Dynamic Modeling of Ascent Abort Scenarios for Crewed Launches

Mark Bigler, NASA Johnson Space Center
Roger L. Boyer, NASA Johnson Space Center

For the last 30 years, the United States' human space program has been focused on low Earth orbit exploration and operations with the Space Shuttle and International Space Station programs. After over 40 years, the U.S. is again working to return humans beyond Earth orbit. To do so, NASA is developing a new launch vehicle and spacecraft to provide this capability. The launch vehicle is referred to as the Space Launch System (SLS) and the spacecraft is called Orion. The new launch system is being developed with an abort system that will enable the crew to escape launch failures that would otherwise be catastrophic as well as probabilistic design requirements set for probability of loss of crew (LOC) and loss of mission (LOM). In order to optimize the risk associated with designing this new launch system, as well as verifying the associated requirements, NASA has developed a comprehensive Probabilistic Risk Assessment (PRA) of the integrated ascent phase of the mission that includes the launch vehicle, spacecraft and ground launch facilities.

Given the dynamic nature of rocket launches and the potential for things to go wrong, developing a PRA to assess the risk can be a very challenging effort. Prior to launch and after the crew has boarded the spacecraft, the risk exposure time can be on the order of three hours. During this time, events may initiate from either the spacecraft, the launch vehicle, or the ground systems, thus requiring an emergency egress from the spacecraft to a safe ground location or a pad abort via the spacecraft's launch abort system. Following launch, again either the spacecraft or the launch vehicle can initiate the need for the crew to abort the mission and return home. Obviously, there are thousands of scenarios whose outcome depends on when the abort is initiated during ascent and how the abort is performed. This includes modeling the risk associated with explosions and benign system failures that require aborting a spacecraft under very dynamic conditions, particularly in the lower atmosphere, and returning the crew home safely. This paper will provide an overview of the PRA model that has been developed of this new launch system, including some of the challenges that are associated with this effort.

Key Words: PRA, space launches, human space program, ascent abort, spacecraft, launch vehicles

I. Introduction

With the retirement of the Space Shuttle in 2011, NASA has been developing a new launch vehicle and spacecraft to provide the return of the United States to deep space. Along with a new objective to go beyond Low Earth Orbit for the first time in over 40 years, the new launch system is being developed with an abort system that will enable the crew to escape launch failures that would otherwise be catastrophic. In order to optimize the risk associated with designing this new launch system, NASA has developed a comprehensive PRA of the integrated system, including the launch vehicle, spacecraft and ground launch facilities. Given the dynamic nature of rocket launches and potential for things to go wrong, developing a PRA model to assess the risk is a challenging effort. This includes modeling the risk associated with explosions and aborting a spacecraft under very dynamic conditions, particularly in the lower atmosphere. This paper provides an overview of the PRA model that has been developed of this new launch system, including some of the challenges that are associated with this effort.

II. Description of Mission and Elements[1]

The analysis was based on the High Lunar Orbit (HLO) Design Reference Mission (DRM), which is a 14 day crewed mission planned for the early 2020's as Exploration Mission-2 (EM-2). The scope of the analysis to date has been focused on the ascent portion of the mission, starting at approximately three hours prior to launch when the crew has ingressed the vehicle and ends with successful insertion into a stable orbit. Future updates to the analysis include the in-space and Earth Entry, Descent, Landing (EDL) and Recovery portions of the mission. The ascent abort portions of the model are assessed to splashdown.

The SLS is the heavy lift capability necessary to support a flexible path approach. The SLS provides the mass to orbit and energy levels necessary to place exploration elements (e.g. Orion) into Low Earth Orbit (LEO) for transfer to higher orbits and beyond.

