

Michael A Canga
*NASA Johnson Space Center,
Mail Code MX, 2101 NASA Parkway
Houston, TX USA 77058
michael.a.canga@nasa.gov*

Use of Probabilistic Risk Analyses within the Space Shuttle Program

Trilateral Safety and Mission Assurance Conference 2008

INTRODUCTION

Within complex programs, Probabilistic Risk Analysis (PRA) results are often considered during decision-making processes.

- What is the Space Shuttle Program's (SSP) experience?
- What can this tell us about better communicating the results of PRA?

RISK MANAGEMENT AND THE RELATIONSHIP TO THE SSP ORGANIZATION

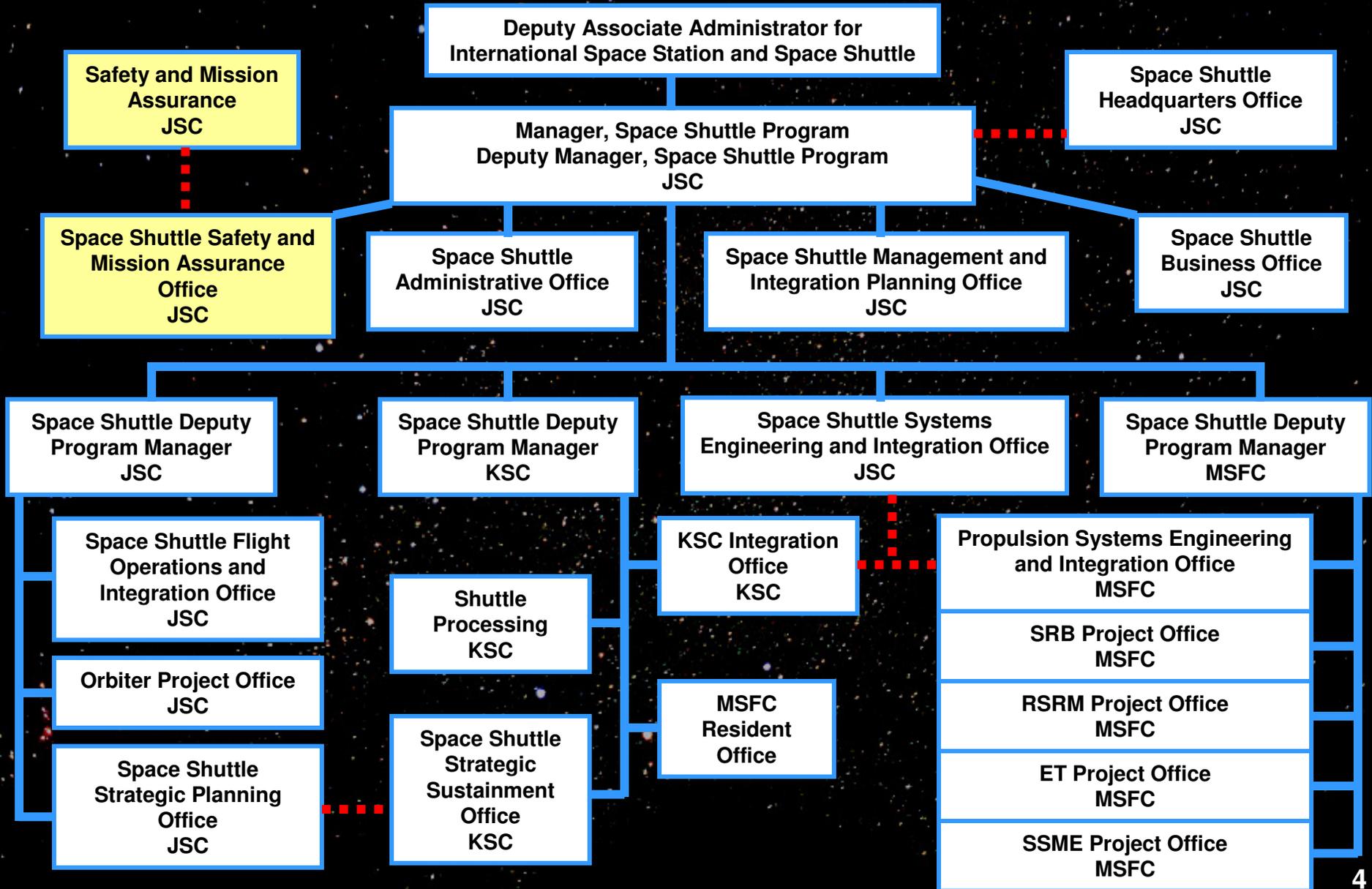
The SSP is charged with flying the Space Shuttle safely through the remainder of the manifest.

