Extravehicular Activity Probabilistic Risk Assessment Overview for Thermal Protection System Repair on the Hubble Space Telescope Servicing Mission

Mark Bigler[a], Michael A. Canga[a], Gary Duncan[b], and Ed Roeschel[a]

[a]National Aeronautics and Space Administration (NASA), Houston, USA

[b]Science Applications International Corporation (SAIC), Houston, USA

EVA PRA Objectives and Scope

The Shuttle Program initiated an Extravehicular Activity (EVA) Probabilistic Risk Assessment (PRA) to assess the risks associated with performing a Shuttle Thermal Protection System (TPS) repair during the Space Transportation System (STS)-125 Hubble repair mission as part of risk trades between TPS repair and crew rescue.

Scope was to assess contingency EVA to perform one of the TPS repairs listed:

- Reinforced Carbon-Carbon (RCC) Crack Repair
- RCC Plug Repair
- Tile Emittance Wash
- Tile Overlay Repair
- Shuttle Tile Ablator Repair

Systems/hazards included in the EVA PRA scope were:

- Extravehicular Mobility Unit (EMU)
- Airlock and Hatches
- Communication System (Comm)
- Remote Manipulator System/Orbiter Boom Sensor System (RMS/OBSS)
- EVA tools/aids (e.g., tether, Portable Foot Restraint (PFR), TPS repair tools, etc.)
- Human interface
- External events/hazards (Micrometeoroid and Orbital Debris (MMOD), sharp edges, etc.)

EVA PRA Overview

The EVA PRA model was developed by a team of PRA analysts <u>and</u> domain experts providing technical inputs.

- PRA analysts were highly skilled analysts with many years of experience in PRA—most were engineers.

- Domain experts included personnel from the following:
  - NASA Johnson Space Center (JSC) Engineering, NASA JSC Safety & Mission Assurance (S&MA), Boeing (Orbiter) and MDA for Orbiter-related systems and hazards (airlock, hatches, Comm, and RMS)
  - EVA S&MA and EVA Project Office for EVA-related systems and hazards
  - Mission Operations Directorate
  - Flight Crew Operations Directorate
  - Astromaterials Research and Exploration Science (ARES) for MMOD

EVA PRA End States

This analysis was developed for two undesirable END STATES— Loss of Extravehicular (EV) Crewmember(s) (LECM) and Loss of EVA Mission Objective (LEMO) as defined below:

- LECM is the immediate death of an EV crewmember.
  LECM does not include potential long-term effects for external hazards such as radiation or decompression sickness.

- LEMO is failure to perform a successful TPS repair. LEMO includes both failure of the EVA to successfully complete the repair and the effectiveness of the repair (i.e., materials).

