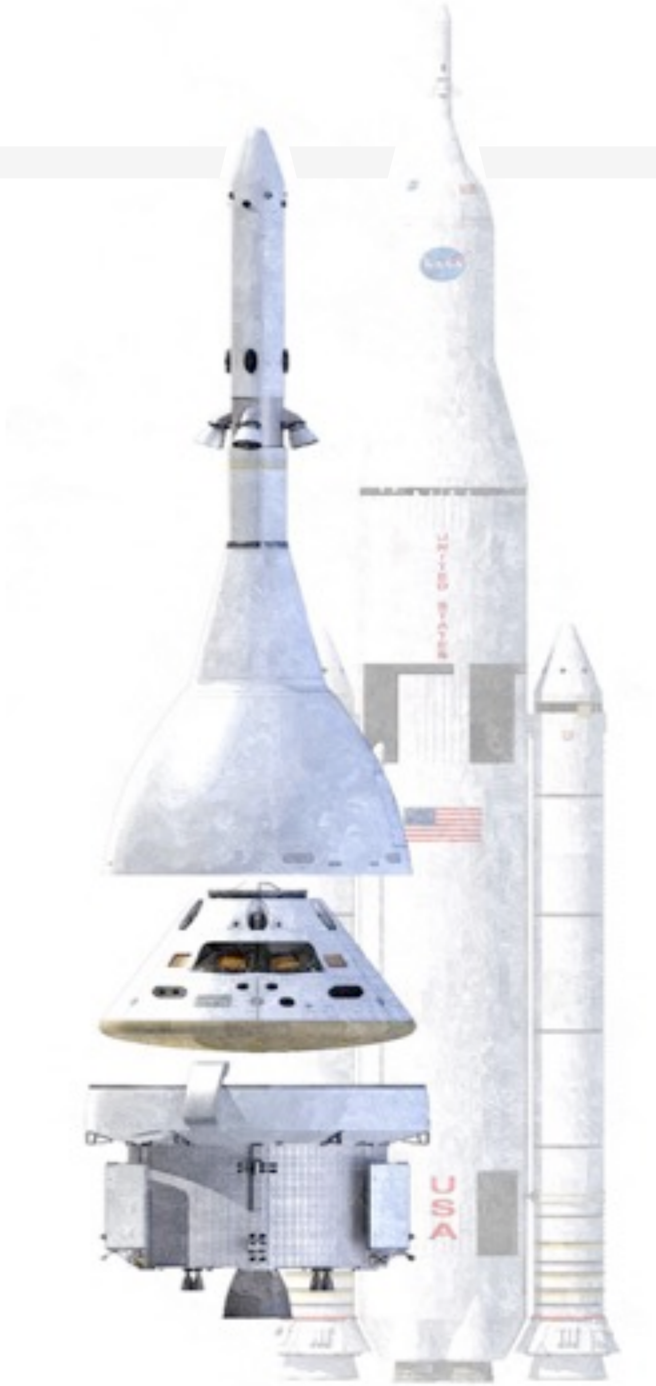


Modeling In-Space Aborts for NASA Human Exploration Missions

Mark A. Bigler
NASA Johnson Space Center, Houston, TX

Presented at the PSAM 14 Probabilistic Safety Assessment & Management Conference at UCLA, CA
September 16 – 21, 2018

