8. Risk and Reliability

8.1 Summary

The risk and reliability assessment of the Exploration Systems Architecture Study (ESAS) was an integral element of the architectural design process. Unlike traditional turnkey assessments used to evaluate results independently derived by designers, the risk assessment approach used in this study allowed designers to examine risk trades concurrent with the design process. This approach resulted in an architecture that met vehicle and mission requirements for cost and performance, while ensuring that the risks to the mission and crew were acceptable. This integrated approach to risk-informed design gave designers a risk-centric view of mission architecture and vehicle design to complement their traditional performance-centric view. This complementary perspective allowed them to see, among other things, that the local risk penalties incurred with some high-performance options might produce greater reliability throughout the overall architecture. That is, as the mission architectures evolved, assessments showed that, while certain element risks might increase, the overall mission risk could decrease by choosing the right combination of these dependent elements. -

Figures 8-1 and **8-2** show the general evolution of mission architectures with component risk defined. The order of architectures considered flow from top to bottom, roughly representing the manner in which the ESAS architectural investigation proceeded. In general, the risk of Loss of Mission (LOM), as well as Loss of Crew (LOC), decreased as the risk assessment guided the architecture design process. As shown in **Figures 8-1** and **8-2**, while certain trades resulted in individual penalties, the proper combination of trades generally resulted in an overall lower risk of LOM. The single-launch mission resulted in the lowest risk of LOM. However, in this case, LOC penalties for the Launch Vehicle (LV) (as shown in **Figure 8-2**) and performance limitations, in terms of landed mass on the lunar surface, prompted designers to select the Earth Orbit Rendezvous-Lunar Orbit Rendezvous (EOR–LOR) 1.5-launch hydrogen descent, pressure-fed ascent option with the lowest LOC risk and LOM risk approximately equal to that of the single-launch architecture. **Figures 8-1** and **8-2,** and the specific trade studies and results summarized in them, will be discussed in more detail in later sections.

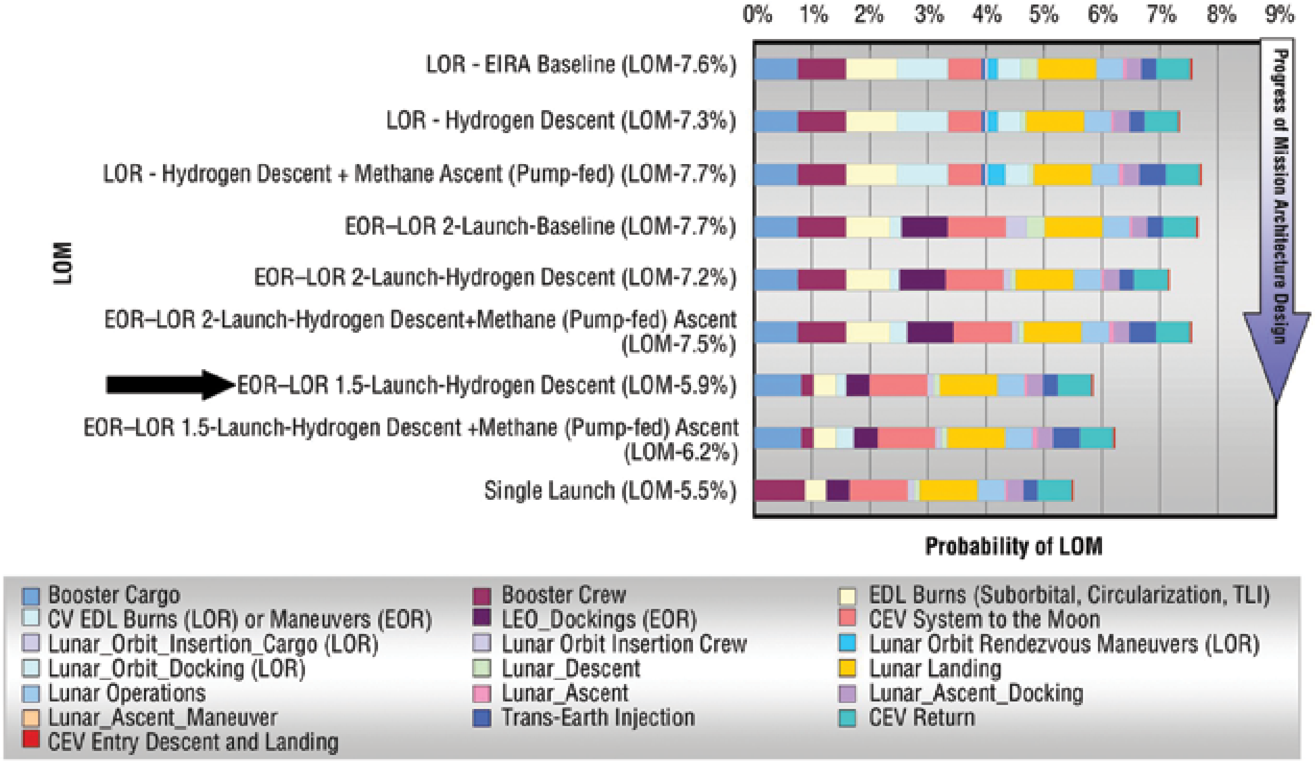


Figure 8-1. Comparison of All (

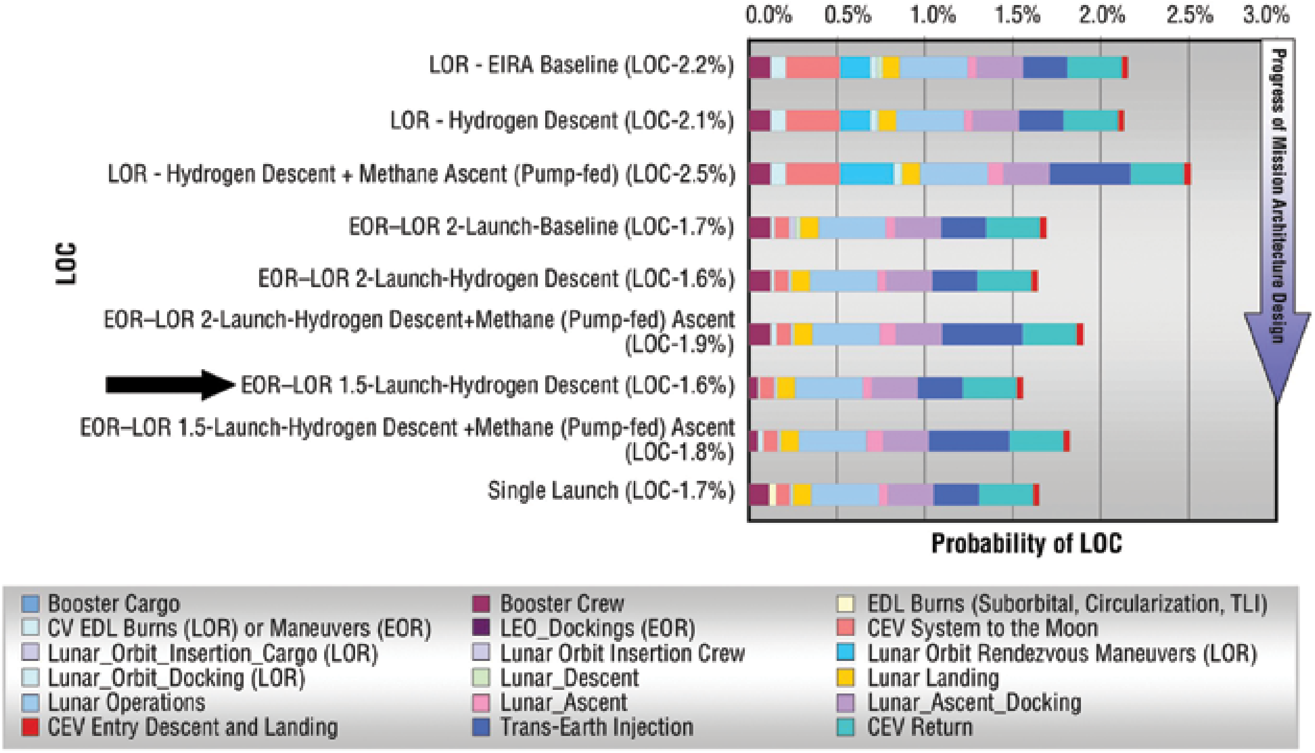


Figure 8-2. Comparison of All Cases for LOC

The risk and reliability portion of the ESAS focused on identifying "differences that made a difference" in architectural risk. The conceptual nature of proposed vehicle designs and the analysis of the mission scenarios at this stage in the process made it essential to identify the architecture-discriminating issues that would drive the risk of the program. The quantification of the individual discriminating risks was also important to ensure that concentration of risk reduction in one area did not compromise the overall risk level of the design and result in increased risk in other areas. This focus allowed program resources (i.e., mass, time, dollars) to be spent in a manner consistent with their importance to the overall architecture, not just their individual importance. Determining these drivers allowed the ESAS team to select the missions and vehicles to create architectures that would produce the highest likelihood of mission success with the least risk to the safety of the crew. Using analysis tools such as the Screening Program for Architecture Capability Evaluation (SPACE) tool (**Appendix 8A**, **SPACE Background**) and the Flight-oriented Integrated Reliability and Safety Tool (FIRST) (**Appendix 8B**, **FIRST Background**), the risks of mission and vehicle elements were quantified, and the top drivers were determined from these results. Classifying the top drivers was intended to provide guidance to future analysts indicating where to properly focus their analytical efforts and suggesting the level of resolution required for the models.

Results from quantitative risk and reliability analysis were an important input to decision-making during the design process. These results provided concrete ways to compare relative risks and to inform the design decision makers of the risk consequences of their decisions. Key programmatic decisions that were influenced by the risk assessment results included:

- Choice of lunar mission mode: The significant safety benefit of a second habitable volume in EOR missions was demonstrated in the analysis. This benefit supported the decision to use this mission mode. The safety benefit of the 1.5-launch mission architecture was demonstrated as well, due to its use of a single Solid Rocket Booster (SRB) for crew launch.
- Choice of Crew Launch Vehicle (CLV): The risk analysis demonstrated the significant benefit of the single SRB launcher with a single Space Shuttle Main Engine (SSME) upper stage, albeit recognizing the residual risk due to the SSME air-start requirement. The risk assessment supported the designer's intuition that the simplest possible system developed from the most mature propulsion elements was superior to other design choices.
- Choice of propulsion systems: The need for reliable propulsion systems for return from the lunar surface requires the propulsion systems for lunar ascent and Trans-Earth Injection (TEI) to be as simple as possible and to employ systems that are mature and have the potential for achieving acceptable reliability. The risk analysis quantified the benefit of maturing these systems during International Space Station (ISS) missions, thereby suggesting that the same propulsion system be used for both applications. This led to the elimination of pump-fed Liquid Oxygen (LOX)/methane systems for the Lunar Surface Access Module (LSAM) ascent stage because the pump-fed system would not likely be ready in time for the ISS missions. The designers discovered that a single-engine ascent stage was a preferable option to a double-engine system because the geometry and physics of the design would make it difficult to achieve a balanced single-engine ascent on a multiple-engine system. The failure predominance of the propellant supply and delivery portion of a pressure-fed system with an ablative combustion chamber and nozzle also suggested the dubious nature of the risk benefits of engine-out in the LSAM ascent stage. Finally, the analysis demonstrated that, although possibly less reliable than a hypergolic

system, the LOX/methane system could be developed in time and with sufficient reliability for the mission. The additional performance benefit of a mature LOX/methane system, along with the choice of a pump-fed LOX/hydrogen engine for LSAM descent, provided the launch mass capability to enable the 1.5-launch architecture, thus allowing for crew launch on the single-stick SRB, which has the lowest LOC probability. The LOX/methane system was also desirable to eliminate the operability issues related to hypergols and to enable the use of in-situ methane on Mars and oxygen on the Moon and Mars. The crew safety and mission success benefits provided to the overall architecture showed the individual local reliability benefits of a hypergolic Crew Exploration Vehicle (CEV) propulsion system would be overwhelmed by architectural benefits of the higher performance, albeit less mature, LOX/methane option. The use of a higher performance pump-fed LOX/hydrogen engine on the LSAM descent stage would increase performance of the engine that enables the 1.5-launch solution. The analysis also led to the elimination of the LSAM descent stage Reaction Control System (RCS), thereby simplifying the design and adding margin.

- Elimination of unnecessary radiation shielding from the CEV: Quantification of risk from radiation led to the elimination of over 1,000 kg of radiation shielding from the CEV, with a reduction in CEV mass of 2.4 mT and a reduction of injected mass by 3.7 mT. This mass enabled the 1.5-launch mission without requiring the use of a pump-fed ascent stage on the LSAM and provided more margin for the design. The 1.5-launch solution sensitivity to CEV radiation shielding is shown in **Figure 8-3**.
- Relaxation of the requirement for aerodynamic monostability: Monostability ensures that the CEV will aerodynamically trim in a single attitude. However, the requirement for monostability, in the context of the entire system, is only one way to achieve the goal of safe trim during reentry given a loss of primary flight controls. Because the monostability requirement adversely constrains the Outer Mold Line (OML) of the CEV, the requirement was relaxed to allow alternate means of maximizing architecture safety levels.
- Definition of acceptable risk: The risk assessment demonstrated that the risk of a lunar mission is significant, but it could be controlled to a level similar to what is accepted on Shuttle missions today. NASA must acknowledge this risk and execute the program accordingly. In addition, the analysis suggested that crew missions to the ISS may be at least 10 times safer than the Shuttle once the CEV service propulsion system is matured, despite the fact that the first several test missions might incur larger initial risk.

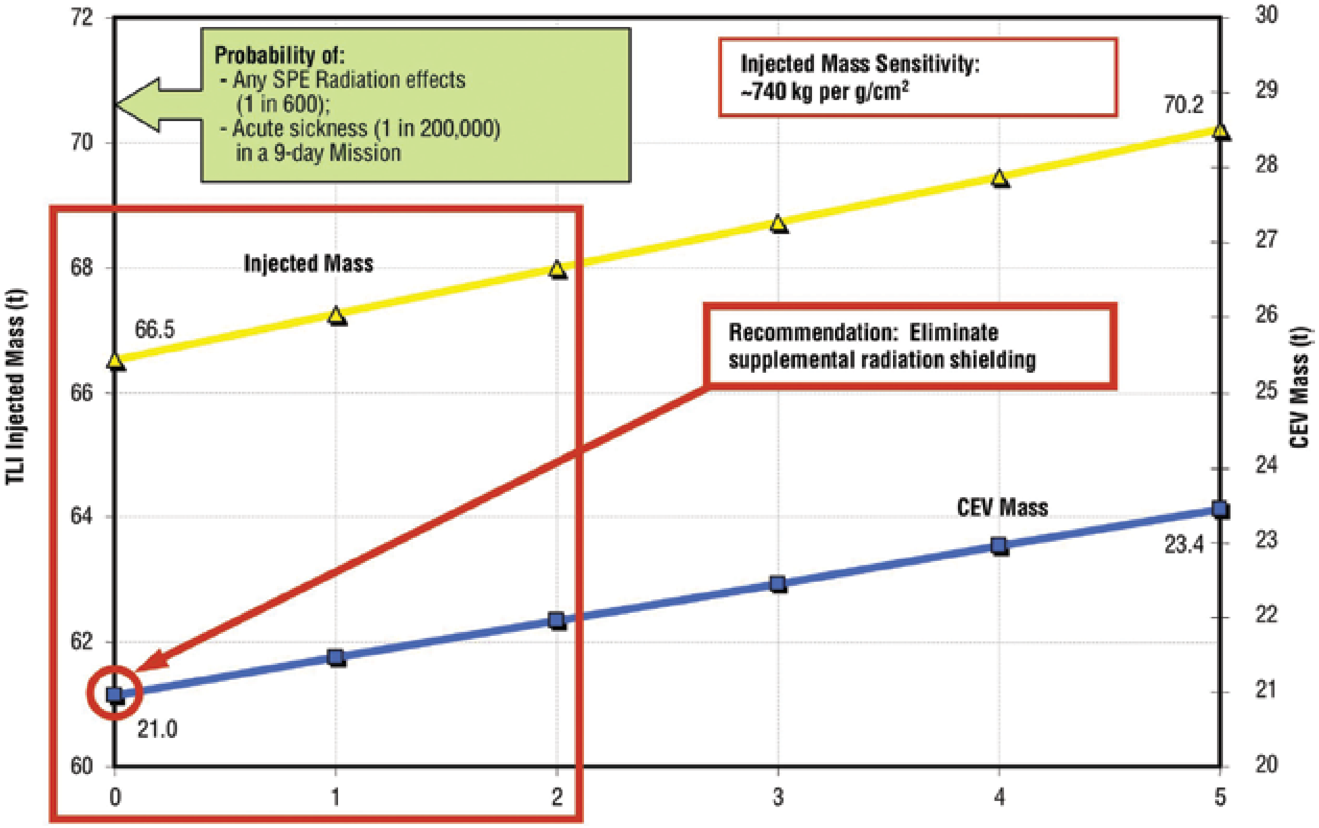


Figure 8.3. 1.5-Launch Solution Sensitivity to CEV Radiation Shielding

Risk assessment results were used to determine the highest-risk flight phases of the ESAS architecture. Pre-mission risks by flight phase are shown in **Figures 8-4** and **8-5**.

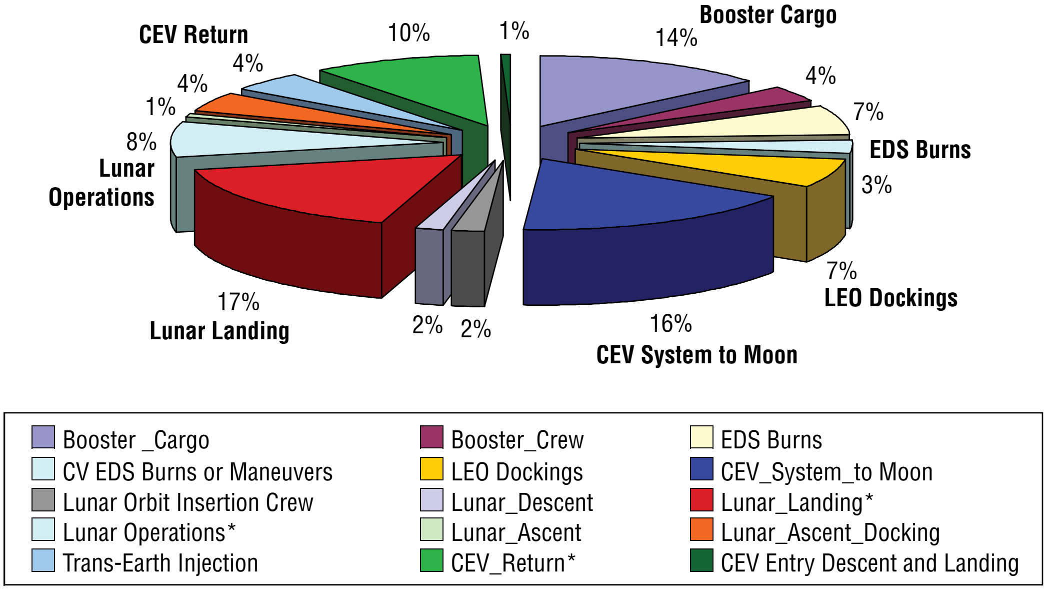


Figure 8-4. LOM Contributors for EOR–LOR 1.5-Launch Mission

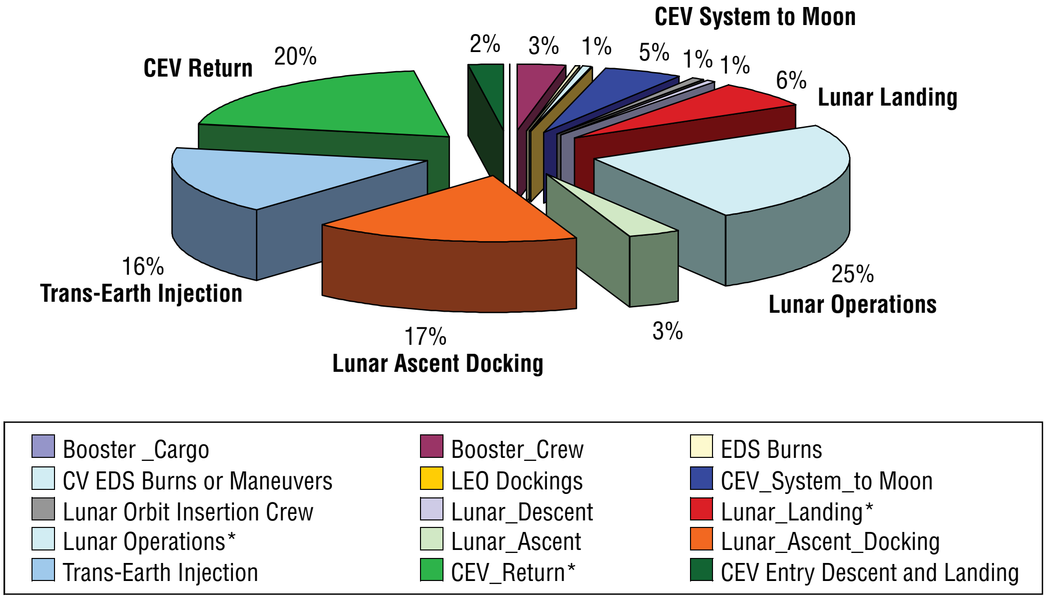


Figure 8-5. LOC Contributors for EOR–LOR 1.5-Launch Mission

The top ten risk drivers were determined to be:

- LOX/methane engine development;
- Air start of the SSME;
- Lunar-Earth reentry risk;
- Crew escape during launch;
- Liquid Acquisition Devices (LADs) in the CEV service propulsion system;

- Lunar vehicle LOX/hydrogen throttling on descent;
- Integration of the booster stage for the Heavy-Lift Vehicle (HLV);
- J–2S development for the Earth Departure Stage (EDS);
- Unmanned CEV system in lunar orbit; and
- Automated Rendezvous and Docking (AR&D).

These identified risks should be examined and tracked carefully as the architecture design and development progresses. Additional risks will certainly be added in the future. Vigilance will be needed throughout the program to assure that other risks remain low.

8.1.1 LOX/Methane Engine/RCS Development

The development of the LOX/methane engine was recognized as one of the largest architectural risks during the course of the ESAS. No LOX/methane engine has had any flight test experience and there has been only a limited number of Russian ground tests. The LOX/methane system was desirable from a performance perspective and also to eliminate the operability issues related to hypergols and to enable the use of in-situ methane on Mars and oxygen on the Moon and Mars. The choice of the simple pressure-fed design over the higher performance, but more complex, pump-fed alternative for the LOX/methane engine should significantly increase the likelihood of the engine maturing in time to meet the 2011 CEV launch date and, ultimately, to rapidly reach a high plateau reliability. Despite this forecasted eventual high reliability, the lack of heritage and flight history suggests an initially low level of maturity. In turn, this lack of maturity is reflected in a low initial forecasted success likelihood of 80 percent. This low initial value suggests that a significant test and flight program to ISS should be planned to lower this risk to the plateau value. In particular, supporting analysis using a Bayesian predictive model suggests that the engine would be forecasted to require 19 flights before this plateau is reached. (See **Appendix 8C**, **Reliability Growth**.) The forecasted growth curve of the LOX/methane engine reliability as a function of the number of test flights is shown in **Figure 8-6**.

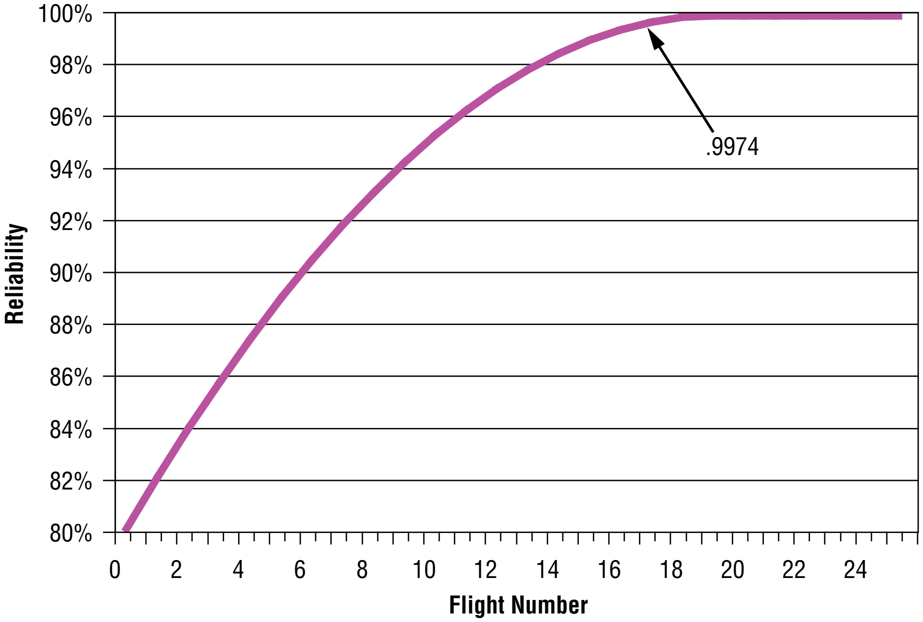


Figure 8-6. Reliability Growth of LOX/Methane Engine

The LOX/methane-based RCS has development and mission risks of its own. Existing RCSs do not require igniters. The liquid propellant for the thrusters will require conditioning prior to each firing. This will present a challenge to the RCS designers in the development of the RCS propellant supply and manifolding scheme. The propellant lines are small and would extend some distance from the tanks without proper manifolding. If individual propellant lines are used for the thrusters, leakage becomes an issue, while shared lines have the potential for common cause failures. All of these issues must be carefully considered by the designers in the ultimate RCS design development.

