Date: Mon, 3 Feb 2003 11:35:42 -0500
To: p.d.arbuckle@larc.nasa.gov, a.kumar@larc.nasa.gov,
w.p.gilbert@larc.nasa.gov, l.r.mcmaster@larc.nasa.gov,
g.r.taylor@larc.nasa.gov, c.e.harris@larc.nasa.gov,
c.c.lee@larc.nasa.gov
From: "Mark J. Shuart" <m.j.shuart@larc.nasa.gov>
Subject: Some info

Folks,

FYI. Also, this is very sensitive information.....Mark

Date: Tue, 28 Jan 2003 14:15:27 -0500
To: "SHUART, MARK J" <M.J.SHUART@larc.nasa.gov>
From: "Robert H. Daugherty" <r.h.daugherty@larc.nasa.gov>
Subject: Foam and Tile
Cc: H.M.ADELMAN@larc.nasa.gov

Mark...attached are two files that I've received regarding the concern about ET foam around the orbiter bipod support coming off and possibly damaging tiles ... perhaps around the main gear doors. So far, our involvement has been one of providing the current model of drag associated with landing with two tires flat prior to touchdown and some thought exercises of what might happen if the wheel well were burned into....something that is arguably very unlikely. Interestingly, in the powerpoint pitch, they talk about a test in which the "crater" caused by an impact test dug out 3 cubic inches of tile. They say their estimated "flight condition" is 1920 cubic inches of "crater". Hopefully I'm reading that wrong, but as they say...that is way outside their test database. No official request has been made upon us at this time. And there is no formal simulation going on as far as I know regarding landing with two tires flat prior to touchdown...its just a coincidence that landing with ONE tire flat is being simulated right now at the Ames VMS in astronaut training where they are using our newest load-persistence model so it is a very convenient time to look at two tires flat if they can squeeze it in. Will keep you informed as I hear more...if I do.
Bob


Debris.ppt

E212.mpg

Orbiter Assessment of STS-107 ET Bipod Insulation Ramp Impact

P. Parker

D. Chao

I. Norman

M. Dunham

January 23, 2003

Order of Analysis

- **Orbiter assessment of ascent debris damage includes**
  - **—Evaluation of potential for debris to damage tile and RCC**
    - **Program Crater is official evaluation tool**
      - ¥ Available test data for SOFI on tile was reviewed
      - ¥ No SOFI on RCC test data available
    - **Even for worst case, SIP and densified tile layer will remain when SOFI is impactor**
  - **—Thermal analysis of areas with damaged tiles**
    - **Thermal analysis will predict potential tile erosion and temperatures on structure**
  - **—Structural assessment based on thermal environment defined above**
    - **Basis is previous Micrometeriod and Orbital Debris (M/OD) study performed in 1996**

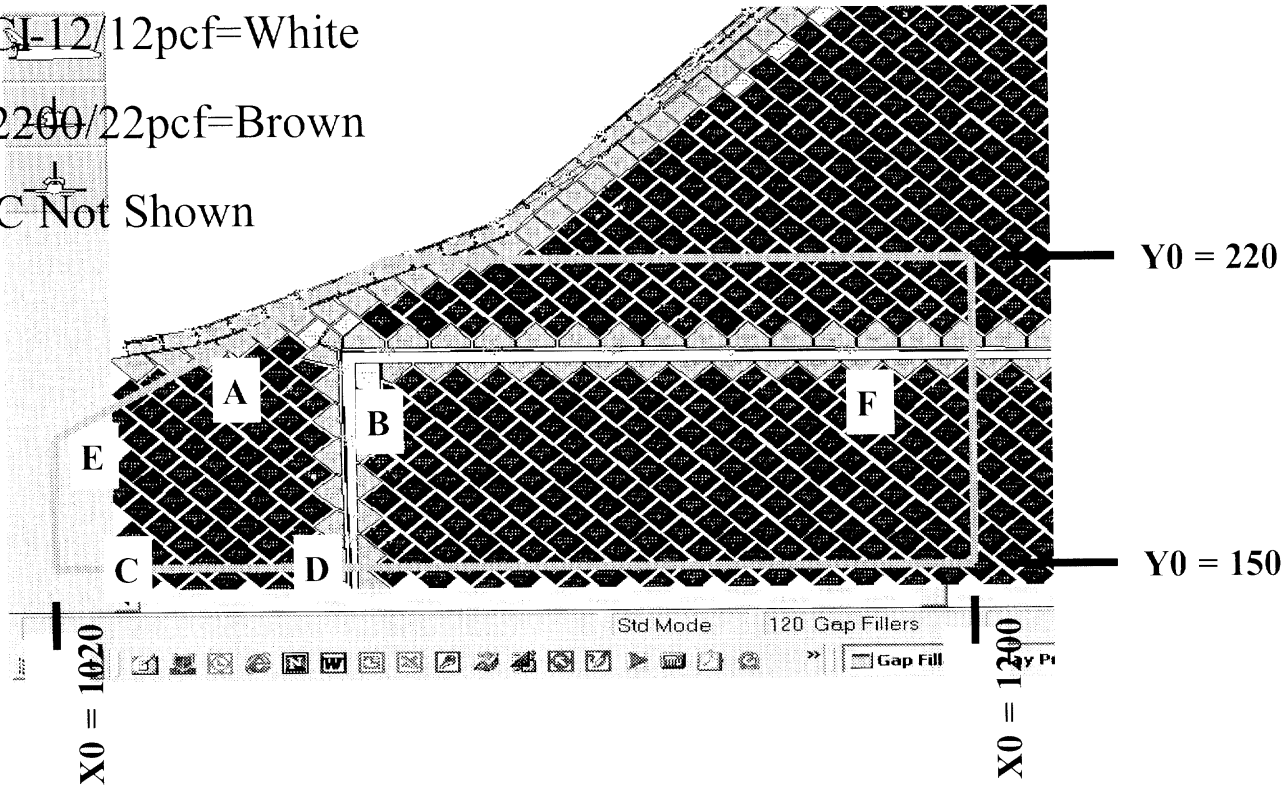
System Integration Inputs Were Matched Against Orbiter Tile/RCC to Determine Critical Locations

LI-900/9pcf=Black

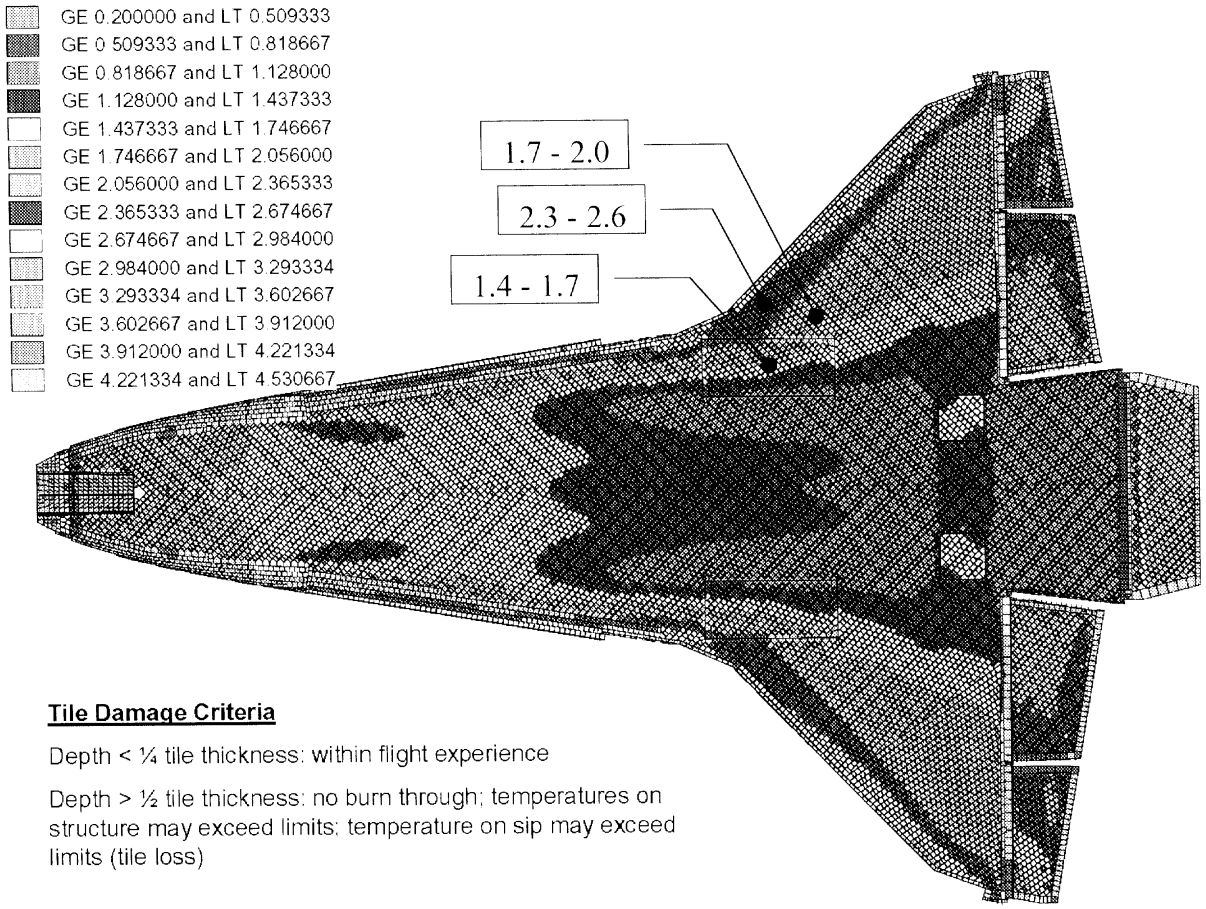
FRCI-12/12pcf=White

LI-2200/22pcf=Brown

RCC Not Shown



Tile Thickness



Tile Damage Criteria

Depth < ¼ tile thickness: within flight experience

Depth > ½ tile thickness: no burn through; temperatures on structure may exceed limits; temperature on sip may exceed limits (tile loss)

Damage Results From Crater Equations Show Significant Tile Damage

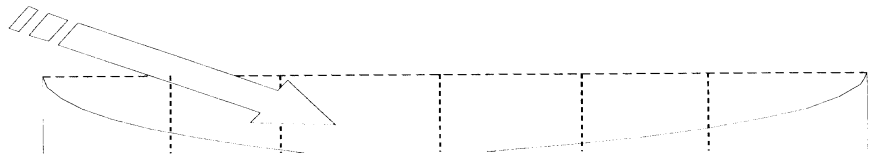
- **Crater indicates that multiple tiles would be taken down to densified layer**
  - **However, program was designed to be conservative due to large number of unknowns**
  - **Crater reports damage for test conditions that show no damage**

Tile Information		Location			Impactor		Calculated Damage		
Type	Thickness	Letter	X	Y	Angle	Velocity	Depth	Length	Width
9 lb	2.6 - 2.8	A	1060	190	13	720	4.7	25.8	7.2
22 lb	2.6 - 2.8	A	1060	190	13	720	3.2	25.8	7.2
9 lb	2.3 - 2.4	B	1090	180	6	700	2.8	31.9	7.2
9 lb	2.0 - 2.4	C	1036	150	8	680	3.3	29.8	7.2
22 lb	2.0 - 2.4	C	1036	150	8	680	2.3	28.6	7.2
9 lb	1.9 - 2.0	D	1075	150	8	710	3.4	32.2	7.2
12 lb	2.8 -3.1	E	1029	177	10	680	2.9	19.0	2.4
22 lb	2.8 -3.1	E	1029	177	10	680	2.6	19.0	2.4
9 lb	1.7	F	1184	182	6	730	2.8	32.8	2.4

Damage data and tile thickness are given in inches.

Debris Size = 20 x 16 x 6

(Density = 2.4 lb/ft^3)



Review of Test Data Indicates Conservatism for Tile Penetration

- **The existing SOFI on tile test data used to create Crater was reviewed along with STS-87 Southwest Research data**
  - **—Crater overpredicted penetration of tile coating significantly**
    - **Initial penetration to described by normal velocity**
      - ¥ Varies with volume/mass of projectile (e.g., 200ft/sec for 3cu. In)
    - **Significant energy is required for the softer SOFI particle to penetrate the relatively hard tile coating**
      - ¥ Test results do show that it is possible at sufficient mass and velocity
    - **Conversely, once tile is penetrated SOFI can cause significant damage**
      - ¥ Minor variations in total energy (above penetration level) can cause significant tile damage
  - **—Flight condition is significantly outside of test database**
    - **Volume of ramp is 1920cu in vs 3 cu in for test**

(Potentially) Similar STS-50 Impact Demonstrates that Damage is Possible

- Damage to aft lower tile (0.5 d x 9 L x 4 W) on wing was found after STS-50 landing; wheel well camera also observed missing ET bipod ramp insulation similar in size
- Small variation in energy input could substantially increase damage
- Incidence angle for STS-107 is predicted higher than STS-50

Volume = 1920in3

L (in)	d (in)	V (ft/sec)	Angle	Vadj (in/sec)	Flt Damage	damage (depth)	Normal Energy	
20	6	**700**	**3.2**	69	**0.50**	0.53	100%	STS-50 (estimated conditions)
20	6	770	3.2	116		0.75	121%	STS-50 plus 10% velocity
20	6	700	5.2	361		1.60	264%	STS-50 plus 2 deg incidence angle
20	6	600	3.2	2		0.05	73%	STS-50 "threshold"
20	6	720	10	1100		3.37	1024%	STS-107
20	6	788	10	1243		3.66	1228%	STS-107 + 10% energy
20	6	914	10	1505		4.16	1650%	STS-107 + 50% energy
20	6	720	10	700		2.49	551%	STS-107 with V* = 800

V*	C	density (SOFI)	density (tile)	Strength (tile)	
400	0.0195	0.0014	0.0052	53	219912

Volume	V* (in/sec)	Ratio	power	V* (ft/sec)	
0.11	6500	1.0	3.5	542	test
0.33	4500	0.8		375	test
1.00	3200	0.8		267	test
3.00	2500	1.0		208	test
1920	400	1.0		33	flight

Volume vs V* (velocity to penetrate tile coating)

RCC Predicted Damage at Incidence Angles Greater than 15 Degrees Based on Ice Database

Impactor		Damage
Angle	Velocity (fps)	Depth (in.)
5	720	0.11
10	720	0.18
15	720	0.23
20	720	0.28
25	720	0.33

Debris Size = 20 x 10 x 6

Density = 2.4 lb/ft^3

45¡ angle of wing was taken into account

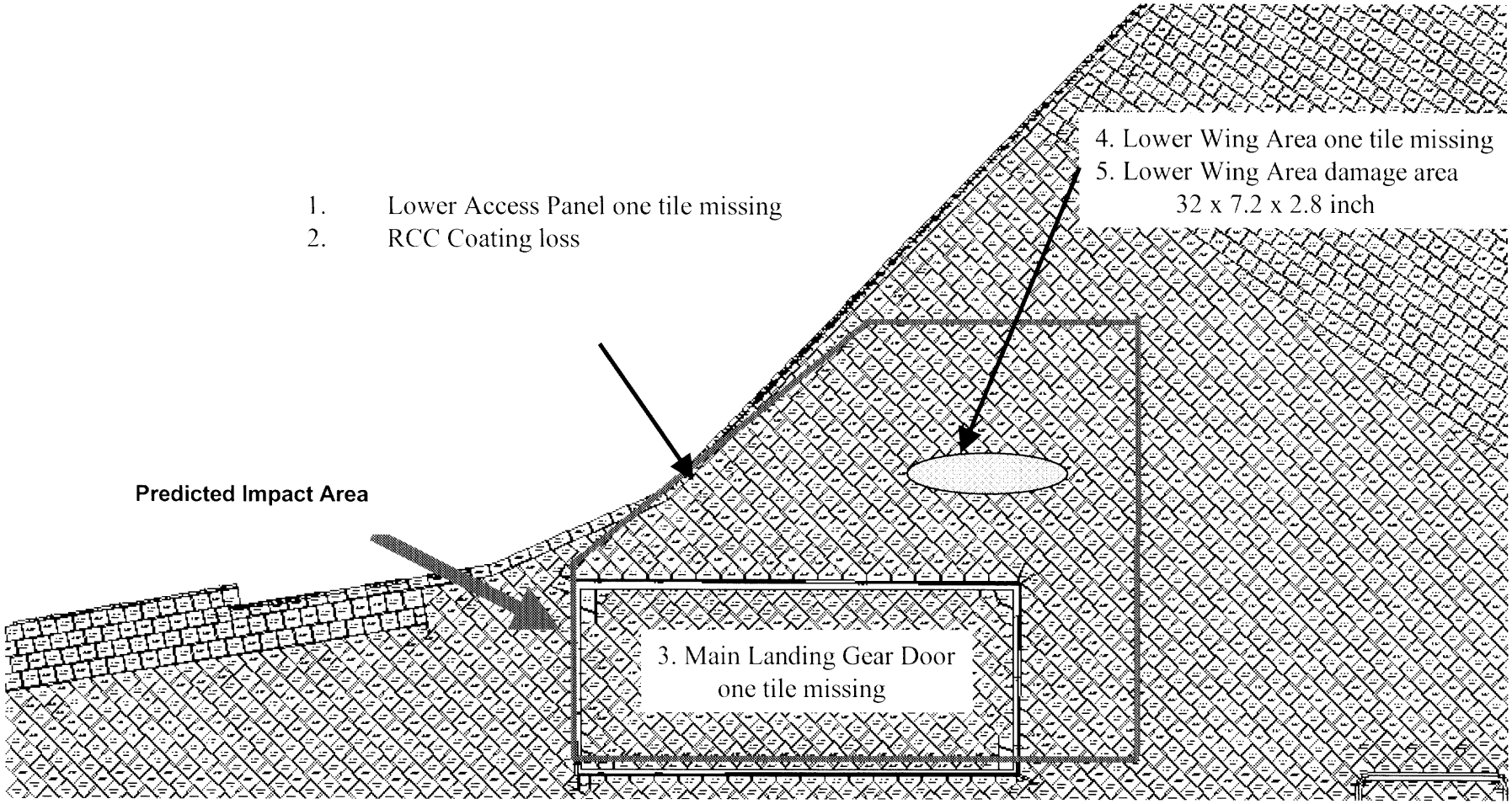
Nominal panel thickness is 0.233 in.