- Program must manage competing priorities**
- Program organization is delegated through Deputy Program Managers and Offices**
- Safety and Mission Assurance (S&MA) Office is one of many inputs contributing to SSP decisions**

SSP S&MA Office manages Space Shuttle safety and S&MA implementation and oversees all activities in support of SSP.

- Responsibilities including Risk Assessment and Risk Management**
- SSP S&MA Office uses matrix support from Center S&MA offices**
- SSP S&MA Office (through the efforts of the JSC Analysis Division) is responsible for developing and maintaining the Shuttle PRA (SPRA) including unique assessments in support of SSP objectives**

SSP FUNCTIONAL ORGANIZATION



SHUTTLE PRA

SSP initiated the SPRA in March 2000, the first iteration was presented to the SSP in 2003, and we are currently developing iteration 3.0.

The SPRA includes hazards which can result in loss of crew or vehicle from T- 0 through wheel stop. The SPRA generally assesses hazards resulting from:

- Equipment Failures**
- Environmental Events**
- Structural Failures**
- Human Errors**

SHUTTLE PRA *(continued)*

SPRA generally follows the best practices outlined in *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*.

- PRA assessment included representatives from Program organizations present**
- External Peer Review for methodology**
- Results have been presented to SSP at all levels**

In addition to the SPRA, the JSC Analysis Division has the capability to perform ad-hoc analysis of specific issues.

USES OF PRA WITHIN THE SSP

The SPRA provides the SSP with a good starting point for mission/issue-specific analysis.

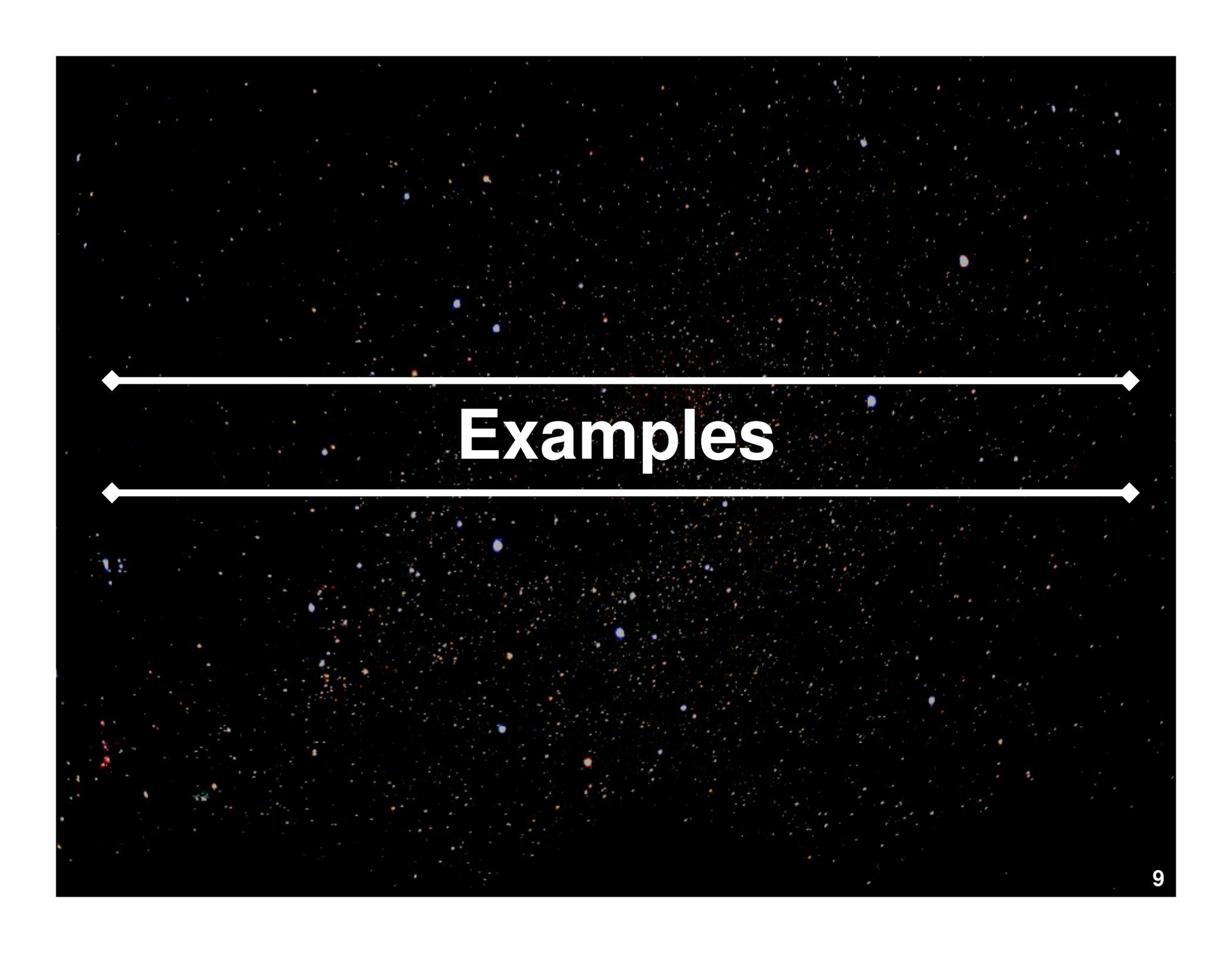
Areas where PRA is used to support SSP include:

