MSFC-820

Factors which Limit the Value of Additional Redundancy in Human Rated Launch Vehicle Systems

Joel M. Anderson[1] and James E. Stott[2]
NASA, MSFC, AL 35812, USA

Robert W. Ring[3], Spencer Hatfield[4], and Gregory M. Kaltz[5]
Bastion Technologies, Inc, MSFC, AL 35812, USA

The National Aeronautics and Space Administration (NASA) has embarked on an ambitious program to return humans to the moon and beyond. As NASA moves forward in the development and design of new launch vehicles for future space exploration, it must fully consider the implications that rule-based requirements of redundancy or fault tolerance have on system reliability/risk. These considerations include common cause failure, increased system complexity, combined serial and parallel configurations, and the impact of design features implemented to control premature activation. These factors and others must be considered in trade studies to support design decisions that balance safety, reliability, performance and system complexity to achieve a relatively simple, operable system that provides the safest and most reliable system within the specified performance requirements. This paper describes conditions under which additional functional redundancy can impede improved system reliability. Examples from current NASA programs including the Ares I Upper Stage will be shown.

I. Introduction

THE Ares I Launch Vehicle is the first in a series of two launch vehicles intended to support continued work on the International Space Station (ISS), as well as to further the United States space exploration initiatives of returning to the surface of the moon with an eventual human mission to Mars. In all mission scenarios, the Ares I vehicle is tasked to launch the crew capsule to Low Earth Orbit (LEO) where it may then proceed to the ISS or loiter for rendezvous with additional space systems to be launched on the Ares V Cargo Launch Vehicle (Fig. 1).

This system configuration was initially identified in the Exploration Systems Architecture Study (ESAS) as a heritage based system most likely to satisfy mission and safety/risk requirements within the tight budget and schedule constraints. The ESAS provided an initial conceptual architecture with identified constraints and heritage systems that impose significant limitations on performance capability. For this reason, performance (as measured by total mass) is a critical characteristic of the detailed design.

---

[1] Chief Safety and Mission Assurance Officer for Ares I Upper Stage, Safety and Mission Assurance Directorate, NASA Mail Stop: QD33, MSFC, AL 35812, USA

[2] Reliability and Maintainability Lead for Ares I Upper Stage, Safety and Mission Assurance Directorate, NASA Mail Stop: QD33., MSFC, AL 35812, USA

[3] Risk Manager, Bastion Technologies, Inc., Mail Stop: BTI, MSFC, AL 35812, USA

[4] Senior Reliability Engineer for Ares I Upper Stage Avionics, Bastion Technologies, Inc., Mail Stop: BTI, MSFC, AL 35812, USA

[5] Reliability Engineer for Ares I Upper Stage Main Propulsion System, Bastion Technologies, Inc., Mail Stop: BTI, MSFC, AL 35812, USA

The Ares I configuration (Fig. 2) includes the First Stage (heritage hardware based on the current Reusable Solid Rocket Motor used on Shuttle), the J2X Engine (based on previous J2S engine used on Saturn) and a new, clean-sheet design for the Upper Stage. Given the inherent difficulty of applying redundancy or reducing mass on the heritage systems, the Upper Stage has been targeted as the system element with the most design flexibility to address system level performance issues. This factor increases the importance of applying redundancy in a judicious manner where limitations imposed by common cause failure, increased system complexity, and combined serial and parallel configurations are fully considered in the trade studies. This approach is contrary to the traditional approach within NASA to implement redundancy or fault tolerance to hazards which may result from either inadvertent operation or failure to operate.

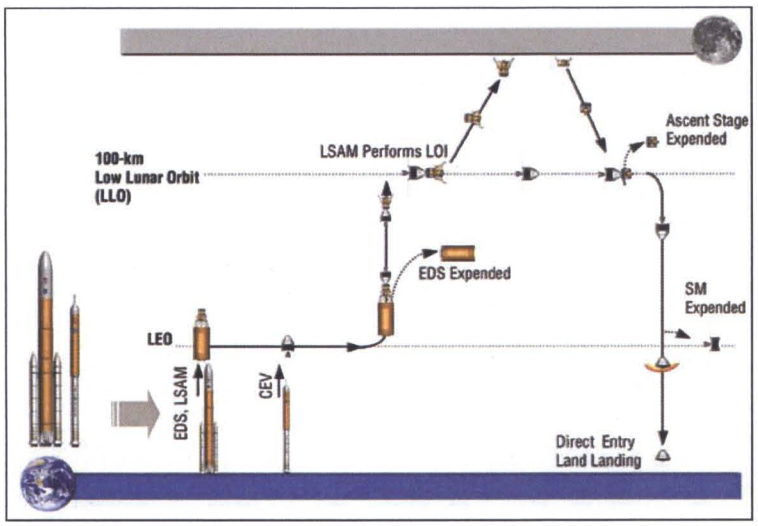

Figure 1. ESAS Lunar Sortie Crew with Cargo DRM.

