When the 9020 was first introduced, the only backup available to controllers in the event of a computer outage was to revert to unprocessed broadband radar data. To convert to the use of broadband radar, each controller had to rotate his or her cathode ray tube display to a horizontal position and reidentify all radar targets using small plastic chips called "shrimp boats" and a grease pencil. The most critical time following a computer failure was during this transitional period. The wide variation in 9020 recovery times further compounded the problem because controllers had no way of knowing how long to wait for the computer system to recover before deciding to switch to the broadband radar system.

Direct access radar channel. Subsequently, a new backup system called the direct access radar channel, or DARC, was developed. This system, which became operational in 1981, is an independent computer system that bypasses the 9020 central computer, providing an alternate path for radar data to the controller's display. This backup system can be quickly activated and provides an automatic tracking capability so that the controllers no longer have to resort to tracking the aircraft manually by pushing plastic chips across the screen.

Although the DARC system provides a significantly improved backup capability for the 9020, it was not designed to provide higher-level functional aids to the controller, such as conflict alert, and therefore is only a short-term backup.

Evolution of AAS RMA requirements

Procurement of the AAS is being conducted in accordance with the Office of Management and Budget policy for major system acquisitions, expressed in *OMB Circular A-109*.[2] The policies in A-109 are intended to "place emphasis on the initial activities of the system acquisition process to allow competitive exploration of alternative system design concepts in response to mission needs" (*OMB Circular A-109*, p. 3). System requirements are to be defined in terms of the operational characteristics needed by the users of the system, not in terms of equipment specifications. The objective is to allow industry the freedom to develop innovative solutions to government needs in a competitive environment. Contractors should not be restricted by a preconceived system concept or by forced compliance with government specifications and standards. The requirements in an A-109 acquisition are to be expressed as functional requirements, not equipment requirements.

In the AAS procurement, this emphasis on functional requirements has been extended to the reliability, maintainability, and availability (RMA) characteristics, traditionally expressed in equipment terms but now specified in terms of delivery of service.

In this article, we will discuss only the main element of the AAS, which is the area control computer coupler, or ACCC. The approach used to define the ACCC requirements illustrates the approach used for the other computer complexes as well.

Concept of operating modes. The overall ACCC system availability should approach unity. However, hardware and software element failures may occur within the system that could temporarily prevent the system from performing all of its required functions. Therefore, a hierarchy of three levels of functional performance has been defined.

The highest level of functional capability is the full-service mode. In this mode, the ACCC performs all of its designated operational functions within the required response times.

If failures within the system have caused some services provided to controllers to be interrupted, while the rest are operating properly, the system is said to be in the reduced-capability mode, provided that a specified minimum level of performance is maintained. This minimum level or "floor" of the reduced capability mode provides all of the basic capabilities required to perform ATC functions, including surveillance, automatic tracking, automatic hand-off, and flight plan processing, but does not include many of the more advanced automation capabilities available in the full-service mode. This level provides the functional capability that enables the facility to maintain a safe and orderly flow of traffic for an indefinite period of time, although airspace users may experience some inconveniences, such as not being able to fly preferred routes or altitudes.

When the minimum level of performance required for the reduced-capability mode cannot be maintained, the system is said to be in the emergency mode. In the emergency mode, the most critical services of surveillance, automatic tracking, and local flight data update are provided. These functions enable the controllers to continue to maintain separation between aircraft—the most critical function of the ATC system. However, the increased bookkeeping workload resulting from the loss of automatic processing of flight plan data would make it impossible for the controllers to maintain a high volume of traffic for any length of time. In the event of a sustained outage of the ACCC, responsibility for the aircraft under the control of the failed facility will be assumed by adjacent facilities. This concept, known as *facility backup*, is the ATC system's defense against the catastrophic failure of an ACF, when it is due to other causes, such as fire or earthquake. Thus, the emergency mode is intended primarily to provide for the continuity of essential services during the transition to facility backup or a return to the full-service or reduced-capability modes of operation.

