Creating a World Class Safety Culture

Lessons Learned from Launch Vehicle Failures

Stan Graves

NESC Academy Webcast

January 20, 2020

QuantiTech

Introduction

I was Chief Engineer for the Space Shuttle RSRM from 1995 to 2005

- Supported more than 50 Space Shuttle launches in Florida
- Perhaps spent more time in front of the Mission Manage Team at Level I FRRs than anyone (we had a lot of technical issues, and the MMT Chair was leery about having solid rocket motors on manned space launch vehicles)

Purpose

- Change culture from "*sell management*" on safe to fly versus "*share the risk*"
- Change culture from *being silent* to one that fosters robust debate and discussion
- Introduce the notion of "Normalization of Deviance": the process by which hardware that does not meet design intent is accepted as "normal".

Challenger and Columbia Disasters
A Personal Retrospection*

**Reference:*

"**Creating a World Class Safety Culture: Lessons Learned from Launch Vehicle Failures and Industrial Accidents**"

Stan Graves, Senior Director, Orbital ATK

64th JANNAF Propulsion Meeting
May 22, 2017

January 28, 1986 - Challenger Liftoff 11:38 a.m.

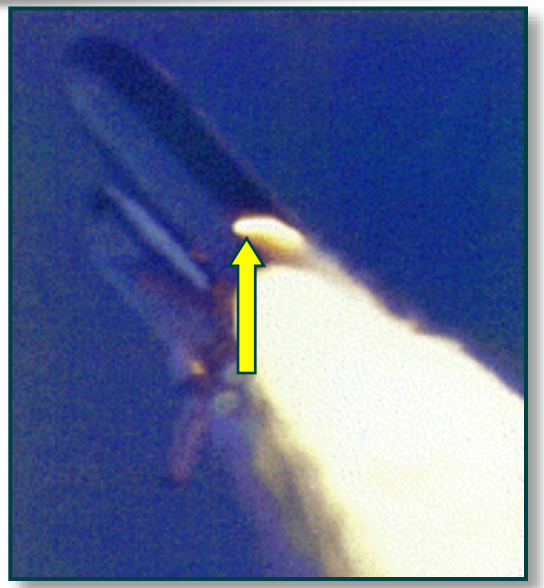
Liftoff

Leak at T + 0.678 Seconds

MAXIMUM DYNAMIC PRESSURE AND WIND SHEAR

Joint Leak Restarts

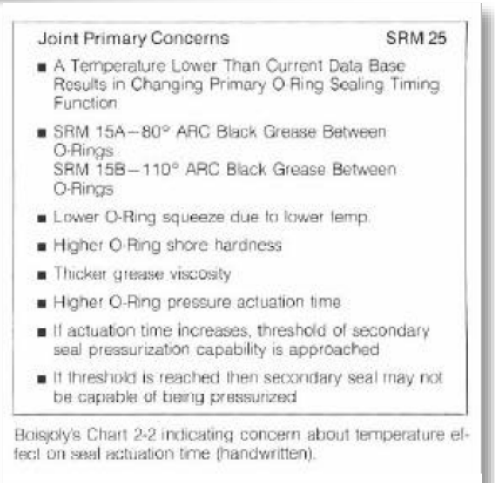
T + 59 Seconds



Explosion

T + 76 Seconds

Evening of January 27, 1986

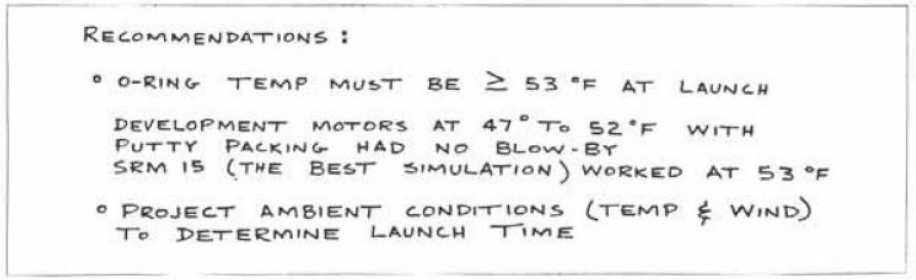


Joint Primary Concerns — SRM 25

- A Temperature Lower Than Current Data Base Results in Changing Primary O-Ring Sealing Timing Function
- SRM 15A—80° ARC Black Grease Between O-Rings
  SRM 15B—110° ARC Black Grease Between O-Rings
- Lower O-Ring squeeze due to lower temp
- Higher O-Ring shore hardness
- Thicker grease viscosity
- Higher O-Ring pressure actuation time
- If actuation time increases, threshold of secondary seal pressurization capability is approached
- If threshold is reached then secondary seal may not be capable of being pressurized

Boisjoly's Chart 2-2 indicating concern about temperature effect on seal actuation time (handwritten).

8:45 p.m.: O-ring temp must be ≥ 53 °F at launch



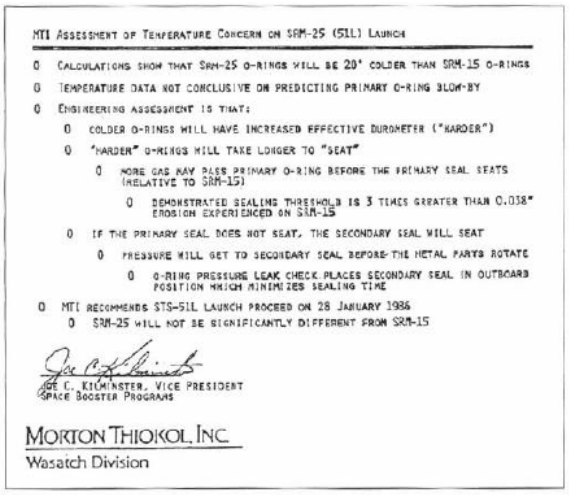
RECOMMENDATIONS :

- O-RING TEMP MUST BE ≥ 53 °F AT LAUNCH

  DEVELOPMENT MOTORS AT 47° TO 52°F WITH PUTTY PACKING HAD NO BLOW-BY
  SRM 15 (THE BEST SIMULATION) WORKED AT 53 °F

- PROJECT AMBIENT CONDITIONS (TEMP & WIND) TO DETERMINE LAUNCH TIME

Initial Thikol recommendation Chart presented by Robert K. Lund at second teleconference prior to Thiolol caucus.



MTI ASSESSMENT OF TEMPERATURE CONCERN ON SRM-25 (51L) LAUNCH

- CALCULATIONS SHOW THAT SRM-25 O-RINGS WILL BE 20° COLDER THAN SRM-15 O-RINGS
- TEMPERATURE DATA NOT CONCLUSIVE ON PREDICTING PRIMARY O-RING BLOW-BY
- ENGINEERING ASSESSMENT IS THAT:
  - COLDER O-RINGS WILL HAVE INCREASED EFFECTIVE DUROMETER ("HARDER")
  - "HARDER" O-RINGS WILL TAKE LONGER TO "SEAT"
    - MORE GAS MAY PASS PRIMARY O-RING BEFORE THE PRIMARY SEAL SEATS (RELATIVE TO SRM-15)
      - DEMONSTRATED SEALING THRESHOLD IS 3 TIMES GREATER THAN 0.038" EROSION EXPERIENCED ON SRM-15
  - IF THE PRIMARY SEAL DOES NOT SEAT, THE SECONDARY SEAL WILL SEAT
    - PRESSURE WILL GET TO SECONDARY SEAL BEFORE THE METAL PARTS ROTATE
      - O-RING PRESSURE LEAK CHECK PLACES SECONDARY SEAL IN OUTBOARD POSITION WHICH MINIMIZES SEALING TIME
- MTI RECOMMENDS STS-51L LAUNCH PROCEED ON 28 JANUARY 1986
  - SRM-25 WILL NOT BE SIGNIFICANTLY DIFFERENT FROM SRM-15

JOE C. KILMINSTER, VICE PRESIDENT
SPACE BOOSTER PROGRAMS

MORTON THIOKOL, INC.
Wasatch Division

Copy of telefax sent Kennedy and Marshall centers by Thiokol detailing the company's final position on the January 28 launch of mission 51-L.

