# USE OF PROBABILISTIC RISK ASSESSMENT (PRA) IN THE SHUTTLE DECISION MAKING PROCESS

**Roger L. Boyer**
Analysis Branch Chief

**Teri L. Hamlin**
Shuttle PRA Lead

NASA Johnson Space Center
Safety & Mission Assurance

Presented at
PM Challenge
February 9 - 10, 2011
Long Beach, CA

# INTRODUCTION

Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and disciplined approach to identifying and analyzing risk in complex systems and/or processes that seeks answers to three basic questions:

- What kinds of events or **scenarios** can occur (i.e., what can go wrong)?
- What are the **likelihoods** and associated uncertainties of the events or scenarios?
- What **consequences** could result from these events or scenarios (e.g., Loss of Crew and Loss of Mission)?

# BACKGROUND

- The Space Shuttle Program (SSP) initiated the development of a Shuttle Probabilistic Risk Assessment (SPRA) in March 2001. Prior to that there were a number of PRA estimates for the Shuttle, but none were sponsored by the SSP.
  - Chart on next page summarizes the Shuttle PRA evolution.
- The “consequence” or metric of concern selected for the SPRA is Loss of Crew and/or Vehicle (LOCV).
- The risk contributors include hardware failures, external events, crew errors, software failures, and phenomenological events.

SPACE SHUTTLE PROGRAM
Space Shuttle Safety and Mission Assurance Office
NASA Johnson Space Center, Houston, Texas

# SHUTTLE PRA EVOLUTION

- The advent of established NASA requirements, standards, and tools - as well as the development of a strong Shuttle program PRA team have resulted in significant recent progress
- Iteration 3.2 is the most comprehensive and used Shuttle PRA to date

**Examples of SPRA uses:** SLEP Risk Trades (2003) · HST Manifest Decision (2006/2007) · STS-128 Flight Rationale (2008) · STS-131 Flight Rationale (2010)

**Mean Probability of LOCV**

| Mean Probability of LOCV | Description | Model |
|---|---|---|
| 1:70 | 1987 Proof of concept study for applying PRA to Space Shuttle. Scope was limited to APUs for Orbiter and SRB | |
| 1:55 | 1988 First somewhat integrated PRA conducted on the Space Shuttle. Done in support of Galileo Mission. (Ascent Only). | Galileo 1988 |
| 1:73 | 1993 Update of the Galileo study results to reflect then current test and operational base of the shuttle. (Ascent Only) | Phase 1 1993 |
| 1:131 | 1995 First major integrated (multi phase) shuttle PRA. Done with input from prime contractors. | Shuttle PRA 1995 |
| 1:234 | 1998 Unpublished analysis using QRAS. No integration of elements. Limited to three Orbiter systems and the Propulsion elements | Shuttle PRA 1998 |
| 1:78 | 2003 Integrated PRA with all elements, 18 Orbiter Systems, MMOD and human actions included. Presented to Peer review Team. | SPRAT PRA Iteration 1.5 2003 |
| 1:61 | 2004/2005 Integrated PRA with all elements, 18 Orbiter Systems, MMOD and human actions included. Peer reviewed. | *SPRAT PRA Iteration 2.0 2004/2005* |
| 1:67 | 2005 Integrated PRA with all elements, 18 Orbiter Systems, MMOD and human actions included. Peer reviewed. Updated Pre-valve modeling | *SPRAT PRA Iteration 2.1 2005* |
| 1:77 | 2006/2007 Updated SPRA iteration 2.1 with Inspection with Repair and Crew Rescue. Updated MMOD and Ascent Debris Modeling | *SPRAT PRA Iteration 2.2 2006/2007* |
| 1:81 | 2008 Updated SPRA iteration 2.2 with Abort modeling, Rendezvous and Docking. Updated Functional Data, MMOD and Ascent Debris | *SPRAT PRA Iteration 3.0 2008* |
| 1:85 | 2009 Updated SPRA iteration 3.0 with corrected APU Hydrazine Leak Probabilities | *SPRAT PRA Iteration 3.1 2009* |
| 1:89 | 2010 Updated SPRA iteration 3.1 with updated MMOD, Ascent Debris, Orbiter Flight Software, Incorporated Orbiter Review Summit Comments | *SPRAT PRA Iteration 3.2 2010* |

# BACKGROUND

- The purpose of the SPRA is to provide a useful risk management tool for the SSP to identify strengths and possible weaknesses in the Shuttle design and operation.
  - SPRA was initially developed to support upgrade decisions, but has evolved into a tool that supports Flight Readiness Reviews (FRR) and near real-time flight decisions.