EVA PRA Phase Definitions

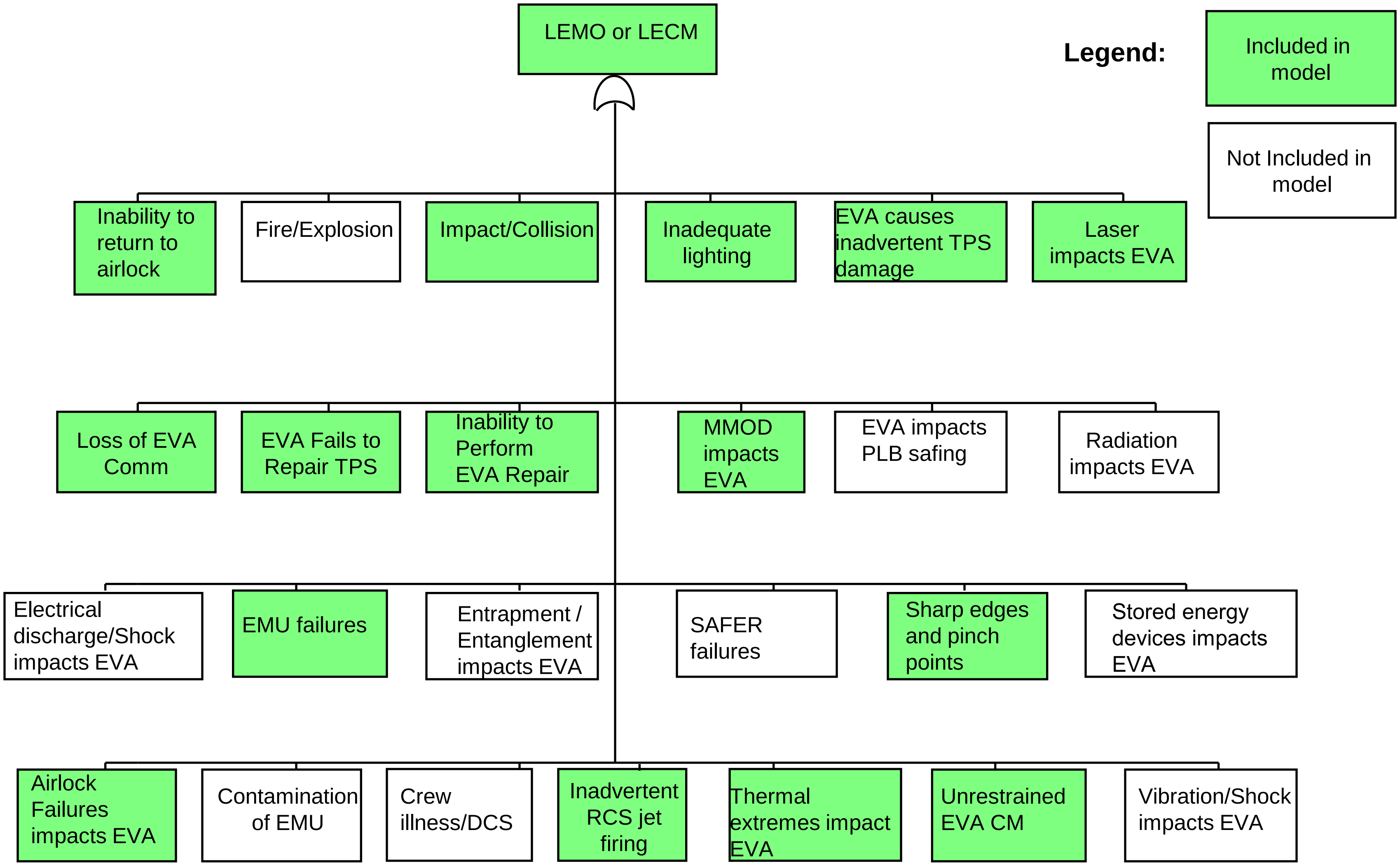
Events trees/fault trees were developed for the following phases to assess the risk of performing a Shuttle TPS repair during the STS-125 Hubble repair mission :

- **EVA preparation** – EMU Day 2 checkout, ingress airlock, close forward hatch and depressurize airlock (40 minute exposure time)
- **Egress setup** – Egress airlock via either aft or upper hatch, tether swap to payload bay, tool setup, tether swap to RMS/OBSS, and ingress the portable foot restraint (30 minute exposure time)
- **Transition to worksite** – Transition to worksite on the RMS/OBSS (1 hour exposure time)
- **TPS repair** – Perform and verify the TPS repair (3.5 hour exposure time)
- **Transition back to payload bay** – Return to payload bay on RMS/OBSS and tether swap to payload bay (1 hour exposure time)
- **Clean up** – Clean up and stow tools (30 minute exposure time)
- **Ingress** – Tether swap to airlock, ingress airlock and close aft or upper hatch, repressurize airlock, and ingress crew cabin via forward hatch (demand only no exposure time)
- **EV Rescue** – Rescue a free floating EV crewmember either pre- or post-repair (pre-repair would result in LEMO).