As this initiative moves forward, the Agency must consider new ways to control risk if performance requirements are to be satisfied within the cost and schedule constraints imposed on the project. NASA has long implemented a rule-based approach to reliability and safety in which redundancy or fault tolerance is specified based on the criticality associated with loss of function or inadvertent function. While this rule-based methodology has been successfully implemented across a great many programs, it results in significant increases in system complexity and cost, while reducing system performance due to added mass and requirements for additional resources (electrical power, thermal control). If no significant challenges exist in resources or performance, these demands are less significant. However, in the design and development of a launch vehicle, it is likely that significant issues exist in performance. In addition to impacts to system cost, complexity, performance and resource limitations, previous systems have not fully considered the limitations on improvements in reliability and risk associated with implementation of redundancy. This impact is particularly significant in systems which remain dormant for some portion of the mission profile where inadvertent operation is as much of a concern as failure to operate when required.

Figure 2. Ares I Launch Vehicle.

This paper addresses the issues associated with redundancy application as a rule based approach to identify the limitations that mitigate against strict adherence to this philosophy, defines an approach to consider the impacts of must work and must not work redundancy configurations, and applies the approach to an actual case to support a configuration trade study.

II. Impacts of Redundancy on System Reliability

A. Impact of Parallel-Series Configuration

In general, the impact of parallel and series redundancy on the reliability of a system can be characterized as follows:

1) Parallel redundancy (redundancy implemented to "assure" operation) increases system reliability.
2) Series redundancy (redundancy implemented to "prevent" unwanted/premature operation) decreases system reliability.

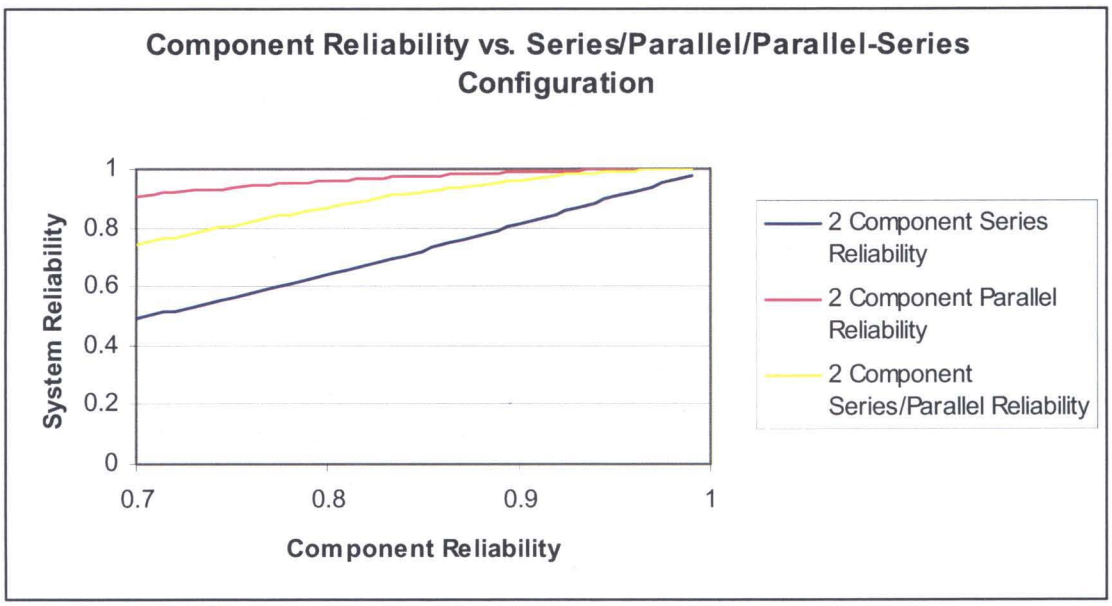

Figure 3. Component Reliability vs. Series/Parallel/Parallel-Series Configurations.

As can be seen in Fig. 3 , for any component reliability, a series configuration reduces the reliability while a parallel configuration increases reliability. If required to protect against both loss of function and premature function (parallel-series configuration), the reliability is improved over a single component but the overall system reliability is reduced from a simple parallel configuration.

B. Impact of Common Cause Failures (CCFs)

Common Cause Failures (CCFs) refer to a class of dependent failures that tend to reduce the effectiveness of parallel redundancy as a means of improving system reliability. Using identical components in a parallel configuration introduces coupling factors that can lead to the failure of multiple components due to a shared cause. Coupling Factors are in essence shared susceptibilities to system challenges. The same susceptibilities that result in the failure of a single component can cause the failure of several identical components in a parallel configuration whenever these components are simultaneously challenged. Coupling factors are numerous for identical components. Examples of coupling factors include the same manufacturer, same inspection process, same maintenance procedures, same operating environment, and same design (Fig. 4). When performing root cause analysis of Common Cause Failures it becomes readily apparent that coupling factors have a significant role.