# LEVELS OF ASSESSMENT

- Full Scope SPRA
  - Establishes baseline risk associated with the overall mission by mission phase, as well as by vehicle elements and subsystems
  - Documented end states, assumptions, approach, and risk drivers
- Focused PRA
  - Answers specific question that doesn't require full model, but benefits from it
- Insights
  - Knowing relative risk contributors provides input for decisions without comprehensive PRA

# KEY INFORMATION FOR MANAGEMENT

- Clear presentation of analysis
  - if the audience doesn't understand the analysis, the information will not be used
  - Difficult because many different ways people process information
- Applicable assumptions and limitations
  - PRA is only as good as the assumptions that go into the analysis, thus important to share for managers to understand the basis of the results
  - Limitations should be understood, so that the results are not misused
- Estimates of uncertainty
  - state of knowledge about the system being modeled (e.g. the real capability of the system to successfully respond to an event)
  - randomness of the probabilistic parameters (e.g. the uncertainty in estimating a failure probability of an event)

# EXAMPLES

# Shuttle Service Life Extension Program (SLEP)

SPACE SHUTTLE PROGRAM
Space Shuttle SR&QA Office
NASA Johnson Space Center, Houston, Texas

## Comparison of Upgrades

Presenter
Date 01/20/2004 Page 1

| | Current Estimated Shuttle Risk (1) | Current Estimated Risk Contribution | Proposed Upgrade Estimated Risk Contribution | Overall Shuttle Risk Estimate With Proposed Upgrade | Percent Change from Current Estimate |
|---|---|---|---|---|---|
| AHMS | 1.28E-02 | 1.14E-03 | 6.94E-04 | 1.24E-02 | -3.5 |
| AHPS | 1.28E-02 | 1.22E-03 | 4.50E-06 | 1.16E-02 | -9.5 |
| SSME CWN (2) | 1.28E-02 | 1.20E-04 | 4.78E-05 | 1.27E-02 | -0.6 |
| Helium APU | 1.28E-02 | 2.34E-04 | 9.05E-05 | 1.27E-2 | -1.1 |

(1) Estimate of Loss of Crew / Vehicle risk based on version 1.5 of shuttle PRA
(2) Estimates based on values used for Rocketdyne baseline analysis

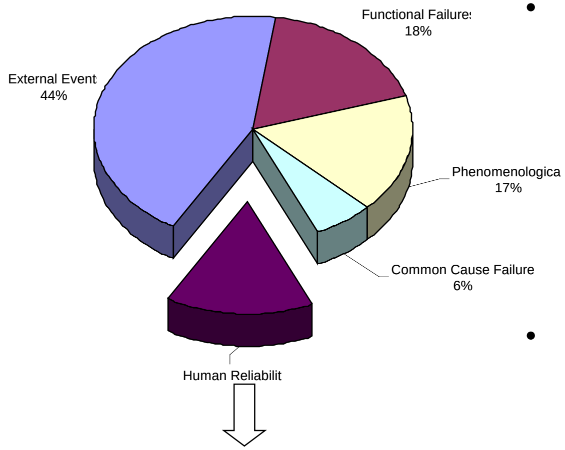
✓ **Assessed the risk of each proposed upgrade <u>and</u> compared relative changes in risk**

# Shuttle Service Life Extension Program (SLEP)

SPACE SHUTTLE PROGRAM
Space Shuttle SR&QA Office
NASA Johnson Space Center, Houston, Texas

| Autonomous Shuttle Risk Evaluation | Presenter | |
|---|---|---|
| | Date 1/26/04 | Page 1 |