Master Logic Diagram

- The next step in the PRA development process was to identify the complete set of Initiating Events (IEs) that serve as trigger events in the sequences of events (accident scenarios) leading to the end states.
- An Master Logic Diagram (MLD) was constructed for the EVA PRA to identify the types of initiating events to be considered for inclusion in the model.
- The IEs were identified from various sources such as hazard report reviews, previous analyses, and discussions with system experts.
- The IEs for the EVA PRA were reviewed with EVA domain experts for completeness and correctness, along with applicability to the scope and objectives for this analysis.
- The high-level MLD for the EVA PRA is shown on the next page.

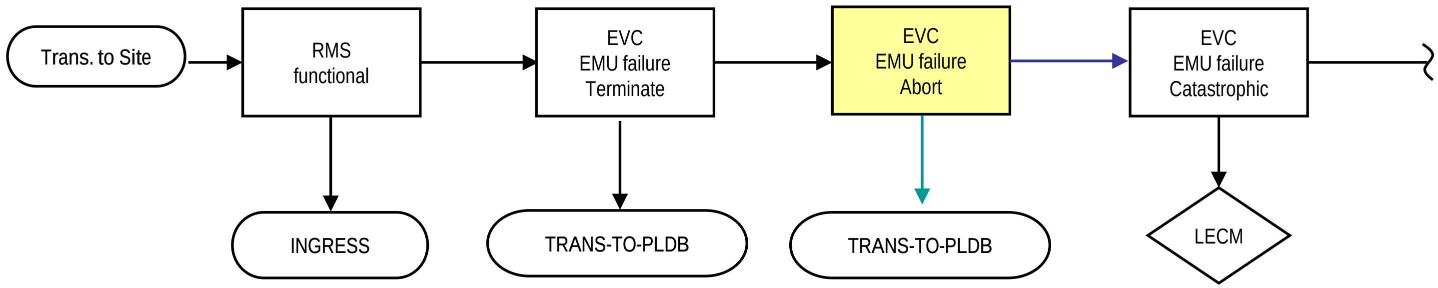
Master Logic Diagram (cont.)



Event Sequence Diagrams

- The scenarios that may ensue from a given IE were initially developed in Event Sequence Diagrams (ESD).
  - The ESD can be mapped into an Event Tree (ET), which relates more directly to a practical quantification of accident scenarios using standard PRA tools.
  - The ESD representation has a significant advantage over the ET for enhancing communication between risk engineers, designers, and crews.
  - A good deal of information (e.g., system-level mission success criteria at each pivotal event) can also be displayed on the ESD, making it a very compact representation of a large amount of modeling information.
- The ESDs for the EVA PRA were reviewed with EVA domain experts for completeness and correctness.
- ESDs were developed for each of the major phases in the EVA as previously described.
- An example ESD for the Transfer-to-Worksite phase of the EVA PRA is shown on the next page.

