Managing Space Shuttle Program Risk for Return to Flight: Why does risk management fail?

N. Wayne Hale

Manager, Space Shuttle Program

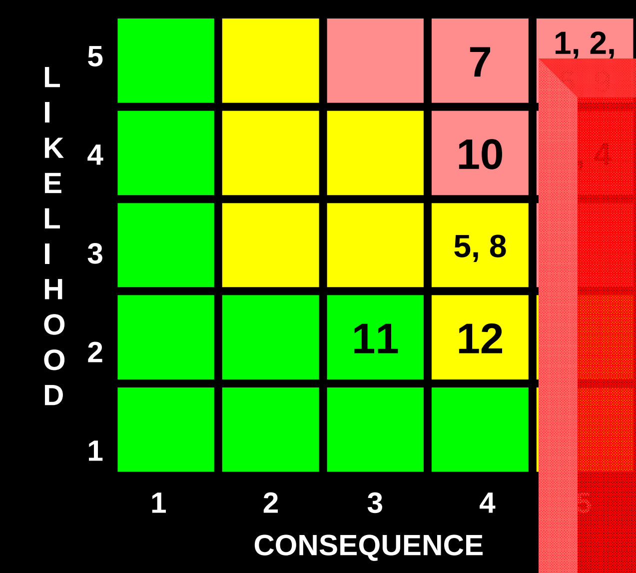
Mr. James Cameron

Risk and Exploration: Earth, Sea, and the Stars

NASA Administrator's Symposium

September 27 – 29, 2004

Where are the key program risks?



▲	1.	2541	STS-114/ET-121 Foam Loss IFAs (Foam Debris > Allowables) - ET (Saf) **(5 x 5)**
▲	2.	2542	STS-114/ET-121 Foam Loss IFAs (Foam Loss Requiring Risk Assessment) - ET (Saf) **(5 x 5)**
▲	3.	2430	MMOD - FOI, SMA [illegible] Orbiter, FCOD, MOD, Engineering, SSP (Saf) **(4 x 5)**
▲	4.	2505	Loss of Critical Per[illegible]nnel - SP (Supp) **(4 x 5)**
▲	5.	2419	Inability to Meet the [illegible]o/No Go Criteria in the Inspection and Repair Roadm[illegible] - JSC_DD (MS, Sch) **(3 x 4)**
▲	6.	2420	Threats to SSP Re[illegible]rve - BusMgmt (C) **(5 x 5)**
▲	7.	[illegible]	LH2 Engine Cut Of[illegible]ECO) Sensor Unexplained Anomaly (UA) - JSC_DD, U[illegible], SEI (Saf, MS, Supp, Sch, C) **(5 x 4)**
▲	8.	2553	Gap Filler Protrusi[illegible] - Orbiter (Sch) **(3 x 4)**
▲	9.	[illegible]	Recovery of Michou[illegible] Assembly Facility (MAF) from Hurricane - ET (Su[illegible]), Sch, C) **(5 x 5)**
▲	10.	2006	OBSS Structural Lo[illegible]ds Exceed MPM Capacity (RTF 1006) - OBSS (Sa[illegible] Supp, Sch) **(4 x 4)**
▲	11.	22[illegible]	STS-121 On-line P[illegible]ocessing (OV-104) - LL (Sch) **(2 x 3)**
▲	12.	2288	Infrastructure - LL (Supp) **(2 x 4)**

Saf - Safety | **MS- Mission Success** | **Supp - Supportability** | **Sch- Schedule** | **C - Cost**

▲ **– Top Program Risk (TPR)**

△ **– Top Director Risk (TDR)**

■ **– Top Organization Risk (TOR)**

□ **– Top Sub Organizational Risk (TSR)**

Low **Medium** **High**

These are the risks that we know about. What about the ones we don't know about?

Top Program Risks, June 2005

	1	2	3	4	5
5				2	5
4			8	1, 7, 11	3, 6
3				9	4
2			10	12	
1					

CONSEQUENCE

Saf - Safety | MS- Mission Success | Supp - Supportability | Sch- Schedule | C – Cost

▲ – Top Program Risk (TPR)

△ – Top Director Risk (TDR)

■ – Top Organization Risk (TOR)

□ – Top Sub Organizational Risk (TSR)

Low | Medium | High

▲ 1. 2146 External Tank LO2 Feedline Bellows Design - ET (Saf, Sch) (4 x 4)

▲ 2. 2152 Debris Certification/Risk Acceptance - SEI, JSC_DD, USA (Saf, MS, Supp, Sch) (5 x 4)

▲ 3. 2430 MMOD - FOI, SMA, Orbiter, FCOD, MOD, Engineering, SSP (Saf) (4 x 5)

▲ 4. 2268 ANALYTICAL CAPABILITY TO ASSESS TILE DAMAGE - Orbiter, TRP (Saf, MS, Supp, Sch, C) (3 x 5)

▲ 5. 2420 Threats to SSP Reserve - BusMgmt (C) (5 x 5)

▲ 6. 2505 Loss of Critical Personnel - SP (Supp) (4 x 5)

▲ 7. 2486 STS-301 On-Time Processing - LL (Sch) (4 x 4)

▲ 8. 2286 STS-114 On-Time Processing (OV-103) - LL (Sch) (4 x 3)

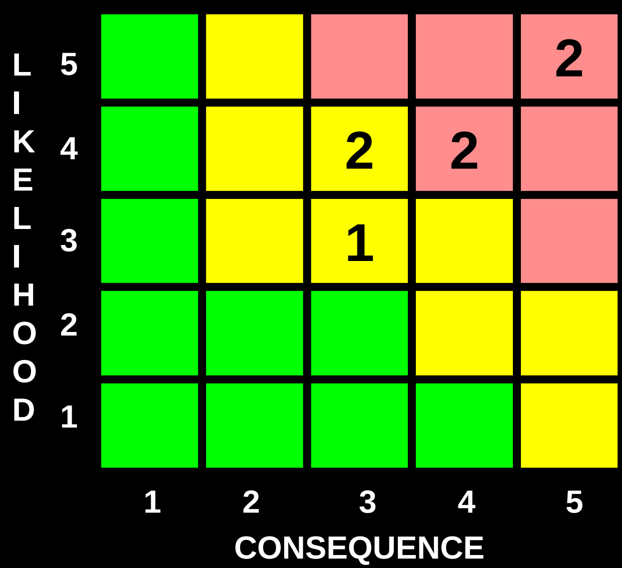
▲ 9. 2419 Inability to Meet the Go/No Go Criteria in the Inspection and Repair Roadmap - JSC_DD (MS, Sch) (3 x 4)

▲ 10. 2291 STS-300/121 On-Time Processing (OV-104) - LL (Sch) (2 x 3)

▲ 11. 2006 OBSS Structural Loads Exceed MPM Capacity (RTF 1006) - OBSS (Saf, Supp, Sch) (4 x 4)

▲ 12. 2288 Infrastructure - LL (Supp) (2 x 4)

