56th International Astronautical Congress 2005

IAC-06-D1.1.08

Cost of Safety for Space Transportation

Zachary C. Krevor
Graduate Research Assistant
Georgia Institute of Technology
Atlanta, GA
zachary_krevor@ae.gatech.edu

Alan W. Wilhite
Georgia Tech Langley Professor
National Institute of Aerospace
Langley, VA
wilhite@nianet.org

Abstract

This paper proposes a methodology that explores the tradeoff between increasing component reliability and utilizing component redundancy as the strategy to meet space transportation reliability requirements. This technique would be employed by design engineers to make decisions about a reliability approach. The tradeoff between component redundancy and making parts more reliable warrants more investigation. System level reliability decisions are being made without a thorough exploration of cost saving opportunities. The impact of using redundancy on a system, including how it affects metrics such as development and operations cost, is presented. Additionally, there is little understood about the resources required to improve component reliability to acceptable levels. The process of making parts more reliable is studied and quantified. To incorporate the uncertainty that exists from reliability applications, a stochastic approach is used. Case studies of historical space systems are presented to demonstrate how this methodology is applicable. The findings show how a different reliability approach may have resulted in significant cost reductions. Conclusions are drawn about how to best meet reliability requirements while remaining within strict budgetary guidelines.

1 Introduction

In human space transportation, component redundancy has been relied upon to satisfy reliability requirements. Component redundancy does have some drawbacks because this reliability strategy adds complexity and additional parts. Little work has been completed to show the life cycle cost impacts of adding redundancy. In other words, if the parts count were reduced by increasing component reliability, how would the life cycle cost change? This paper will begin to address that tradeoff with by combining reliability models with a model for determining the cost of reliability upgrades.

Quantifying the cost of upgrading component reliability is a difficult task in the face of uncertainty. Several models have been proposed and this paper will use one of them [1]. Monte Carlo Simulation (MCS) will also be included to lessen the importance of some of the assumptions that are required. MCS will show the sensitivity of the assumptions in the model used for determining the cost of upgrading component reliability. Results will be presented for two human rated space transportation vehicles: the Space Transportation System (STS) and the Apollo Command and Service Module (CSM). These results will discuss the cost of upgrading a subsystem and whether the life cy-

cle cost of the overall program would have justified an increase in development cost. The development cost is the cost associated with the design, development, testing and evaluation of the concept through the first prototype. This cost is also known as the DDT&E cost. The development cost will be compared with the operations cost for each of the space transportation vehicles. The operations cost is defined as the cost associated with program implementation. This cost is both the fixed annual cost required for supporting mission capability and the per flight cost expended when an actual mission is flown. By understanding the impacts of redundancy on the operations cost, a justification can be made about whether or not increasing component reliability would worth the development resources required.

2 Notation

APU	Auxiliary Power Unit
CCF	Common Cause Failure
CEV	Crew Exploration Vehicle
CSM	Command and Service Module
DDT&E	Design, Development, Testing and Evaluation
LCC	Life-Cycle Cost
MCS	Monte Carlo Simulation
MGL	Multiple Greek Letter
STS	Space Transportation System
SSME	Space Shuttle Main Engines
	Formula Notation
B	Beta MGL
G	Gamma MGL
R_i	Desired Component Reliability
$R_{i,min}$	Current Component Reliability
$R_{i,max}$	Maximum Component Reliability
f	Feasibility
C	Dimensionless Cost

3 Methodology

High system reliability can be achieved through multiple methods. A common manner is to use component redundancy. Using component redundancy has some drawbacks due to common cause failure and the increase in system complexity. Another method for increasing system reliability is to increase component reliability. Strategies for increasing component reliability include building in larger design and environmental margins [2]. During manufacturing, high component reliability can be assured by carefully screening parts once they are produced. Carefully controlling the manufacturing process with tight tolerances will also increase component reliability. These stringent methods are one reason that increasing component reliability is typically associated with higher costs and development time. Yet, the benefit of using increased component reliability will be realized later in the program during the operational phase. By using lower amounts of components, the time spent verifying proper operation is decreased [3]; this time will be multiplied many times over for a reusable system. The verification process includes all inspections, testing, and processing required before a mission can begin. Lower numbers of components can also benefit performance by weighing less and using less volume when compared with relying on component redundancy. Quantifying the cost of increasing component reliability is a difficult problem with a lot of investigation still required. This paper will use an exponential model to determine the cost of increasing component reliability. MCS will be utilized to study the sensitivity of the main assumption made in this model.