The SLS provides an evolvable configuration to meet the needs of the capability driven framework in an affordable manner. The initial SLS configuration provides a liquid oxygen/liquid hydrogen (LOX/LH2) Core Stage (CS) with two Solid Rocket Boosters (SRBs) to place 70 metric tons (t) into LEO. This SLS configuration also employs the Interim Cryogenic Propulsion Stage (ICPS), a LOX/LH2 based element that provides an initial capability sufficient to perform the early Tactical DRMs, such as the HLO DRM. To support early operational missions, the SLS evolves with a block upgrade approach to a 105-t mass to orbit configuration using the Core Stage with advanced boosters. SLS supports longer term architectural DRMs with a 130-t mass to orbit configuration by adding a propulsion element to the 105-t configuration.

The Orion Multi-Purpose Crew Vehicle (MPCV) is a pressurized, crewed element that transports up to four crew members (evolvable to six) from the Earth's surface to exo-LEO destinations or staging points and brings the crew members safely back to the Earth's surface at the end of a mission. The MPCV provides all services necessary to support the crew members while onboard for shorter duration (1-21 days) missions or until they are transferred to another vehicle for longer duration missions.

The MPCV consists of a Crew Module (CM), a Service Module (SM), Spacecraft Adaptor (SA), and a Launch Abort System (LAS). The CM provides a habitable pressurized volume to support crew members and cargo during all phases of a given mission - from Launch Operations to Earth Entry, Descent, Landing (EDL) and Recovery. The SM provides services to the CM in the form of propulsion, consumables storage, heat rejection and power generation. The LAS provides an abort capability to safely transport the CM away from the launch vehicle stack in the event of an emergency on the launch pad or during ascent. The SM also provides some abort capability for higher altitude aborts. The abort system was a major focus of this analysis.

Ground Systems Development and Operations (GSDO) provides common infrastructure, and services to perform processing, launch, and recovery of flight elements. These capabilities include receiving, ground processing, integration, integrated and interface testing, vehicle servicing, launch operations, recovery, de-integration, refurbishment, disposal, emergency egress/escape, and contingency flight crew rescue/crew module retrieval operations.

Finally, there are several different abort modes that are available to save the crew in the event of a life threatening failure. MPCV Mode 1 abort (i.e., LAS Abort) capability is provided by the Orion LAS and may be performed any time after the LAS is armed on the launch pad until LAS jettison during CS ascent. Prior to LAS arming on the pad, emergency egress using a slide wire system is the only way to try to save the crew. Post-LAS arming and prior to launch, both emergency egress and LAS abort are available to the crew, with the choice depending on the failure. The LAS pulls the CM away rapidly during early parts of ascent in the lower atmosphere.

At higher altitudes, the SM is used to try to save the crew. However, given its lower thrust capability compared to the LAS, it pulls away from the SLS much more slowly and also requires the launch vehicle to terminate its thrust first prior to separation. MPCV Mode 2 aborts (i.e., Untargeted Abort Splashdown (UAS)) are performed using the Orion Crew and Service Module (CSM) and may be performed any time after LAS jettison through completion of the ICPS insertion maneuver into a stable orbit. MPCV Mode 2 does not use the SM thrust. The spacecraft separation mechanism springs provide the initial separation impulse, after which the only active propulsion required from the SM is a short Auxiliary (Aux) thruster burn to provide sufficient clearance of the Orion spacecraft from the SLS.

MPCV Mode 4 abort (i.e., Abort to Orbit (ATO)) capability is provided by the Orion CSM and may be performed once sufficient orbital energy exists such that SM-only propulsion can place Orion in a safe obit while preserving the capability to perform an eventual deorbit burn. MPCV Mode 4 aborts are available until completion of the nominal ICPS insertion maneuver into a stable orbit. For EM-2, the first MPCV Mode 4 capability exists prior to MPCV Mode 2 aborts impacting Africa. Unlike MPCV Mode 2 aborts, MPCV Mode 4 leverages the SM Orbital Maneuvering System (OMS) engine and auxiliary thrusters after separation from SLS to achieve an orbital target.

In all abort cases, the MPCV landing systems (e.g., chutes, etc.) must operate to ensure a successful abort and safe recovery of the crew. Higher altitude aborts also may require use of the Thermal Protection System (TPS) and require a deorbit burn (Mode 4 aborts only).