"My God, Thiokol, when do you want me to launch, next April?"
Larry Mulloy

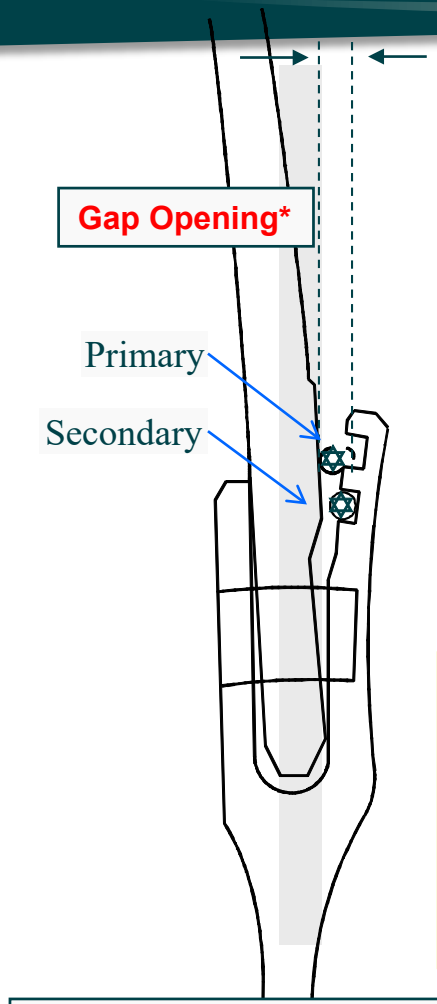
"I'm appalled."
George Hardy

"Bob, take off your engineering hat and put on your management hat."
Jerry Mason.

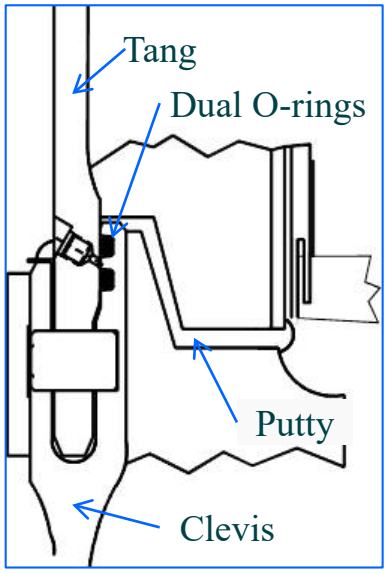
11:00 p.m.: "MTI recommends STS-51L launch proceed on 28 January 1986"

- **How and why did this happen?**
- **What would I have done if I had been the Engineering vice president in 1986?**

Field Joint Design Overview

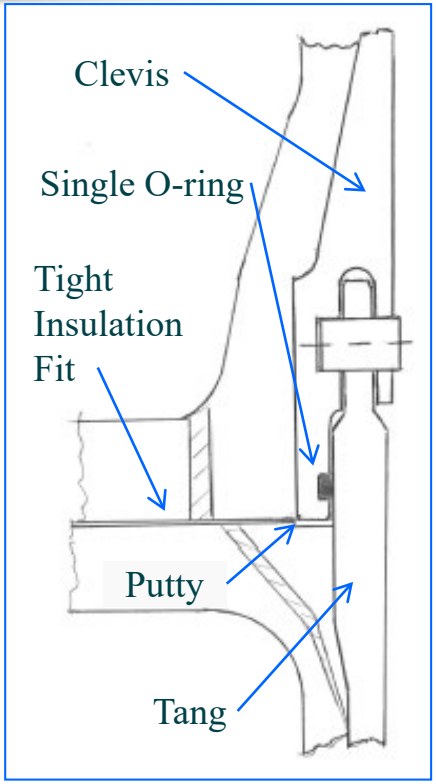


Pressurized Joint: Rotation Effect (exaggerated)



Shuttle SRM

- Dual O-rings
- Leak check port
- Putty thermal barrier
- Clevis facing up
- No heater strip



Titan IIIC Clevis

- Single O-ring
- Tight insulation fit
- Clevis facing down
- Heater strip
- *Over 1,000* successful joints flown

Space Shuttle SRM clevis field joint design based on successful Titan IIIC design, circa 1972

*Early finite element models used nodal constraints to attach the tang to the clevis. Improper radial constraints made the joint appear static.

Development Program 1973 - 1980

Contract Award 11/20/1973
DM-1 7/18/1977
Hydroburst Test **9/1977**
DM-2 1/18/1978
DM-3 10/19/1978
DM-4 2/17/1979
QM-1 7/13/1979
QM-2 9/27/1979
QM-3 2/13/1980

Because the static test motors were assembled horizontally, Thiokol was worried that the assembled condition would result in a different configuration than the vertical assembly at Cape Kennedy

- Visible gas path or blow holes in the **putty were tamped** tight in all static test motors via personnel entry into the motor bore
- No hot gas impingement on the O-rings occurred

The **September 1977** hydrotest data showed the *field joints were rotating open to the point* where the O-rings could lose contact with the mating surfaces

- Thiokol did not believe the test results were valid
- This was the beginning of an 8-year debate over the magnitude of the joint gap opening

In October 1977, NASA expressed serious concerns **that the field joint did not meet the design intent** (dynamic sealing versus static sealing), and **recommended a redesign**

The design certification review completed in **September 1980** concluded:

- Design has adequate margins with updated design: Larger O-rings, thicker shims
- The joint has been sufficiently verified with Titan IIIC history, lab scale tests, a full-scale structural test article, and 7 static tests

1981 - 1983

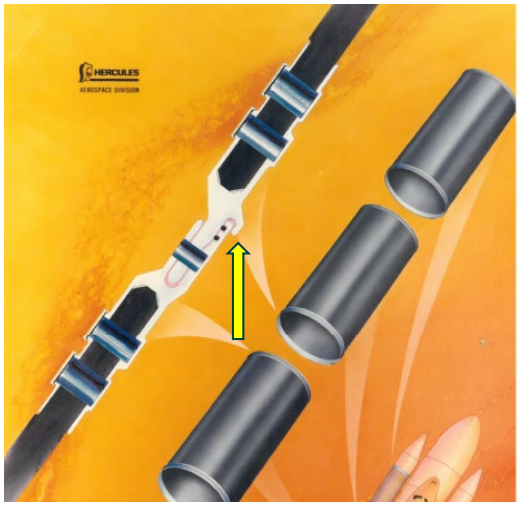
STS-1 4/12/1981
STS-2 11/12/1981 *0.053 in. erosion at **70°F***
STS-3 3/22/1982
STS-4 6/27/1982
DM-5 10/21/1982
STS-5 11/11/1982
QM-4 3/21/1983
STS-6 4/4/1982
STS-7 6/18/1983
STS-8 8/30/1983
STS-9 11/28/1983

STS-2: 0.053 in. *primary O-ring erosion* on right SRB aft field joint due to "blow holes" in the putty

- Flight rationale
  - Bounding case shows max possible erosion 0.090 in.
  - Thermal environment is self-limiting – heating stops when free volume is filled
  - O-ring with 0.095 in. simulated erosion sealed at 3,000 psi (3x design operating pressure)
  - Design has adequate margin

May 1982: NASA starts development program for a graphite/epoxy Filament Wound Case (FWC)

- Higher performance motors needed for DoD missions requiring polar orbits out of Vandenberg
- Design includes a "capture feature" to limit joint rotation



1984 – May 1985

Note that each time the hardware performance got worse, it was accepted and became the new basis for "in-family". Diane Vaughn called this "Normalization of Deviance".