The exponential model that is employed for determining the cost of increasing component reliability is taken from the reliability community [1]. The model was proposed as a general function with intuitive characteristics. Equation (1) is the formulation used in this paper for quantifying the cost of increasing component reliability.

$$C = e^{(1-f)*\frac{R_i - R_{i,min}}{R_{i,max} - R_i}} \quad (1)$$

The result of this formula is a dimensionless number that represents the cost of increasing component reliability. R_i is the desired reliability of the component. $R_{i,min}$ is the current reliability of the component and $R_{i,max}$ is the maximum achievable reliability of the component [1]. $R_{i,max}$ is assumed to be 99.99999% for all calculations in this paper. F is the feasibility number, which will be discussed later.

This model was chosen because it exhibits a number of good characteristics. First, the cost is always

increasing as the reliability increases. There are no dips in the cost formulation with the monotonic function [1]. With this formula, the cost of achieving high reliability is large. This represents the difficulty in creating high reliability hardware. Finally, the exponential function makes it harder for a component to increase its reliability from 95% to 99% than from 70% to 75%. Other functions would not represent the difficulty of increasing the reliability of a high reliability component as well as this exponential function. This function must be mapped to actual cost values before it can become useful in understanding the tradeoff between increasing component redundancy and increasing component redundancy.

The cost function will be mapped using available hardware data. There are very limited instances in space flight history where reliability increases were planned and a development number was calculated. Other instances such as the evolution of a subsystem between programs will also have to be used to determine how the dimensionless cost function correlates to an actual development cost value. These cost correlations will be kept separate between subsystems because the subsystems perform very different functions. Another reason to keep the cost correlations separate is because the subsystems are at various technology levels and receive different amounts of resources. The use of MCS will help to understand the possible range of costs required to increase component reliability. MCS will mitigate the lack of available data and show the sensitivity of the initial assumptions. The biggest assumption in this model is the feasibility value.

The feasibility estimate is an assumption that is used to reflect the difficulty in increasing component reliability. A lower value, such as 0.1, will increase the cost result compared to using a higher value, such as 0.9. In this paper, a number was assumed with MCS wrapped around the feasibility value. The MCS shows the sensitivity of this assumption and will eventually lead to a range of cost values for increasing the component reliability. [1] does mention correlating the feasibility value with component characteristics, such as the current state of the art, the past history of reliability increases, and future technology growth, but the lack of data made this correlation difficult. More discussion about this feasibility value occurs later in the paper.

Using component redundancy can be an effective means for meeting system reliability requirements. On the STS-9 mission, two general purpose computers failed [4]; however, since the STS carries five general purpose computers, the orbiter was able to land. Additionally, landing occurred with two out of three auxiliary power units (APUs) on fire [4]. While the fire occurred shortly before landing, the final mission phase would have been much more difficult if the orbiter did not have a triple redundant APU system. However, using component redundancy does have its drawbacks. As mentioned earlier, increased component redundancy will add complexity and parts count. One of the main shortfalls of the STS is the large number of parts due to the use of dual and triple redundant systems [5]. The processing time is doubled or tripled for certain subsystems because each string of components must be verified for proper operation. Much of this time could have been reduced if the component reliability was higher. Finally, Common Cause Failure (CCF) can bypass any use of component redundancy.

All models using component redundancy must consider CCF. CCF is a failure mode inherent in all components of the same type. An example of CCF could be a manufacturing defect found in all components produced from the same assembly plant. With space hardware produced in such little amounts, CCF is very prevalent and must be considered. CCF is included in all reliability models within this paper. The multiple Greek letter model (MGL) [6] is used to account for CCF in the reliability calculations. In this model, the β (Beta) value is 0.1 and the γ (Gamma) value is 0.75. The β value is the percentage of all failures of the first component that are inherent in the second component. The γ value is the percentage of failures in the first two components that are inherent in the third component. Therefore, if the first two components fail, there is a 75% chance that the third component will also fail due to CCF. These numbers are referenced from various STS problem report databases along with the historical experience of leading NASA reliability experts [7]. When CCF is accounted for, the benefits of increasing beyond dual redundancy are very small. Even the benefits of dual redundancy are mitigated quite a bit when

CCF is included. Therefore, the tradeoff between using component redundancy and increasing component reliability should be considered by design engineers.