Transparent recovery. The objective of the AAS is to make all recovery actions transparent to the controllers. In order to quantify the meaning of "transparent," it was necessary to establish the system's normal response time requirements. If the system could recover from a failure and still respond within the required response time interval, then the controllers would not be able to detect any interruption of service and the recovery could be considered transparent to the user. Therefore, the system must be designed to perform all required processing within the designated maximum response times, as well as any automatic recovery actions necessitated by hardware or software failures. If the system recovers within the maximum response times, the ATC services are not considered to be interrupted. Exceeding these response times for any reason will result in perceptible delays in the information being presented to the controllers and will be counted as downtime, which reduces the availability of the services provided.

Definitions of failure. The definition of a system failure in the AAS derives from the concept that if the system fails to re-

Table 1. ACCC availability requirements.

	Goal	Requirement
Full-service mode	1.0	.999995 (2.6 min/yr)
Reduced-capacity mode	1.0	.999999 (32 s/yr)
Emergency mode	1.0	.9999999 (3 s/yr)
Operational position	.999999 (32 s/yr)	.999995 (2.6 min/yr)

spond to a controller's request, then from the user's viewpoint the service requested is unavailable. The reason for the unavailability is of little concern to the user. Therefore, failures are defined with respect to the inability to provide a required service within the specified response time.

In addition to a hardware or software failure, a response time failure can result from an accumulation of processing, recovery, and restoration time delays. Failures are thus defined with respect to the system's functional requirements and are independent of the equipment configuration.

An operational-position failure occurs whenever the set of logical displays and associated input and control capabilities associated with that position cannot be provided within the specified response time. A system-level mode failure occurs whenever any specified maximum response time is exceeded at two or more operational positions.

AAS response time performance is specified in terms of a mean, ninety-ninth percentile, and maximum response time associated with each of a set of response time classes. If a failure occurs within the system and recovery is performed quickly enough to permit the response to be provided within the specified maximum, then no system level failure has occurred. Exceeding the maximum response time results in accumulated downtime and reduces the system availability accordingly.

Quantitative requirements. Availability of ATC services is considered the most important consideration in the design of the AAS. The overall design goal is to provide safe, full-service operation within the required response times, 100 percent of the time. Although hardware and software element failures can be expected to occur within the system, fault tolerance (automatic fault detection, isolation, and recovery) along with judicious functional partitioning will be utilized to assure the availability of essential functions and to minimize full-service interruptions.

The AAS system availability requirements in the system-level specification are stated in terms of the probability of having at least a given level of functional capability (operating mode) available to the air traffic controllers. The requirements thus address the availability of ATC services to the system's users and do not necessarily represent the availability of specific equipment configurations.

The ACCC availability requirements appear in Table 1. The figures in parentheses translate the requirements into the average amount of time per year that the functional capability associated with a given mode or position would be unavailable. Thus, for 3 seconds per year the system may be completely down and the controllers will be without the essential surveillance and tracking functions defined for the emergency mode. For 28 seconds per year the system may be operating at the emergency-mode level of capability. For 2.1 minutes per year the system may be operating at or above the minimum capability required for the reduced-capability mode, but below full service. The sum of these times corresponds to 2.6 minutes per year of full-service unavailability. Of course, the nature of the availability parameter means that the "downtime per year" is the average taken over an infinitely long time. Depending on the frequency of failure, the actual duration of outages could be longer or shorter than the average.

It is important to note that the availability requirements are stated with the assumption that the system is fault tolerant, and that recovery management remains in control during the reduced-capability and emergency modes. Under this assumption, the availability requirements define the hardware element redundancy needed to avoid system outages due to the exhaustion of hardware resources.

In addition to the availability requirements, specific reliability constraints have been imposed to limit the maximum allowable frequency of failure to one full-service mode failure every four weeks and one operational position failure per year.

Qualitative requirements. To ensure that the frequency and duration of service interruptions are minimized and system safety is maintained, additional qualitative reliability and maintainability design criteria were specified. The additional criteria make the use of fault tolerance imperative. The reliability design criteria address the avoidance of single points of failure and the functional partitioning of the system so that when service interruptions are unavoidable, the number of functions and operational positions affected are limited to operationally tolerable levels. The maintainability design criteria address features and techniques that will enable the rapid detection, isolation, repair, and recertification of failed items. In order for a repairable, fault-tolerant system to meet its reliability and availability potential, virtually all necessary maintenance actions must be performed immediately and quickly, so that the failed item can be restored to operational status before additional failures exhaust the available spares and result in a system failure.