III. Overview of Model

The Integrated Design Analysis Cycle 2a (IDAC-2a) Cross PRA (XPRA) is a linked event tree – fault tree model. The event trees were constructed using the SAPHIRE[2] tool by the XPRA Team (XPRAT) based on the major mission milestones of the current EM-2 mission of record's pre-launch and ascent phases, along with their associated aborts. A Cross Program PRA Methodology Document[3] was created to guide all participating programs in development of their models for input into the IDAC-2a XPRA model. This methodology document is based on standard PRA practices, including PRA practices used in the nuclear industry.

Fault trees developed by PRA teams from the SLS, GSDO, and Orion MPCV programs were linked in the integrated model. In addition, the XPRAT created fault trees to integrate the abort performance simulation results from the MPCV Flight Performance Group and Human Reliability Analysis (HRA) inputs into the abort phases of the model.

The IDAC-2a XPRA consists of four event trees that are linked to hundreds of fault trees through decision logic and event tree rules as illustrated in Figure 1. The four event trees include major timeline events, or top events, for the pre-launch, nominal ascent, ascent abort, and abort EDL mission phases. Fault trees for Orion, SLS, and GSDO are mapped to the top events. These fault trees represent Orion, SLS, or GSDO system failures that result in a LOC, a LOM, or an abort scenario. In all of the event trees, there are instances where multiple fault trees are mapped to a single top event. For these particular instances, event tree rules assign specific fault trees to the corresponding top event branch based on a particular failure condition that has occurred.

The four end-states that exist in the IDAC-2a XPRA SAPHIRE model are as follows: LOC, LOM, LOMAT and OK. LOC is defined as death of, or permanently debilitating injury to, one or more crew members; LOM is defined as the inability to complete any significant/primary mission objective; LOMAT, which is not shown in the figure, is defined as the abortable failure scenarios initiated by Orion, SLS or GSDO that occur during the Prelaunch and Ascent phases that will ultimately result in either LOC or LOM, and is used in off-line calculations of conditional abort LOC; and OK is defined as the successful completion of all nominal mission phases.

Key inputs to the model are the SLS and Orion conditional ascent abort probabilities. If the abort environment (e.g., debris, blast, fireball) created by an SLS failure exceeds the capability of the Orion, it is captured in SLS fault tree logic that maps directly to LOC in the integrated ascent LOC model. These conditional abort probabilities are calculated separately outside the model based on off-line time-dependent analysis using a

