STI 10-001

Constellation Probabilistic Risk Assessment (PRA): Design Consideration for the Crew Exploration Vehicle

Peter G. Prassinos[a], Michael G. Stamatelatos[a], Jonathan Young[b], Curtis Smith[c]
[a]National Aeronautics and Space Administration, Washington DC, USA
[b]Pacific Northwest National Laboratory, Hanford, WA, USA
[c]Idaho National Laboratory, Idaho Falls, ID, USA

Managed by NASA's Office of Safety and Mission Assurance, a pilot probabilistic risk analysis (PRA) of the NASA Crew Exploration Vehicle (CEV) was performed in early 2006. The PRA methods used follow the general guidance provided in the NASA PRA Procedures Guide for NASA Managers and Practitioners[1]. Phased-mission based event trees and fault trees are used to model a lunar sortie mission of the CEV – involving the following phases: launch of a cargo vessel and a crew vessel; rendezvous of these two vessels in low Earth orbit; transit to the moon; lunar surface activities; ascension from the lunar surface; and return to Earth. The analysis is based upon assumptions, preliminary system diagrams, and failure data that may involve large uncertainties or may lack formal validation. Furthermore, some of the data used were based upon expert judgment or extrapolated from similar components/systems. This paper includes a discussion of the system-level models and provides an overview of the analysis results used to identify insights into CEV risk drivers, and trade and sensitivity studies. Lastly, the PRA model was used to determine changes in risk as the system configurations or key parameters are modified.

Keywords: PRA, Space Systems

1. INTRODUCTION

The pilot CEV probabilistic risk assessment (PRA) was conducted for the Constellation Program and in particular, to gain safety and performance insights involving into the design and operation of a Crew Exploration Vehicle (CEV) for a Lunar Sortie Mission[2]. The assessment was initiated to gain an increased understanding of possible design trades associated with systems and operations for this mission. This effort was coordinated with other analyses to assess the feasibility of establishing safety and reliability requirements associated with the probability of loss-of-mission (LOM) and the probability of loss-of-crew (LOC)[3]. The study team worked to address overall analysis scope and methods, mission event tree structure, system dependencies, success criteria, and basic event and component failure data.

The initial objectives of this study were to help optimize the CEV design by conducting integrated assessments and trade studies among the systems and across the entire mission profile. The scope of this assessment is the CEV consisting of the Crew Module (CM), Service Module (SM) and Launch Abort System (LAS). This assessment does not include models for other mission vehicles or operations [Cargo Launch Vehicle (CaLV), Earth Departure Stage (EDS) and Lunar Surface Access Module (LSAM)]. For these vehicles and operations, data were derived from the ESAS[4] Study.

The objectives of this study were to:

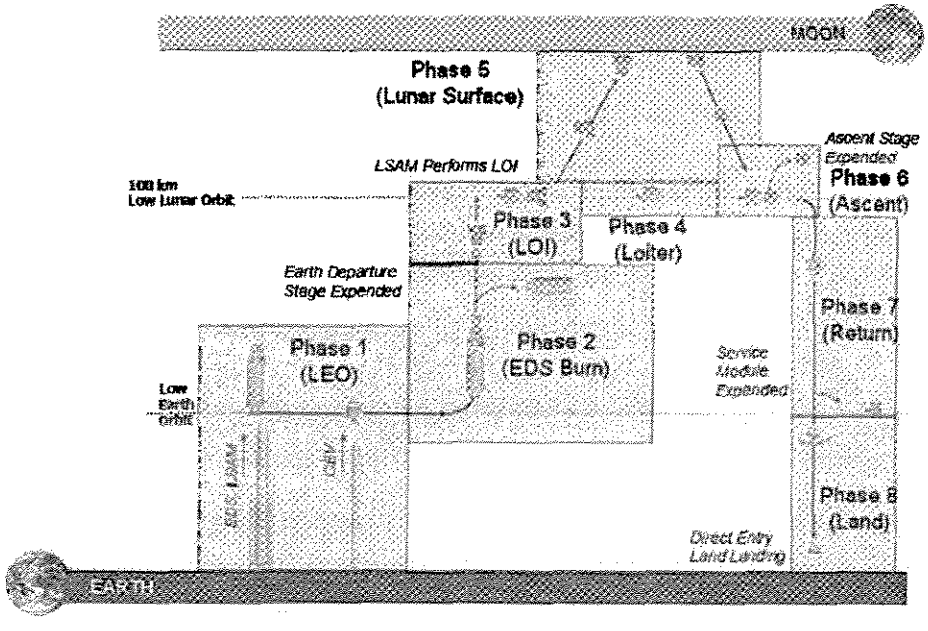
- Provide insight into designs options needed to meet mission reliability requirements.
- Provide a framework to evaluate proposed CEV designs.
- Provide a basis for the development of a complete detailed phased mission integrated PRA of proposed vehicles included in associated missions.
- Provide a quantitative model that can be used to support trade studies, operational decisions, and upgrade improvements throughout the program life-cycle.