MSFC/ET Risks before STS-114, June 2005



▲ – Top Program Risk (TPR)

△ – Top Director Risk (TDR)

April Risk Score	June Risk Score	Risk
5 x 5	5 x 5	▲ 2313 - TPS Mock-Up and Spray Center and Production Facility Modifications (2006 Funding Needed) - ET (Sch, C)
5 x 5	5 x 5	▲ 2455 - Level II Requirement Changes - ET (Sch, C)
4 x 4	4 x 4	▲ 1176 - SSME HPOTP Knife Edge (KE) Seal cracking - SSME, BusMgmt (Supp, Sch, C)
4 x 4	4 x 4	▲ 2146 - External Tank LO2 Feedline Bellows Design - ET (Saf, Sch)
5 x 2	4 x 3	△ 2219 - SRB Range Safety System (RSS) Test Capability - BusMgmt, SRB (Supp, Sch, C)
4 x 3	4 x 3	△ 2401 - Range Safety Carrier Frequency Change - SRB (Supp, C)
3 x 3	3 x 3	△ 2400 - Hardware supportability (HPOTPs & LPOTPs) - SSME (Supp)

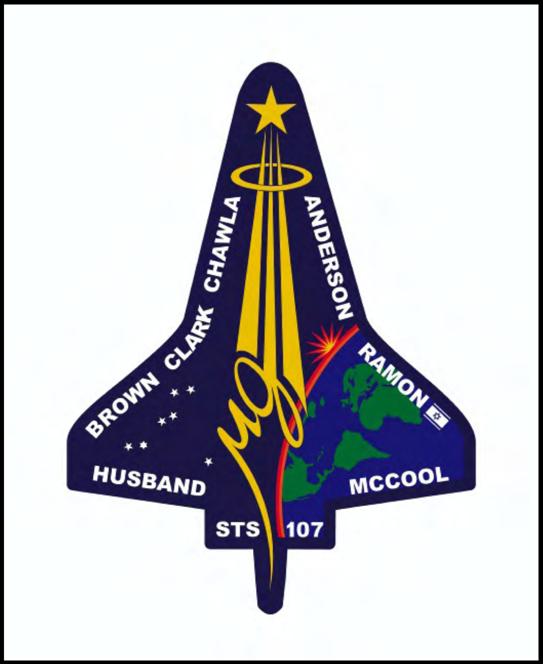
PAL Ramps were not captured as a risk in the system

Risk Assessment Example

ET PAL Ramps

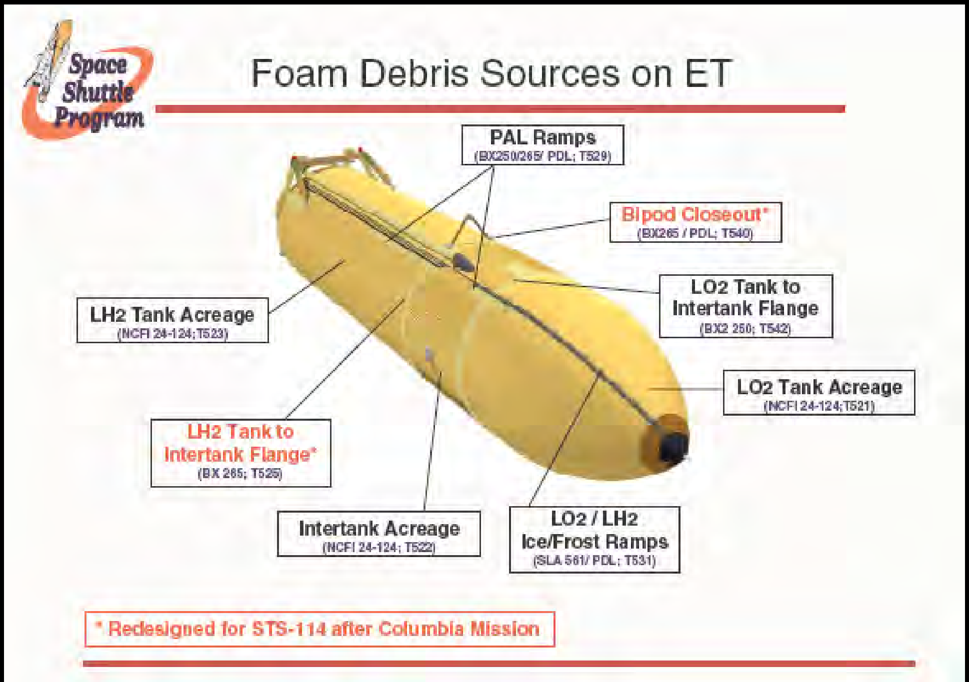
Assessing Risk: Foam Loss

- Background:
  - During STS-107, a large chunk of foam from the Bi-Pod Ramp dislodged during ascent and struck *Columbia*’s wing leading edge, punching a large hole in the RCC panel that protects the wing from entry heating.
  - Although there were indications that there might have been a problem during the mission, we did not attempt an inspection of the vehicle, and we had no ready imagery that would have told us the vehicle’s status.
  - During entry, *Columbia’s* TPS failed because of the large hole. The crew and vehicle were lost.