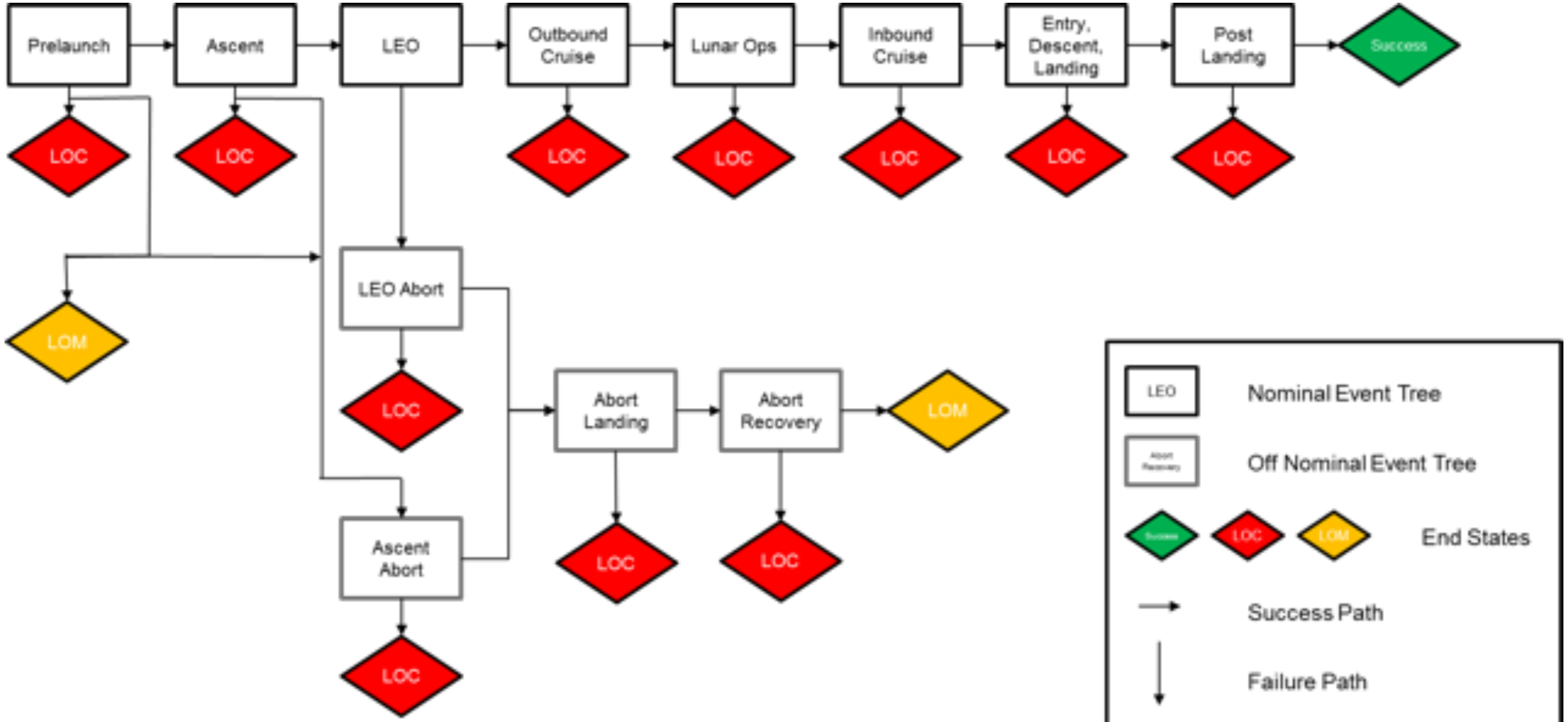
Introduction

- 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.
- NASA has developed a Cross Program PRA (XPRA) of the integrated vehicle, from pre-launch through landing and rescue of the crew.
- An ascent abort model has already been developed as part of this XPRA model to assess the risk associated with failures during pre-launch and ascent (see 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).
- The scope of the analysis discussed here is focused on aborts associated with the in-space portion of the mission up to and including the Trans-Lunar Injection (TLI) burn, which places the Orion spacecraft on a trajectory to the Moon.

Overview of Mission Model

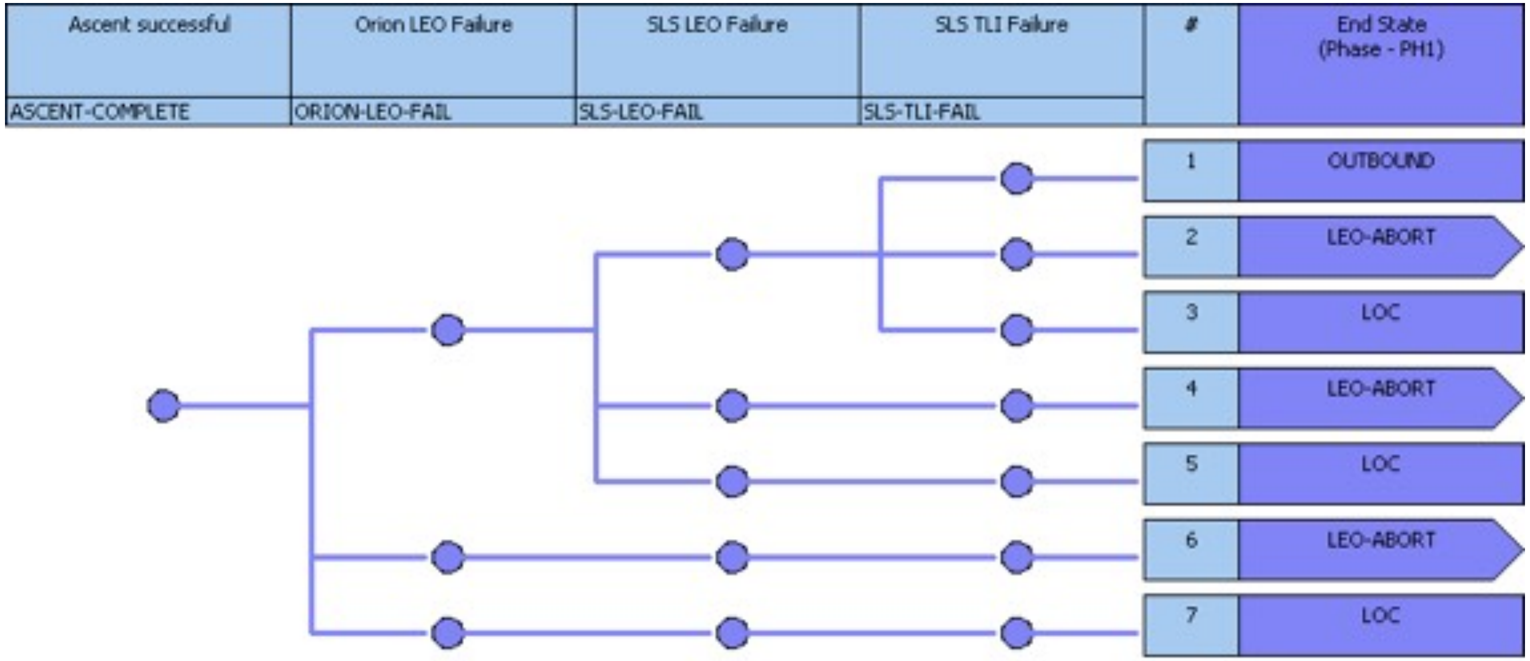
- The XPRA model consists of linked event trees and fault trees and associated rules built using the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) tool.
- This model integrates PRA models from the Orion Multi-Purpose Crew Vehicle (MPCV), Space Launch System (SLS) and Exploration Ground Systems (EGS) Programs.
- Event trees representing each of the major mission phases have been developed as shown on the next slide.