8.1.2 Air Start of the SSME

The SSME is a fuel-rich, combined-cycle, pump-fed LOX/hydrogen engine with significant maturity, heritage, and strong test- and flight-proven reliability. However, the CLV upper stage requires the SSME to start in flight. SSME air starts have never been demonstrated on the ground or in flight. The upper stage SSME test program will include simulated vacuum starts to aid in maturing the system. However, there is always the risk that exact conditions at staging and ignition may not be adequately simulated on the ground. The air-start function is considered moderately complex with no heritage, making it a risk driver. The initial reliability was estimated to be 70 percent due to the possibility of unknown risks. However, because of the significant SSME heritage, the system is expected to mature rapidly and reach plateau reliability in five flights. The reliability growth of an SSME air start is shown in **Figure 8-7**.

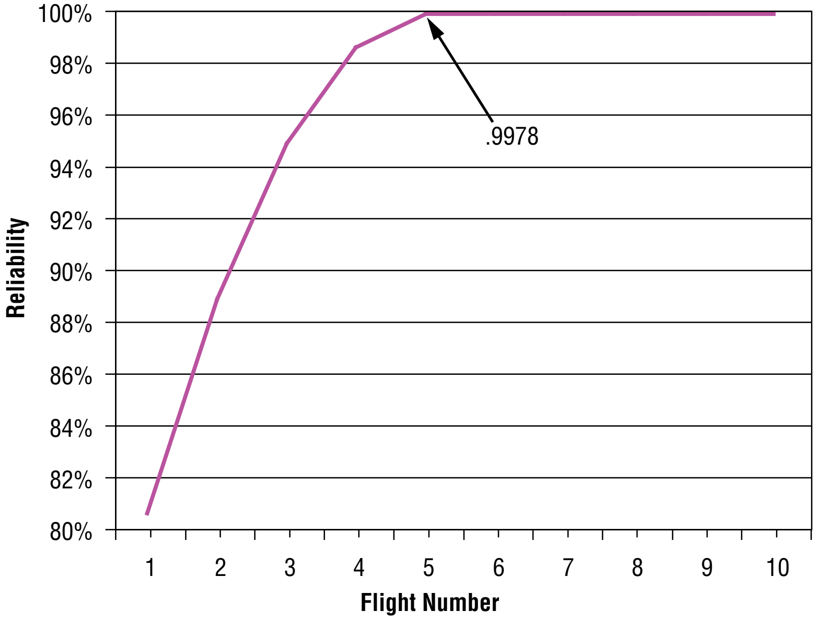


Figure 8-7. Reliability Growth of SSME Air Start (Pump-fed LOX/ Hydrogen)

8.1.3 Lunar-Earth Reentry Risk

The Thermal Protection System (TPS) is responsible for the vehicle integrity throughout reentry. Although ablative heat shields were successfully developed for the Apollo program, the development was not problem-free. **Figure 8-8** shows the many repair plugs that had to be added during the manufacture of the Apollo VII heat shield.

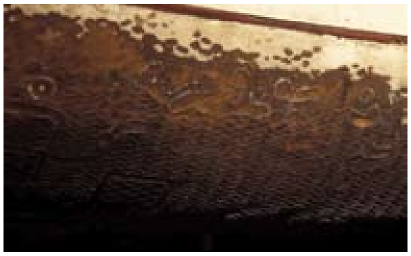


Figure 8-8. Apollo VII Heat Shield (with Repair Plugs)

In the case of the CEV versus Apollo, the much larger area of the CEV suggests significant development of the TPS would be required in spite of existing Apollo heritage. The development of the TPS for the CEV would require the certification of the manufacturing process and the ability to recreate the Apollo material. Initial analysis indicates that the performance benefits of a new material would be worth the extra effort required, instead of recertifying Apollo material. However, analysis has shown that the additional development step is not something that should be taken for granted in terms of schedule. Certifying an existing material generally leaves the methane engine development as the leading risk driver, but, if technology development is needed for the TPS, then the TPS becomes the dominant schedule driver in technology development.

Improvements in Computational Fluid Dynamics (CFD) will allow tests and simulations of vehicle reentry to be modeled to further understand this risk. Fortunately, significant progress has been made since Apollo in the area of CFD simulations of reentry conditions. **Figure 8-9** shows an initial simulation that was performed to model the contours of constant axial velocity experienced by the CEV on reentry. Such accurate representations of reentry physics were unavailable during the Apollo era and would be expected to be extremely helpful during CEV TPS design development.

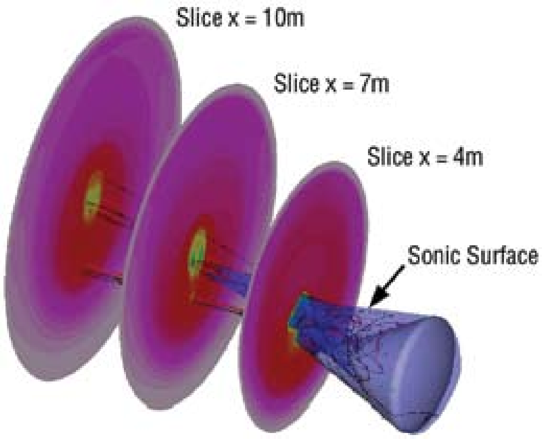


Figure 8-9. Contours of Constant Axial Velocity

8.1.4 Crew Abort During Launch

The loads applied to the vehicle on ascent, as well as other aspects of the accident environment, can pose a high risk to the crew if an abort is required. To analyze this risk, physical and logical simulations and tests are required. The required physical simulations would include: fracture and breach physics, cloud interaction and combustion physics, Navier-Stokes CFD analysis of escape and recovery, and an integrated comprehensive evaluation of both logical sequences and physical environment. **Figure 8-10** shows an example of a model of the normal aerodynamic loads applied to a vehicle on ascent. Such accurate representations of the ascent aerodynamics require the use of advanced CFD codes, representative geometric models of the vehicles, and technically adequate methodology to tie the geometry to the physics. In addition, construction of pressure and velocity profiles requires significant computational capability to represent the ascent accurately. The addition of fracture models mapping to internal motor or engine conditions, the combustion physics, and the fracture fragment propagation in the air stream makes the problem even more challenging.

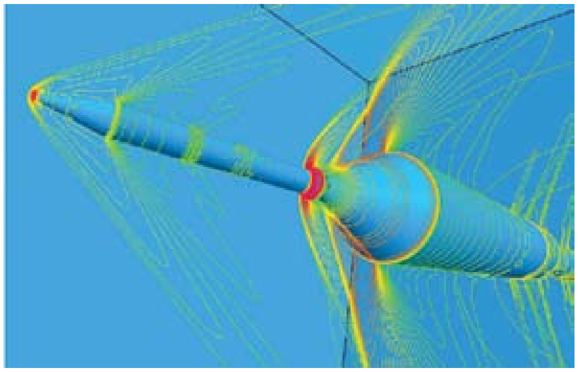


Figure 8-10. Aerodynamic Loads on Steady-State Ascent

8.1.5 LADs in the CEV Service Propulsion System

The LADs in the CEV service propulsion system will require much testing and certification to meet the required level of reliability. The Space Shuttle uses screen channel LADs in both RCS and service propulsion system tanks. Key issues are fluid properties for the design region, screen bubble point data for fluids, and modeling of temperatures of interest (i.e., subcooled LOX viscosities). A review of the history of LADs revealed several issues with their use, including the fact that the Shuttle LADs qualification program took 7 years to complete. **Figure 8-11** shows the Space Shuttle service propulsion system tank internals, including the dividing bulkhead and LAD gallery in the lower compartment.

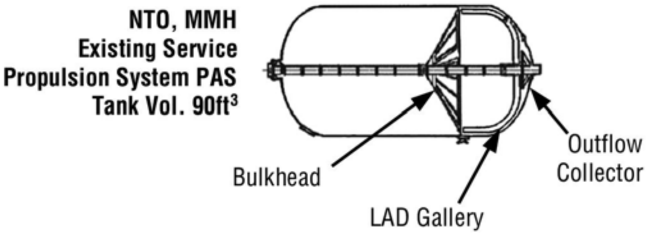


Figure 8-11. Space Shuttle Service Propulsion System Tank Internals

8.1.6 Lunar Vehicle LOX/Hydrogen Throttling on Descent

For all throttling engines, it is critical to maintain the injector pressure drops necessary for proper propellant injection and mixing over the throttling range without causing instabilities in combustion. This requirement creates a substantial risk to the LOX/hydrogen engine on the lunar vehicle for descent. One of the approaches that can be used for deep-throttling, pressure-fed engines is a sliding pintle to control engine orifice size. While experience on the LEM descent engine indicates a pintle can be used, the LEM descent engine was fueled with hypergols. No previous sliding pintle applications were found for a hydrogen-fueled engine. However, if a sliding pintle development proves problematic, there are alternative approaches that have been used successfully on at least one hydrogen-fueled engine. One throttling application was the RL–10 throttling approach shown in **Figure 8-12**. The throttling experience with the RL–10, using dual throttling valves, was used on the Delta Clipper Experimental (DC–X) program. This approach suggests alternatives that might be employed in addition to the sliding pintle. However, regardless of the approach taken, this is still an area that represents a risk to the mission and should be analyzed further.

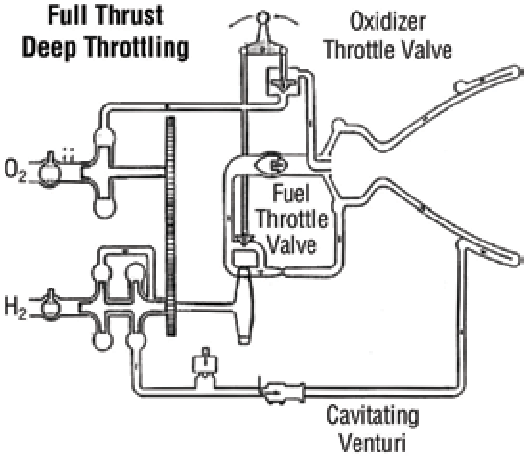


Figure 8-12. RL–10 Throttling Approach

8.1.7 Integration of Booster Stage for the Heavy-Lift Vehicle

The integration of the booster stage engines for the heavy-lift Cargo Launch Vehicle (CaLV) (**Figure 8-13**) is an element that poses a fair amount of risk. This risk is driven by the integration of two five-segment Reusable Solid Rocket Boosters (RSRBs) with five SSME cores for the booster stage. Integration risk is prominent because the SSMEs themselves are mature and reliable, as are the Shuttle SRBs, albeit in a four-segment design. Possible risks include engine propellant manifolding, thrust imbalance, thrust vectoring, and the possible interaction between the two Reusable Solid Rocket Boosters (RSRBs) and the liquid core, as well as residual uncertainties due to the addition of a fifth segment to the SRB.

Figure 8-13. CaLV Propulsion System Integration

8.1.8 J–2S Development for the EDS

The use of a J–2S engine for an Earth Departure Stage (EDS) is an area of high risk because a J–2S engine has never been flown. The J–2S (J–2 simplified) was designed to replace the Saturn vehicle upper stage J–2 engines. While the J–2S replaces the J–2's gas generator engine cycle with a simpler tap-off engine cycle, the development program for the J–2S ended in 1972. The J–2S is more than just a paper engine, however. It has significant ground test experience and was almost certified for flight. However, the J–2S development was not completely trouble-free. There were some problems with the tap-off cycle and the engine had no flight experience. Thus, the estimated time of 4 years for qualification, fabrication, and testing of the engine poses a significant risk to the program. A test firing of a J–2S engine is shown in **Figure 8-14**.

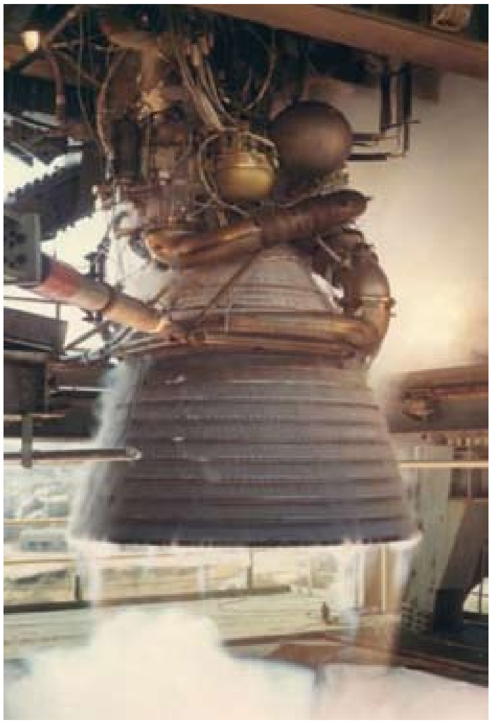


Figure 8-14. J–2S Test Firing

8.1.9 Unmanned CEV System in Lunar Orbit

For the first time, the mission will require leaving an uncrewed vehicle in lunar orbit for an extended period with eventual crew return. This vehicle must be operationally ready and must perform reliably after its quiescent period when called upon. It is expected that this risk will be effectively mitigated by the early CEV flights to the ISS since the CEV (**Figure 8-15**) is likely to remain quiescent at the ISS for even longer periods than would be required for lunar missions.

Figure 8-15. CEV

8.1.10 Automated Rendezvous and Docking (AR&D)

The final lunar mission architecture selected does not require AR&D. Pressurized cargo delivery to the ISS will require some level of AR&D; however, ISS crew will be available to provide backup capability. Other lunar missions that were considered did use AR&D. In many of these missions, the risk presented from AR&D was a driver. Even a manned vehicle docking with a passive vehicle involves significant risk as shown in **Figure 8-16**. However, it is expected that the experience gained from early CEV missions to the ISS would substantially mitigate the risk.

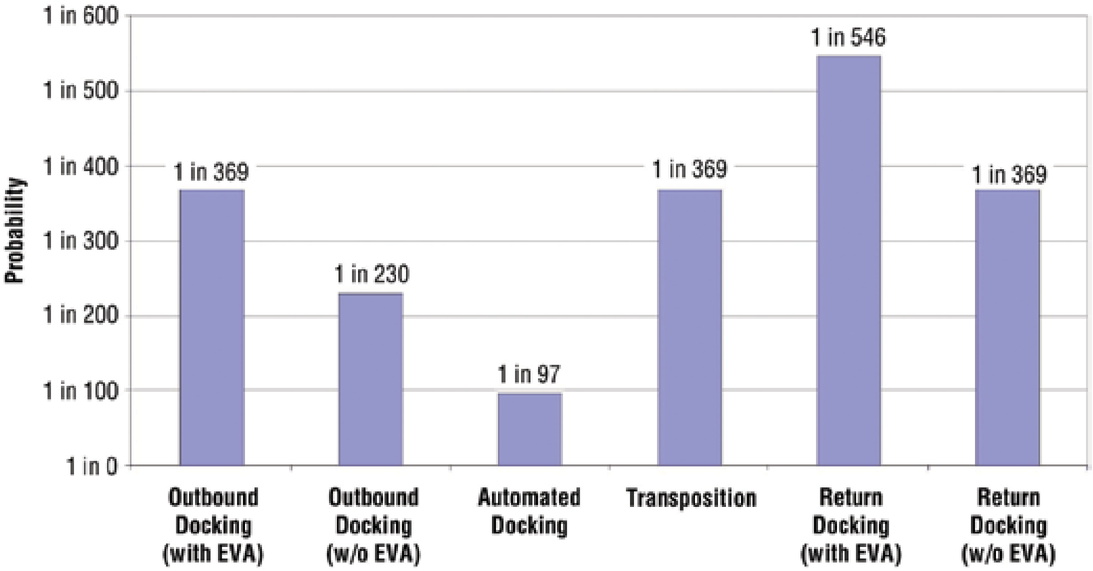


Figure 8-16. Docking Comparisons for Lunar Missions Probability of Docking Failure

8.2 Methodology

The risk assessment methodology for this project was based on a variety of techniques developed over the past few years (References 1 and 2 in **Section 8.7**, **References**). The top-down, scenario-based risk assessment approach utilized by this study is a complex process that incorporates many sources of information to produce a representative analysis. This approach combines modules that represent risk drivers in a transparent fashion so that design teams can easily understand risks, and analysts can quickly generate models. An intensive review of heritage information back to Apollo, past risk assessments, and interaction with vehicle designers and operations experts was performed by experienced analysts to identify risk drivers for ISS and lunar missions. The risk drivers of individual mission elements were combined into models for the specifics of each mission implementation. This initial risk and reliability analysis does not claim to quantify exact estimates of the reliability, instead its goal is to arrive at reasonable estimates that can be used to identify "differences that make a difference." Once these elements are identified, more analysis may be performed if a more exact estimate is required.

Three fundamental mission types were analyzed: (1) LOR, (2) EOR, and (3) direct missions. Also, three alternative propulsion system configurations were analyzed: (1) all pressure-fed LOX/methane, (2) LOX/hydrogen pump-fed lunar descent stage, and (3) pump-fed LOX/methane engines on the CEV Service Module (SM) and lunar ascent elements. Analysis showed the mission modes and propulsion options were the fundamental drivers for the risk assessments. (See **Appendix 8D**, **Mission and ISS Models**.) Once these elements were established, the risk drivers could be assembled and quantified. Once the missions were modeled, an integrated campaign model was developed to assess the integrated risks of the program.

A key aspect of the analysis was the development of maturity models for the early stages of the program. The traffic model for the campaign was combined with the maturity model to account for the benefit of flight operations on later flights. In particular, the maturing of the LOX/methane pressure-fed engine was used as a means of returning from the Moon. The campaign risk model can be used to understand the risks of missions of space flight. These risks can be combined with consequence models to understand the impacts of the risks on achieving NASA objectives and to develop strategies for coping with failures that are likely to occur. These models can discount program and performance costs based on the likelihood of accidents and quantification of risk to the overall program—such as LOC, loss of a key asset, or program cancellation due to unexpected poor performance.

The process architecture is illustrated in **Figure 8-17**. The mission description provided the fundamental basis for the analysis. The mission designers worked with design engineers to create missions that were physically realizable based on the mass and performance capabilities of feasible systems. Abort options were identified as part of the mission design. The mission elements were iterated until a mission could be described in terms of actual systems consisting of vehicles capable of being produced and launched on a feasible launcher. The mission description identified vehicles (propulsion system type, vehicle systems, redundancy). This information was used to create modular element reliability models tailored to key mission events (i.e., engine burns, rendezvous and docking, landing, Earth entry) and associated time durations (if applicable). The missions are described in **Section 8.3**, **Model Elements.**

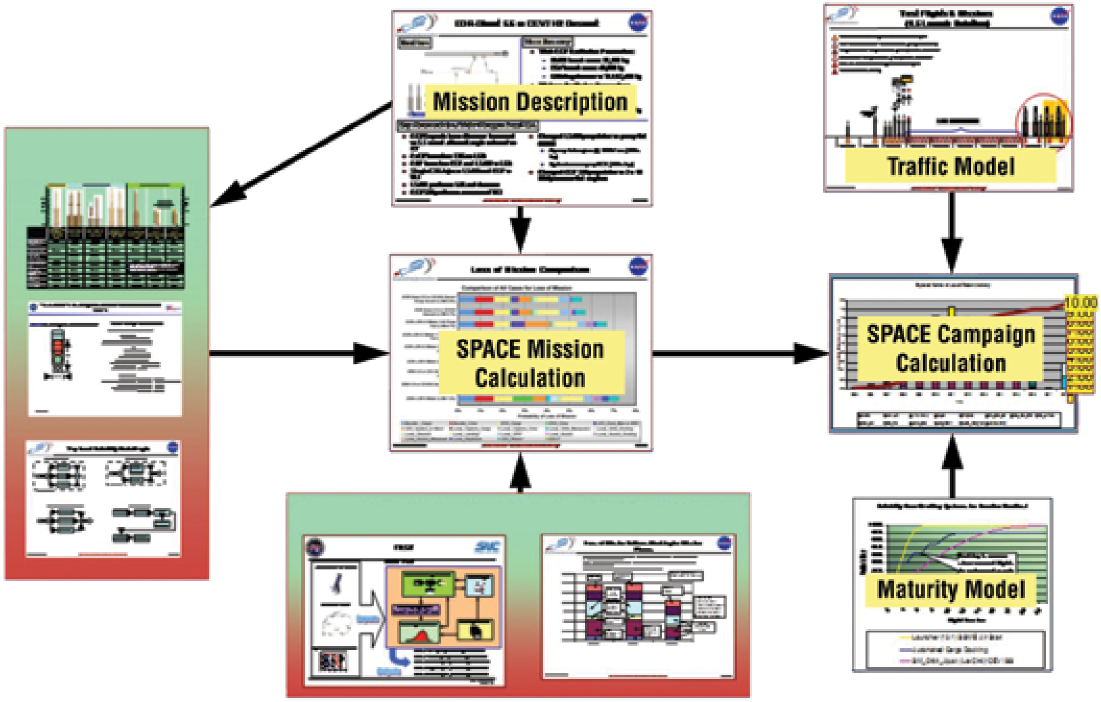


Figure 8-17. Elements of the Risk Model

Heritage information and analysis identified elements that were most likely to contribute to mission risk. These elements are shown in **Table 8-1** for each of the mission modes.

Table 8-1. Mission Elements for Mission Modes

Phase	Mission Element	Mission Mode		
		LOR	EOR	Direct
Launch	Booster Cargo	Variable**	Variable	Variable
	Booster Crew	Variable	Variable	Variable
Low Earth Orbit (LEO) Operations	EDS Burns (Suborbital, Circularization, Trans-Lunar Injection (TLI))	Variable	Variable	Variable
	Crew Vehicle EDS Burns (LOR) or Maneuvers (EOR)	Variable	Variable	Variable
	LEO_Dockings (EOR)	N/A	Variable	Variable
Transit	CEV System to the Moon	Variable	Variable	Variable
Lunar Orbit	Lunar_Orbit_Insertion_Cargo (LOR)	Variable	N/A	N/A
	Lunar Orbit Insertion Crew	Variable	Variable	Variable
	Lunar Orbit Rendezvous Maneuvers (LOR)	Variable	Variable	Variable
	Lunar_Orbit_Docking (LOR)	Variable	N/A	N/A
Lunar Descent	Lunar_Descent	Variable	Variable	Variable
	Lunar_Landing*	Constant***	Constant	Constant
Lunar Operations	Lunar Operations	Variable	Variable	Variable
Lunar Departure	Lunar_Ascent	Variable	Variable	Variable
	Lunar_Ascent_Docking	Variable	Variable	N/A
	Trans-Earth Injection (TEI)	Variable	Variable	Variable
Return	CEV_Return	Variable	Variable	Variable
Entry, Descent, and Landing System (EDLS)	CEV Entry Descent and Landing	Constant	Constant	Constant

** Indicates use of placeholder value as a conservative reliability estimate.*
*** "Variable" indicates element reliability changes with each mission mode.*
**** "Constant indicates element reliability does not change with each mission mode.*

The launch phase contains the booster vehicles. The reliability of the boosters was dependent on the number and type of engines and burn times. Crew survival was dependent on the type of failure mode (i.e., immediate without warning or delayed with sufficient warning for a crew escape system to actuate). Engine-out capability was examined and rejected due to performance requirements, while crew escape was a part of all launcher designs. The details of the launcher analysis are described in **Section 8.3.1**, **Launch Vehicles**.

The next mission phase was Low Earth Orbit (LEO). The LOR mission mode only requires a circulation and TLI burns for the CEV and LSAM. The EOR and direct missions require rendezvous and manual docking of the elements before a single TLI burn. EOR missions with two launches require an additional transposition and docking maneuver for the LSAM and CEV prior to docking with the EDS. All of the activities in this mission phase have abort capability. The reliability of the in-space propulsion systems is documented in **Section 8.3.2**, **In-Space Propulsion Systems**, and the docking maneuver reliability is documented in **Section 8.3.4**, **Reliability Estimates for the Rendezvous and Docking of the CEV and Lunar Mission Architecture Elements**. The reliability of abort capability was estimated at 90 percent. This reliability is judged to be conservative given the proximity of the CEV to Earth and will be refined when a detailed analysis of failure modes is performed.

