IMPACT OF FAULT-TOLERANT AVIONICS ON LIFE-CYCLE COSTS

Andrei L. Schor, Frank J. Leong and Philip S. Babcock IV

The Charles Stark Draper Laboratory, Inc.
Cambridge, Massachusetts

Abstract

This paper focuses on the effects of a fault-tolerant implementation of a mission-critical avionics function on the aircraft life-cycle costs. A triplex redundant architecture is contrasted to a simplex implementation of the same function. The cost analysis employed in this study accounts for the major contributors to the cost of ownership. It will be shown that an increased mission readiness as well as a higher function reliability during the mission combine to provide a much higher overall mission success level and consequently a significant cost advantage for the fault-tolerant architecture.

1 Introduction

The military avionics systems have been and still are rapidly increasing in capability. The advances are made possible by the fast progress in computers and solid-state technologies. Higher levels of functional integration are being pursued with the aim of reducing the total resources required for meeting performance and fault- and damage-tolerance objectives.

The unavoidable increase in the complexity of these systems has lead to large increases in overall operating costs. The key contributing cost factors are the basic equipment, the spares required for adequate readiness, the various levels of repair and maintenance and the necessary test and diagnostics equipment. Last, but by no means least, there is an enormous penalty being paid in additional aircraft necessary to insure desired levels of mission success. Indeed, the fleet must be able to accommodate the fact that, for any given mission, not all the planes are available and also, even if available at the start of the mission, not all the planes sent out will have the particular mission-critical equipment operational throughout the flight.

Two implementations of a hypothetical mission-critical (but *not* flight-critical) function are examined, integrating availability, reliability and cost analyses. While the cost analysis is relatively simplified, it does contain the main ingredients to render realistic the conclusions of this study.

2 Alternative Implementations

2.1 Functional Objective

The focus of this study is on a subsystem of the avionics suite. This subsystem is assumed dedicated to performing a function critical to the success of a mission. Examples of functions of this type are: Global Positioning System Receiver, Digital Communication Receiver, Fire Control Radar, etc. Such a function is, however, considered not flight-critical. In other words, its loss may compromise a mission, but generally it will not lead to the loss of the aircraft.

Maintaining this function obviously incurs the regular life-cycle costs associated with one plane. Not having this function throughout the mission, either because it was not available at the inception of the mission and therefore required repair or because of in-flight failures, causes a considerable increase in the effective cost-of-ownership due to the additional aircraft needed to achieve a desired mission success level. This very substantial contribution is reflected in the cost model used in this study.

2.2 Single-string ("Simplex") Implementation

The single-string design is typical of current fighter implementation. It relies on hardware- and/or software-based built-in tests to detect faults in its operation. The fault-detection probability is at best in the range 90-95%. Current experience and wisdom casts considerable doubt on claims of better performance for this type of fault detection mechanism.

2.3 Triplex Implementation

The alternative implementation considered in our study is a redundant, fault-tolerant design consisting of three identical units [1]. A tightly synchronized microframe voting achieves nearly perfect coverage (detection and isolation) of the first fault, as well as nearly perfect detection of the second fault. Isolating the second fault brings into

CH2759-9/89/0000-1893 $1.00

play the less than perfect self-test process, therefore rendering the second fault coverage less than perfect. Since the probability of occurrence for two faults is much lower than that for the first fault, the overall coverage of the triplex architecture is very much superior to that which may be anticipated from the single-string alternative.

It should be noted that the redundant design can operate in degraded modes, i.e., two-out-of-three or even one-out-of-three, with unavoidable deterioration in the expectation of coverage success.

2.4 Repair Policy

The single-string design requires a simple repair-as-needed approach. Upon detection, a repair action is initiated. During the repair process, the plane is not available.

The fault-tolerant triplex design allows more flexibility in deciding on a repair policy. It can be repaired as soon as a fault is detected or the repair action may be postponed for a later time in conjuction with other aircraft maintenance or inspection tasks. In this study, a repair action is assumed to take place after the second fault. Consequently, a triplex-equipped aircraft is assumed available when either all three or any two out of the three components are still operational.