### Orbiter Risk Estimates



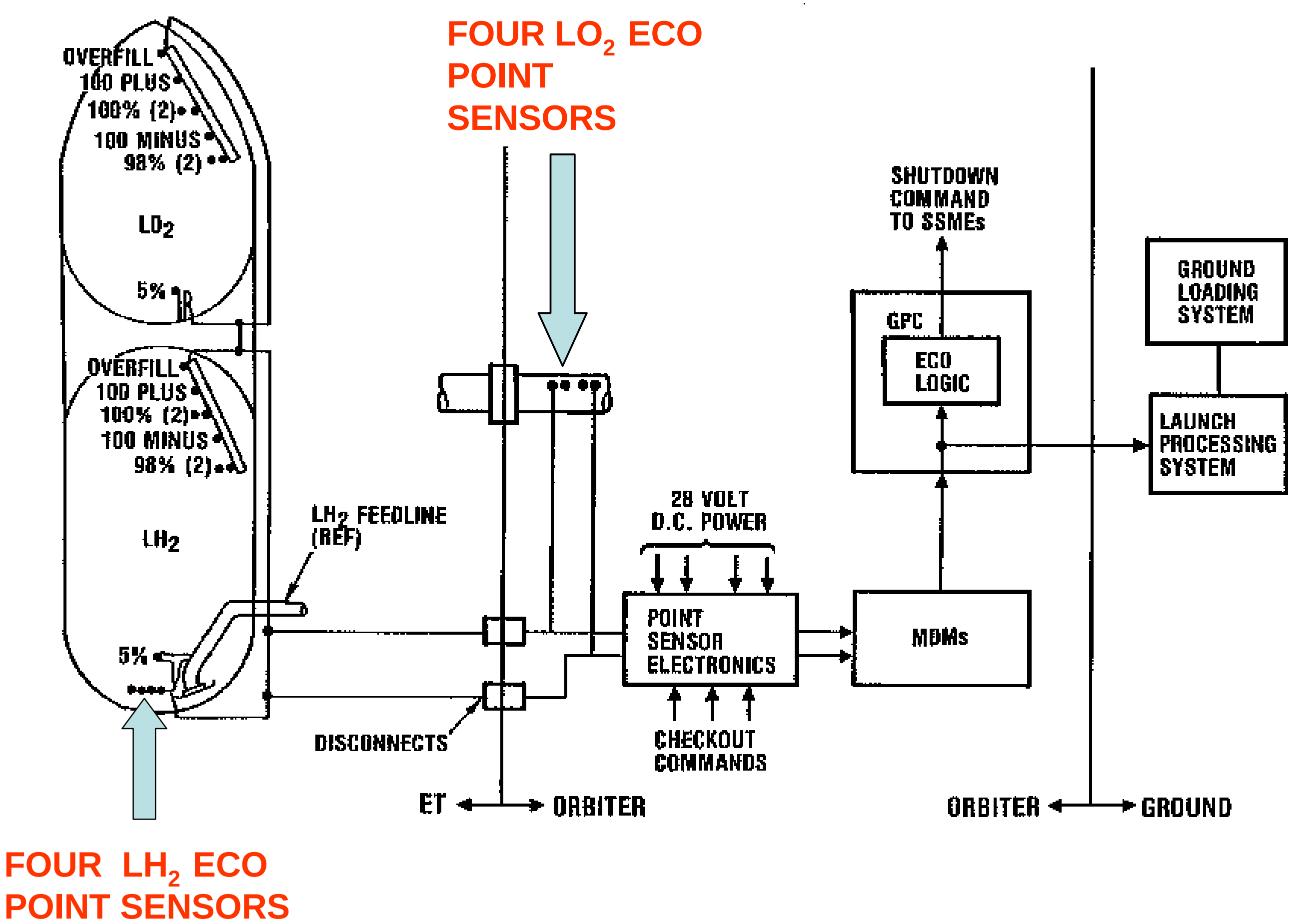

- Preliminary Shuttle Probabilistic Risk Assessment (SPRA) results show crew actions during entry are a risk driver.
  - Contributions were developed with the assistance of the Astronaut Office (Dom Gorie).
  - Results / methods are currently undergoing an independent review.
- These actions are or could be automated, potentially reducing the risk of entry.

- Of the approximately 200 crew actions modeled, the top four contribute about 11% of the 15% human reliability total.

1) Crew fails to deploy landing gear
2) Crew Brakes at the Wrong Time
3) Crew Improperly Performs Pre-flare
4) Crew Lands too Hard

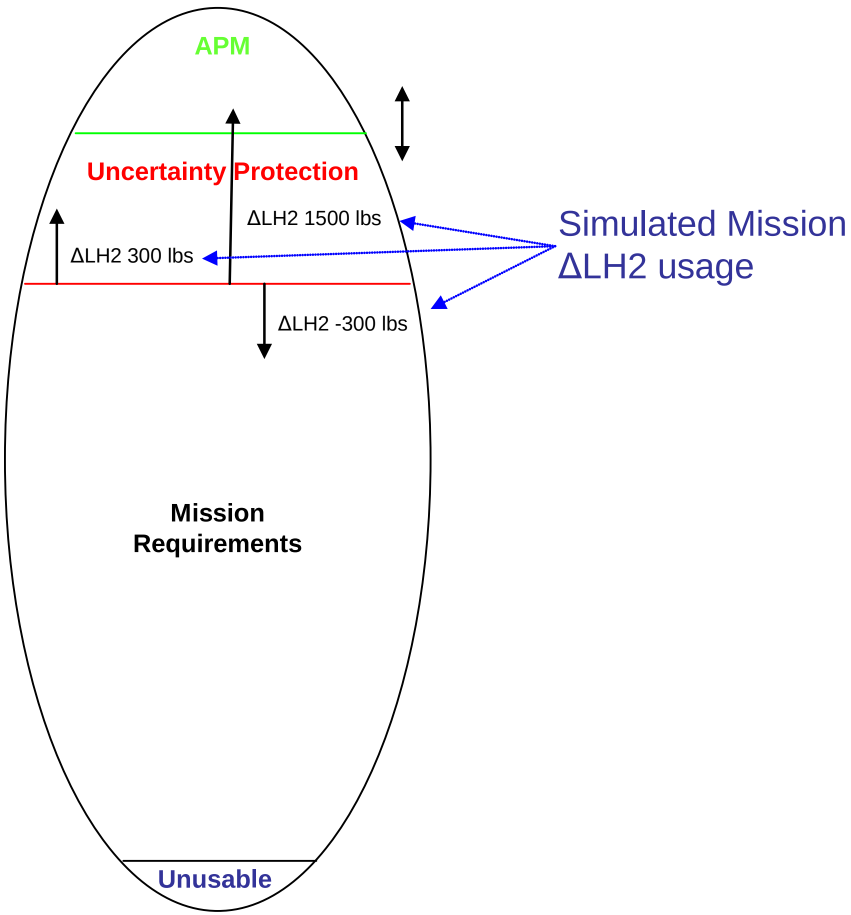
✓Showed that ~70% of calculated risk due to crew error occurs during entry, descent, and landing

# Engine Cutoff (ECO) Sensors



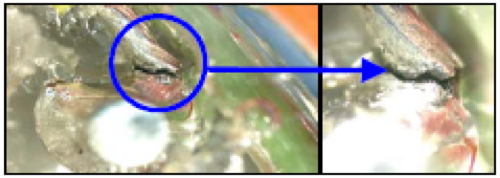

- ✓ Assessed the risk of changing the Launch Commit Criteria (LCC) for these ECO sensors from requiring four of four sensors to only requiring three of four sensors.
- ✓ Pointed out the need to better understand the other side of the risk trade when a launch is scrubbed due to ECO sensor failures, i.e., scrub turnaround risk.