STS-41B
2/3/1984
*Erosion at **57°F***

STS-41C
4/6/1984
*Heat affect at **63°F***

STS-41D
8/30/1984
*0.026 in. erosion at **70°F***

STS-41G
10/5/1984

DM-6 (FWC)
10/25/1984

STS-51A
11/8/1984

STS-51C
1/24/1985
*Blow-by in 2 joints with heat-affected secondary seal at **53°F***

STS-51D
4/12/1985

STS-51B
4/29/1985

O-ring erosion recurs on STS-41B, 41C, and 41D

- Flight rationale
  - Observed erosion less than previous worse case (STS-2)
  - Motors are in-family; erosion on future motors possible
  - Bounding case shows max possible erosion 0.090 in.
  - Thermal environment is self-limiting
  - O-ring with 0.095 in. erosion sealed at 3,000 psi
  - Design has adequate margin

"100-year Cold Spell" for three days prior to STS-51C

- Nighttime temperatures ranged 17 to 22 °F
- Launch delayed one day because temps were below freezing
- *No one raised concerns about cold temperature effects*
- It doesn't get cold in Florida, right?

A new worst case event occurs on STS-51C - blow-by of 2 primary O-rings with heat- affected secondary O-ring

- Flight rationale
  - Cold temperature effects: putty becomes stiffer, O-ring becomes harder, O-ring squeeze reduced
  - Low temperature enhances probability (STS-51C coldest in history)
  - Erosion within experience base and within established margins
  - Secondary seal in proper position via leak check
  - Secondary O-ring is redundant
  - STS-51D could exhibit the same behavior.
  - Condition is not desirable, but is acceptable

June 1985 - January 1986

DM-7 (FWC) 5/9/1985	• In mid-1984, the design team began a 27-month development program to fix the seal erosion problems. One solution: eliminate the putty. • **July 1985 -** Forgings put on order to incorporate a capture feature on steel case segments
STS-51G 6/17/1985	
STS-51F 7/29/1985	• **August 19, 1985 –** 54-page presentation on O-ring issue at NASA HQ • "*….secondary seal may not seal the motor*" • "…ways to eliminate joint rotation should be incorporated *as soon as possible*" • "Efforts need to continue *at an accelerated pace*" • No mention of cold temperature concerns • Recurrence of a "100-year" cold day viewed an improbable event
STS-51I 8/27/1985	
STS-51J 10/3/1985	• Events in family of previous experience; no change in flight rationale
STS-61A 10/30/1985 *Primary O-ring blow-by in 2 joints at **75°F***	
STS-61B 11/26/1985	• **STS-61C** was scrubbed 4 times; Temps below 53°F for each day • Temperatures were in the *low 40s* on the first scheduled launch attempt • No concerns about temperature were raised
STS-61C 1/12/1986 *Erosion at **58°F***	
STS-51L 1/28/1986 *Total joint failure at ≤28°F*	• January 26 - Launch delayed due to weather - rain and high winds • January 27 - Launch delayed due to faulty latch handle • January 27 midday - NASA's Larry Wear called Thiokol, "*What did we say about STS-51C and potential cold temperature effects*?" "*Any concerns*?"

It's All About the Putty

Discussions prior to Challenger were all about the O-rings

Post-Challenger testing revealed *unknown variation* in the putty performance

Pre-Challenger assertion

- Putty is plastic and will flow into the joint acting like a hydraulic ram to seat the primary O-ring

Post-Challenger discovery

- *The putty **can maintain motor pressure;*** consequently the O-rings are not pressurized
- ***Pressure** flow through putty blow holes **can be delayed** during the ignition transient. Tests showed:*
  - *Pressure was delayed for 530 milliseconds at 75°F*
  - *Pressure was delayed for 1.9 seconds in a test at 20°F*

Consequences of pressure delays

- The primary O-ring ***will** be* unseated at room temperature
- The secondary O-ring will seal consistently down to 55°F
- The secondary O-ring **can** seal (intermittently) down to 30°F
- The secondary O-ring *will* consistently *fail* at temperatures below 30°F

Primary seal requires pressure-assist to seal.

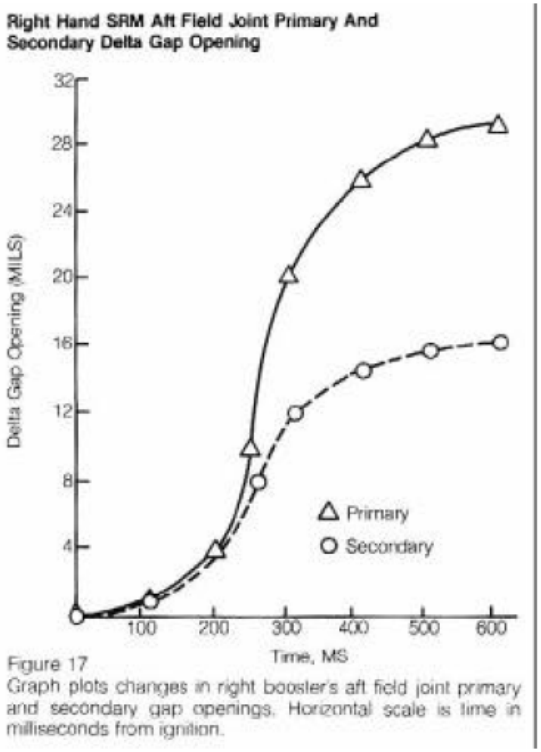
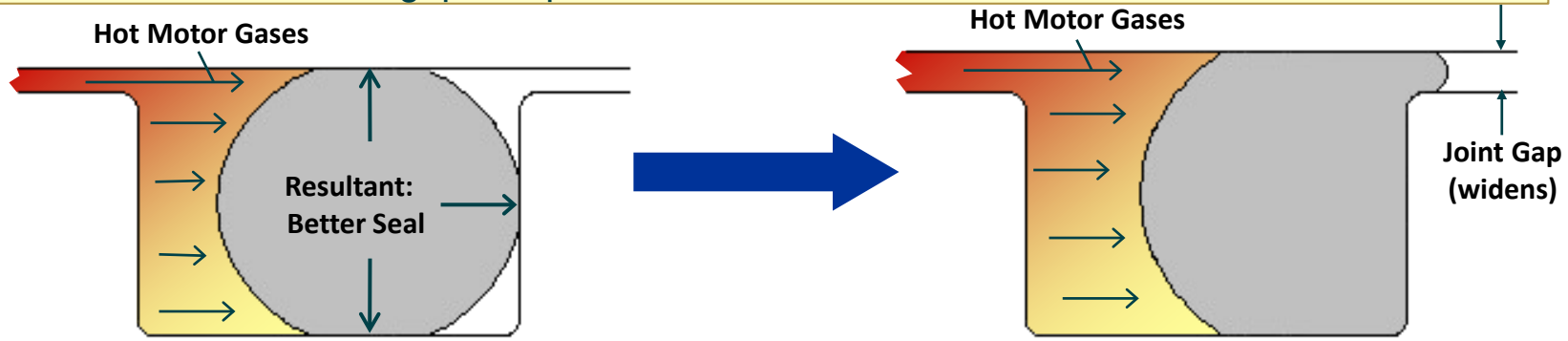


Figure 17
Graph plots changes in right booster's aft field joint primary and secondary gap openings. Horizontal scale is time in milliseconds from ignition.