2.5 Undetected Faults

As already mentioned, there is a finite probability that faults will go undetected. This is a far more important issue for the simplex implementation than for the triplex one. We postulate that during normal aircraft operation, a certain percentage of faults will defeat the detection mechanism. Without knowing of the fault condition, no repair action is initiated and it is not unreasonable to assume that the plane will take off in this state. What this implies is a compromised mission due to the degraded initial condition, rather than in-flight failures. To compensate for this possibility, additional aircraft must be provided in the fleet. It turns out that for the simplex configuration this may become a major contribution to the cost of the fleet.

Of course, an undetected condition cannot last indefinitely. (If it did, it would mean that particular function is never needed!) Undetected faults may be exposed by periodic maintenance actions, comprehensive pre- or in-flight tests or use in missions of particularly demanding nature. It will be seen in the modeling section that an exposure mechanism is postulated that basically transforms the undetected faults into detected faults, thus triggering a repair action which leads to system restoration.

3 Analysis

3.1 Basic Figures of Merit

To compare the two implementations of an arbitrary avionics function, the following figures of merit were selected:

- mission readiness,
- mission success,
- life-cycle cost.

Mission readiness represents the availability of the particular avionics function considered onboard the plane at the start of a mission. The plane is not available during the time the repair action is taking place. It should be noted that a repair action is initiated as a result of:

- a detected component failure or
- the exposure of an undetected failure.

The availability of an aircraft is a long-term issue, requiring a model reflecting the operational lifetime of the plane. It is affected by equipment failure rate, coverage, repair policy and time and the rate of undetected fault exposure. We postulate the existence of a mechanism for exposing undetected faults. This exposure could result from periodic maintenance actions, stringent pre- or in-flight tests or failed attempts to use the defective equipment during a mission.

Mission success addresses the reliability of the subsystem being examined, i.e., the probability that the subsystem will be operational throughout the flight, given that it was operational when the aircraft left the ground. This is a quantity reflecting the short term evolution of the subsystem. During flight, only automatic reconfigurations are allowed, i.e., no repairs or replacement are assumed possible. The success of the mission depends on equipment failure rate and coverage.

The life-cycle cost provides a measure by which competing designs can be judiciously and comprehensively compared. The cost contributions accounted for in this study are:

- repair actions, triggered by either one of the two above mentioned events,
- cost of equipment added to the aircraft to carry out the desired avionics function,
- cost of the additional aircraft necessary to ensure a required mission success level.

A consistent life-cycle cost evaluation requires the integration of the more traditional "stand-alone" life-cycle

analysis with an appropriate availability/reliability analysis. The approach presented in this paper represents an attempt to consistently merge these analyses into a framework facilitating a well-founded design trade-off study.

3.2 Reliability/Availability Modeling Approach

In order for an aircraft to successfully carry out a mission requiring a particular avionics function, two conditions must be met. First, the subsystem representing the actual implementation of the function must be operational at the start of the mission. In other words, with respect to this function, the plane must be mission-ready. If the subsystem is not operating properly, the need for a repair (replacement) action temporarily removes the aircraft from the pool of resources available for the mission. Second, the subsystem must remain operational throughout the flight. While the loss of this subsystem will not entail, in and of itself, the loss of the aircraft, we assume nonetheless that the mission will fail. During the mission, no repairs are possible and therefore the reliability of the system becomes crucial.

It is clear that in determining the availability and the reliability of the subsystem in question we have to deal with two very different time scales. The availability of the subsystem has to reflect the long-term operation, with repair and maintenance actions taken when needed to return to operational status. Given the assumed economical lifetime of the aircraft (5000 flight hours) and the MTBF of the basic, single string subsystem (1000 hrs), steady-state (instead of time-dependent) availability models were generated for the two function implementations. These Markov models include transitions representing covered and uncovered failures, repairs and the undetected fault exposure processes. The resulting systems of linear algebraic equations have been solved by symbolic Gaussian elimination to obtain analytical expressions for the state probabilities.

Unlike the lifetime system availability, the reliability of the subsystem during a particular mission must be modeled as a short-term, transient process. Time-dependent models for the two designs were constructed and analytically solved for the state probabilities characterizing the system during flight. The transitions represented reflect failure and, where applicable, reconfiguration processes.

The availability and reliability models for the two designs are merged into the life-cycle cost model through our definition of mission success. In the cost model, the probability of the subsystem being available at the start of the mission *and* being operational throughout the flight constitutes a mission success path.

3.2.1 Single-string design

The Markov models used to evaluate the availability and reliability of the simplex implementation are shown in Figure 1. The system is assumed to have a self-test capability providing a certain level of coverage, C.