2. METHODOLOGY AND MODELING

The pilot CEV PRA utilizes a "phased" approach to decompose portions of the mission. As shown in Figure 1, the mission is covered by eight phases from launch to earth return. The mission phases are:

- *Phase 1 – Two launches to Low Earth Orbit (LEO).* The first launch is the Cargo Launch Vehicle (CaLV) consisting of a Lunar Surface Access Module (LSAM) and an Earth Departure Stage (EDS). The second launch is the Crew Launch Vehicle (CLV) which contains the CEV, consisting of a Crew Module (CM), a Service Module (SM), and a Launch Abort System (LAS).
- *Phase 2 – Rendezvous of the CaLV and the CEV.* The EDS is used (via Trans-Lunar Injection (TLI burn)), then expended, leaving the CEV and LSAM.
- *Phase 3 – Lunar-Orbit Insertion (LOI).* The LSAM performs the LOI for both the CEV and LSAM. All members of the CEV crew transfer to the LSAM and it undocks from the CEV for descent to the lunar surface.
- *Phase 4 – CEV in lunar orbit. The* unmanned CEV remains in a lunar orbit, but will descend to a parking orbit during the seven-day lunar mission.
- *Phase 5 – Lunar mission.* The LSAM is used to descend to and ascend from the lunar surface. A typical lunar mission will last up to seven days.
- *Phase 6 – Re-crew CEV.* Following the LSAM ascent (the descent stage is left on the lunar surface), the crew docks with and transfer back to the CEV. The LSAM (ascent stage) is expended back to the lunar surface.
- *Phase 7 – Return to Earth.* The CEV returns to earth, where the SM is expended when no longer needed.
- *Phase 8 – Earth landing.* The CEV lands on the Earth with a direct entry and parachute-assisted land touchdown.

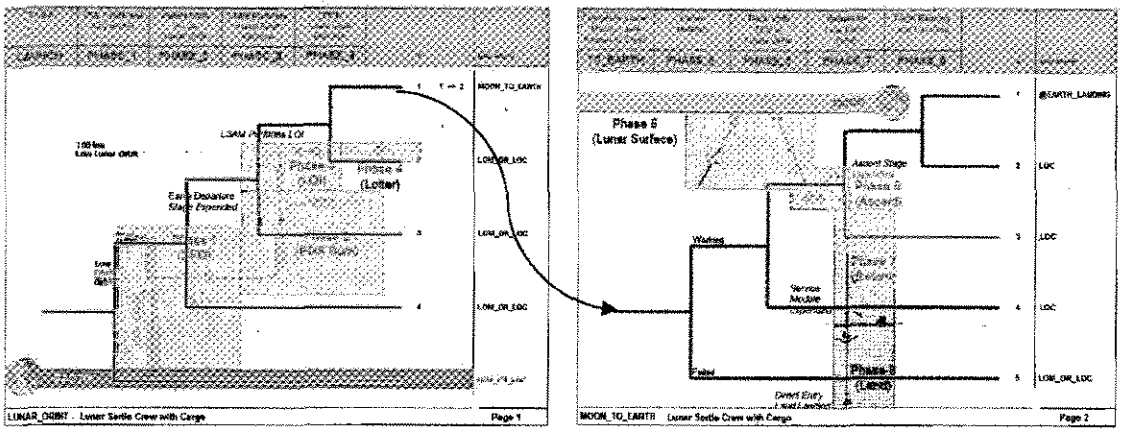
Figure 1. Mission phases for the lunar sortie crew with cargo.



