ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis
Wilmington, NC, March 13-17, 2011, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2011)

METHODOLOGY FOR DEVELOPING A PROBABILISTIC RISK ASSESSMENT MODEL OF SPACECRAFT RENDEZVOUS AND DOCKINGS

Steven J. Farnham II, Joel Garza, Jr., Theresa M. Castillo
ARES Corporation
Houston, TX
steven.j.farnham@nasa.gov; joel.garza-1@nasa.gov; theresa.m.castillo@nasa.gov

Michael Lutomski
NASA
NASA-JSC
Houston, TX
michael.g.lutomski@nasa.gov

ABSTRACT

In 2007 NASA was preparing to send two new visiting vehicles carrying logistics and propellant to the International Space Station (ISS). These new vehicles were the European Space Agency's (ESA) Automated Transfer Vehicle (ATV), the Jules Verne, and the Japanese Aerospace and Explorations Agency's (JAXA) H-II Transfer Vehicle (HTV). The ISS Program wanted to quantify the increased risk to the ISS from these visiting vehicles. At the time, only the Shuttle, the Soyuz, and the Progress vehicles rendezvoused and docked to the ISS. The increased risk to the ISS was from an increase in vehicle traffic, thereby, increasing the potential catastrophic collision during the rendezvous and the docking or berthing of the spacecraft to the ISS. A universal method of evaluating the risk of rendezvous and docking or berthing was created by the ISS's Risk Team to accommodate the increasing number of rendezvous and docking or berthing operations due to the increasing number of different spacecraft, as well as the future arrival of commercial spacecraft. Before the first docking attempt of ESA's ATV and JAXA's HTV to the ISS, a probabilistic risk model was developed to quantitatively calculate the risk of collision of each spacecraft with the ISS. The 5 rendezvous and docking risk models (Soyuz, Progress, Shuttle, ATV, and HTV) have been used to build and refine the modeling methodology for rendezvous and docking of spacecrafts. This risk modeling methodology will be NASA's basis for evaluating the addition of future ISS visiting spacecrafts' hazards, including SpaceX's Dragon, Orbital Science's Cygnus, and NASA's own Orion spacecraft. This paper will describe the methodology used for developing a visiting vehicle risk model.

Key Words: NASA, Space, PRA, Risk, Vehicle

1 INTRODUCTION

As the International Space Station (ISS) surpasses 12 years in space the major challenges of the ISS are maintaining functionality and how to extend the ISS lifetime to 2020 and possibly beyond. The retirement of the Space Shuttle amplifies these challenges of maintenance and resupply. Previously, the Space Shuttle along with the Russian Soyuz and Progress spacecraft have maintained the ISS with 30 to 40+ years of operational experience. With the development of the International Partners (IPs) Automated Transfer Vehicle (ATV) and H-II Transfer Vehicle (HTV) spacecraft and the retirement of the Space Shuttle, NASA has transferred the inherent risk

of logistics resupply to the IPs. In the near future, SpaceX's Dragon and Orbital Science's Cygnus will be additional spacecrafts visiting the ISS. A methodology has been developed with NASA to build probabilistic risk models for spacecraft rendezvous and docking/berthing to understand the increase in risk due to increased spacecraft traffic to the ISS. This paper outlines the process that is in use at NASA for developing a Probabilistic Risk Assessment (PRA) model of spacecraft interaction with the ISS. This process will set the foundation for all future PRA models of spacecraft interaction between a space station and another visiting spacecraft.

Visiting vehicles create dynamic events with multiple operations occurring both in series and in parallel. This paper will explain how a probabilistic model comprised of fault and event trees is used to model the risk of a collision. The models of the visiting vehicles are based on the reliability of the key system components (or hardware) that make up the vehicle, not the performance of the vehicle as a whole. Ideally a performance-based model or time-based simulation - combined with a probabilistic approach - would be more ideal to predict the path and ultimate risk of collision of a particular vehicle. The technique spelled out below will be the foundation for increasing the fidelity of the models in the future. To help emulate a time-based simulation until those techniques are better developed, the PRA model was split up into four separate mission phases; approach, docking or berthing, attached phase, and undocking or unberthing. These phases will be explained in the following sections.