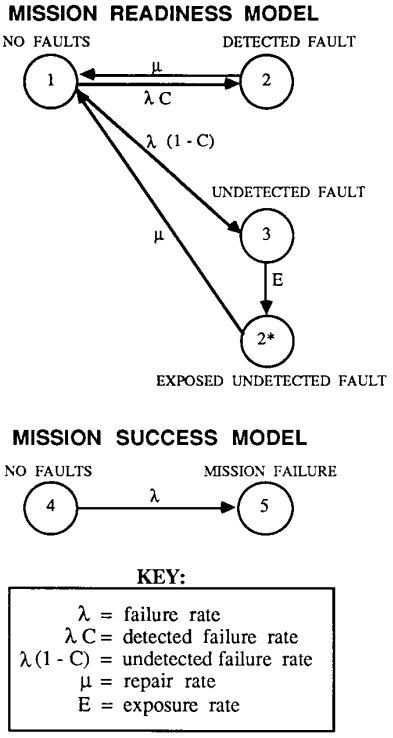

Figure 1. Simplex Markov Models

In the availability model, once a failure occurs and is detected, a repair process is initiated and proceeds at a rate μ. The undetected failures are assumed to be exposed at a rate E, followed by a repair action. The system is assumed mission-ready only in state 1. Repair actions are carried out from states 2 and 2^*, in which the system is therefore not available.

The reliability model simply tracks covered and uncovered failures. Either type of failure constitutes a loss of function; mission success is associated with state 4, which represents the subsystem being fully operational throughout the mission.

3.2.2 Fault-tolerant triplex design

The availability and reliability models of the triplex implementation are illustrated in Figure 2. These models are considerably "richer" than their simplex counterparts. In the triplex case the voting/reconfiguration process is explicitly represented. However, given its essentially instantaneous nature, on the time scale of the failure events, a simplified treatment is fully justified and used. That is, instead of actually having voting and reconfiguration transitions, they are represented as additional, modified failure branchings. This is the origin of the transitions whose rates include the factor λ/σ, i.e., the ratio of the failure rate to the rate of the reconfiguration process. For our choice of parameters, this ratio is equal to 10^{-6}. With regard to the availability model, we assume that repairs of detected faults are initiated only after the second fault. In the triplex configuration, second fault detection is considered essentially perfect and its imperfect isolation is accounted for in the cost model through an enhancement of the overall repair cost. After the second fault, the system is considered shutdown for repairs, therefore there is no transition to a three-fault state. This implies, of course, no dormant failures. Just as in the case of the simplex design, undetected faults are exposed at a rate E, followed by the appropriate repair action. Repairs are therefore initiated from both states 4 and 4*.