- Mission Pre-briefs: mission-specific risk assessments for the Mission Management Team (MMT)
- Risk Trades: analysis of decision alternatives to support SSP decision processes
- Ad-hoc: risk analysis which supports specific issues or problems currently of interest to the SSP
- Other: support of risks identified in the Shuttle Risk Management System, identification of risk contributors

CONSIDERATIONS

Analyses results are reported as one input (among many) during a decision process.

- **How can we assist the decision process?**
- **What can we do to ensure our message is heard?**
- **What do we need to do to assure that the message is accurate?**



Examples

OPERATIONAL USE OF PRA - MMT

The MMT is the Program decision-making body responsible for making programmatic trades and decisions associated with launch countdown and in-flight activities.

- MMT Chair will make risk trades that result in decisions to operate outside of the established Launch Commit Criteria, Operations and Maintenance Requirements and Specifications, and Flight Rules**
- Operationally, the MMT holds a mission pre-brief approximately 2 weeks prior to the mission and convenes daily from L-2 to review mission data**
- The SSP S&MA Office provides an in-line safety oversight of MMT activities and will specifically address all MMT activities concerning issues and/or anomalies having safety ramifications**

OPERATIONAL USE OF PRA – MMT *(continued)*

SSP S&MA Office provides a mission pre-brief package consisting of mission-specific analysis for requested issues:

- Purpose of the briefing is to provide MMT with “situational awareness” of issues of interest to the MMT based on experience or expectations
- Purpose is to brief results (minimize methodology discussions)
 - Analysis method has been established and vetted, inputs vary by mission
 - Analysis (and assumptions) have been coordinated with technical owners

MMT Pre-brief Needs



- **MMT time is valuable**
 - **Be brief**
 - **Product should be familiar**
 - **Communicate important points quickly**
- **Important points:**
 - **Results with risk contributors**
 - **Uncertainty**
 - **Assumptions**

MMT Pre-brief Sample

STS-120 LOSS OF CREW RESCUE (Based on Simulation Model Developed from Historical Events)

Probability Loss of Crew Rescue

Loss of Both Crews	1:XX	Entry LOCV ~ 1:--
		Ascent LOCV ~ 1:---
ISS Inability to Sustain CSCS Leads to Loss of Original Shuttle Crew (73 Days of Consumables)		Ascent Abort ~ 1:---
		ISS EVAC / LOCV ~ 1:556
		Pad Abort ~ 1:--
		Launch Delay ~ 1:--

Mean Loss of Crew Rescue

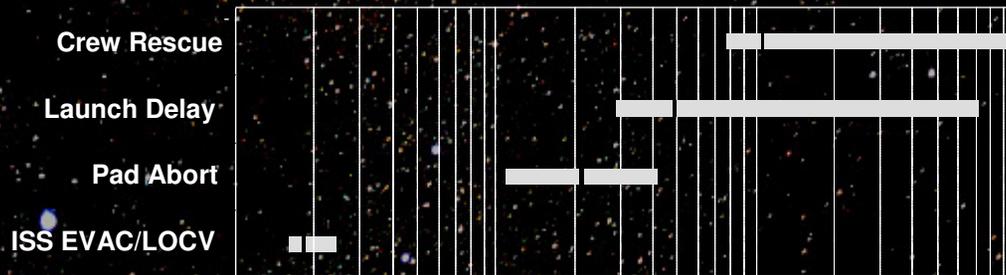
Key Finding

Launch delay risk decreases as the number of days remaining in the OPF flow decreases and as the CSCS duration increases

- This is the reason for difference between STS-118 (1:3) which had 30 days remaining in the OPF and 68 days of CSCS and STS-120.

Uncertainty

Note: Bar length represents generic crew rescue uncertainty (uniform distribution) and black marks are STS-120 estimates.