Advances in fault-tolerant system design

In the two decades since the initial design of the 9020 system, significant progress has occurred in the design and successful implementation of highly dependable, fault-tolerant systems for several important applications, including spacecraft and aircraft control, telecommunications, process control, and transaction handling.[3-5]

Much progress has been made in defining the *coverage* concept with its many aspects that quantize the effectiveness of fault-tolerance mechanisms within a design. Strong new insights have been gained in fault modeling, error detection, fault location and removal, and system state restoration techniques. Many of

these techniques have been implemented at the hardware level, especially in VLSI technologies.[6]

Pioneering work has been done in the study of design diversity techniques for the tolerance of design faults, including recovery blocks and N-version programming for software,[7] and diverse multichannel computation for hardware.[8]

Most important of all, the insights gained during the research and design processes have led to the convergence of many diverse viewpoints into a cohesive framework of concepts of dependability and fault tolerance.[8] The existence of such a framework makes it possible to approach the design and subsequent evaluation of the AAS with a structured design approach that integrates the performance and fault-tolerance goals during the evolution of system architecture. The AAS is by far the most complex system yet specified that depends on fault tolerance for its viability, and highly structured design is of critical importance for the successful implementation of its fault tolerance.

Current challenges and problems

Concurrently with the successes discussed above, new and difficult problems in fault tolerance arose from the rapid evolution of large distributed computing systems and the growing complexities of their individual nodes that were made possible by the application of VLSI technology.

Foremost among the new threats to system dependability we find the following challenges:

(1) The need to tolerate new fault modes unique to distributed systems, even though they lead to errors in synchronization and in state consistency of concurrent processes and distributed databases, making system state recovery very difficult.

(2) The need to tolerate residual design faults that remain undiscovered by testing and validation of software or VLSI logic, and later may cause concurrent, identical errors in multiple redundant computing channels.

(3) The need to cope with unanticipated, failure-inducing improper interactions of otherwise well-designed fault-tolerant subsystems that have not been perfectly integrated into a distributed fault-tolerant system. Especially difficult to integrate are the various hierarchical fault diagnosis and recovery sequences that support the localized fault tolerance of subsystems and those that support the fault tolerance of functional services ("threads") provided by two or more subsystems.

(4) The need to handle more than one nearly concurrent fault manifestation. The large size and distributed nature of new systems lead to the possibility of two or more independent fault manifestations occurring at nearly the same time. This, in turn, will require two or more recovery algorithms to be concurrently active, with the resulting risks of mutual interference, deadlocks, and unpredictable behavior.

In ATC systems, for which long service life is a critical goal, one additional specific challenge is the need to deal with changes to a hierarchy of error-handling mechanisms. For this reason the FAA is making an investment in the AAS design competition phase, or DCP, to ensure that inherent robustness and extensibility are incorporated in the design. It is recognized that this requires a balancing of fault tolerance extensibility and ATC service extensibility concerns in order to ensure that ATC service changes made to the AAS design are also reflected as extensions to the fault tolerance mechanisms.

Assuring the availability and safety of the AAS

Obviously, the AAS is a distributed system of high complexity and therefore likely to be affected by all the problems discussed above. The choice of AAS dependability goals and of the means to verify their attainment by an AAS design have undergone evolutionary changes over the past two years. We summarize the current view of the major dependability goals for the AAS below.

The quantitative reliability/maintainability/availability, or RMA, requirements in the AAS system level specifications[9] set goals for the system assuming that very complete fault-tolerance provisions are made in the design. Availability goals are set with the expectation that system recovery management will always remain in control, but that some exceptionally difficult recovery sequences will reduce the services that remain available to the air traffic controllers from the standard *full-service mode* to those defined as *reduced-capability mode* and *emergency mode*, respectively, for short periods of time.

However unlikely, there exists the possibility of a "collapse" of system recovery management capabilities. This may lead to the temporary outage of the central portion of the system. In this event, air traffic control would revert to emergency mode operations and manual methods to avoid any impact on system safety. The facility backup by adjacent ATC centers is provided to maintain safety in the case of natural disasters, such as floods and earthquakes.

The near-100 percent availability of the AAS system is attainable through the pursuit of three design goals:

(1) The system should contain sufficient hardware element redundancy to avoid system outagesdue to exhaustion of hardware resources.