The mission phases are modeled using the two event trees, shown in Figure 2, to identify scenarios. Fault trees were used to model system failures within a specific phase. The undesirable outcomes addressed in this PRA are based upon two figures of merit (or end states) for the CEV, namely; LOM and LOC:

- LOC provides safety insight for conducting this mission and returning the crew safely to earth.
- LOM provides insight on mission performance for a lunar sortie.
- These above two figures of merit are not mutually exclusive. A LOM end state results in an attempted return-to-Earth. If the abort or return-to-Earth and landing fail, the LOM leads to an LOC.

Figure 2. Phased Mission Event Trees



The system models in this PRA (fault trees) are consistent with the proposed design architecture associated with the initial design reference mission. The fault trees capture the conceptual train design and the interconnected nature of the various systems and subsystems both within a mission phase and across the mission profile. An inter-system dependency matrix was used to identify the operating condition and dependencies among the systems during each particular mission phase modeled in the event trees. The operating condition for each system along with the definitions of LOC and LOM led to the development of success criteria:

- After the lunar mission has been completed successfully (Phase 5), the mission is assumed to be complete and LOM is no longer considered; only LOC is considered. This assumption implies that the "mission" part of the lunar mission is completed during Phase 5.

- Catastrophic failures provide no chance for crew survival leading directly to LOC. Success of systems needed for an abort and landing result in LOM but not LOC. Failure of systems needed for a successful abort or landing during a return-to-Earth scenario result in LOC.

- Generally for the systems modeled; for a three string system, LOM is assumed to occur when two of three strings fail and only one string is left functional (i.e., 2-out-of-3 strings failed). For a two string system, LOM is assumed to occur when one of the strings fail and only one string is left functional (i.e., 1-out-of-2 strings failed). LOC occurs upon loss of all strings in a single system.

- Common-cause failures are modeled for all redundant systems.

The PRA model contains seven primary systems that perform the major functions for the mission to the lunar surface and return to earth:

- Propulsion including the main engine (ME), reaction control system (RCS), mechanical equipment (pumps, valves and controllers), and the propellant/helium tanks.
- Avionics system that receives inputs from the crew, sensors and external communications; perform navigation, guidance, and internal state calculations; and provides control and actuation signals.
- Electric Power System (EPS) including batteries, solar arrays and electrical distribution and control subsystems.
- Active Thermal Control System (ATCS) including heaters, coolers, condensate controller and mechanical equipment.
- Environmental Control and Life Support System (ECLSS).
- Launch Abort System (LAS).
- Pyrotechnic (PYRO) devices that affects component separation.

Each system is modeled for each phase in the mission. The overall PRA contains: 2 event trees with 2 end states (LOC and LOM), 155 fault trees (973 gates) and 874 basic events. This PRA was developed by the OSMA team over the course of approximately 90 days using the SAPHIRE[5] PRA software. The basic event data were derived from the Space Shuttle PRA, the International Space Station (PRA), the ESAS Study and similarity to heritage systems/components.

3. RESULTS

The overall results of the PRA indicate that the mean probability of LOC is 0.017 with 5% and 95% uncertainties of 4.6E-05 and 0.071, respectively. The mean probability of LOM is 0.12 with 5% and 95% uncertainties of 3.7E-04 and 0.48, respectively. The overall mission probability and uncertainty for LOC and LOM are shown in Figure 2. The cumulative mean probability of LOC is given in Figure 4.

The dominant contributors to LOC for the overall mission account for about 66% of the overall mean probability of LOC:

- During Phase 4 (CEV in lunar orbit) the CEV fails to stay in Lunar orbit and the crew fails to recover the CEV upon return from the Lunar surface (P=5.0E-03).
- During Phase 8 (Earth Landing) failure to recover the crew (search and rescue) after landing (P=2.6E-03).
- During Phase 8 (Earth Landing) common cause failure of 2 parachutes (out of 3) during deployment (P=9.8E-04).
- During Phase 8 (Earth Landing) the CM RCS fails to provide correct attitude (P=9.0E-04).