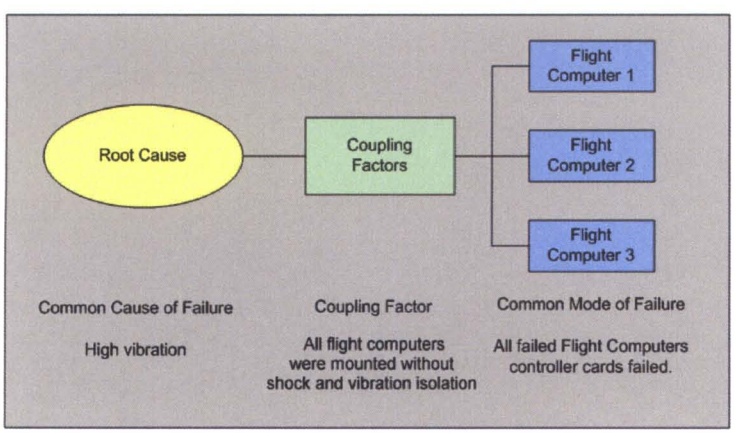

Figure 4. Common Cause Failure Diagram

The process of mitigating common cause failures incorporates many of the same strategies for improving component reliability, such as de-rating of EEE parts, poka yoke (mistake proofing), robust design, HALT/HASS to identify and eliminate failure modes, and inspection. These methods not only improve reliability significantly, but also reduce the need for a greater amount redundancy. Whenever redundancy is employed to improve reliability and fault tolerance, it's important to systematically identify coupling factors and take steps to mitigate or eliminate them. One of the ways this can be done is by employing functional redundancy using dissimilar redundant components. However, this approach introduces other issues because

dissimilar functional redundancy increases cost and complexity and introduces additional failure modes. Taking steps to mitigate the effects of the same environment should also be explored. For example, routing redundant cabling on opposite sides of the vehicle to prevent common exposure to location hazards. Strategies can be used during manufacturing, inspection, and maintenance to use different personnel on critical inspections and maintenance procedures.

Several rules should be applied to ensure adequate design needs are met.

Rule 1 — Reduction of the probability of common stress (separation/shock mounting)
Rule 2 — Design redundant units to respond differently to a common stress (diversity)
Rule 3 — Make the design more rugged (high strength/de-rating/robust design)

These methods will reduce the risk of failures due to Common Cause significantly enough to improve the reliability to an acceptable level for man rated vehicles. If it were possible from the safety, reliability, and economic perspective to build completely independent redundant strings of avionics instrumentation, CCF analysis would not be required.

C. Notional Example

To illustrate the impacts of the fault tolerance rule-based approach to reliability of a system, we take the following example:

Suppose we have a simple fluid control valve whose function is to control the flow of fluid through the valve by opening and closing an orifice. Now, suppose that the reliability of this particular valve is R=0.95. If a failure of the valve to open causes fluid not flow through the valve when commanded and this, in turn, would cause a catastrophic loss, the fault-tolerance rule based approach would be applied and a second, redundant valve would be

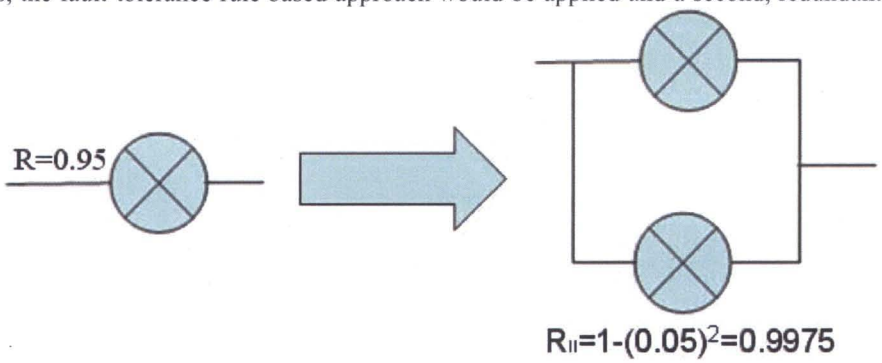

Figure 5. Increasing Failure Tolerance to a Valve Control Failure to Open.

added to the system. Adding this additional valve increases the reliability of the system to 0.9975, exclusive of CCFs (Fig. 5). In addition, if a failure to close or an inadvertent opening of the valve also causes a catastrophic loss, then again the fault-tolerance rules apply and additional redundancy is added (Fig. 6). This decreases the reliability in the parallel only configuration as also increases the mass fourfold from the initial configuration while increasing complexity, requiring more inspection, maintenance, etc.