RCC is clearly capable of withstanding impacts of at least 15 degrees; relative softness of SOFI (compared to ice) would indicate greater capability

¥Maximum reported angle of 21 degrees is not an problem

¥Looking at using Window ice and RTV data as an analog

Thermal Analysis Assessment of Debris Impacted Lower Surface in STS-107 Mission Locations



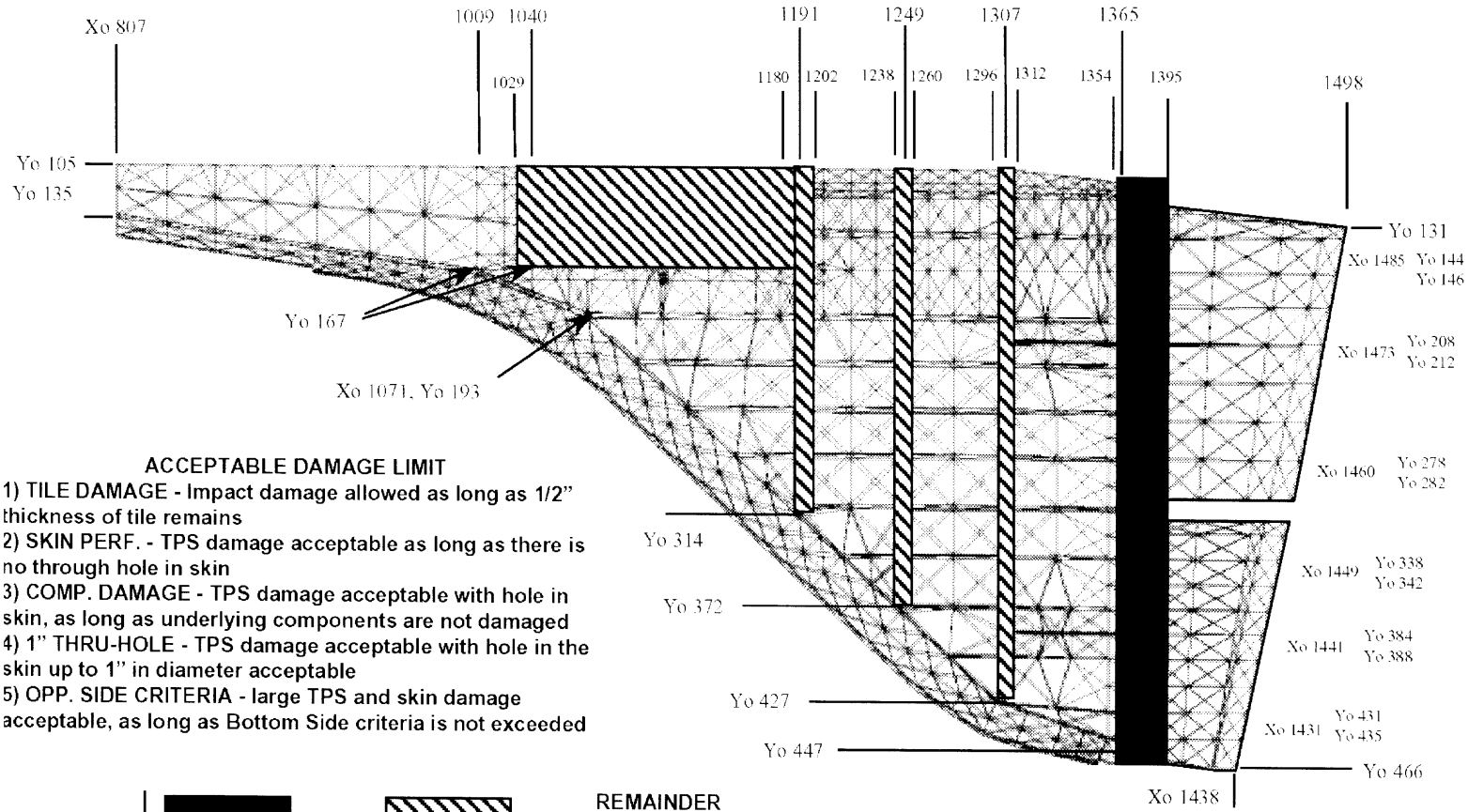
Impacted Lower Surface Location Thermal Predictions

Case	Location	Assumptions	Results
1	Access Panel (one tile missing)	Loss to last layer of TMM Densified layer ~ .2 inches	Temperature of Al Tube Carrier 790 ¡F No issue
2	RCC Panel 9 Lower Flange OML (Coating Missing)	Coating loss and Carbon substrate exposed	Substrate thickness: 0.193 inches Loss .09 inches No issue
3	Main Landing Gear Door (one tile missing)	Loss to last 2 layers of TMM Densified layer ~ .4 inches	Temperature of Structure 540 ¡F No issue
4	Lower Wing Area (one tile missing)	Loss to last 2 layers of TMM Densified layer ~ .4 inches	Temperature below 350 ¡F design req. No issue
5	Lower Wing Area (32 x 7.2 x 2.8 inch) Damage	Loss to last layers of TMM Densified layer ~ .2 inches	
6	Main Landing Gear Door (several tiles Lost)	Loss to last layers of TMM Densified layer ~ .2 inches	

Structural Assessment Provides for Intact Contingency Landing with Damaged Tiles

- Criteria for M/OD study were to assess on-orbit risk that cannot be controlled
- Study allowed for significant degradation beyond design criteria
  - —Structural temperatures well beyond 350F design (due to loss of tile)
    - Repair of structure required
  - —Small holes in structure, allowing internal plasma flow, were permissible if not in critical area
    - Not expected for STS-107
  - —Factor of Safety not maintained for design conditions
  - —Critical subsystems were included in evaluation
    - Wing has few subsytems except in landing gear box and elevon cove
    - Wing spars are considered critical structures
- Conditions identified to ensure intact contingency landing

Wing Lower Surface M/OD Failure Criteria



ACCEPTABLE DAMAGE LIMIT

1) TILE DAMAGE - Impact damage allowed as long as 1/2" thickness of tile remains
2) SKIN PERF. - TPS damage acceptable as long as there is no through hole in skin
3) COMP. DAMAGE - TPS damage acceptable with hole in skin, as long as underlying components are not damaged
4) 1" THRU-HOLE - TPS damage acceptable with hole in the skin up to 1" in diameter acceptable
5) OPP. SIDE CRITERIA - large TPS and skin damage acceptable, as long as Bottom Side criteria is not exceeded

AREA			REMAINDER OF WING
Top Side	3) COMP. DAMAGE	3) COMP. DAMAGE	5) OPP. SIDE CRITERIA
Bottom Side	1) TILE DAMAGE	2) SKIN PERF.	4) 1" THRU-HOLE

Summary and Conclusion

- Impact analysis (Crater) indicates potential for large TPS damage
  - — Review of test data shows wide variation in impact response
  - — RCC damage limited to coating based on soft SOFI
- Thermal analysis of wing with missing tile is in work
  - — Single tile missing shows local structural damage is possible, but no burn through
  - — Multiple tile missing analysis is on-going
- M/OD criteria used to assess structural impacts of tile loss
  - — Allows significant temperature exceedance, even some burn through
    - Impact to vehicle turnaround possible, but maintains safe return capability

<u>Conclusion</u>

- Contingent on multiple tile loss thermal analysis showing no violation of M/OD criteria, safe return indicated even with significant tile damage

X-Sender: j.m.seaton@express.larc.nasa.gov
Date: Mon, 03 Feb 2003 10:26:22 -0500
To: w.p.gilbert@larc.nasa.gov, c.c.lee@larc.nasa.gov
From: Jeff Seaton <j.m.seaton@larc.nasa.gov>
Subject: Weekend report

Bill & Cindy,

After this weekend's loss of the Columbia and her crew, HQ requested that several field center personnel help address the tragedy through the Educator Astronaut web site. Saturday and Sunday I worked with HQ and MSFC to create/modify several elements for the program web site including a letter to our nation's youth, information about the Columbia crew, and video of Administrator O'Keefe's initial briefing. NASA senior staff approved the changes and has been briefed on the status by Adena Loston. I am making a few last modifications to the site at the request of HQ today. http://edspace.nasa.gov is operational and has been displaying the new information since early Sunday morning.

No response needed - just wanted you to be aware of one of the many ways that Langley is providing support in this difficult time.

Jeff

Jeff Seaton
Learning Technologies Project Leader
Robotics Education Project Leader

Aerospace Systems, Concepts, and Analysis Competency
NASA Langley Research Center Voice: (757) 864-6687
18D W Taylor St, Room 185A Fax: (757) 864-9713
Mail Stop 139, Bldg 1192D
Hampton, VA 23681
E-mail: j.m.seaton@larc.nasa.gov

X-Sender: a.h.phillips@pop.larc.nasa.gov
Date: Mon, 3 Feb 2003 10:57:59 -0500
To: "KUMAR, AJAY" <A.KUMAR@larc.nasa.gov>,
"SHUART, MARK J" <M.J.SHUART@larc.nasa.gov>,
"SAUNDERS, MARK P" <M.P.SAUNDERS@larc.nasa.gov>,
"LEE, CYNTHIA C" <C.C.LEE@larc.nasa.gov>,
"KURKE, KATHY A" <K.A.KURKE@larc.nasa.gov>,
"DWOYER, DOUGLAS L" <D.L.DWOYER@larc.nasa.gov>,
"Delma C. Freeman, Jr." <d.c.freeman@larc.nasa.gov>
From: "Alan H. Phillips" <a.h.phillips@larc.nasa.gov>
Subject: Information from this mornings meeting

Enclosed are two documents that may be of value to you.

1) NTSB/NASA Briefing on Mishap Investigation Process

2) Press Release with Columbia Accident Investigation Board (External Team?) named

Alan

Mishap+Investigation+Process+NT
03-034.txt

> See RA-05 for attachments

--
****
Alan H. Phillips
Director, Office of Safety and Mission Assurance
NASA Langley Research Center
5A Hunsaker Loop
Building 1162, Room 112C
Mail Stop 421
Hampton, VA 23681

(757)864-3361 Voice
(757)864-6327 Fax
****

To: "POWELL, RICHARD W" <R.W.POWELL@LaRC.NASA.GOV>
From: Cindy Lee <c.c.lee@larc.nasa.gov>
Subject: Fwd: Information from this mornings meeting
Cc:
Bcc:
X-Attachments: Mishap+Investigation+Process+NT 03-034.txt

X-Sender: a.h.phillips@pop.larc.nasa.gov
Date: Mon, 3 Feb 2003 10:57:59 -0500
To: "KUMAR, AJAY" <A.KUMAR@larc.nasa.gov>,
"SHUART, MARK J" <M.J.SHUART@larc.nasa.gov>,
"SAUNDERS, MARK P" <M.P.SAUNDERS@larc.nasa.gov>,
"LEE, CYNTHIA C" <C.C.LEE@larc.nasa.gov>,
"KURKE, KATHY A" <K.A.KURKE@larc.nasa.gov>,
"DWOYER, DOUGLAS L" <D.L.DWOYER@larc.nasa.gov>,
"Delma C. Freeman, Jr." <d.c.freeman@larc.nasa.gov>
From: "Alan H. Phillips" <a.h.phillips@larc.nasa.gov>
Subject: Information from this mornings meeting

Enclosed are two documents that may be of value to you.

1) NTSB/NASA Briefing on Mishap Investigation Process

2) Press Release with Columbia Accident Investigation Board (External Team?) named

Alan

--
****
Alan H. Phillips
Director, Office of Safety and Mission Assurance
NASA Langley Research Center
5A Hunsaker Loop
Building 1162, Room 112C
Mail Stop 421
Hampton, VA 23681

(757)864-3361 Voice
(757)864-6327 Fax
****

RA-05

Meeting of NTSB/NASA on NASA Mishap Investigation Process

September 18, 2002

Jim Lloyd
NASA Headquarters
Office of Safety and Mission Assurance

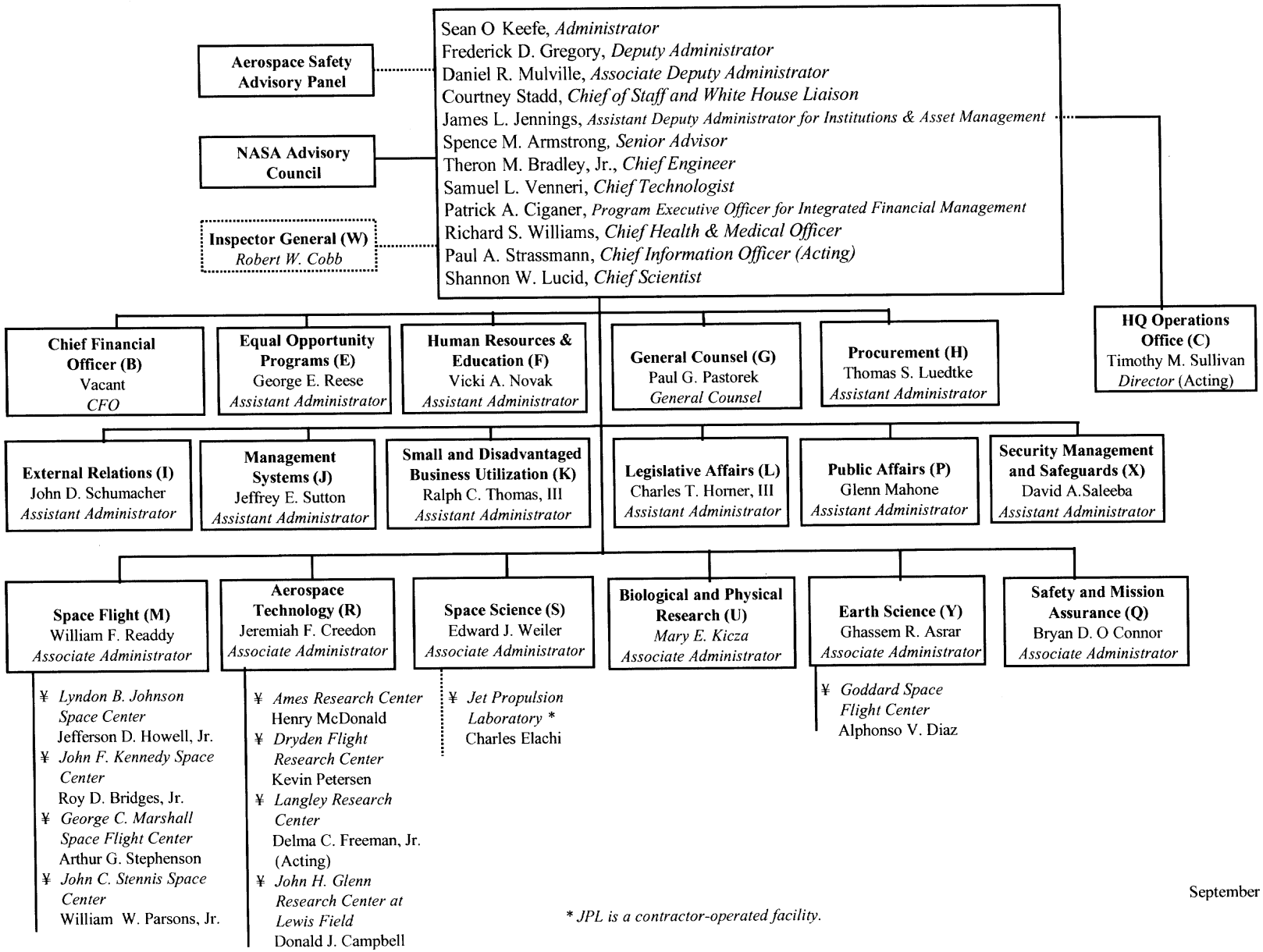
David Whittle
Space Shuttle Program Integration
Johnson Space Center

Content

- General (Lloyd)
  - Organization
  - Policy Overview
  - Procedural Overview
  - Techniques and Methods
  - Capability
  - Corrective Action Tracking
- Space Shuttle (Whittle)
  - Capability
  - Activity
  - Components and Mission Profile
  - Contingency Preparedness
    - Activation
    - MIT (Go Team)
    - Standing Mishap Board (Interagency)
- Summary (Lloyd)

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Office of the Administrator



* *JPL is a contractor-operated facility.*

September 9, 2002

NASA Policy Support

- NASA has policy and contingency planning in place to direct the investigation of all mishaps (including Space Shuttle)
  - NASA Policy Document (NPD) 8621.1, NASA Mishap Reporting and Investigating Policy, December 10, 1997.
  - NASA Procedures and Guidelines (NPG) 8621.1, Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping, June 2, 2000.
- Policy may be downloaded from:
  http://www.hq.nasa.gov/office/codeq/doctree/doctreec.htm

NPD 8621.1G, Mishap Reporting and Investigating Policy

Office of Prime Responsibility : Office of Safety and Mission Assurance (Code Q)

Bryan O Connor,
Associate Administrator

- Establishes NASA-wide policy for mishap reporting and investigating signed by the Administrator.
- Applies to mishaps occurring during NASA operations involving NASA or contractor personnel, and/or when NASA equipment/property is involved.
- Describes purposes of mishap investigation, board appointment authorities, roles of responsible officials, board levels, and responsibilities for final report acceptance and approval.