(2) The design should incorporate a hierarchy of complete, protected, and sufficiently fast error detection, fault location, and state recovery algorithms for every defined class of faults within the system in order to provide near-unity fault coverage. Design faults should be considered, and the possibility of nearly concurrent manifestations of two (or more) faults in the subsystems of the AAS should be taken into account.

(3) There should exist error detection, containment, and system state recovery features in the system and application software to provide fast-reacting defenses against the consequences of the anticipated, but not precisely definable, forms of abnormal behavior that may be caused by unrecognized fault modes and by improper interaction of multiple recovery sequences, as discussed previously.

To attain these goals the FAA has tasked the design competition phase, or DCP, prime contractors to provide evidence that their design includes mechanisms for detecting and recovering from the known set of possible faults. This requirement may be described in terms of a coverage validation process, as illustrated in Figure 1.

In the AAS contract each DCP prime contractor is required to identify, through failure mode effects analysis, or FMEA, and a fault tree analysis, those fault events (including potential failures) that are an inherent consequence of the functional partitioning, and those potential failures that may result from deficiencies in automatic fault isolation and recovery mechanisms and techniques. Furthermore, design modifications to eliminate or control critical failures shall be identified and introduced into the design process throughout the design evolution.[10]

As Figure 1 indicates, each type of fault is covered by one or more layers of protection. In fault tolerance these layers comprise a hierarchy of error detection/recovery mechanisms that might range from memory error correction (SEC/DED) logic at the module level through application-specific error recovery block algorithms, and finally to an independent monitor that detects faults in processing threads (that span distributed processors) and initiates operations on backup resources.

Each layer or layers in the hierarchy represent an allocation of functions to subsystems and processors or stations in a distributed network (shown in Figure 1 as "System architecture"). The consequence of this design allocation is the capture of critical detection and recovery decisions by each prime contractor in the failure mode effects analysis and fault tree analysis that are to be presented in a System Safety Report.[10]

The Software Requirements Specification and Software Top Level Design Document represent specifications for each computer software configuration and item identified by the prime contractor. Each major software item contains an allocation of both fault-handling responsibilities and error detection/recovery actions that were identified by the system safety analysis. The software error detection/recovery requirements and designs contained in these documents represent the contractor's approach to achieving fault tolerance and a balanced implementation of mechanisms that eliminate or contain the effects of identified classes of faults.

Verifying the fault tolerance of the AAS

The most difficult question that remains to be answered after the fault-tolerant design approach (discussed above) has been defined is "How closely does a proposed AAS design come to the complete attainment of these objectives?"

Four fundamental techniques need to be applied here in order to gain confidence in the design and to eliminate residual imperfections of its defense mechanisms. These techniques are

(1) The rigorous application of a highly structured design process, expressed in the form of a design paradigm for fault-tolerant systems.

(2) The documentation (empirical modeling) of the design by means of a complete, integrated, structured specification of all fault-tolerance assumptions and fault-tolerance attributes of the entire AAS system that makes it possible to assess the design for completeness, consistency, and the coverage of defined faults. The major elements of such a specification are fault definitions, partitioning for error containment, fault-detection techniques, diagnostic procedures, recovery sequences and their integration, system state restoration, and validation of recovery.

(3) The judicious use of state-of-the-art analytic reliability and performance modeling techniques to assure the presence of sufficient hardware resources. Modeling also serves as a designers' tool for the refinement of the AAS design for fault tolerance, especially by the modeling of various coverages and of performance/fault tolerance trade-offs and interrelationships.

(4) The development, maintenance, and continuing use of a set of software V&V software, system testing, evaluation, and maintenance tools to assure the