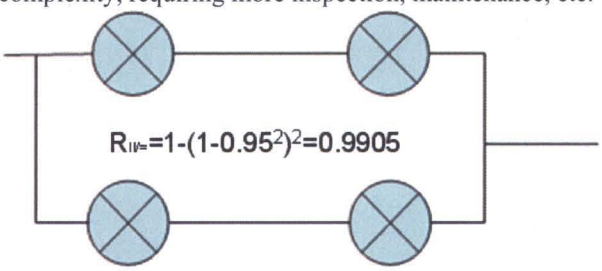

Figure 6. Parallel/Series Valve Control Configuration.

If we include common cause failures, we see that the reliability is even more degraded. Using the Beta Factor modeling approach to modeling common cause basic events, we get the results listed in Table 1. The beta factor of 3.09% comes from the Nuclear Regulatory Commission's CCF database (2003 update) of generic priors.

Table 1 Comparison of Reliability With and Without Common Cause Failures

	Rel w/o CCF	Rel w CCF
Single Valve	0.9500	0.9500
Parallel Configuration	0.9975	0.9961
Parallel/Series Configuration	0.9905	0.9895

III. Historical and Current Examples

A. International Space Station Centralized Fire Suppression System

The issue of applying rule-based approaches to system design to address reliability and safety concerns has not historically been addressed in upfront trade studies. There are historical examples of the impact associated with failure to consider the limitations on benefits of additional redundancy, as well as the impact to system complexity and mass driven by rigid application of these rules.

Among the more well known cases is the centralized fire suppression system initially identified for the Space Station Freedom (later known as the International Space Station). As a safety system, the rule-based approach required single failure tolerance to provide CO2 to each of the powered racks on space station. Application of the rule resulted in a relatively simple design implementation as shown in Fig. 7.

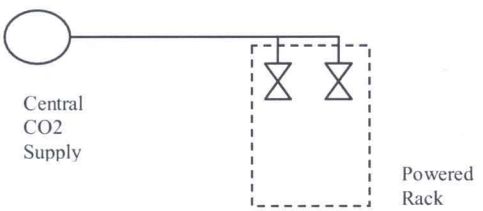

Figure 7. ISS centralized fire suppression system.

The configuration in Fig. 7 assured that CO2 was available as a fire suppressant in the event one of the rack supply valves failed closed, meeting the rule-based requirement for single failure tolerance with minimum additional mass and complexity. The problem is that this is only part of the required rule application. Since the CO2 represents a potential asphyxiation hazard to the crew if inadvertently discharged, the rule also required single failure tolerance to that event.

The configuration in Fig. 8 applied the rule-based redundancy requirements for both failure to activate and inadvertent activation, resulting in significant increases in system mass, complexity and cost. The system reliability associated with the parallel configuration decreased when additional series valves were added. Each powered rack was required to include four valves to provide fire suppression capability to the rack while protecting against the asphyxiation hazard. This design solution was ultimately rejected due to cost and complexity and replaced with an approach using a portable fire extinguisher connected to a valve/port in the rack face, a very simple method to provide the required protection without significant cost and performance impacts. A great deal of time and effort was expended developing a design implementation that was prohibitively expensive from a cost, mass, and complexity perspective. It is also unclear that the ultimate solution, with its man-in-the-loop requirement, was an optimal solution. For this reason, it is appropriate to consider approaches during the upfront concept development phase which may not rigidly comply with rule-based approaches, yet provide a reasonable and balanced consideration of all safety, reliability, and performance impacts of the configuration.

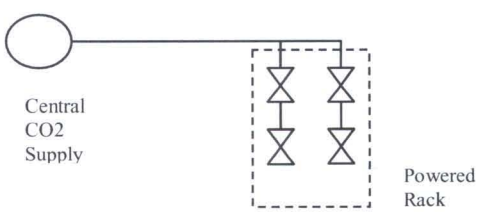

Figure 8. ISS centralized fire suppression system – rule based approach.

B. Ares I Upper Stage Main Propulsion System Solenoid Control Valves

1. Introduction

The need for study of the example described in this subsection first became apparent due to a proposed design change affecting the total number of solenoid control valves to be used as well as the design configuration of solenoid control valve package (Fig. 9) that controls the MPS LH2 (fuel) and LO2 (oxidizer) propellant feed prevalves.

A proposal was made to reduce the total number of solenoid control valves that control both the LH2 and LO2 prevalves in order to reduce the overall cost and weight, while increasing the overall system reliability. This proposed change involved reducing the eight 2-way solenoid control valves used to control the LH2 and LO2 prevalves down to a single 3-way solenoid control valve (Fig. 10).