2 SPACECRAFT PRA METHODOLOGY

2.1 Spacecraft Mission Phases

The first step in modeling a spacecraft's interaction with the ISS is to build an Event Sequence Diagram (ESD) for each spacecraft's operational sequence of events that can ultimately negatively impact the ISS. However using conventionally PRA methods, this first step created a problem with the model endstates when using a spacecraft's total mission time. A spacecraft would have an approximate mission time of 6 months when it is attached to the ISS for 6 months. If a single total mission time of 6 months is used for a spacecraft's entire PRA model, then dynamic operations (like docking) at the beginning of the 6 months, which only effect ISS for a few hours, would have a failure probability equal to a 6 month continuous docking event. The failure probability would be unreasonably conservative because the higher risks of dynamic operations would be over estimated by a longer mission time. The majority of the total 6 month mission time is when the spacecraft is attached to the ISS; during this attached phase the spacecraft is mostly dormant to prevent unnecessary run-time failures. The spacecraft total mission time and overall mission design - in addition to the current modeling software - require the spacecraft's PRA model to be separated by phases to account for the unique operations, systems, component run times, and component demands that are attributed to each phase. Each spacecraft's PRA model can be separated into a Final Approach Phase, a Docking (or Berthing) Phase, an Attached Phase, and an Undocking Phase.

2.1.1 Final Approach Phase

The Final Approach Phase of the PRA model is initiated when a spacecraft receives the final "Go" command to target the ISS and the spacecraft begins the "Final Approach" for docking or berthing. The "Go" command is given after holding orbit at a range of 100 to 200 meters from the ISS, depending on the spacecraft. This command is only given after mission control and/or the spacecraft crew has made the final system checks on the spacecraft. Prior to reaching the 100 or 200 meter hold point, all spacecraft flight paths are required to have "Off-set" targeting. "Off-set" targeting may be implemented differently for each spacecraft, but the basic principle is that the spacecraft's flight path must be targeted away from the ISS. If there is a failure leading to an off-nominal operation of the spacecraft, the trajectory will ensure that the spacecraft's flight path will not impact the ISS.

All failures and off-nominal operations before the "Go" for Final Approach are assumed in the PRA model to not contribute to the likelihood of the vehicles collision with ISS. This assumption is permissible because the ISS PRA team's model endstates of concern are the crew evacuation of the ISS and the loss of crew life on the ISS. A more detailed model of a spacecraft would include all possible model endstates for a spacecraft while in orbit (for example, loss of the spacecraft, loss of mission), but those end states are not currently modeled.

All systems that can affect the outcome of the Final Approach phase are modeled. These systems include the electrical power system (EPS), command and data handling of required hardware (CDH), the communication system, the motion control system (MCS) and propulsion, the thermal control system (TCS), and flight crew or ISS crew interactions with the vehicle. Some system's subsystems are used only during the first few days of orbit, and are not used during the Final Approach, and are therefore not modeled. The flight crew and the ISS crew human errors that can impact the spacecraft's performance are modeled. These errors are errors of both commission and omission, related to flight path monitoring and Abort initiation commanding.

The component mission time and component demands vary for all spacecraft from eight minutes to three and a half hours. A mission time of 5 hours was chosen for each spacecraft's Final Approach phase to baseline comparative analysis between the vehicles, and to account for a varying amount of uncertainty that is attributed to the operational unknowns. The 5 hour mission time also adds conservatism to the surrogate NASA failure rate/demand rate data that is used for each spacecraft's components. This surrogate failure rate and demand rate data will be described in more detail in Section 1.3.

The Final Approach phase assumes that a loss of a spacecraft's system or required subsystem, as defined in Flight Rules, will trigger the spacecraft's Abort sequence, Collision Avoidance Maneuver (CAM), or Retreat. The Soyuz flight crew has the ability to assume manual control of the vehicle in off-nominal operations as well as the ability to initiate an Abort sequence anytime during the Final Approach. The ISS crew can also send a command to the approaching Progress, ATV, or HTV spacecraft to initiate the Abort sequence after a system failure or Flight Rule violation. Failure of any spacecraft's Abort sequence in the PRA model will lead to the endstate of collision with the ISS; this collision is assumed catastrophic for the crew on the ISS. A collision endstate is assumed for this failure scenario because the orbital mechanics cannot be predicted after both a system or partial system failure and an Abort failure, so a worst case is assumed. Additionally, the last known flight path trajectory was directed at the ISS.