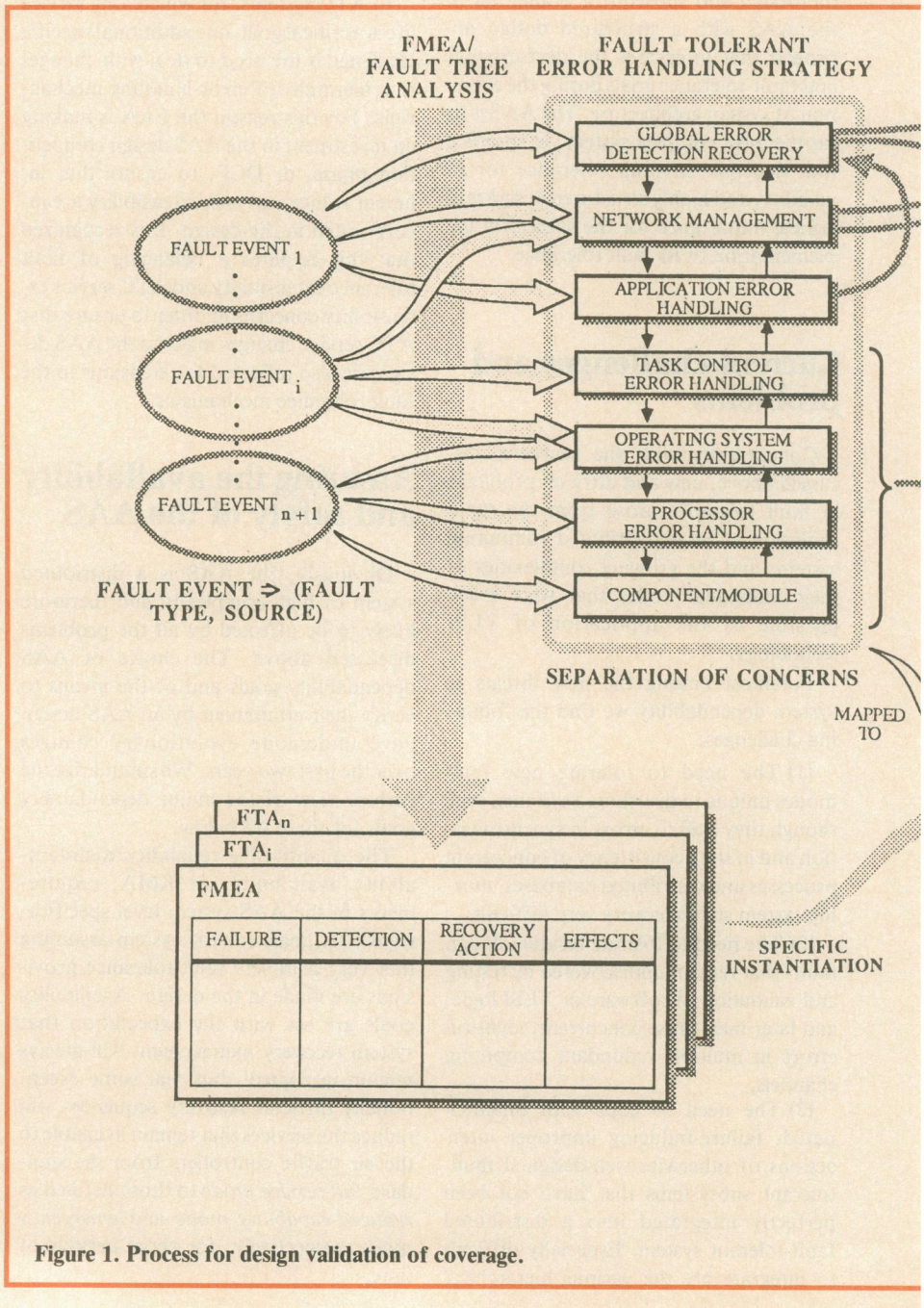


Figure 1. Process for design validation of coverage.