Gap Opening vs Time
Primary and Secondary Seals

4-Wall Contact

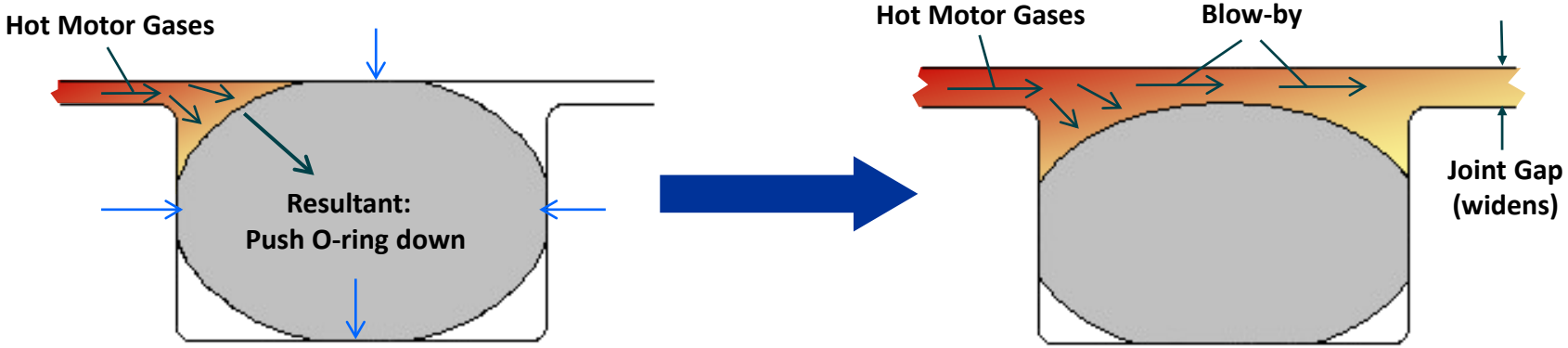
Prior to Challenger, it was believed that the secondary O-ring would be in a position to be forced into the extrusion gap via “pressure assist”



O-ring as Pressurization Begins: Desired Configuration

O-ring After Pressurization: No Blow-by

After Challenger, it was learned that design changes to create ever greater O-ring squeeze could result in “4-wall” contact resulting in potential blow-by of both the primary and secondary O-rings *at any temperature*



O-ring as Pressurization Begins: 4-wall Contact

O-ring After Pressurization: Blow-by Occurs

Outcomes for Various Putty Configurations

Event	Frequency	Primary Seal Outcome	Secondary Seal Outcome
No gas paths in putty (Unknown that putty could hold pressure)	**140**	No hot gas to O-ring, system seals at any temperature	No hot gas to O-ring, system seals at any temperature
Gas paths with *instant pressure* to primary O-ring	**5** STS-2 at 70°F STS-41B at 57°F STS-41C at 63°F STS-41D at 70°F STS-61C at 58°F	Impingement erosion on primary O-ring. Seals will function well below 30°F. Bounded and self limiting condition.	No gas to the secondary seal
Gas paths with *instant pressure* to the primary O-ring, *but O-ring has 4-wall* contact (Unknown domain prior to Challenger)	**2?** STS-61A at 75°F?	Blow-by and erosion of primary O-ring can occur at room temperature	Secondary seal can function below 30°F with no 4-wall contact Secondary can fail at **room temperature** with 4-wall contact
Gas paths with *pressure* to primary O-ring *delayed* by 250 – 500+ ms (Unknown domain prior to Challenger)	**3?** STS-51C at 53F°? **STS-51L at ≤28°F**	Blow-by and erosion of primary can occur at room temperature	1. Secondary will seal down to 55°F 2. Intermittent secondary seal failure 30 to 55°F 3. Secondary seal failure below 30°F

O-ring Damage vs Temperature: Complete Data Set

Why didn't management believe there was a temperature effect on O-ring damage?

Condition	Flight	Temp	Comments
Impingement Erosion	STS-2 STS-41D STS-41C STS-61C STS-41B	70F 70F 63F 58F 57F	In models used to predict bounding, worst case erosion, temperature has no effect on the physics of impingement erosion. O-ring damage is controlled by fill volume and gas path dimensions.
Blow-by and Erosion of Primary O-ring	STS-61A STS-61A STS-51C STS-51C	75F 75F 53F 53F	We know today that low temperature affects O-ring resiliency, but this is all the data available to management on the evening of January 27, 1986

They had 9 data points to look at. Frequency and damage at room temperature were indistinguishable from that at lower temperatures, albeit the damage on -51C was worse….

(Side note. 5 of the 6 joints on STS-51L worked fine at <28F. If the aft field joint didn't have a gas path, the total data set would have included 6 successes at very low temperatures.)

What Did We Learn After the Accident?

Prior to the accident, neither NASA nor Thiokol fully understood the mechanism by which the joint sealing function took place

The design was unacceptably sensitive to a number of factors

- Temperature
- Physical dimensions
- Character of materials
- Effects of reusability
- Processing and handling
- Complex interactions due to joint dynamic loading

Ironically, design fixes (like the capture feature and putty modifications) were on the way and would have been incorporated by mid-1986

Management thought that they had a little more time….

Personal Retrospection:

The launch rate in 1985 and 1986 is incomprehensible

- 13 launches and 2 static tests in a 15 month period. *Holy Cow*!
- STS typically launched 4 to 6 times a year (8 maximum one year)
- The pace to keep up with post-flight results and resolve technical issues prior to each subsequent launch was incredible

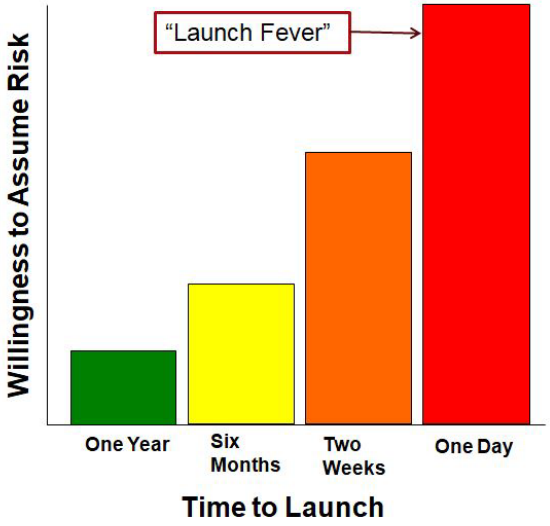
Schedule pressure to keep flying in 1986 must have been palpable

- Months before a launch, the design team is very risk adverse
  - *Adverse events are anticipated and Launch Commit Criteria (LCC) are vetted*
  - *Tendency is to anticipate and define when not to fly*
- Risk taking (launch fever) gets intense as the next launch date approaches
  - *Tendency is to find a reason to fly*

What would I have done..?