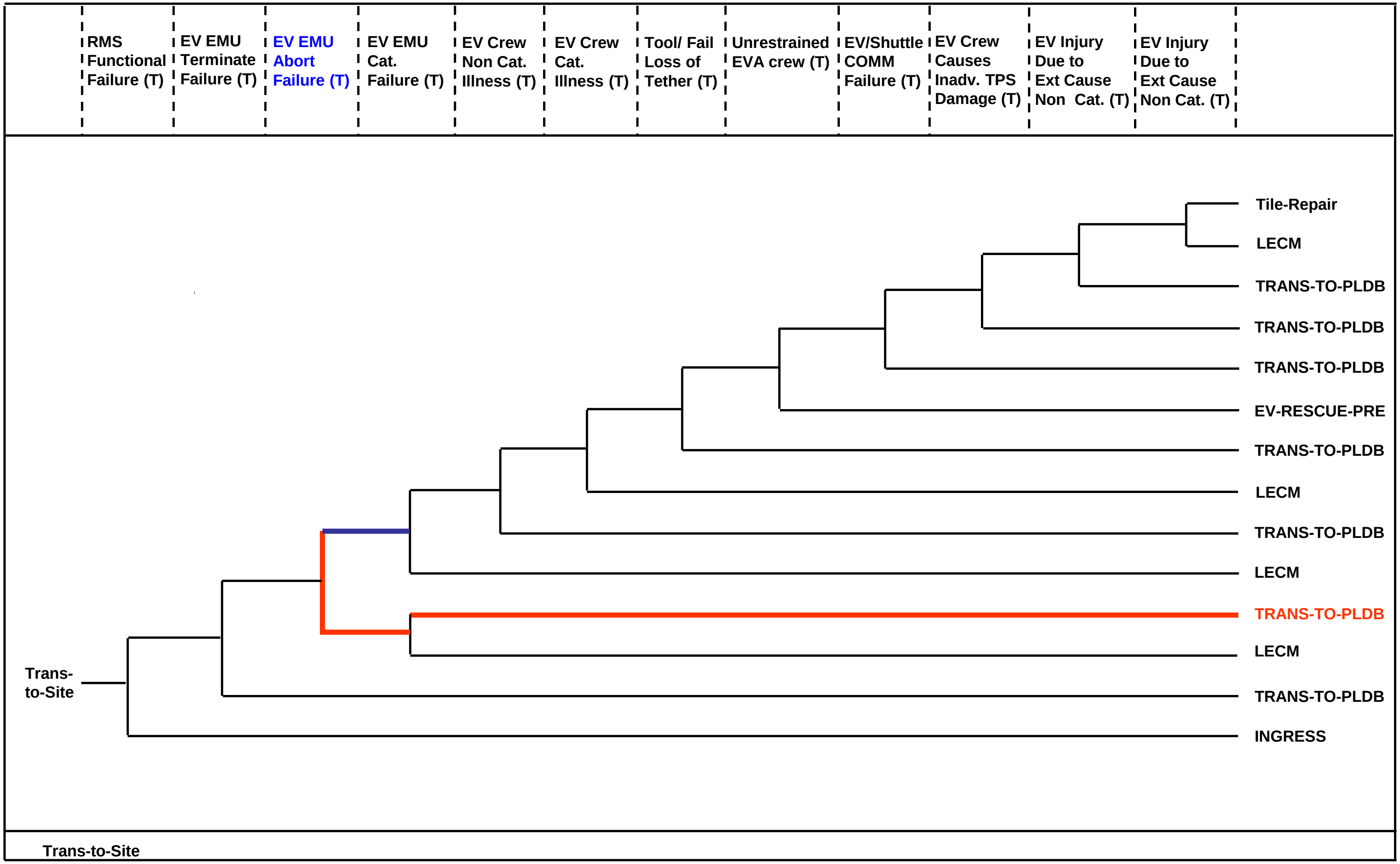
Event Sequence Diagrams (cont.)



Event Trees

- From the ESDs corresponding ETs were developed.
  - An ET distills the pivotal event scenario definitions from the ESD and presents this information in a tree structure that is used to help classify scenarios according to their consequences.
  - The ET headings are the IE, the pivotal events, and the end state. The “tree” structure below these headings shows the possible scenarios ensuing from the IE in terms of the occurrence or non-occurrence of the pivotal events.
  - Each distinct path through the ET is a distinct scenario.
- In the EVA PRA, the initiating event for the overall ET was the occurrence of TPS damage, requiring either an EVA repair or crew rescue. The IEs identified in the previously discussed steps were included in the fault trees developed to support the pivotal events in the ETs, as described in the following pages.
- An example ET from the EVA PRA, which corresponds to the ESD example on the previous page, is shown on the next page (by convention, the “down” branch is considered to be “failure”).