# Probability of LH2 Low Level Cutoff (STS-122)



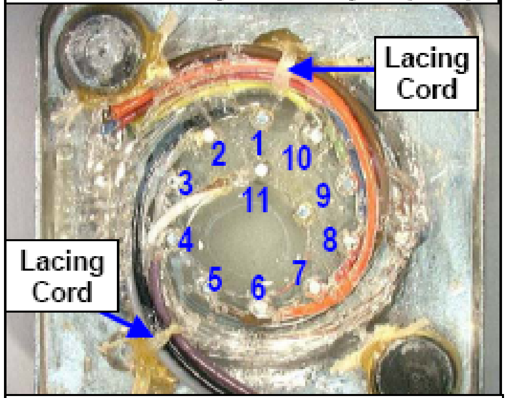

- ✓ Shuttle Program Manager requested and used
- ✓ Model used historical data in a simulation model
- ✓ Shuttle Program Manager could see it impact of adding Ascent Performance Margin (APM) on risk

# Solid Rocket Booster Power Bus Isolation Supply Analysis



Wire Broken at Pin 10 Post

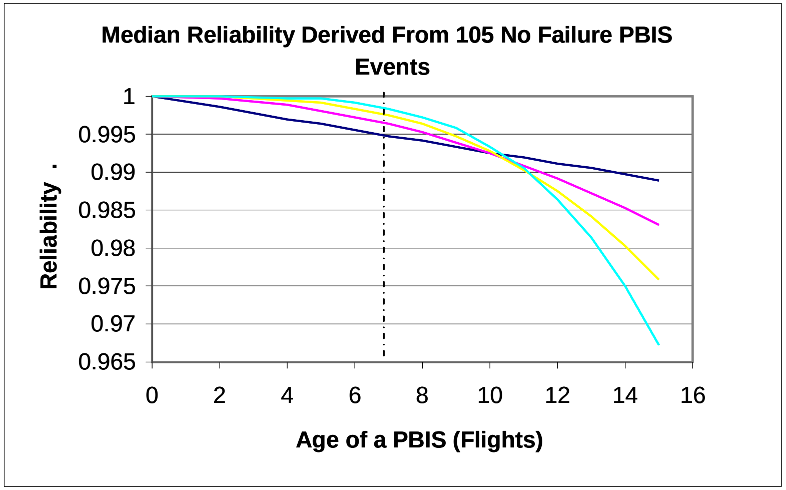
Destructive Physical Analysis (DPA)




Critical Pins: 2, 3, 4, 5, 6

Non Critical Pins: 1, 7, 8, 9, 10, 11

PBIS T2 Transformer Leads

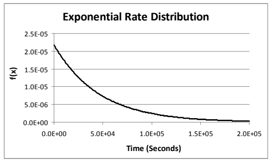



- ✓ **Emphasized the need to implement a design change that would eliminate the failure in future flights**