Before approving the change, a formal reliability trade study was requested to quantify the impact on reliability compared to the baseline design in Fig. 9. During the course of this study, additional valve design configurations that are more fault tolerant were examined. These alternative design configurations were investigated in order to maintain a one fault tolerant design with respect to catastrophic hazards.

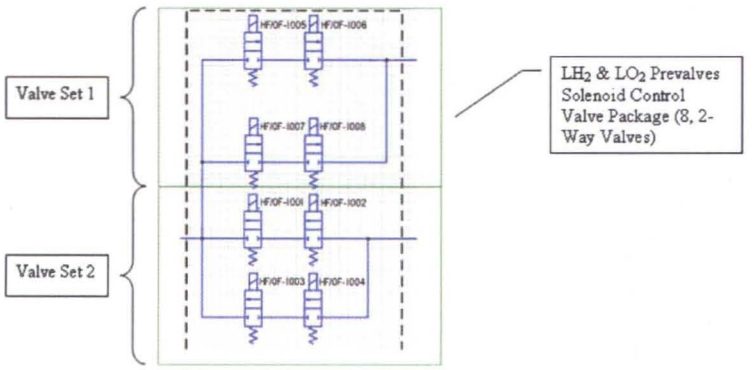

Figure 9. LH2 & LO2 Prevalves Solenoid Control Valve Package (8, 2-Way Valves)

2. System Description

For the baseline design, there are two "valve set" packages that control the opening and closing of the LH2 and LO2 propellant supply prevalves and one "valve set" that controls the opening and closing of the LH2 and LO2 recirculation valves. These are illustrated in Fig. 9 below. Likewise, the alternative designs are shown in Figs 10, 11, and 12 respectively.

In the baseline design there are eight 2-way solenoid control valves in a parallel-series arrangement that control the opening and closing of two 2-way prevalves, one each for the LH2 (fuel) and LO2 (oxidizer) upper stage propellant feed supply systems. In addition, there are two ascent time intervals of primary interest here. The first time interval (130 seconds) is the time interval covering first stage boost and the second time interval (430 seconds) is the time interval covering upper stage burn. While on the ground, or during first stage boost, the LH2 and LO2 prevalves are required to be in the "closed" position. Prior to initiation of upper stage ignition and burn, these prevalves are required to open in order to supply the upper stage engine (USE) with LH2 (fuel) and LO2 (oxidizer).

Valve set 1 and valve set 2 that control the operation of the LH2 and LO2 prevalves are "energized" at different times in the ascent mission profile. When de-energized, all of these valves are in the spring loaded closed position. That is, all valves in valve sets 1 & 2 consist of normally spring closed, energized open 2-way valves. While on the ground and during first stage boost (t = 0 sec to t = 130 sec), valve set 1 is in the "de-energized" or "closed" position, or the spring-loaded closed position, as valve set 1 is responsible for providing the vent during upper stage burn. During this same time period, valve set 2 is in the "energized" or "open" position which corresponds to the LH2 and LO2 prevalves being closed due to pneumatic helium pressure supplied to the prevalves by valve set 2.

Likewise, during upper stage burn, valve set 2 is de-energized which allows these valves to go to their spring loaded closed position thereby cutting off pneumatic helium actuation pressure to the LH2 and LO2 prevalves. During this same time period, the valves in valve set 1 are energized thereby opening these valves and allowing the pneumatic helium pressure that had been keeping the LH2 and LO2 prevalves closed to vent. Providing this vent allows the LH2 and LO2 prevalves to open since, without pneumatic helium pressure applied, the prevalves are normally spring loaded open valves. This allows LH2 and LO2 propellant to enter their respective feedlines to supply the J2X with fuel and oxidizer during upper stage engine ignition and burn.

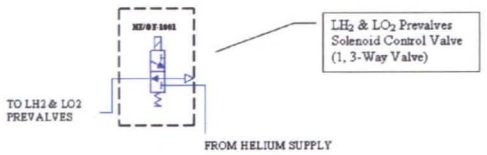

Figure 10. Proposed Valve Configuration – Alternative 2.

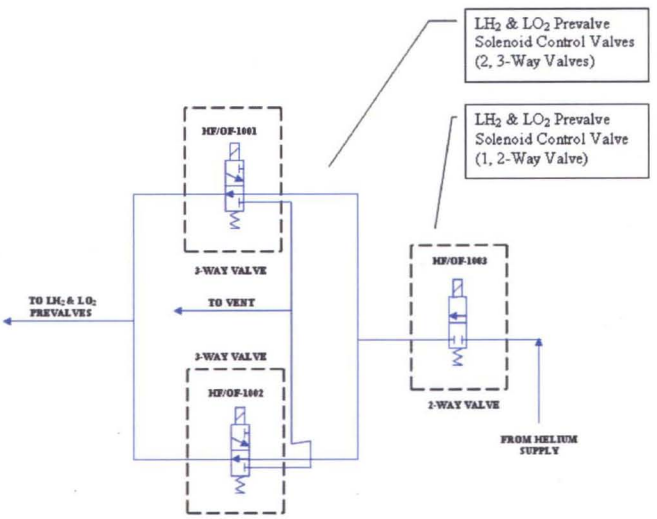

Figure 11. Proposed Valve Configuration – Alternative 3.