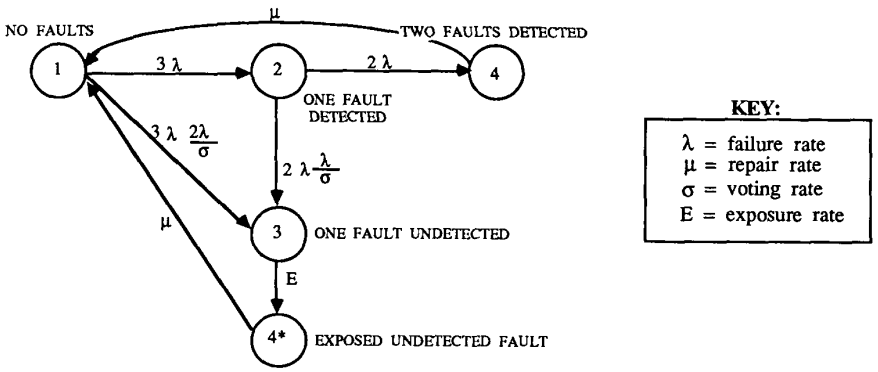

Figure 2A. Triplex Markov Model – Mission Readiness Model

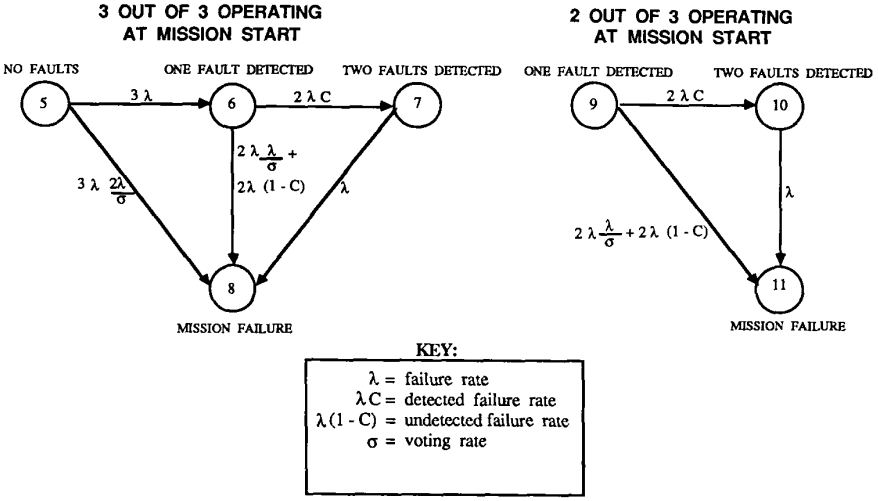

Figure 2B. Triplex Markov Models – Mission Success Models

The above mentioned repair policy, allowing operation in a two-out-of-three state, leads to both states 1 and 2 being associated with a mission-ready system. Consequently, two mission reliability models are generated, one for each of the two conditions that may prevail at the start of the mission: the three-of-three operational and the two-of-three operational. The subsystem is assumed capable of carrying out its function in flight when at least one out the three components is still operational. The subsystem fails as a result of either uncovered failures or component exhaustion.

3.3 Life-Cycle Cost Model

The life-cycle cost model used in this study comprises a number of contributions which are all affected, to various degrees, by the particular function implementation. These contributions are summarized in Figure 3 and briefly discussed below.

3.3.1 Repair Cost

According to our previous discussion, repairs are initiated following a detected fault or by the exposure of an undetected fault. In either case, the repair cost over the aircraft lifetime is given by the number of repair actions times the cost of a repair action. The number of repair actions is in turn given by the expected time in the repair initiation state (i.e., the probability of being in that state times the aircraft lifetime), multiplied by the rate at which repairs are performed (i.e., the reciprocal of the MTTR). The cost of a repair action has two components, the labor cost and the cost of the replacement part(s). When a repair action is initiated by the exposure of an undetected fault, our cost model provides for a penalty due to the additional labor and/or diagnostic equipment required to isolate the fault and to the potential use of additional parts because of imperfect isolation.

- **Cost of Repairs = Number of Repairs * Cost of a Repair Action**

  Number of Repairs = Probability of being in a Detected Fault State * Aircraft Lifetime / MTTR

  Cost of a Repair = fn(Part Cost, Condemnation Ratio, MTTR, Reconditioning Cost, Labor Rate)

- **Cost of Parts added to the aircraft**

  = Number Required for specific implementation * Part Cost

- **Cost of Extra Aircraft required for a specified mission effectiveness level**

  = Number of Extra Aircraft * Lifetime Cost of One Aircraft

  Lifetime Cost = fn(Original Purchase Cost, Operating Cost)

  Extra Aircraft = Number of Planes Owned - Number of Successful Planes

  Number of Successful Planes / Number of Planes Owned

  = Sum of success paths over all operating modes

Figure 3. Cost Contributions

4 Life-Cycle Cost Analysis Results

Two operational scenarios have been considered. In the first one, no particular constraints are placed on repairability and consequently a typical mission time of 2 hours is assumed. The total cost per "successful" aircraft for the two implementations is shown in Figure 4. The very substantial advantage displayed by the fault-tolerant architecture is due to the much higher aircraft availability made possible by this approach. The availability of the single string design is significantly lower because of the large impact of the undetected faults. The correction of these faults is delayed due to the slow exposure process. For this short mission, the reliability advantage is relatively minor. The advantage increases with a lower part cost, shorter MTBF, lower self-test coverage and longer intervals between events causing the exposure of undetected failures.

The other operational scenario assumes surge conditions. This translates into requiring about 200 flight hours before allowing any repair action. Figure 5 illustrates this scenario. In this case, the overwhelming advantage of the triplex implementation is due mainly to its much higher reliability, which assures a high degree of mission success even under these adverse conditions. This advantage is almost insensitive to part cost, exposure rate and coverage. As might be expected, it is however very much dependent on the MTBF, increasing rapidly with a decrease in the MTBF. Clearly, the very high cost of the simplex alternative makes its use unrealistic for this scenario. If its use is to be pursued, then it will most likely result in additional maintenance and a lower number of aircraft available for a required mission.