- Engineering team had been saying it was safe to fly for over 4 years
- Engineering team had not put much work into understanding cold temperature effects
  - *100-year storms only occur every 100 years…. It doesn't get cold in Florida*
- Their attempt to establish a new LCC at 53°F the evening before a launch was ill timed and their concerns about cold temperatures were not technically well-founded

I certainly would have challenged the team and their logic…



Columbia Disaster: Bipod Ramp Foam Loss

Foam loss has never been a "Safety of Flight" issue

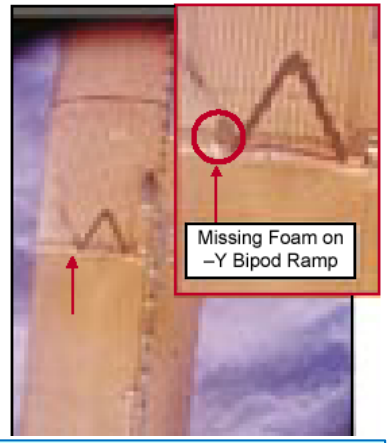
***Columbia* – 1 February 2003**

SPACE SHUTTLE PROGRAM
Space Shuttle Projects Office (MSFC)
NASA Marshall Space Flight Center, Huntsville, Alabama

STS-112/ET-115 Bipod Ramp Foam Loss

Presenter: Jerry Smelser, NASA/MP31
Date: October 31, 2002
Page 3

- **Issue**
  - Foam was lost on the STS-112/ET-115 –Y bipod ramp (≈4" X 5" X 12") exposing the bipod housing SLA closeout
- **Background**
  - ET TPS Foam loss over the life of the Shuttle Program has never been a "Safety of Flight" issue
  - More than 100 External Tanks have flown with only 3 documented instances of significant foam loss on a bipod ramp



The Mission Management Team wasn't concerned about the impact*.

"Like hitting a Styrofoam cooler with your car…"

Except, the car is going 550 miles per hour, and the chunk of foam weighs 1.7 pounds

*Why the Mission Management Team wasn't completely puckered by the foam impact on ignition is baffling to me. They knew the mass and velocity of the foam at impact. A simple kinetic energy calculation would show that the impact energy was 2 orders of magnitude higher than that required to damage the Orbiter carbon-carbon leading edge.

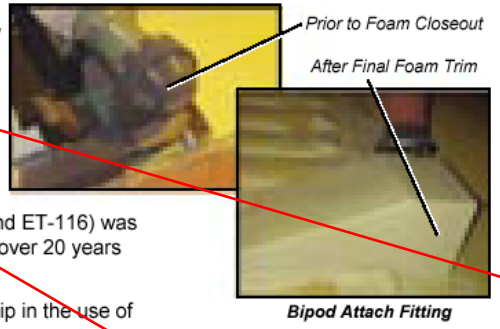
STS-113 Level I FRR (two missions before Columbia)

SPACE SHUTTLE PROGRAM
Space Shuttle Projects Office (MSFC)
NASA Marshall Space Flight Center, Huntsville, Alabama

STS-112/ET-115 Bipod Ramp Foam Loss

Presenter: Jerry Smelser, NASA/MP31
Date: October 31, 2002
Page 4

- **Rationale for Flight**
  - Current bipod ramp closeout has not been changed since STS-54 (ET-51)
  - The Orbiter has not yet experienced "Safety of Flight" damage from loss of foam in 112 flights (including 3 known flights with bipod ramp foam loss)
  - There have been no design / process / equipment changes over the last 60 ETs (flights)
  - All ramp closeout work (including ET-115 and ET-116) was performed by experienced practitioners (all over 20 years experience each)
  - Ramp foam application involves craftmanship in the use of validated application processess
  - No change in Inspection / Process control / Post application handling, etc
  - Probability of loss of ramp TPS is no higher/no lower than previous flights
  - ***The ET is safe to fly with no new concerns (and no added risk)***



"**Not Yet**" implies it *could* experience "Safety of Flight Damage"

- Hazards Analysis identified foam loss as a potentially *catastrophic event*

ET PM cites 3 known foam loss events. Actual number of known events was 5 prior to STS-112.

- He stated that the last event was over 10 years ago, making it sound like the next event wouldn't happen for another 10 years
- Foam loss was deemed "normal".

"Craftsmanship" suggests a finicky process that requires an expert to make it work

There had been design, material, and process changes over the years

Should have said, "*The probability of loss of ramp TPS **on the next flight** is just as high as it was on STS-112.*"

Columbia Disaster: Personal Retrospection

- I was present at the STS-113 FRR when foam loss was presented by NASA ET Project Manager
- The presentation was technically awful
- Members of the FRR board were generally quiet
- NASA HQ S&MA Director began asking flight safety related questions, but quit probing when told that foam loss was an *accepted risk* in the formal hazards assessment system
- When polled, I answered, "**Go**" like everyone else
  - The audience in the room would never challenge other Shuttle elements, and only speak if called on to answer a question
- In the hall outside the conference room, I told NASA's RSRM project manager, "*The foam loss presentation was terrible*! *If I were on the Board, I'd be* '*No Fly*'. He said, "We have to trust the other Shuttle elements to do their job. We've done ours."

A culture of silence existed in the formal FRR setting in 2003

Once an anomaly investigation team determines it is safe to fly, they get into "sell mode", rather than "share the risk mode"

January 21, 2003 email from Mission Management Team Chair to Shuttle Program Manager: "*The ET rational for flight for the STS-112 foam loss was lousy.* ***Rationale was lousy then, and still is.***."

7 Elements of Good Flight Rationale

https://sma.nasa.gov/vids/video-item/return-to-flight

Elements of Good Flight Rationale

STS-51D Flight Rationale (April 1985)

Cause of erosion and blow-by on STS–51C *understood*

O-ring erosion on STS-51C within *experience* base

***Tests* showed O-ring seals at 3,000 psi with 0.095-in erosion**

- *Greater than worst case prediction*
- *Almost twice as great as worst observed in SRM history*

Heat effects on secondary O-ring well below worst case *prediction*

Secondary O-ring sealed by leak check

Erosion and blow-by confirmed to be *self-limiting*

STS-51D could exhibit same behavior as 51C

Note: Central to risk assumption at Level III was notion that record low temps seen for -51C would not occur again