Mission Event Tree Structure



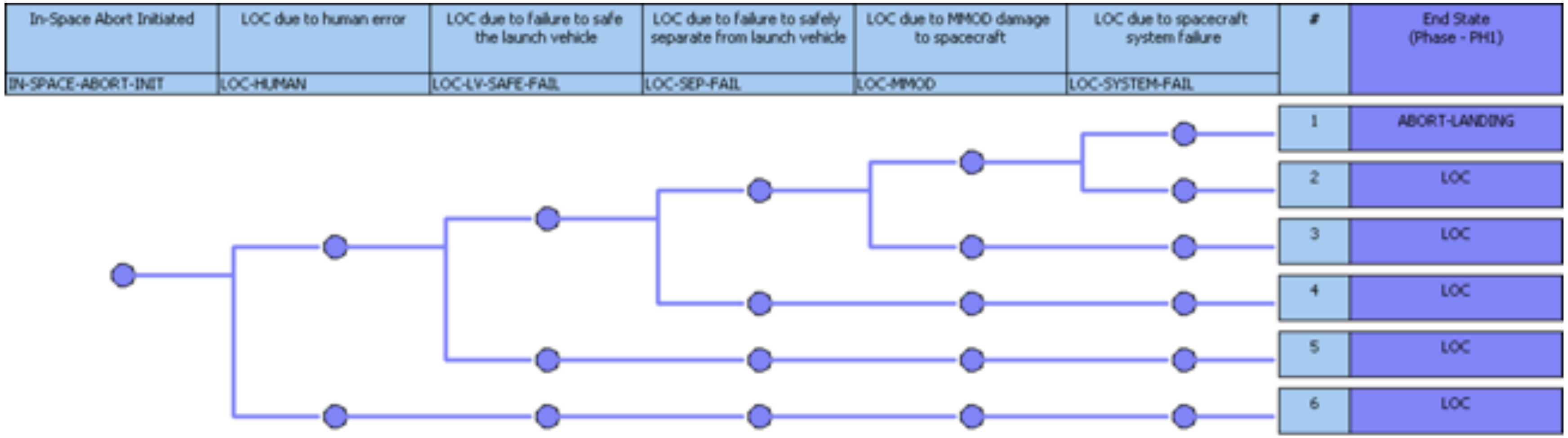
LEO Event Tree Description

- The LEO event tree and its associated linked fault trees contain the failure logic for the scenarios that can lead to either Loss of Crew (LOC) or LEO abort.
- The LEO phase is broken down into two major phases, LEO and the TLI burn.
- Failures that occur during the TLI burn are handled separately from the failures that occur during LEO because of the orbital mechanics.



LEO Abort Event Tree Description

- The abort can fail due to:
  - Failure of the crew and/or mission control to detect and evaluate a condition and initiate a manual abort for those conditions.
  - Failure to terminate the SLS thrust and perform other safing actions.
  - Failure to safely separate from SLS.
  - Micro Meteoroid Orbital Debris (MMOD).
  - Orion system failures prior to re-entry, such as power or cooling failures.