The dominant contributors to LOM for the overall mission account for approximately 63% of the overall mean probability of LOM:

- During Phase 5 (Lunar Mission) unspecified failures occur and the crew fails to recover from those failures (P=3.5E-02).
- During Phase 1 (Two launches to Low Earth Orbit [LEO]) EDS fails to loiter in LEO (P=1.0E-02).
- During Phase 1 (Two launches to Low Earth Orbit [LEO]) LSAM fails to loiter in LEO (P=1.0E-02).
- During Phase 2 (Rendezvous of the CaLV and CEV) the EDS, LSAM, and CEV TLI burn fails (P=1.0E-02).
- During Phase 2 (Rendezvous of the CaLV and CEV) the EDS, LSAM, and CEV TLI mid-course correction burn fails (P=1.0E-02).

Figure 3. Overall Mission Probability and Uncertainty for LOC and LOM

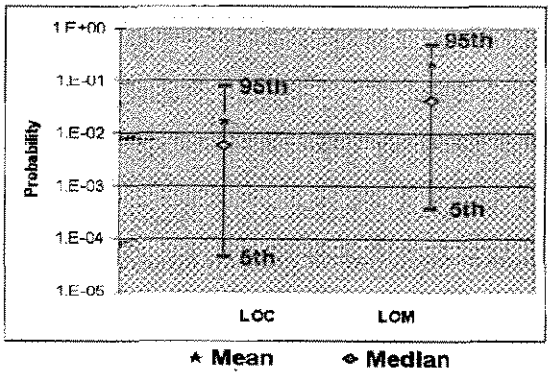
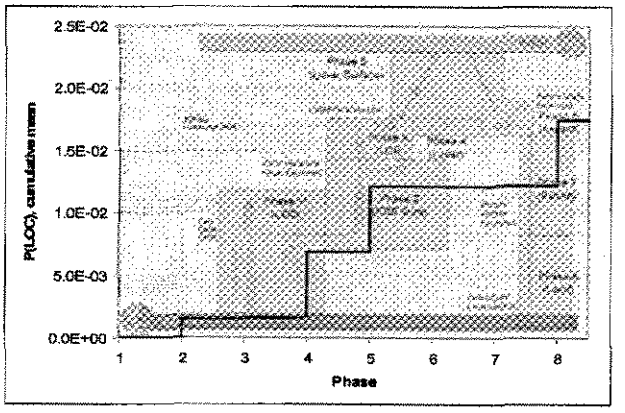


Figure 4. Cumulative Mean Probability of LOC



The mission phases with the largest contribution to mission LOC mean failure probability are:

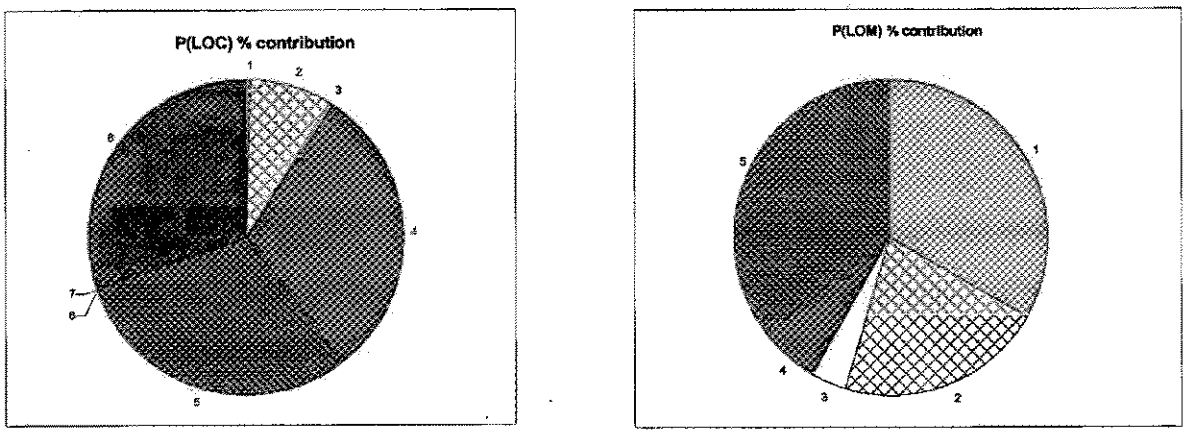
- Phase 4, *CEV in Lunar Orbit*: 5E-03 (30%)
- Phase 8, *Earth Landing*: 5E-03 (30%)
- Phase 5, *Lunar Mission*: 5E-03 (30%)

The mission phases with the largest contribution to mission LOM mean failure probability are:

- Phase 5, *Lunar Mission*: 4E-02 (35%)
- Phase 1, *Two Launches to Low Earth Orbit (LEO)*: 4E-02 (34%)
- Phase 2, *Rendezvous of the CaLV and CEV*: 3E-02 (21%)

The relative contribution to of LOC and LOM from each phase is shown in Figure 5.