Physics-based understanding

Within experience base

Adequate margins

Assessment based on extensive testing and analysis

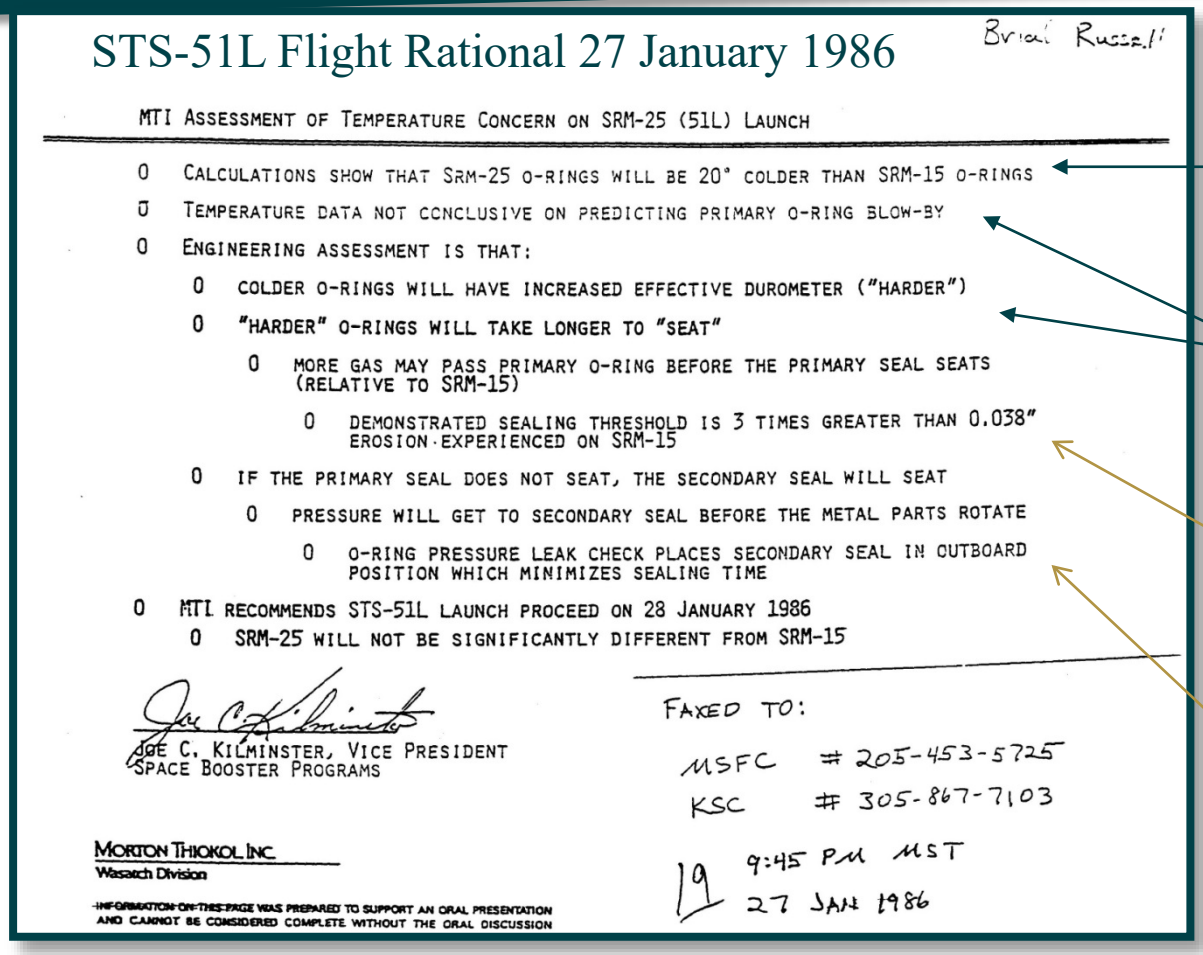
Bounding case

Self-limiting

Diane Vaughn* noticed a consistent pattern in developing rationale for safe flight following each mission

*Diane Vaughn, "*The Challenger Launch Decision*", The University of Chicago Press, 1996.

Elements of Good Flight Rationale



STS-51L Flight Rational 27 January 1986

Brian Russell

MTI ASSESSMENT OF TEMPERATURE CONCERN ON SRM-25 (51L) LAUNCH

- CALCULATIONS SHOW THAT SRM-25 O-RINGS WILL BE 20° COLDER THAN SRM-15 O-RINGS
- TEMPERATURE DATA NOT CONCLUSIVE ON PREDICTING PRIMARY O-RING BLOW-BY
- ENGINEERING ASSESSMENT IS THAT:
  - COLDER O-RINGS WILL HAVE INCREASED EFFECTIVE DUROMETER ("HARDER")
  - "HARDER" O-RINGS WILL TAKE LONGER TO "SEAT"
    - MORE GAS MAY PASS PRIMARY O-RING BEFORE THE PRIMARY SEAL SEATS (RELATIVE TO SRM-15)
      - DEMONSTRATED SEALING THRESHOLD IS 3 TIMES GREATER THAN 0.038" EROSION EXPERIENCED ON SRM-15
  - IF THE PRIMARY SEAL DOES NOT SEAT, THE SECONDARY SEAL WILL SEAT
    - PRESSURE WILL GET TO SECONDARY SEAL BEFORE THE METAL PARTS ROTATE
      - O-RING PRESSURE LEAK CHECK PLACES SECONDARY SEAL IN OUTBOARD POSITION WHICH MINIMIZES SEALING TIME
- MTI RECOMMENDS STS-51L LAUNCH PROCEED ON 28 JANUARY 1986
  - SRM-25 WILL NOT BE SIGNIFICANTLY DIFFERENT FROM SRM-15

JOE C. KILMINSTER, VICE PRESIDENT
SPACE BOOSTER PROGRAMS

FAXED TO:

MSFC # 205-453-5725
KSC # 305-867-7103

19 9:45 PM MST
27 JAN 1986

MORTON THIOKOL INC.
Wasatch Division

INFORMATION ON THIS PAGE WAS PREPARED TO SUPPORT AN ORAL PRESENTATION AND CANNOT BE CONSIDERED COMPLETE WITHOUT THE ORAL DISCUSSION

Out of family

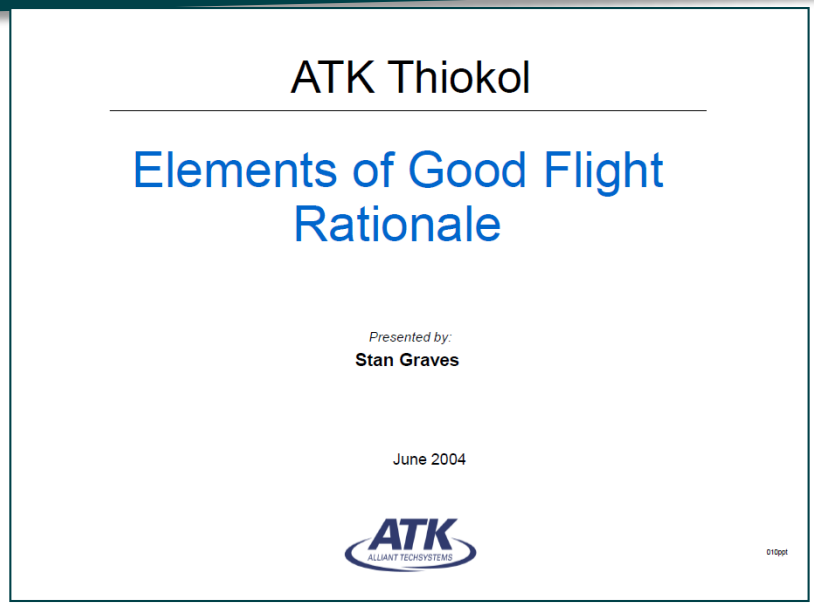
Poor data, physics not understood

Large margins, self limiting

Bounding assessment

A critical assessment of the flight rationale for STS-51L would have revealed several weaknesses that reflected increased risk for the mission

7 Elements of Flight Rationale



ATK Thiokol

Elements of Good Flight Rationale

Presented by:
Stan Graves

June 2004

ATK ALLIANT TECHSYSTEMS

010ppt

After studying the communication breakdown between the engineering teams and the management team on both Challenger and Columbia disasters, I developed a **standard format** for **presenting technical issues** at the **FRR board meeting**