NPG 8621.1G, NASA Procedures and Guidelines for Mishap Reporting and Investigating and Recordkeeping

Office of Prime Responsibility : Office of Safety and Mission Assurance (Code Q)

Bryan O Connor,
Associate Administrator

- Establishes NASA-wide procedures and guidelines for mishap reporting, investigating and recordkeeping.
- Provides definitions of types of mishaps, reporting procedures, investigative techniques, report format, report timelines, report approval process, corrective action process, and lessons learned process.

NASA Mishap Investigation Policy

- The objective of a NASA mishap investigation is to:
  - Use information from the NASA mishap investigation process as a key element of NASA's mishap prevention program.
  - That is, understand what happened and prevent recurrence.
- The results of mishap investigations are not to be used in matters related to civil, criminal, or administrative culpability or liability, or for disciplinary actions.
- Witness statements given in the course of a NASA mishap investigation are treated as privileged and non-releasable (to the extent allowed by law)
- Mishap reporting process is overseen by Code Q to assure independence of mishap investigation process.

Mishap Report Timelines

- NASA requires quick and thorough investigation to ensure safe operations and the safety of the Shuttle fleet, which, in turn supports the Agency pursuit of mission objectives in science and engineering.
- Mishap investigations are thorough and timely, allowing recommendations to be implemented quickly.

— Report due to appointing official	60 calendar days *
— Appointing official accepts (or rejects)	5 working days
— Approving official approves for agency	10 working days
— Appointing official tasks responsible organization(s) to develop corrective action plan (CAP) and lessons learned (LL)	5 working days
— Appointing official approves CAP and LL	15 working days
— Lessons learned entered into system when approved	6 weeks

* This time can be lengthened by the appointing official

NASA Strategy for Staffing MIB

- Membership of an Mishap Investigation Board (MIB), team, or activity:
  - Chairperson (federal personnel)
  - Executive secretary (federal personnel)
  - *Ex officio* representative (federal person representing Code Q)
  - Board members (federal personnel only — odd number)
  - Members must have no vested interest in the outcome
  - All others duties of mishap board members are superceded by MIB activities.
  - Consultants
  - Observers, advisors and support staff
- Training -- investigators should have:
  - Completed the NASA mishap investigation course (or equivalent) and received refresher training every 3 years.
  - Sufficient experience and technical expertise.

NASA Strategy for Staffing MIB

- Type A Mishaps (death and/or damage, including mission failure equal to or exceeding $1M or selected high-visibility cases):
  - Administrator (or AA, Code Q) assigns a Board for the investigation or
  - Enterprise Associate Administrator (EAA) assigns a Board
  - Members require AA for Code Q concurrence to assure technical capability and independence.
- Type B Mishaps (personal disability or damage greater than $250K but less than $1M) and lesser mishaps —the Center Director or program executive will form the board.
- Shuttle Mishaps (More detail provided later in presentation)
  - Trained, experienced investigators on call according to Agency Contingency Action Plan for Spaceflight Operations
  - Special outside senior level board arrangement for Administrator level board. Membership includes Senior FAA, Air Force, Navy, others as needed.

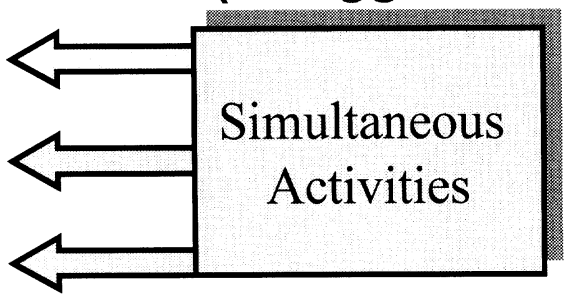
Investigation Techniques and Methods

- Depth of investigation is determined by the severity of the mishap, potential for reoccurrence, and visibility.
- A variety of methods are used to determine root cause and significant contributing factors.
- Methods listed, suggested, and briefly described in NASA Procedures and Guidelines for Mishap Reporting, Investigating & Recordkeeping (NPG 8621.1):
  - Root cause analysis
  - Evidence and data analysis
  - Events and causal factors diagramming
  - Management Oversight and Risk Tree (MORT)
  - Change analysis
  - Fault tree analysis

Investigation Techniques and Methods

Comprehensive systematic method (a suggested NASA practice):

- **Gather data.**
- **Create time line.**
- **Create fault tree.**



- **Merge fault tree and time line to create events and causal factor tree.**
- **Further investigate root cause — (5 why approach and failed barriers).**
- **Perform cause test.**
- **Document findings along with dominant root cause, contributing root cause(s) and significant observations.**
- **Each finding requires a recommendation in the final report.**

Investigation Capability

- NASA has experienced professionals trained in investigation approaches by NASA.
- Courses at NASA Safety Training Center include:
  - Management Oversight and Risk Tree (MORT)
  - MORT-based Mishap Investigation
  - Human Factors in Mishap Investigation
  - Space Shuttle Crash Investigation
  - Aircraft Mishap Investigation
  - Mishap Board Chairperson training
- Technical professionals augment the core of the Board with special knowledge and expertise, e. g., Shuttle systems when Shuttle is an object for investigation.

Investigation Capability (continued)

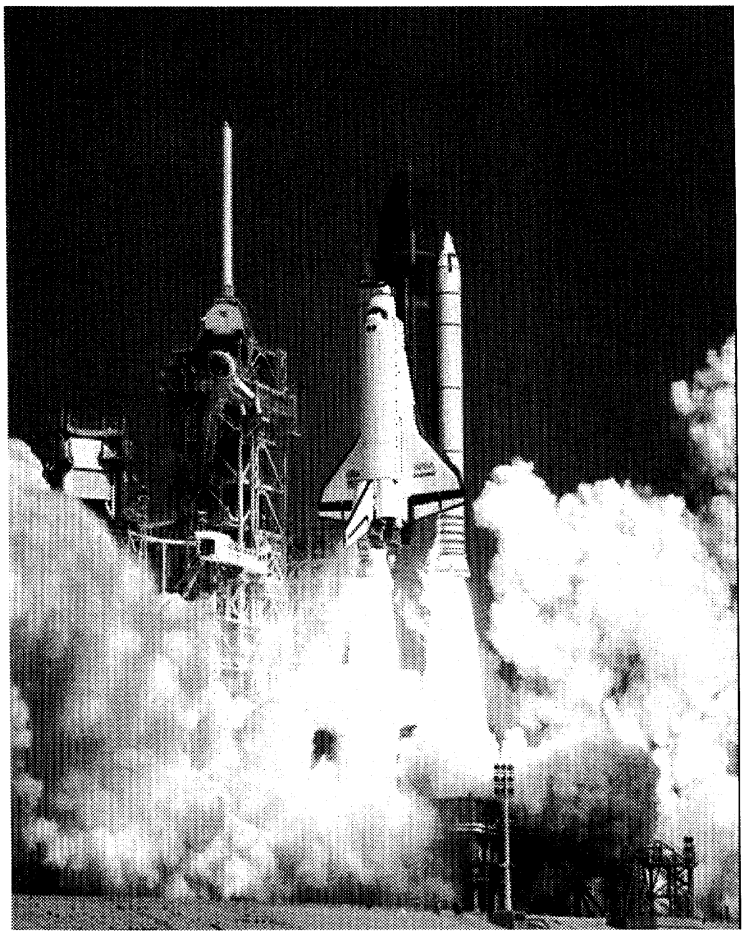
- Core Competencies and Capability (human and laboratory resources):
  - Structures (metallurgy, corrosion, fracture, etc.)
  - Flight dynamics (turbulence, wake vortex, wind shear, etc.)
  - Propulsion (air breathing and rocket)
  - Aerodynamics (modeling, evaluation in wind tunnels, etc.)
  - Others (icing, air traffic operations & modeling, etc.)
  - Human factors, Human error analysis, root cause analysis, stress and fatigue analysis, ergonomic assessment, etc.

Closeout and Tracking of Mishaps and Corrective Action

- Formal acceptance and approval process (AA Code Q is final approving authority for all HQ appointed boards).
- Automated system--Incident Reporting Information System (IRIS).
- Closed-loop system to track recommendations through completion.
- Trending capabilities.
- Documents lessons learned.

Special Considerations - Contingency Planning

- Special Space Shuttle contingency boards.
  - On call rapid response team trained in agency investigation policies with supporting sub teams with expertise in specific Shuttle systems and operations.
  - Standing Interagency board of senior personnel independent of NASA for Administrator level boards.



NASA Space Shuttle Contingency Plans

September 18, 2002

David Whittle

Space Shuttle Program Overview

Goals:

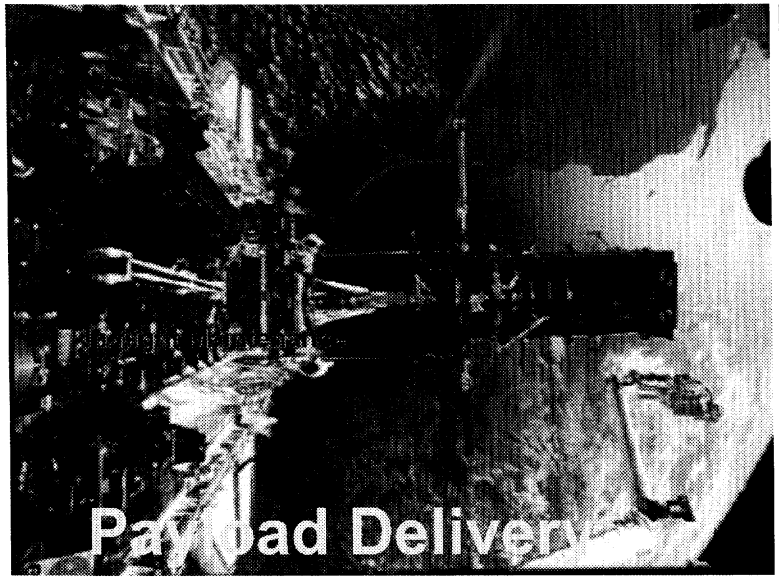
Fly Safely

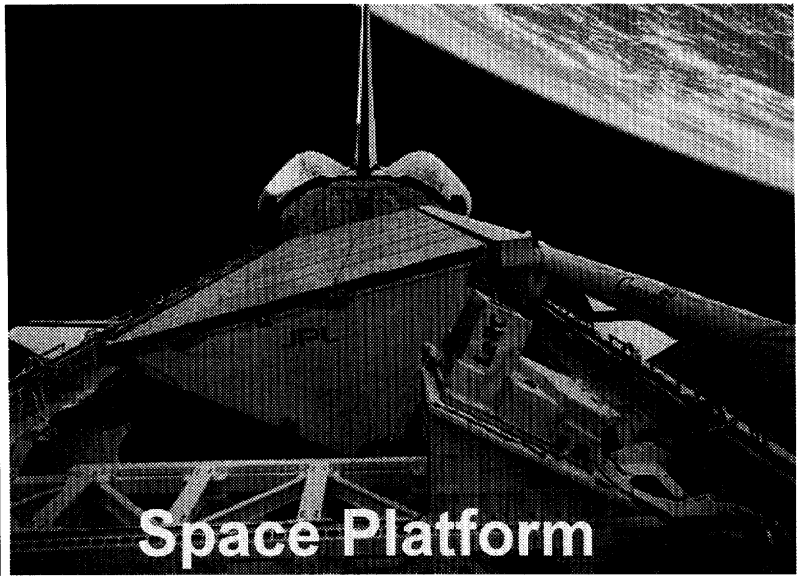
Meet The Manifest

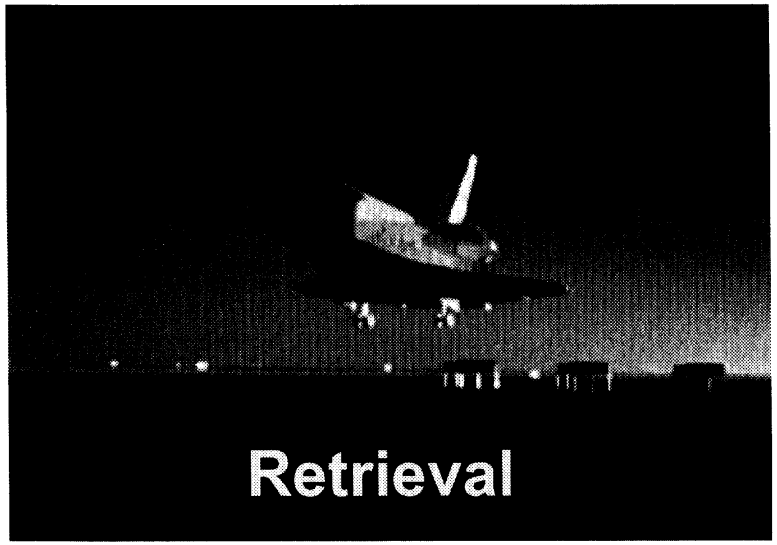
Improve Mission Supportability

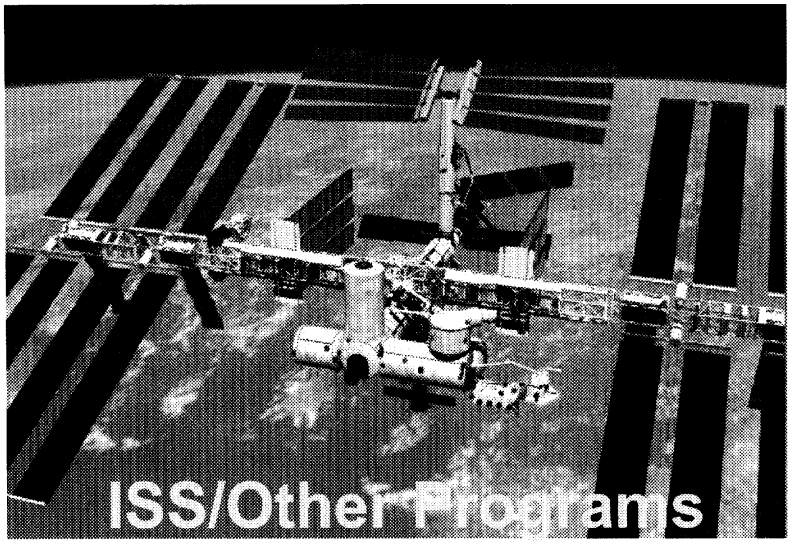
Improve The System

Space Shuttle Program Overview - Capabilities





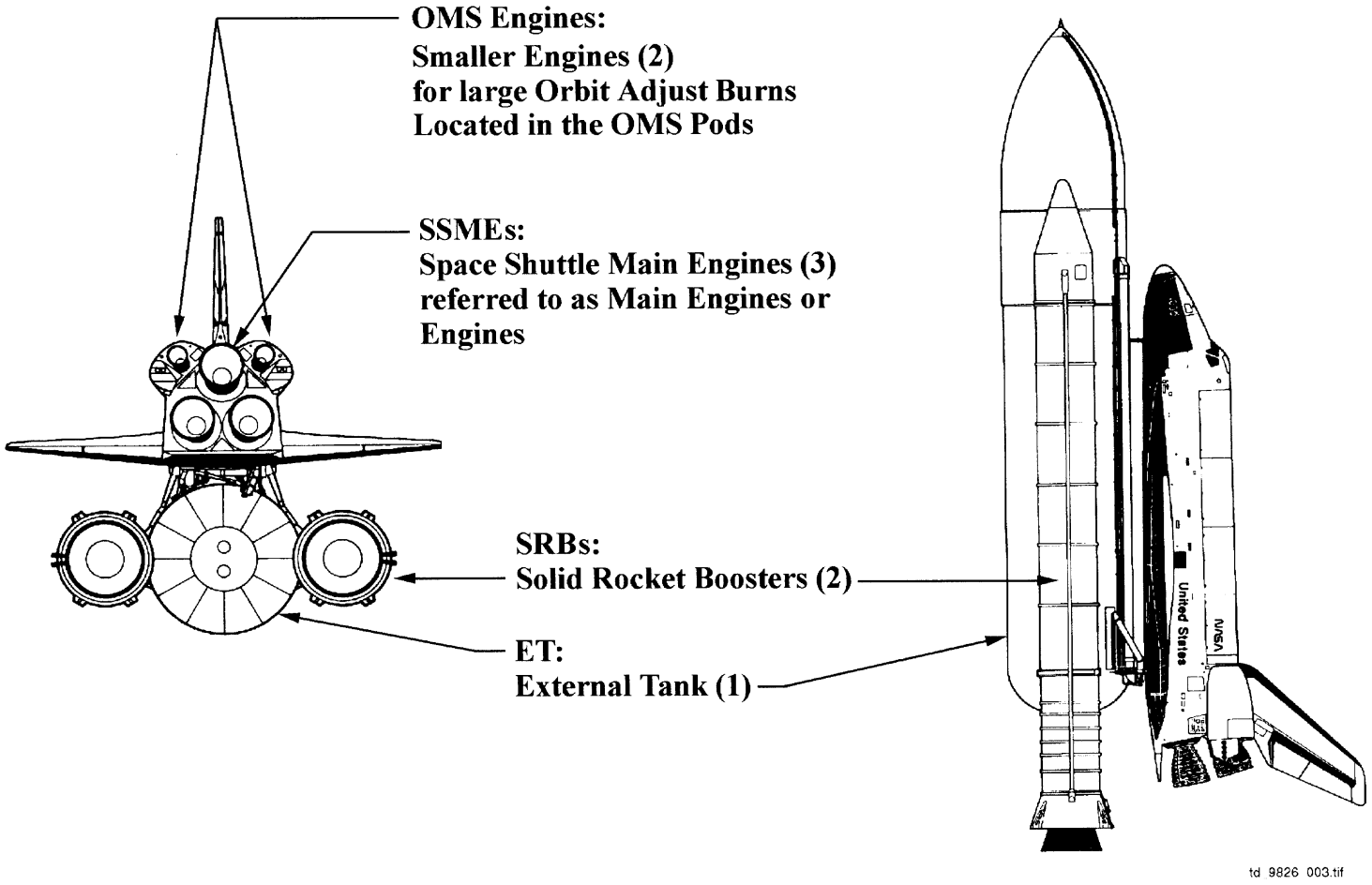




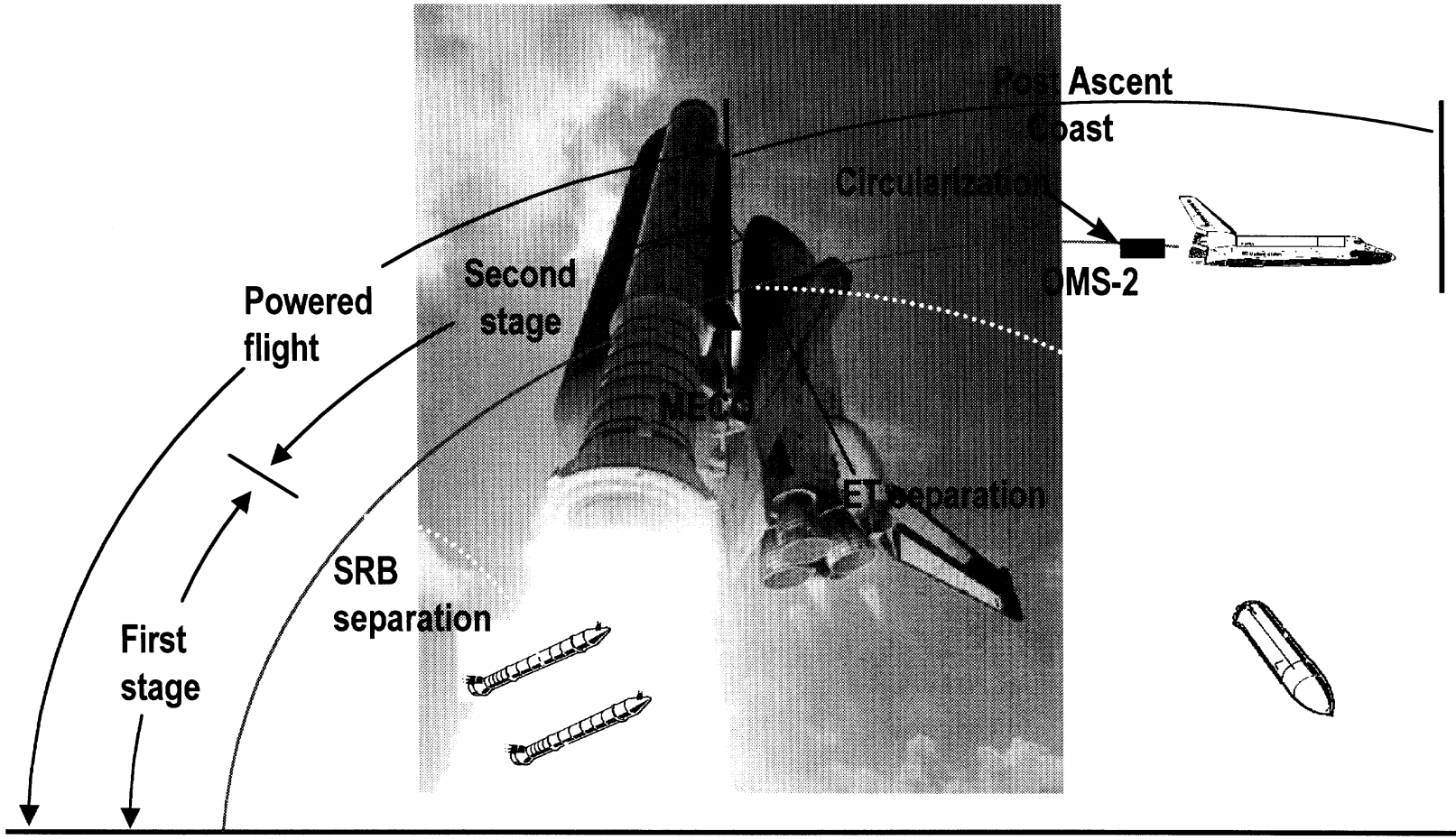
Shuttle Activity Since Challenger

- 40 scientific platforms (stay attached to shuttle)
- 1 commercial deployable (25 before Challenger)
- 3 planetary deployables
- 25 scientific/technology deployable platforms (some retrievable and also shown in retrievable payloads category)
- 8 major ISS element deployables
- 17 spacecraft retrieved/returned
- 5 spacecraft repaired and/or serviced
- 7 ISS utilization/logistics cargos
- 8 DoD missions

Shuttle Components



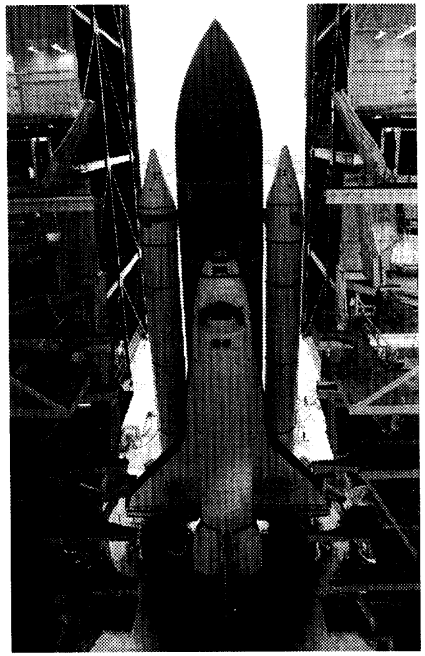
Ascent Definitions



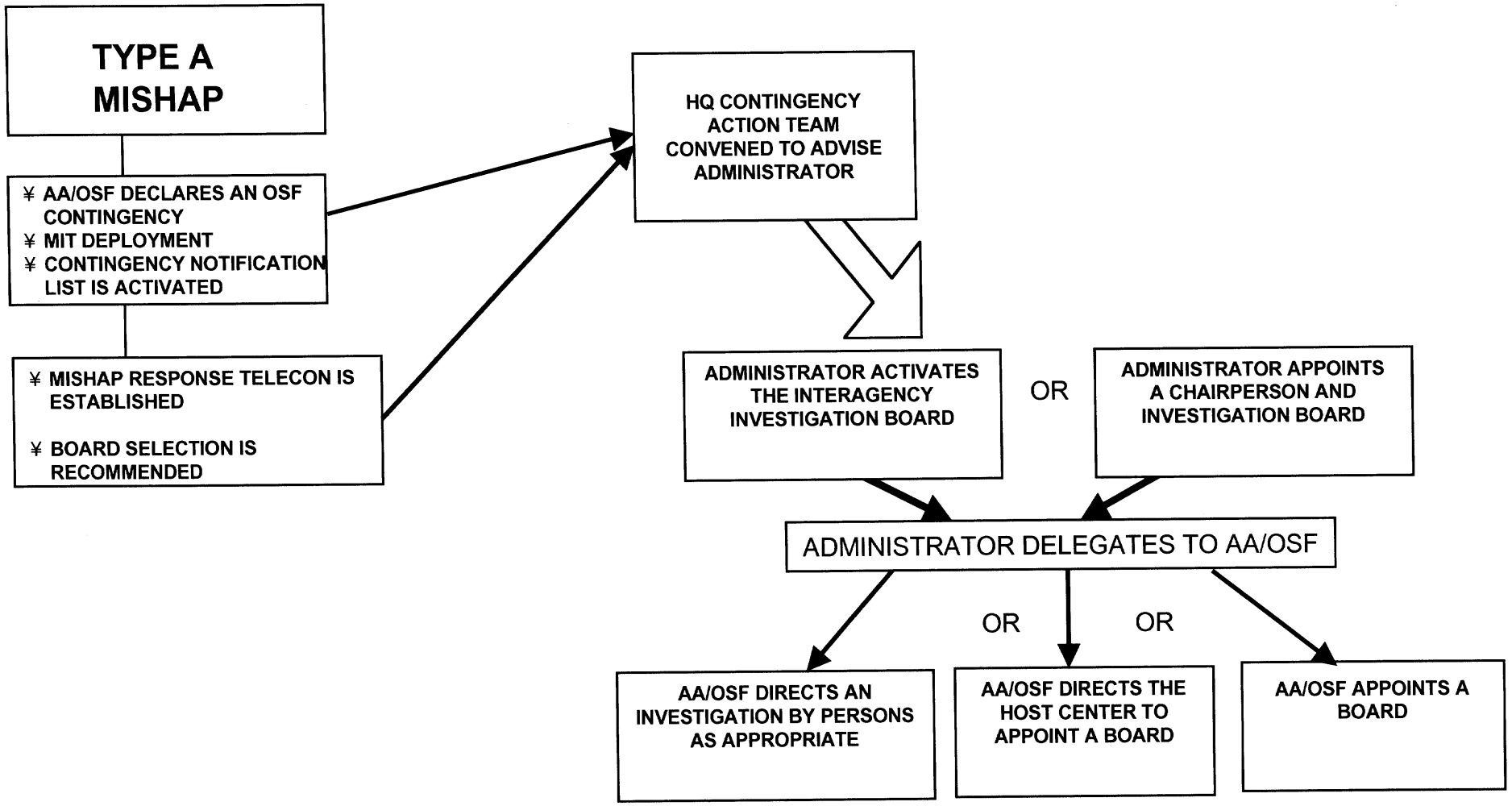
Spaceflight Operations Contingency Preparedness

- NASA has in place the plans, training, and the independent review processes to address contingency and catastrophic situations.
- These situations may present themselves in a variety of ways some of which represent loss of mission, others loss of vehicle and crew:

  - Major malfunction on launch pad
  - Transoceanic abort (TAL)
  - Contingency abort
  - Return to launch site (RTLS)
  - Major vehicle malfunction during ascent
  - Major vehicle malfunction on orbit
  - Major vehicle malfunction during entry
  - Crash landing at landing site
  - Incident while mounted on Shuttle Carrier Aircraft (SCA)
  - Major incident in the Orbiter Processing facility (OPF)
  - Major incident in the vehicle assembly building (VAB)



Activation of Agency Contingency Action Plan for Spaceflight Operations



Mishap Investigation Team (MIT) aka go team

- A trained, rapid response team that the Space Shuttle Program may deploy to any Shuttle incident site in a contingency situation.
- The team consists of the following personnel:
  - -- Chairman
  - -- Flight-trained crew representative
  - -- Flight Surgeon
  - -- Orbiter engineer
  - -- Main propulsion system engineer
  - -- Photographer
  - -- DDMS * representative
  - -- Payload representative
  - -- Safety representative
  - -- Administrative manager
  - -- Ground Operations manager

  *(DDMS: Department of Defense Manager s Space Shuttle Support)

  (Note: All of the above must have attended either the Shuttle Crash Investigation or an Aircraft Mishap Investigation Course.)
- The MIT travels to the incident site on a rapid response aircraft and they are the initial Accident Investigation Board. Their primary responsibilities are to:
  - -- Secure the site and control access.
  - -- Document the original state of the evidence.
  - -- Locate witnesses and obtain initial statements, names, and addresses.

MIT Supporting Teams

SPACE SHUTTLE
MISHAP INVESTIGATION TEAM
RAPID RESPONSE TEAM
CREW RECOVERY TEAM

WORKING GROUPS

KENNEDY SPACE CENTER

- RECORDS AND WITNESSES
- FIRE, EXPLOSIVES, TOXICOLOGICAL AND RADIOLOGICAL
- LAUNCH, LANDING, AND RETRIEVAL OPERATIONS
- FACILITIES AND GROUND SUPPORT
- PAYLOADS
- FLIGHT OPERATIONS AND NETWORKS
- FLIGHT CREW
- PROCEDURES REVIEW
- NATIONAL RESOURCES PROTECTION
- INTERCENTER TIMELINE
- INTERCENTER PHOTO/TV
- CLASSIFIED DATA
- SEARCH, RECOVERY AND RECONSTITUTION
- PUBLIC AFFAIRS

JOHNSON SPACE CENTER

IMPOUNDMENT/CLASSIFIED DATA
- SYSTEMS INTEGRATION
- ORBITER AND GFE PROJECTS
- PROPULSION AND POWER
- NAVIGATION, CONTROL & AERONAUTICS
- STRUCTURES AND MECHANICS
- CREW AND THERMAL SYSTEMS
- MISSION OPERATIONS
- FLIGHT CREW OPERATIONS

PAYLOADS/CARGO
- PHOTO AND TV ANALYSIS
- RECORDS AND WITNESS
- TIMELINE
- PUBLIC AFFAIRS
- FIRE EXPLOSIVES AND RADIOLOGICAL
- MEDICAL AND TOXICOLOGICAL
- MEDICAL CONTINGENCY

DRYDEN FLIGHT RESEARCH CENTER

INSTITUTIONAL/ADMINISTRATIVE
- NETWORKS
- GROUND OPERATIONS
- AIR FORCE FLIGHT TEST CENTER

MARSHALL SPACE FLIGHT CENTER

- EXTERNAL TANK
- SOLID ROCKET BOOSTER
- REDESIGNED SOLID ROCKET MOTOR

SPACE SHUTTLE MAIN ENGINE
- SPACE SHUTTLE SYSTEMS
- TRANSPORTATION

GODDARD SPACE FLIGHT CENTER

MANAGEMENT OPERATIONS
- PAYLOADS
- NETWORKS

Preparedness

The following actions have been taken to ensure that the Office of Space Flight (OSF) maintains its readiness to handle any OSF-related program mishaps:

- Contingency simulation exercises have been performed in the past and are scheduled approximately every 18 months to provide training to space Shuttle program managers in addressing specific contingency situations.
- Top-level OSF program contingency policy documents are revised regularly to maintain currency.
- Field centers are required to provide an updated list of single points of contact and to maintain a listing of working group chairpersons.
- Members of the mishap investigation team, the rapid response team, and the crew recovery team, are in place prior to each mission.
- Office of Space Flight program contingency notification lists are updated periodically and distributed to HQ OSF managers, as required.
- Office of Space Flight program contingency-related information is updated as required and is reviewed, at a minimum, prior to each mission.

Standing Mishap Interagency Investigation Board

The board consists of seven members, supported by the Office of Space Flight (OSF) Headquarters, OSF Field Centers, and technical consultants as required. Board Membership is as follows:

1. USAF Chief of Safety, Maj. Gen. Ken W. Hess (Kirtland AFB, NM)
2. FAA Director of Accident Investigation, Mr. Steven B. Wallace (Washington, DC)
3. Commander, 14th Air Force, Maj. Gen. Michael A. Hamel (Vandenberg AFB, CA)
4. Commander, Naval Safety Center, Rear Adm. Stephen Turcotte (Norfolk, VA)
5. DOT Chief of Aviation Safety Division, Dr. James N. Hallock (Cambridge, MA)
6. Commander, Air Force Flight Test Center, Maj. Gen. Wilbert D. Pearson (Edwards AFB, CA)
7. NASA Field Center Director or NASA Program Associate Administrator (non-OSF or non-mission-related)

Ex-officio member: NASA Associate Administrator, Office of Safety and Mission Assurance, Mr. Bryan O Connor (NASA Headquarters, Washington, DC)

Executive Secretary: NASA Chief Engineer, Mr. Theron M. Bradley Jr. (NASA Headquarters, Washington, DC)

Note: The NASA Administrator will select the Board chair from the names in 1-6 above. The Board may obtain technical support from government or non-government sources on an as needed basis.

Board Operating Guidelines

- The investigation board duties of each board member will take precedence over all other duties
- The conduct of this investigation will be done using the established NASA support structure of working groups, NASA field centers contingency support plans, and supporting facilities as provided in the office of space flight contingency action plan. This includes staff advisors as required for expertise in areas such as public affairs, legal, medical, safety, and security.

Any questions on the Shuttle MIT and Interagency Mishap Investigation Board?

Summary

- NASA philosophy:
  - Identify root cause and contributing factors to prevent mishap recurrence using structured and proven investigation methodology.
  - Non-punitive system.
- NASA needs quick and thorough investigation to ensure safety of process and return to flight to support Agency mission objectives.
- Policy and guideline:
  - Ensures an unbiased, independent, and thorough investigation of the facts.
  - Provides closed-loop tracking system to implement recommendations.
  - Provides maximum cross fertilization through lessons learned.