Probability Loss of Crew Rescue

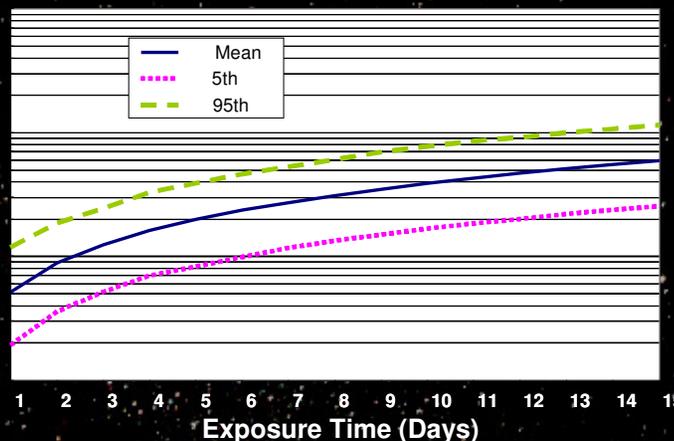
Major Model Assumptions

- Based on STS-120 CSCS capability, 73 days CSCS and 10 days remaining in OPF
- There are launch opportunities every day
- No unprecedented waivers to launch criteria or LCC violations assumed
- Launch delay does not include the potential for extraordinary effort in processing the rescue mission
- ET on dock and subsequent ET processing, SRB stacking, ET mate & closeouts completed in time to support orbiter mate
- Ascent, entry, and abort values based on historical events. Orbit risk assumed negligible as compared to other crew rescue risks.
- ISS EVAC/LOCV includes: MMOD, fire scenarios, USOS hardware failures, ECLS failures
- ISS EVAC/LOCV does not include: failure of exercise equipment, medical emergencies, running out of consumables (which is captured in CSCS duration)

MMT Pre-brief Sample

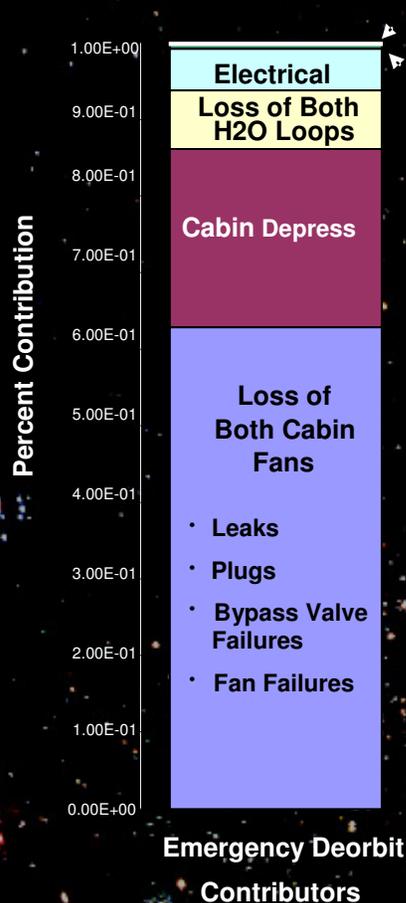
EMERGENCY DEORBIT RISK

Uncertainty



Mean Emergency Deorbit Risk By Number of Days Exposed

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Mean	INCREASING RISK: →														



Major Model Assumptions

- Shuttle flight rules were evaluated that would require immediate entry
- The following were explicitly modeled:
 - Loss of cabin pressure, loss of 2 cabin fans, loss of 2 Freon loops, loss of 2 H2O loops, loss of PP02 control
 - Loss of both A/G voice and CMD, OMS/RCS prop leaks, as well as loss of all cryo tanks was considered to be insignificant compared to other contributors
 - Fire in AV bay or cabin was not considered
 - Impending loss of all APU/HYD was not considered because it is quiescent during the time frame of concern and failure while quiescent is considered to be insignificant compared to other contributors
- Model does not include the ability to recover via IFM (e.g. filter cleaning)
- The model conservatively includes failures that would lead to LOCV (i.e. an inability to successfully perform the emergency deorbit)
- Shuttle PRA Iteration 2.1 data was not used

RISK TRADE – HST REPAIR BACKGROUND

STS-125 is scheduled to perform the final Shuttle Hubble Space Telescope (HST) servicing mission in August 2008.

- Only post-Columbia mission where International Space Station safe-haven is not available**
- If crew rescue is required, a second vehicle will be launched (STS-400)**
- Original mission concept was to have second vehicle on second pad available for launch**

Due to competing priorities, the question was asked whether it would be possible to execute the HST mission from a single pad.