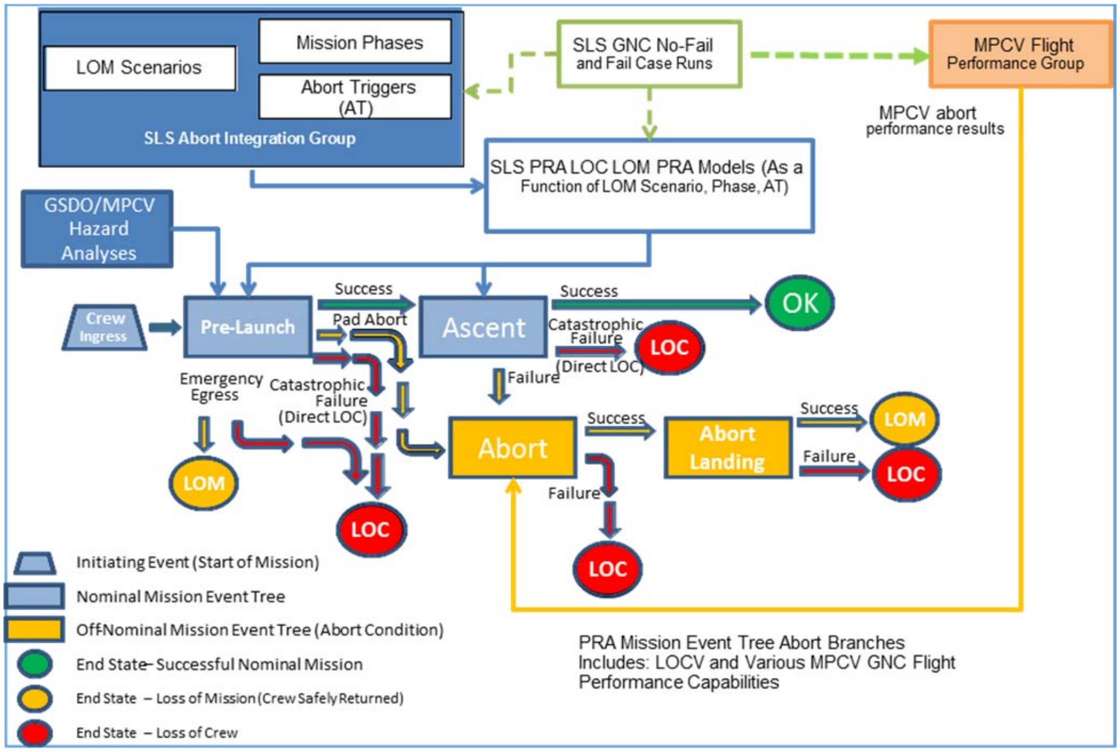
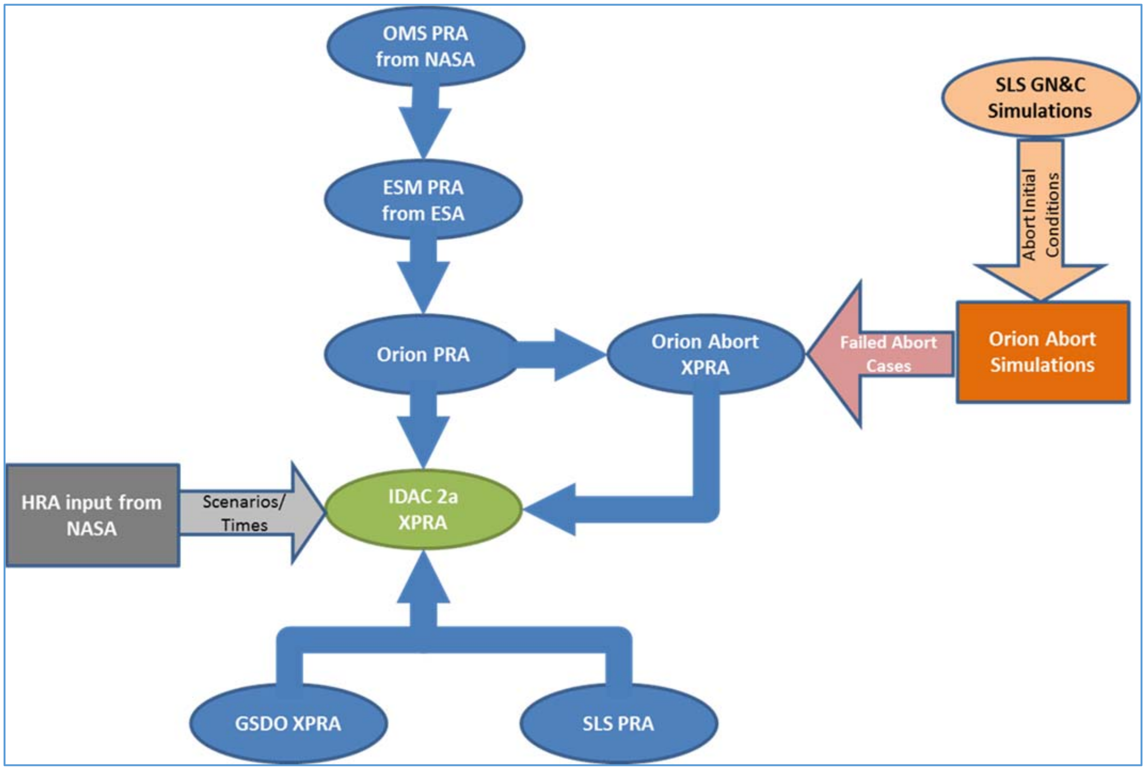