4 Problem Statement

The tradeoff between component reliability and increased redundancy will focus on two subsystems from two different human space flight eras. The first problem reveals the tradeoff between increasing the reliability of the previously mentioned APU and using the triple redundancy strategy employed by NASA in their final design of the STS. The second problem discusses the redundancy versus reliability tradeoff by highlighting the landing system of both the Gemini and Apollo capsules. These two cases were picked because they both use redundancy but the hardware are built for different lifetimes. The STS is a reusable spacecraft while the Gemini and Apollo capsules were meant for single missions. With NASA about to finalize the Crew Exploration Vehicle (CEV) design, the reliability strategy may be influenced by the reusability of the vehicle.

In the first problem, the STS APU system is studied. The APU system consists of the three separate, but identical APUs, hydraulic pumps and hydraulic systems [8]. The APUs create mechanical shaft power to drive the hydraulic pumps that generate the pressure required by the hydraulic system. Each APU is a hydrazine fueled component that creates mechanical power through the catalytic action of its fuel. The hydraulic system provides pressure for the hydraulic actuators that drive the thrust vector control of the Space Shuttle Main Engines (SSMEs), retract the umibilicals connecting the External Tank (ET) to the orbiter, and control the aerosurfaces of the orbiter along with landing gear. An illustration of the APU is shown in Figure 1.

A reliability model was created of the whole APU system based upon the work of the STS PRA [9]. While the PRA examined the contribution to loss of vehicle by specific subsystems, the estimates will be used as a most conservative value for reliability. Another reason for utilizing the PRA value is due to the overall lack of reliability data. A single

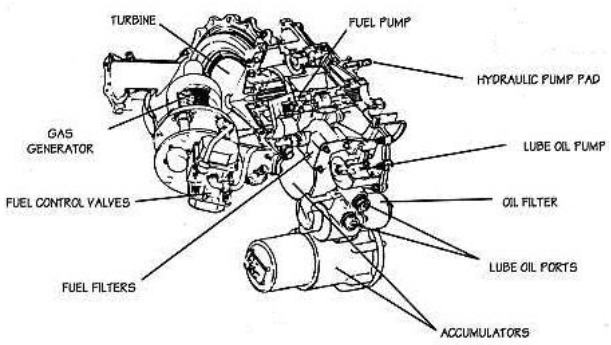

Figure 1: APU Diagram.

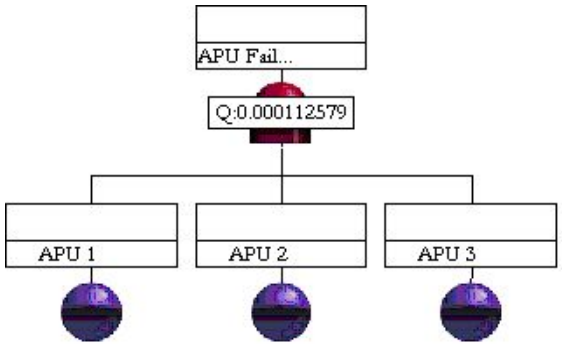

Figure 2: APU Reliability Model.

APU is approximately 98.8% reliable as determined from the STS PRA. According to the shuttle reference documents, this system is triple redundant and can function on only one APU system in emergencies (as evidenced by STS-9 example). An upgrade was planned for the APU to switch to the Electric Auxiliary Power Unit (EAPU) for the fiscal year 2001 [10]. With the upgrade, the total APU system would be, at a minimum, 99.99% reliable [11]. Using this system estimate along with CCF analysis, a single, upgraded APU was calculated to be 99.9% reliable. Both estimates account for a single, complete APU system, including the hydraulic pump and distribution. A model of the triple redundant APU system is shown below in Figure 2. As mentioned earlier, CCF is also included using the MGL model with the above assumptions.

The cost model from Equation (1) was used to calculate the cost of the reliability upgrade. The development cost of the upgrade was estimated at \$241 M FY '06 [10]. The original estimate was \$224 M FY '01 but the new value was calculated using an inflation calculator [12]. While this devel-

opment is not solely focused on upgrading reliability, the assumption is made that to achieve such high system reliability the full development cost is required. Additionally, by using this value as the cost of the reliability upgrade, consistency will be maintained by always using the most conservative values. The non-dimensional result from Equation 1 is mapped to the actual cost values by using a linear relationship.

The final portion of the APU problem is to calculate the cost of upgrading the APU system further so that a single APU system can achieve the reliability of the triple redundant system. An assumption is made about the feasibility value; it is assumed to be 20% more difficult to move from a triple redundant system to a single APU system with increased reliability. The feasibility values are used with a MCS to calculate a range of cost values. Therefore, the cost sensitivity to this assumption is explored and the importance of this assumption is decreased.