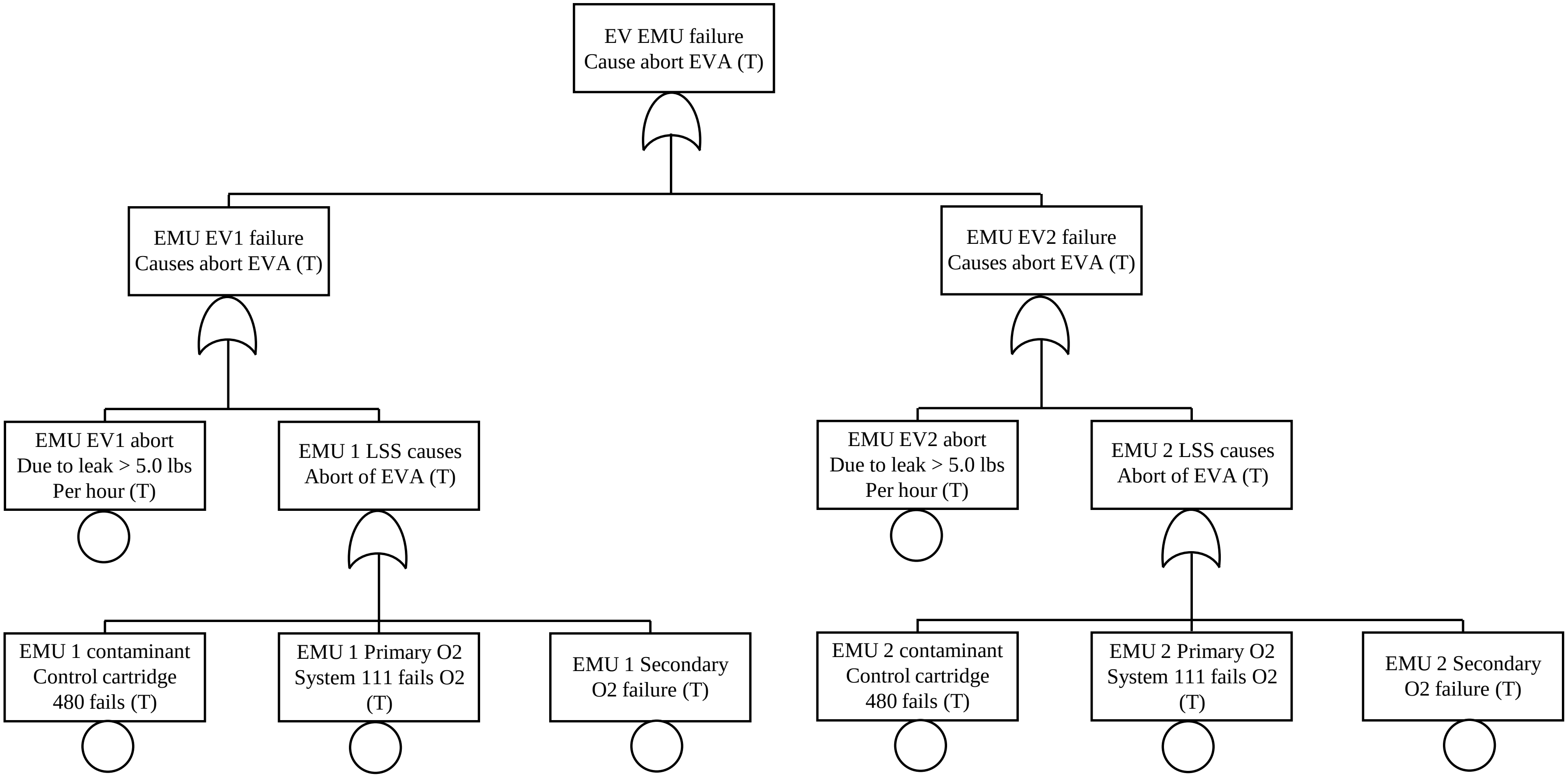
Event Trees (cont.)



Fault Trees

- Top events from the ETs—corresponding to the pivotal events—were developed into Fault Trees (FTs).
  - FTs depict a set of logical relationships between more complex (more aggregated) events, such as system-level failures, and more basic (less aggregated) events, such as component-level failures.
  - FT modeling is not only applicable to modeling hardware failures, but also to other complex event types, including descriptions of the circumstances surrounding phenomenological events and crew actions.
- Domain experts (engineering and operations) reviewed the EVA PRA FT models and associated assumptions for completeness and correctness.
- FT models were developed to a level of detail that data exists to support quantification. Modeling must be conducted in such a way that dependencies between the pivotal events are properly captured.
- An example FT corresponding to one of the pivotal events in the previous ET example is shown on the next page.