After a successful Abort the spacecraft may be able to attempt another docking, but our models currently accounts for only one docking attempt.

A successful end to the Final Approach phase is the initial contact of Probe to docking Cone, or successful entry into the berthing spacecraft's Capture Box.

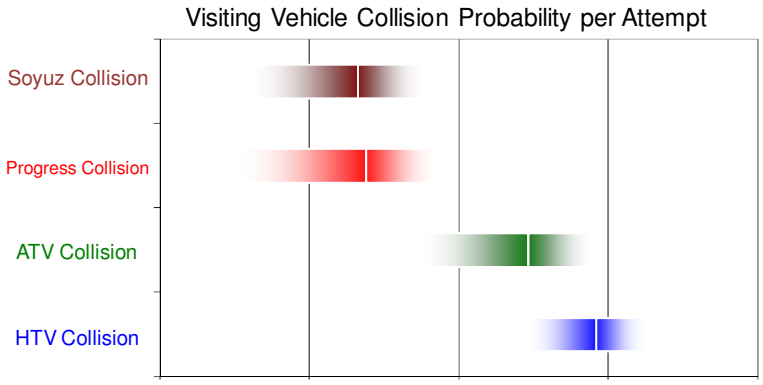

Figure 1. PRA calculated probabilities of collision for the ISS's four current visiting vehicles with relation to their magnitude and uncertainty.

2.1.2 Docking Phase

There are two different attachment methods for visiting vehicles (other than Space Shuttle) to the ISS. The first is docking, which uses a Probe and Cone used by the Soyuz, Progress, and ATV spacecrafts. The second method is called berthing, which requires the Space Station Remote Manipulator System (SSRMS) to grapple the spacecraft and then attach the spacecraft to the ISS through a Common Berthing Mechanism (CBM). Currently only the HTV uses the berthing method. For the duration of this paper, regardless of whether a vehicle attaches to the ISS via docking or berthing, this phase will be referred to globally as the "Docking Phase."

The Docking Phase for docking spacecrafts is comprised of the operation of all docking mechanism systems and components, including the hooks that achieve the structural integrity between the spacecraft and the ISS, and the hatch components. The Cone ports are on the Russian section of the ISS; therefore, all spacecrafts using the docking method must comply with Russian design requirements.

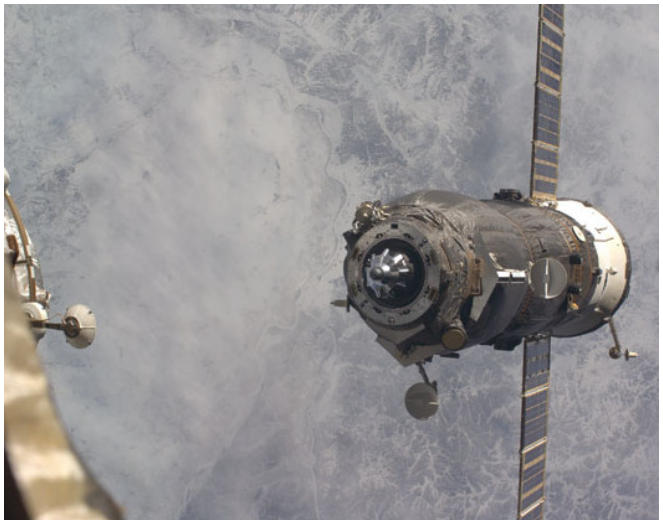

Figure 2. Final Approach of the Russian Progress while docking with the ISS.

There is not a defined mission time for the Docking Phase for docking vehicles; instead, the risk in this phase is strictly dependent on component demand failures. Most components in this phase experience only one demand. If there is a system failure, the model captures the spacecraft's attempt to reverse the docking process and undock from the ISS. If the reversal of the

docking process also fails then the resultant endstate would be a loss of mission (LOM) for the spacecraft and a loss of port access for the ISS. The final event in the Docking phase is the hatch pressure seal checks and the hatches being opened between the visiting spacecraft and the ISS. Failures from the Final Approach phase do not impact the Docking phase for docking spacecraft because the systems used in the Docking phase are different from those used in the Final Approach phase.