The transit phase represents the operation of the vehicles on the way to the Moon. The mission modes are configured differently. The main effect of this configuration is the availability of a second habitable crew volume (the LSAM) for the EOR missions, which allows for an Apollo-13-type of abort capability. Recovery after the CEV failure is assessed for each failure mode. The reliability and recovery of the CEV is documented in **Section 8.3.3**, **Mission Elements – CEV, SM, and LSAM Systems Probability Estimates**.

Lunar orbit includes the Lunar Orbit Insertion (LOI) burns for the vehicles and maneuvering and docking for the LOR missions. These events are quantified based on the engine burns employed for specific propulsion systems. Most of the missions employed either the EDS or LSAM for these maneuvers, leaving the SM service propulsion system as a backup for abort. The docking activities were quantified in **Section 8.3.4**, **Reliability Estimates for the Rendezvous and Docking of the CEV and Lunar Mission Architecture Elements**, and the propulsion maneuvers were modeled in **Section 8.3.2**, **In-Space Propulsion Systems**.

The lunar descent phase includes the engine burns for lunar descent documented in **Section 8.3.2**, **In-Space Propulsion Systems**. Abort from lunar descent is possible for all mission modes using the upper stage of the LSAM for LOR and EOR missions and the SM service propulsion system for the direct missions. A reliability of 99 percent was estimated for this event. The reliability of initiating an abort, given engine or landing failure, is assessed to be 90 percent. A more detailed assessment will be performed when additional details of the mission are specified.

The lunar operations phase was modeled for the LSAM for the EOR/LOR missions and the CEV for the direct missions. These models are documented in **Section 8.3.4**, **Reliability Estimates for the Rendezvous and Docking of the CEV and Lunar Mission Architecture Elements**. This analysis considered the operability and recovery failures of the crew habitat. No Extra-Vehicular Activities (EVAs) were modeled. Additional detail will be added to the model when specific activities and modes are identified. Crew survivability after an LOM failure was quantified in a similar fashion to the transit failures, by assessing the ability to return to the CEV for each LOM failure mode. Effects of risk from extension of lunar stay time are modeled in **Section 8.3.5**, **Lunar Surface Stay Risk Change**.

The lunar departure phase includes ascent from the lunar surface and TEI burn by the propulsion systems quantified in **Section 8.3.2**, **In-Space Propulsion Systems**. There is no diverse backup for these events, so LOM failures lead directly to LOC. LOR and EOR missions require rendezvous and docking which is documented in **Section 8.3.4**, **Reliability Estimates for the Rendezvous and Docking of the CEV and Lunar Mission Architecture Elements**.

The return portion of the mission is represented by the CEV modeled in **Section 8.3.3**, **Mission Elements – CEV, SM, and LSAM Systems Probability Estimates**. There is no diverse backup for these events, so LOM failures lead directly to LOC.

The final phase of the mission is the Earth Entry, Descent, and Landing (EDL). This mission phase is assessed in **Section 8.3.6**, **CEV Stability Impacts on Crew Safety During Entry**. There is no diverse backup for these events, so LOM failures lead directly to LOC.

The SPACE model was used to combine the results of the analysis of each element within each mission. The SPACE model directly captured the risk results for each mission element. These elements were identified by event name and then identified in an element database. The SPACE model also provided a way to capture specific engine burn definitions for each stage. These values were input into the FIRST propulsion model which returned the probability that failure occurred in the specified engine burn. The SPACE model extracted the burn failure probabilities from the propulsion database. LOM and LOC probabilities were calculated by summing the event probabilities together. The LOC probability was calculated by multiplying the LOM failure probability by the conditional probability that there is a fatality given the LOM risk. Since the ISS missions matured most of the critical hardware used for the lunar mission, the SPACE model for lunar missions did not vary. A sample SPACE mission model is shown in **Table 8-2**.

Table 8-3. SPACE Campaign Model

EOR–LOR 1.5-launch - Hydrogen Descent						
Generic Event	**Mission Event**	**Event_Name**	**Number**	**LOM**	**Fatal**	**LOC**
Booster _Cargo	Booster _Cargo	Booster-27-3 Cargo	1	0.81%	0%	0.00%
Booster_Crew	Booster_Crew	Booster-13.1	1	0.22%	23%	0.05%
EDS_Cargo	S2–44.9 TLI Burn Eng Out 1.5-Launch	S2–44.9	1,2,3	0.40%	1%	0.00%
EDS_Crew	SM Rendezvous and Docking	SM_EOR_H2 Descent	1,2	0.17%	5%	0.01%
LEO_Dock	LEO_Dock	DOC_Man_Pass	1	0.40%		0.00%
CEV_System_to Moon	CEV/lander trans-lunar coast	CEV_LSAM_EOR_LOR	1	1.00%	8%	0.08%
Lunar_Capture_Cargo			0	0.00%		0.00%
Lunar_Capture_Crew	LSAM perform lunar capture	LSAM_EOR_H2 Descent_Descent	1,2,3	0.11%	10%	0.01%
Lunar_Orbit_Maneuvers			0	0.00%		0.00%
Lunar_Orbit_Docking			0	0.00%		0.00%
Lunar_Descent	LSAM lunar descent 4 5K 2 burns	LSAM_EOR_H2 Descent_Descent	4,5	0.10%	10%	0.01%
Lunar_Landing*	Lander/CEV lunar landing	LSAM-Landing	1	1.00%	10%	0.10%
Lunar_Ops**	Surface mission – 96 hours, 4 EVAs	Lunar_OPS EIRA_EOR_LOR	1	0.47%	82%	0.39%
Lunar_Ascent	Lunar_Ascent	LSAM_EOR_H2 Descent_Ascent	1	0.05%	100%	0.05%
Lunar_Ascent_Docking	Lunar_Ascent_Docking	DOC_Man_Ascent	1	0.26%	100%	0.26%
Lunar_Ascent_Maneuver	Lunar_Ascent_Maneuver			0.00%		0.00%
Lunar_Departure	CEV "ascent stage" (SM) performs TEI burn, CEV trans-Earth coast	SM_EOR_H2 Descent	3,4,5	0.25%	100%	0.25%
CEV_Return	CEV trans-Earth coast	CEV_Return_EIRA_EOR_LOR	1	0.58%	53%	0.31%
EDLS	CEV direct Earth entry	CEV-EDLS	1	0.04%	100%	0.04%

** Indicates use of placeholder values as conservative reliability estimates.*
*** Does not include EVA risk.*

Failure probabilities of ISS missions changed with time as key systems matured. ISS missions were characterized as Launch, Orbital Maneuvers to Station, and Docking (manual for crew, automated for cargo). With the exception of the manual docking mission, a maturity model was used to address the risk of ISS operations while the CEV matured. A maturity model was developed for many different technologies. When the final missions were identified, specific vehicle maturity models were developed. This analysis is documented in **Section 8.6, Forward Work**.

The SPACE campaign model integrates all the models together to provide a risk profile for the integrated program. The SPACE campaign model is shown in **Table 8-3**. The traffic model was used to call out the individual missions for each year. CEV missions are captured and mapped into the elements of the maturity model and used to calculate the reliability of each mission as the elements mature. The LOM risk is calculated from the individual mission risk models and integrated with the maturing elements to calculate the expected number of lost missions per year. The LOC model calculates the probability of LOC for each mission for each year. The probabilities are then converted to reliabilities and multiplied together to calculate the probability of total success. The probability of failure is the complement of the probability of success.

Table 8-3. SPACE Campaign Model

Mission Flight Rates														
Missions	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Shuttle	1	3	5	5	3	3	0	0	0	0	0	0	0	0
HTV (H2)	0	0	0	0	1	1	1	1	1	1	1	1	0	0
ATV (Ariane)	0	1	1	1	1	1	1	1	1	1	1	0	0	0
Soyuz	0	1	1	2	2	2	1	0	0	0	0	0	0	0
Progress	0	0	0	3	3	4	5	0	0	0	0	0	0	0
CEV_DEV_SO	0	0	0	0	1	1	2	0	0	0	0	0	0	0
CEV_DEV_ORB	0	0	0	0	0	0	2	0	0	0	0	0	0	0
ISS_UnPress	0	0	0	0	0	0	1	0	1	1	1	1	0	0
CEV_ISS	0	0	0	0	0	0	1	2	2	2	2	2	0	0
ISS_Pres	0	0	0	0	0	0	0	3	3	3	3	3	0	0
Con-1	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Con-2	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Con-3	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Con-4	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Maturity Model														
SM_Orbit_Ajust (LOXCH4)/CEV ISS	20.0%	20.0%	20.0%	20.0%	20.0%	20.0%	20.0%	12.7%	5.9%	1.2%	0.3%	0.3%	0.3%	0.3%
Launcher (13.1)	30.0%	30.0%	30.0%	30.0%	30.0%	30.0%	30.0%	1.5%	0.2%	0.2%	0.2%	0.2%	0.2%	0.2%
Docking_Auto_ station	10.0%	10.0%	10.0%	10.0%	10.0%	10.0%	10.0%	7.2%	2.3%	2.0%	2.0%	2.0%	2.0%	2.0%
Loss of Mission Risk														
Shuttle	0.01	0.03	0.05	0.05	0.03	0.03	–	–	–	–	–	–	–	–
HTV (H2)	–	–	–	–	0.29	0.27	0.26	0.25	0.24	0.23	0.22	0.21	–	–
ATV (Ariane)	–	0.06	0.05	0.05	0.04	0.03	0.03	0.03	0.02	0.02	0.02	–	–	–
Soyuz	–	0.01	0.01	0.02	0.02	0.02	0.01	–	–	–	–	–	–	–
Progress	–	–	–	0.12	0.12	0.16	0.20	–	–	–	–	–	–	–
CEV_DEV_SO	–	–	–	–	0.01	0.19	0.21	–	–	–	–	–	–	–
CEV_DEV_ORB	–	–	–	–	–	–	0.44	–	–	–	–	–	–	–
ISS_UnPress	–	–	–	–	–	–	0.33	–	0.08	0.03	0.02	0.02	–	–
CEV_ISS	–	–	–	–	–	–	0.19	0.22	0.08	0.02	0.01	0.01	–	–
ISS_Pres	–	–	–	–	–	–	–	0.37	0.14	0.08	0.07	0.07	–	–
Con–1	–	–	–	–	–	–	–	–	–	–	–	–	0.03	–
Con–2	–	–	–	–	–	–	–	–	–	–	–	–	0.03	–
Con–3	–	–	–	–	–	–	–	–	–	–	–	–	–	0.05
Con–4	–	–	–	–	–	–	–	–	–	–	–	–	–	0.06
Total Incidents	**0.01**	**0.11**	**0.22**	**0.46**	**0.96**	**1.68**	**3.35**	**4.21**	**4.78**	**5.16**	**5.51**	**5.83**	**5.88**	**5.99**
Loss of Crew Risk														
Shuttle	1.0%	3.0%	5.0%	5.0%	3.0%	3.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Soyuz	0.0%	0.3%	0.3%	0.5%	0.5%	0.5%	0.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
CEV_ISS	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	1.9%	2.2%	0.8%	0.2%	0.1%	0.1%	0.0%	0.0%
Con-3	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.6%
Con-4	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	1.5%
Total Success	**99.0%**	**95.8%**	**90.8%**	**85.8%**	**82.8%**	**79.9%**	**78.2%**	**76.5%**	**75.9%**	**75.7%**	**75.6%**	**75.5%**	**75.5%**	**75.5%**
Probability_LOC	**1.0%**	**4.2%**	**9.2%**	**14.2%**	**17.2%**	**20.1%**	**21.8%**	**23.5%**	**24.1%**	**24.3%**	**24.4%**	**24.5%**	**24.5%**	**24.5%**

8.3 Model Elements

8.3.1 Launch Vehicles

A team led by the MSFC Safety and Mission Assurance Office (S&MA) assessed more than 30 LV concepts to determine LOM and LOC estimates. Evaluations were based on preliminary vehicle descriptions that included propulsion elements and Shuttle-based LV subsystems. The team ensured that every analysis used a strictly uniform methodology for combining vetted failure rates and probabilities for each subsystem.

Assessment results were validated using available LV reliability estimates and a simple point-estimate reliability model. Complete descriptions of the analyses methodology, results evaluations, and assessment validations are provided in **Appendix 6D**, **Safety and Reliability**. A complete description of how the team developed reliability predictions for each LV system considered in the similarity analyses is provided in **Section 6.8**, **LV Reliability and Safety Analysis**.

The stochastic LOC and LOM distributions for each of the CLV results are shown graphically in **Figures 8-18** and **8-19**, respectively. **Figures 8-20** and **8-21** show similar graphics for lunar CaLV LOC and LOM. Detailed LV reliability information is provided in **Sections 6.5**, **Crew Launch Vehicle**, **6.6**, **Lunar Cargo Vehicle**, **6.8**, **LV Reliability and Safety Analysis**, and **Appendix 6D**, **Safety and Reliability**.