Premise

Use of a *common template* for discussing the basis for safe flight will help *communicate risk* and *identify "holes" or weaknesses in the flight rationale*

- The FRR board should understand quickly the level of risk associated with the issue
- The board should probe and enthusiastically debate those technical issues with varying degrees of unknowns or uncertainties

Conops

The ideal case is to have all six (see next page) elements in place for every technical issue

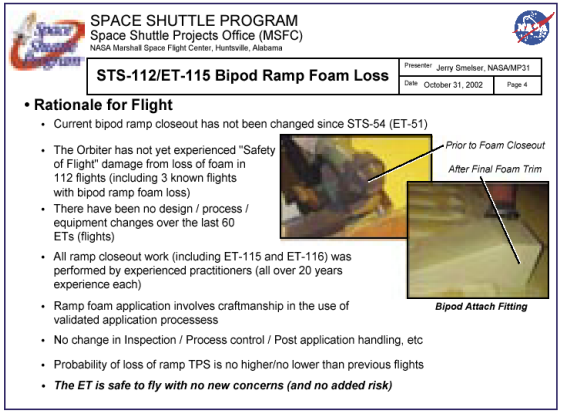
The FRR board can choose to accept the risk and fly without every element being in place, but every element has to be addressed in the presentation

Flight Rationale: Necessary Elements

1. Physics-based understanding
2. Within experience base (flight or test)
3. Adequate margins
4. Bounding case
5. Self limiting
6. Assessment based on data, testing and analysis
7. Interactions with other elements or conditions addressed

Applying the 7 Elements to STS-112 Foam Loss

- **Are physics of foam loss understood?**
  - Charts do not address physics of the problem
- **Is the observation within the experience base?**
  - Yes – prior instances of bipod foam loss with damage to the carbon-carbon leading edge
- **Is there an adequate safety margin?**
  - Charts do not address potential outcomes and margins
- **Has a bounding case been established?**
  - Yes. Loss of vehicle and crew. Accepted risk.
- **Is the observed behavior thought to be self limiting?**
  - Charts do not address potential outcomes and damage limiting rationale
- **Is safe-flight assessment based on data, testing, and analysis?**
  - Charts do not provide engineering data or analysis


SPACE SHUTTLE PROGRAM
Space Shuttle Projects Office (MSFC)
NASA Marshall Space Flight Center, Huntsville, Alabama

STS-112/ET-115 Bipod Ramp Foam Loss

Presenter: Jerry Smelser, NASA/MP31
Date: October 31, 2002
Page 4

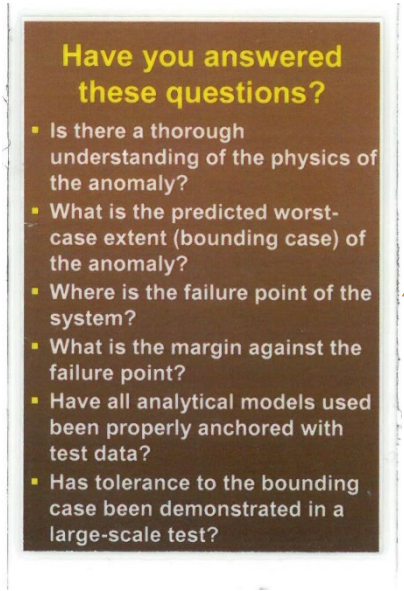
• Rationale for Flight
- Current bipod ramp closeout has not been changed since STS-54 (ET-51)
- The Orbiter has not yet experienced "Safety of Flight" damage from loss of foam in 112 flights (including 3 known flights with bipod ramp foam loss)
- There have been no design / process / equipment changes over the last 60 ETs (flights)
- All ramp closeout work (including ET-115 and ET-116) was performed by experienced practitioners (all over 20 years experience each)
- Ramp foam application involves craftmanship in the use of validated application processess
- No change in Inspection / Process control / Post application handling, etc
- Probability of loss of ramp TPS is no higher/no lower than previous flights
- ***The ET is safe to fly with no new concerns (and no added risk)***

Prior to Foam Closeout
After Final Foam Trim
Bipod Attach Fitting

Risk Assessment or Flight Rationale Elements

Elements of Flight Rationale

1. Solid technical understanding
2. Condition relative to experience base
3. Bounding case established
4. Self-limiting aspects
5. Margins understood
6. Assessment based on data, testing, and analysis
7. Interactions with other elements or conditions addressed



NASA Badge Overlay

Necessary elements, expanded:

1. Physics-based or root cause understanding of issue, based on engineering data (perhaps using a fault tree)
2. Experience base includes full-scale flight, ground test, or qualification-level tests
3. Using physics-based understanding, determine the bounding case (e.g., lower A-basis allowables, upper three sigma loads and environments, anchored with test data)
4. Physical reasons why it can't get any worse than the bounding case or show the part is fail-safe
5. Adequate margins, ideally not substantially reduced from baseline
6. Final risk assessment based on test data and analysis, not gut feel or expert opinion
7. Address interactions with other conditions (MRB, changes, technical issues), and vehicle elements

Nozzle Wedge Shift Issue

Observation

- Leading edge insulator wedge-shift has occurred on static test motors -1 and -2
- No performance anomalies occurred

Concern

- Nozzle is not performing as designed, and technical understanding of phenomenon is not 100% solid

- Two static test nozzles worked, but performance did not meet design intent
- Design Team concluded that the risk of nozzle failure was low, and *recommended that the program proceed without modification*
- ***After seeing the 7 Elements Risk Assessment, Management found the risk to be unacceptable***
  - The nozzle was successfully redesigned

Nozzle Wedge Shift Risk Assessment:

Solid technical understanding?

- Poor physics based understanding. Current models do not predict wedge shifting phenomena.

Condition relative to experience base (flight or test)?

- FT-2 delaminations are bounded by conditions tested in SFT-1 and SFT-2

Margins understood?

- Design intent is to have the ablative rings remain bonded. Wedgeout conditions are much less robust, and consequences are difficult to predict

Bounding case established or condition self-limiting?

- Credible (possible) cases evaluated that result in nozzle failure
  - *Ejection of a 360-degree wedge*
  - *Hot gas flow between the ablative ring and the metal housing*

Assessment based on data, testing and analysis?