# Main Propulsion Flow Control Valve

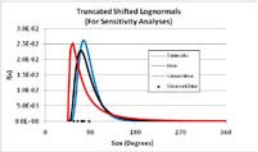
**INPUTS**

**Failure Rate**




**Chance of multiple failures**

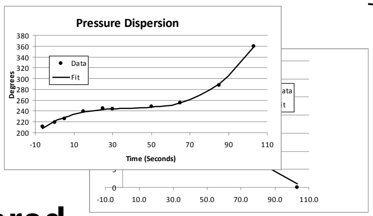
**Poppet Break Size Distribution**

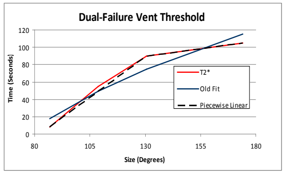



**# of failures, size and time**

**Compared to Thresholds**

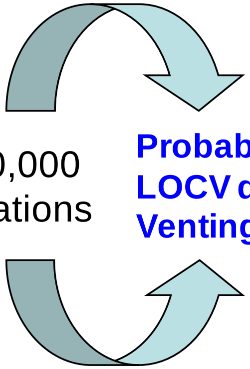
**Thresholds**




3 poppet failures are assumed to vent if occur before 120 seconds

5,000,000 replications

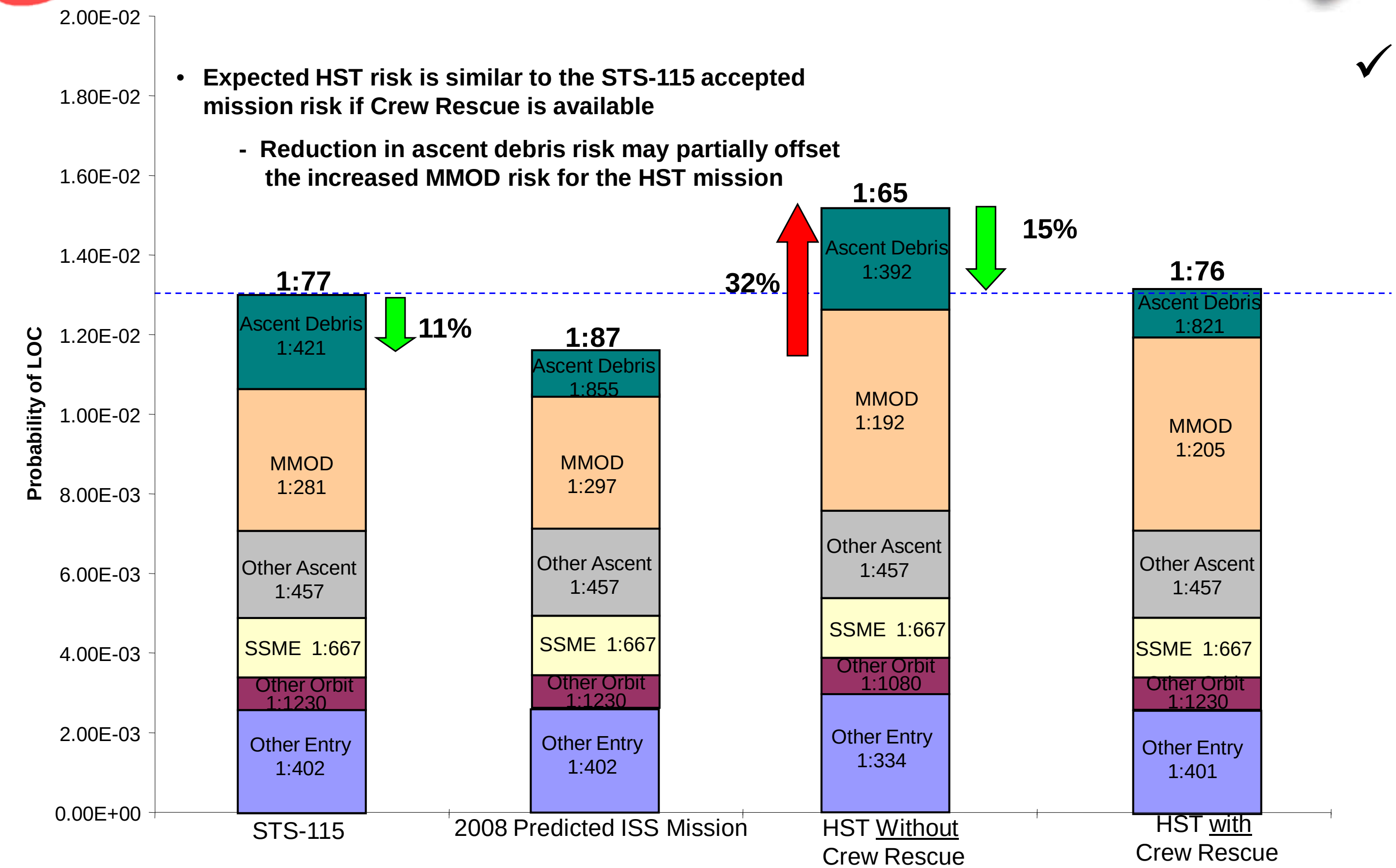


**Probability of LOCV due to Venting**

- ✓ **Shuttle Program used these risk estimates as supporting flight rationale for STS-119, combined with FCV inspection and impact testing**