Once the development cost increases are determined, they can be compared with the operations cost for processing the APU. The lifetime operations cost is calculated using the cost of life-cycle cost (LCC) of the STS program and its development cost. Then an operations cost per flight is determined and the APU processing costs are examined. A break-even point is determined where the cost of the reliability upgrade would have been more valuable than using a triple redundant system. An assumption is made that the development would occur at the start of the STS program and the savings would occur over 115 flights. The final comparison is between the predicted savings on the operations cost over the life of the STS with the additional development cost of the upgraded APU.

The second problem examines the cost of changing the CSM landing system from three parachutes to a single parachute. The CSM required a drogue and two of the three main parachutes to operate before failure [13]. The landing system also would have worked if only two of the three main parachutes operated (i.e. the drogue parachute failed). The Apollo engineers did change the main parachute reliability value for the second scenario since the parachutes would be required to operate at a higher dynamic pressure. In this problem it is acknowledged that size considerations for moving to a single parachute were not considered.

To formulate the cost equation, the upgrade from the Gemini capsule to the Apollo CSM was studied. For the Gemini capsule, only a single drogue and main parachute were required for the landing system [14]. The initial reliability for the Gemini landing system was estimated at 98.5% [15]. The Apollo landing system was estimated at 99.69% reliability by creating a model incorporating CCF along with the appropriate two out of three voting gates. The model is too large for inclusion within this paper, but interested parties can contact the author directly for more information. A single main parachute was estimated by the Apollo engineers at 99% [13]. Therefore, to match the landing system reliability with only one main parachute, the parachute must increase its reliability to 99.84%, while holding the drogue parachute reliability constant at 99.85

The cost of the upgrade is determined by using the development cost of the Apollo CSM landing system. The acknowledgement is made that the CSM landing system most likely deployed at higher velocities due to its higher energy entry from the moon. Therefore, only 50% of the CSM development cost was considered to calibrate the non-dimensional cost equation to an actual development cost. While the parachute deployment velocities are most likely not too different between Apollo and Gemini, a 50% value will continue to err on the conservative side. Using this mapping, a cost is calculated to change from a two out of three main parachute system to a single parachute. The same assumption is made about the feasibility value; the difficulty is increased by 20% to move from the lower component reliability system to one with higher component reliability. Also, MCS is used to again explore the sensitivity of the feasibility assumption.

5 Results

The calculation of the cost of increasing APU component reliability is listed in Table 1. The cost is a non-dimensional cost number that is mapped to an actual development cost. Using the published estimates for the initial reliability upgrade, the non-dimensionless cost can be calibrated. The cost of

Table 1: APU Reliability Upgrade Results.

Upgrade	$R_{i,min}$	f	R_i	DDT&E FY '06
APU to EAPU	0.988	0.9	0.999	241 $M
APU Upgrade	0.999	0.7	0.9999	1194 $M

Table 2: APU MCS Upgrade Results Range.

Cost Range: $M FY '06		
Minimum	Mean	Maximum
480	1243	3054

the upgrade to a single EAPU system is then estimated and included in Table 1. These estimates relied upon the feasibility assumptions discussed earlier. Therefore, a MCS is used to vary the feasibility assumption. These assumptions are varied by +/- 5% to understand the cost sensitivity. Table 2 lists the range of the MCS and Figure 3 shows the result of the MCS to calculate the cost of upgrading to a single EAPU.

The reliability upgrade to a single EAPU system would be very costly. According to this analysis, an additional $1.2 B FY '06 would have been required for only the APU upgrade. Additionally, the MCS simulation shows that the upgrade could have cost has much as $3 B FY '06 for only the APU. This cost is now compared with the operations cost of the STS.

Table 3 has a top level breakdown of the STS costs. Using the mean value of the upgrade, a break even point is found where the upgrade plus the processing cost of a single APU is equivalent to the processing costs of three APUs. The break even point is found as a function of the total APU processing cost. The break even point is found to be at an APU processing cost of $16.3 M FY '06 per flight. In other words, if total APU processing (i.e. for all three APUs) has cost more than $16.3 M FY '06 per flight, then the upgrading to a single APU at the start of STS development would have been worthwhile. Figure 4 illustrates the tradeoff as a function of APU processing cost per flight. The vertical axis shows the total cost of APU processing, assuming 115 flights.