- Two static test nozzles with more severe initial conditions worked
- Risk assessment is largely based on empirical observations and expert judgment

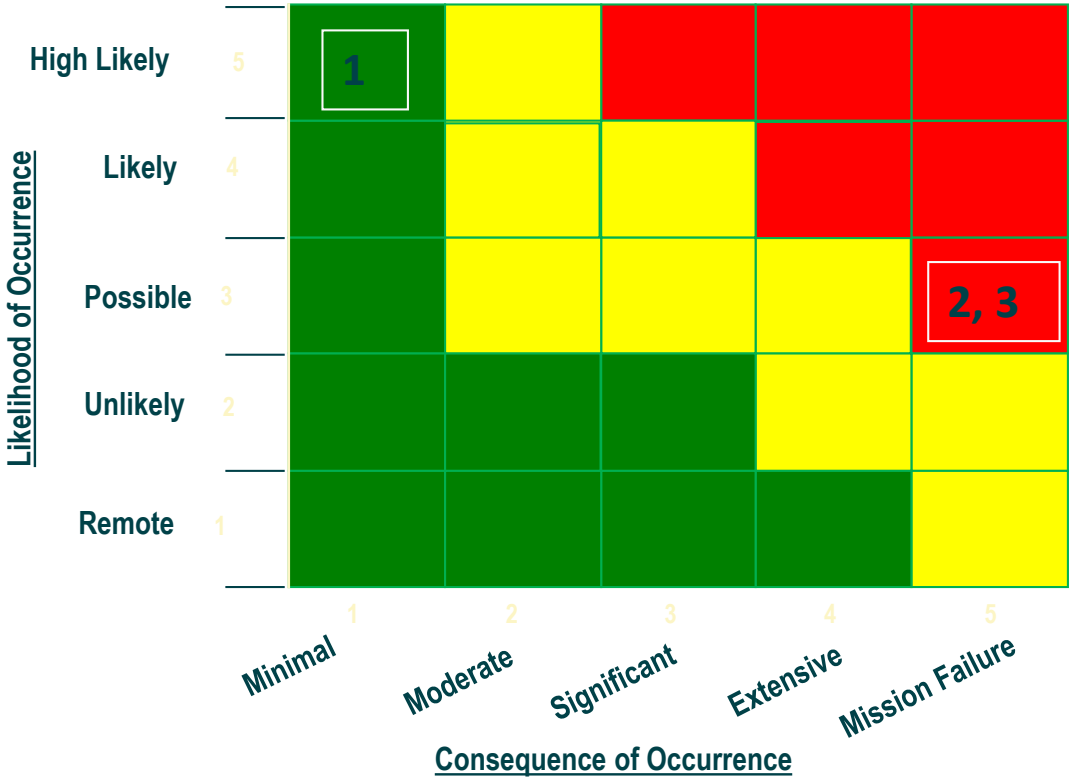
Interactions with other elements or conditions?

- None identified

Nozzle Risk Assessment

Possible Events:

1. Nozzle experiences minor wedge-out
   - Performance similar to SFT-1 and SFT-2
   - **No impact on motor ballistic performance**
2. Delaminations propagate full circumference within a single ply
   - Entire wedge is ejected
   - Nozzle is destroyed
3. Small (7 mil) gap between rings allows hot gas flow to the metal housing
   - Nozzle is destroyed



Nozzle Wedge Recommendation to Management

- Probability of nozzle failure is judged to be low
  - The FT-2 nozzle is enveloped by the SFT-1 and SFT-2 results and any wedge creation is expected to be less severe than previously experienced
  - Expect no effect on ballistic performance
- Nozzle failure is possible
- Failure risk can be mitigated by removing the current nozzle and replacing it with rayon based ablative rings

Based on this risk assessment, the flight nozzle was changed out and flew successfully

Chief Engineer's Council

As I mentioned earlier, a culture of silence existed in the Level I Flight Readiness Reviews

We would often criticize the other element's presentations after the meeting out in the hallway

Every element had significant technical issues:

- Inter-tank foam loss: 100s of hits on the Orbiter tiles
- Missing SSME turbine tip seals
- Payload bay door motors well under specified torque.

We called issues like these the "big rocks"

We formed a cross element Chief Engineers Council to share best practices and flight rationale for the "big rocks"

- Forum provided an opportunity to achieve cross-element technical consensus on the risks that were being shared with the MMT

Broad Area Review

Systemic Causes of 5 Unmanned Launch Vehicle Failures in the Late 1990s

Broad Area Review (BAR)

The "Space Launch Vehicle Broad Area Review (BAR)", chaired by General Larry Welch in November 1999 was established to

- Examine recent launch failures and determine causes of the failures

Delta III 259 (August 26, 1998)

- Vehicle ran out of hydraulic fluid while trying to respond to rocket vibrations

Titan IV B-32 (April 30, 1999)

- Centaur upper stage experienced instability during burn resulting in uncontrolled tumbling and improper orbit of payload

Titan IV A-20 (August 1998)

- A short in the power supply wiring harness caused the guidance system malfunction

Titan IV B-27 (April 9, 1999)

- IUS stage 1 failed to separate from stage 2
- One of 6 stage 1/2 connectors did not disconnect due to interference with thermal tape
- Engineering ambiguous, engineering intent not understood

Delta III 269 (May 4, 1999)

- Second burn of second stage lasted only 1 second placing satellite in wrong orbit

Figure 5. An unforgiving business: "one strike and you're out."

BAR Findings

1. **Failure to fully carry out engineering intent**
   - Lack of design robustness
   - Hardware performance dependent on process controls and inspections
   - **Shop floor did not understand design intent**
   - Lack of engineering **attention to detail**
   - **Ambiguous engineering**, or errors in analysis or engineering data input
   - Accepting conditions that do not meet design intent without **in-depth technical understanding**
   - Inadequate test what you fly

2. **Inadequate systems engineering**
   - Inadequate problem reporting and resolution
   - Inadequate postflight **data assessment** (symptoms of design flaws pre-existed)
   - Inadequate **independent reviews** (design and analysis errors not found)
   - Lack of formal **risk management** program
   - **Inadequate change control** (including sub-tier suppliers) and change review

3. **The engineering challenge has been exacerbated by inadequate manufacturing discipline**
   - Inadequate **process definition**
   - Unexpected outcomes due to **material and process variation**
   - Unplanned (unrecognized) **process changes**
   - Inadequate systems to control changes to critical support materials (solvents, cloths, brushes, tape, etc.)
   - Issues listed above evident at major subcontractor/ suppliers

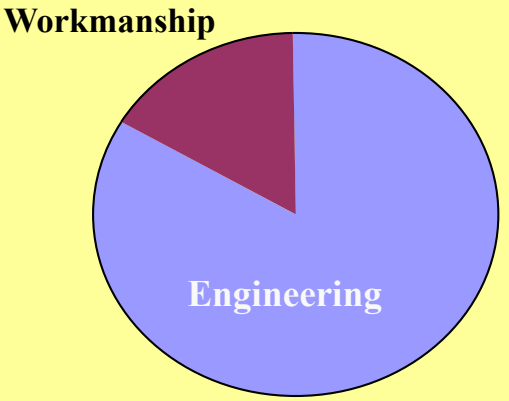
Causes Launch Vehicle Failures

1. Design process failure — 70%
- Lack of design robustness
- Shop floor did not understand design intent
- Inadequate technical or physics-based understanding
- Inadequate process definition

2. Inadequate systems engineering — 20%
- Inadequate problem reporting
- Inadequate postflight assessment
- Inadequate test like you fly
- Inadequate independent reviews
- Lack of formal risk management
- Inadequate change control

3. Inadequate manufacturing discipline — 10%
- Workmanship
- Unexpected material & process variation
- Unplanned process changes
- Inadequate FOD/contamination control

Failures -- 76% Engineering Caused



Causes of 13 launch vehicle failures (1985 – 1999)

- **76%** of launch vehicle failures involve breakdown in the *engineering communication chain*:
  - Engineering requirements wrong
  - Shop traveler wrong
  - Failure to execute on the shop floor

We tend to focus initiatives on improving the Manufacturing disciplines
We need to focus initiatives on improving the Engineering disciplines

Preview.

Turn in in a few weeks for the sequel:

Part II
Lessons Learned from Industrial Accidents

We will explore *causes* of industrial accidents, and provide several proactive best practices that will help *prevent* accidents.

Questions or Comments?