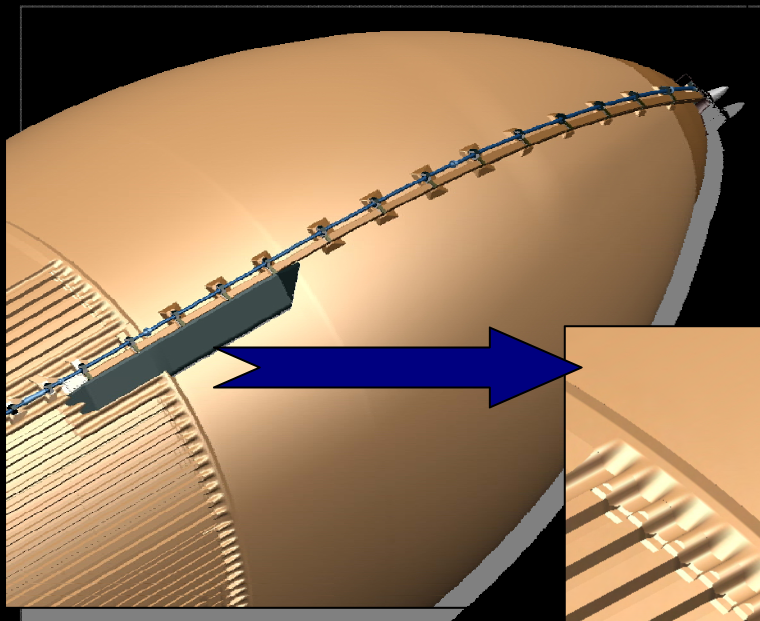


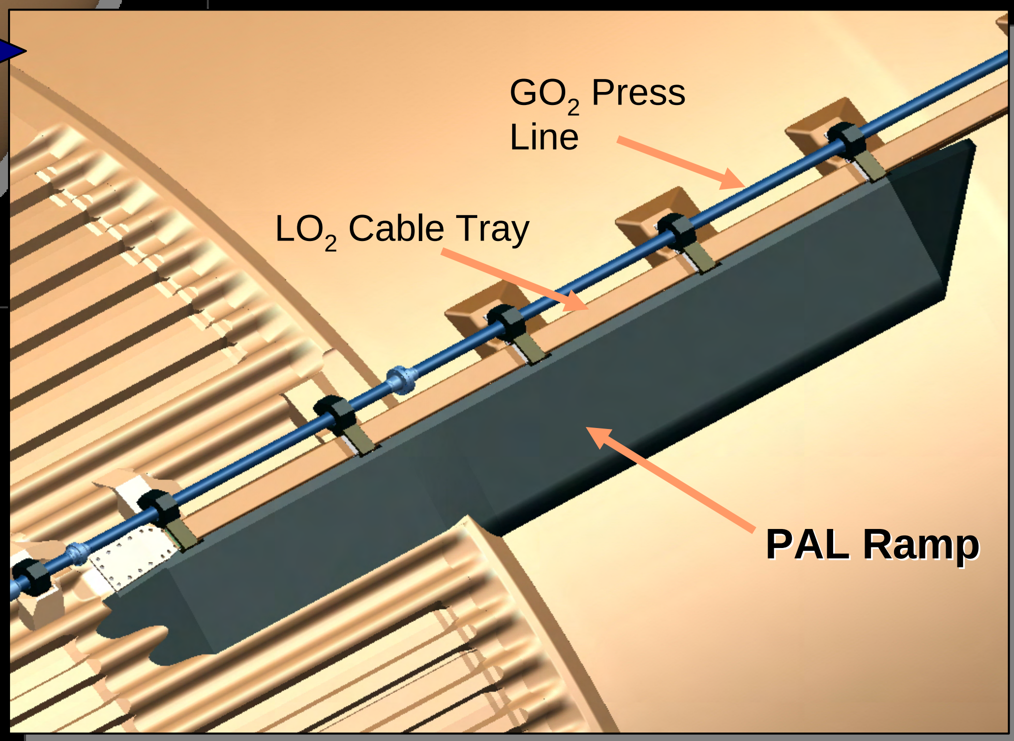
Assessing Risk: The PAL Ramps

- Background—Post-*Columbia:*
  - The CAIB quickly identified the loss of Bi-Pod Ramp foam as the proximate cause of the *Columbia* accident.
  - SSP committed eliminating critical debris.
  - Eliminating all debris was not possible without a full redesign of the ET
  - SSP did a comprehensive review of the ET to identify areas of potential critical debris.
  - Sixteen critical areas were identified. Six areas were redesigned or changed.

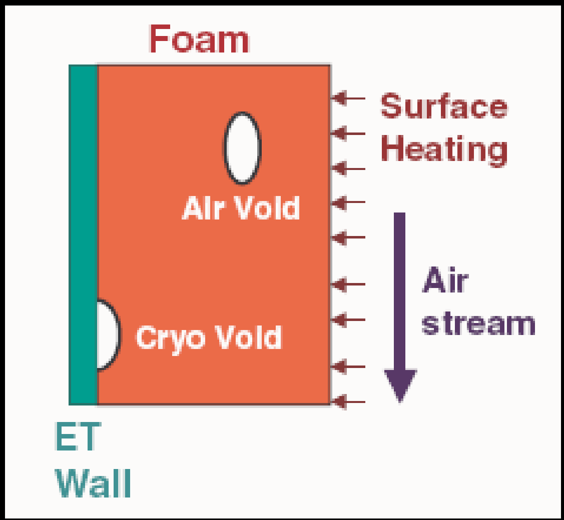


PAL Ramp Basics





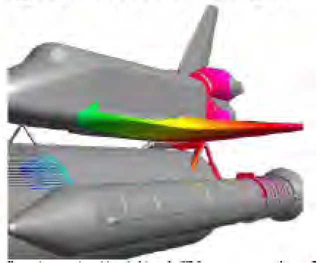
PAL Ramps Risk Assessment: Foam Divots



Test Verified Assumptions (ie pop-off velocity, shape and impact sensitivity)

Foam Divots from ET Ogive and Flange

F-15B Foam Trajectory Flight Test

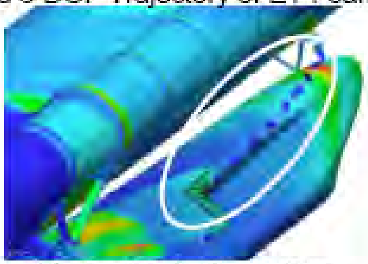


Impact Sensitivity Zones

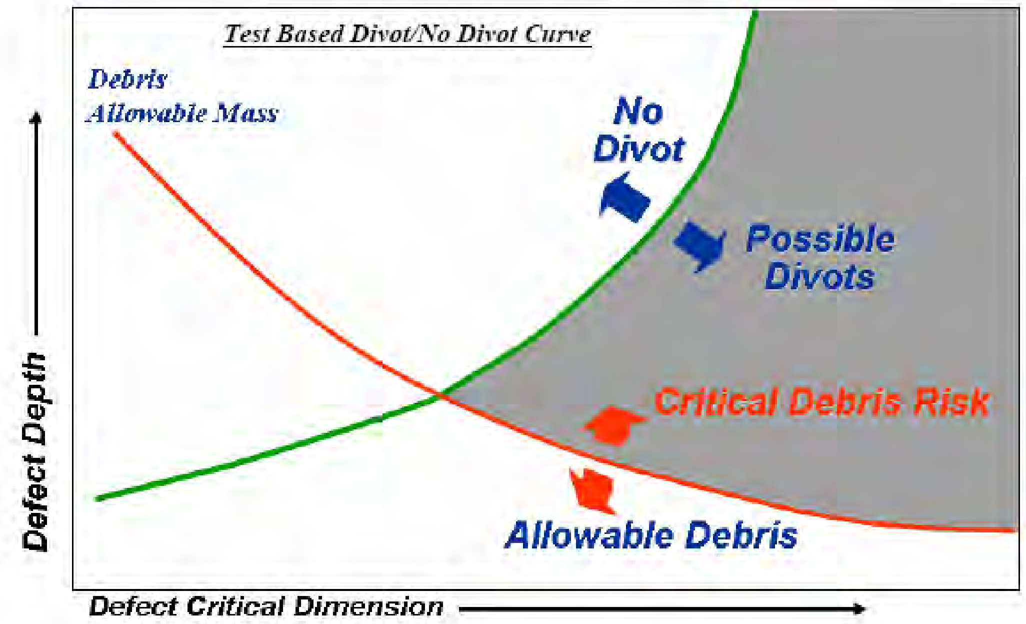
PAL Ramps Risk Assessment: Acceptance Rationale