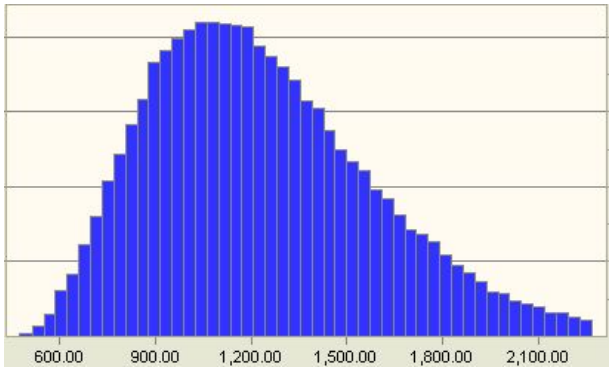

Figure 3: MCS for EAPU Upgrade.

Table 3: STS Total Program Costs [16].

Cost Category	$M FY '06
Total Program Cost	150000
Total Development	18
Total Operations Cost	149982
Operations Cost/Flight	1304

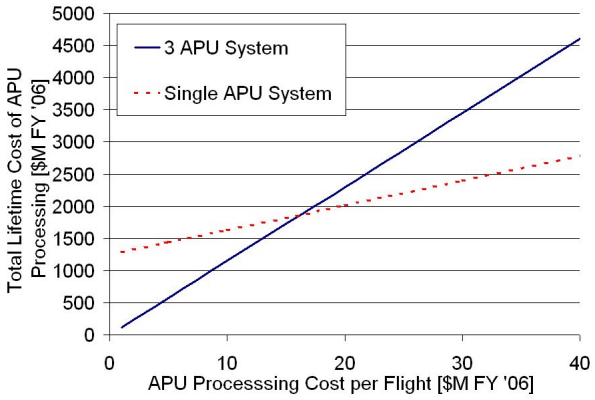

Figure 4: LCC of APU Processing.

The next problem was evaluating the potential of upgrading the reliability of a single main parachute on the CSM. The results of upgrading the main parachute are listed in Table 4. Again, the reliability and development cost increase between the Gemini and CSM programs was used to estimate the cost of increasing the reliability of a single main parachute. The same assumptions regarding the feasibility values were made and another MCS was run to explore the sensitivity of this assumption. Table 5 lists the range of cost values while Figure 5 shows the results from the MCS.

Table 4: Main Parachute Reliability Upgrade Results.

Upgrade	$R_{i,min}$	f	R_i	DDT&E FY '06
Gemini to CSM	0.985	0.9	0.9969	178 $M
Chute Upgrade	0.99	0.7	0.9984	586 $M

Table 5: Main Parachute MCS Upgrade Results Range.

Cost Range: $M FY '06		
Minimum	**Mean**	**Maximum**
383	591	891

The total operations cost for the time that the Apollo program was performing missions is estimated at $809 M FY '06 [16]. With a mean value of $591 M FY '06 for upgrading the landing system from three parachutes to a single parachute, the value for the upgrade is non-existent. The operations cost for the Apollo program were lower due to the number of years Apollo operated (five) and because it was an expendable system. There was no processing time required once the vehicle landed back on Earth. Therefore, reducing the complexity of the landing system would not have been worthwhile for the Apollo engineers.

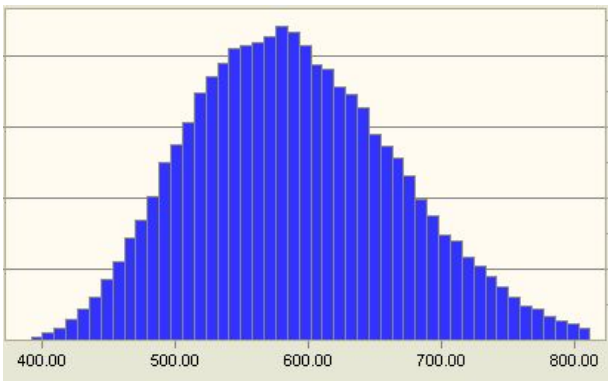

Figure 5: MCS for Main Parachute Upgrade.

6 Conclusion & Recommendations

For the STS upgrade, only one subsystem was selected. By examining more detailed operations cost data, a subsystem with a higher processing cost could have been selected for a reliability upgrade. One example could be the RCS system, which relies upon hypergolic propellants. Hypergolic propellants require unique handling and greatly increase the operations cost. If higher reliability jets could be used, then possibly some of the jets could be removed to speed up the processing time. Other redundant systems include the general computers, and the fuel cells, which all may warrant investigation for a reliability upgrade depending on their impact on STS processing.