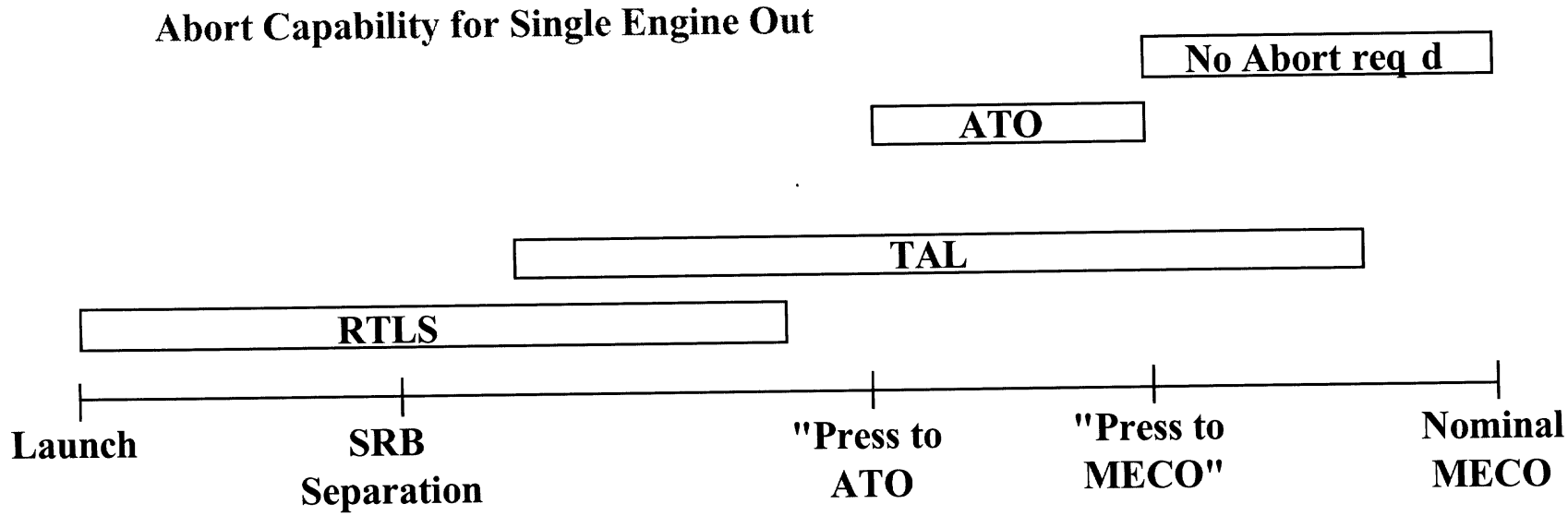
Summary (continued and completed)

- Capability and competencies:
  - Trained and experienced professionals.
  - Capability to perform all analysis required to complete the investigation.
  - Separate independent, interagency board for Administrator-level needs
  - Status/level of members ensures credibility.

Back-Up Slides

Timeline for Ascent Aborts

Our trajectory is designed such that we always have the capability (performance) to successfully complete at least one of the aborts. This is true even if one of the SSMEs has failed



Witness Statements

Basic NASA mishap investigation policy/philosophy regarding witnesses and their statements:

- **Witness statements given in the course of a NASA mishap investigation are privileged and non-releasable.**
- **NASA may also withhold other information in a NASA mishap investigation report from release, depending on such factors as to whether such information is classified, privileged, or involves privacy considerations.**
- **NASA recognizes that the ultimate decision on release of statements or information in a NASA mishap investigation report may reside in a court or administrative body outside NASA.**

Investigation Training

- NASA personnel have training and experience in accident investigation.
- NASA offers the following training to potential NASA investigators:
  - Management Oversight and Risk Tree (5 days)
    - Covers MORT, barrier analysis, cause effect analysis, witness interviewing and more
  - Shuttle aircraft investigation (5 days)
  - MORT refresher (3 days)
  - Human Factors in mishap Investigation (3 days)
  - Mishap investigation (computer-based training)

Key Definitions

- **NASA Mishap-** Any unplanned occurrence or event resulting from any NASA operation or NASA equipment anomaly, involving . loss of property or equipment, or mission failure provided that a written agreement or contract between NASA and another party did not otherwise allocate operational control and corrective action responsibility.

- **Type A Mishap -** A mishap causing death and/or damage to equipment or property equal to or greater than $1 million. Mishaps resulting in damage to aircraft, space hardware, or ground support equipment that meet these criteria are included, as are test failures in which the damage was unexpected or unanticipated.

- **NASA Mishap Investigation Board-** A NASA-sponsored board, consisting of a single individual or a group of individuals with expertise in the area under investigation which is appointed to investigate a NASA Mishap. Board members must not have any vested interest in the outcome of the investigation. Board members may be selected from NASA, or other Government agencies. Observers may be obtained from these same sources or from non-Government sources, such as consultants.

Key Definitions

- **Mission Failure.** A mishap of whatever intrinsic severity that, in the judgment of the Enterprise Associate Administrator and the Associate Administrator for Safety and Mission Assurance, prevents the achievement of primary NASA mission objectives as described in the mission operations report or equivalent document.
- **Appointing Official.** The official authorized to appoint the mishap investigation board, mishap investigator, medical board, Center-level investigation, or technical investigation team to investigate a mishap or close call, or to accept the investigation of another authority. This official is also authorized to accept the final mishap investigation report, direct the responsible organization to develop a Corrective Action Plan (CAP), accept the CAP, track and close corrective actions, and produce a summary report of mishap-related activities upon completion.
- **Approving Official.** The official with the final responsibility to review and accept the NASA mishap investigation report as complete and in conformance with NASA policy.

Key Definitions

- **Significant Observation.** A factor, event, or circumstance identified during the investigation that did not contribute to the mishap or close call, but if left uncorrected has the potential to cause a mishap, injury, or increase the severity should a mishap occur.
- **Finding.** A conclusion based on facts established during the investigation by the investigating authority.
- **Recommendation.** An action developed by the investigation board to correct the cause or a deficiency identified during the investigation. The recommendations may be used in the preparation of the corrective action plan.
- **Corrective Actions.** Changes to design processes, work instructions, workmanship practices, training, inspections, tests, procedures, specifications, drawings, tools, equipment, facilities, resources, or material that result in preventing, minimizing, or limiting the potential for recurrence of a mishap.

Key Definitions

- **Root Cause Analysis.** The root cause analysis is a structured process for identifying the basic factors, reasons, and causes for conditions that result in mishaps or close calls. Once identified, the conditions can be corrected and future mishaps or close calls prevented.
- **Dominant Root Cause.** Along a chain of events leading to a mishap or close call, the first causal action or failure to act that could have been controlled systemically either by policy/practice/procedure or individual adherence to policy/practice/procedure.
- **Contributing Root Cause.** A factor, event, or circumstance which led, directly or indirectly, to the dominant root cause, or which contributed to the severity of the mishap or close call.

Mishap Investigation Training Courses

Back Up Information

NASA Mishap Investigation Training

- Management Oversight and Risk Tree Based Mishap Investigation and Refresher
- Human Factors in Mishap Investigation
- Space Shuttle Crash Investigation
- Aircraft Mishap Investigation
- Mishap Investigation Board Chairperson

NSTC 006, MORT-based Mishap Investigation

Course length - 5 Days

The purpose of this workshop is to provide the student the knowledge and the analytical tools and techniques to conduct effective and efficient investigations and to report the results of those investigations clearly and concisely. While the basics of mishap investigation and evidence collection are discussed, the focus of the course is on the application of analytical techniques based on the Management Oversight and Risk Tree (MORT) approach to accident investigation. Lecture and theory are reinforced by practical examples and exercises. The information presented is sufficient for investigation of major type A and B mishaps by members of boards of investigation, but is also easily adapted for use by individuals investigating lesser mishaps

NSTC 014, Management Oversight and Risk Tree (MORT)- Based Mishap Investigation Refresher

Course length - 2 Days

The MORT-based Mishap Investigation. Refresher course is provided to update the student's knowledge of NASA mishap investigation policies, procedures, and requirements. The practical aspects of investigation and reporting - initial response, collecting and interpreting evidence, managing an investigation, writing the report — will be briefly reviewed, and proficiency in the application of commonly used analytical tools, including MORT, will be sharpened through classroom training and student group exercises. Students participating in this course should have previously taken a MORT-based Mishap Investigation course.

NSTC 012, Human Factors in Mishap Investigation

Course length - 3 Days

This course is specifically focused on the analysis of human error and human factor contributions to mishaps. It will discuss the human factors aspects of mishap causation and also advocate the use of the Management Oversight and Risk Tree (MORT) and/or the Incident Analysis Tool (Modified) for an in-depth analysis of mishaps to identify human factors contribution. The course provides an overview of basic human factors and MORT concepts. The human error analysis aspects of MORT will be expanded using concepts from other analytical techniques and a modified MORT diagram will be presented and used during class on scenarios based on actual NASA mishaps.

NSTC 018, Space Shuttle Crash Investigation

Course length - 4 Days

This course provides instruction in aviation accident investigation basics and policy, with a focus on investigation of mishaps concerning the Space Shuttle. Topics discussed include: fast response requirements, investigator qualifications, board organization and field techniques. Evidence identification, recovery and protection, medical issues, photography, witness interviewing and site mapping are key areas discussed during sessions on field investigation. Course content also addresses OSHA 1910.1030, bloodborne pathogen requirements and NASA requirements on addressing the news media. The course is focused on Space Shuttle crashes and references SSP MIB documents and guidelines, but also contains extensive accident investigation information generally applicable to aviation accidents.

NSTC 019, Aircraft Mishap Investigation

Course length - 3 Days

This course provides field investigation and management techniques for the individual who must respond to the crash scene and assure the capture of as much evidence as possible in a minimum amount of time. Topics of discussion include pre-mishap preparation, witness interviewing, systems investigation, medical issues, response to the scene, photography, preserving evidence, site mapping, and structural failure mode determinations. Discussion of supporting analytical services and laboratory methods is included for familiarization, but not covered in depth. The course instructor uses practical examples and discussion of actual aircraft mishaps in teaching the do's and don'ts of field investigation.

NSTC 024, Mishap Investigation Board Chairperson

Course length - 1 Day

The Mishap Investigation Board Chairperson course is provided to update the student's knowledge of NASA mishap investigation policies, procedures, and requirements as they relate to leading/managing a board. The practical aspects of investigation and reporting - initial response, collecting and interpreting evidence, managing an investigation, writing the report — will be reviewed, and the application of commonly used analytical tools, including MORT, will discussed. Principles and practices of use to any type of mishap investigation will be included.

Date: Tue, 4 Feb 2003 17:21:47 -0500
To: "GILBERT, WILLIAM P" <W.P.GILBERT@larc.nasa.gov>
From: "Darrel R. Tenney" <d.r.tenney@larc.nasa.gov>
Subject: Fwd: Tile Damage Update

> X-Sender: d.l.dwoyer@express.larc.nasa.gov
> Date: Thu, 30 Jan 2003 13:01:17 -0500
> To: d.r.tenney@larc.nasa.gov
> From: Doug Dwoyer <d.l.dwoyer@larc.nasa.gov>
> Subject: Fwd: Tile Damage Update
>
> > Date: Thu, 30 Jan 2003 08:15:38 -0500
> > To: d.l.dwoyer@larc.nasa.gov, r.m.martin@larc.nasa.gov
> > From: "Mark J. Shuart" <m.j.shuart@larc.nasa.gov>
> > Subject: Fwd: Tile Damage Update
> >
> > Doug, Ruth,
> >
> > The latest info on the Shuttle is below. It will be interesting to see the extent of the damage after landing on Saturday.....Mark
> >
> > > Date: Wed, 29 Jan 2003 15:51:28 -0500
> > > To: "SHUART, MARK J" <M.J.SHUART@larc.nasa.gov>
> > > From: "Robert H. Daugherty" <r.h.daugherty@larc.nasa.gov>
> > > Subject: Tile Damage Update
> > > Cc: H.M.ADELMAN@larc.nasa.gov
> > >
> > > Hi Mark,
> > > Nothing terribly new but a few things talked about today with some folks at the Ames VMS. Apparently the current "official" estimate of damage is 7 inches by 30 inches by half the depth of the tiles down to the densified level. One of the bigger concerns is that the "gouge" may cross the main gear door thermal barrier and permit a breach there. No way to know of course. A JSC colleague and I talked to the sim guys and are urging them to simulate a landing with two tires flat prior to touchdown...it is as simple as hitting a software button and simply doing it...but since no Orbiter Program Management is "directing" the sim community to do this it might need to get done "at night". An anecdote they told us is that this was already done by mistake this week and the commander lost control of the vehicle during our load-persistence simulations. It seems that if Mission Operations were to see both tire pressure indicators go to zero during entry, they would sure as hell want to know whether they should land gear up, try to deploy the gear, or go bailout...we can't imagine why getting information is being treated like the plague. Apparently the thermal folks have used words like they think things are "survivable", but "marginal".
> > > I imagine this is the last we will hear of this.
> > > Take care,
> > > Bob

--
Doug Dwoyer
Associate Director for Research and Technology Competencies
Mail Stop 103 Office of Director
11 langley Boulevard Building

Jan 06

1219, Room 133
NASA Langley Research Center
757 864 6114
Hampton, VA 23681-2199
8915

Phone:

FAX: 757 864

Glenn Mahone/Bob Jacobs
Headquarters, Washington
(Phone: 202/358-1898/1600)

February 2, 2003

RELEASE: 03-034

NASA ANNOUNCES SPACE SHUTTLE COLUMBIA
ACCIDENT INVESTIGATION BOARD (THE GEHMAN BOARD)

NASA Administrator Sean O'Keefe today announced the members of the Space Shuttle Mishap Interagency Investigation Board, which will provide an independent review of the events and activities that led up to the tragic loss of the seven astronauts Saturday on board the Space Shuttle Columbia.

The board's first meeting is scheduled for tomorrow at Barksdale Air Force Base in Louisiana.

Retired U.S. Navy Admiral Harold W. Gehman, Jr., who co-chaired the independent commission that investigated the attack on the U.S.S. Cole in Aden, Yemen, Oct. 12, 2000, and once served as the commander-in-chief of U.S. Joint Forces Command, will chair the panel.

"While the NASA family and the entire world mourn the loss of our colleagues, we have a responsibility to quickly move forward with an external assessment to determine exactly what happened and why," said Administrator O'Keefe. "We're honored to have such a distinguished panel of experts, led by Admiral Gehman."

Other members of the investigative board includes:

* Rear Admiral Stephen Turcotte, Commander, U.S. Naval Safety Center, Norfolk, Va.
* Major General John L. Barry, Director, Plans and Programs, Headquarters Air Force Materiel Command, Wright-Patterson Air Force Base, Ohio
* Major General Kenneth W. Hess, Commander, U.S. Air Force Chief of Safety, Kirtland Air Force Base, N.M.

* Dr. James N. Hallock, Aviation Safety Division Chief, U.S. Department of Transportation, Cambridge, Mass.
* Steven B. Wallace, Director of Accident Investigation, Federal Aviation Administration, Washington
* Brigadier General Duane Deal, Commander 21st Space Wing, Peterson Air Foce Base, Colo.

Several senior NASA leaders also will be a part of the panel, including G. Scott Hubbard, Director, NASA Ames Research Center, Moffett Field, Calif. Bryan D. O'Connor, NASA Associate Administrator and former astronaut, Office of Safety and Mission Assurance, Headquarters, will serve as Ex-Officio Member, and Theron Bradley, Jr., NASA Chief Engineer, NASA Headquarters, Washington, will be Executive Secretary.

"We need to be responsible, accountable, and extremely thorough in this investigation," added Administrator O'Keefe. "This panel is charged with a most difficult task, but I am confident in their ability, their integrity, and their dedication to doing what's right. Their findings will help push America's space program successfully into the future."