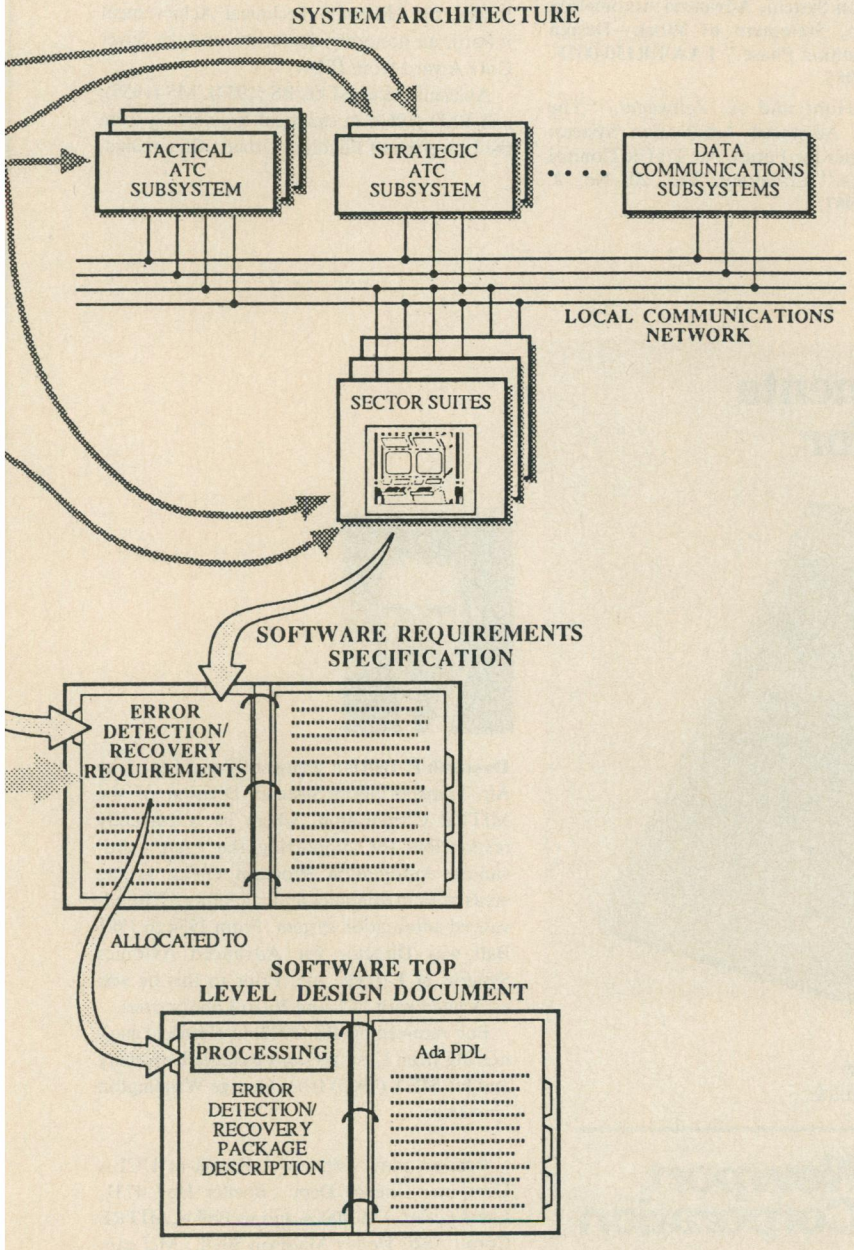
growth of AAS software and system reliability, availibility, and safety.

The application of the above techniques began with the start of the AAS design competition phase, and will need to continue throughout the entire life cycle of the AAS system. Extensions of the ATC service as delivered by the AAS are expected throughout the entire 20- to 30-year life cycle of the AAS system. They will consist of subsequent refinements of existing functions as well as of the addition of new ATC capabilities.[11] The protection of the AAS system that is offered by fault tolerance techniques needs to be systematically extended with every improvement and addition of ATC functions. For this reason, the verification that is offered by fault tolerance techniques needs to be systematically extended with every improvement and addition of ATC functions. For this reason, the verification that fault tolerance of the AAS system has remained intact and able to meet the dependability goals is a capability that needs to remain intact and be continuously refined as long as the AAS system remains operational.

The attainment of a system that will satisfy the FAA's rigorous RMA requirements demands constant attention throughout the design, development, and testing of the AAS. The selection of a hardware architecture that has well-characterized fault tolerance provisions and adequate levels of redundancy to meet the RMA requirements is only a first step.

During the development of the AAS software, advanced software development tools and techniques need to be used to reduce the number of design faults and to structure the software for improved testability. Following software development, an effective reliability growth program must be instituted to remove as many of the remaining design faults as possible. In order to accelerate fault removal it will be necessary to simulate realistically a heavy system workload to increase the rate at which latent faults are exposed. In addition, effective data reduction and analysis tools must be developed to characterize the causes of system failures and to facilitate the removal of design faults.

The AAS goal of neary-unity availability makes it clear that fault-tolerant design, quality control during software development, and an effective "test, analyze, and fix" program for reliability growth will all be essential. Accordingly, during the AAS design competition phase, the FAA has placed considerable emphasis on "front-end" investment in the tools and techniques that will facilitate the important downstream development and test activities necessary to assure the availability and safety of the AAS.



