Modeling In-Space Aborts for NASA Human Exploration Missions

Mark A. Bigler*
NASA Johnson Space Center, Houston, USA

Abstract: NASA is developing new capabilities to send humans beyond low Earth orbit (LEO) for the first time in several decades with the new Multi-purpose Crew Vehicle (MPCV) Orion spacecraft and Space Launch System (SLS) launch vehicle. As part of these capabilities, NASA is developing means to terminate missions prior to reaching mission destinations in order to save the crew in the event of critical life-threatening failures. This abort capability exists for both ascent and in-space operations. While the risk associated with ascent aborts has been modeled in detail, less has been done in the area of in-space aborts (e.g. Apollo 13). Recent efforts have started to better assess the risk associated with in-space aborts. This paper will describe these efforts. The in-space abort model described in this paper is part of a larger Cross-Program PRA (XPRA) model of exploration missions planned in the next few years to the vicinity of the Moon. The model consists of linked event trees and fault trees and associated rules built using the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) tool. This model structure is being built with flexibility in mind in order to perform risk trades and further expansion of the model.

Keywords: XPRA, abort, fault tree, event tree, SAPHIRE

1. INTRODUCTION

NASA is developing capabilities for crewed missions beyond Low Earth Orbit (LEO) for the first time in nearly 50 years. Given the greater distances from Earth that these missions will entail, it is prudent to develop in-space abort capabilities in order to save the crew in the event of critical life-threatening failures that may occur. Risk is an important consideration in the design and development of this capability. NASA is developing integrated XPRA models for these missions, from pre-launch through landing and rescue of the crew. Much effort has been expended on developing an ascent abort model as part of these XPRA models to assess the risk associated with failures during pre-launch and ascent and the subsequent aborts from these failures [1]. Recent efforts have started to extend the XPRA model to include aborts following orbit insertion, considered the start of in-space operations. The latest model now assesses aborts up to and including completion of the Tran-Lunar Injection (TLI) burn, which places the Orion spacecraft on a trajectory to the Moon. A description of the current state of the in-space abort model is provided in the following sections.

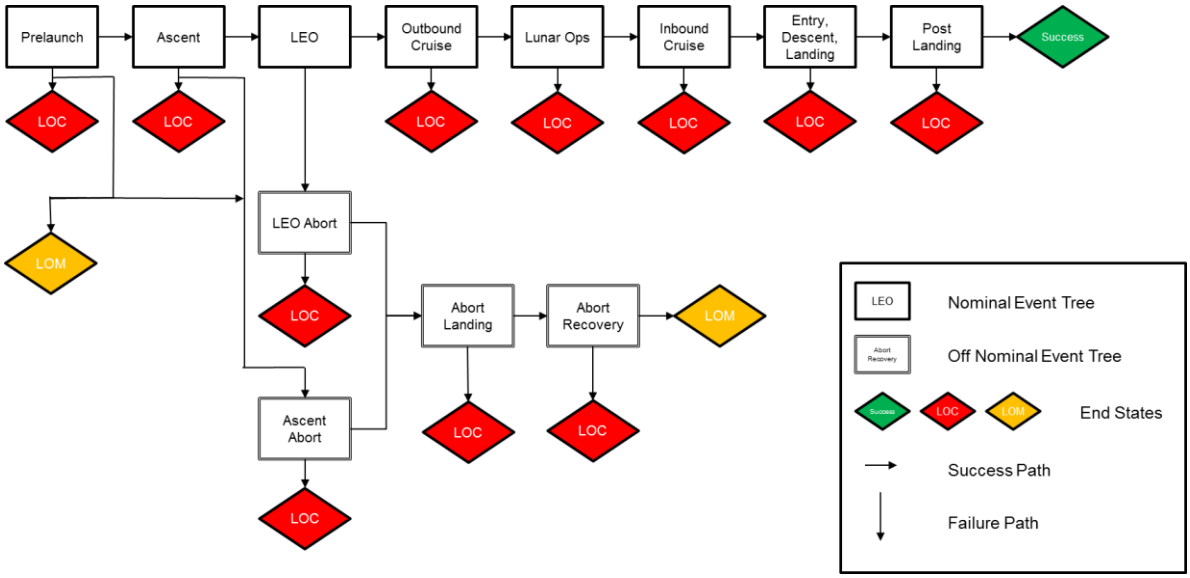
2. OVERVIEW OF THE MISSION MODEL

The XPRA model that NASA is developing for the new deep space missions consists of linked event trees and fault trees and associated rules built using the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) tool [2]. This model integrates PRA models from the MPCV, SLS and Exploration Ground Systems (EGS) Programs. Event trees representing each of the major mission phases have been developed as shown in Figure 1. The single line boxes represent nominal mission phases (e.g. Ascent), while the double line boxes represent off-nominal mission phases (e.g. Ascent Abort) given some survivable failure in one of the nominal mission phases. The end states of interest in the model are either Loss of Mission (LOM), indicated in yellow, or Loss of Crew (LOC), indicated in red. Pad aborts during pre-launch and ascent aborts during ascent have been