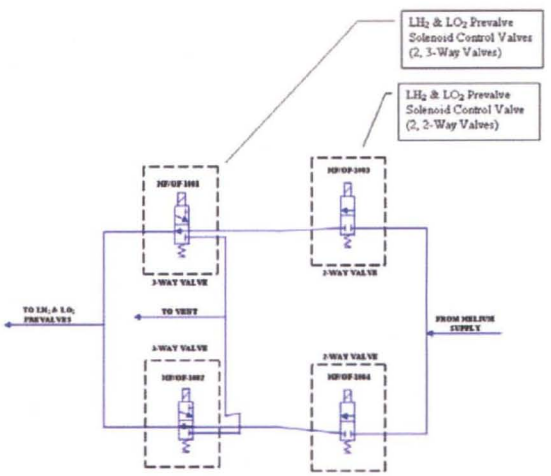

Figure 12. Proposed Valve Configuration – Alternative 4

3. Results

Design alternative 4 (Fig. 12) was shown to provide the greatest increase in overall system reliability. This is followed by design alternative 2 (Fig. 10), then the baseline design (Fig. 9), and lastly design alternative 3. It should be noted that while design alternative 2 (Fig. 10) has a lower overall failure probability as compared to the original, baseline design (Fig. 9), design alternative 2 is clearly not better than the baseline design or alternatives 3 and 4 from the standpoint of fault tolerance. Alternative 2 does not maintain the requirement for a one fault tolerant system whereas the baseline design does, even though its overall system failure probability is higher. The same results apply when comparing design alternatives 2 & 3 where alternative 3 is more fault tolerant than alternative 2. Similarly, alternative 4 provides a higher level of fault tolerance when compared to both alternatives 2 or 3, but does not provide for complete fault tolerance as does the original baseline design.

C. Ares I Upper Stage Avionics

1. Introduction

In September of 2006, a trade study was performed with participation from the author(s) to determine a reliability goal for the Ares I Avionics. To establish the level of reliability for the Ares I avionics subsystem, a notional allocation was performed based on an assumed vehicle Loss Of Mission (LOM) risk requirement of no greater than 1 in 500. As a goal, the avionics allocation was assumed to be a negligible contributor to the overall risk.

Figure 13 shows the avionics contribution to overall Ares I LOM risk as a function of avionics reliability. If less than 1 percent contribution to overall risk is deemed negligible, then an avionics reliability greater than 0.99998 would be required. An avionics reliability of 0.99999 would represent 0.5 percent of the overall system risk. Note that the risk in Fig. 13 is plotted on a logarithmic scale to amplify the relationship to avionics reliability. There exists a point at which increasing levels of avionics does virtually nothing to decrease mission risk. A better way of demonstrating this principle is shown in Fig. 14. By fixing the rest of the vehicle (CLV minus avionics) at a reliability of 0.998, or a LOM risk of 1 in 500 and adding in the avionics at increasing levels of reliability, the effect on overall system risk can be observed. Fig. 14 shows an "S" curve where initially the avionics reliability has a significant impact on overall system risk. Beyond 0.99995, the impact becomes negligible as the overall system risk asymptotically approaches the 1-in-500 allocation. Thus, an avionics reliability of 0.99995 was selected as a goal in determining the appropriate level of fault tolerance.

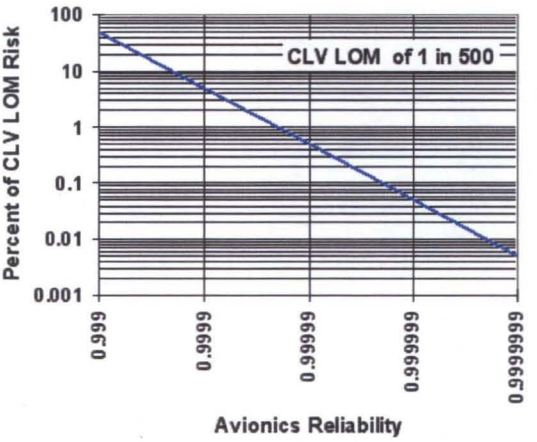

Figure 13. Avionics contribution to overall mission risk of 1 in 500—logarithmic scale.