- Manifest and Constellation Program impacts**
- Risk**
- Funding**

RISK TRADE – HST NEEDS AND APPROACH

The Program needs for this trade were to understand:

- What is the difference in risk accepted with each scenario?
- What are the risk contributors?

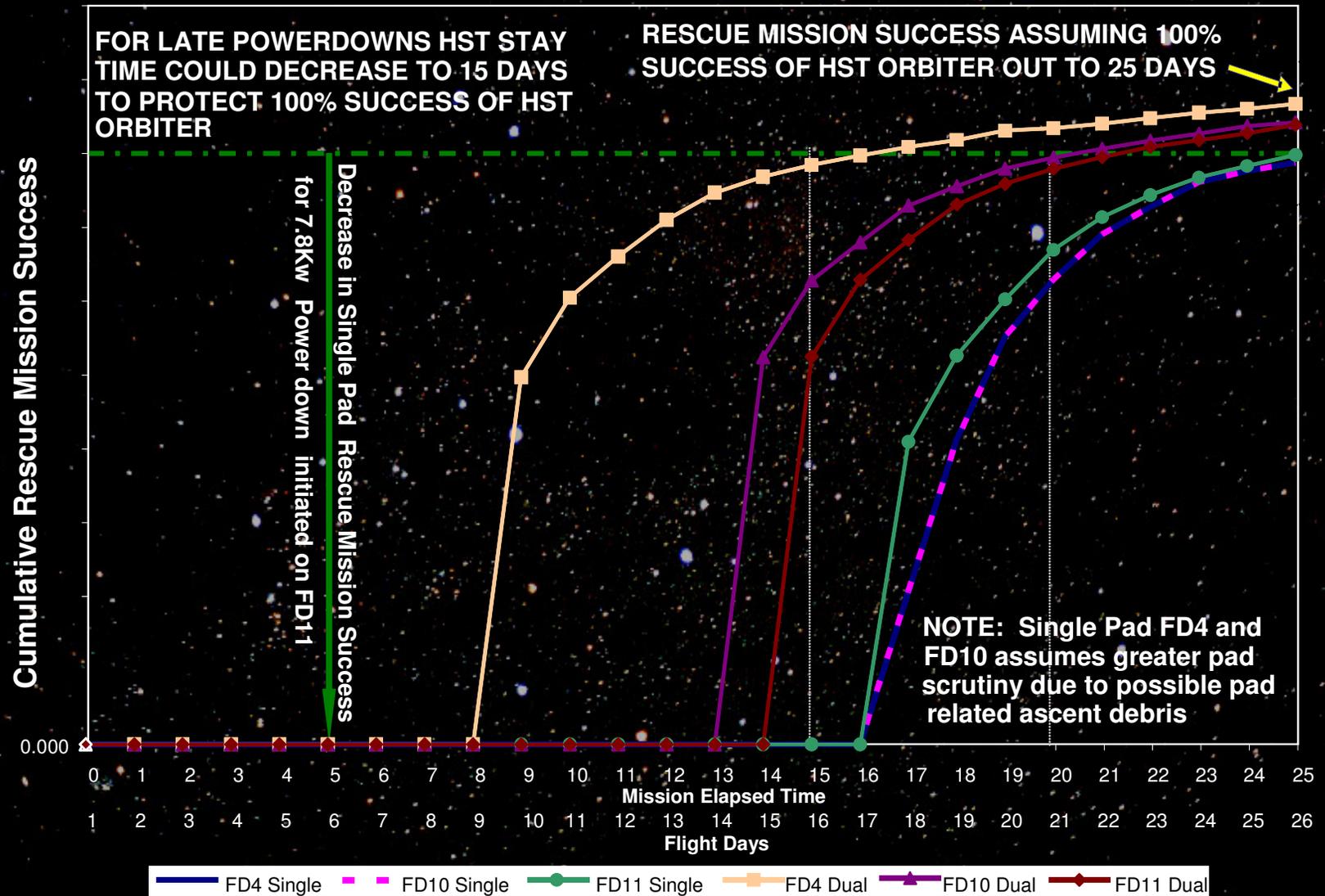
Analysis approach:

- Simulation based on Program experience to estimate probability of launch on a given date
- Use of existing SPRA to assess:
 - Probability of second launch call-up
 - Probability of loss of crew
- A major risk driver, the success of HST orbiter for required mission extension, was not modeled due to time constraints.

Results were incorporated as part of a larger decision package.