Trajectory Reconstruction of Specific Observed Flight Debris

Computed 6-DOF Trajectory of ET Foam Divot

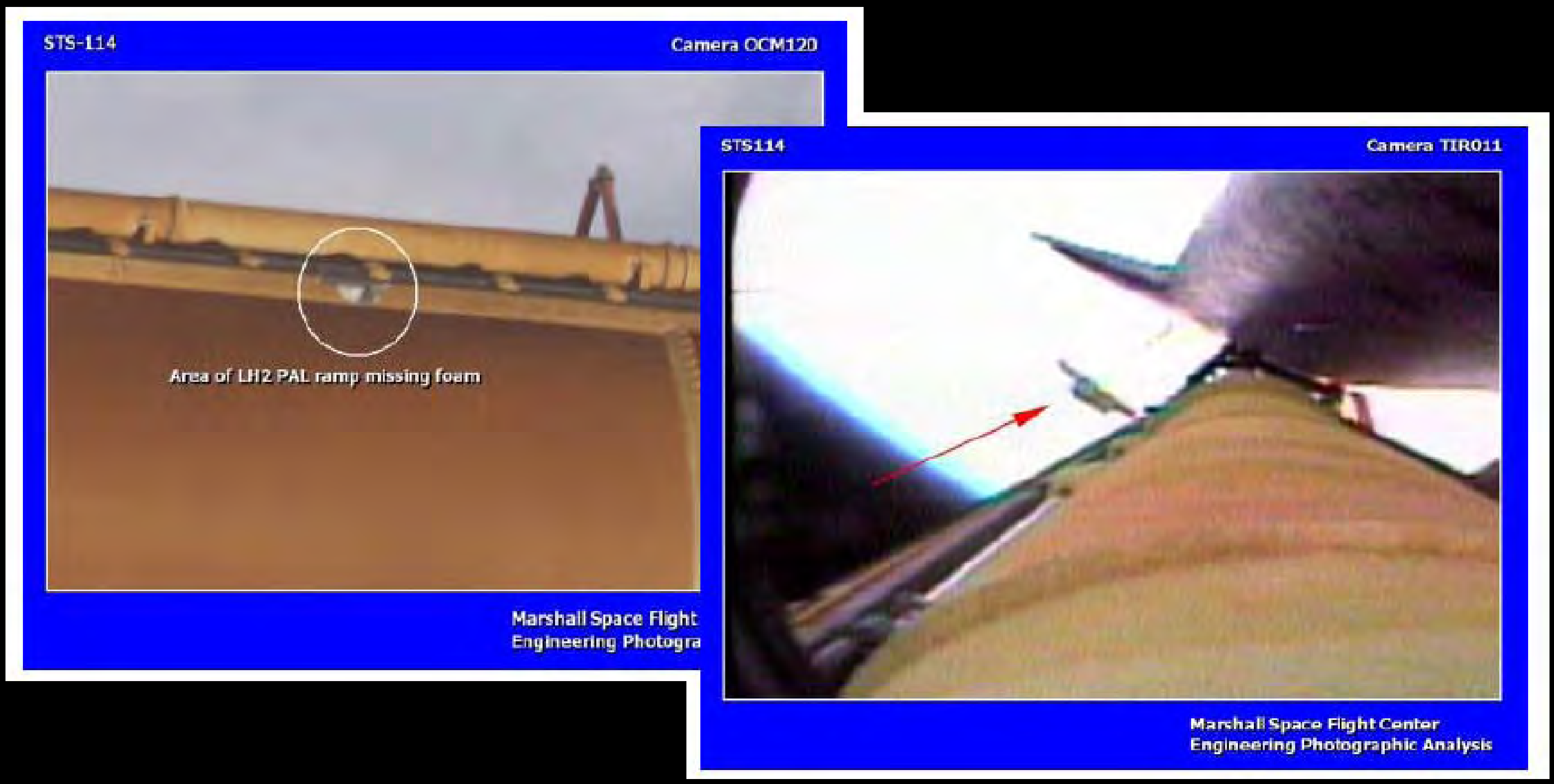


Moving Body Simulation of STS-107 Debris

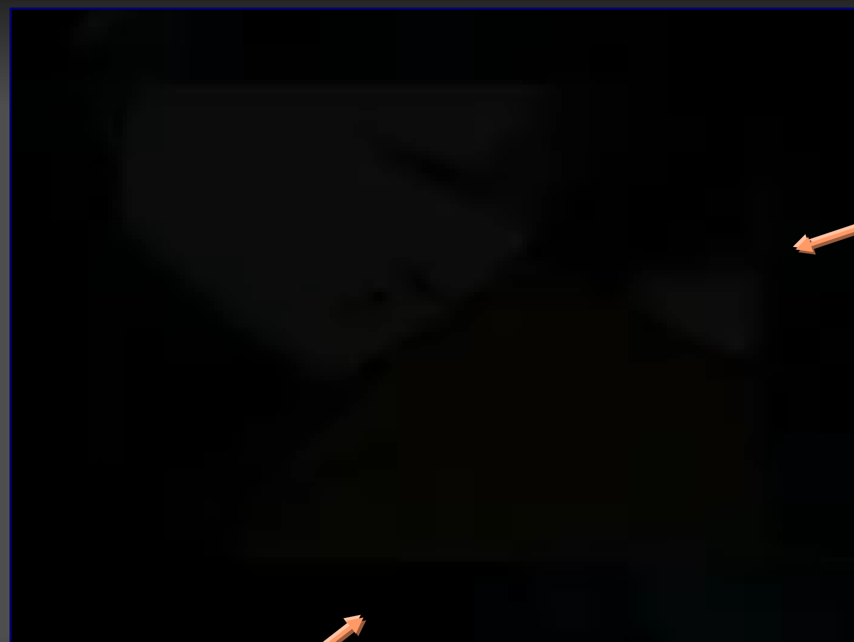


Theory Vs. Reality

- We saw some unexpected foam losses on STS-114, including a significant loss from the LH2