"Currently, NASA is beginning an internal investigation, drawing on the extensive expertise throughout the agency. Public officials for NASA, the Federal Emergency Management Agency, and other federal, state, and local entities are coordinating talents to help find the cause of this tragedy," concluded Administrator O'Keefe

Additional information about the investigation and the STS-107 mission is available on the Internet at:

http://www.nasa.gov

http://spaceflight.nasa.gov

-end-

X-Sender: v.k.crisp@pop.larc.nasa.gov
Date: Mon, 03 Feb 2003 13:52:49 -0500
To: g.j.bobskill@larc.nasa.gov, RICHARD.W.BROWN@larc.nasa.gov,
P.C.CALHOUN@larc.nasa.gov, J.A.CERRO@larc.nasa.gov,
T.M.CHYTKA@larc.nasa.gov, P.F.COVELL@larc.nasa.gov,
v.k.crisp@larc.nasa.gov, p.n.desai@larc.nasa.gov,
d.l.doucet@larc.nasa.gov, a.m.dwyer@larc.nasa.gov,
k.t.edquist@larc.nasa.gov, w.c.engelund@larc.nasa.gov,
S.M.FERLEMANN@larc.nasa.gov, j.l.hanna@larc.nasa.gov,
S.B.HARRIS@larc.nasa.gov, g.a.hrinda@larc.nasa.gov,
C.P.LEONARD@larc.nasa.gov, r.a.lepsch@larc.nasa.gov,
m.k.lockwood@larc.nasa.gov, j.g.martin@larc.nasa.gov,
Z.N.MARTINOVIC@larc.nasa.gov, m.l.mcmillin@larc.nasa.gov,
w.d.morris@larc.nasa.gov, B.N.PAMADI@larc.nasa.gov,
j.w.paulson@larc.nasa.gov, R.J.PEGG@larc.nasa.gov,
D.H.PETLEY@larc.nasa.gov, r.w.powell@larc.nasa.gov,
e.m.queen@larc.nasa.gov, b.raiszadeh@larc.nasa.gov,
J.S.ROBINSON@larc.nasa.gov, M.SCHOENENBERGER@larc.nasa.gov,
B.R.STARR@larc.nasa.gov, s.a.striepe@larc.nasa.gov,
c.a.sullivan@larc.nasa.gov, p.v.tartabini@larc.nasa.gov,
L.W.TAYLOR@larc.nasa.gov, r.f.vause@larc.nasa.gov,
d.w.way@larc.nasa.gov, n.h.white@larc.nasa.gov,
K.C.WU@larc.nasa.gov,
k.e.wurster@larc.nasa.gov, g.m.ware@larc.nasa.gov
From: "Vicki K. Crisp" <v.k.crisp@larc.nasa.gov>
Subject: Columbia Investigation
Cc: "LEE, CYNTHIA C" <C.C.LEE@larc.nasa.gov>

Del Freeman has volunteered the best of our people, tools, and facilities in this time of need.

Specifically we have poc in the following areas:
aero/aerothermal - Vince Zoby
hypersonics - Charles Miller
trajectory/entry - Dick Powell
metals/composites - Mark Shuart

Memorial at JSC to be held tomorrow at 1 pm (eastern). We're not sure how the other Centers will participate.

There may be a candlelight vigil at the Air and Space museum tonight with local ministers.

Any allegations of wrong doing (e.g. the e-bay fiasco) should be reported to the Office of Chief Counsel (757-864-3221 Kathy Kurke).
Any requests based on Freedom of Information Act should be reported to the Office of Chief Counsel.

If contacted by the media please forward them to Office of External Affairs (Mike Finneran 757-864-6124). Do NOT answer any questions or speculate.

If contacted by NASA personnel or NASA contractors or members of the investigative teams (internal and external) please assure them that we will help but you must obtain requirements first (the who or what that they want) and then discuss those requirements with your management

BEFORE responding. Let the caller know that you will get back to them within the hour. THEN YOU take the request to Cindy Lee (864-6533) to determine the appropriate action. Anything we provide to the Code M Centers will aslo be provided to Code Q (safety and mission assurance).

A small team at Langley (to include Cindy Lee) are meeting with Del Freeman every morning for updates at 8:30 am. Updates from HQ are being provided to the public at 11:30 am and from JSC at 4:30 pm. Feel free to watch these updates on any televisions within the building.

ASCAC would like to put together a small team (comprised of selected VAB and SSB personnel) to braistorm other issues that the investigative teams should look at. Examples: APUs, subsystem corrosion, etc....

I will be on travel from Tuesday - Friday (MSFC for the NGLT Program).

I hope John will return late in the week.

Until then, Jeff Cerro will be in charge. Good Luck Jeff.

vicki

Reply-To: <[redacted]@saic.com>
From: "Darrell N. Walton" <[redacted]@verizon.net>
To: "William Cirillo" <w.m.cirillo@larc.nasa.gov>
Subject: TPS Report from 1995 Shuttle PRA
Date: Mon, 3 Feb 2003 14:15:41 -0500
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
X-Authentication-Info: Submitted using SMTP AUTH at pop016.verizon.net from [141.157.193.75] at Mon, 3 Feb 2003 13:11:27 -0600

Darrell N. Walton
Office Administrator
Science Applications
(p)516-764-5899
(f)516-764-5286

Pages from Space Shuttle 1995 PRA - Vol V.pdf

THE SPACE SHUTTLE PROGRAM IN TRANSITION: KEEPING SAFETY PARAMOUNT

HEARING

BEFORE THE

SUBCOMMITTEE ON
SPACE AND AERONAUTICS

OF THE

COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

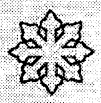
ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

SEPTEMBER 27, 1995

[No. 20]

Printed for the use of the Committee on Science



U.S. GOVERNMENT PRINTING OFFICE
20-277CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052053-3

Mr. SENSENBRENNER. Thank you.
Mr. Fragola?

STATEMENT OF JOSEPH R. FRAGOLA, VICE PRESIDENT AND MANAGER OF THE ADVANCED TECHNOLOGY DIVISION, SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, NEW YORK, NEW YORK, ACCOMPANIED BY GASPARE MAGGIO, RISK ANALYST FOR SHUTTLE PRA, AND ERIN COLLINS, RISK ANALYST

Mr. FRAGOLA. Thank you, Mr. Chairman. In the interests of time, I've prepared a written statement that I'd like to have entered into the record.

Mr. SENSENBRENNER. Without objection, so ordered.

Mr. FRAGOLA. And I'd like to summarize just a few points from that written statement if it would be appropriate.

I'm pleased to be here today to speak about a recently completed Space Shuttle probabilistic risk assessment and how it may play a role in keeping safety paramount.

This risk assessment was developed as a direct result of the Rogers and Slay Commissions after Challenger. It was a comprehensive study that took over 18 months.

And as a result of that study, we feel that we have indicated that NASA has achieved a significant launch risk improvement since the Challenger, about a two-thirds reduction.

This also indicated the effectiveness of the design changes that NASA has implemented in the solid rockets, in between flight testing programs, on both the solid rockets and the SSME.

It also pointed out that the planned SSME improvements that NASA has planned for the future are in areas of risk importance.

We think also that this study may provide a basis for NASA monitoring of prime contractor safety performance in this era of transition.

What everyone must understand is that the safest flight is one that never leaves the pad, so zero risk is not an option for space flight, but managing risk between acceptable limits is.

The limits are set not only on what risk is acceptable but also on how certain we are what that acceptable risk might be. The greater the uncertainty, the more the operating limits must be constrained.

This is not a new concept with NASA. It corresponds to NASA's concept of safety margin, that is, the margin above the safety limit that is required to operate.

Early on in programs with high uncertainty, high margin must be available. But later margin can be reduced as experience increases provided that reduction is balanced by reductions in uncertainty.

The risk assessment type of analysis expands the concept of safety margin beyond the traditional areas of structure, space structures to the entire system. And it allows the increased knowledge base with continued operations to understand where margins may be reduced without compromising the level of safety.

Direct NASA implementation of safety oversight then early on, when uncertainty is high, is prudent and it requires the use of large margins. Indirect oversight could produce the same or even

higher levels of safety if the shuttle knowledge base has increased to compensate for the loss margin, especially if safety enhancing design improvements are effective.

The issue then is not whether the conversion from direct involvement to indirect oversight provides adequate safety assurance, given this current shuttle design and this current knowledge base. That's the issue, I think.

Risk assessment might support the resolution of this issue by assessing safety margins and establishing a set of monitoring indicators to ensure that safety level is not eroded by the transition.

Risk assessment provides for a proper weight to be assigned to on-going occurrences or lack thereof, and to anomalies and observed unsatisfactory conditions.

We don't believe that risk assessment is the only answer but we believe that it provides significant input into keeping safety paramount as the shuttle program undergoes future transitions. And with that, Mr. Chairman, I'd like to make myself available for questions.

[The prepared statement of Mr. Fragola follows:]

TESTIMONY BY JOSEPH R. FRAGOLA
BEFORE U.S. HOUSE OF REPRESENTATIVES SCIENCE COMMITTEE, SUBCOMMITTEE ON SPACE AND AERONAUTICS

Genesis of Shuttle PRA:

In the aftermath of the Challenger accident, the Rogers Commission recommended that NASA reconsider quantitative risk assessment approaches and, in fact, by the time the Slay Commission put forth its even more strongly worded suggestions for quantitative assessment initiatives, NASA already had two PRA "Proof-of-Concept" studies underway. These initially limited efforts focused on particular shuttle systems with the objective of indicating potential benefits to be gained from the quantitative approach over the traditional FMEA/CIL process. One study was performed on the Shuttle Auxiliary Power System and its three Auxiliary Power Units (APUs), and the other on the Main Propulsion Pressurization Subsystem (MPPS).

The former study in particular provided initial insight into the power of quantitative approaches by showing that "not all CIL listed items are equal" even though they were theoretically to be treated so; in terms of management and engineering attention each had the potential for leading to a loss of vehicle (LOV). At about the same time, an effort was undertaken under the auspices of the shuttle integration office at JSC in Houston, which became known as the "Shuttle Integrated Risk Assessment". Despite the implication of its name, the study focused initially and primarily on a linked functionality assessment of the Shuttle Main Propulsion System Propellant Management System. Although the thrust varied considerably from a conventional quantitative risk analysis the effort did introduce the PRA concept to a broader segment of NASA and the contractor community.

Soon thereafter the first associate administrator of the recently created Office of Safety, Reliability, and Quality Assurance (Code Q) established a new Safety Division staff position in risk assessment. One of the first assignments of this newly selected individual was to review the risk study submitted by the Galileo program to Interagency Nuclear Safety Review Panel (INSRP) and to recommend that an independent quantitative study be undertaken by NASA Code Q using a PRA approach. This study, when completed, represented the first quantitative assessment of the risk of the total shuttle system. Although it was limited to the ascent portion of the mission, was necessarily top level in nature, and focused primarily upon scenarios which presented a risk to the Galileo nuclear payload, it differed dramatically in kind and in its results from the previous effort undertaken by the payload program office. The study indicated that while the loss of vehicle probability of the shuttle was uncertain, the 90% uncertainty range (based upon all the shuttle flight and test history available at the time, even considering substantial growth in reliability, but keeping the design and operational configuration constant) was between 1/350 and 1/18 missions with a median estimate of 1/78. Code Q released these study results to the press and they were widely quoted. Because of its systematic traceable nature and because its format was familiar to the courts (in dealing with Nuclear Power intervenor suits), the study was used as evidence against a suit brought to delay the Galileo launch. The study's prediction of low public risk despite NASA's forthright admission of possible high shuttle

failure probability convinced the court to deny the intervenor's petition and the launch proceeded on schedule.

Eventually the approach was unanimously endorsed by both the Ulysses program and Code Q for submission to INSRP for this subsequent nuclear powered payload. The study proceeded without fanfare and the launch again was not delayed. Then the approach began to get wider exposure within NASA. It was applied to problems as diverse as wind tunnel design, the assessment of the viability of leak checking the field joint of the proposed Advanced Solid Rocket Motor, the support of the 1990 Space Station design via EVA maintenance, the structure and nature of redesign solutions, and the assessment of the risk of launch delay and other factors on the ability of the current station design to maintain a berthable attitude.

The Deputy Associate Administrator for Space Flight, familiar with PRA techniques from his tenure with the space station redesign team, decided to apply the approach to a comprehensive investigation of space shuttle risk throughout all mission phases from main engine start on lift-off to nose-wheel stop on touchdown. This new study was also to utilize, to the maximum extent possible, not only NASA experience but also contractor experience in an attempt to credit the unique features of the shuttle design and test program as well as the unique insights provided by its reusability. A report on this study, referred to as the Space Shuttle Risk Assessment,has been provided for the Subcommittee's review.

Scope:

The primary objective of this project was to support management and engineering decision-making with respect to the Shuttle program by producing...

(1) a quantitative probabilistic risk model of the Space Shuttle during flight,

(2) a quantitative assessment of in-flight safety risk,

(3) an identification and prioritization of the features of design and operations that principally contribute to in-flight safety risk, and

(4) a mechanism for risk-based evaluation of proposed modifications to the Shuttle system.

Secondary objectives were to provide a vehicle for introducing and transferring PRA technology to the NASA community, and to demonstrate the value of PRA by applying it beneficially to a real program of great international importance.

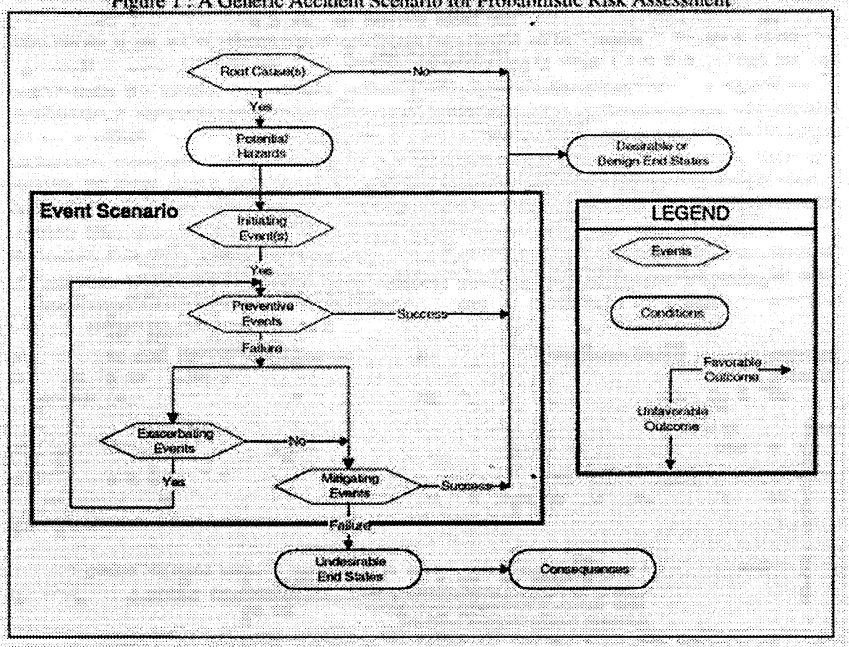
Approach:

The fundamental approach used in this Shuttle risk assessment is that of scenario-based probabilistic risk assessment. The concept of scenarios is basic to any understanding of the PRA process. As the name implies, a scenario is simply the chronological "story" of a sequence of events that is triggered by some incident and proceeds through intervening events to an end state. (In fact, a scenario is often called an "event sequence," and if it deals with an accident, an "accident sequence.")

Figure 1 depicts an accident scenario in the most generic form, including some of the terminology used to describe the elements of scenarios. The key terms are (1) *initiating events* (or trigger events), which — in conjunction with pre-existing potential hazards — begin the scenario; (2) *pivotal events*, which have the potential to change the course of the scenario, and can have preventive, exacerbating, or mitigating effects; and (3) *end states*, which can represent desirable, benign, or unfavorable consequences. In all but the simplest systems, there are several alternative sequences of events that can follow an initiator, depending on the outcomes of the intervening events; each such path is considered a scenario. PRA is simply a systematic technique to evaluate the probabilities and consequences of the various scenarios that can occur in a process or system as well as their associated uncertainties.

The probabilistic risk assessment that is the subject of the report provided to the Subcommittee is the first full-mission risk assessment to be performed on the Shuttle vehicle to date. However, as has been mentioned, NASA and SAIC have conducted a number of previous risk analyses on various aspects of the vehicle and mission. It may be noted that the new results have considerably narrower bounds of uncertainty than the old ones. There are two main reasons for this situation. First, much of the data underlying the current PRA is based on statistical analysis of Shuttle flight and test experience; the additional failure free experience accumulated since the earlier studies necessarily narrows the uncertainty bounds of the risk estimates. Second, the current PRA has analyzed the risk-driving systems in much greater detail than the earlier analyses. In many cases, but not all, a deeper analysis reduces the uncertainty in the results.

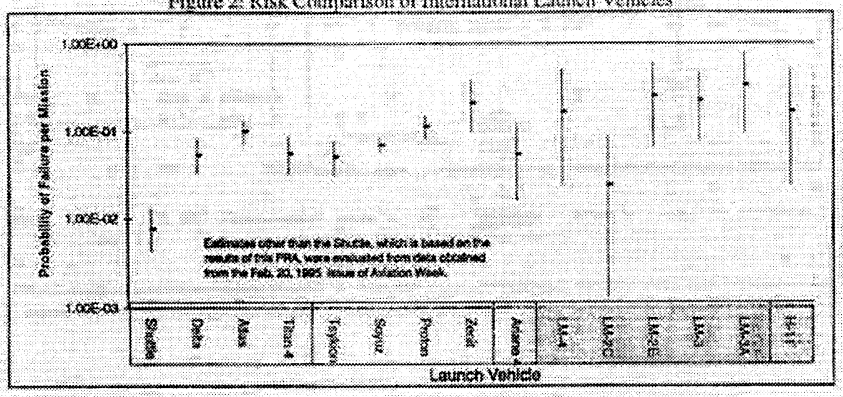
Figure 1 : A Generic Accident Scenario for Probabilistic Risk Assessment



Major Results:

The results of the PRA indicate that the Shuttle has been demonstrated to be by far the most reliable and least risky of all launch vehicles in the world[1] (see Figure 2). However the distinctive advantage of the Shuttle as a returnable and reusable vehicle makes even this comparison fall short of the Shuttle's clear dominate position with respect to other vehicles. Despite this dramatic improvement of the Shuttle over the current inventory of launch vehicles Shuttle LOV risk continues to be substantial. The probability of having a catastrophic failure during a nominal flight was assessed to be, with 90% confidence, between 1 in 76 and 1 in 230 per mission. This implies that if the Shuttle is flown until the year 2030 with an average of 7 missions per year (245 missions), the risk of the occurrence of at least one more catastrophic failure is substantial. Flying the Shuttle until 2015 at the same launch rate corresponds to a 50-50 chance of a catastrophic failure occurring. Note that these risk estimates correspond to the current Shuttle design; changes in design or processing could substantially improve the reliability of certain components thereby reducing the risk to the Shuttle.