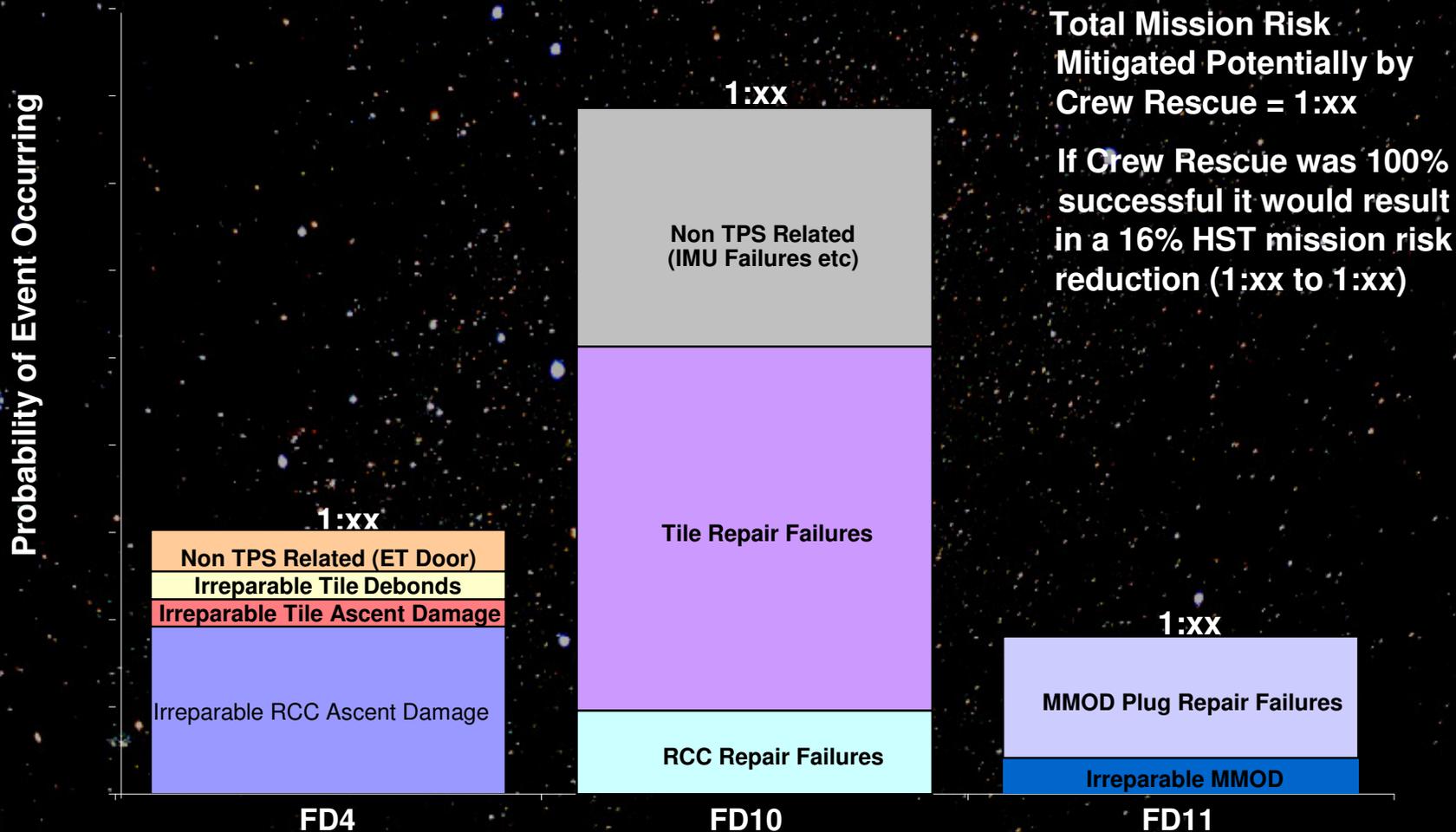
HST RISK TRADE – SAMPLE

CUMULATIVE RESCUE MISSION SUCCESS BY HST MISSION STAY TIME



HST RISK TRADE – SAMPLE

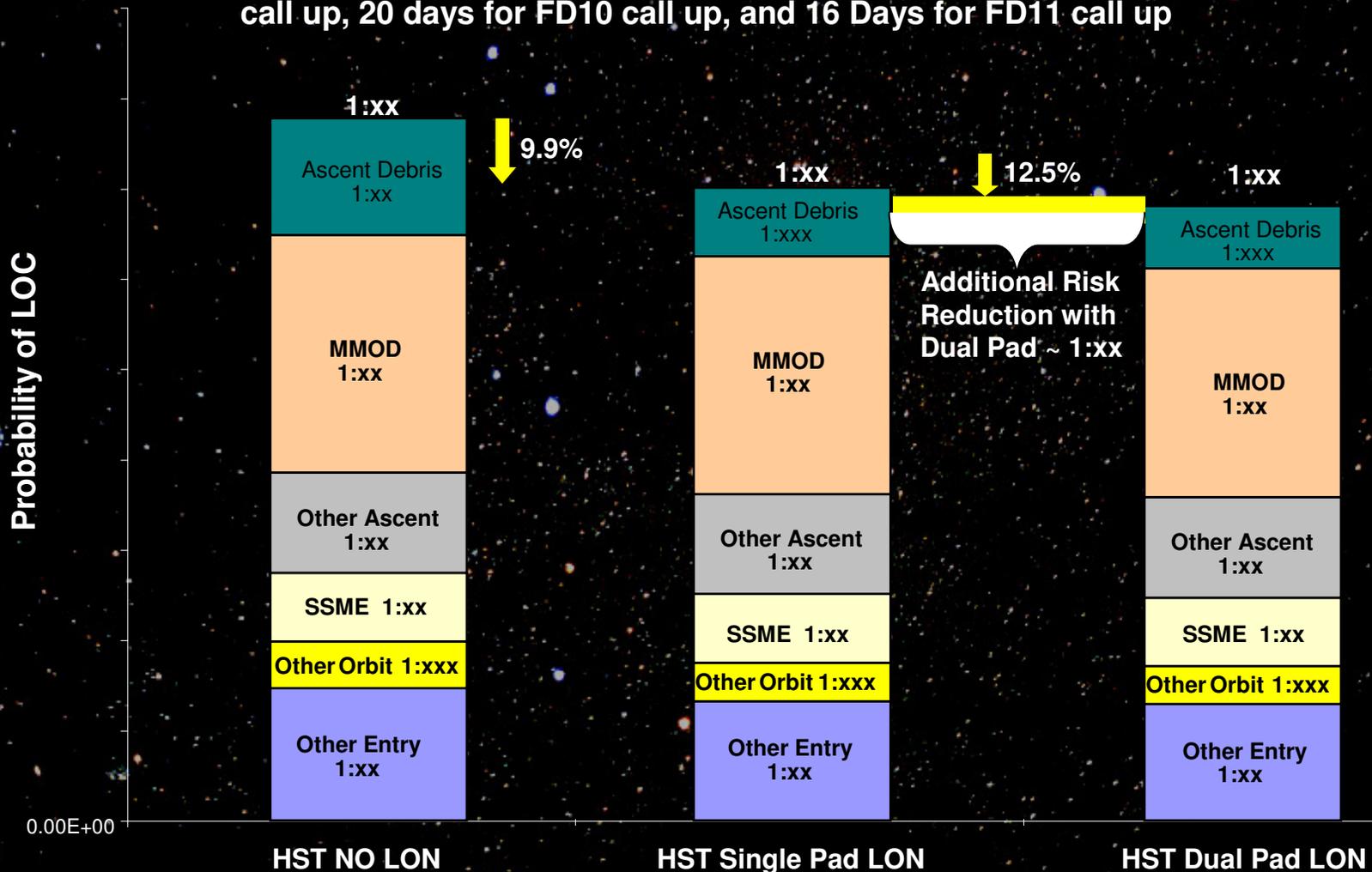
PROBABILITY OF NEEDING CREW RESCUE BY DECISION FLIGHT DAY



HST RISK TRADE – SAMPLE

HST MISSION RISK COMPARISONS

Assumes 100% success of HST Orbiter out to 25 days for FD4 call up, 20 days for FD10 call up, and 16 Days for FD11 call up



STS-122 LH2 LOW LEVEL CUT-OFF SENSOR

STS-122 launch on December 6, 2007, was postponed due to multiple failures within the LH2 Low Level Cutoff (LLCO) System. Subsequent launch attempts were also scrubbed. STS-122 successfully launched on February 10, 2008, after system modifications were performed.