Fault Trees (cont.)



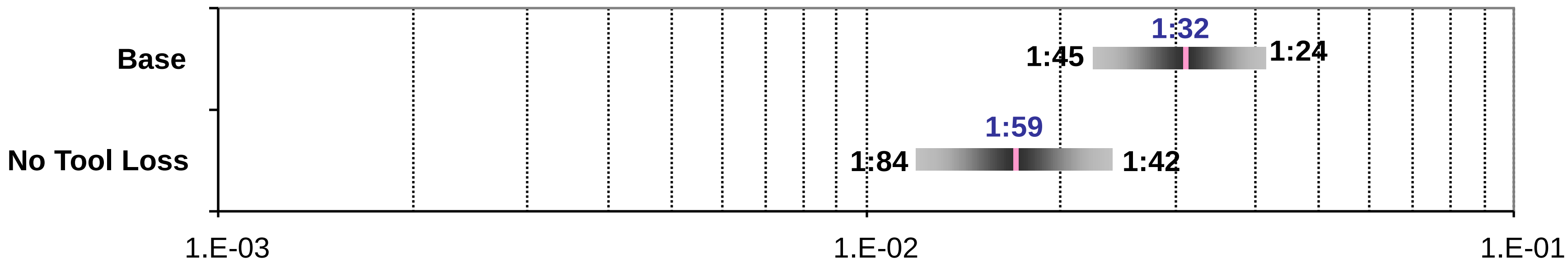
Data Development

- **Functional** – A functional failure event is generally defined as failure of a component type, such as a valve or pump, to perform its intended function.
  - Functional failures are specified by a component type (e.g., motor pump) and by a failure mode for the component type (e.g., fails to start).
  - Functional failures typically fall into two categories, time-based and demand-based.
  - Functional data was Bayesian updated whenever Shuttle- or EVA-specific data was available.
- **Phenomenological** – Phenomenological events include non-functional events that are not solely based on equipment performance, but on complex interactions between systems and their environment or other external factors or events (i.e., sharp edges, leaks, MMOD and other similar situations).
- **Human** – Three types of human errors are generally included in fault trees: pre-initiating event, initiating event (or human-induced initiators), and post-initiating event interactions.
- **Common Cause** – Common Cause Failures (CCFs) are multiple failures of similar components within a system that occur within a specified period of time due to a shared cause.

Model Quantification

- The fault trees and associated data were linked to the event trees, and the event trees linked together using the Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) PRA tool to generate the EVA PRA model results (cut sets) for each end state of interest.
- The cut sets were combined into higher level logical groupings called "super tables" for external review by the domain experts for relative risk rankings of systems and hazards.
- Results of these reviews were fed back into the EVA PRA model and the model iterated until agreement was obtained on the overall results and relative risk rankings.
- Uncertainty associated with the data was also included in the EVA PRA model quantification to obtain overall uncertainty associated with the end states of interest.
- The overall results and relative risk rankings for the LEMO and LECM end states are shown on the following pages.

Overall Results – LEMO



	5th	Median	Mean	95th
LEMO (Base)	2.24E-02	3.04E-02	**3.09E-02**	4.09E-02
	1:45	1:33	**1:32**	1:24
LEMO (No Tool Loss)	1.19E-02	1.62E-02	**1.68E-02**	2.37E-02
	1:84	1:62	**1:59**	1:42

Base case included all EVA-related systems and hazards, and excluded repair material failures and human error associated with the repair installation.