Figure 5. Relative Contribution to the Mean Probability of LOM and LOC from each Phase



Inspection of Figure 4 provides insight into which mission phase contributes most to the risk of both LOC and LOM. Comparing the two pie charts indicates that there are two mission phases that contribute most to both LOC and LOM. From these results, further consideration with respect to the design and operations involved in Mission Phase 5; descend to, lunar surface activities and ascend from the lunar surface, will have the most impact on reducing risk for both safety and performance. In the same way but to a lesser degree, more attention to Mission Phase 2; low earth orbit rendezvous of the CaLV and the CEV and transit to moon, will have similar affects.

These results identify potential significant risk drivers that require further study to completely understand their failure contribution and to identify design and operational measures and controls that will prevent (reduce the likelihood of) and/or mitigate (reduce the consequences associated with) the risk of LOC and LOM. The list of dominant risk contributors indicates what types of failures during which mission phases may require attention to manage mission risk. This contributor information is often referred to as risk insights, because it provides both qualitative information (e.g., a description of combinations of mission failure events) as well as quantitative risk results. This type of information may suggest alternative system designs, operating modes, backups, and/or diverse methods to accomplish mission functions.

4. TRADE AND SENSITIVITY STUDIES

Numerous trade and sensitivity studies were conducted with this PRA model of the CEV Lunar Mission. The results of selected studies are presented below.

4.1 Removal of One Active Thermal Control System (ATCS) String

The nominal ATCS is modeled with two redundant strings. Removing one ATCS string from the model simulates a CEV design with a single ATCS string. The evaluation of the mission with a single string ATCS shows a small effect on LOC (~5% increase) indicating that the single string ATCS is robust with respect to other contributors to overall mission LOC. With a one string ATCS, the dominant contributor to the mean probability of LOC are: CEV fails to stay in lunar orbit; failure to recover the crew after landing; and failure of the Service Module burn for return to Earth.

Under the model assumptions, LOM is not applicable. When LOC occurs from failure of the single ATCS string, a LOM also occurs. This result occurs because the model assumes that LOM results if one ATCS string (out of 2) fails

4.2 Removal of Launch Abort System (LAS)

This trade study was performed to evaluate the importance of the LAS. This study is only pertinent to Phase 1, since the LAS is jettisoned prior to CEV injection into LEO. Removal of the LAS increases the overall mission mean probability of LOC by a factor of about 2 (100%). This is a significant result. With the LAS, failures during Phase 1 leading to LOC contributes only about 0.6% to overall mission mean probability of LOC. Removal of the LAS results in increasing the mean probability of LOC for Phase 1 by a factor of about 170 and makes Phase 1 the dominant contributor to the overall mission probability of LOC.

4.3 Failure of One Avionics String

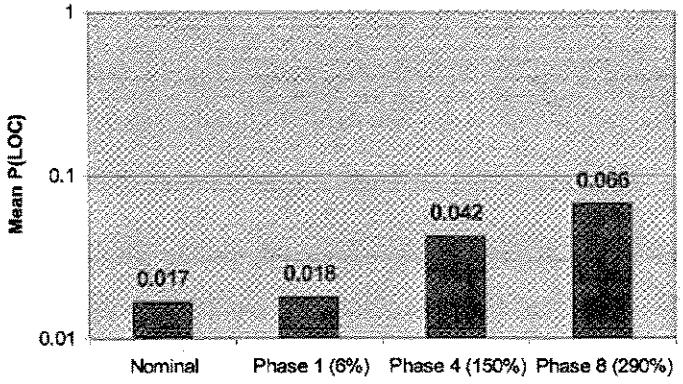
This sensitivity study was conducted to evaluate failure of Avionics string during the three sequential phases: Phase 1, Launch to Low Earth Orbit; Phase 4, CEV in Lunar Orbit; and Phase 8, Earth Landing. Since this system has three redundant strings, this sensitivity study provides insight concerning the importance to the overall mission probability of LOC and LOM of the two failure tolerance requirement.