Berthing requires more ISS components, such as robotics and integrated systems, and also specifically/notably includes human error due to the use of robotics. For berthing vehicles, the Docking Phase is comprised of the grappling of the vehicle by the SSRMS, robotic movement of the spacecraft, berthing the spacecraft, and finally hatch opening. All of the vehicle's systems must function nominally up until the hold point, at which point, the vehicle is grappled, and all risk becomes associated with the SSRMS, SSRMS operator, and the CBM. Unlike the docking vehicles, failures in the Final Approach all of the vehicle's systems must continue to function because the same systems will later be used for unberthing. The resultant endstates with berthing vehicles are the same as docking vehicles, with an additional Stuck SSRMS endstate. A successful berthing phase has occurred once the hatches are opened between the spacecraft and the ISS; at that time, the Attached Phase is initiated.

2.1.3 Attached Phase

The Attached Phase of a spacecraft's PRA model begins at the moment the hatches are opened, and can continue for up to 6 months. Newer spacecraft, such as Orion, may be designed to stay longer than 6 months. A spacecraft's Attached Phase ends when the vehicle attempts to close the hatch for undocking/ unberthing.

All spacecraft remain mostly dormant while attached to the ISS, so the majority of a spacecraft's components are not modeled during this phase. The chief function modeled out of all the spacecraft while attached is the availability for Progress and ATV to provide reboost and attitude control capability to the ISS, because this is the preferred method for the ISS.

Currently, HTV does not provide any redundant system capability to the ISS. The Soyuz spacecraft's Attached Phase is unique because it provides the emergency evacuation capability for the ISS crew. The Soyuz does not provide any redundant system capability to the ISS, but it must be able to perform a quick power-up and systems check to support an emergency evacuation.

Figure 3. HTV berthed to the underside of Node 2. SSRMS is still attached to the HTV. The use of the robotic arm creates increased risk of collision.

A spacecraft's components that are modeled during the Attached Phase may also account for a previous phase's failures, if it impacts capabilities specifically modeled in the Attached Phase,

such as system redundancies relied on by the ISS. For example, if a redundant MCS component failure occurs during the Final Approach Phase (with a mission time of 5 hours) then that component cannot be relied upon for redundancy during a reboost maneuver during the Attached Phase of 6 months. Any new system or component failures during the Attached Phase must also be incorporated during the spacecraft's Undocking Phase (detailed below).

All visiting vehicle spacecraft contribute to the negative end states of the ISS PRA model while attached to the ISS. The presence of these spacecraft creates increased risk by way of fire ignition and greater exposure to the risk of micro meteoroid or orbital debris penetration of the habitable ISS volume; these scenarios can lead to an ISS evacuation or loss of ISS crew life.

2.1.4 Undocking Phase

The final phase of a spacecraft's influence on the ISS is the Undocking Phase, which begins undocking or unberthing preparations by closing the spacecraft's hatch. This phase only captures the undocking or unberthing of the spacecraft and its orbital flight until it safely escapes the ISS Keep Out Zone; it does not track the spacecraft to successful landing or successful break-up on re-entry of the Earth's atmosphere. The PRA models of the Soyuz, Progress, and ATV spacecraft account for the spacecraft's required undocking orientation relative to ISS to prevent a catastrophic collision endstate. This orientation is determined by assuming that the spacecraft's MCS/propulsion has failed and the ISS has a worst case drift rate toward the undocking spacecraft after the spacecraft has undocked. The ISS orientation provides inertial physics-based justification to exclude MCS, propulsion, and partial undocking mechanism failures from these PRA models as contributors to a collision endstate.

If there is a complete undocking mechanism failure then pyrotechnics may be used as a last resort to undock a spacecraft from the ISS. Pyrotechnics are located on all ISS docking ports as well as each visiting spacecraft. After undocking Progress and ATV at the desired ISS vehicle orientation, orbital mechanics will safely remove these spacecraft from the ISS Keep Out Zone. A successful PRA model endstate is achieved once the spacecraft is removed from the Keep Out Zone.

The Soyuz spacecraft has additional PRA modeling requirements for a successful undocking scenario - the spacecraft must be able to leave the ISS Keep Out Zone with all required systems functioning to ensure human survivability until reentry. MCS and propulsion must function, not to prevent collision, but to ensure that the Soyuz crew can maneuver the spacecraft in orbit until reentry. Additional systems required for Soyuz crew survival until reentry support life support systems: EPS, CDH, and TCS. Atmospheric reentry of the Soyuz is not modeled in either the Soyuz PRA model or the ISS PRA model.