# Hubble Space Telescope (HST) Manifest Decision

## Risk Comparisons

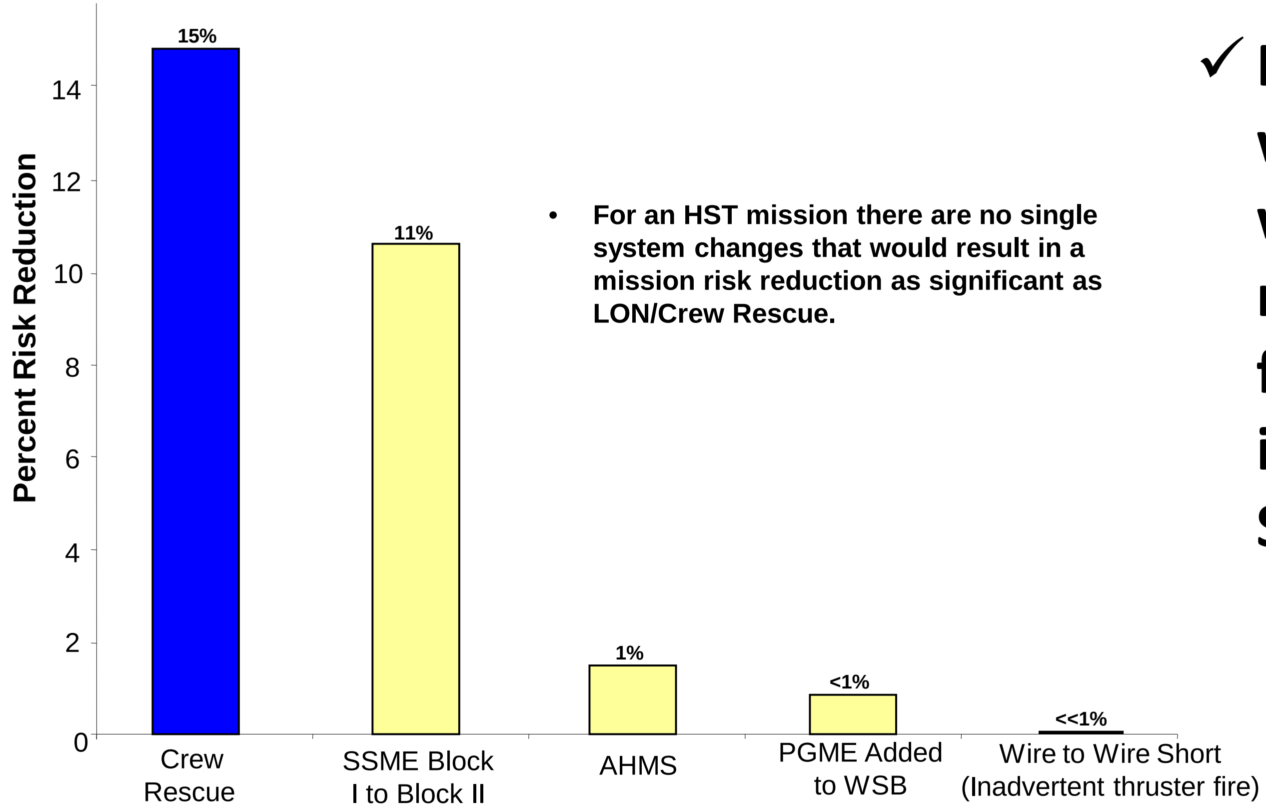



✓ **Analysis compared HST risk with and without crew rescue to other Shuttle missions in order to help NASA Administrator decide whether or not the HST mission was an acceptable risk**

Oct 27, 2006

# Hubble Space Telescope (HST) Manifest Decision (2)

## RISK REDUCTION COMPARISON

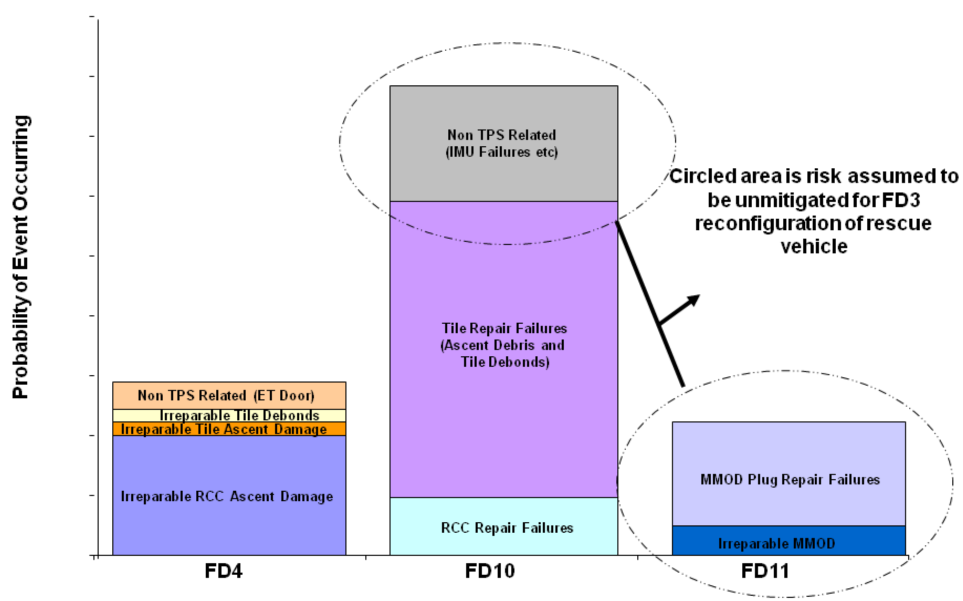



✓ **Risk reduction with crew rescue was compared to risk reductions from implemented Shuttle upgrades**

# Probability of Launch on Need

✓ **Assisted the Shuttle Program Manager with making an informed decision not to release the HST rescue vehicle**