* mark.bigler-1@nasa.gov

modeled extensively, while in-space LEO aborts have only been recently modeled. The Ascent Abort event tree consists of major events and failures associated with an initial abort from the SLS launch

Figure 1: Mission Event Tree Structure



vehicle with separation and thrust away from the SLS. The Abort Landing event tree models events and failures associated with the entry, descent and landing associated with the abort, including chute deployment and thermal protection system failure, if applicable. This event tree, along with the Abort Recovery event tree, which models failure of the EGS ground forces to successfully rescue the crew post-landing, are used for both ascent aborts and in-space aborts. The major events in each event tree are linked to fault trees, and event tree rules are used to substitute appropriate fault trees depending on whether the abort is initiated on ascent or in-space, along with what the failure is and when it occurred within those phases. If the abort fails, it results in a LOC. Otherwise, if the abort is successful, it goes to the LOM end state. Some failures that occur in the nominal phases are not abortable and lead directly to LOC, as indicated in Figure 1. The XPRA model does not currently account for aborts following the LEO phase, thus these phases either result in direct LOC or continue with the mission on to the next phase until nominal end of mission and success post-landing with rescue of the crew.

3. OVERVIEW OF THE IN-SPACE ABORT MODEL

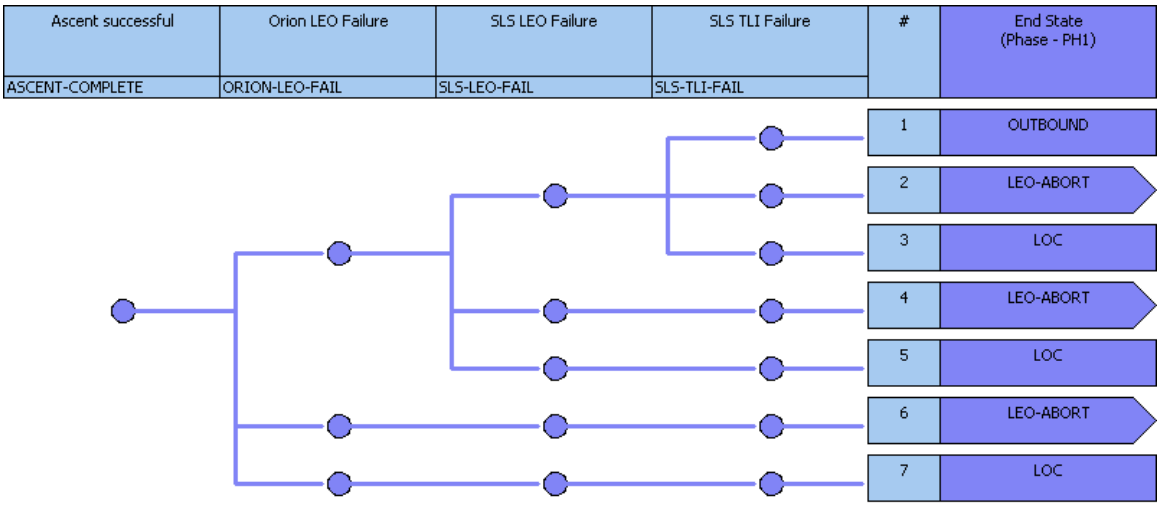
The in-space abort model involves the LEO nominal event tree in Figure 1, along with the LEO Abort, Abort Landing and Abort Recovery off-nominal event trees. This section describes how the in-space abort model is structured and works.