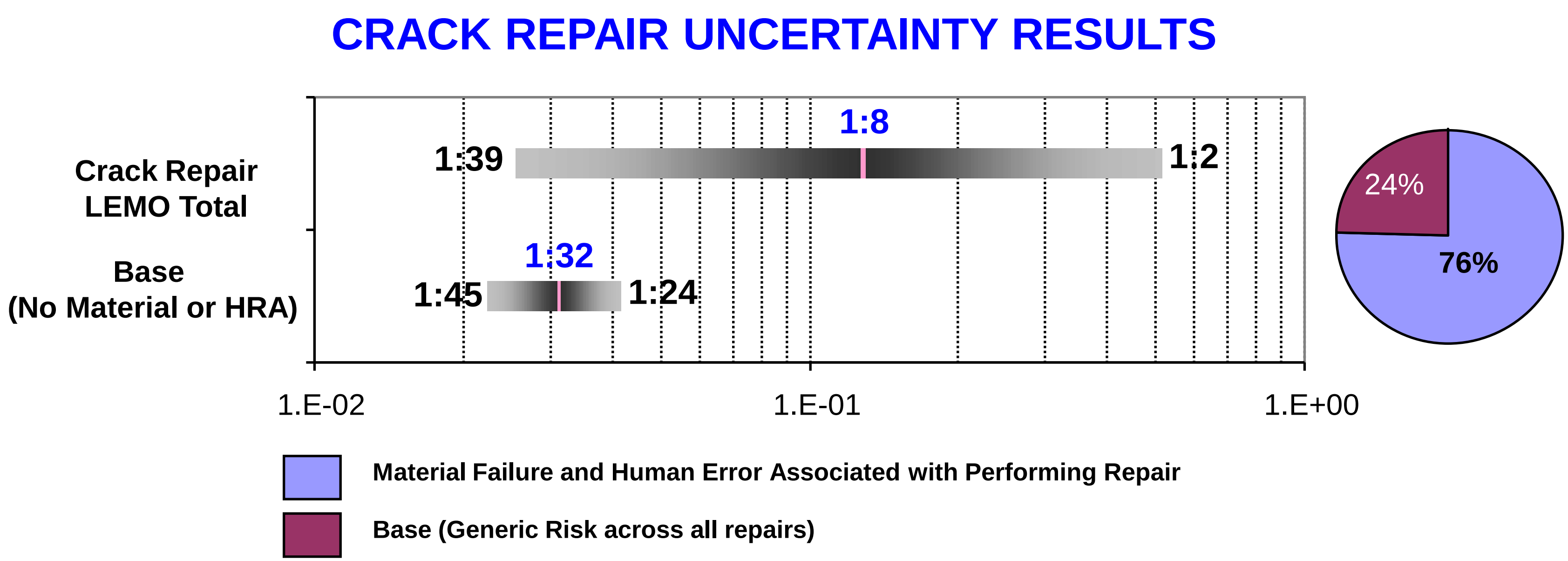
The table on the following page provides a risk ranking of the LEMO contributors.

Overall Results – LEMO (continued)

Rank	Probability (1:n)	%age of Total	Cumulative Total	Failure Scenario Description
1	1.4E-02 (1:70)	45.8	45.8	Loss of EVA Repair Mission due to Loss of Critical Tool
2	6.2E-03 (1:160)	19.8	65.6	Loss of EVA Repair Mission due to EMU Initiated Suit Leaks Which Lead to EVA Termination
3*	2.0E-03 (1:500)	6.5	72.1	Loss of EVA Repair Mission due to Crew Operation of the Shuttle Remote Manipulator System (RMS) Causes Additional Damage due to Collision and/or Fails to Support Repair Effort
4*	1.3E-03 (1:770)	4.1	76.2	Loss of EVA Repair Mission due to Inadequate Lighting
5	1.1E-03 (1:940)	3.4	79.6	Loss of EVA Repair Mission due to EMU Feedwater Circuit Failure
6	9.8E-04 (1:1,000)	3.1	82.8	Loss of EVA Repair Mission due to EMU Electrical Failures
7*	7.7E-04 (1:1,300)	2.5	85.2	Loss of EVA Repair Mission due to Sharp Edges
8	6.3E-04 (1:1,600)	2.0	87.3	Loss of EVA Repair Mission due to Airlock Functional Failures
9*	6.3E-04 (1:1,600)	2.0	89.3	Loss of EVA Repair Mission due to RMS Failures
10	5.5E-04 (1:1,800)	1.8	91.1	Loss of EVA Repair Mission due to EMU Initiated Suit Leaks Which Lead to an EVA Abort