LOM Scenarios
Mission Phases
Abort Triggers (AT)
SLS Abort Integration Group
SLS GNC No-Fail and Fail Case Runs
MPCV Flight Performance Group
MPCV abort performance results
SLS PRA LOC LOM PRA Models (As a Function of LOM Scenario, Phase, AT)
GSDO/MPCV Hazard Analyses
Crew Ingress
Pre-Launch
Success
Pad Abort
Ascent
Success
OK
Catastrophic Failure
LOC
(Direct LOC)
Failure
Emergency Egress
Catastrophic Failure (Direct LOC)
LOM
LOC
Abort
Success
Abort Landing
Success
LOM
Failure
LOC
Failure
LOC
Initiating Event (Start of Mission)
Nominal Mission Event Tree
Off-Nominal Mission Event Tree (Abort Condition)
End State- Successful Nominal Mission
End State – Loss of Mission (Crew Safely Returned)
End State – Loss of Crew
PRA Mission Event Tree Abort Branches Includes: LOCV and Various MPCV GNC Flight Performance Capabilities

Figure 1: XPRA Event Tree Logic

combination of physical models, engineering-level physics models, and empirical data results from historical tests to characterize the prevailing conditions to which the crewed vehicle is exposed. Probabilistic estimates for successful abort attempts are based on the failure environment conditions, the vehicle design thresholds and capabilities, and the amount of warning time provided.

MPCV Guidance, Navigation and Control (GN&C) abort performance factors, provided via the MPCV/SLS Abort Integration Team (MSAIT), and SLS ascent failure scenarios, otherwise known as LOM scenarios which are mapped to Orion LOM Abortable (LOM_A) Initial Conditions (ICs), are combined through logic and rules in the model for successful abort attempts. The Orion GN&C abort performance factors account for the probability that the Orion could fail to successfully fly out the abort trajectory given that it has survived the initial environment generated by a major failure of the SLS, Orion, or ground systems. Fault trees from these programs are combined and linked to the appropriate top event branches in the event trees. These combinations help to determine the most significant integrated ascent abort LOC risks.

Another major input into the model is HRA. In some cases, it was determined that automatic abort triggers were impractical or undesirable, thus manual aborts by the flight crew or ground would be required in these cases. Human error events were identified in these cases and the XPRAT created fault trees to integrate the HRA inputs into the abort phases of the model. This input is illustrated in Figure 2. Given the immaturity in the understanding of the operations of the vehicle at this early stage of the design, a screening methodology was utilized by the XPRAT to quantify any human error events that were identified. The screening analysis assigns conservative values to the human actions based on a basic characterization of the action as a function of the time available for the human to identify the failure, decide what to do, and act on that decision, along with consideration of adverse condition like environment and stress. Human error events identified in this analysis were provided to the crew and operations for review. At this point in the design, all of the assessments are considered preliminary.



For the pre-launch part of the model, emergency egress is also a crew survival option, and is the only option prior to LAS arming as described earlier. For those failures which would lead to an emergency egress, an emergency egress model was included to account for the LOC due to a failed emergency egress.

Event tree rules were used extensively in this model. There are three principle uses of event tree rules in the IDAC-2a XPRA: to substitute one top event for another given a special condition, to assign different fault trees whenever multiple-split branches are used for any particular top event, and to prevent the creation of nonsensical sequences and their cut sets.