3.1. LEO Event Tree Description

The LEO event tree and its associated linked fault trees contain the failure logic for the scenarios that can lead to either LOC or LEO abort. Figure 2 shows a simplified example of the LEO event tree in the XPRA model. The LEO phase is broken down into two major phases, LEO and the TLI burn. There are three top events in this event tree, two representing failures of either Orion or SLS that occur during LEO, while the third top event represents failures of SLS that occur during the TLI burn. Under each top event there are two failures branches, branch one for failures of Orion or SLS that result in an in-space abort, and branch two failures of Orion or SLS that lead directly to LOC. Failures that occur during the TLI burn are handled separately from the failures that occur during LEO because of the orbital mechanics associated with aborts in each case. Aborts initiated earlier in the TLI burn can result in lower apogees and multiple orbits of the Earth before re-entry in order to return to the

desired landing site, while aborts initiated later in the TLI burn may result in fewer orbits but longer return to Earth. Multiple orbits can also introduce higher risk due to multiple passes through the worst portions of the orbital debris (OD) field surrounding the Earth. To further complicate matters,

Figure 2: LEO Event Tree



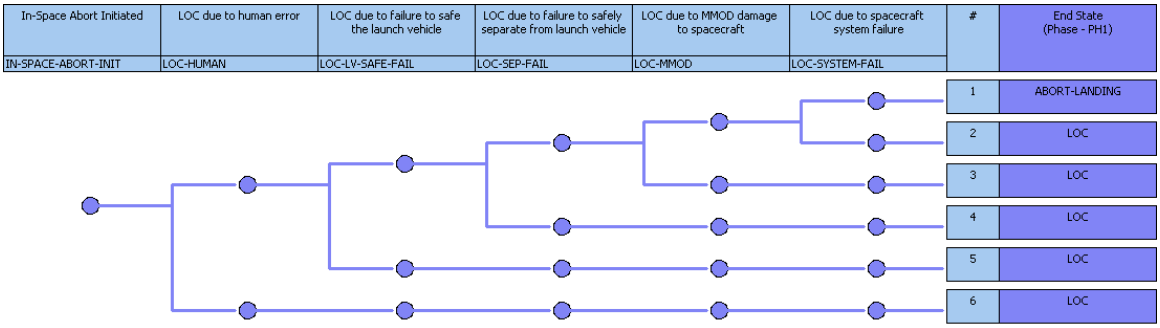
different orbits can also involve multiple burns of the Orion to adjust the orbits and target the desired landing site. Aborts from LEO are generally simpler and involve a de-orbit burn to reach the desired landing site.

3.2. LEO Abort Event Tree Description

As discussed in the previous section, the abort response can be quite different depending on whether the abort is initiated during LEO or during the TLI burn. In addition, the response can be different even depending on when the abort is initiated during the TLI burn. These dependencies are managed in various ways in the XPRA model. The first way is through the use of event tree rules for the LEO Abort event tree to substitute the appropriate fault tree for the scenario conditions. The second way is through the combination of fault trees in both the LEO and LEO Abort event trees and Boolean reduction and cut set minimization. A simplified version of the LEO Abort event tree is shown in Figure 3. There are several ways that the in-space abort can fail prior to re-entry. Many of these aborts are manual aborts, meaning that either the crew and/or mission control are required to detect, evaluate and initiate the abort. This is captured under the first top event in the LEO Abort event tree. The abort can also fail due to failure to safe the SLS, such as terminate thrust, which is captured under the second top event. The abort can fail if the Orion fails to safely separate from the SLS, as indicated under the third top event. A significant concern for safely aborting is the risk associated with the exposure of the Orion to Micro Meteoroid Orbital Debris (MMOD) following the abort prior to re-entry. Finally, the abort can fail due to various Orion system failures prior to re-entry, such as power or cooling failures. The last two failure cases are dependent on when in the TLI burn the abort is initiated and subsequent responses to the abort. In general, the goal is to get the crew back safely on Earth as quickly as possible. However, due to orbital mechanics and the rotation of the Earth, the fastest return to Earth could result in landing in an undesirable location far from rescue forces to retrieve the crew and thus increase the overall risk to the crew. This risk is captured in the Abort Recovery event tree. A more desirable landing location for the crew may necessitate that the Orion make multiple orbits prior to re-entry in order to allow the return trajectory to line up with the desired landing location. This can result in an increase in risk due to increased exposure of Orion to system failures, but perhaps more importantly there is an increased exposure to MMOD due to multiple passes through the worst part of the OD field associated with multiple orbits prior to re-entry.

The first way to account for this dependency is by use of event tree rules for the LEO Abort event tree. Branches in an event tree may have different conditional probabilities depending on the path taken to that point, and the use of event tree rules allows substitution of the appropriate fault tree for the conditions. For instance, if Orion or SLS fail in LEO prior to the TLI burn, represented by the first two top events in Figure 2, and the result is a LEO abort, then the LOC due to MMOD event (LOC-

Figure 3: LEO Abort Event Tree



MMOD) in the LEO Abort event tree is assigned the LEO-MMOD fault tree because of the conditions of the abort. If SLS fails during the TLI burn, represented by the third top event in Figure 2, the default MMOD event TLI-MMOD is used instead. System failures for Orion and SLS are handled similarly, and an example of the rules is shown in Figure 4.