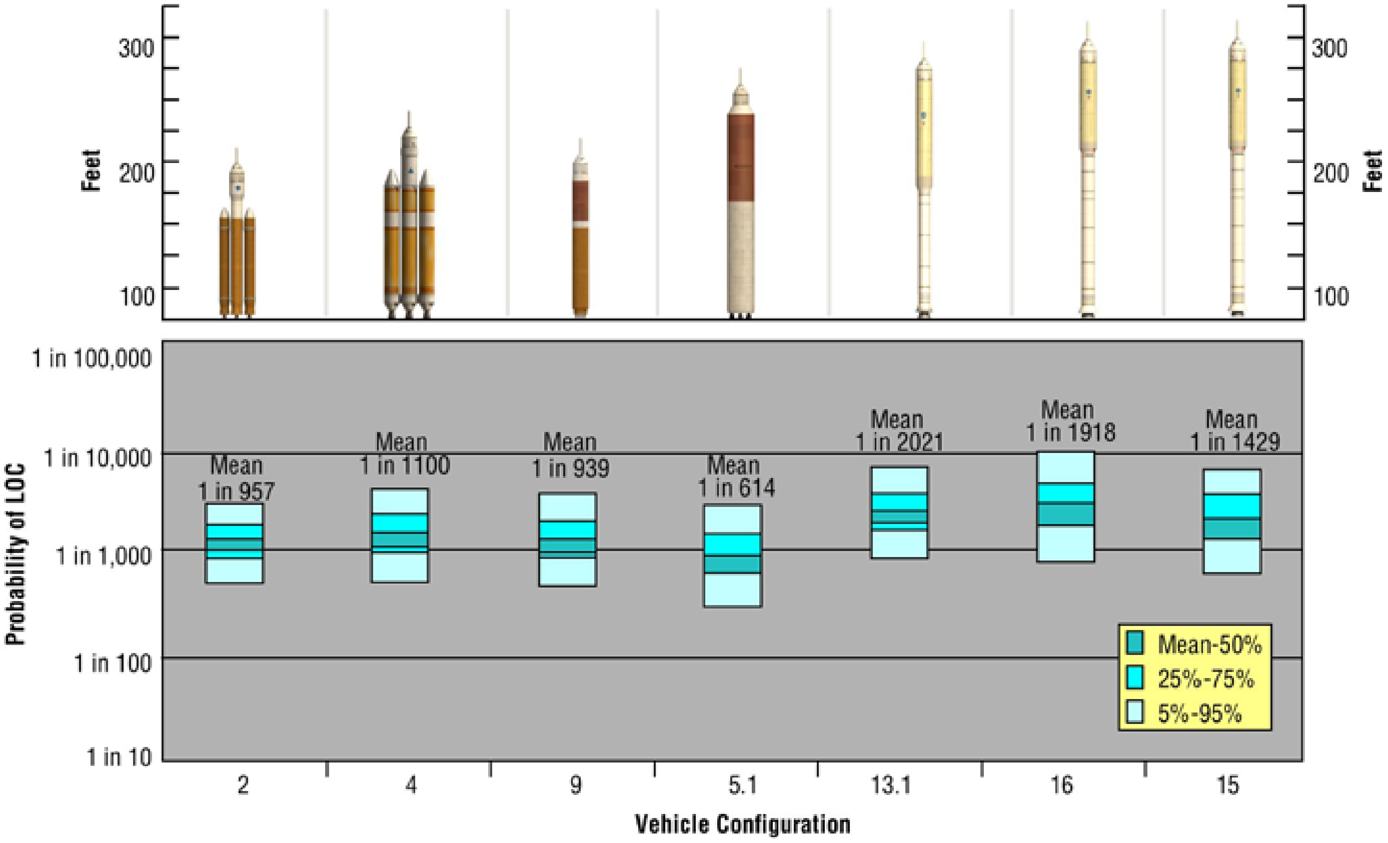


Figure 8-18. CLV LEO Launch Systems LOC

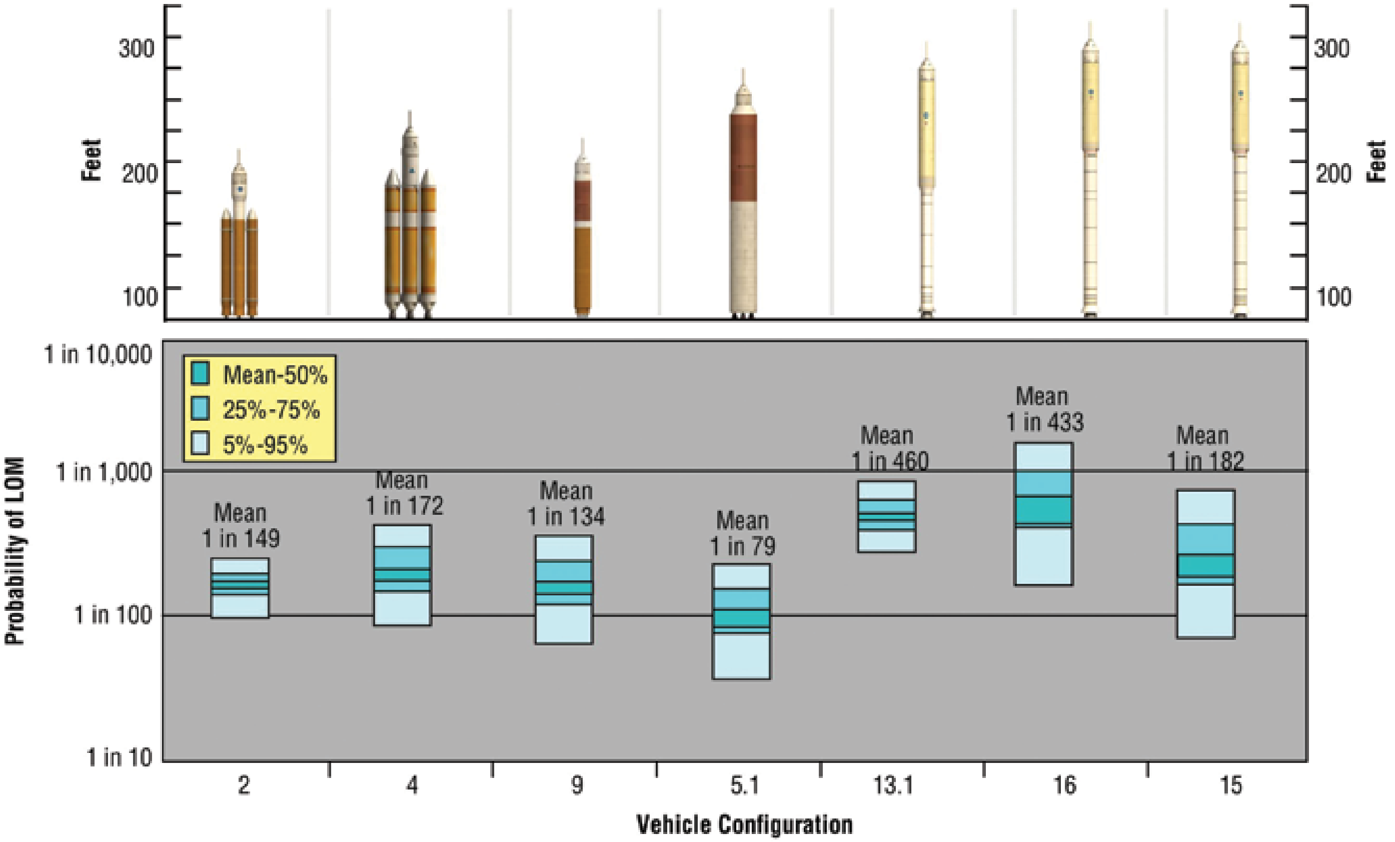


Figure 8-19. CLV LEO Launch Systems LOM

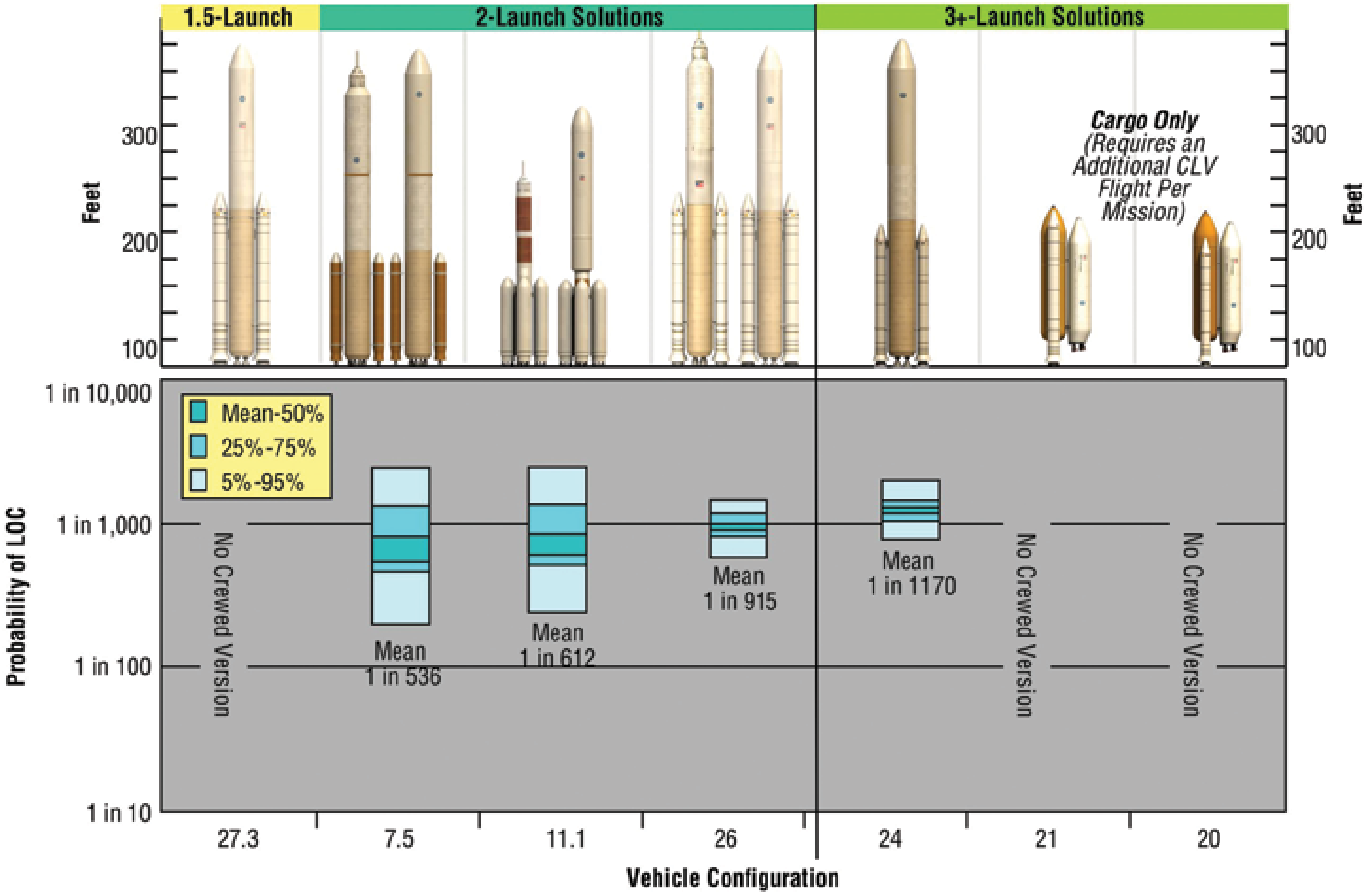


Figure 8-20. Lunar CaLV Launch Systems LOC

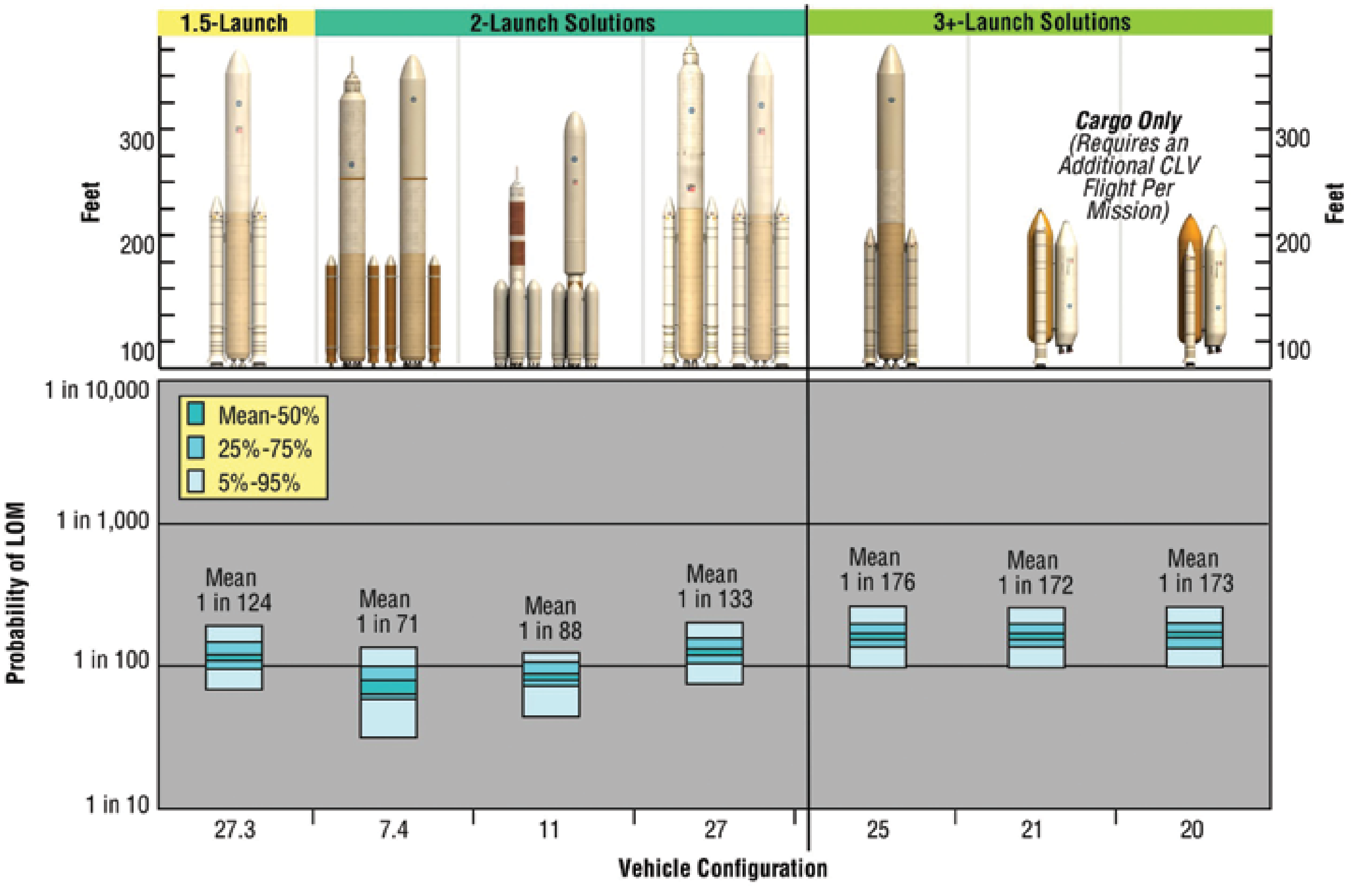


Figure 8-21. Lunar CaLV Launch Systems LOM

8.3.2 In-Space Propulsion Systems

A liquid propulsion system reliability model was developed in support of the ESAS. Reliability trades on number of engines, engine cycle, propellant type, and engine-out scenarios were performed. The model was then used to predict the propulsion stage reliability for specific in-space architecture.

The liquid propulsion system reliability model reflects a systems approach to reliability modeling, i.e., the model simulates an engine in a propulsion system that includes Main Propulsion System (MPS) elements and avionics elements. **Figure 8-22** shows a schematic of the modeled liquid propulsion system. The schematic shows the engine boundaries. For pressure-fed configurations, the engine boundaries contain injector, chamber, nozzle, and igniters. For pump-fed configurations, the engine boundaries also contain the turbopumps and engine propellant valves.

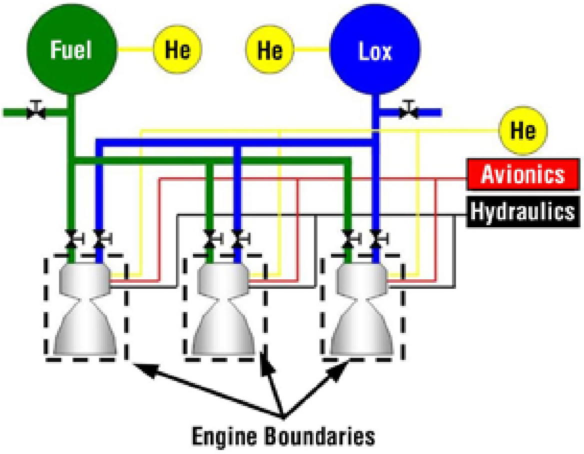


Figure 8-22. Liquid Propulsion System Schematic

The model reflects those physical elements that would have a significant contribution to stage reliability. For example, an engine purge system is indicated because of the potential requirement for restart. However, while a fill-and-drain system would be present physically, such a system would be verified and latched prior to launch commit and, therefore, is not modeled here. Note that, because the engine interface requirements are not known, the avionics, pneumatics, and hydraulic subsystems are modeled as grouped elements. For the purpose of this assessment, MPS refers to the non-engine components of the propulsion system including avionics, hydraulics, pneumatics, and propellant-feed systems.

The liquid propulsion system reliability model described here is an event-driven, Monte Carlo simulation of the schematic shown in **Figure 8-22**. For each event, the cumulative failure distribution is randomly sampled to obtain a time-to-failure. The time-to-failure is compared to mission burn time. If the time-to-failure is less than the burn time, a failure is recorded. The event logic for the reliability model is shown in **Figure 8-23**. Note that parallel events indicate that a failure in any one path is a system failure, as indicated on the event tree as an "OR" failure scenario. **Figure 8-23** shows the top-level events where the engine cluster is modeled in parallel with failures in the purge system and external leakage events. **Figure 8-23** shows the breakdown of the cluster where each engine is modeled along with support systems. It also shows the further breakdown of the engine support systems to include the avionics, pneumatics, and hydraulics provided to the engines. **Figure 8-23** shows the sequence of events modeled at the individual engine level to include isolation valve failures and engine start and main stage failures. All steps must be successful for a successful engine burn.

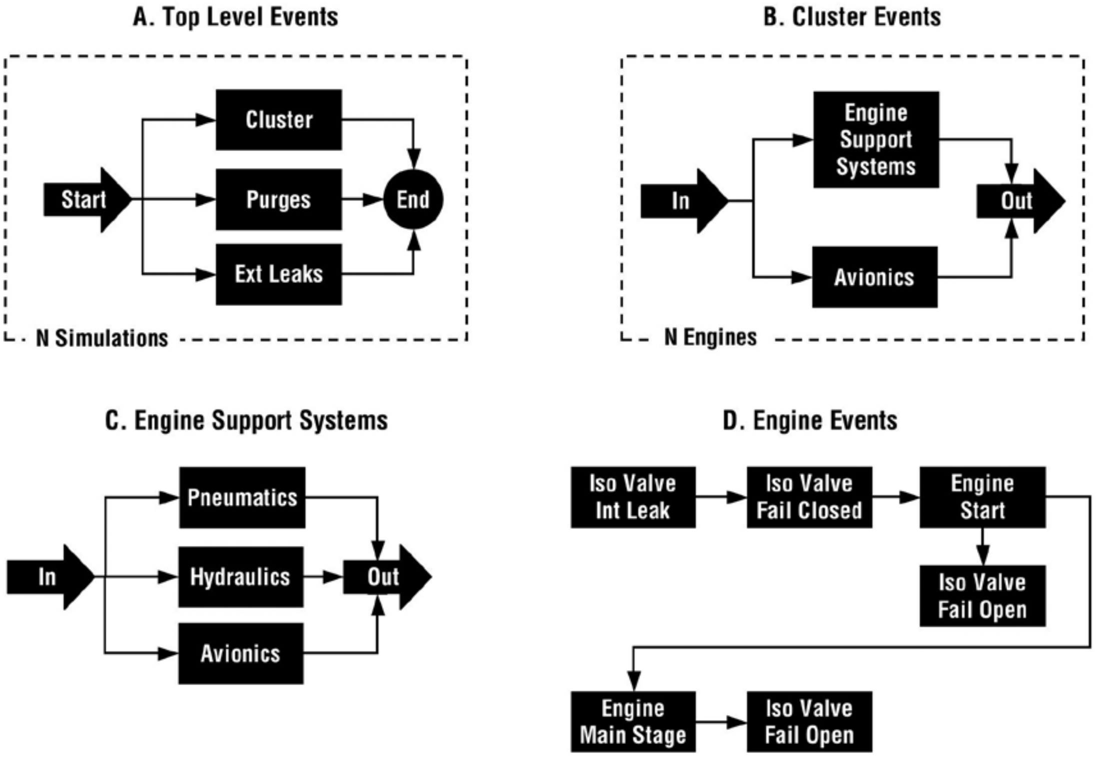


Figure 8-23. Event Logic Model

For engine-out cases, if a first benign failure is recorded, then the burn time is scaled by the ratio of the original number of engines divided by the number of operational engines remaining. The time-to-failure for the remaining operational engines are compared to this new extended burn time. If the time-to-failure of any one of the remaining operational engines is less than the new extended burn time, then a stage failure is recorded.

8.3.2.1 Data Sources and Event Quantification

The data source for quantifying the non-engine events is the Space Shuttle Probabilistic Risk Assessment , Iteration 2.0 (Reference 3 in **Section 8.7**, **References**). The one exception is that the avionics failure rates for the Space Shuttle Orbiter were not available; the engine controller failure rates for the SSME were used instead. **Table 8-4** shows the failure parameters that were used for quantifying the non-engine failure events. The effect of using Space Shuttle data to quantify event probabilities is that Space Shuttle design and operational philosophies are inherently assumed.

Table 8-4. Non-Engine Failure Event Parameters

Event	Number Per Engine	Distribution Type	Distribution Parameters

Purge Valve Failure	2	Weibull	Shape = 0.5
			Scale = 8.02×1012

External Leakage	6	Weibull	Shape = 0.5
			Scale = 1.73×1012

Pneumatic System Failure	1	Weibull	Shape = 0.5
			Scale = 5.12×1018

Hydraulic System Failure	1	Weibull	Shape = 0.5
			Scale = 5.12×1018

Avionics System Failure	1	Weibull	Shape = 0.5
			Scale = 1.14×1011

Isolation Valve – Internal	2	Demand	Mean = 3.15×10^{-6}
Isolation Valve – Fail Open	2	Demand	Mean = 3.88×10^{-4}
Isolation Valve – Fail Closed	2	Demand	Mean = 2.23×10^{-4}

For pump-fed engine cycles, a similarity analysis using SSME as a baseline was performed to obtain main stage engine failure rates. The isolation valve failures events represented valves with redundant actuation (i.e., SSME valves). The similarity analysis provided main stage engine catastrophic failure probability per second and the catastrophic failure fraction. For pressure-fed engine cycles, the Space Shuttle Orbital Maneuvering System (OMS) was used as a baseline. The data source for the failure rates for the OMS was the Space Shuttle Probabilistic Risk Assessment, Iteration 2.0 (Reference 3 in **Section 8.7**, **References**). For a single OMS thruster, a catastrophic failure probability of 1.03×10^{-6} is predicted for a typical four-burn mission. Each burn was assumed to be 200 sec. This results in a per-second catastrophic failure probability of 9.72×10^{-9}. **Table 8-5** shows the engine failure parameters used for this study.

Table 8-5. Engine Failure Parameters

Engine	Pstart	Pcat/s (First Launch)	Pcat/s (Mature)	CFF
In Space Stages				
LH–10K	0.0001	–	1.89^{-07}	0.05
LH–15K	0.0001	–	1.97^{-07}	0.05
LH–20K	0.0001	–	2.03^{-07}	0.05
LM–10K Pump	0.0005	–	1.89^{-07}	0.05
LM–15K Pump	0.0005	–	1.97^{-07}	0.05
LM–20K Pump	0.0005	–	2.03^{-07}	0.05
LM–XK Pressure-fed	0.0005	–	9.72^{-09}	0.25

The difference in Pstart (probability of engine start) between the hydrogen and methane engines is an impact of the propellant. LOX/methane flammability limits are only 58 percent as wide as LOX/LH2. Thus, tighter mixture ratio control is required for LOX/methane systems. Additionally, the minimum ignition energy for LOX/methane is an order of magnitude higher than for LOX/LH2. Thus, higher performing spark igniters are required for LOX/methane. A technology development program would most likely reduce the fail-to-start probability for a LOX/methane system. However, until such a program can be completed, the benefit of such a program cannot be incorporated into the analysis. The contribution to stage unreliability of main stage engine failures is much less for the pressure-fed configurations as compared to the pump-fed configurations. This is in keeping with the data from the Space Shuttle, which indicated that pressure-fed engines are more reliable.

8.3.2.2 Architecture Case Study

Many alternative propulsion options were considered during the ESAS. The possibility of engine-out capability was considered for pump-fed stages due to the significantly higher failure rates for pump-fed systems. However, because of the smaller mass and volume of the LSAM ascent stage and the restrictions on thrust vectoring the ascent engine(s), it would be physically difficult to implement engine-out, even if there were theoretical reliability benefits. That is, there would be great difficulty maintaining the thrust vector with one engine because of thrust imbalances without a significant increase in RCS capability. Therefore, the only stage that had engine-out was the LOX/hydrogen LSAM descent stage.

A reliability case study of the in-space propulsion stages for the 1.5-launch configuration was performed. **Figure 8-24** shows the results of the architecture case study both by stage and burn.

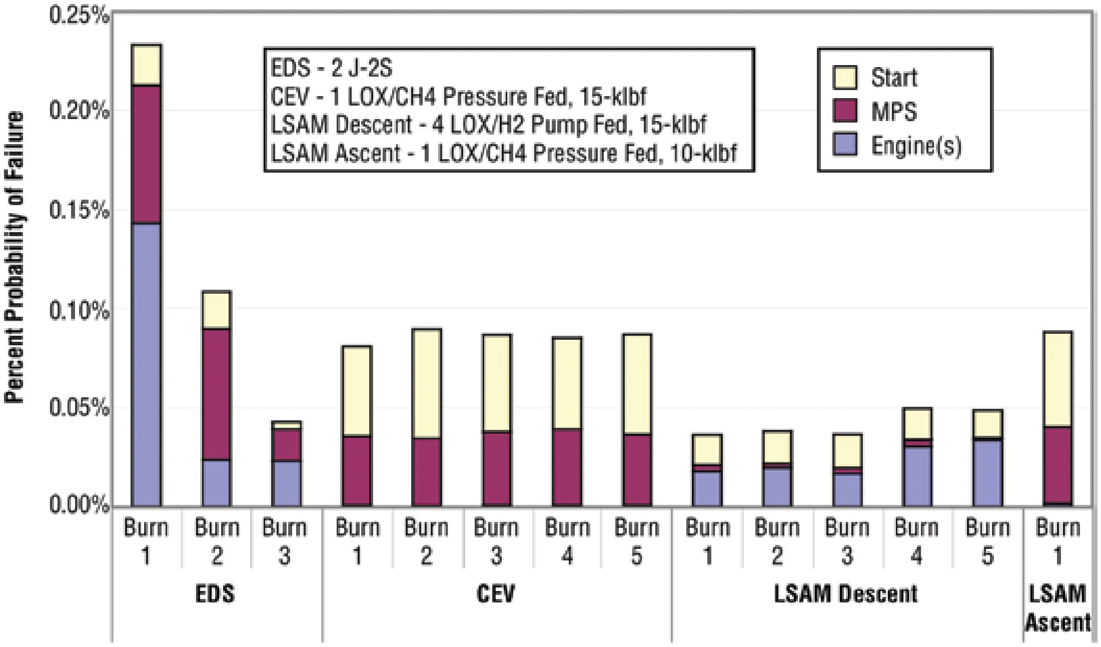


Figure 8-24. Propulsion Stage Reliability Results for the 1.5-Launch Configuration

The risk associated with first burn of the EDS is dominated by failure of the two engines operating without engine-out (61 percent). The remaining risk for the first burn of the EDS is associated with the MPS (30 percent) and engine-fail-to-start (9 percent). The second burn of the EDS is a short burn, with MPS comprising the bulk of the risk (61 percent). The third burn of the EDS incorporates an engine-out capability, with the dominant risk being the two engines (53 percent) and the MPS (37 percent).

The risk of the LOX/methane stages was dominated by failure to start (55 percent) and failure of the MPS propellant isolation valves to open and close (45 percent). Consideration was given to adding redundancy to the valves, but the additional complication in the system was seen to be adding additional failure modes that would offset the benefit.

The LSAM descent stage with engine-out was dominated by double start failures (30 to 45 percent) and catastrophic engine failures (45 to 70 percent) because engine-out effectively eliminates benign engine and MPS (isolation valve) failures from contributing to system failure. It was assumed that the gap between Lunar Orbit Insertion (LOI) and lunar descent burns would not affect engine reliability during descent. Some architectures employed two pressure-fed LOX/methane engine systems without engine-out capability. The start and MPS failures (no engine-out) caused this configuration to be approximately a factor of 3 less reliable than the LOX-fed system with engine-out.

Results indicate that pressure-fed configurations are significantly more reliable than pump-fed configurations with like number of engines and no engine-out capabilities. Results also indicate that detailed vehicle/mission/architecture design studies are needed to determine if the benefits of additional redundancy (engine-out, redundant valves, etc.) will have significant reliability benefit.

8.3.3 Mission Elements – CEV, SM, and LSAM Systems Probability Estimates

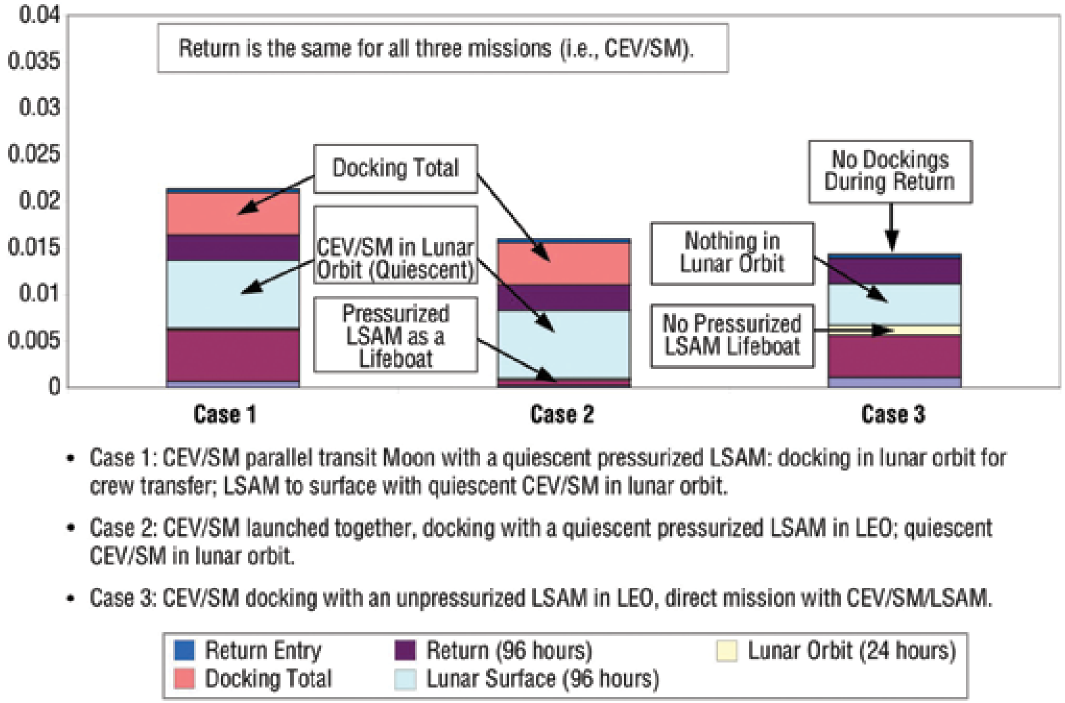
For this study, the subsystem descriptions supporting the failure rate estimates were obtained directly from members of the ESAS team, with a significant level of interaction and iteration. Failure rate estimates for these subsystems are derived whenever possible from other space subsystem applications; otherwise, surrogate data is used. Each estimate is a failure-per-hour unless the mission event is a demand; then the failure probability is listed as a demand (e.g., parachute deployment). No attempt is made in this assessment to develop exact failure rates for every system, nor is there an uncertainty applied to the numbers. Therefore, this data should not be assumed to be detailed subsystem failure rates. The intent is to apply an estimate for a top-level mission architecture comparison. Propulsion system dormant states are given failure rates for estimated dormant failures (e.g., leakage of propellant). Engineering judgment is employed to provide sanity checks for the probability values. LV and propulsion burn failure rates are estimated in **Section 8.4**, **Architecture Summary**.

For mission phases where the mission element is uncrewed, the element is assumed to be quiescent, or in a powered-down state, where some of the subsystems are removed from the list. The LSAM is considered quiescent for Case 1 outbound to lunar orbit until docking with the CEV/SM, and also in Case 2 outbound while docked with the CEV/SM. The CEV/SM is only quiescent in Cases 1 and 2 when it is unoccupied in lunar orbit. The estimate of nominal mission phases times are: 24 hours in LEO, 96 hours for lunar transit, 24 total hours for lunar orbit operations, 96 hours lunar surface mission, and 96 hours return-to-Earth—for an approximate 14-day mission. Data is selected from the list for the different mission phases depending on the subsystems that are assumed to be operational during those phases.

The CEV, SM, and LSAM elements reliabilities are aggregated for three basic mission cases:

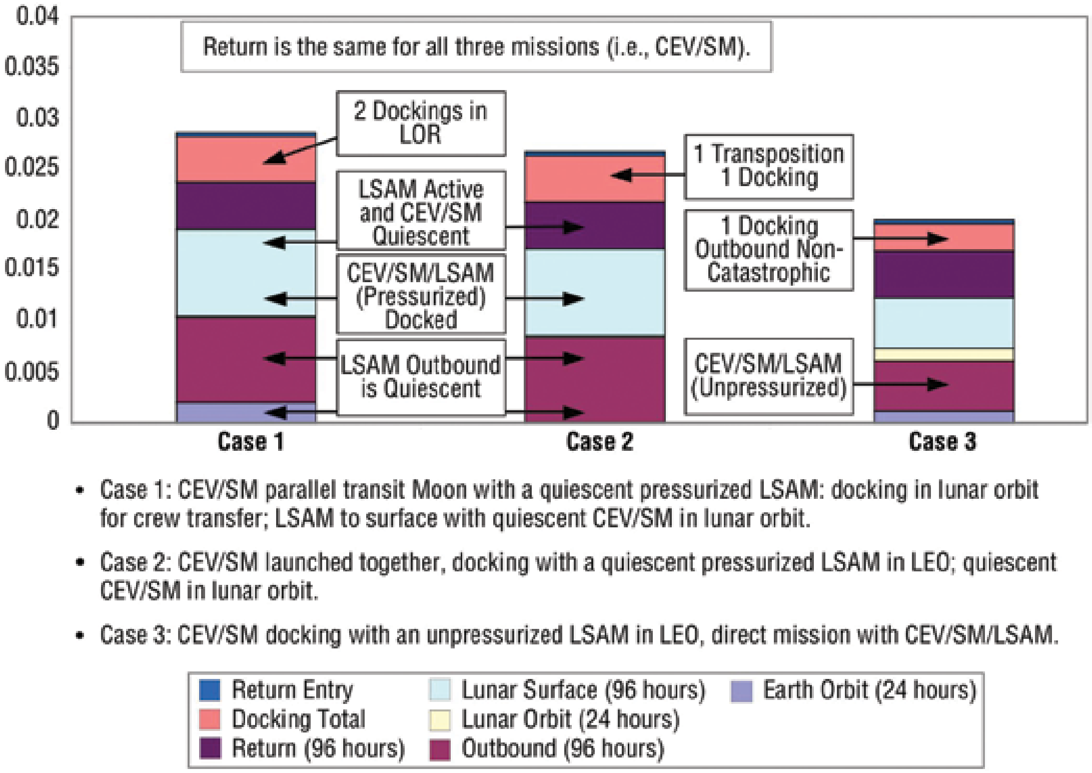
- Case 1: CEV/SM parallel transit Moon with a quiescent pressurized LSAM, docking in lunar orbit for crew transfer, and LSAM to surface with quiescent CEV/SM in lunar orbit.
- Case 2: CEV/SM launched together, docking with a quiescent pressurized LSAM in LEO, and quiescent CEV/SM in lunar orbit.
- Case 3: CEV/SM docking with an unpressurized LSAM in LEO and direct mission with CEV/SM/LSAM.