Berthed vehicles have a different separation process from docked vehicles. Berthed spacecrafts, again require a fully functioning CBM, robotics, and vehicle systems to unberth. The process to unberth is the same as berthing in reverse order. The SSRMS attaches to the docked spacecraft, moves it outboard, and releases the spacecraft. Unlike the docking vehicles, berthing spacecrafts cannot rely on orbital mechanics or pyrotechnics and must maneuver itself away from the ISS. A failure of the spacecraft MCS or propulsion can lead to a collision with ISS which would lead to the loss of crew (LOC) endstate for the ISS crew.

The Undocking Phase mission time for each spacecraft is different. Progress and ATV Undocking Phase components modeled are the hatches and the undocking mechanism which are

based on demands; therefore, these spacecrafts do not have a defined mission time. The mission time for Soyuz system components is set to the life of the non-rechargeable battery, which is 5 days. Soyuz's undocking mission time conservatively accounts for any unseen failure that would require the Soyuz spacecraft and crew to remain in orbit for a maximum of 5 days. The Soyuz PRA model also includes the previously mentioned hatches and undocking mechanism, which are based on demand failure rates.

When modeling the Undocking Phase, consideration is given to components that have failed in previous model phases. A continuation of the example from Section 1.1.3, tailored for a Soyuz spacecraft, would indicate that failures from the Final Approach Phase (5 hours of mission time), Docking Phase (a demand of 1), and Attached Phase (mission time and demands depend on spacecraft operations) must be incorporated into the Undocking Phase (120 hours of mission time) to ensure that the impact of all spacecraft failures are accurately being captured in the model.

2.2 Vehicle Expert Review

After a spacecraft's PRA model is complete and has been internally reviewed, the preferred method to achieve model completeness is to engage system and vehicle subject matter experts to review the model ESDs, assumptions, and key contributors for the failure endstates. This review process also ensures accountability and highlights organizational collaboration when presenting PRA model results to NASA management.

2.3 Surrogate Failure Rates

One issue with developing a PRA model of a foreign nation's spacecraft is the lack of part manufacturer failure data. Usually, there is no insight into the component manufacturer nor any data provided about component reliability information. This lack of component reliability information leads to the use of surrogate NASA component failure data for foreign components. Foreign spacecraft components are investigated to the extent that the basic functionality is known and then a similar functioning NASA component is chosen to determine for component reliability. Most of the ISS components have failure rates available. In looking for component failure rates for an international vehicle, data is typically extrapolated from known failure rates. For example, valve latch failure data from the ISS or Shuttle PRA serves as an adequate approximation of latch valve failure data for HTV or ATV.

U.S. commercial spacecraft will use commercial off the shelf (COTS) components that typically have associated failure data provided by the manufacturers. Special care should be taken when using this data, as manufacturer's failure rates may be artificially low or failures may be alternately defined. In the case of lacking part numbers or failure data as mentioned above, the same method of surrogate failure rates can be used to approximate COTS component failure rates.

2.4 Future Vehicles

There are several new vehicles on the horizon for NASA and the ISS Program. These new vehicles will be operated for NASA by commercial providers or private companies, through a new type of contractual mechanism where NASA will purchase up-mass on these vehicles to the

ISS. This is analogous to paying a shipping company to deliver goods to a specific destination. NASA's ISS Program currently has a Commercial Resupply Services (CRS) contract with two companies to bring logistics to the ISS, following Space Shuttle retirement. This is a high risk strategy because both of the providers are developing new vehicles, and in one case use a new launcher.

Figure 4. SpaceX C1 Demonstration Flight including the Falcon launcher and the Dragon spacecraft. December 8th, 2010

The first company is SpaceX - it has successfully completed its first demonstration flight know as C1 on December 8th, 2010. This was a critical milestone for not only SpaceX but also the ISS Program. The ISS Program is counting on these new transportation systems to be successful in order to maintain ISS logistics resupply so that six crew can be maintained in orbit. This is critical for fully utilizing the ISS and ensuring it continues to meet its purpose as an orbiting science laboratory. SpaceX will hopefully continue to succeed in their remaining CRS milestones, which will culminate in the first CRS flight in late 2011 or early 2012, bringing logistics to the ISS.