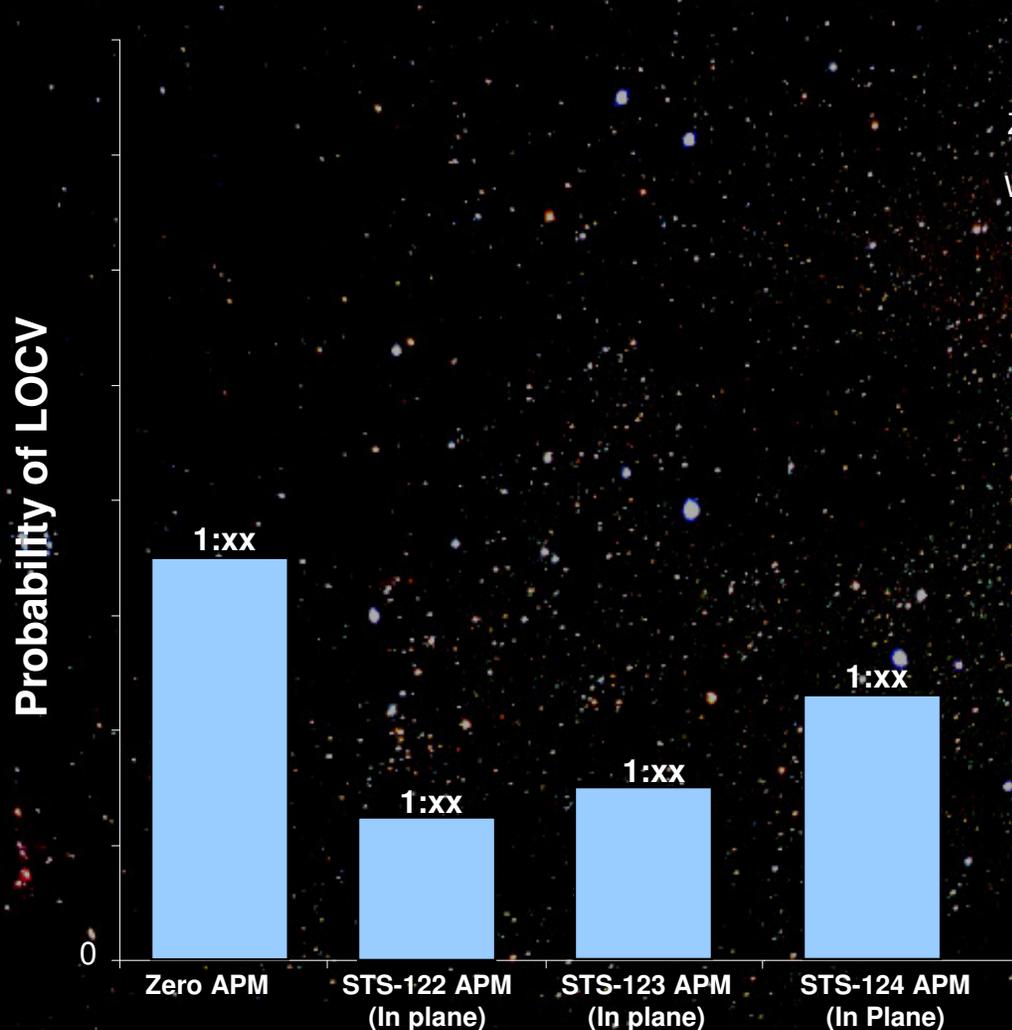
SSP S&MA was asked to review the PRA to determine the likelihood of having a LLCO event on a per-mission basis with enough granularity to see the impact of potential improvements.

The potential contributors were identified through review of the IMPS-03 Hazard Report, historical events, and team discussions.

- System dispersions (variability of input parameters, flight conditions, etc.)
- Anomalous events such as Space Shuttle main engine shifts, hydraulic lockups, etc.

STS-122 LH2 LOW LEVEL CUT-OFF SENSOR

UPDATED LH2 ENGINE CUT-OFF PRA BASED ON STS-114 AND SUBS)



Uncertainty

Note: black mark is STS-123 estimates



Major Model Assumptions

- Probability of LOCV = Probability of needing ECO sensors * conditional probability of 3 or more ECO failures
 - Probability of needing ECO sensors is based upon LLCO PRA estimates presented on previous page combined with Engine out (details provided in backup)
 - Conditional probability of 3 or more eco failures is based on history (# of 2 or more failures/ total # of failures * # of 3 or more failures / total # of 2 or more failures)
- STS-122 failures have not been discounted
- Estimates assume first ECO failure has occurred (i.e. 3 of 4)
- STS-122 abort boundaries assumed for engine out estimates (details provided in backup). Zero APM abort boundaries assumed for zero APM and STS-124 APM and STS-122 APM abort boundaries assumed for STS-123 APM
- Results shown are based ECO sensor history since return to flight (RTF). A higher failure rate of eco sensors has been seen since RTF.

THINGS WE HAVE LEARNED

PRA capability must be accepted by Program

- PRA methodology must be vetted
- PRA models have been reviewed by Program
- Personnel are visible and active within the Program community

As important as good PRA capability is the ability to efficiently communicate the results

- Understand the needs of the forum
 - Need to provide salient information efficiently
 - One size format does not fit all
- Provide all of the necessary information
 - Results
 - Assumptions
 - Uncertainty