Figures 8-25 and **8-26** show the results for LOM and LOC. The LOM includes the LOC within its results. Cases 1 and 2 are virtually equivalent for LOM risk because a failure of a subsystem may simply preclude the completion of the mission. However, Case 2 has a much lower potential LOC risk since it has the LSAM as a “lifeboat” should a critical failure occur with the CEV/SM. Case 3 appears to have a better chance for mission success simply because of the fewer number of subsystems in the LSAM. For LOC, Cases 2 and 3 are roughly equivalent where the LSAM “lifeboat” capability of Case 2 equals the reduced number of subsystems and eliminated return docking of Case 3. Redundancy is taken into account by, in most cases, allowing for a two-fault tolerant system with the critical systems.



- Case 1: CEV/SM parallel transit Moon with a quiescent pressurized LSAM: docking in lunar orbit for crew transfer; LSAM to surface with quiescent CEV/SM in lunar orbit.
- Case 2: CEV/SM launched together, docking with a quiescent pressurized LSAM in LEO; quiescent CEV/SM in lunar orbit.
- Case 3: CEV/SM docking with an unpressurized LSAM in LEO, direct mission with CEV/SM/LSAM.

Figure 8-25. Catastrophic Failures Aggregation for CEV/SM and LSAM Mission Phases



- Case 1: CEV/SM parallel transit Moon with a quiescent pressurized LSAM: docking in lunar orbit for crew transfer; LSAM to surface with quiescent CEV/SM in lunar orbit.
- Case 2: CEV/SM launched together, docking with a quiescent pressurized LSAM in LEO; quiescent CEV/SM in lunar orbit.
- Case 3: CEV/SM docking with an unpressurized LSAM in LEO, direct mission with CEV/SM/LSAM.

Figure 8-26. LOM Failures Aggregation for CEV/SM and LSAM Mission Phases

8.3.4 Reliability Estimates for the Rendezvous and Docking of the CEV and Lunar Mission Architecture Elements

Historical accounts of rendezvous and docking by spacefaring nations provide an assessment of the reliability of conducting these sequences of events. However, the differences between the Russian Space Agency and NASA rendezvous-and-docking mission success requires a more in-depth review of the failures, precursors to failure, and rendezvous and docking technology. Both agencies have had a relatively large number of precursors to failure; however, U.S. missions have succeeded in applying contingency and malfunction procedures to achieve a 100-percent success rate. The conceptual lunar missions using the CEV will require rendezvous and docking maneuver events that are conducted in Earth or lunar orbit. Given the 2-launch solution and an LOR for the return mission, there are two types of rendezvous and docking maneuvers that will take place with differing contingency measures. These maneuvers are shown in **Figure 8-27**.

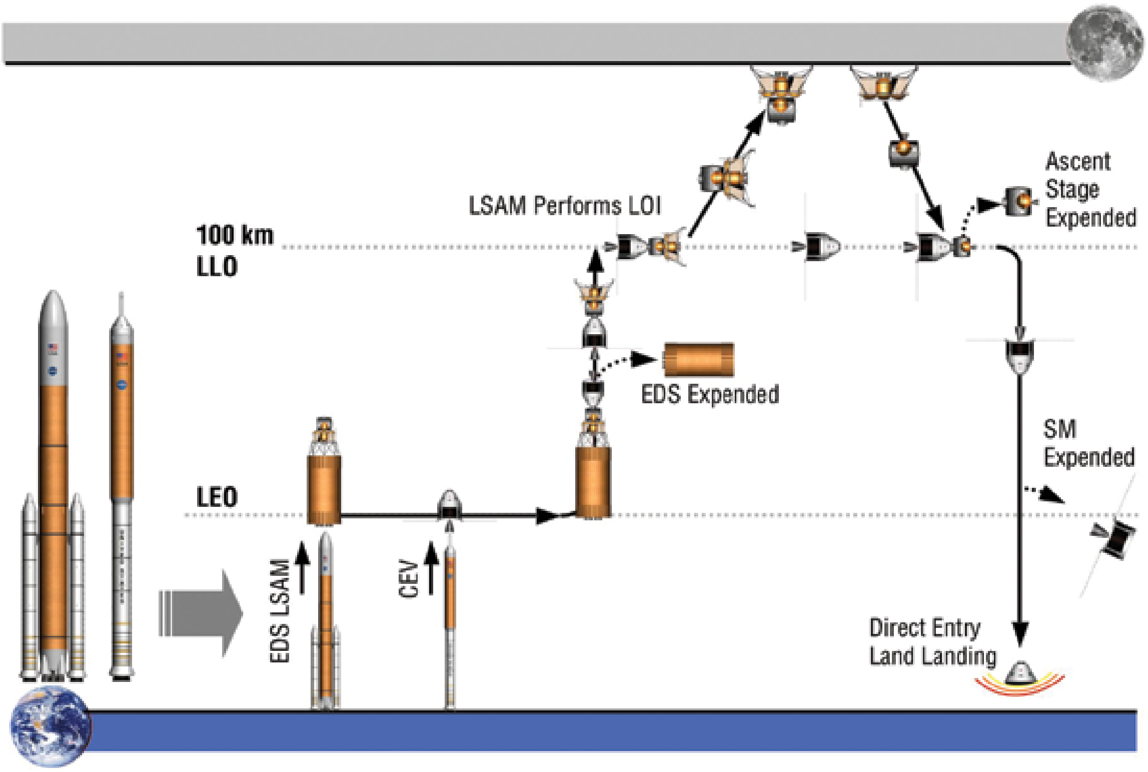
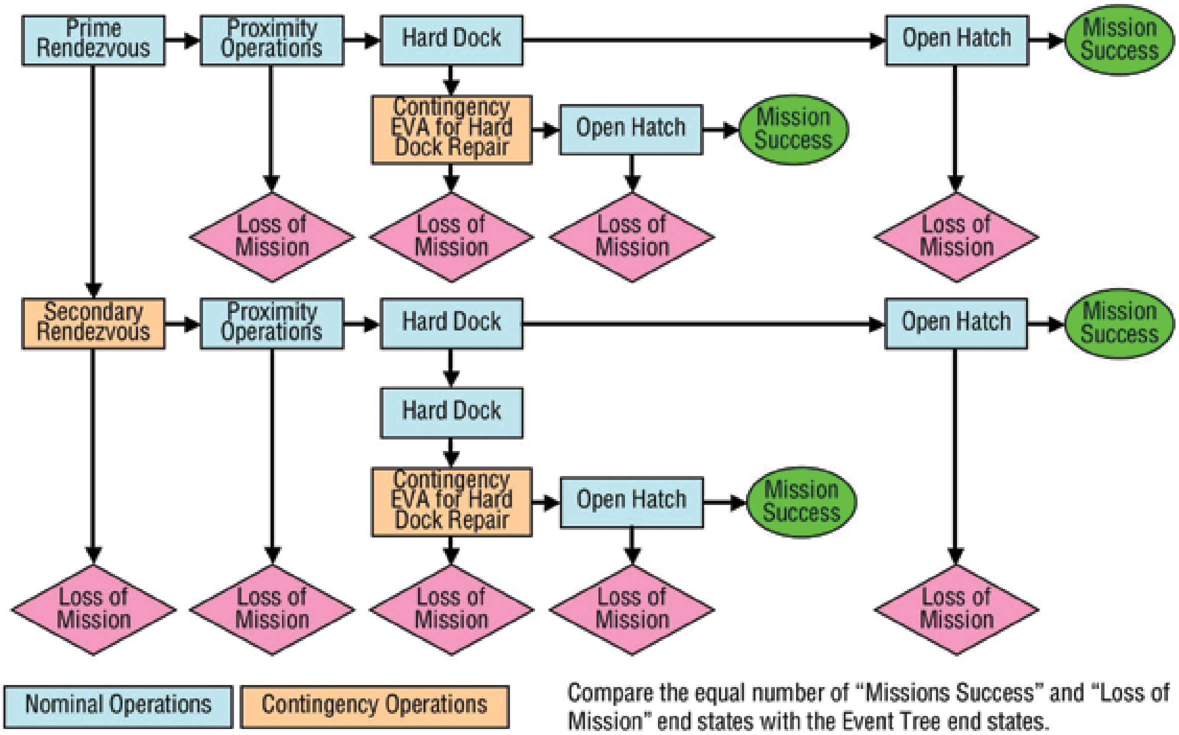


Figure 8-27. Lunar Mission Requiring Rendezvous and Docking Maneuvers

This analysis will assess the risk of failing to rendezvous and dock in Earth orbit and on the return mission. If a failure to dock occurs on the outbound leg of the mission, the mission may abort and return to Earth, depending on the perceived risk of continuing the mission. If an initial failure to dock occurs on the return leg, many more contingency procedures will likely be attempted to save the crew.

8.3.4.1 Rendezvous and Docking Mission Sequence

For this analysis, a mission sequence for a mission rendezvous and docking is developed in the form of a mission Event Sequence Diagram (ESD) and, in turn, converted to an event tree. Even though there are many detailed steps that must be accomplished prior to a hard docking, these steps can be broken down into any acceptable level of resolution. In this case, the steps are: (1) Rendezvous, (2) Proximity Operations, and (3) Docking. (An introduction to rendezvous and docking can be found in References 4 and 5 which are identified in **Section 8.7**, **References**. (See **Appendix 8E**, **Reliability Estimates for the Rendezvous and Docking of the CEV and Lunar Mission Architecture Element**.) In past missions, failed docking mechanisms or processes have been replaced by exceptional events, especially in the proximity operations and dockings. Rendezvous techniques are well established and are conducted by either an approach from below the target vehicle's orbit or from above. Primary systems used to conduct the rendezvous maneuver include the data processing system, electrical power distribution and control, digital autopilot, Star Tracker, Ku-band radar, translational and rotational hand controllers, cameras, Inertial Measurement Units (IMUs), general-purpose computer, and crew optical alignment sight. Each of these subsystems has some form of redundancy, which is referred to as the secondary rendezvous. These redundancies may be like or unlike. **Figure 8-28** shows an ESD of a typical rendezvous and docking maneuver with contingencies for failed events in the outbound leg of the lunar mission. In an ESD, arrows to the right are considered a success of the event and arrows downward are considered a failure. The ESD can be directly converted into an event tree.



Compare the equal number of "Missions Success" and "Loss of Mission" end states with the Event Tree end states.

Figure 8-28. ESD for a CEV Lunar Mission Outbound Rendezvous and Docking

In the event of an unstable target vehicle in the return mission (e.g., a CEV that is oscillating due to a malfunctioning thruster or some propulsive venting), requirements may be in place to dampen the oscillations remotely, or the crew could take action to arrest the CEV using EVA. This would likely not be easy since it would require a set of thrusters in the EVA backpack that may not be required for a nominal mission. Contingency EVA procedures will likely be in place for anomalous conditions during the return mission that may not be attempted during the outbound leg of the mission. Returning from the Moon could take this propensity to an extreme if numerous failures occur. The crew will try many more options to get back to the CEV even with a seemingly unattainable transfer. When these challenges are included in the return mission, many more options will be included in the flight rules, and the ESD will appear as in **Figure 8-29**. Most of the events in this ESD are for contingency EVA which is employed to stabilize or repair the docking mechanisms or open the hatch between the elements.

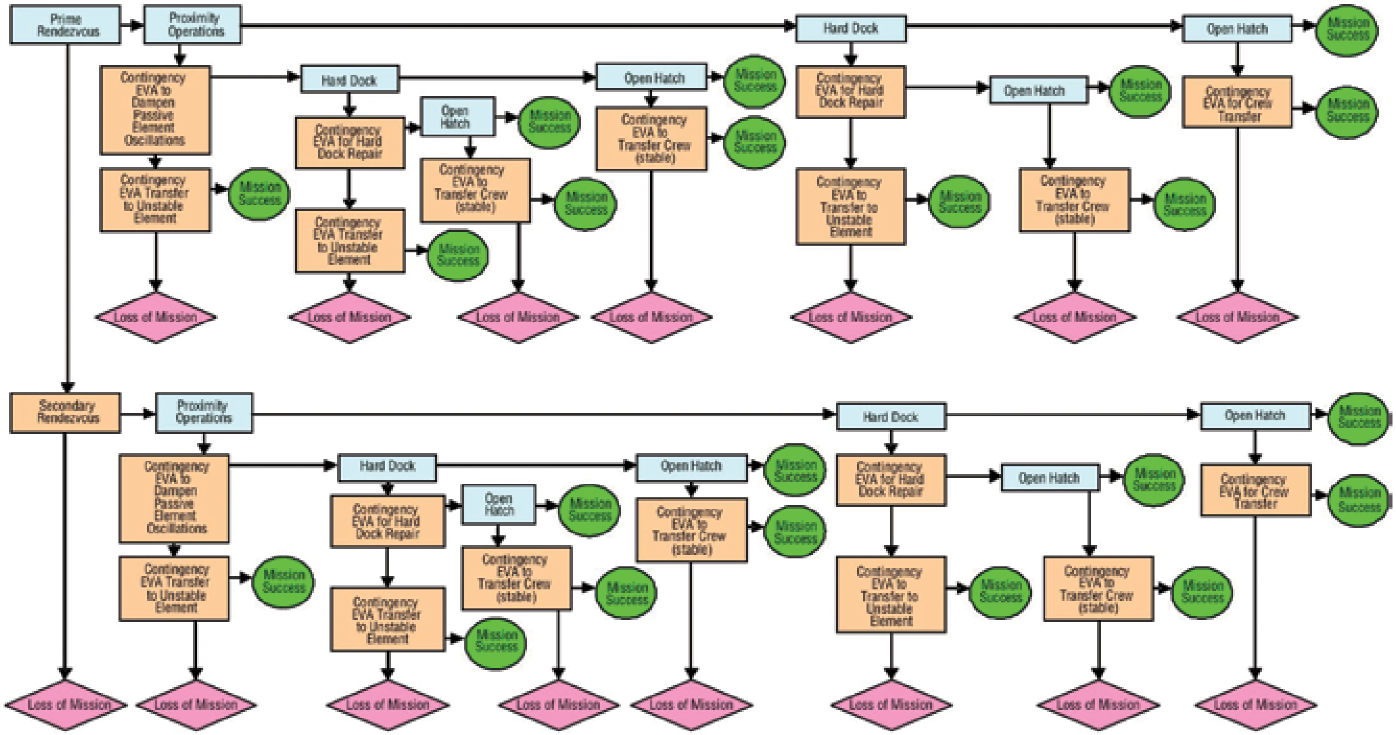

Prime Rendezvous
Proximity Operations
Hard Dock
Open Hatch
Mission Success
Contingency EVA to Dampen Passive Element Oscillations
Hard Dock
Open Hatch
Mission Success
Contingency EVA for Hard Dock Repair
Open Hatch
Mission Success
Contingency EVA for Crew Transfer
Mission Success
Contingency EVA for Hard Dock Repair
Open Hatch
Mission Success
Contingency EVA to Transfer Crew (stable)
Mission Success
Contingency EVA Transfer to Unstable Element
Mission Success
Contingency EVA to Transfer Crew (stable)
Mission Success
Contingency EVA to Transfer to Unstable Element
Mission Success
Contingency EVA to Transfer Crew (stable)
Mission Success
Contingency EVA Transfer to Unstable Element
Mission Success
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission
Secondary Rendezvous
Proximity Operations
Hard Dock
Open Hatch
Mission Success
Contingency EVA to Dampen Passive Element Oscillations
Hard Dock
Open Hatch
Mission Success
Contingency EVA for Hard Dock Repair
Open Hatch
Mission Success
Contingency EVA for Crew Transfer
Mission Success
Contingency EVA for Hard Dock Repair
Open Hatch
Mission Success
Contingency EVA to Transfer Crew (stable)
Mission Success
Contingency EVA Transfer to Unstable Element
Mission Success
Contingency EVA to Transfer Crew (stable)
Mission Success
Contingency EVA to Transfer to Unstable Element
Mission Success
Contingency EVA to Transfer Crew (stable)
Mission Success
Contingency EVA Transfer to Unstable Element
Mission Success
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission
Loss of Mission

Figure 8-29. ESD for a CEV Lunar Mission Return Rendezvous and Docking

8.3.4.2 Rendezvous

The prime rendezvous event is assumed to have the same technology as the current Space Shuttle, i.e., the Ku-band antenna used in the radar mode to track the target vehicle. Should a failure of the Ku-band occur, the rendezvous can be conducted using Star Trackers or with upload commands from Mission Control. The Shuttle rendezvous radar supplies range, range rate, and angular measurements. The radar system does contain single point failures. In the event of radar failure, two Star Trackers are available to conduct the rendezvous, and the crew is trained in these procedures. In this model, the Ku-band is assumed to be the primary rendezvous equipment, and the Star Trackers are assumed to be the secondary rendezvous equipment. Data exists for each of these components; however, the history of failure and the available failure rate is not that consistent. One Ku-band failure in the radar mode has occurred during STS–92, and one Star Tracker failed during STS–106. There have been other Ku-band antenna failures, but these failures would not have affected a rendezvous. A “resource-rich” spacecraft such as the Space Shuttle is equipped with redundant systems and more than adequate margin in thermal control, power storage and generation, propellant, on-board computer capacity, and communications bandwidth. These redundant systems and margin work together to enhance mission success and to lower mission risk in the presence of failures and off-nominal conditions. This approach has a lot to do with the success rate of NASA rendezvous and dockings. Therefore, the actual Ku-band and Star Tracker data for the prime and secondary rendezvous will be used in this assessment. With the existing failures over 113 missions, the values are 0.991 for the Ku-band antenna and 0.99992 for the redundant Star Trackers.

8.3.4.3 Proximity Operations

Since there are several unlike redundancies for proximity operations, the probability for failure will be accounted for with an "and" gate in the event tree of the Ku-band radar, crew optical alignment sight, Ku-band radar, hand-held lidar (i.e., Light Detection and Ranging), trajectory control sensors, ranging-rulers and overlays, and the laptop computers used to process data. The failure rates for these components are shown in **Table 8-6** (Reference 6 in **Section 8.7**, **References**). A Global Positioning System (GPS) may be included in this list of navigation instruments; however, current GPS technology is not accurate enough to use for proximity operations. The resulting probability of failure of all proximity operations navigation instruments calculated at 6.4^{-7} is quite low; however, there are very few common cause failures with these instruments. The next driving system risk will likely be the RCS.

Table 8-6. Proximity Operation Navigation Instruments

Proximity Operation Instruments	Failure Rate for 113 Shuttle Flights
Ku-band Radar	0.00885
Trajectory Control Sensor	0.0619
Hand-held Lidar	0.0442
Star Tracker	0.0265
Probability (product of all failure rates)	6.4^{-7}

Current vernier RCS failure rates for all Shuttle missions indicate a failure rate of 4.42 percent for an RCS jet off (i.e., a failure of the RCS jet to burn when commanded); however, there are several primary jets in each axis (Reference 6 in **Section 8.7**, **References**). The vernier jets are not redundant, but the primary jets have multiple redundancies that could be used to abort proximity operations. For example, in the case of a closing rate and range where a collision is imminent (possibly due to a crew failure), a failure of all RCS jets in the forward firing axis can be estimated. For the CEV, a required two-fault tolerant system and a non-hypergolic thruster system will reduce the probability of failure for the RCS because the Shuttle hypergolic system is susceptible to leakage from the oxidizer. Even with a 4.42-percent failure rate, the resulting probability of system failure is 3.8^{-6} with three additional levels of redundancy. So, the next candidate for failure of proximity operations is human error.

The process for rendezvous and docking is tightly controlled by mission control, but it can be assumed that the crew is performing the proximity operations on their own. There is no data for proximity operations for human error, so the Shuttle PRA estimate for the crew failure to fly the Heading Alignment Circle (HAC) is used as the surrogate data. The HAC procedure is performed just prior to landing, and the value is estimated at 4.6^{-5} by a flight crew representative from the Shuttle PRA. The result is a summation of the values above ($6.4^{-7} + 3.8^{-6} + 4.6^{-5} = 5.0^{-5}$), which is still quite low.

When rendezvous and docking are assessed, however, it should be apparent that two vehicles are involved, and that the target vehicle cannot always be assumed to be stable. In June 1997, a power failure aboard the Mir space station was reported in which the ship's computer disconnected from the control system overnight after some critical batteries ran low. A month later, the stabilizing gyroscopes that point the Mir toward the Sun shut down temporarily. Still later, the Mir lost power after a vital computer cable was accidentally disconnected, sending the Mir into free drift.

Leaky thrusters or uncontrolled venting can also send a vehicle into oscillations. In a case involving STS–72, a remote-manipulator-system-deployed satellite experienced unexpected propulsive venting that caused trajectory dispersions. On STS–52, there was a strong correlation between periods of increased RCS propellant consumption to maintain attitude and operation of the Flash Evaporator System (FES). Later analysis showed that FES impingement on the elevons produced a pitch moment. Gemini 8 was probably very close to disaster when a reaction control thruster was stuck open. Based on historical failures, the ESAS team estimated that a half a failure will occur for 200 rendezvous missions and that there is a probability of 1/400 for encountering an unstable target vehicle. When this is substituted into the other probabilities, the resulting value is 0.99745 for a proximity operations success.

8.3.4.4 Docking and Hard Docking

Several docking mechanisms have been used throughout spaceflight history, ranging from the simple to the very complex. Currently, the CEV is planning to employ a Low-Impact Docking System (LIDS). Of course, there is no direct docking failure history for this mechanism, so other docking systems must be assessed. All docking systems employ some type of mechanical latch and a motorized mechanism to pull the two vehicles together. Soyuz docking systems using probe and cone have an estimated failure rate of 3.27^{-3}, which is probably reasonable given the scattering of initial docking failures that have occurred from Gemini through Shuttle and from Soyuz through Progress, and including all of the initial failed capture and berthing events. The ESAS team estimated a probability of success of approximately 0.9967.

8.3.4.5 Contingency EVA

In a review of the previous Skylab mission where a contingency EVA was performed to resolve a serious docking problem and other contingency EVAs conducted for capturing satellites, it is obvious that U.S. space missions have gone to great lengths to ensure mission success, even when aborting the mission was certainly an option. There have been cases where planned EVAs were performed to capture a rotating satellite (e.g., Westar and Palapa II). For the CEV, this capability is not required; however, there will be contingencies for the return rendezvous since the only way to get back to Earth is with the CEV/SM. The only EVA where the Lunar Excursion Module (LEM) and Command Module were attached was Apollo IX, when the lunar rendezvous was tested in LEO. Both Command Module and LEM hatches were open, with crew members emerging from each hatch at the same time, but no transfer was made outside the spacecraft, even though it probably could have been done. Even with the possibilities so high, the estimate of a contingency EVA transfer probability of success to a docked vehicle is 50 percent and is 25 percent for a drifting vehicle. As discussed before, there may also be some failure modes of the docking hardware that can be repaired by EVA, as with Skylab.

8.3.4.6 Automated Docking

The only automated docking maneuvers of any statistical note are the Russian Progress vehicles, which began in 1978 with Progress 1 docking with Salyut 6 (though the first automated docking was with a Soyuz vehicle in 1975). The docking mechanism is the same probe and cone as on the Soyuz. Very little detailed history exists for the Progress vehicle in the early years of rendezvous and docking, and all of the failures listed in historical accounts have occurred since 1990. This is probably an artifact of the data collection process because more recent dockings have been covered by non-government news media representatives who have access to this information. The set of data indicates that, of 102 Progress rendezvous and dockings, there have been 93 successes, 8 significant anomalies (which include collision with space station equipment), and 1 failure (the infamous collision with the SPEKTR module on Mir). NASA has performed many automated or remotely controlled rendezvous but few, if any, automated dockings. The model was used with an assumed Ku-band antenna, but no Star Trackers, which effectively removes the secondary rendezvous option. When the model was implemented, the probability of success is similar to the Progress results, which are approximately 0.99.

8.3.4.7 Results of the Rendezvous and Docking Model

The inclusion of contingency events to ensure the success of rendezvous and docking is assumed because great lengths have been employed in past missions to achieve mission success. In many cases, ground support and simulations have also contributed to mission success. This support cannot be ignored, and, with enough resources, docking success should not be a major risk driver. **Figure 8-30** shows a comparison of probability of docking failure for lunar missions.