The AAS system is unique among current large-scale systems because of its exceptional availability requirements during a long service life and because of the early and rigorous emphasis on fault tolerance as the main means to assure such availability.

It is evident that a successful delivery of the AAS as a replacement of the current ATC system will not only provide a new level of dependability and safety for air traffic control in the United States but will also serve as the major milestone in the evolution of a new generation of fault-tolerant systems. The timely transfer of the AAS experience to benefit other large-scale system projects remains an important challenge to the FAA, the industrial contractors, and the research community at large. □

Acknowledgments

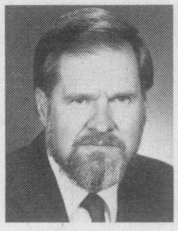
The authors wish to thank Phil DeCara of the FAA Advanced Automation Program Office and Gregory V. Kloster of Knowlex Technology Corporation for many valuable discussions and for their comments on this article. Suggestions received from Robert Wiseman and Philip Yoh of the DOT Transportation Systems Center are also sincerely appreciated.

References

1. "An Application-Oriented Multiprocessing System," *IBM Systems J.*, Vol. 6, No. 2, 1967.
2. Office of Management and Budget, Major Systems Acquisition, *OMB Circular A-109,* April 1976.
3. A. Avižienis, ed., *Proc. IEEE*, Vol. 66, No. 10, special issue on fault-tolerant digital systems, Oct. 1978.
4. W. N. Toy and M. Morganti, eds., *Computer*, Vol. 17, No. 8, special issue on fault-tolerant computing, Aug. 1984.
5. D. A. Rennels, "Fault-Tolerant Computing: Concepts and Examples," *IEEE Trans. Computers*, Vol. C-33, No. 12, Dec. 1984, pp. 1116-1129.
6. B. Courtois and M. Messalama, eds., *Proc. IEEE*, Vol. 74, No. 5, special issue on fault tolerance in VLSI, May 1986.
7. A. Avižienis, "The N-Version Approach to Fault-Tolerant Software," *IEEE Trans. Software Engineering,"* Vol. SE-11, No. 12, Dec. 1985, pp. 1491-1501.
8. A. Avižienis and J.C. Laprie, "Dependable Computing: From Concepts to Design Diversity," *Proc. IEEE*, Vol. 74, No. 5, May 1986, pp. 629-638.
9. "Department of Transportation/Federal Aviation Administration, Advanced Automation System, System Level Specification—Design Competition Phase," FAA-ER-130-005F, May 1985.
10. "Department of Transportation/Federal Aviation System, Advanced Automation System, Statement of Work—Design Competition Phase," FAA-ER130-005F, May 1985.
11. V.R. Hunt and A. Zellweger, "The FAA's Advanced Automation System: Strategies for Future Air Traffic Control Systems," *Computer,* Vol. 20, No. 2, Feb. 1987.

Algirdas Avižienis has served as a member of the AAS Technical Advisory Group of the FAA since its formation in 1984. At UCLA, he is the director of the Dependable Computing and Fault-Tolerant Systems Laboratory at the Computer Science Department, where he has directed research in this field since 1972 and has served on the faculty since 1962. He is a fellow of the IEEE and has received the NASA Apollo Achievement Award, the AIAA Information Systems Award, the NASA Exceptional Service Medal, the IEEE-CS Technical Achievement Award, an honorary doctorate, and the Silver Core Award from IFIP.

Avižienis received his BS (1954), MS (1955), and PhD (1960) in electrical engineering from the University of Illinois at Urbana-Champaign.



Danforth E. Ball is a senior staff member of the Air Transportation Systems Division of the MITRE Corporation, where he is currently responsible for supporting the FAA's Advanced Automation Program Office in the areas of fault tolerance and reliability of the advanced automation system. From 1974 to 1981 Ball was Director for Advanced Avionics Systems at E-Tech, Inc. Prior to this he was associated with ITT and Vitro Laboratories.

Ball received his BS (1962) in electrical engineering from Case Western Reserve University and his MEA (1965) from George Washington University.

Readers may write to Avižienis at UCLA Computer Science Dept., Boelter Hall 4731, Los Angeles, CA 90024 and to Ball at MITRE Corp., 1820 Dolley Madison Blvd., McLean, VA 22102.