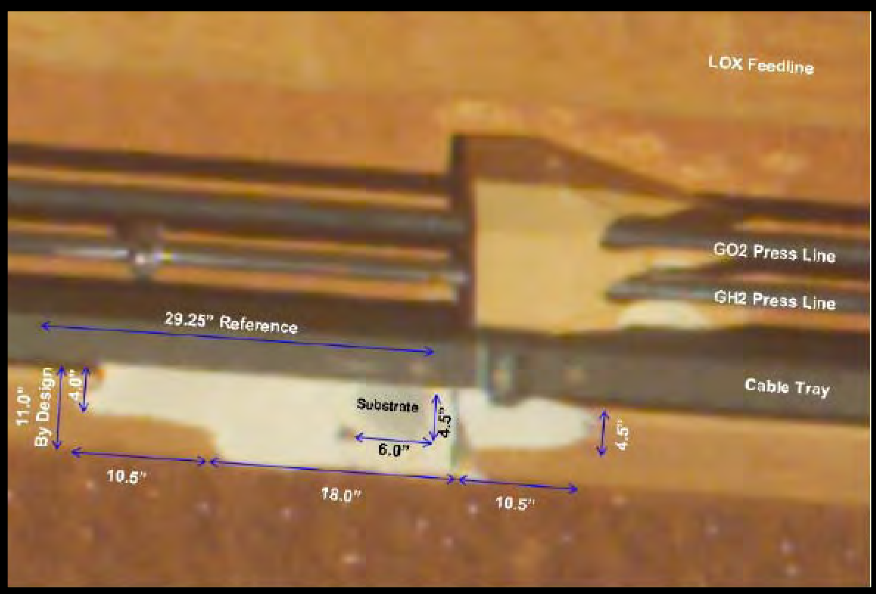


PAL Ramp Foam Loss on STS-114



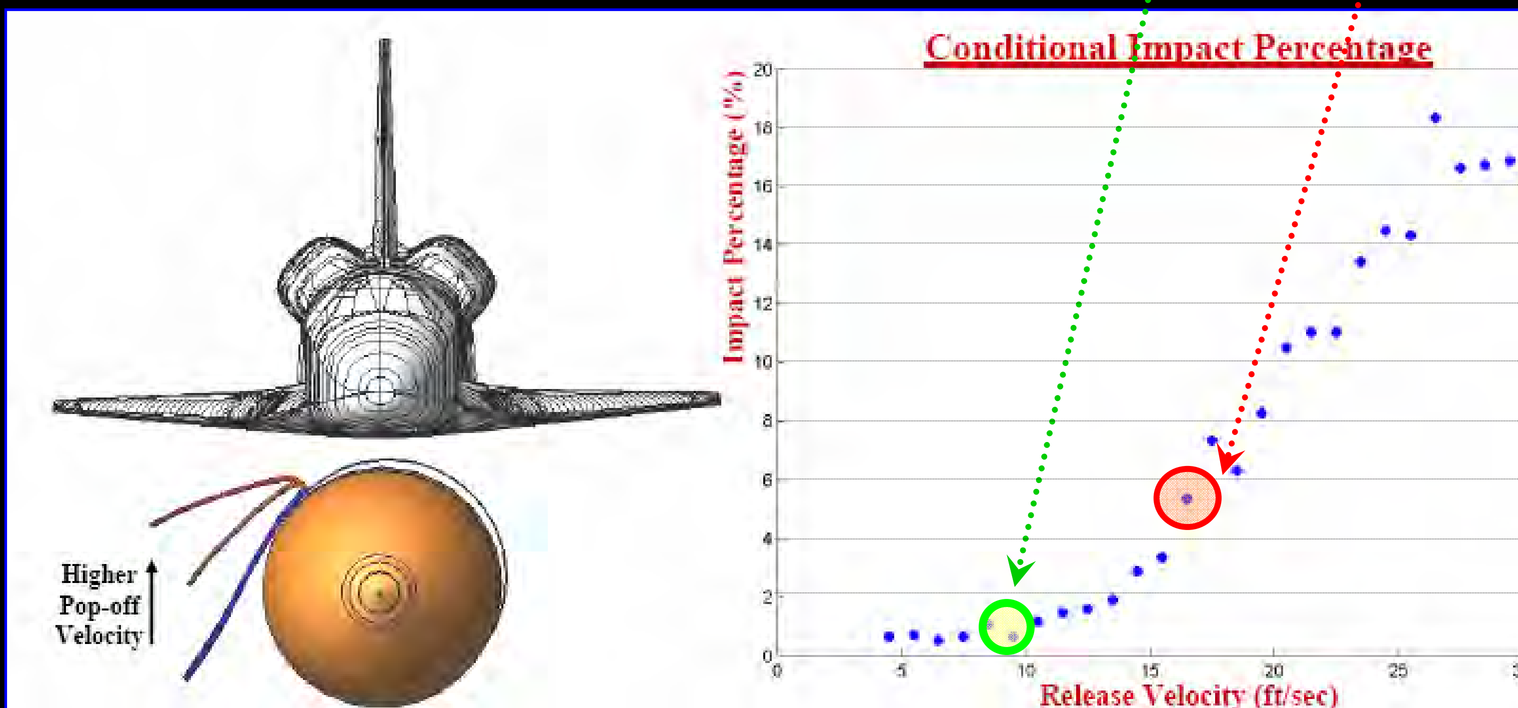
LH2 PAL Ramp Foam Loss

- Large foam loss occurred late enough in the ascent that it did not impact the Orbiter; aerodynamic forces carried it away from the Shuttle.
- The foam mass was 1.01 lbs; the certified Orbiter capability was 0.017 lbs.
- Did we get lucky? Or unlucky? Were our assumptions bad?



STS-114 Risk Posed by PAL Ramp Foam

- Post STS-114, SSP SE&IO calculated that the risk of the PAL Ramp foam released on STS-114 hitting the Orbiter and causing damage was 1 in 26.
- This is a conservative assessment enveloping pop-off velocities up to 17 feet per second (FPS).
- Imagery suggests that the velocity of the STS-114 foam was about 9 FPS, which would significantly lower the risk of impact.
- Where do you draw the line between acceptable and unacceptable risk?



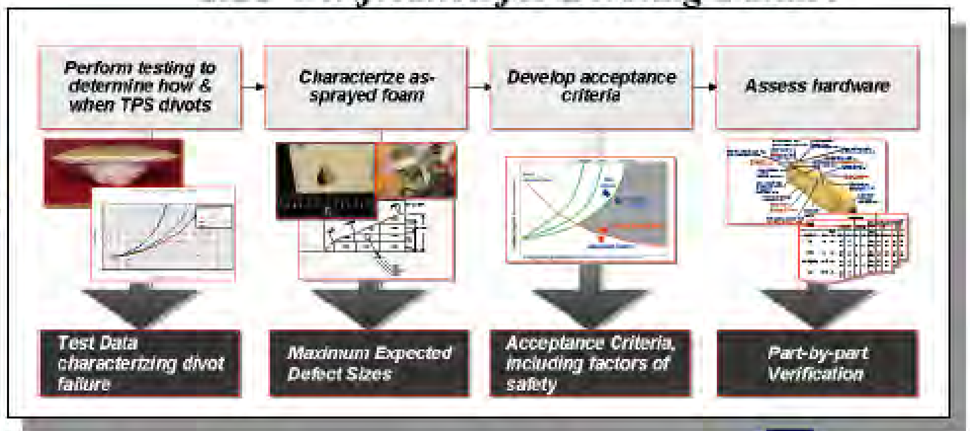
What did we miss?

Why did we miss it?