IV. Applications of the Model

As stated earlier, this model serves two important purposes. First, it is used to verify whether the integrated system is meeting LOC/LOM requirements. There are several requirements which the model serves to verify. These include ascent LOC and LOM requirements for SLS, along with ascent LOC and conditional abort LOC requirements for MPCV. Perhaps more importantly, this model also provides a capability of showing risks of the integrated system that the individual program models (SLS or Orion) do not capture that can support a risk-informed design process. This information can be used for example to optimize the abort triggers to try to maximize the risk reduction achievable with the abort system. It can also point out areas of uncertainty where our knowledge of the design, operations and/or interfaces is not well understood, and more analysis and/or testing needs to be performed to better understand them. It can also point out areas that are very sensitive to assumptions made regarding the model, for example the abort initial conditions associated with some failure scenarios.

V. Challenges

Several challenges have been encountered in the development of the ascent abort model. First, there are some issues associated with using the PRA in the design phase as opposed to the operational phase. For example, in trying to model human error for ascent aborts, HRA screening analysis was used to populate the human error events in the model because the operations and training are either very immature or non-existent at this point. As a consequence, these events show up as very high risk drivers. This can have the unintended consequence of causing outside stakeholders to be skeptical of the PRA and unwilling to use it.

Trying to integrate very complex and dynamic events, which are not well understood, pose another challenge to this effort. For example, for some failure cases such as thrust vector control failures, very detailed simulations have been performed to understand the initial conditions at abort so that the response of the aborting vehicle can be better characterized. However, for other failure cases such as vehicle explosions, the abort initial conditions are not as well understood or easy to model. Thus, a more subjective approach has been used until these scenarios can be better modeled.

Following a self-integration approach across these NASA programs yields some variations in modeling. For example, some programs attempted to model down to a level of detail not supported by data. This is partially in response to the types of questions being asked of the PRA by the decision makers, for example abort trigger trade studies. In these cases, the analysts use engineering judgment to come up with estimates of the events. In order to deal with this situation, the analysts should consider performing sensitivity analyses on these events and/or look at the importance measures associated with these events. For those events that are high importance and/or the model is very sensitive to the estimates of these events, more analysis and/or testing may be necessary to validate or better characterize the assumptions that went into these estimates. The other alternative is to model at a higher level where data exists.

Given multiple programs with or without a LOC requirement, one must assign an owner for the risk. In many cases, such as pre-launch, the programs are so intimately integrated that it is very difficult, if not impossible, to separate the risks and assign to the various programs. For most failures, the programs have agreed to define the capabilities of the Orion to environment generated by SLS, which are then used to assign risk between the programs, depending on the likelihood of exceeding these defined limits. However, in recent iterations of the model, new situations have been identified that may need to be defined in order to assign the risk to the various programs. For example, for manual aborts where sufficient time for the crew or ground to respond to a failure is not available, the program that initiates the risk becomes the owner. The other situation that could arise from this LOC requirement by program is that it could actually be counterproductive and actually result in a higher overall risk to the integrated system in order to meet the individual program requirements. So far this has not been an issue.

Finally, reviewing a model of this size and complexity is not trivial, particularly when the analysts are faced with challenging schedules and limited resources. In trying to review a model of this size, it is attempted to verify there are no errors in the integrated model by doing both vertical and horizontal checks of the model, including checking for missing sequences, comparison with the program model LOC/LOM results, missing flag events, rules, basic event values, and so on. It is possible that some errors could slip through the cracks. The main objective is to make sure that any errors that do would not significantly impact the results of the model. It is believed that all major modeling errors have been identified and corrected to date.

VI. Conclusion

Given these challenges, it is believed that this model represents a very useful tool to help verify LOC/LOM requirements and to support trade studies to optimize the allocation of resources to obtain the most risk reduction within all other constraints. The model will be expanded in future updates to include additional mission phases, such as in-space and nominal EDL, and challenges identified in the previous section will be addressed to improve the overall quality of the model.

References

1. "Exploration Systems Development Concept of Operations, ESD 10012, Baseline, Release Date: May 18, 2012," 2012.
2. "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 1 Summary Manual, NUREG/CR-6952".
3. "Cross Program Probabilistic Risk Assessment Methodology, ESD 10011, Baseline, Release Date: November 5, 2012," 2012.