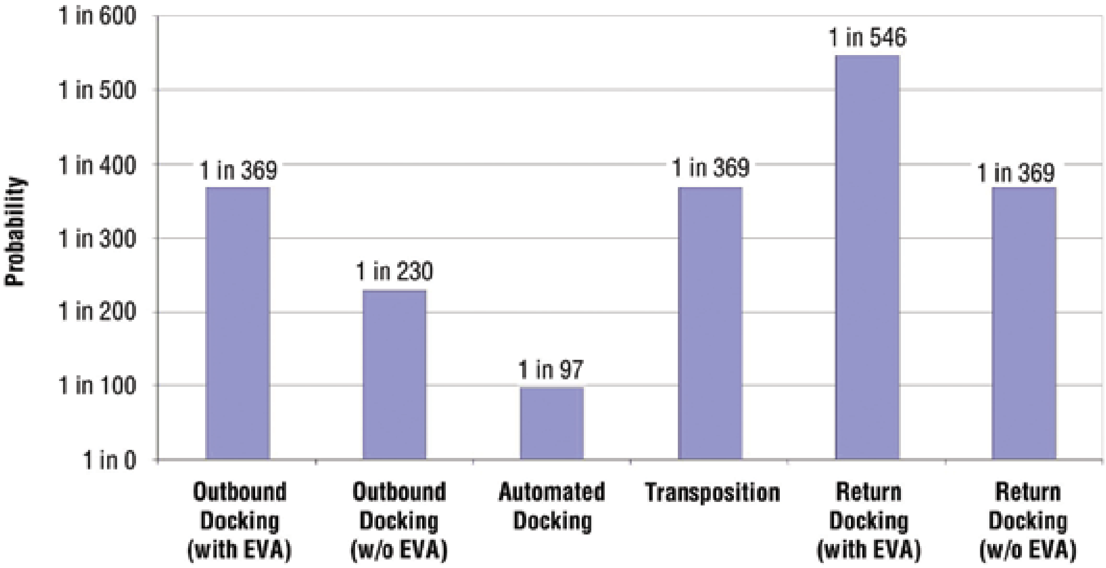


Figure 8-30. Docking Comparisons for Lunar Missions Probability of Docking Failure

8.3.5 Lunar Surface Stay Risk Change

The lunar surface stay time will affect the total mission risk in terms of how long the LSAM and the CEV/SM remain in standby for the return trip. The LSAM is launched prior to the CEV/SM and loiters until the CEV/SM arrives and docks. Given an initial checkout prior to TLI, the LSAM will likely be powered down to a quiescent or semi-dormant state. For a typical sortie mission, the pressurized LSAM will become active just prior to undocking from the CEV/SM which will, in turn, become quiescent as the crew leaves to burn to the surface. For expediency, the system probability of failure inputs were assumed as a λ failure rate, with the system probabilities as simply a summation of the probability of failure per hour for all systems involved in the mission. Because the probability values are relatively low, this approach gives an adequate approximation. Most of the system failures were less than 1^{-5} failures per hour or better. For this mission, the probability of LSAM vehicle failure was 4.86^{-5} per hour and the CEV/SM vehicle quiescent failure rate was 6.51^{-5} per hour. Multiplying the summation of these two by 24 gives the 2.73^{-3} per-day result. The catastrophic fraction is the percentage of system failures that would result in a failure of the crew to return to Earth. **Figure 8-31** presents the mission failure probabilities over an extended mission.

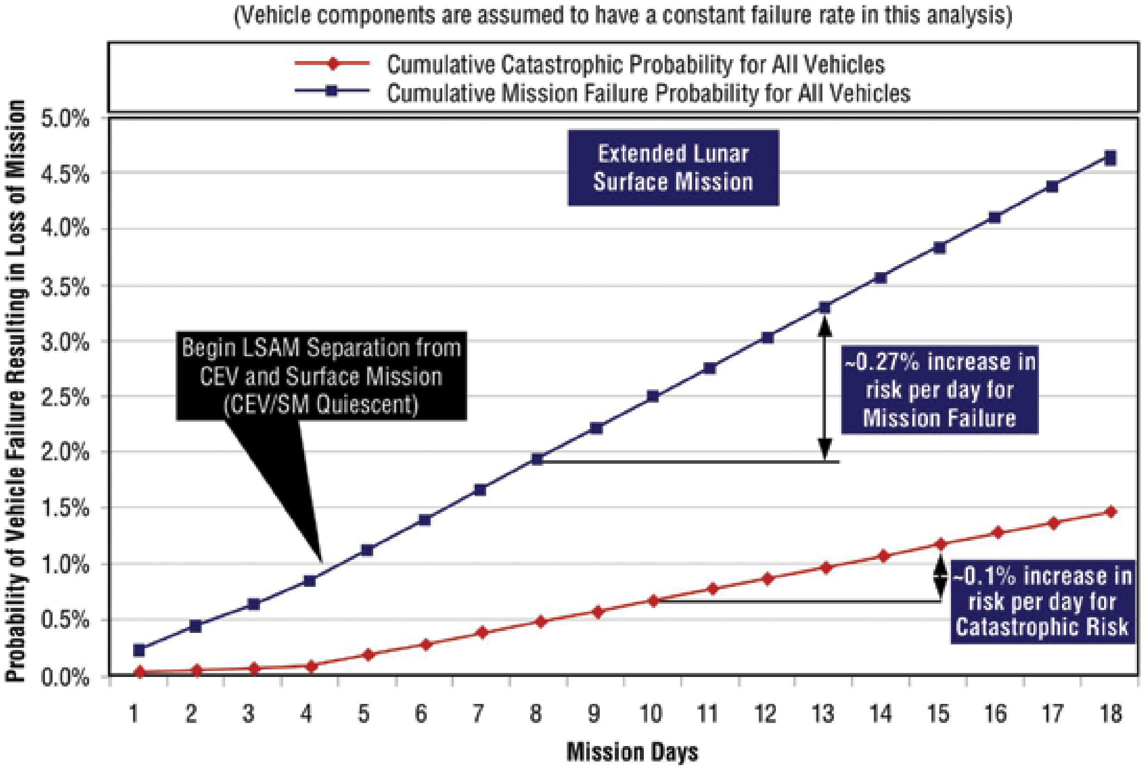


Figure 8-31. Mission Failure Probabilities Over an Extended Mission

8.3.6 CEV Stability Impacts on Crew Safety During Entry

One of the issues arising frequently for crew return is that of monostability of the CEV entry vehicle (Crew Module (CM)). In this context, a monostable CEV will only aerodynamically trim in one attitude, such that the vehicle would always be properly oriented for entry (similar to Soyuz). Requiring a CEV to be inherently monostable results in a CEV OML with weight and packaging issues. This study looked at how much benefit, from a risk standpoint, monostability provides so that the costs can be traded within the system design. In addition, this study looked at additional CEV systems that are required to realize the benefits of monostability and considered systems that could remove the need to be monostable. (See **Appendix 8F**, **CEV Stability Impacts on Crew Safety During Entry**.)

This study consists of two parts: a flight mechanics stability element and a risk assessment. The two pieces are combined to analyze the risk impact of CEV stability. The risk assessment was performed using the simple event tree shown in **Figure 8-32** representing the pivotal events during the entry mission phase. Each pivotal event was assigned a success probability determined from historical reliability data. In addition, mitigations to key pivotal events were modeled using the results from the stability study.

The success probabilities for the ballistic entry were determined from the aerodynamic stability study outlined below. In the event tree, the “Perform Ballistic Entry” event mitigates the “Perform Entry” (attitude and control) event, while the “Land and Recover from Ballistic Entry” event replaces the “Land and Recover” event should a ballistic entry occur.

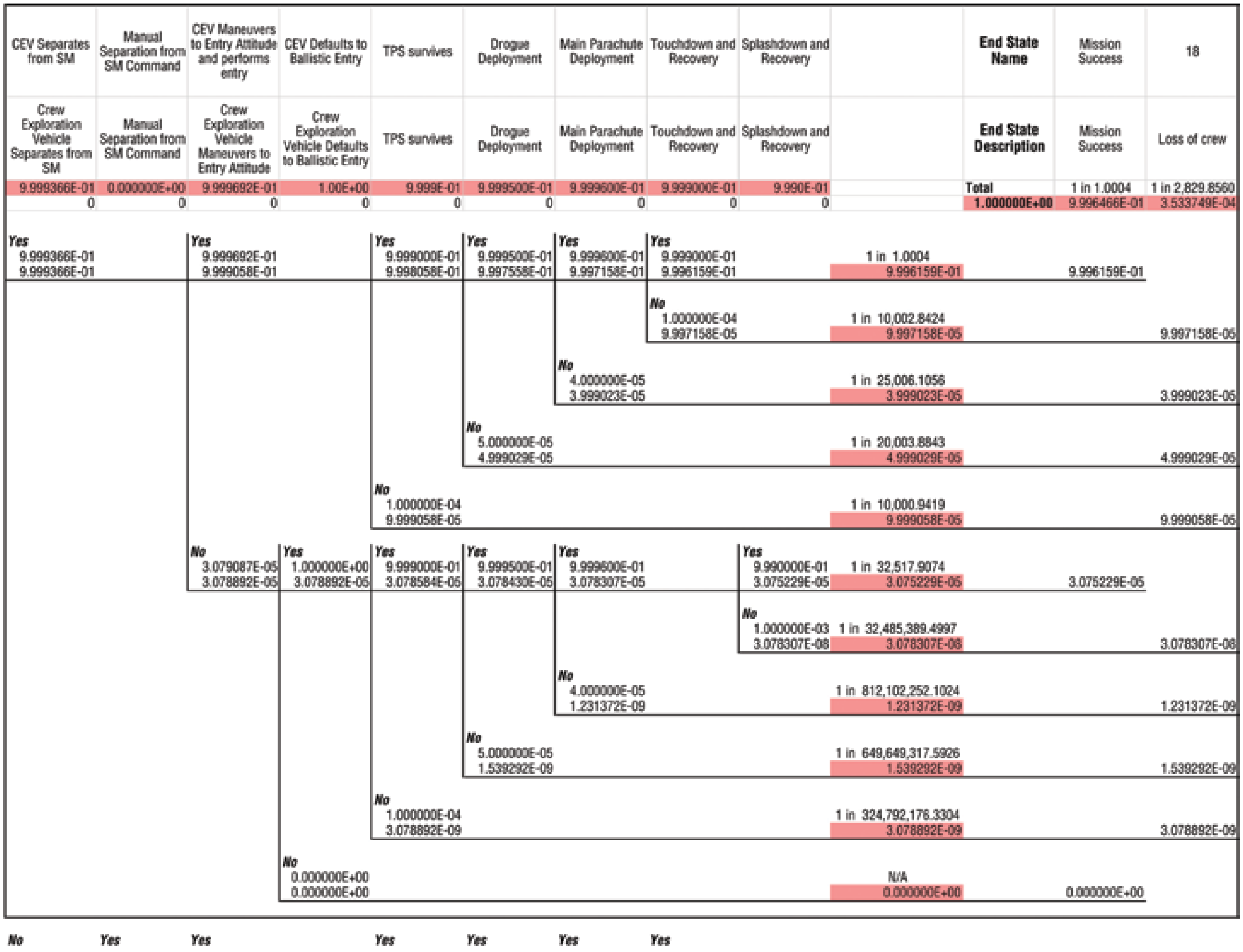


Figure 8-32. Entry, Descent, and Landing Event Tree

8.3.6.1 Results

The analysis process was used to generate range limits for load and heat rate violations for atmospheric entry from LEO/ISS. Initial attitudes from 180 to –180 deg were analyzed with no initial heat rate. In addition, initial pitch rates from –5 to 5 deg/sec were simulated at a constant initial attitude.

In addition to the initiating failures, there are additional actions that must occur to realize the risk benefit of strong stability. Most importantly, the CEV must roll to modulate the lift vector and establish a ballistic entry trajectory. If the lift vector is not rotated, a skip or excessive gravity dive can occur. This requires the use of RCS, which would be unavailable in the event of an RCS or total power loss, or an alternate means of roll initiation. To perform the roll initiation, a navigation aid must exist to indicate when to activate the roll or to initiate the roll automatically. These systems imply some form of active power source as well.

There are several options for systems to perform the above functions. The simplest system would include a solid, or cold jet, spin motor and a mark on the CEV window to orient the crew. If the only navigation aid was the visual window mark, the crew would have to visually determine the CEV attitude and activate the spin motor. This would require a conscious and coherent crew. The simplicity of this system could make it incredibly reliable, but the approach depends on monostability, or an alternate way to reach primary trim, to guarantee success.

An alternate approach would be based on four small, opposing cold jets near the apex of the CEV. These jets would also depend on a navigation aid such as the window mark or a backup gyroscope. The additional benefit of this system is that some pitch control would be available, reducing the need for monostability. This system could also be very reliable, but the operation itself is more complex. In addition, the weight of this system would be higher that the simplest system due to tanks, plumbing, controllers, etc.

A complete backup power system, RCS, and avionics system could be included, but the weight and packaging constraints would make this unattractive. This system would remove virtually all monostability requirements, because the vehicle could fly the nominal mission, as long as the system is completely independent to rule out any common cause failures.

All of these systems would mitigate the loss of primary power, avionics, and RCS. The specific system used will depend on the overall design trade results. If, for example, monostability drives the design to severely compromise the CEV, then a system that eliminates the need for monostability would add value. On the other hand, if the CEV is not largely hindered by the inclusion of monostability, the simplest system may be desirable.

For the risk analysis, the two simplest systems were assumed to have a reliability of 1.0; for the complete backup system, the reliability was assumed to be the same as for the original system, which was 0.99997.

8.3.6.2 Lunar Return

For the lunar return scenario, the same pivotal events were used in the event tree as in the LEO/ISS case. Events like separating the CEV from the SM, chute deployment, landing, and recovery are exactly the same in both cases; thus, the same reliability numbers were used. The Thermal Protection System (TPS) could be different, though the systems will likely be designed to the same margin. For this study, the TPS reliability number was held constant for the two missions. The RCS would endure more firings for the lunar case, so the failure rate was doubled to reflect a higher usage. The effective combination of these factors resulted in the same LOC probability of 1 in 2,780 for the lunar return entry.

The initial study results showed that the relative effect of CEV stability did not provide any measurable benefit for lunar cases. Further examination of the results showed that a large number of entry conditions resulted in skips due to the analysis approach. In this case, the initial attitude drives the results for the most stable cases, so there is little difference in the initial rate ranges. For the bistable case, the initial attitude and pitch rate limits are limiting, and a greater difference is seen. In addition, there are possible trajectories, with a short initial skip phase, which could be survivable if the CEV was tumbling. Predicting how likely this would be requires simulation of the vehicle heating as it enters the atmosphere. These computations would be sensitive to the specifics of the CEV OML, as well as the TPS distribution. For the current study, it was assumed none of the cases were survivable, but it is worth further investigation when more design definition exists. The actions required to perform ballistic entries in the event of primary system failures are the same as discussed above. The implications on the CEV design remain the same and will not be repeated here.

8.3.6.3 High-altitude Abort

High-altitude abort occurs after the ejection of the escape tower during the ascent phase. For a large portion of this mission phase, gravity and heat rate limits do not apply because the vehicle's speed is below the critical values. For a representative Shuttle-derived mission (500 sec in length), the escape tower would be ejected at approximately 150–200 sec of Mission Elapsed Time (MET). Entry gravity limits become important for mission aborts around 400–450 sec MET, and heat rate is an issue around 450–500 sec MET.

As with the previous cases, the absolute abort effectiveness, estimated at 89 percent using the event tree and numbers from **Appendix 8F**, **CEV Stability Impacts on Crew Safety During Entry**, does not change with the degree of stability. An LOC probability can be computed by assuming an upper stage failure probability of 1 in 625 (Reference 1 in **Section 8.7**, **References**). An 89-percent abort system leads to an LOC risk of 1 in 5,680 for this phase. These absolute figures are included for context only and need to be revisited once the design details are established.

8.3.6.4 Low-altitude Abort

The low-altitude abort regime is fundamentally different from the modes discussed so far. The aero forces are largely coupled and damping derivatives are important. For this reason, the simulation approach used in this study does not apply. In addition, a low-altitude abort would likely depend on an escape tower to perform the abort. The escape tower would shift the Center of Gravity (CG) and change the aerodynamic characteristics of the CEV and tower. The tower could be used as a stabilizing device, as used on Apollo, or could be ejected after the escape so strong stability could add some benefit. Unlike the previous cases, gravity load and heat rate limits are not of concern to a low-altitude abort. The primary concern with a tumbling, or improperly trimmed, CEV stems from the need to deploy the drogue chute. The explosive charge should have no problem propelling the drogue into the freestream, but some minor risk would occur from the possibility of the drogue lines wrapping around the CEV and interfering with the use of the primary chutes. It is suggested that the drogue would deploy in nearly every condition that would cause the CEV to attain its desired attitude.

8.3.6.5 Monostablility Summary

The benefit of stability manifests in two ways: monostability and strength of the attractor. Monostability relates to the lack of the possibility of an off-design trim, while the strength of the attractor (stability) determines the likelihood of trimming to the possible states within the required time.

In this study, stability effects were studied for lunar and LEO/ISS entries as well as high-altitude aborts. The extension to low-altitude aborts was mentioned but not quantitatively evaluated.

For LEO/ISS and lunar returns, the absolute benefit of strong monostability is negligible in terms of the LOC estimates. However, if the CEV does enter into a situation where an off-nominal entry is required, a strong primary trim attractor can result in aerodynamic positioning of the CEV in a safe-entry attitude between 6 and 80 percent of the time, depending on the strength of the attractor and the initial conditions. The expected benefit is in the range of 30 to 50 percent. Analysis approach refinements midway through the study suggest that LEO/ISS benefits may be larger than the current results suggest, and should be requantified if the success rate becomes a safety driver.

High-altitude aborts are energetically similar to LEO/ISS entries but originate from a different initial situation. Only initial attitude was investigated as a driving parameter for high-altitude aborts due to limited study time. It is expected that the benefit of strong monostability will be similar to the LEO/ISS results, but the range of potential initial pitch rates could be much higher.

Realization of strong stability benefits requires additional actions, e.g., putting the CEV into a roll to nullify the net lift of the capsule for a ballistic entry. Three approaches were discussed to accomplish ballistic entries, and the choice for a specific application depends on the overall vehicle trade space.

8.4 Architecture Summary

The risk analysis was performed in a number of iterations in concert with the design cycles of the study. Initially, placeholder values based on expert opinion were used. These values were updated as more information about the design was quantified, and detailed models were produced. The level of detail of the models was chosen based on the determination of the degree each would affect the architecture's overall risk. This concept focused on identifying "differences that make a difference." Lunar mission modes and ISS mission modes were analyzed in this study.

8.4.1 Lunar Missions

The initial study considered three mission modes: LOR, EOR, and EOR (direct). Each of these mission modes was evaluated with alternative levels of technology that enabled the missions to be launched on fewer or smaller launchers. The study had a set of ground rules which eliminated missions that required more than four launches due to the inherent unreliability of these concepts. Mission modes requiring three launches were eventually eliminated from consideration due to their cost and reliability issues (i.e., multiple launches, AR&D). Cost and mission reliability considerations tended to correlate with one another because simpler, mature systems have higher reliability and lower cost.

The mission modes are shown in **Figure 8-33**. The initial reference mission was LOR. In this mission mode, the crew and LSAM travel separately to lunar orbit where they dock. At this point, the mission becomes like Apollo, except the CEV is uncrewed. The LSAM is activated and descends to the lunar surface. At the end of the lunar stay, the LSAM ascends and docks with the CEV/SM which then returns to Earth. Risk drivers for this mission are:

- Two EDSs;
- Crew must be launched on a complex heavy vehicle; and
- The separation of the LSAM from the CEV eliminates the opportunity for the LSAM to serve as a safe haven during the trip to the Moon (as was done with Apollo 13). The CEV/SM is required to make additional burns in lunar orbit to rendezvous and dock with the LSAM. If the engine fails during these burns, the crew will be stranded in lunar orbit.

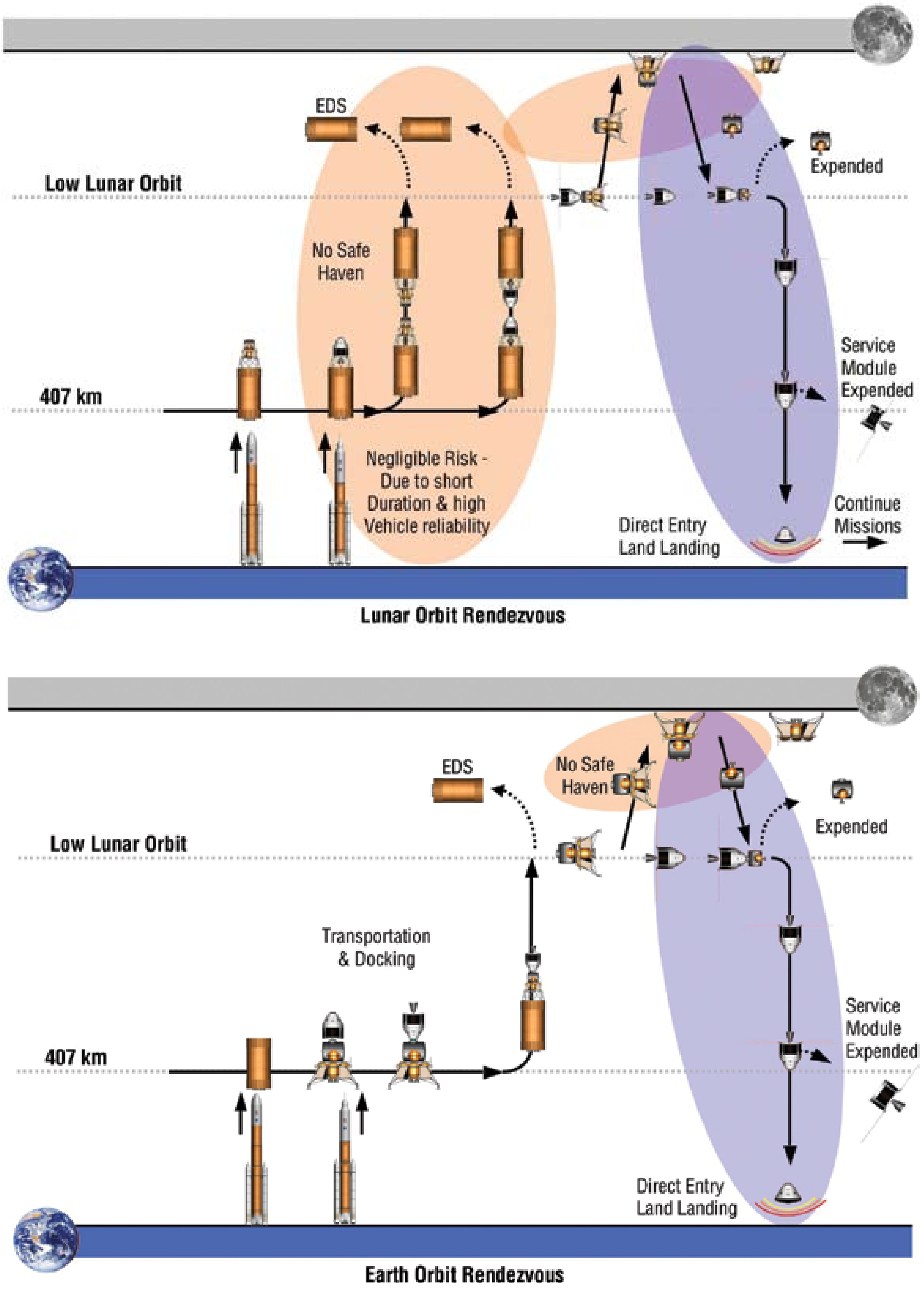


Figure 8-33. Lunar Mission Modes

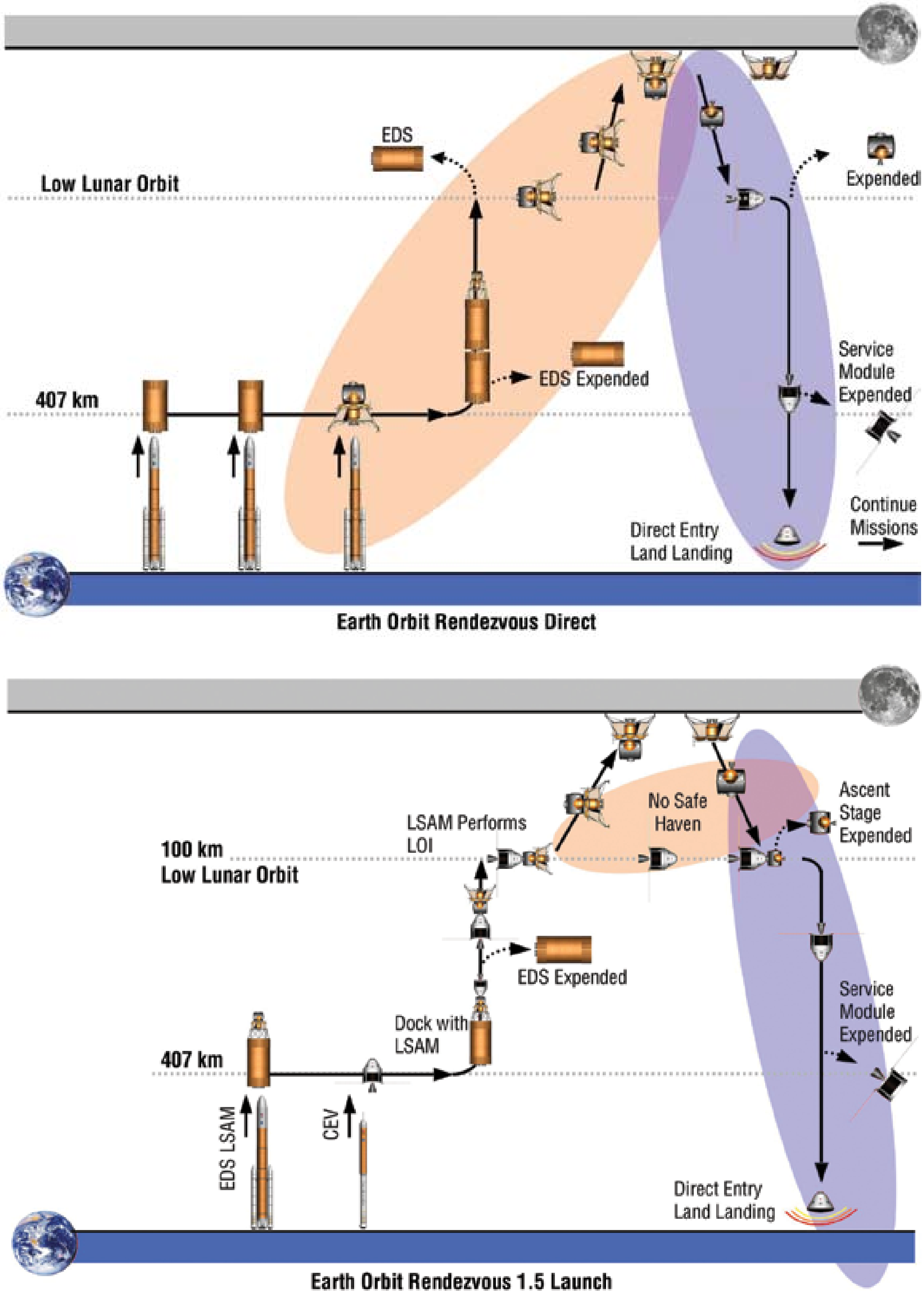


Figure 8-33. Lunar Mission Modes (continued)

The EOR mission is similar to the LOR mission except that the vehicle is assembled in LEO and a single EDS burn is required. Once in lunar orbit, the EOR mission is the same as LOR after docking. The EOR mission has several safety benefits over the LOR mission, including:

- LSAM is a potential safe haven during outbound legs;
- CEV/SM burns for rendezvous occur in LEO; and
- Reduced launch requirements, including:
  - Possibility for using the ISS CLV, thereby reducing the launch risk to the crew and eliminating a docking maneuver, and
  - Launching the mission on a single vehicle eliminates a docking maneuver, but increases risk to the crew due to the larger vehicle.