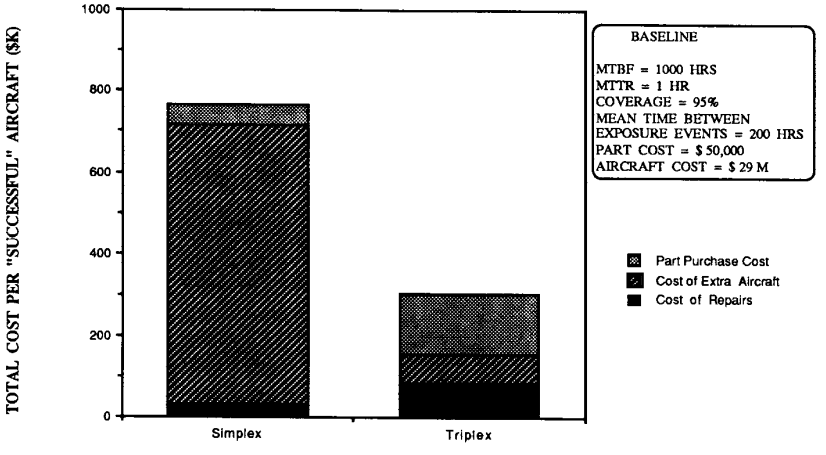

Figure 4. Breakdown of Aircraft Costs – Mission Time = 2 Hours

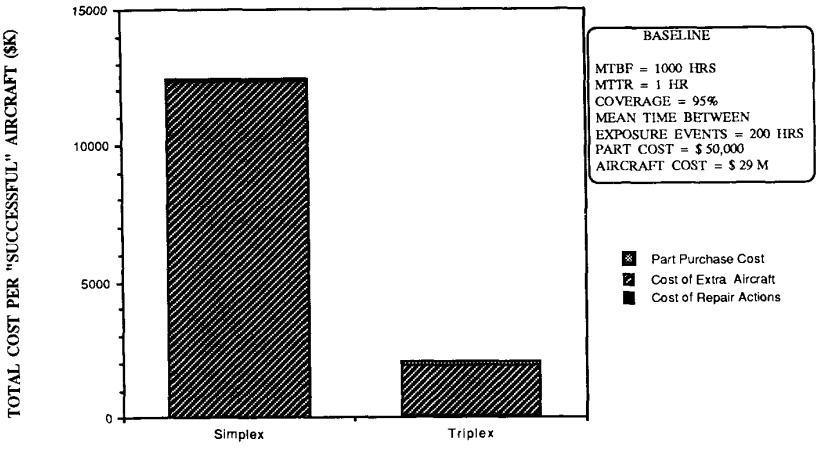

Figure 5. Breakdown of Aircraft Costs – Mission Time = 200 Hours

5 Conclusions

A number of conclusions can be drawn from this study. A fault-tolerant implementation of an avionics function can significantly reduce life-cycle costs by reducing the number of additional aircraft required to achieve desired levels of mission readiness and success. The high fault coverage inherent in such an implementation increases the probability of mission success by reducing the probability of undetected faults prior to the start of the mission and mitigating the effects of faults during the mission.

The methodology used in this study is suggestive of a more rigorous analysis that could be performed to evaluate the benefits of fault tolerance for complex, integrated avionics systems.

Acknowledgement

The work reported in this paper was performed as part of the MASA program [3], under contract F04606-87-D-0051-RZ02 with the U.S. Air Force. Publication of this paper does not constitute approval by the Air Force of the findings or conclusions contained herein. It is published for the exchange and simulation of ideas.

References

1. Lala, J.H., "Advanced Information Processing System: Fault Detection and Error Handling," AIAA Guidance, Navigation and Control Conference, Snowmass, Colorado, August 1985.

2. US Air Force Cost and Planning Factors, Report AFR 173-13.

3. Larry D. Brock and John J. Deyst, Jr., "Modular Avionics Systems Studies", AIAA/IEEE 8-th Digital Avionics Systems Conference, San Jose, California, October, 1988.