Orbital Sciences Corporation is the second company under NASA's CRS contract that will be resupplying the ISS. They have yet to test their vehicle in orbit, but they are using an existing launcher. Orbital expects to have their first CRS flight in the first half of 2012.

Like the JAXA HTV, both of these vehicles will be berthed using the SSRMS. The ISS PRA Team will model these operations and quantify the risks of collision, loss of port, and loss of mission in a similar method as was used with HTV.

Figure 5. Orbital Sciences Corporation Cygnus Spacecraft

Looking further ahead, these and other companies hope to eventually deliver crew in addition to logistics to the ISS. NASA is currently defining how they will certify a commercial spacecraft that could transport NASA and IP astronauts. One approach involves the use of quantitative risk management or PRA at its core. NASA is in the process of baselining risk "thresholds" that will be acceptable for crew transportation. NASA is planning on defining a minimum acceptable "threshold," a minimum requirement, and a design goal for a mature crew transportation system. These overall mission numbers therefore would apply to both the launcher and the spacecraft, to cover both ascent and descent.

The use of these quantitative risk thresholds will create the need for a high fidelity quantitative risk model for each of these crew transportation launchers and spacecraft. The models will have to be defendable, traceable, repeatable, and verifiable.

2.5 Docking versus Berthing

Research is currently under way to quantify the risks associated with both docking and berthing visiting vehicles. Docking vehicles directly approach the ISS and nominally have autonomous control throughout the docking process. Their systems must be able to nominally function until the spacecraft is within inches of the ISS. Since the berthing process is different, a berthing vehicle must be able to nominally function until it reaches the Capture Box, 10 m away from ISS. This process includes risks associated with the SSRMS and the two interfaces between the visiting vehicle and the ISS; one to the SSRMS Tip LEE and one to the ISS CBM.

Preliminary results show that berthing may result in a higher risk of LOC than docking. A docking vehicle, given that it functions nominally, has the ability to command a retreat or Abort all the way up until it reaches the ISS. A berthing vehicle reaches the Free Drift stage, and is then fully in the control of the SSRMS operator. Use of the SSRMS, aside from its own inherent hardware malfunction risks, adds human error into the risk equation; the operator must now carefully control the SSRMS and place the vehicle in position for CBM operations. Human errors are currently a major contributing factor to the collision end state.

2.6 Model Verification

The PRA spacecraft models have undergone revisions as knowledge is gained on each new spacecraft, and each new launch increases the level of fidelity that can be added to the models. Phasing of the models has significantly changed the PRA methodology from a single mission run time for all spacecraft components to a more structured approach as described in Section 1.1.

Although spacecraft endstate probabilities are generally difficult to verify (from lack of missions and mission failure data), the PRA models have been successfully verified against the one endstate that has sufficient real life statistics for comparision. The Soyuz and Progress PRA model results have accurately matched the real life statistics for Abort. This is a pioneering effect for spacecraft interactions, and the ISS PRA team is continuing to develop this unique modeling process – verification against Abort statistics is an early indication that the process is sufficient.

3 CONCLUSIONS

The ISS will soon be the only operational manned spaceflight program remaining at NASA. Any collision between a spacecraft and the ISS would be a high visibility event with significant consequences for not only the safety of the ISS crew and vehicle, but also for the ISS program and politically for NASA at large.

The process developed for modeling the risk of spacecraft rendezvous and docking will help quantify and understand the risk of collision for each of the visiting vehicles. This information will assist ISS program managers with understanding the risk for an individual docking/berthing operation, as well as the cumulative risk of many docking/berthing operations over the duration of the program. For example, in the year 2011 alone, there are 18 planned docking and berthing events of visiting vehicles with the ISS. This information will help ISS program managers better determine where to commit resources to effectively decrease risk to the ISS. These PRA models will also help SpaceX and Orbital Science design a safer and more reliable spacecraft, and spacecraft operations for their vehicles. This methodology will also assist in the future development of as-yet unnamed commercial and government developed spacecraft.

4 REFERENCES

Systematic Approach for Caturing Inter-phase Failure Combinations in an Integrated, Multiphase Linked Fault Tree Model of the Space Shuttle, Bigler, M., Stewart, M., PSAM7 Technical Paper, Science Applications International Corporation (SAIC), 5/3/07.