Assessing the Risk of ET TPS Failure

RTF TPS Debris Requirements

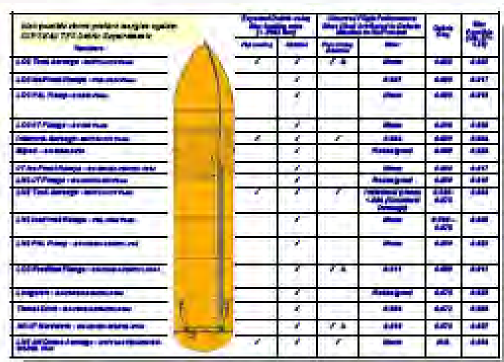
RTF Verification for Divoting Failure



ET TPS Verification Modified for RTF to Include Assessment of Internal Defects

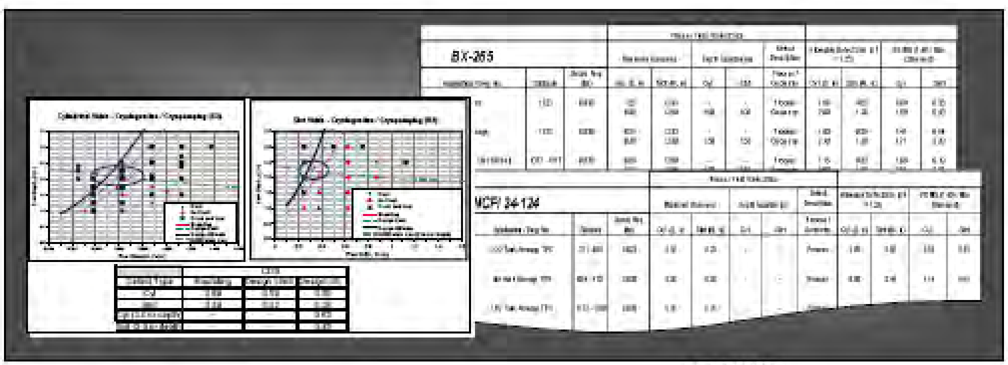
- Results: Positive Design Margin and Acceptable Mass Conditions Exist for All ET TPS Applications

(Based on ET TPS Debris Requirements)



Assessing the Risk of ET TPS Failure

- *Each TPS component is assessed for each TPS failure mode*



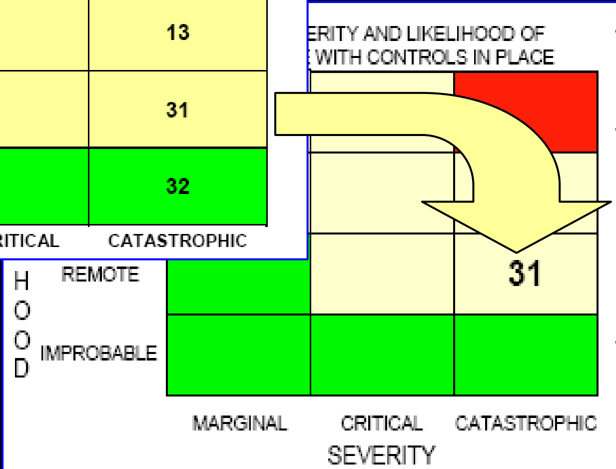
- *A margin of safety using maximum expected defect assessments and component specific environments is calculated for each component*

Assessing Risk from the PAL Ramps

(HAZARD SEVERITY LEVEL AND LIKELIHOOD OF OCCURRENCE WITH CONTROLS IN PLACE)

	MARGINAL	CRITICAL	CATASTROPHIC
PROBABLE			
INFREQUENT			13
REMOTE			31
IMPROBABLE			32

Risk of Ascent Debris Impact



Window Impacts

1 Cause for BSM Plume Constituents

1 Cause for ET Foam

RCC Impacts

3 Ice Causes

- TPS Defects Ice
- ET Acreage Ice
- LO_2/LH_2 Ice/Frost Ramps Ice

1 Cause for Bipod Jack Pad foam

Special Tile Impacts

(Umbilical/Landing Gear Doors)

8 Foam Causes

- LO_2 Tank Acreage
- Intertank Acreage
- LH_2 Tank Acreage
- LH_2 PAL Ramp
- LH_2 Tank Ice/Frost Ramps
- Aft Attach Hardware
- GO2 Pressline Support Bracket
- Bipod Jack Pad Closeout

1 Cause for Protective Barriers

1 Cause for BSM Products

1 Cause for SRB Separation Products

Tile Impacts

9 Foam Causes

- LO_2 Tank Acreage
- Intertank Acreage
- LH_2 Tank Acreage
- LO_2 Feedline
- LO_2 Feedline Flanges
- LO_2 Feedline Support Brackets
- LO_2 to Intertank Flange Closeout
- Aft Attach Hardware
- LH_2 PAL Ramp
- LH_2 Tank Ice/Frost Ramps
- GO_2 Pressline Support Bracket
- Bipod Jack Pad Closeout

1 Cause for Engine Mounted Heat Shield Ice

1 Cause for Protective Barriers

1 Cause for BSM Products

1 Cause for SRB Separation Products

Hazard Report IDBR-01

The likelihood of Orbiter Tile impacts from ET foam located on the LO_2 Tank Acreage (IDBR-01-H), Intertank Acreage (IDBR-01-K), LH_2 Tank Acreage (IDBR-01-N), Aft Attach Hardware (IDBR-01-AR), LH_2 Pal Ramp (IDBR-01-AL), LH_2 Tank Ice/Frost Ramps (IDBR-01-W), GO_2 Pressline Support Bracket (IDBR-01-AO), and Bipod Jack Pad Closeout (IDBR-01-AQ) is classified as remote due to minor uncertainties in the bounding analysis cases and the foam application/process. The likelihood of Orbiter Tile impacts from foam from the LO_2 to Intertank Flange Closeout (IDBR-01-AC) is classified remote due to minor uncertainties in the foam application/process and the probability of an impact not exceeding the capability of the tile.

Assessing Risk from the PAL Ramps

Risk of Ascent Debris Impact

(HAZARD SEVERITY LEVEL AND LIKELIHOOD OF OCCURRENCE WITH CONTROLS IN PLACE)

	MARGINAL	CRITICAL	CATASTROPHIC
PROBABLE			
INFREQUENT			13
REMOTE			31
IMPROBABLE			32

Window Impacts

1 Cause for the RCS Tyvek Cover

1 Cause for ET Ice

RCC Impacts

12 Foam Causes

- LO_2 Tank Acreage
- Intertank Acreage
- LH_2 Tank Acreage
  - LO_2 Feedline
  - LO_2 Feedline Flanges
  - LO_2 Feedline Support Brackets
- Intertank Ice/Frost Ramps
- LH_2 Tank Ice/Frost Ramps
- LH_2 to Intertank Flange Closeout
- LO_2 PAL Ramp
- LH_2 PAL Ramp
- LO_2 Tank Ice/Frost Ramps
- LO_2 to Intertank Flange Closeout
- GO_2 Pressline Support Bracket
- Bipod Closeout Foam

1 Cause for the RCS Tyvek Cover

1 Cause for Feedline Bellows Ice

1 Cause for Feedline Bracket Ice

1 Cause for BSM Plume Constituents

Tile Impacts

1 Cause for the RCS Tyvek Cover

1 Cause for SRB Froth-Pak Foam

4 Foam Causes

- LO_2 PAL Ramp
- LH_2 to Intertank Flange Closeout
- Bipod Closeout Foam
- LH_2 Aft Dome