Figure 2: Risk Comparison of International Launch Vehicles



The redesign of the solid rocket boosters seems to have significantly reduced the risk due to the failure mode which caused the Challenger accident. However the Integrated Solid Rocket Booster (ISRB) still remains an operationally risky element of the Shuttle vehicle. Although the SAIC team was convinced that the Shuttle booster is the most reliable rocket motor of its type to be built,

[1] Whether the Space Shuttle deserves this distinction could be argued. Although the Russian Soyuz had problems early on, it has experienced only three failures in its recent history of over 1000 flights. Therefore, on a recent experience basis, its record would surpass that of the Shuttle. Considering its entire flight history, however, it compares with other conventional launch vehicles.

operating such powerful propulsion systems will always pose a challenge to the safety of a launch vehicle. This is substantiated by the fact that the ISRB risk rate (risk per unit time of operation) continues to be by far the highest of all the Shuttle elements.

The three SSMEs were shown to contribute a significant portion of the Shuttle risk. They account for 37% of the overall Shuttle flight risk even though they are active only during ascent. Practically all of the SSME risk is due to sudden catastrophic structural failure of one of the high energy components (HPOTP, HPFTP and MCC). The redlines which were established to shutdown the engine in the event of off-nominal operation were found to be extremely effective at accomplishing this task. However, an SSME shutdown leads to Shuttle operational conditions which may prove to be even more dangerous than continuing to fire the engine which was to be shutdown. Abort scenarios were not included in this study because of their second order impact. However the results of the study indicate that they should probably be considered in any extension of this study.

The risk of the Orbiter is dominated by failures of two of its main systems, the APU driven hydraulic system and the tiled thermal protection system (TPS). The APU system was found to be susceptible to common cause failures which resulted in multiple APU losses. Although the system was designed to be redundant the propensity for multiple failures negates the advantages of having back-up components. A significant amount of the common cause failures are due to hydrazine leakage. The TPS risk was found to be dominated by certain portions of the tiles which are susceptible to debris generated during separation of the right ISRB. Even though this damage occurs during ascent there is currently no opportunity for inspecting the tiles and repairing damaged ones before they are required during re-entry.

Figure 3 depicts the approximate relative contributions of the principal elements of the Shuttle vehicle to the mean risk of loss of vehicle in pie-chart format.

The "risk drivers" of a system or operation are the factors that dominate the total risk, and consequently should be targeted for further evaluation and potentially for risk-mitigation efforts. The PRA process identifies an event or accident sequence as a risk driver when (1) its occurrence leads to loss of vehicle with little or no chance of recovery, (2) it has a high probability of occurrence, and/or (3) its probability of occurence or consequence severity are subject to so much uncertainty that it is impossible to say with confidence that it is not a risk driver.

Figure 3 : Distribution of Mean Loss-of-Vehicle Risk Among Shuttle Vehicle Elements.

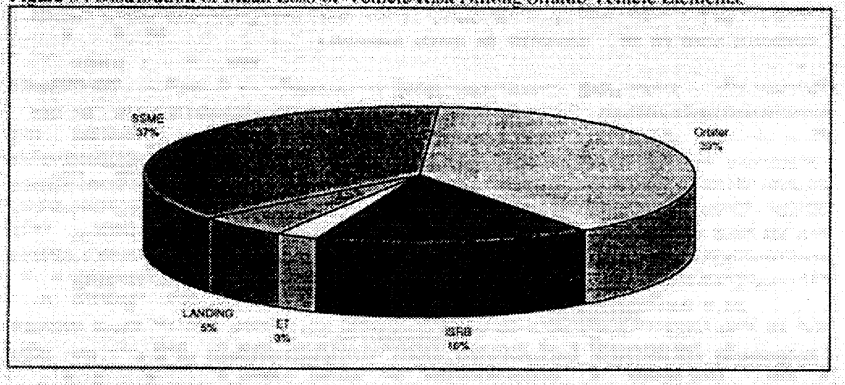


Table 1 summarizes the risk statistics for the most important Shuttle flight risk drivers identified by the base-case risk assessment. (Please refer to *Approach* on page 3 for an explanation of the term "accident sequences.")

Table 1 : Risk Summary Statistics of Most Significant Accident Sequences

	Top 10 Accident Seq.	Top 20 Accident Seq.		Top 10 Accident Seq.	Top 20 Accident Seq.
Percent of Total Risk	38.88%	61.17%			
Orbiter	47.49%	41.98%	Auxiliary Power Units	39.16%	28.99%
			Thermal Protection System	8.31%	12.99%
SSME	45.48%	45.51%	Turbomachinery	37.01%	29.95%
			Combustion Devices	8.47%	15.56%
ISRB	7.03%	12.51%	Redesigned Solid Rocket Motor	7.03%	8.73%
			Solid Rocket Booster	-	3.78%

Strategic Results:

The Space Shuttle PRA not only provided a management tool to assist in making future decisions on safety but also provided quantifiable justification for program decisions made in the past. The PRA has shown that NASA has maintained a proper risk focus by proposing and making significant design modifications to the Space Shuttle, specifically to the solid rocket motor joints (RSRM), main engine turbomachinary (SSME), and orbiter auxiliary power units (APU). These components were shown to consistitute approximately 60% of the estimated Shuttle risk. Although the design modifications being made address the major risk contributors as they have been identified in the PRA, the risk reduction effectiveness of the changes must still be verified.

PRA Insights into Keeping Safety Paramount:

From the safety perspective alone, the safest flight is one that never leaves the pad. Operation of any system regardless of the attention paid to safety is never risk free. Therefore, the issue on an operational system never is to operate with zero risk but rather to operate with a risk that is managed or controlled within acceptable limits. However, to do this, the risk being accepted must be known or if not known, the limits of acceptable risk must be reduced to account for this uncertainty. This is not a new concept in the NASA community. It is analogous to the concept of safety margin. It is well accepted that the safety margin may be reduced where the environment is well known and not reduced where it is not. It is also a well accepted concept to require an increased safety margin early in the program and to decrease that safety margin as the program matures and the uncertainty is reduced. Notice that reducing safety margin does not necessarily mean increasing the risk beyond the level considered acceptable, nor the level of risk incurred, as long as the reduction made is balanced by the increase in knowledge of, and experience with, the system and the environment in which it is operated. (In the case of a reusable system, such as the shuttle, the environment also includes the effects of the required processing between uses.)

What the Shuttle PRA does is essentially expand the scope of the safety margin concept beyond the structures area where it has traditionally been applied to the entire vehicle and mission. By addressing uncertainty directly and quantitatively, it allows the determination of the safety margin to be assessed across the entire program in a consistent fashion. For a given level of acceptable risk, it allows for safety margin reductions as the shuttle experience is continually factored into the risk assessment.

Therefore, it might be possible to maintain the same level of acceptable risk, or alternatively, to maintain the same level of safety while reducing margin, as the experience with the shuttle increases. Safety might be kept paramount even as safety margins decrease provided NASA had some mechanism to ensure that the reduction of these margins was consistent with its increased knowledge of the vehicle. From this perspective, it is quite reasonable to expect direct NASA participation in implementing its safety oversight functions early on (when uncertainty is high and where large margins are required), and it is just as reasonable to expect that the same or even higher levels of safety might be maintained later in the program even if direct NASA participation is reduced. This would be possible as knowledge in the shuttle system is increased, especially if this operational

experience leads to (as it has in the case of the shuttle) safety-enhancing design improvements.

The question, therefore, is whether or not the conversion of the NASA oversight from a direct involvement approach to a monitoring and regulation approach provides enough assurance that an acceptable level of safety is maintained at this time given the knowledge and experience base available for the shuttle program. The shuttle PRA might be useful in this regard if it could support the establishment of a level of risk that is considered acceptable, the amount of margin there is above that level given the available shuttle experience base, and whether that margin is unacceptably being eroded by the transfer of the primary responsibilities to a private contractor. Further, if the PRA could support the resolution of these issues, it might provide an objective input for NASA to ensure that contractor cost reduction efforts are consistent with the safety margins supported by the shuttle experience base at the time they are proposed. Additionally, the PRA might provide a method to monitor the safety performance of the shuttle program on an on-going basis to guard against possible unknown adverse downstream impacts on safety caused by previously implemented economies, or by an aging shuttle fleet.

More specifically, the PRA might be applied to the establishment of a set of systematic integrated observable post-flight physical indicators which provide insight into the ongoing level of shuttle risk. These indicators would continually measure the "distance" between the occurrence frequency of post-flight anomalous events and the paths available to actual Loss of Vehicle (LOV). In this way, the anomalous events would act as precursors and early warning signs that the potential for a LOV event may be increasing. For such a set of precursor indicators to be a valid measure of on-going LOV risk, they must be integrated into the LOV risk framework provided by the shuttle PRA. Each event could thus be viewed in terms of steps along the way to a potential vehicle loss and the residual safety margin measured by the risk of progressing from that anomalous condition to an actual vehicle loss.

Establishing such a set of indicators would not be easy. It would require a detailed understanding of all the steps in the shuttle pre-launch process and a further understanding of how anomalous events uncovered during the process would ultimately relate to shuttle mission risk. While the establishment of such a set of risk-based indicators would certainly require a significant extension of the existing risk framework, the current framework is believed to provide a significant step towards the achievement of this goal.

While it is important to allow for a continual learning process from flight and test experience and to take maximum advantage of the reusability of the shuttle, it is also important that this learning be incorporated from a proper risk management perspective. Without a risk basis, a profit-motivated contractor might review the number of anomalies uncovered as time went on. They might then review each investigatory step in shuttle processing in terms of its "efficiency" in detecting or preventing anomalies. One simple measure of efficiency might be how often an anomalous condition is detected. Without a risk-based perspective, there is tendency to say that if anomalies are never detected, then the analogous process step should be eliminated. However, a risk focus sometimes requires relatively rare events, (which progress with high probability to LOV consequences) to be considered even if they have no historical precedent. For those process steps that are directed at the

detection of anomalous conditions, the risk assessment might indicate the retention of these associated detection tasks in areas of risk significance even if no anomalies have as yet been detected.

On the other hand, in those cases where process steps have detected anomalies, the risk level would be measured by embedding these anomalies into the scenarios developed for the PRA thereby consistently weighting them according to their significance as precursors to a LOV event.

Such a system of processing risk management, utilizing the shuttle PRA as a backdrop, might offer direct assistance toward the solution of the shuttle operations cost vs. safety dilemma. Managing shuttle processing in this way maintains in place only those assurance tasks with the highest mitigation cost-effectiveness and might permit shuttle operational experience to be substituted for process step assurance in an orderly fashion, thereby maintaining shuttle flight frequency without risk increases even in the severely constrained budgetary environments of the future. It also might provide a way to assure NASA that the current shuttle safety level is not compromised when shuttle operations are transferred to a private contractor operating under a profit motive.

Potential Applications:

The PRA model developed herein does not represent a complete Shuttle risk model. Nor does SAIC claim it to be. However it is SAIC's belief that the model has been developed to a stage which captures a significant portion of the Shuttle risk. Additional expansions would certainly be worth considering. For example although abort scenarios were identified they were not developed and therefore the associated potential risk can only be roughly estimated. For this reason the model has been developed to be a "living" model which may be modified and amended as deemed necessary to provide risk insights to a variety of management inquiries.

For example the model might be used to establish realistic cost objectives for redesigning the risk driving components. The cost estimates for any proposed design improvement could be tied to exact improvement objectives by risk based criteria. This methodology will assure that limited resources are focused towards solving the problems which will have the most impact on safety.

The model may also be extended and modified to include turnaround processing and maintenance to illustrate the effect on operational risk. Such an analysis would provide a mechanism for ensuring that cutbacks in processing budgets do not significantly influence Shuttle safety. Extensions of this sort would allow processing tasks to be ranked according to their risk reduction worth and the cost incurred to perform the task. In this way management may quickly and concisely compare a task's overall worthiness in meeting future cost constraints and safety objectives.

The current study indicates that it would be useful to consider abort scenarios. The current conservatively estimated probability of their occurrence warrants attention. The risk analysis of abort scenarios differs from the current PRA in that the time at which the initial event occurs is crucial to the criticality of the final consequence. The dynamic nature of this problem further increases the complexity of the analysis process in order to properly represent the true abort risk.

A part of the nominal mission risk, as well as abort risk, originates from landing related processes. Although this study did account for this risk, the associated uncertainty was found to be rather high. This may not be as much of an issue for a nominal flight as it would be for an abort scenario which would require Shuttle pilots and equipment to operate under less tolerant and more strenuous conditions. Therefore a more involved study of the landing process would offer more concise bounds on the related risk and provide insights and set the groundwork for the an analysis of abort scenarios.

In the near future the Shuttle will be utilized in constructing the International Space Station Alpha (ISSA) and will later dock with the ISSA for extended periods of time. These activities introduce processes which differ appreciably from today's nominal orbital operations and in effect introduce associated risks. One of the more obvious risks being the potential for problems during the docking maneuvers which involve two large space structures rendezvousing, precisely maneuvering in close proximity and docking to allow exchange of materials and personnel. Not unlike the propagation of accidents from one Shuttle system to another, attaching two complex systems together for extended periods of time introduces interfacing risks which should be studied and understood. Extensions to the existing study might provide better insight into the nature and magnitude of these risks.

Finally, as the shuttle fleet ages there may come a time that NASA becomes concerned with not just the risk of the shuttle systems, but the basic structure of the reusable portions of the system, especially the orbiter vehicles. Alternatives such as fleet life extension, even though not initially considered, might become viable options as processing costs are reduced and alternatives are limited by economic realities. (The age of the current commercial jet aircraft and the B-52 bomber fleet give witness to this possibility.) In this instance, extensions of the current PRA to include a probabilistic damage tolerance assessment of the shuttle structure might provide evidence of the risk acceptability of proposed fleet life extensions.

- END -

X-Sender: m.p.saunders@express.larc.nasa.gov
Date: Wed, 5 Feb 2003 15:25:02 -0500
To: "CIRILLO, WILLIAM M" <W.M.CIRILLO@larc.nasa.gov>
From: "Mark P. Saunders" <m.p.saunders@larc.nasa.gov>
Subject: Fwd:

Thanks, Bill. I will include this in our formal LaRC file and will read it today or tomorrow.

Mark

X-Sender: sreidcar@mail.hq.nasa.gov
Date: Tue, 4 Feb 2003 10:38:22 -0700
To: w.p.gilbert@larc.nasa.gov, m.p.saunders@larc.nasa.gov
From: Sandra Reid <sreidcar@hq.nasa.gov>
Bill and Mark,

Attached is a copy of a report on:

This ← section is a repeat

Safety of the Thermal Protection System of the Space Shuttle Orbiter:
Quantitative Analysis and Organizational Factors
Phase 1: Risk-Based Priority Scale and Preliminary Observations

by

M. Elisabeth Pate-Cornell
Department of Industrial Engineering and Engineering Management
Stanford University

Paul S. Fischbeck
Department of Engineering and Public Policy
and Department of Decision Sciences
Carnegie-Mellon University

REPORT TO
THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Cooperative Research Agreement No. NCC 10-0001
between Stanford University and NASA (Kennedy Space Center)

The study was conducted in 1995 and provides a probabilistic risk-based assessment of

the ramifications to the Space Shuttle given certain TPS damage states. The report clearly indicates that there is a high potential for Space Shuttle system damage resulting in a high probability of Space Shuttle Loss of Vehicle and Crew given certain TPS damage states.

The study noted:

"...that the two areas just in board of the main landing gear have been noted as being in the high burnthrough area. This is not strictly speaking a burnthrough problem. The structure in those areas is extremely sensitive to temperature differences and would fail even without a burn-through. However, because of their sensitivity to temperature, these two areas were grouped in the high burn-through category."

If you have any questions please call me at (757) 218-7391 (cell) or send me an e-mail. I will be back in the office on Friday, February 4.

Thanks.

Bill Cirillo

Reply-To: <[redacted]@saic.com>
From: "Darrell N. Walton" <[redacted]@verizon.net>
To: "William Cirillo" <w.m.cirillo@larc.nasa.gov>
Subject: Joe's Testimony
Date: Tue, 4 Feb 2003 17:26:15 -0500
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
X-Authentication-Info: Submitted using SMTP AUTH at pop017.verizon.net from [141.157.193.75] at Tue, 4 Feb 2003 16:22:00 -0600

Here it is.

Darrell N. Walton
Office Administrator
Science Applications
(p)516-764-5899
(f)516-764-5286


Testimony_JRF.doc

Bill and Mark,

Attached is a copy of a report on:

Safety of the Thermal Protection System of the Space Shuttle Orbiter:
Quantitative Analysis and Organizational Factors
Phase 1: Risk-Based Priority Scale and Preliminary Observations

by

M. Elisabeth Pate-Cornell
Department of Industrial Engineering and Engineering Management
Stanford University

Paul S. Fischbeck
Department of Engineering and Public Policy
and Department of Decision Sciences
Carnegie-Mellon University

REPORT TO
THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Cooperative Research Agreement No. NCC 10-0001
between Stanford University and NASA (Kennedy Space Center)

The study was conducted in 1995 and provides a probabilistic risk-based assessment of the ramifications to the Space Shuttle given certain TPS damage states. The report clearly indicates that there is a high potential for Space Shuttle system damage resulting in a high probability of Space Shuttle Loss of Vehicle and Crew given certain TPS damage states.