The EOR direct mission is the simplest in terms of mission events. The mission is assembled in LEO, proceeds directly to the Moon, and lands. It returns directly from the lunar surface, eliminating the need for docking on the return. However, this mission requires a third launcher and an AR&D, or higher performance of the propulsion on the in-space vehicles to achieve two launches. Risk drivers for this mission are:

- A single volume for the crew;
- A third launch with AR&D for low-performance vehicles; and
- Larger LVs and EDSs.

The additional risk from these aspects more than offsets the benefit of eliminating the need to rendezvous and dock with the SM on the return from the lunar surface, resulting in higher overall risk.

The mission mode preferred by this study was the EOR mission with the crew and CEV/SM being launched on the ISS CLV, and the LSAM and EDSs being launched on a heavy launcher (the 1.5-launch EOR mission). Risk impacts of this mode are:

- The ISS CLV is the safest, most reliable launcher with considerable experience in servicing the ISS; and
- Elimination of a transposition and docking maneuver for assembling the stack when the LSAM is launched with the CEV.

The risk analysis of each mission was developed from the individual events occurring in each type of mission. The direct mission modes were eliminated. The final analysis considered nine mission alternatives for the LOR and EOR mission modes. These alternatives explored the risks and benefits of increasing performance of the in-space propulsion stages, which is the key mission driver. Increasing performance of the in-space elements allows the same mission to be mounted with less mass delivered to orbit, thereby simplifying the mission.

The risk analysis also considered radiation risk and Micrometeoroid/Orbital Debris (MMOD) risk. These risks are moderated by the relatively short time the vehicle is exposed during ISS and lunar missions, and by the fact that the CEV has significant inherent shielding for these events. An analysis of the CEV radiation shielding requirements is contained in **Section 4, Lunar Architecture**. The shielding requirements for the CEV will cause these hazards to be controlled to a level where they will not affect overall risk. Spacecraft in LEO are threatened by the impact of either meteoroids or MMOD. The probability of being struck by MMOD is dependent on the geometry of the vehicle. The results of the assessment of the probability of being struck by an MMOD and this causing Loss of Vehicle (LOV) are shown below in **Table 8-7**.

	MMOD Probability of No LOV Damage	MMOD Risk	Odds of MMOD Impact exceeding LOV failure criteria
Twelve 6-month missions (6 years from 2011 through 2016)	0.980	2.0%	1 in 50
Requirement for 12 missions	≥ 0.992	≤ 0.8%	Better than (≤) 1 in 120

Table 8-7. Cumulative MMOD Risk for Multiple Missions to the ISS

The risk analysis analyzed the missions for LOM and LOC. The results of this analysis are shown in **Figures 8-34** and **8-35**, respectively. The EOR mission with 1.5 launches and pressure-fed engines on the CEV SM and lunar ascent stage have the lowest mission and crew risk.

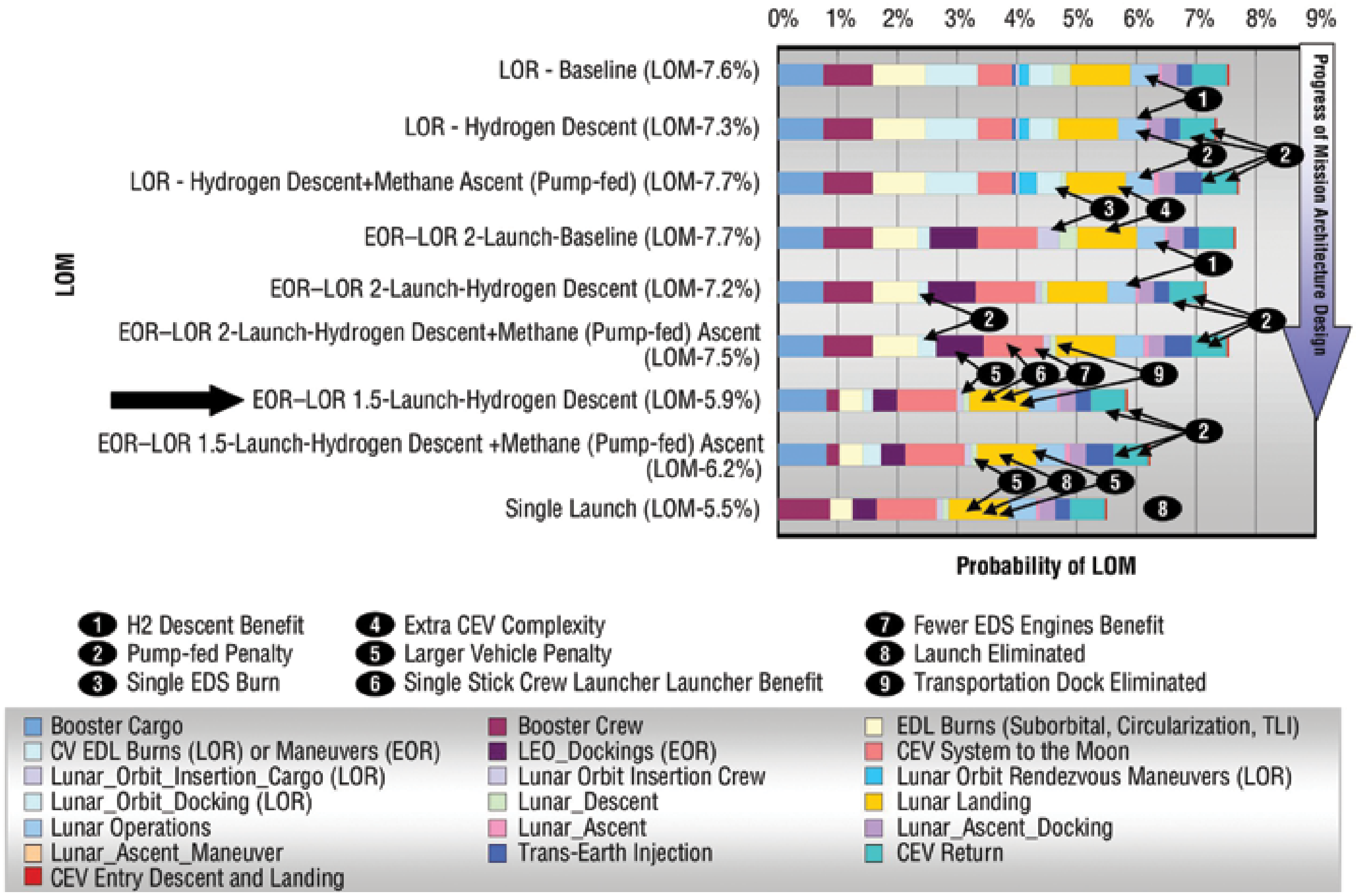


Figure 8-34. Comparison of LOM Risk for LOR and EOR Mission Alternatives

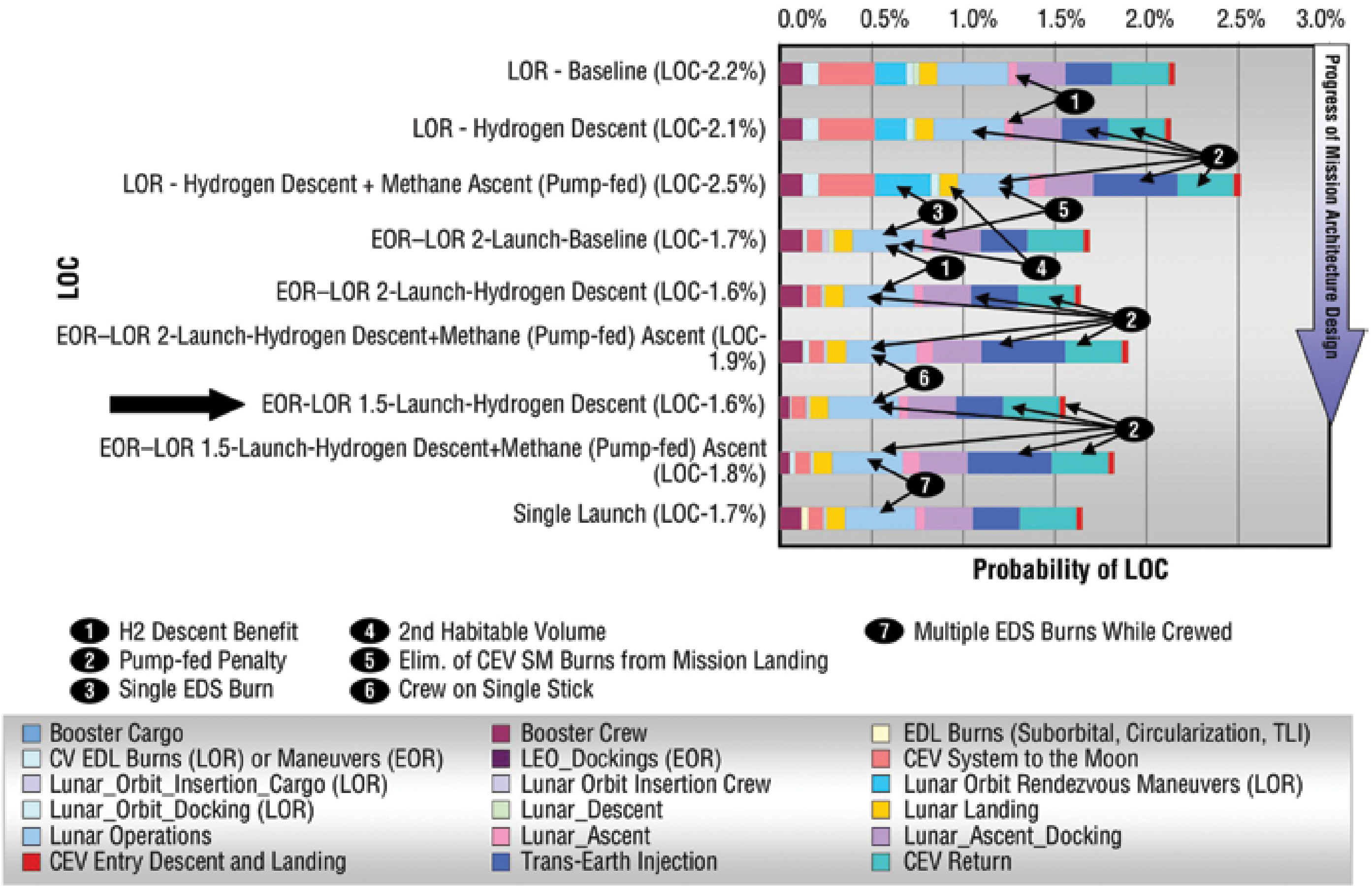


Figure 8-35. Comparison of LOC Risk for LOR and EOR Mission Alternatives

Annotations in the figures identify places where the risks vary. The application of the LOX/hydrogen engine (1) with engine-out capability on the LSAM descent stage is more reliable than two non-redundant pressure-fed LOX/methane engine systems. Replacing the pressure-fed LOX/methane engine on the SM and LSAM (2) increases risk because pump-fed engines are inherently less reliable than pressure-fed engines. Engine-out capability for these stages, however, presented a packaging problem that could not be solved. Changing the mission mode from LOR to EOR (3) eliminates an EDS burn, thereby increasing reliability. Combining the LSAM with the CEV (4) increases complexity, causing LOM risk to increase, but the extra habitable volume reduces LOC. This mode also eliminates the CEV/SM burns in lunar orbit for rendezvous and docking, shown in **Figure 8-35**. If the engine fails during this maneuver, the CEV will be marooned in lunar orbit. Combining the LSAM with the EDS and launching the crew on the single SRB requires slightly larger stages (5), with corresponding increase in risk for the larger vehicle. This risk is offset by replacing one launcher with the higher-reliability single-stick SRB (6). The 1.5-launch solution also employed an EDS with two J–2S engines rather than four LR–70 engines (7), further reducing risk. The 1.5-launch solution also elimiates a transportation and docking maneuver in LEO (4). Combining all the vehicles into a single launch reduced LOM risk by eliminating the single-stick CLV (8), but increased LOC risk by putting the crew on a larger, more complex vehicle (5).

Table 8-8 highlights the risk contributors for the preferred EOR mission with 1.5 launches (pump-fed LSAM descent hydrogen engines with engine-out, pressure-fed LSAM methane ascent and CEV SM engines). The yellow mission elements are the key drivers for LOM. The events in red indicate where the mission does not have a diverse abort mode on the lunar surface and on the return.

Table 8-8. EOR 1.5-Launch Mission with Pressure-fed SM and LSAM Ascent Engines

Phase	Mission Element	EOR–LOR 1.5-launch—Hydrogen Descent and Methane (pump fed) Ascent		
		LOM	Fatal	LOC
Launch	Booster _Cargo	124	–	–
	Booster_Crew	460	4	2,021
LEO Ops	EDS_Cargo	252	145	36,506
	EDS_Crew	332	10	3,319
	LEO_Dock_Man or ARD	250	–	–
Transit	CEV_System_to Moon	100	13	1,250
Lunar Orbit	Lunar_Capture_Cargo	–	–	–
	Lunar_Capture_Crew	905	10	9,046
	Lunar_Orbit_Maneuvers	–	–	–
	Lunar_Orbit_Docking	–	–	–
Lunar Descent	Lunar_Descent	1,018	10	10,178
	Lunar_Landing*	100	10	1,000
Lunar_OPS**	Lunar_OPS**	213	1	259
Lunar Departure	Lunar_Ascent	1,089	1	1,089
	Lunar_Ascent_Docking	381	1	381
	Lunar_Ascent_Manauver	–	–	–
	Lunar_Departure	218	1	218
Return	CEV_Return	172	2	325
EDLS	EDLS	2,830	1	2,830
		16		**55**
Probability of Failure		6.2%		1.8%
Reliability		**94%**		**98%**

* *Indicates use of placeholder values as conservative reliability estimates.*
** *Does not include EVA risk.*

Figure 8-36 shows the breakout of LOM contributors. The risk contributors for this mission are relatively evenly distributed. The most significant LOM risks for this mission are the launch of the HLV, the CEV systems on the way to and from the Moon, and the lunar landing. The next highest risks include the docking maneuvers in Earth and lunar orbit.

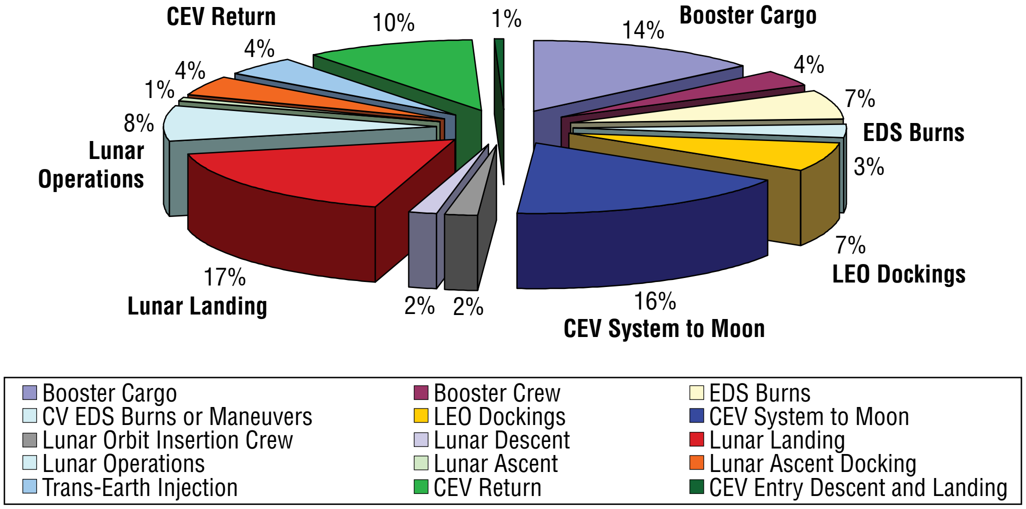


Figure 8-36. LOM Contributors for EOR 1.5-Launch Mission

The LOC risk breakout is shown in **Figure 8-37**. LOC is dominated by mission elements occurring after lunar landing where there are no diverse backups. These elements are the operations on the lunar surface; the ascent docking lunar departure return cruise; and entry, descent, and landing. Typically, the crew launcher would be a contributor, but the high reliability of the single-stick CLV significantly reduces this risk.

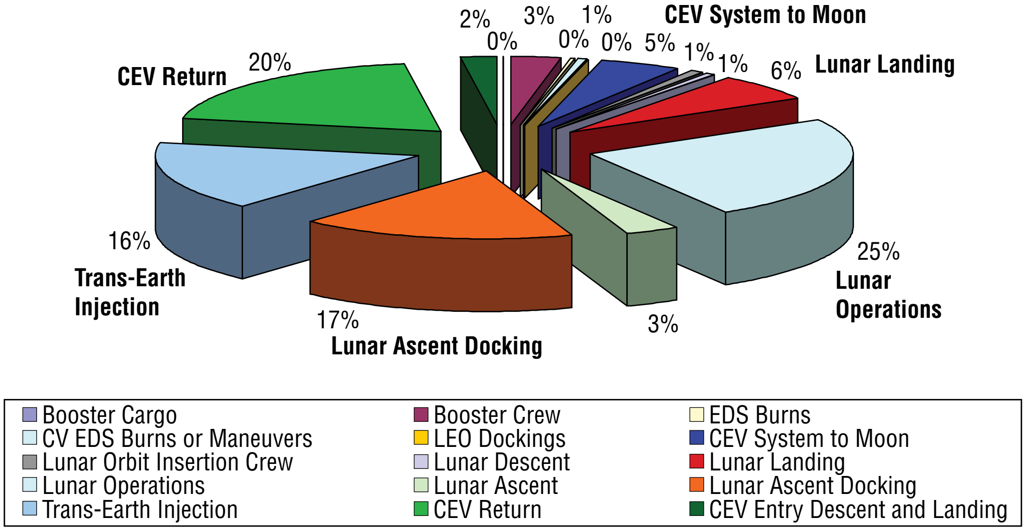


Figure 8-37. LOC Risk Contributors

Spaceflight will remain risky for the foreseeable future. The results of this analysis show that a lunar mission can be developed with acceptable, but not negligible, risk to the crew. The key factor causing the risks to be as low as they are is the application of existing technology for most mission elements and the extensive flight experience gained by operating critical CEV/SM in support of the ISS. Early failures of the CEV/SM system will occur in LEO, with simple abort options, rather than in lunar orbit with no possibility of return. This process helps mitigate the most significant source of risk to space systems, which is often referred to as unknown "unknowns."

8.4.2 ISS Missions

Missions for servicing the ISS are to be performed by derivatives of the CLV and CEV/SM system. For crewed missions to ISS, the CEV/SM is identical to the lunar mission. Pressurized cargo missions will require an automated docking capability similar to Progress. A simple mission model was developed from the CLV and the SM propulsion stage, combined with manual docking maneuver, and EDLS. The LOM and LOC results for the mature vehicle after 19 launches are shown in **Figures 8-38**, **8-39**, and **8-40**. Initially, the CEV/SM, and CLV will have higher failure rates due to the immaturity of the SSME air start (matures over 5 missions) and the LOX/methane engine of the SM (matures over 19 missions).

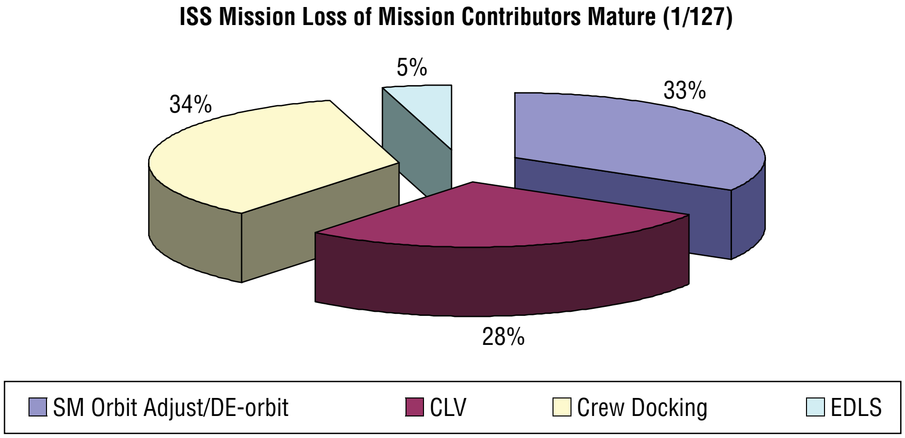


Figure 8-38. LOM Contribution for Mature Vehicle Crewed Missions

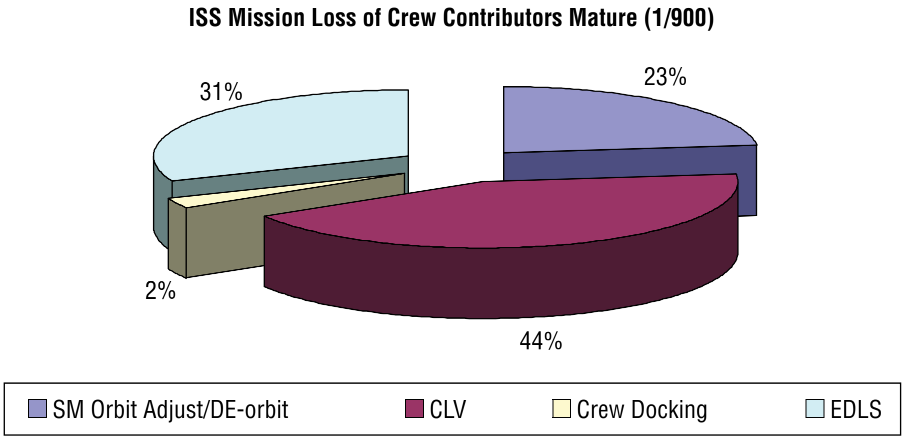


Figure 8-39. LOC Contribution for Mature Vehicle

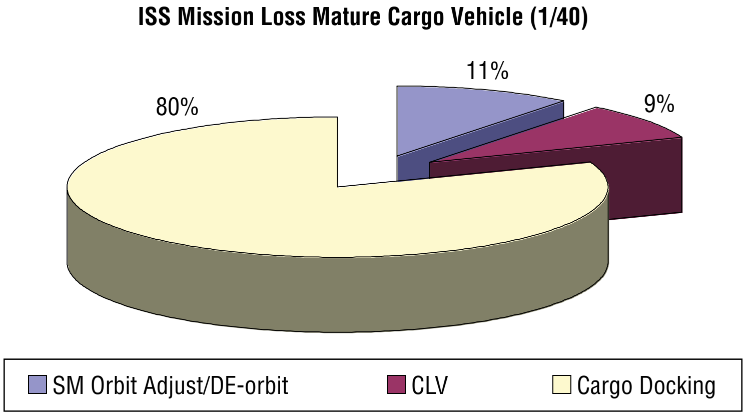


Figure 8-40. LOM Contributors for Cargo Vehicle

The cargo missions include automated docking maneuvers similar to the Progress, the Automated Transfer Vehicle (ATV), and the H–11 Transfer Vehicle (HTV). The LOM contribution for the mature cargo vehicles is shown in **Figure 8-38**.