PROBABILITY OF NEEDING CREW RESCUE BY DECISION FLIGHT DAY



# STS-128 Power Controller Assembly Risk Presented at L-2

## STS-128 PCA FAILURE RATE RESULTS

| | | OV103 | | | Weibull (β=2.024, η=25538) | | |
|---|---|---|---|---|---|---|---|
| | | S/N | ASSEMBLE | Cycles | P(f) | 5th | 95th |
| | FPCA-1 V070-763320 | -032 / 266775 | | | | | |
| K1 | AC Inverter 1, Phase A | 127 | 4/16/1982 | 6100 | 1.8E-05 | 8.4E-06 | 3.3E-05 |
| K2 | AC Inverter 1, Phase B | 128 | 4/16/1982 | 6100 | 1.8E-05 | 8.4E-06 | 3.3E-05 |
| K3 | AC Inverter 1, Phase C | 126 | 4/16/1982 | 6100 | 1.8E-05 | 8.4E-06 | 3.3E-05 |
| K11 | RJDF Bus A | 092 | 11/14/1979 | 1245 | 3.6E-06 | 1.6E-06 | 6.6E-06 |
| | FPCA-2 V070-763340 | -013 / J12867 | | | | | |
| K1 | AC Inverter 2, Phase A | 096 | 1/20/1981 | 6300 | 1.9E-05 | 8.7E-06 | 3.5E-05 |
| K2 | AC Inverter 2, Phase B | 112 | 1/20/1981 | 6300 | 1.9E-05 | 8.7E-06 | 3.5E-05 |
| K3 | AC Inverter 2, Phase C | 117 | 1/20/1981 | 6300 | 1.9E-05 | 8.7E-06 | 3.5E-05 |
| K13 | RJDF-1 Bus B PWR (RPC#36) | 111 | 1/20/1981 | 1245 | 3.6E-06 | 1.6E-06 | 6.6E-06 |
| | FPCA-3 V070-763360 | -019 / EJ3166 | | | | | |
| K-1 | AC Inverter 3, Phase A | 212 | 10/12/1978 | 6900 | 2.1E-05 | 9.5E-06 | 3.8E-05 |
| K-2 | AC Inverter 3, Phase B | 214 | 10/12/1978 | 6900 | 2.1E-05 | 9.5E-06 | 3.8E-05 |
| K-3 | AC Inverter 3, Phase C | 215 | 10/12/1978 | 6900 | 2.1E-05 | 9.5E-06 | 3.8E-05 |
| K-6 | RJDF-2B Manif F4/F5 Drivers | 216 | 12/10/1985 | 1245 | 3.6E-06 | 1.6E-06 | 6.6E-06 |
| | MPCA-1 V070-764400 | -039 / ER1634 | | | | | |
| K4 | SPARE | 221 | 7/11/1989 | 700 | 2.0E-06 | 9.1E-07 | 3.6E-06 |
| K5 | ODS/ECLSS | 228 | 7/11/1989 | 1180 | 3.4E-06 | 1.6E-06 | 6.2E-06 |
| | MPCA-2 V070-764430 | -033 / F71099 | | | | | |
| K4 | SPARE | 103 | 3/31/1980 | 700 | 2.0E-06 | 9.1E-07 | 3.6E-06 |
| K5 | ODS/ECLSS | 106 | 3/31/1980 | 1180 | 3.4E-06 | 1.6E-06 | 6.2E-06 |
| | APCA-1 V070-765310 | -003 / AM6520 | | | | | |
| K1 | Reaction Jet Driver Bus A | 138 | 11/10/1982 | 1245 | 3.6E-06 | 1.6E-06 | 6.6E-06 |
| | APCA-2 V070-765320 | -009 / F66222 | | | | | |
| K1 | Aft Payload Bay Power B | 137 | 3/29/1982 | 700 | 2.0E-06 | 9.1E-07 | 3.6E-06 |
| K2 | RJDA Manif Drivers Bus B | 180 | 2/9/1984 | 1245 | 3.6E-06 | 1.6E-06 | 6.6E-06 |
| | APCA-3 V070-765330 | -013 / J43296 | | | | | |
| K1 | Aft Payload Bay Power C | 072 | 10/10/1979 | 700 | 2.0E-06 | 9.1E-07 | 3.6E-06 |
| K2 | RJDA Manif Drivers | 079 | 10/10/1979 | 1245 | 3.6E-06 | 1.6E-06 | 6.6E-06 |

**Failure rates between 2.0E-06 and 2.1E-05 per cycle**

### Probability of a Broken Contactor on STS-128

**Mean – 1:7400**
95th- 1:5500
5th – 1:10000

Low Risk due to limited # of cycles in flight

**Using a Random failure rate the mean probability of a broken contactor on STS-128 is: 1:4100**

**Analysis was used to help Shuttle Managers decide that PCA risk was acceptable for flight**

### Probability of a Broken Contactor on the Ground

The probability of a SAIL contactor of ~15700 cycles old breaking in a **6 week period** (Assuming 15 contactor s and 2 cycles per day) is: **~1:20**

The probability of a vehicle inverter contactor of ~4700 cycles old breaking in a **6 week period** (Assuming 27 contactors and 4 cycles per week) is: **~1:100**

**Analysis showed that it was much more likely to have a broken contactor on the ground**

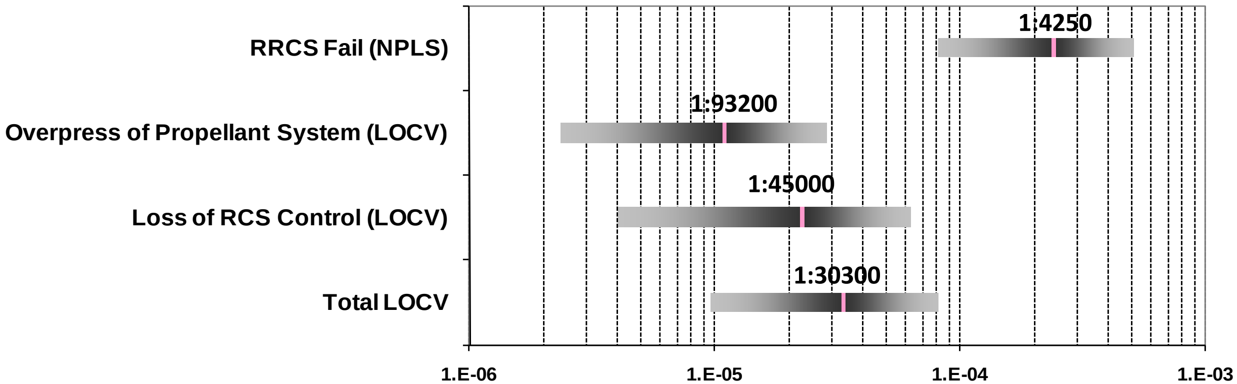
### KEY ASSUMPTIONS

- Assumes 0.5 cycles for AC inverter contactor, 1.5 cycles for RJD contactor and 1.5 cycles for ODS and Payload contactors for STS-128
- Analysis assumes failure rate based upon contactor cycles
- 5 broken contactor failures are used in the analysis
- Assumes contactor failure will result in inadvertent "off" or failure to turn "on"
- Non-latching contactors are not included in the analysis
- Contactor cycles based upon engineering judgment