Special Tile Impacts

(Umbilical/Landing Gear Doors)

1 Cause for SRB Froth-Pak Foam

4 Foam Causes

- LO_2 PAL Ramp
- LH_2 to Intertank Flange Closeout
- Bipod Closeout Foam
- LH2 Aft Dome

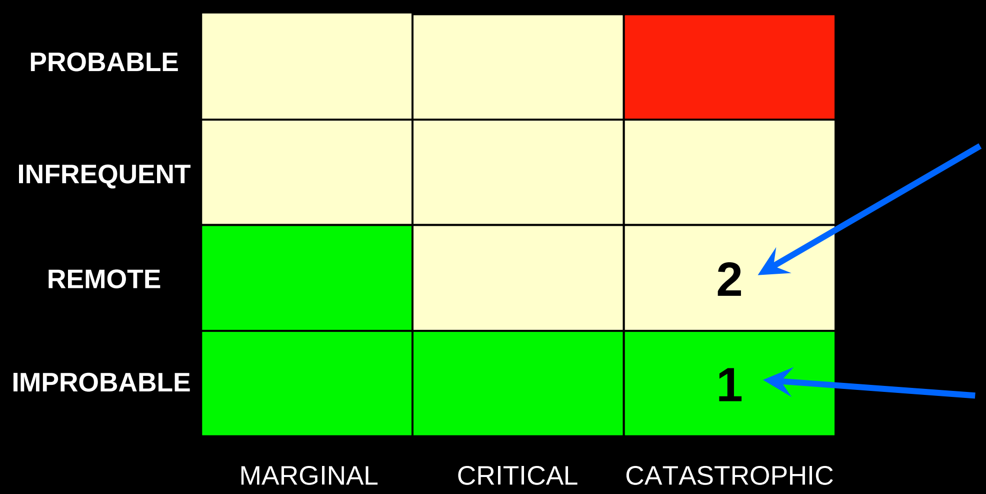
1 Cause for the RCS Tyvek Cover

General Causes

1 Cause <0.0002 lbm

1 Cause for Error in Debris Transport Analysis

LH2 PAL Ramps Risk Assessment
June 2005



Tile Impacts (All)

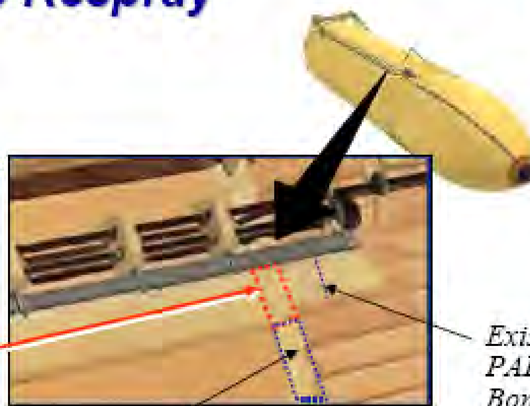
RCC Impacts
- **Probability of exceeding impact capability is 1 in 10,000**

Flight Rationale:
- Replaced forward 10 ft. of LH2 PAL ramp with enhanced, verified and validated TPS spray process.
  - Void count has been significantly reduced due to the process improvements.
- PAL Ramps are low complexity single sprays which reduce the likelihood of creating critical defects.
- LH2 PAL Ramp TPS application is defined as a High Confidence Process Control item per the RTF TPS Integrated Process Control Plan.
  - Plug pull and density data indicate that the process is stable and repeatable.
  - Critical performance requirements are verified by as-sprayed acceptance testing.
- The probability of exceeding the tile impact capability is bounded by the analysis performed for the LO2 PAL Ramps.
  - Aft Location results in lower impact energy.

Systems DCR, April 2005

Partial LH2 PAL Ramp Respray

- *Change*
  - Replace forward 10 ft. of LH2 PAL ramp with enhanced, verified and validated TPS process
- *Reason for Change*
  - Required to access underlying flange closeout
    - Design unchanged



- *Details of Change*
  - Replaced PAL ramp section using process recommendations and enhancements identified by the TPS Working Group and the Manual Spray Enhancement Team (MSET)
    - Removed and replaced GO2 and GH2 pressline sections and top half of forward LH2 ice/frost ramp
    - PAL ramp bondline relocated
    - Outer mold line unchanged
  - Closed out plug pulls with verified and validated repair method

ET-120 LH2 PAL Ramp Fwd 10 ft. Re-spray

Systems DCR, April 2005

Partial LH2 PAL Ramp Respray

- *Certification Summary*
  - Demonstration
    - Manual spray process verified / validated on full-scale article
      - Pre-control used to establish process performance requirements
      - As-sprayed acceptance testing used to verify critical performance requirements
        - Tensile strength, dissections, and density tests performed and inspected on HFPTA and/or witness panels
  - Tests / Analyses
    - Test-based verification demonstrates FS > 1.25 for critical failure modes
      - Outer Fiber Cracking / Bondline Delamination
        - Cryogenic / Flexure testing demonstrates 125% design limit structural flexure induced loading
      - Cohesive Strength
        - Min. MS = 0.25 (SF req'd = 1.25) using maximum observed defect size x 1.40
        - Critical max. observed defect size is 0.40 in. slot width
  - Non-destructive inspection (using development techniques) of existing and replace PAL ramps showed no defects in excess of criteria dimension acceptance criteria

Systems DCR, April 2005

Hazard Summary

- *Acceptance Rationale - T.02, Loss of ET Thermal Protection System*
  - Design Verification

Rationale: Empirically derived defect acceptance criteria based on cohesive failure due to internal voids, cryoingestion, and cryopumping testing of conservatively engineered voids

Material Specific Determination of Critical Defect Size (Acceptance Criteria)

Rationale: Flight hardware dissections used to characterize TPS internal foam structure and indicate defect dimensions/ locations for non-redesigned applications

Maximum Expected Critical Defect Size

Part-Specific/ Environment Specific Assessment (e.g. local temp effects)

OK?