Before the Ares I Upper Stage Preliminary Design Review, a Fault Tolerance study was performed on actual Ares I Avionics system candidate configurations. This trade study was performed using a detailed model of the avionics system configurations which included mission times, appropriate logic gates, and common cause failure calculations. The basis of this study was to assess candidate fault tolerant avionics architectures. Among the primary objectives was to compare the fault tolerant architectures in terms of reliability, and risk to compare against cost and weight. A bottom-up analysis was performed to parametrically examine reliability as a function of fault tolerance and redundancy schemes. Results of the analysis showed that going to higher levels of fault tolerance yields a negligible increase in reliability regardless of the redundancy scheme. For the Ares I avionics architecture, the impact of increasing levels of fault tolerance (beyond 1-fault tolerant) is limited by the probability of common-cause failure.

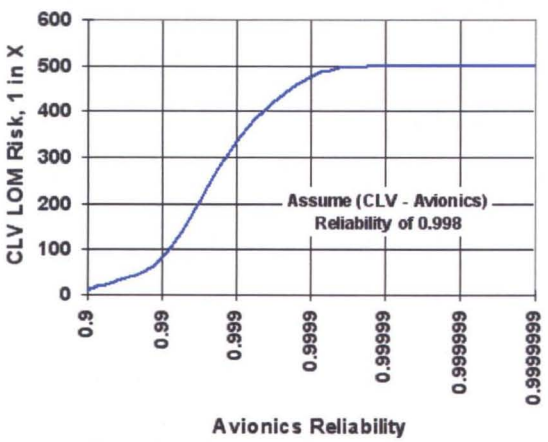

Figure 14. CLV LOM risk as a function of avionics reliability.

2. System Desription

The various system designs included two fault tolerant and one fault tolerant designs as depicted in Figs. 15 and 16. The trade study model also included the first stage avionics, upper stage avionics, electrical power, and engine control unit electronics as part of the study. The CCF model was based upon Space Shuttle Beta factors for both demand and time based failures. A conservative approach was taken by utilizing International Space Station mission time lines, and adjusting electronics component failure rates to the appropriate flight environment based upon guidelines found in MIL-HDBK-338B.

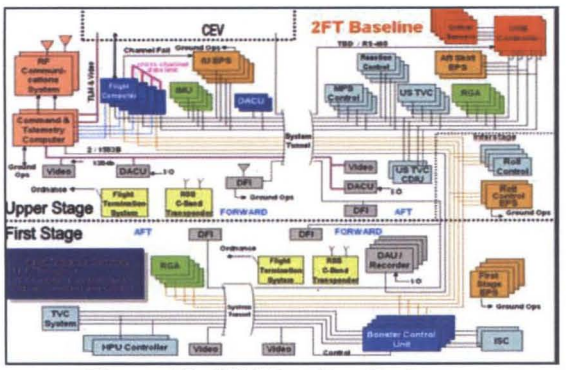

Figure 15. 2FT Baseline Design

The ARES I Avionics System was originally designed as a four string two fault tolerant system (Fig. 15). In general this design included quadruple components across the design. Each independent string of avionics transmitted commands and received data from each strings components. Data was processed across the system in a parallel voting scheme with cross strapped flight computers that provide data sharing among all flight computers. This system would have to experience three independent failures of flight critical components to reach a potential abort condition. The system was comprised of Command and Data Handling, Guidance Navigation and Control, Electrical Power, Flight Safety, and Operational Instrumentation sub-systems which encompass the primary flight critical components. Data communications to upper and first stage components was provided via a 1553B flight critical data bus with crew exploration vehicle communications was via a 1394B data bus. Operational and Engineering data will be collected and transmitted to ground operations via the two Command and Telemetry Computers and the Radio Frequency Communications sub-systems.

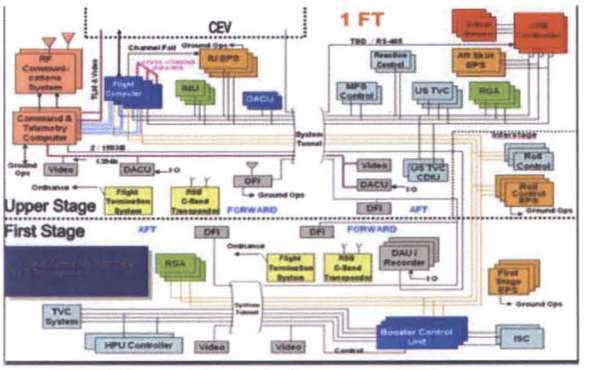

Figure 16. 1FT Avionics Design

The current ARES I Avionics System is a modified three string parallel voting system with cross strapped flight computers that provide data sharing among all flight computers (Fig. 16). The system is comprised of Command and Data Handling, Guidance Navigation and Control, Electrical Power, Flight Safety, and Operational Instrumentation sub-systems which encompass the primary flight critical components. Data communications to upper and first stage components is provided via a 1553B flight critical data bus. Data communications to the crew vehicle is via a Giga-Bit Ethernet data bus. Other sub-systems such as Radio Frequency Communications and Motion Imagery encompass the non- flight critical components. Each Flight computer will contain duplicate copies of the flight software. Operational and Engineering data will be collected and transmitted to ground operations via the two Command and Telemetry Computers and the Radio Frequency Communications sub-systems.