A comparison of the change in the probability of LOC from the failure of one Avionic string for the three phases is shown in Figure 6. If one Avionic string fails during Phase 1, there is a 6% increase in the probability of LOC (a factor of about 1.06) and a negligible increase in the probability of LOM. Following the failure of one Avionics string for Phase 4, the probability of LOC increases by a factor of about 2.5 (150% increase), and for Phase 8, by a factor of about 4 (290% increase).

Failure of one Avionics string during Phase 1 has a negligible effect on the probability of LOM (<1%). For Phase 4, failure of one Avionics string leads to an increase in the probability of LOM by a factor of about 2 (128%). For failure during Phase 8, there is no effect on LOM since the mission is assumed to be complete and LOM is not considered.

These results show the dependence of these phases on the Avionics and the sensitivity of the analysis on the common cause failures of this three string system. The Avionics system is relatively robust and a two string Avionics system only reduces the overall probability of LOC and LOM by about 1%. However, because of the potential for common cause failures, the failure of one string during Phase 1 increases the probability of LOC and LOM by about 6%. As the mission progresses, the safety and performance of the CEV become more dependent on the Avionics system.

Figure 6. Comparison of the Failure of One Avionics on the Probability of LOC for Selected Mission Phases



5. OBSERVATIONS AND CONCLUSIONS

The information generated by a PRA includes qualitative and quantitative results that support risk informed decisions to manage mission risk by providing a perspective on risk contributors. The PRA for this study produced design level (formulation phase) risk related information concerning a Lunar Sortie Mission for the Constellation Program. As more design details become available, more complex risk assessment and management issues can be addressed by the PRA. Among these perspectives, assessments, and issues are:

- Assessment of compliance to mission reliability requirements
- Identification of significant mission risk contributors
- Determination of the importance of events, systems, mission phases, etc to mission risk
- Continued support of trade studies
- Support mission planning and development
- Assessment of the impact of external events
- Assessment of alternative or supplemental operating modes
- Assessment of alternative mission profiles
- Support for operational risk management
- Assessment of important precursors

Acronyms

ATCS - Active Thermal Control System
CaLV - Cargo Launch Vehicle
CEV - Crew Exploration Vehicle
CLV - Crew Launch Vehicle
CM - Crew Module
ECLSS - Environmental Control and Life Support System
EDS - Earth Departure Stage
EPS - Electric Power System
ESAS - Exploration System Architecture Study
ISS - International Space Station
LAS - Launch Abort System
LEO - Low Earth Orbit
LOC - Loss of Crew
LOI - Lunar Orbit Injection
LOM - Loss of Mission
LSAM - Lunar Surface Access Module
PYRO - Pyrotechnic Device
RCS - Reaction Control System
SM - Service Module
TLI - Trans-Lunar Injection

References

[1] Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Office of Safety and Mission Assurance (August 2002).

[2] Peter Prassinos, OSMA/HQ/NASA; Michael Stamatelatos, Director - SARD/OSMA/HQ/NASA; Curtis Smith, Idaho National Laboratory; Jonathan Young, Pacific Northwest National Laboratory; and Chester Everline, Jet Propulsion Laboratory: "Constellation Probabilistic Risk Assessment (PRA): Design Consideration for CEV, OSMA-PRA-07-01 (May 1, 2006).

[3] Evaluation of SRD Reliability/Probability/Statistics Requirements, CEV Project SE&I Task TDS20, January, 2006, TE/Katy Hurlbert, Ph., JSC/NASA.

[4] Exploration Systems Architecture Study, NASA-TM-2005-214062 (November 2005).

[5] Smith, C.L., J. K. Knudsen, K. Kvarfordt, and S. T. Wood, 'Key Attributes of the SAPHIRE Risk and Reliability Analysis Software for Risk-Informed Probabilistic Applications,' Reliability Engineering and System Safety, 93 (2008) 1151–1164.