Y: *Proceed with remaining assessment*

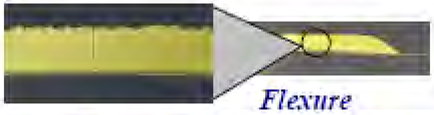
N: *Further Action Req'd*

Rationale: Flight history performance used to confirm that performance was consistent with results of verification. Confirms that non-redesigned areas of the tank were at a relatively lower risk to lose TPS under flight environments

Systems DCR, April 2005

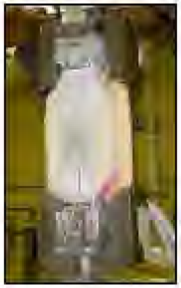
Hazard Summary

- *Acceptance Rationale - T.02, Loss of ET Thermal Protection System*
  - Design Verification (cont'd)
    - Cryogenic panel tests (cryoflex, combined environments) testing performed to demonstrate critical load environments (mechanical strain >125% DLL, TPS temperature) for bondline delamination failure mode
    - Configuration specific tests performed for PAL ramp applications to demonstrate >125% of DLL flexure for the outer fiber cracking failure mode
    - Wind tunnel performance testing performed to demonstrate design capability for design certification aero and aero thermal load environments
    - Flat panel and system level thermal / vacuum testing performed to verify critical load environments for cohesive strength failure mode (divoting) (Delta P, TPS temperature) - *New for RTF*
  - Personnel training / certification
    - Personnel performing TPS spray operations were certified TPS technicians or were allowed to apply TPS through On-the-Job Training (OJT)
      - Applications identified as suspect during Personnel Certification Investigation were assessed and dispositioned (Remove/replace of UAI)
        - UAI dispositions based on no flight hardware impact, acceptance testing, or certified QC witness/inspection
      - All personnel certification issues cleared for ET-120



Flexure

PAL Ramp Capability



Cryoflex

System (Flange) Thermal/Vac

Systems DCR, April 2005

Hazard Summary

- *Acceptance Rationale - T.02, Loss of ET Thermal Protection System*
  - TPS Debris Verification Summary

Max possible shows positive margins against SSP/SE&I TPS Debris Requirements

Hardware	Expected Debris using Max heating rates (< .0002 lbm): Popcorning	Expected Debris using Max heating rates (< .0002 lbm): Ablation	Observed Flight Performance Mass (lbm) Attributed to Defects Inherent to the Process: Popcorning /Ablation	Observed Flight Performance Mass (lbm) Attributed to Defects Inherent to the Process: Other	Debris Req.	Max Possible (Ult. SF= 1.25)
LO2 Tank Acreage - NCFI 24-124 Foam	✓	✓	✓ A	None	0.023	0.003
LO2 Ice/Frost Ramps - PDL-1034 Foam		✓		0.007	0.023	0.017
LO2 PAL Ramp- BX-250 Foam		✓		None	0.023	0.013
LO2-I/T Flange - BX-250 Foam		✓		None	0.026	0.026
Intertank Acreage- NCFI 24-124 Foam	✓	✓	✓	0.004	0.030	0.004
Bipod – BX-250/BX-265		✓		Redesigned	0.030	0.025
I/T Ice Frost Ramps - BX-250/BX-265/PDL-1034		✓		None	0.030	0.017
LH2-I/T Flange - BX-265/BX-250 Foam		✓		Redesigned	0.030	0.010
LH2 Tank Acreage - NCFI 24-124 Foam	✓	✓	✓	Individual pieces <.004 (Collateral Damage)	0.030-0.075	0.004
LH2 Ice/Frost Ramps - PDL-1034 Foam		✓		None	0.030 – 0.075	0.008
LH2 PAL Ramp - BX-250/BX-265/PDL-103		✓		None	0.030	0.023
LO2 Feedline Flange - BX-250/BX-265/PDL-1034		✓	✓ A	0.011	0.030	0.011
Longeron - BX-250/BX-265/PDL-1034		✓		Redesigned	0.075	0.035
Thrust Strut - BX-250/BX-265/PDL-1034		✓		0.004	0.072	0.005
Aft I/F Hardware - BX-250/BX-265/PDL-1034		✓	✓ A	0.016	0.075	0.037
LH2 Aft Dome Acreage - NCFI 24-57/BX-250/BX-265/PDL 1034	✓	✓	✓	None	N/A	0.004

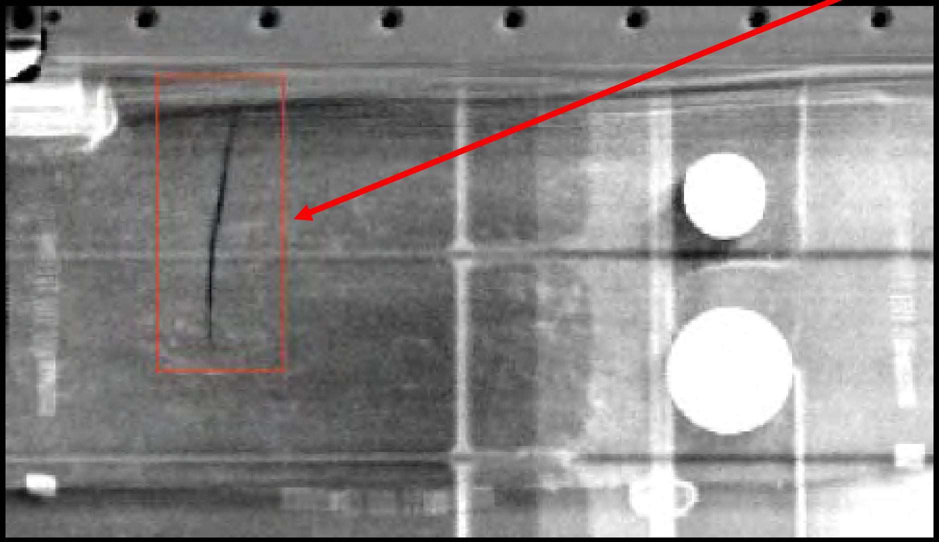
Post-STS-114

- Following STS-114, the Program shipped two tanks back to the factory for destructive and non-destructive inspection.
- Both had been modified in similar ways.
- One tank had not been through tanking and thermal cycles; it showed no cracks.
- The other tank had been through two tanking cycles….

Post-Flight Analysis

ET-120 PAL
Ramp Foam
dissection
showed
significant cracks

Post-Flight Analysis



- NDE of tank after thermal cycle also showed significant defects in the foam on the PAL Ramps.
- These defects could have resulted in critical foam loss during launch.
- This represents a previously unknown foam failure mechanism.
- Because it was unknown, it was not accounted for in our risk assessments.

What Did We Miss?

- Our mistake was that we did not understand the failure mechanism that drives foam loss.
- As a result, we did not accurately capture the risk.
- The RM system is only as good as the engineering that informs it.
- The RM system can also lead to the illusion that we have a comprehensive portrait of program risk when we don't.

Lessons

- We will never have enough missions that flight will become routine, nor will we ever have a comprehensive, exhaustive understanding of the flight systems and environments.
- Engineers and Program & Project Managers need to acknowledge and preserve their “ignorance” about the vehicle systems and remain humble before those systems.

Lessons

- As a result, we will have to
  - Keep questioning the performance of the vehicles and looking for unidentified risks
  - Define what we mean by acceptable risk
  - Demonstrate that we have sufficient confidence in our risk assessments to get there
  - Respond appropriately to failure by learning from our mistakes; preserving those lessons; and continuing our mission

All of the serious accidents in the history of human space flight were due to a failure by the community to recognize the real risks.

Reenactment of Frank Borman testimony before the Senate committee reviewing the Apollo 1 Fire

from “From the Earth to the Moon”

The cause of the accident was a failure of imagination