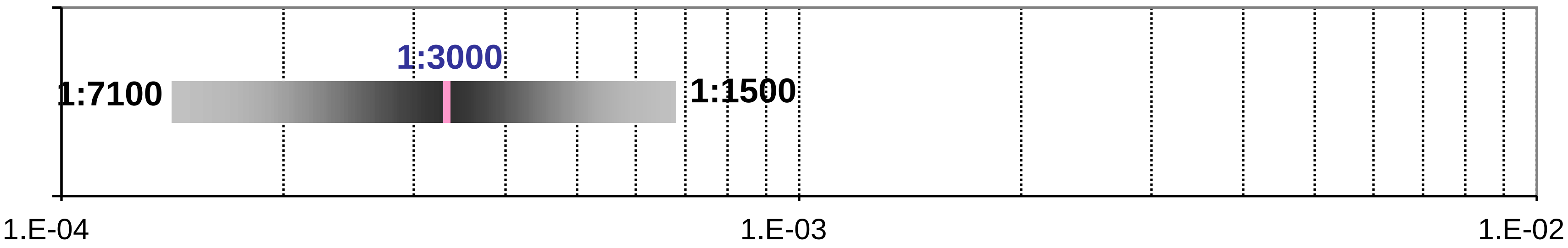
*** Risk drivers that could be updated near real-time during mission**

Overall Results – LEMO (continued)



The LEMO end state was processed for each of the five repair scenarios. The RCC Crack Repair results are presented in the figure above. The figure shows the probability of failure for the RCC Crack Repair and the probability of failure for a generic repair scenario without the repair included.

Overall Results – LECM



	5^{th}	Median	Mean	95th
LECM	1.41E-04	2.78E-04	**3.29E-04**	6.72E-04
	1:7,100	1:3,600	**1:3,000**	1:1,500

The table on the following page provides a risk ranking of the LECM contributors.

Overall Results – LECM (continued)

Rank	Probability (1:n)	%age of Total	Cumulative Total	Failure Scenario Description
1*	1.6E-04 (1:6,300)	48.8	48.8	Loss of EVA Crewmember due to Catastrophic MMOD Penetration
2	1.1E-04 (1:8,700)	35.0	83.8	Loss of EVA Crewmember due to Catastrophic EMU Initiated Suit Leaks
3	1.7E-05 (1:60,000)	5.1	88.9	Loss of EVA Crewmember due to Hatch Valve Failure to Repress
4*	1.6E-05 (1:62,000)	5.0	93.8	Loss of EVA Crewmember due to Inadvertent Release of OBSS
5*	1.5E-05 (1:67,000)	4.6	98.4	Loss of EVA Crewmember due to Sharp Edges
6	1.7E-06 (1:600,000)	0.5	98.9	Loss of EVA Crewmember due to Airlock Repress Failure
7	1.5E-06 (1:690,000)	0.4	99.3	Loss of EVA Crewmember due to Hatch Repress Failure
8*	1.4E-06 (1:730,000)	0.4	99.8	Loss of EVA Crewmember due to MMOD Impact to SSP Airlock
9	7.1E-07 (1:1,400,000)	0.2	100.0	Loss of EVA Crewmember due to Trapped Crewmember in Hatch

*** Risk drivers that could be updated near real-time during mission**

Conclusions

- The EVA PRA provided the first end-to-end integrated PRA for performing a standalone TPS repair.
- The EVA PRA was available to provide a means for risk trades during the May 2009 Hubble Space Telescope (HST) Servicing Mission in the event of suspected critical TPS damage.
- The HST Servicing Mission was successfully completed on May 24, 2009, with no critical TPS damage.
- The EVA PRA laid the foundation upon which future EVA quantitative risk assessments could be based.