3. Results

Trade study results showed that the one Fault Tolerant design was sufficient to meet NASA's LOM requirements, as discussed in the introduction, for Avionics systems as seen in Table 2. These results further validate the previous Avionics Fault Tolerant trade study results that indicated reliability beyond three strings of avionics is minimized by the prevalence of CCFs.

Table 2. Trade Study Risk Mean Values

2FT Baseline	1/38000
1FT Configuration	1/27000

Figure 17 shows the impact of CCFs to the avionics LOM risk. At 10 percent, the LOM risk is around 1 in 7,200. As the Common Cause Failure Fraction (CCCF) for a single-fault tolerant system is reduced, a significant reduction in risk can be realized. For the Shuttle Probabilistic Risk Assessment (PRA) values of 2.5 percent for electronics, the risk would be approximately 1 in 15,000. However, this value has been attained only after several decades of development and reliability growth. To reach the originally targeted reliability of 0.99995 (or 1 in 20,000) the CCFF would have to be reduced to around 1 percent, which may not be possible.

As a result of the trade study results in conjunction with the September 2006 study, the decision to change the avionics system to a one fault tolerant design was approved by the Constellation Program Safety, Reliability, and Quality Assurance Board.

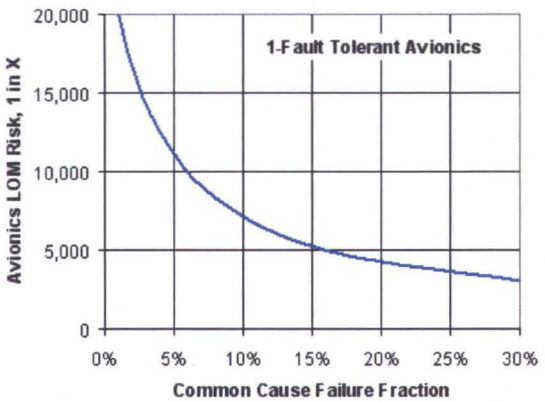

Figure 17. Avionics LOM risk versus CCFF.

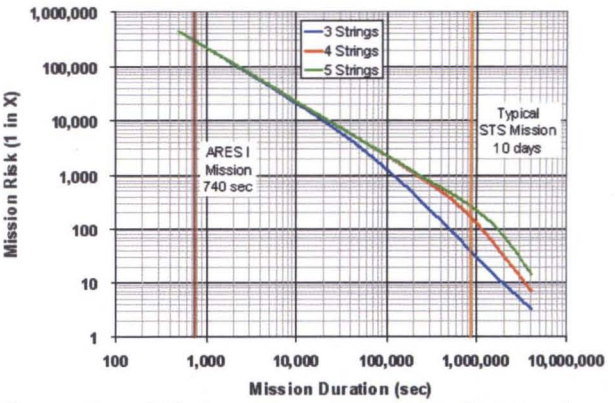

Figure 18. Mission risk versus mission duration for Ares I Upper Stage.

IV. Conclusion

We can conclude from this paper that reliability can be degraded by relying on the traditional rule-based fault tolerance approach. By showing several empirical examples, flexibility to these rules must be taken into account in order to balance safety, reliability, weight, cost, and performance. NASA has now taken a more flexible design approach to ensure that all factors are considered, which will allow us to ultimately arrive at the best possible launch vehicle architecture that will take us forward in NASA's future endeavors to the moon and beyond.

References

A. Mosleh, D.M. Rasmuson, and F.M. Marshall, NUREG CR-5485, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment", *Idaho National Engineering and Environmental Laboratory and University of Maryland*, Prepared for U.S. Nuclear Regulatory Commission, June 1998

G. Kaltz, Upper Stage Probabilistic Risk Assessment Memorandum, "Ares I Upper Stage Main Propulsion System (MPS) - LH2/LO2 Prevalve & LH2/LO2 Recirculation Valve Solenoid Control Valve Reliability Trade Study", *Marshall Space Flight Center, Huntsville, AL.*, February 2008.

G. S. Hatfield, et. al. "Crew Launch Vehicle Avionics Architecture Fault Tolerance Assessment", *Marshall Space Flight Center, Huntsville, AL.*, September 2006.

NASA-TM-2005-214062 "NASA's Exploration Systems Architecture Study", November 2005