Figure 4: Example Event Tree Rules for LEO Abort Event Tree

```
*****
***** MMOD for LEO Abort substitution rule
|*****
 **** MMOD assigned to each failure scenario
if (ORION-LEO-FAIL[1] + SLS-LEO-FAIL[1]) then  ** Orion or SLS LEO failure
/LOC-MMOD = LEO-MMOD;
LOC-MMOD = LEO-MMOD;
elseif (SLS-TLI-FAIL[1])          ** SLS TLI failure
/LOC-MMOD = TLI-MMOD;
LOC-MMOD = TLI-MMOD;
endif

|*****
***** Orion system failure for LEO Abort substitution rule
*****
 **** Orion system failure assigned to each failure scenario
if (ORION-LEO-FAIL[1] + SLS-LEO-FAIL[1]) then  ** Orion or SLS LEO failure
/LOC-SYSTEM-FAIL = LEO-SYSTEM-FAIL;
LOC-SYSTEM-FAIL = LEO-SYSTEM-FAIL;
elseif (SLS-TLI-FAIL[1])          ** SLS TLI failure
/LOC-SYSTEM-FAIL = TLI-SYSTEM-FAIL;
LOC-SYSTEM-FAIL = TLI-SYSTEM-FAIL;
endif
```

Boolean reduction and cut set minimization is used to simplify the model and accurately account for the dependence on when an MMOD or system failure occurs during an abort. Because it is important when the failure occurs in the TLI burn, the burn has been broken up into five segments from the start of the TLI burn (TLI-0) to when the burn is complete (TLI-100) in equal increments of 25 percent after the burn has started. A basic event for each segment (e.g. TLI-25) is then included in the SLS

failure and MMOD fault trees and each then gets combined with a failure as shown in Figures 5 and 6. The result is cut sets of the form:

SLS-TLI-FAIL1 * TLI-0 from Figure 4
SLS-TLI-FAIL1 * TLI-25 from Figure 4
MMOD-0 * TLI-0 from Figure 5
MMOD-0 * TLI-25 from Figure 5

When the fault trees are used in the SLS sequences for aborts, the SLS failures are combined with the MMOD failures to result in LOC and have the form:

SLS-TLI-FAIL1 * TLI-0 * MMOD-0 * TLI-0

Through Boolean reduction this cut set is reduced to

SLS-TLI-FAIL1 * TLI-0 * MMOD-0

Other cut sets that are produced are of the form:

SLS-TLI-FAIL1 * TLI-0 * MMOD-0 * TLI-25

This cut set is discarded because it is non-minimal to the previous one.