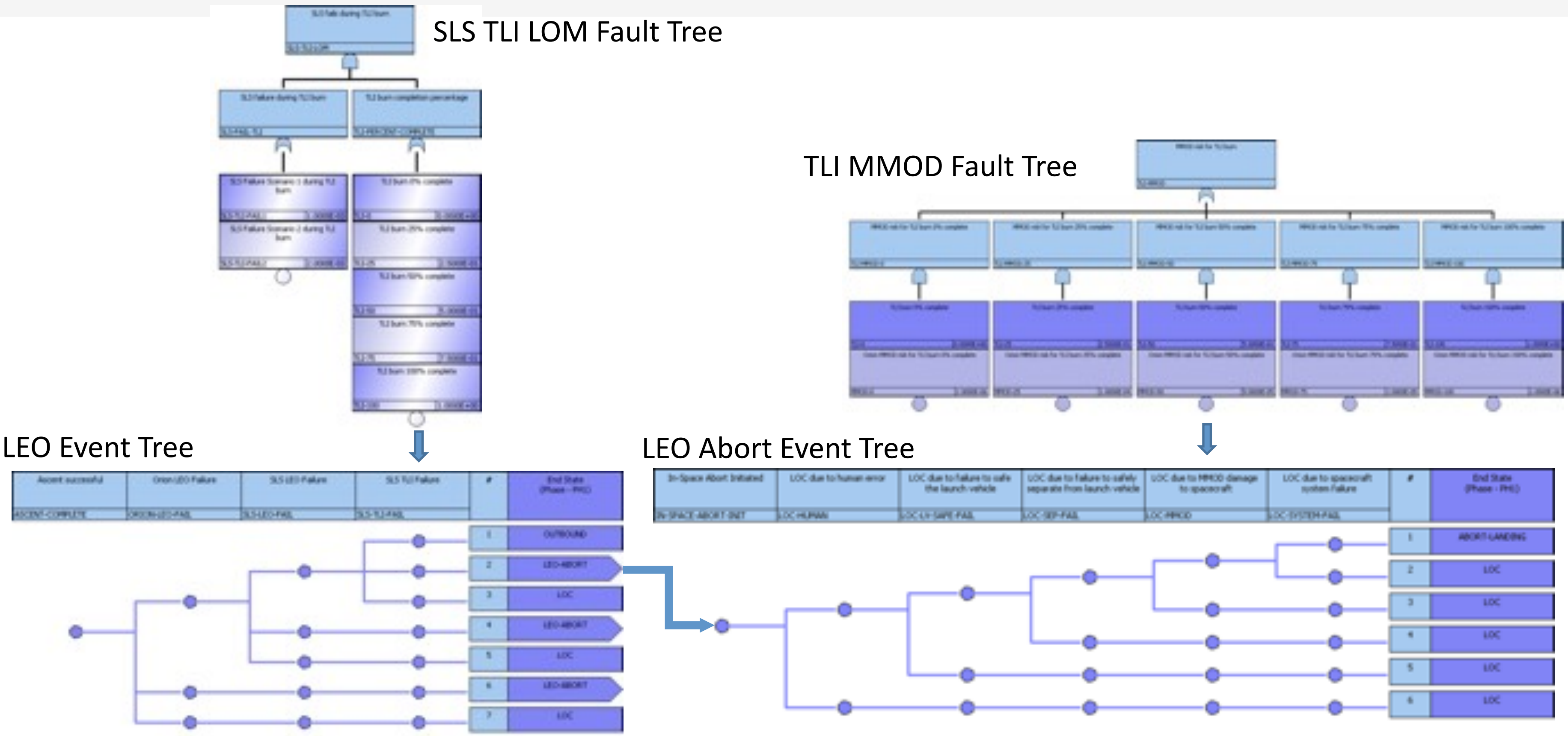
Modeling Dependencies for In-Space Aborts

- 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 the XPRA model as follows:
  - 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.

```
*****
***** 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



Fault Tree Combination and Boolean Reduction

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.

Example cut sets from SLS TLI LOM FT:

SLS-TLI-FAIL1 * TLI-0

SLS-TLI-FAIL1 * TLI-25

Example cut sets from TLI MMOD FT:

MMOD-0 * TLI-0

MMOD-25 * TLI-25

Example cut set from combining the TLI LOM and the TLI MMOD FTs:

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

Through Boolean reduction this cut set is reduced to:

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

Other cut sets that are produced are of the form:

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

This cut set is discarded because it is non-

Abort Landing and Recovery Event Tree Descriptions

- The Abort Landing and Abort Recovery event trees also utilize rules to assign conditional 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 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.

Conclusions and Future Work

- The in-space abort model has added to the capabilities of the XPRA to help the Orion and SLS Programs make risk-informed decisions (e.g., selection of abort trajectories).
- It has shown the benefit of having an in-space abort capability.
- 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.