The ISS mission model included in the architecture study includes the effect of maturity based on the actual traffic for the particular architecture. This effect is shown in **Section 8.5, Cumulative Campaign Summary**. LOM risk for the cargo vehicle is dominated by failure of the automated docking process.

8.5 Cumulative Campaign Summary

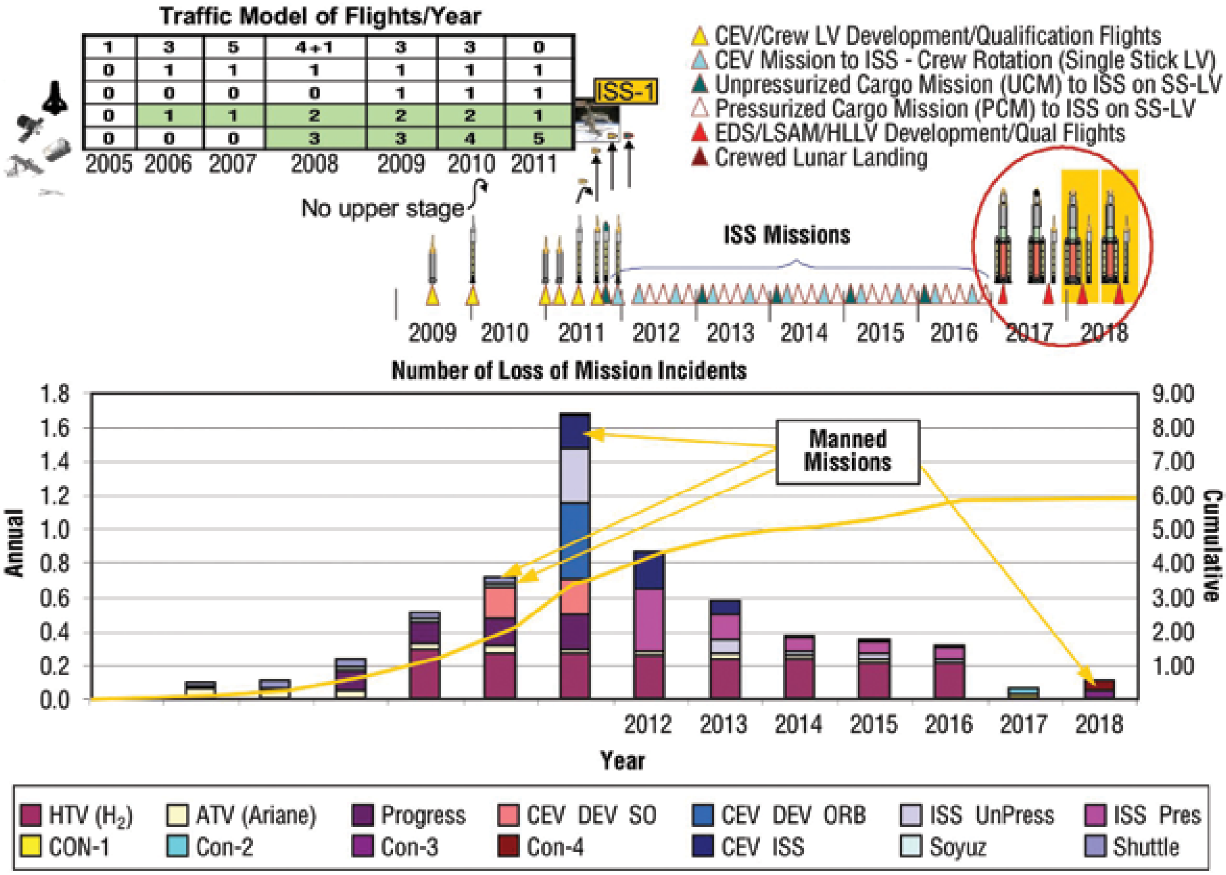
The risks of the lunar missions discussed in **Section 8.4**, **Architecture Summary**, were developed in the context of the NASA manned spaceflight program. This study recognized the importance of ISS missions in maturing the reliability of the most critical systems for the lunar mission (CEV, CEV/SM, and lunar ascent). This maturation process puts a significant burden of coping with failures on the ISS, but provides a tremendous opportunity for reliability growth of these systems (if NASA chooses to recognize this risk, learn from this experience, and continue flying if failures occur). The integrated mission model indicates that there is a significant likelihood that failure will occur, and analysis has shown that early crewed CEV missions will be riskier than the Shuttle. With the ISS cargo missions, the CEV reaches maturity in 2015 and is safer than the Space Transportation System (STS) by the third crewed flight. Moving the crewed flights within the schedule has a significant effect on the estimated risk.

The results of the analysis are shown in **Table 8-9**. The upper portion of the table shows the planned flight schedule for crew and cargo missions to the ISS and Moon. The maturity model shows how the key technologies mature during the process. The risk for LOM and LOC is shown in the bottom of the table.

Table 8-9. Cumulative Campaign Results

Mission Flight Rates														
Missions	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Shuttle	1	3	5	5	3	3	0	0	0	0	0	0	0	0
HTV (H2)	0	0	0	0	1	1	1	1	1	1	1	1	0	0
ATV (Ariane)	0	1	1	1	1	1	1	1	1	1	1	0	0	0
Soyuz	0	1	1	2	2	2	1	0	0	0	0	0	0	0
Progress	0	0	0	3	3	4	5	0	0	0	0	0	0	0
CEV_DEV_SO	0	0	0	0	1	1	2	0	0	0	0	0	0	0
CEV_DEV_ORB	0	0	0	0	0	0	2	0	0	0	0	0	0	0
ISS_UnPress	0	0	0	0	0	0	1	0	1	1	1	1	0	0
CEV_ISS	0	0	0	0	0	0	1	2	2	2	2	2	0	0
ISS_Pres	0	0	0	0	0	0	0	3	3	3	3	3	0	0
Con-1	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Con-2	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Con-3	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Con-4	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Maturity Model														
SM_Orbit_Ajust (LOX/ CH4)/CEV ISS	20.0%	20.0%	20.0%	20.0%	20.0%	20.0%	20.0%	12.7%	5.9%	1.2%	0.3%	0.3%	0.3%	0.3%
Launcher (13.1)	30.0%	30.0%	30.0%	30.0%	30.0%	30.0%	30.0%	1.5%	0.2%	0.2%	0.2%	0.2%	0.2%	0.2%
Docking_Auto_station	10.0%	10.0%	10.0%	10.0%	10.0%	10.0%	10.0%	7.2%	2.3%	2.0%	2.0%	2.0%	2.0%	2.0%
Loss of Mission Risk														
Shuttle	0.01	0.03	0.05	0.05	0.03	0.03	–	–	–	–	–	–	–	–
HTV (H2)	–	–	–	–	0.29	0.27	0.26	0.25	0.24	0.23	0.22	0.21	–	–
ATV (Ariane)	–	0.06	0.05	0.05	0.04	0.03	0.03	0.03	0.02	0.02	0.02	–	–	–
Soyuz	–	0.01	0.01	0.02	0.02	0.02	0.01	–	–	–	–	–	–	–
Progress	–	–	–	0.12	0.12	0.16	0.20	–	–	–	–	–	–	–
CEV_DEV_SO	–	–	–	–	0.01	0.19	0.21	–	–	–	–	–	–	–
CEV_DEV_ORB	–	–	–	–	–	–	0.44	–	–	–	–	–	–	–
ISS_UnPress	–	–	–	–	–	–	0.33	–	0.08	0.03	0.02	0.02	–	–
CEV_ISS	–	–	–	–	–	–	0.19	0.22	0.08	0.02	0.01	0.01	–	–
ISS_Pres	–	–	–	–	–	–	–	0.37	0.14	0.08	0.07	0.07	–	–
Con-1	–	–	–	–	–	–	–	–	–	–	–	–	0.03	–
Con-2	–	–	–	–	–	–	–	–	–	–	–	–	0.03	–
Con-3	–	–	–	–	–	–	–	–	–	–	–	–	–	0.05
Con-4	–	–	–	–	–	–	–	–	–	–	–	–	–	0.06
Total Incidents	**0.01**	**0.11**	**0.22**	**0.46**	**0.96**	**1.68**	**3.35**	**4.21**	**4.78**	**5.16**	**5.51**	**5.83**	**5.88**	**5.99**
Loss of Crew Risk														
Shuttle	1.0%	3.0%	5.0%	5.0%	3.0%	3.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Soyuz	0.0%	0.3%	0.3%	0.5%	0.5%	0.5%	0.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
CEV_ISS	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	1.9%	2.2%	0.8%	0.2%	0.1%	0.1%	0.0%	0.0%
Con-3	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.6%
Con-4	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	1.5%
Total Success	**99.0%**	**95.8%**	**90.8%**	**85.8%**	**82.8%**	**79.9%**	**78.2%**	**76.5%**	**75.9%**	**75.7%**	**75.6%**	**75.5%**	**75.5%**	**75.5%**
Probability_LOC	**1.0%**	**4.2%**	**9.2%**	**14.2%**	**17.2%**	**20.1%**	**21.8%**	**23.5%**	**24.1%**	**24.3%**	**24.4%**	**24.5%**	**24.5%**	**24.5%**

The integrated LOM risk for the traffic model is shown in **Figure 8-41**. This shows that the manned missions are a small contributor to the total mission losses. The LOM estimate is dominated by the HTV due to the estimated unreliability of the Japanese HII launcher. The CEVs are less reliable during their early missions, but improve dramatically after 2013. The ATV is a small contributor because it flies only once a year and is relatively mature. This result indicates that it would be prudent for NASA to develop a method to cope with failures and be able to return to flight as soon as possible. It would be wise to treat all early flights as test flights and thoroughly examine anomalies, perhaps even having a preconvened accident investigation board ready to investigate and close out incidents.



Traffic Model of Flights/Year

2005	2006	2007	2008	2009	2010	2011
1	3	5	4+1	3	3	0
0	1	1	1	1	1	1
0	0	0	0	1	1	1
0	1	1	2	2	2	1
0	0	0	3	3	4	5

Figure 8-41. Probability of LOM Per Year

Figure 8-42 shows the integrated LOC results. This result indicates that STS launches present the greatest risk to the crew. The CEV missions to ISS are initially risky, but become small after the first 3 years. A close look at the maturity model shows how the ISS cargo missions are effective in lowering risk for the crew since they share the same SM.

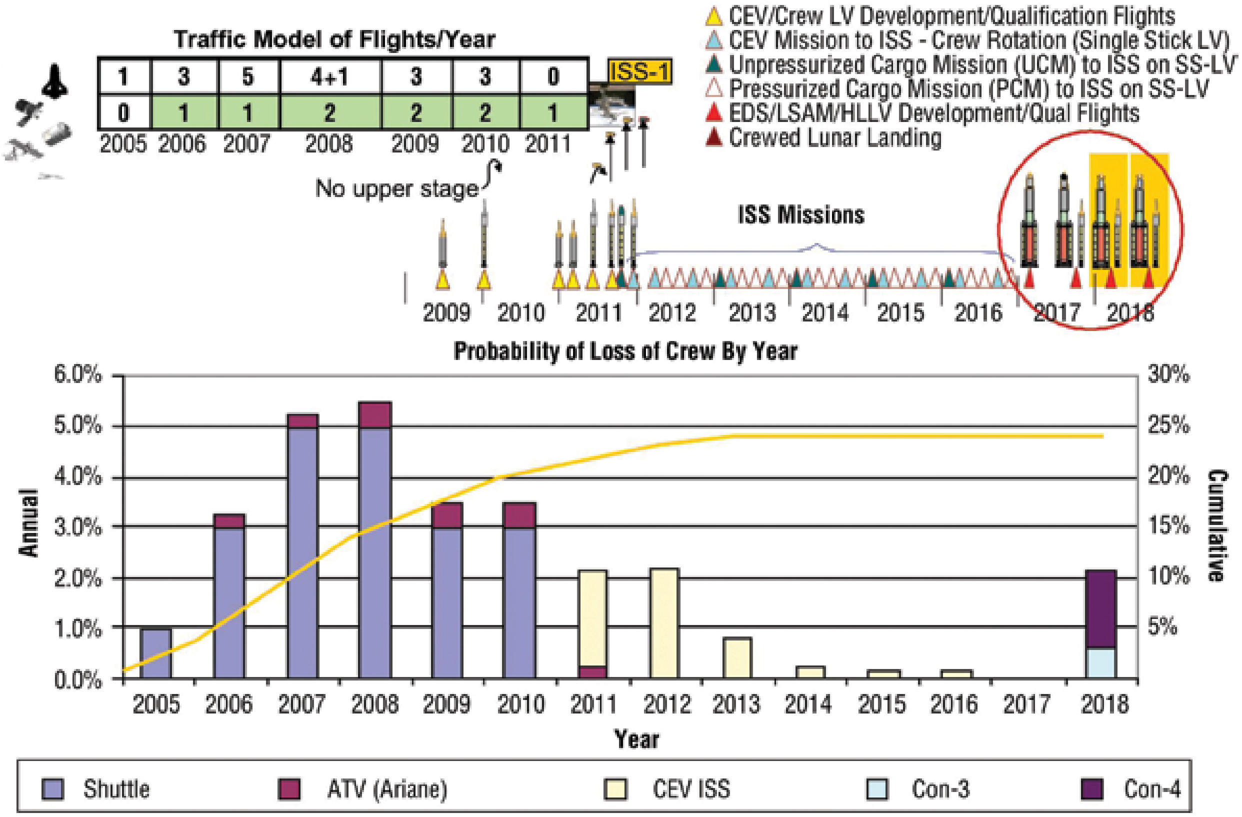


Figure 8-42. Probability of LOC Per Year

Figure 8-43 illustrates how ISS cargo missions aid in the maturation of the CEV crewed vehicle since they share the same SM. The upper curve shows crewed flights only, with no cargo and two test flights. The bottom curve shows the current schedule, which is two test flights, one cargo flight, and then alternating crewed and cargo flights (two and four per year, respectively). In either case, it takes five flights, in addition to the two test flights, to surpass the Shuttle safety level of 1 in 100.

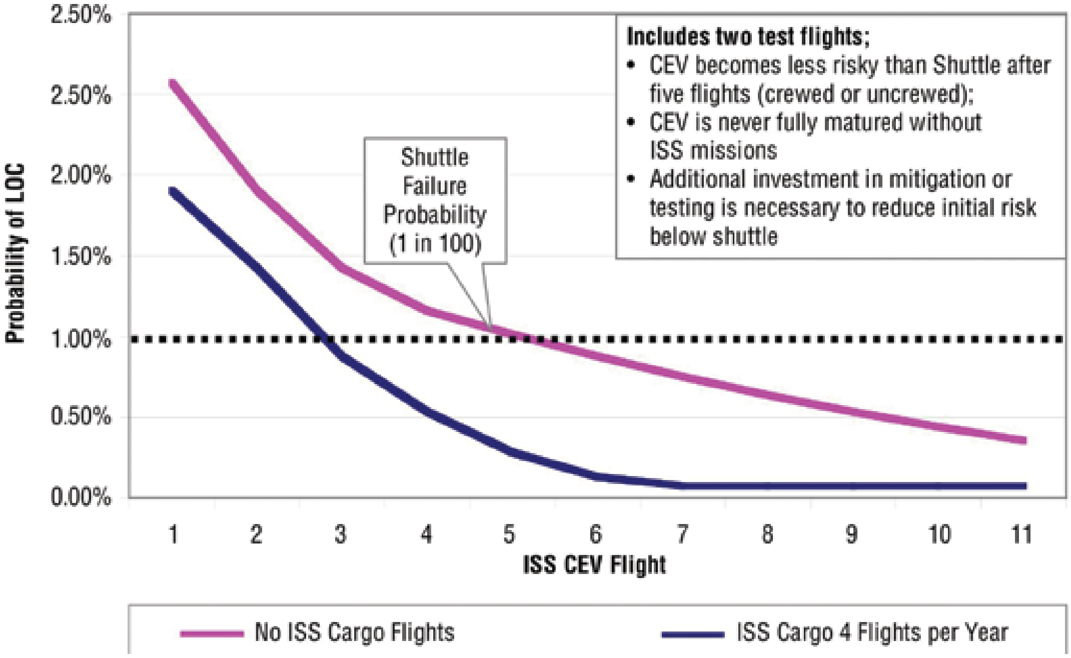


Figure 8-43. Benefit of ISS Cargo Flights on Crew Safety

If the schedule is followed, the first crewed flight would have three maturity flights (two test and one cargo) before it flies. Therefore, it would be less than twice the Shuttle risk, approximately 1 in 50. If there were no cargo flights beforehand, the risk of the first crewed flight after the two test flights would be approximately 1 in 40, or approximately 2.5 percent (2.5 times the Shuttle).

The additional cargo flights allow the system to mature at a faster rate, achieving a factor of 10 improvement over the Shuttle in the seventh flight. Without the cargo flights, the CEV is only about 3 times better than the Shuttle at the end of the 11 ISS missions.

8.6 Forward Work

By organically including quantitative risk assessment into the design process, the ESAS was able to perform complex trades across multiple Figures of Merit (FOMs) and arrive at a solution that effectively blended performance and risk within time and budget constraints. These blends applied technology to enable safer mission modes and reduced mass in areas that were overprotected. This organic process can be applied at any level. SPACE models can be developed to assure that lunar basing strategies account for potential failures during the campaign and effectively blend in new capabilities without undue increases in risk. This blending process will allow the benefits of system maturity to be applied to developing new systems. This process can also be applied at the systems and component level of the architecture. Employing these techniques in developing requirements for crew escape could help NASA develop a balanced design that is focused on risk drivers.

As the SPACE models are developed to higher and lower levels, they can be combined with development risk models and cost model results to provide an integrated view of the overall program. This view will allow NASA to make decisions on an integrated basis such that the program is structured to reduce the vulnerability to failure, balance the resources used to prevent failure, and assure that resources and activities are organized to maximize return given the inherent uncertainties.

Most importantly, this approach can be applied to enhance the decision-making process within the concept of an "Observation, Orientation, Decision, Action (OODA) Loop" (Reference 7 in **Section 8.7**, **References**) shown in **Figure 8-44**. This process can be applied by NASA to create a decision-making environment that will allow NASA to cope with the uncertainty in space programs. This is done by improving the capability to apply heritage information with information gleaned from unfolding circumstances within an integrated analytical framework that is agile enough to allow the synthesis of multiple responses that affect cost, risk, performance, and schedule. Currently, NASA is hobbled by complex analytical tools that make it difficult to explore a decision space effectively. The quality of the analysis is perceived to increase with additional fidelity. However, as fidelity increases, the interactions between model elements grows exponentially, and it becomes impossible to analyze more than a few design reference architectures or missions, even with the current significant growth in computational power. By using the SPACE analysis process, model fidelity is increased where the increase in fidelity provides insight to the decision at hand. The analytical framework must be simple enough and flexible enough to provide answers at an appropriate level of detail as both the environment and questions themselves change.

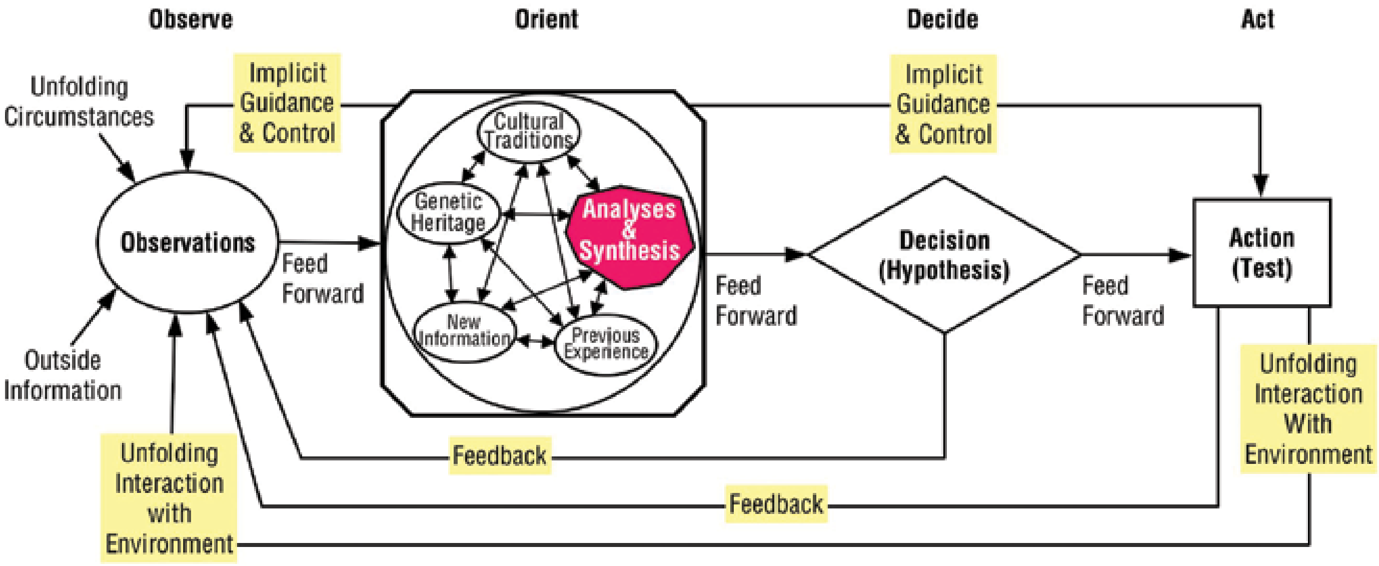


Figure 8-44. Boyd's OODA Loop

An initial application of this approach is the decision-making process regarding the interaction between the Shuttle manifest to the station (i.e., number of flights and content) and the progress being made on the CEV. Given the current uncertainty in the projections of equipment reliability and the lack of a probabilistic model for the performance of the ISS, decisions might be made that will result in either too many or too few logistics flights to the ISS. Since each Shuttle flight is so precious to NASA and its partners, integrated models that can adapt to new information will be extremely valuable. These models can capture operating experience of ISS equipment and project that reliability into the context of ISS operability with different sparing strategies and gaps in logistic flights. These models can be combined with development risk models to determine the likelihood and consequences of gaps between Shuttle termination and CEV missions. If this model is updated on a continuous basis, the program will be able to assimilate new information from both sides and make decisions that will most effectively apply the Shuttle assets.

8.7 References

1. Fragola, J.R. 2005, "Reliability and Crew Safety Assessment for Solid Rocket Boost/ J–2S-Based Launch Vehicle," SAIC, New York, April 2005.
2. Cirillo, W.M., Letchworth, J.F., Putney, B.F., Fragola, J.R., Lim, E.Y., Stromgren, C., "Risk-Based Evaluation of Space Exploration Architectures," January 11, 2005.
3. NASA, Space Shuttle Probablistic Risk Assessment, Iteration 2.0, Space Shuttle Program, February 2005 (Draft).
4. United Space Alliance, Introduction to Rendezvous Guidance, Navigation and Control.
5. Rendezvous GPO Console Handbook.
6. JSC – 49626, February 2003, Space Shuttle Rendezvous and Proximity Operations Experience Report.
7. Col John Boyd, USAF (Ret) coined the term "OODA loop" describing the process of Observation, Orientation, Decision, Action, used to dominate an adversary in an uncertain environment. (See http://www.d-n-i.net/second_level/boyd_military.htm.)