Figure 5: SLS TLI LOM Fault Tree

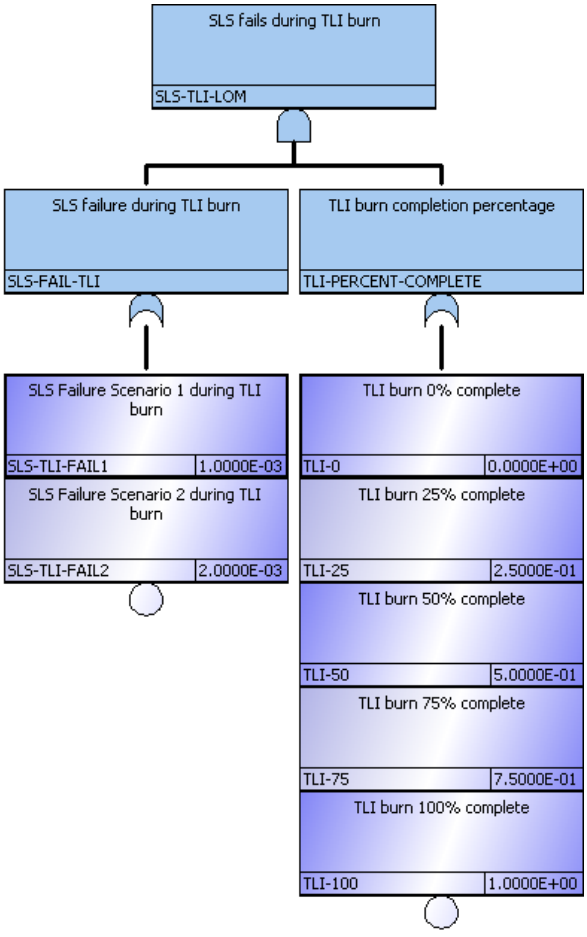
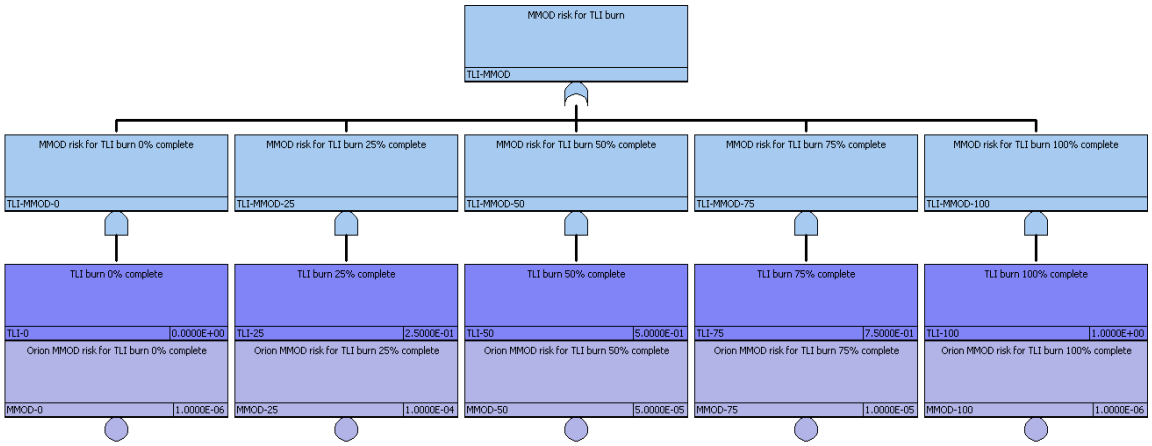


Figure 6: TLI MMOD Fault Tree



The MMOD risk values associated with each of the TLI burn percentages are provided by the Orion MMOD team for the particular return trajectories assumed for those particular percentage completions. Note that all probabilities shown in this paper are purely notional. All of the return trajectories and associated return times are provided by the flight dynamics teams. Thus, development of the in-space abort model involves many different teams besides the PRA teams, including engineering and operations.

3.3. Abort Landing and Abort Recovery Event Tree Descriptions

The Abort Landing and Abort Recovery event trees also utilize rules to assign appropriate failure logic depending on when the failure occurs. For example, the event tree rules apply different risk to the failure of the thermal protection system for an abort from LEO as opposed to an abort from a partial TLI burn.

Of particular interest is the risk associated with rescue of the crew following an abort landing. Ideally, the return trajectory would be targeted to achieve a landing site where the crew can be rescued immediately. For the current in-space abort model in the XPRA, the baseline case assumes return of the crew to the most desirable landing site. Once this baseline case has been established, it is now possible to perform risk trades on various criteria to help the Program identify the options with the lowest overall risk. For example, the return trajectories that minimize the MMOD and system risk may actually result in an overall higher risk due to the potentially higher risks associated with crew landings in areas with a higher probability of adverse sea states and much longer times for rescue forces to arrive.

4. CONCLUSION

The in-space abort model described in this paper has added to the capabilities of the XPRA to help the Orion and SLS Programs make risk-informed decisions. It has shown the benefit of having an in-space abort capability. It has also already provided insights to the Program that could help lead to more risk-informed decision making with respect to the selection of abort trajectories. The model structure has been developed with flexibility in mind in order to perform risk trades and potentially include aborts following successful TLI burn. Future work could also incorporate other related aspects of aborts, including risk impacts of trajectories due to power and thermal performance considerations for example.

Acknowledgements

The author would like to acknowledge the Science Applications International Corporation (SAIC) PRA team located at Johnson Space Center (JSC) located in Houston Texas for their significant contributions to the development of the in-space abort model described in this paper, along with the overall XPRA model in general.

References

[1] M. Bigler and R. L. Boyer, *"Dynamic Modeling of Ascent Abort Scenarios for Crewed Launches,"* International Topical Meeting on Probabilistic Safety Assessment and Analysis, April 2015, Sun Valley, Idaho.

[2] S. T. Wood, C. L. Smith, K. J. Kvarfordt and S. T. Beck, *"NUREG/CR-6952, Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 1 Summary Manual,"* Idaho National Laboratory, Idaho Falls, ID, September 2008.