The drawback for the reliability upgrade is that a much larger development cost would have been required. When considering budget profiles, the increase in development cost most likely would have delayed operational capability. However, the decrease in operations cost would have made the program more sustainable with a higher capability for launches per year. Overall, the STS has been an excellent vehicle for space missions, but the lessons learned regarding less complexity for better operations cost must be considered for future programs.

The reliability tradeoffs deserve consideration in order to make future programs more sustainable. In today's environment of limited budgets, a large program such as the Crew Exploration Vehicle (CEV) must use every cost saving opportunity possible. Therefore, tradeoffs between more reliable hardware and the use of redundancy should be examined during the detailed design phase. For a reusable CEV, a small increase in development cost could lead to much greater savings in LCC. With greater savings later in the program, NASA would have more freedom to support additional programs for exploration. Additionally, higher reliability components could increase performance by decreasing the total weight. More usable volume could also result from limiting the number of components through the increase of component reliability. There are enough benefits from using a fault avoidance strategy as opposed to a fault tolerant strategy that resources should be devoted to studying this tradeoff for the next vehicle design.

The methodology in this paper is not without drawbacks. Assumptions were made about the feasibility value, which has a large affect on the final cost number. The feasibility value requires a closer investigation before the methodology can be fully implemented. As mentioned earlier, the feasibility value could be linked to specific subsystem characteristics, such as the current state of the art and future technology growth. Additionally, the reliability values were assumed to be deterministic point values. For high reliability hardware, the verification process becomes much tougher as the lifetime is increased. Longer tests and development periods are required to confirm that the hardware will behave like its reliability model. However, these are small challenges to overcome considering the overall impact that could be realized. The original goal of the STS was to have aircraft-like operations; moving towards higher reliability components would help implement that vision. Future cost savings are required to make exploration a sustainable program and this methodology is one technique that could be used to help fulfill those reductions.

References

[1] A. Mettas. Reliability allocation and optimization for complex systems. In *Reliability and Maintainability Symposium, 2000. Proceedi gs. Annual*, pages 216–221, 2000.

[2] M.D. Griffin and J.R. French. *Space Vehicle Design*. Blacksburg, VA: AIAA, 2nd edition, 2004.

[3] R. Rhodes and et al. *Proposed Operability Design Requirements (TPMS)*. NASA, KSC, 2006.

[4] Shuttle mission archives. http://www.nasa.gov/mission_pages/shuttle/shuttlemissions/archives/sts-9.html, Accessed on August 11th 2006.

[5] R. Rhodes and et al. *Current Space Shuttle System Shortfalls Assessment*. NASA, KSC, 2005.

[6] M. Modarres. *What Every Engineer Should Know About Reliability and Risk Analysis*. New York: Marcel Dekker, Inc., 1993.

[7] B. Putney. Personal interview, Mar. 2006.

[8] J. Dumoulin. Auxiliary power units. http://science.ksc.nasa.gov/shuttle/technology/sts-newsref/sts-apu.html#sts-apu, Accessed on August 5th, 2006.

[9] J. Fragola and et al. Probabilistic risk assessment of the space shuttle. Technical Report N95-26398, Science Applications International Corporation, New York, NY 28 Feb. 1995.

[10] General Accounting Office. *Space Shuttle: Human Capital and Safety Upgrade Challenges Require Continued Attention*. U.S. GAO, Washington, D.C., 2000.

[11] R. Smith and et al. *Quantitative Reliability Analysis Of The STS Electric Auxiliary Power Unit Prototypes*. USA & ARES Corporation, 2000.

[12] K. Cyr. Gross domestic product deflator inflation calculator. http://www1.jsc.nasa.gov/bu2/inflateGDP.html, Accessed on August 18th, 2006.

[13] Hershkowitz. Apollo technical manual. Technical Report Z65-11545, NASA, 15 Oct. 1963.

[14] J. Duncan. Landing system. http://www.apollosaturn.com/geminiNR/sec9.htm, Accessed on August 16th, 2006.

[15] W.H. Douglas. *Gemini Reliability and Qualification Experience*. NASA, Houston, TX, 1967.

[16] R. Orloff. *Apollo By The Numbers: A Statistical Reference*. Washington, D.C.: NASA, 2001.