**Important to inform managers of the analysis assumptions**

# STS-131 Helium Isolation Valve Risk

## FAILURE SCENARIO RISK UNCERTAINTIES

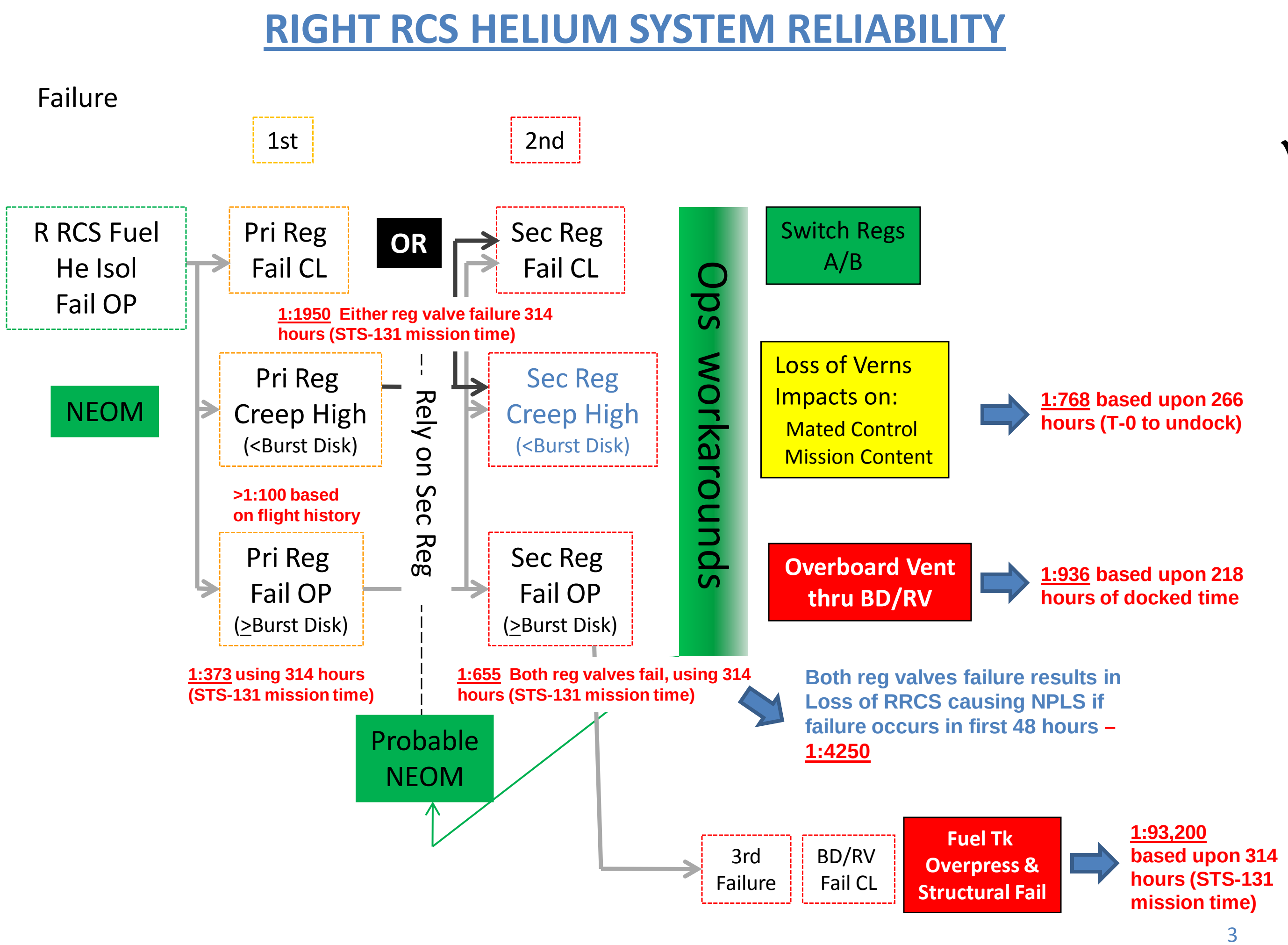



- Given the failed helium isolation valve failed open, the identified risk scenarios have various mission impacts as shown in backup chart 6.
- **Loss of Right RCS Function** is failure of both regulators and assumes a mission time of **48 hours** (prior to reaching 82% which is expected late FD2, early FD3) and results in NPLS
- **Overpressurization of the Propellant System** is failure of both regulators and failure of either the burst disc or the relief valve and uses **314 hours** (STS-131 mission time)
- **Loss of RCS Control** is failure of both regulators and either cross-feed or LRCS failure and uses **48 hours** (prior to reaching 82% which is expected late FD2, early FD3)
- Each scenario is developed to the point where the mission impact is reached.
- No change of state in the failed isolation valve is assumed.
- If both helium isolation valves are assumed to be failed open, the calculated risk for regulator fail open will double, which will impact all of the risk estimates.

2

✓ **Analysis was used to support STS-131 flight rationale at the HQ Flight Readiness Review**

# Right RCS Helium System Reliability




- ✓ **Analysis results combined with graphical display to help communicate to Management at HQ Flight Readiness Review**

# SUMMARY

- Showed various ways of communicating  and using PRA findings in the Shuttle Program
- Stated that it is important to provide management:
  - Clear presentation of analysis
  - Applicable assumptions and limitations
  - Estimates of uncertainty
- Maintain consistency and accuracy across the program to make it relevant
- Used various levels of PRA to answer the mail
- The Shuttle Program has benefited from using PRA and others can too