The study noted:

"...that the two areas just in board of the main landing gear have been noted as being in the high burnthrough area. This is not strictly speaking a burnthrough problem. The structure in those areas is extremely sensitive to temperature differences and would fail even without a burn-through. However, because of their sensitivity to temperature, these two areas were grouped in the high burn-through category."

If you have any questions please call me at [redacted](cell) or send me an e-mail. I will be back in the office on Friday, February 4.

Thanks.

Bill Cirillo

RA-13

SAFETY OF THE THERMAL PROTECTION SYSTEM OF THE SPACE SHUTTLE ORBITER: QUANTITATIVE ANALYSIS AND ORGANIZATIONAL FACTORS

Phase 1: RISK-BASED PRIORITY SCALE AND PRELIMINARY OBSERVATIONS

by

M. Elisabeth Paté-Cornell*

Department of Industrial Engineering and Engineering Management

Stanford University

and

Paul S. Fischbeck**

Department of Engineering and Public Policy

and Department of Decision Sciences

Carnegie-Mellon University

REPORT TO

THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Cooperative Research Agreement No. NCC 10-0001

between Stanford University and NASA (Kennedy Space Center)

* Associate Professor

** Assistant Professor, Commander USNR. Formerly: Graduate Research Assistant, Department of Industrial Engineering and Engineering Management, Stanford University.

C4

TABLE OF CONTENT

FIGURES

TABLES

SUMMARY

This report describes the first phase of a study designed to improve the management and the safety of the black tiles of the Space Shuttle orbiter. This study is based on the coupling of a probabilistic risk assessment (PRA) model and relevant organizational factors. In this first-phase report, a first-order PRA model is developed and used to design a risk-based criticality scale combining the probabilities and the consequences of tile failures. This scale can then be used to set priorities for the maintenance and gradual replacement of the black tiles.

A risk-criticality index is assessed for each tile based on its contribution to the probability of loss of the vehicle. This index reflects the loads to which each tile is subjected (heat, vibrations, debris impacts etc.) and the dependencies among failures of adjacent tiles. It also includes the potential decrease of tile capacity caused by imperfect processing (e.g., a weak bond), and the criticality of subsystems exposed to extreme heat loads at re-entry in case of tile failure and burn-through. Using this model and some preliminary data, it is found that the (mean) probability of loss of an orbiter due to failure of the black tiles is in the order of 10^{-3} per flight, with about 15% of the tiles accounting for 80% of the risk. One of the report's key findings is that not all the most risk-critical tiles are in the hottest areas of the orbiter's surface; some are in zones of highest functional criticality (see Figure 23).

Management factors that can affect tile safety are identified as: (1) time pressures that increase the probability of cutting corners in processing; (2) liability concerns and conflicts among contractors, which affect the flow of information; (3) the low status of the tile work and the turnover among tile technicians, which may increase the work load and decrease its quality; (4) the need for more random testing to detect imperfect bonds and to monitor the evolution of the system over time; and (5) the handling of the external tank and the solid rocket boosters whose insulations constitute a major source of the debris that could hit the tiles at take-off.

Safety of the Thermal Protection System of the Space Shuttle Orbiter: Quantitative Analysis and Organizational Factors

Phase 1:

Risk-based priority scale and preliminary observations

Section 1:
INTRODUCTION

The National Aeronautics and Space Administration (NASA) manages many aspects of the Space Shuttle Orbiter program under tight resource constraints: time, money, human resources, personnel and management's attention, etc. The maintenance of the orbiter's Thermal Protection System (TPS) is an example of operations that must reckon with these limitations. The processing of the tiles between flights is labor intensive and time consuming and, because it is often on the critical path to the next launch, the work has to be done under sometimes severe time constraints. Although great attention is dedicated to the tile work, its quality is occasionally affected by the demanding schedule. The importance of the tiles varies according to their location on the orbiter's surface. Over some areas of the orbiter's surface, several tiles could be lost without causing major damage or risking the lives of the crew; in other areas the loss of a single tile could be catastrophic. This report shows that the contributions of different tiles to the overall probability of failure (defined here as "risk-criticality") vary widely according to their locations on the orbiter's surface. A large percentage of the probability of loss of vehicle (LOV) due to failure of the orbiter's TPS can be attributed to a small fraction of the tiles. Because there will always be resource constraints, *setting priorities* is a first critical step towards ensuring that the most risk-critical tiles receive maximum care and quality control so as to minimize the probability of failure.

The level of risk-criticality of a tile depends on several factors and not exclusively on the maximum heat load (temperature and duration) to which it is subjected. These factors include: (1) the heat loads, (2) the location of the tile with respect to possible trajectories of debris (e.g., pieces of insulation from the external tank (ET) and the solid rocket boosters (SRBs)), (3) the vibrations and aerodynamic forces, and (4) the criticality of the subsystems located directly under the aluminum skin of the orbiter. Failure of a single tile located directly over one of the most critical systems (such as the avionics, fuel cells, or hydraulic lines) is likely to cause a LOV even though these tiles are not exposed to the maximum heat loads. By contrast, severe tile damage next to the base of a wing has been survived in past missions. Therefore, the loads and consequence factors must be combined to estimate the probability of failure and to determine the risk-criticality of each tile.

A tile fails because the *loads* on it reach values that exceed its *capacity*. Understanding both factors, loads and capacities, is thus critical to the quantification of the risk associated with the TPS. The capacities vary considerably among individual tiles because of differences in installation conditions and procedures. For example, inspections have shown that several tiles have been installed with bonding on 10% only of the contact surface. In addition, the capacities of some tiles have decreased over time because of chemical reactions of the bond with some of the water proofing agents used on the orbiter. Similarly, the loads on the tiles are not uniform. In addition to expected loads of heat, vibrations, and aerodynamic forces, a tile may also be subjected to unexpected loads caused by debris impacts. The source of most of the debris is poorly-installed and maintained insulation on the ET and the SRBs. Therefore, both loads and capacities can be greatly affected by a variety of possible human errors.

Some of these errors can be traced back to weak organizational communications, misguided incentives, and resource constraints, which in turn, can be linked to the rules, the structures, and the culture of the organization (Paté-Cornell

and Bea, 1989; Paté-Cornell, 1990). Efficiency of the risk management process for the TPS requires an integrated approach (National Research Council, 1988.) Considering only organizational solutions or only technical solutions to minimize the risk of failure would be counterproductive and wasteful. Furthermore, each individual system cannot be evaluated and managed independently. The performance of the ET and SRBs affects the reliability of the tiles which, in turn, affects the performance of the subsystems that they protect from heat loads. Therefore, when setting priorities, the management teams for the ET and SRBs must account for the potential detrimental side effects of their procedures on the orbiter's TPS. By tracing back, even roughly, the location of the insulation on the ET and SRBs that could hit the most risk-critical spots on the orbiter's surface, it may be possible to identify the spots that should be given top priority.

1.1 Objectives of the overall project

The objective of this study is to provide recommendations to improve the tiles management at Kennedy Space Center (KSC), Florida, based on the development and extension of a Probabilistic Risk Analysis model (PRA) for the TPS of the Space Shuttle Orbiter with emphasis on the *black tiles*. The approach is to include in the analysis not only *technical aspects* that are captured by classical PRA (for example, resistance of the tiles to debris impact), but also the *process* of tile maintenance (for instance, when and how are the tiles tested) and the *organizational procedures and rules* that determine this process (see Appendix 1: Paté-Cornell, 1989.) The question is whether these organizational factors affect the reliability of the tiles, and if they do, to what extent. Linking the PRA inputs to some aspects of the process and the organization allows addressing the often-raised question that PRA, although it captures human errors, is of little help when considering more fundamental managerial and organizational problems. This model is designed to allow management to set priorities in the allocation of limited resources in a continuous effort to improve the reliability of the Space Shuttle. The method thus allows for a global approach to risk management, involving technical as well as organizational

improvements, while accounting for the uncertainties about the system's properties and human performance. In cases where the problem is sufficiently well defined, one can then assess (even if only coarsely) the corresponding increase of reliability.

Uncertainties about the performance of a complex system such as the TPS of the Space Shuttle can be first described by its probability of failure (first-level uncertainties). When computing this probability, one faces uncertainties about the probabilities of the basic events including technical failures of individual components and human errors. These uncertainties can be described by placing probability distributions on the inputs, then computing the resulting uncertainty of the overall failure probability (second-level uncertainties). The role and importance of these second-level uncertainties depend on the intended use of the study. PRA can generally support two types of decisions: (1) whether or not a system is safe enough for operation on the basis of a chosen safety threshold or other acceptance criteria, and (2) (the main objective of this study) how to allocate scarce resources among different subsystems on the basis of risk-based priorities in order to achieve maximum overall safety. The depth of the supporting risk analysis must be adapted to the decision to be made

In the first type of decision, where one is trying to decide if a system is safe enough, it is important to describe the result of the risk assessment not only by a point estimate of the failure probability but by a full distribution of this probability reflecting all the uncertainties of the input values. Second-order uncertainties, which are particularly critical for repeated operations, become important because they give the decision makers an indication of the accuracy of the analysis. A different launch alternative may be preferred if, for example, the mean probability of mission failure is less than one in a thousand but can take values as high as one in fifty. Note however that *the* overall failure probability per operation is the mean of that distribution.

In the second type of decision, where the objective is an optimal allocation of resources, the priority ranking has to be based on a single point estimate for the probability of failure. For optimality reasons, the mean of the distribution of the failure probability is the relevant characteristic. In this case, critical factors are, first, the relative values of the probabilities of mission failure associated with failure of each component, and second, the variations of these relative probabilities with additional units of resources (e.g., time). The combination of these two factors then allows giving priority to the components for which more resources will bring the greatest increase of safety.

In this study, we construct first a priority scale for the black tiles based on our current estimates of the means of the partial failure probabilities, i.e, the mean probability of LOV associated with the potential failure of each tile (first-order PRA). An analysis of the second-order uncertainties may change the priorities if they change the means of these partial failure probabilities. Across subsystems (e.g., tiles versus main engines), the uncertainty of the failure probabilities may vary widely because the failure modes involve a spectrum of basic events whose probabilities are known with different degrees of uncertainty. In this case, full analysis of uncertainties may well change the means themselves and the optimal resource allocation. Within a given subsystem, such as the tiles, the inputs of the analysis for the different elements (e.g., the initiating events) are generally of similar nature and the variations of uncertainties may be less important. Yet, uncertainties about extreme values of the heat loads clearly vary according to the location of a tile on the orbiter's surface. Furthermore, the probabilities of failure (and associated uncertainties) of the subsystems located directly under the skin given a loss of tile(s) and burn-through vary widely. Further study should therefore investigate the effect of second-order uncertainties to determine their impact on the resource allocation.

Our work on this problem is divided into two separate phases. The first phase, which is presented in this report, involves the development and illustration of

a first-order PRA model for the black tiles of the TPS based on a probabilistic analysis of different failure scenarios. In this analysis, we use mean probabilities to construct a risk-criticality estimate for each tile and to establish a scale of priorities for management purposes. Key features of this model are the *dependencies of failures* among adjacent tiles, and between failures of tiles in specific TPS zones and failures of the subsystems located in these zones under the orbiter's aluminum skin. The analysis thus relies on a *partitioning of the orbiter's surface* (1) among zones of temperature, debris, and aerodynamic loads, and (2) among critical system locations. For each tile, we compute a *risk-criticality* factor that represents its contribution to the overall risk of orbiter failure due to TPS failure accounting both for loads (*load-criticality*) and failure consequences at the location of the tile (*functional criticality.*)

The second phase of the work will involve refinement and implementation of the model, including (1) an analysis of (second-order) uncertainies about probabilities in order to determine if these uncertainties can affect management priorities, and (2) organizational extensions. The organizational extensions involve identification and evaluation of the mechanisms by which potential problems occur, are detected, and can be corrected. This second phase will thus involve a study of the maintenance process accounting for its ability to detect and correct past mistakes (weak tiles), ensure satisfactory quality control of the current work, and track the possibility of weakening of the TPS over time. The objective of Phase 2 will be to identify, with the help of experts, the organizational roots of technical and human problems and to make recommendations for possible improvements. The PRA model will be used to assess the relevance of these factors to the reliability of the black tiles and the effectiveness of proposed solutions.

In this study, the PRA model is not an end in itself, but a tool designed to assess specific management practices. The level of detail of the analysis is set with this goal in mind. One key limiting factor in this effort is the unavailability of precise

values for the probabilities of failure of the subsystems located under the orbiter's skin conditional on burn-through. Such data would be the natural results of a complete top-down PRA for the whole orbiter. Because NASA has chosen to do the analysis piecemeal and only for selected subsystems, these results have not been generated. Therefore, we use expert opinions instead of analytical results to assess globally these conditional failure probabilities.

1.2 Scope of the work in Phase 1:

As stated in the proposal, the objectives of this first phase are: (1) to understand the basic properties of the tiles, (2) to identify the main experts and establish working relationships with them, (3) to identify the main data bases and sources, (4) to design the Probabilistic Risk Assessment (PRA) model, and (5) to identify some of the relevant organizational features that affect the reliability of the Thermal Protection System (TPS) with emphasis on the black tiles and on the maintenance process. This first phase of the project was funded in part under SIORA (Stanford Space Systems Integration and Operations Research Applications), and in part as a separate research project (both under cooperative agreement NCC10-0001). Under the SIORA funding, we identified some fundamental issues involved in the linkage between the reliability of the black tiles and various features of the organizations that participate directly or indirectly in their maintenance (including, but not exclusively, NASA at the different space centers, Lockheed Corporation, and Rockwell International). The problem formulation was presented in a paper delivered at a major Probabilistic Safety Analysis conference (PSA'89) held in Pittsburgh, in 1989, in a session chaired by Mr. B. Buchbinder (NASA Headquarter, SRM&QA) on probabilistic safety assessment for space systems. This paper won the Best Paper Award of the American Nuclear Society for PSA'89. It is included in this report as Appendix 1.

This Phase 1 report is organized as follows:

1. Background information: functioning, maintenance, and failure history of the

tiles.

2. Description and illustration of the PRA model; inputs, preliminary results (means); sources of expertise and data.
3. Preliminary observations and (qualitative) coupling of organizational factors and the reliability model.

1.3 Gathering of information and technical points of contact

The data and the relevant information used in this study were gathered through meetings and informal interviews of tile specialists, tile personnel (technicians and inspectors), and management at Kennedy Space Center (NASA and Lockheed Corporation), Johnson Space Center (NASA), and in Southern California (Rockwell International in Downey). We conducted, in particular, extensive (although informal) interviews of tile technicians including both old-timers and newcomers. Several of them came from Rockwell and had participated in the initial tile installation work. They described to us procedures and problems and offered suggestions.

The probability estimates were obtained in two ways: frequencies of events from official or personal records (e.g., debris hits; frequency of tile damage), and subjective assessments (e.g., probability of failure of the subsystems under the orbiter skin if subjected to excessive heat loads due to a hole in the orbiter's skin). Note that:

1. The data used here for the illustration of the first-order PRA model are realistic but coarse estimates that can be refined in the implementation part of the second phase.
2. Second-order uncertainties about the probability estimates themselves have not been encoded at this stage. The probability figures that are used here represent implicitly the means of possible probability distributions of the probabilities of events. Assessment of these second-order probabilities or probability distributions for future frequencies of events (Garrick, 1988) will be

part of the implementation phase if it is judged necessary for the relevance of the results to management decisions.

For this study, the key technical points of contact were the following:

At KSC:

- David Weber (Lockheed)
- Frank Jones, Susan Black, Carol Demes, and Joy Huff (NASA)

At JSC (NASA):

- James A. Smith
- Robert Maraia
- Carlos Ortiz
- Raymond Gomez

In Southern California (Rockwell, Downey):

- B. J. Schell
- Frank Daniels
- Jack McClymonds

Section 2:
BACKGROUND INFORMATION

2.1 System description

The designers of the thermal protection system (TPS) for the space shuttle had to solve a series of complex problems due to the wide range of environments in which the orbiter has to operate. A single-component design could not meet all the necessary requirements of withstanding extreme temperatures and vibrations while remaining light weight and flexible and lasting for 100 missions. Instead, a complete, integrated system was developed relying on different components to solve different problems (Cooper and Holloway, 1981.)

In the highest-temperature areas, reinforced carbon carbon (RCC) is used. This material is extremely heat resistant and able to withstand temperatures up to 2800°F on a reusable basis and up to 3300°F for a single flight. The use of this material is limited to the leading edges of the wing and the nose cone. In areas of the orbiter where heating rates are lower, a flexible reusable surface insulation (FRSI) is used. This material is made of a silicon elastomeric coated Nomex felt, which is heat-treated to allow using it for 100 missions at temperatures up to 700°F. In areas where surface temperatures are above 700°F but below 1500°F, advanced flexible reusable insulation (AFRSI) is used. AFRSI is a "blanket" composition with one-inch stitch spacing. It consists of an outer layer of 27 mil silica "quartz" glass fabric and of an inner layer of glass fabric ("E" glass) which encompass a silica-glass felt material (microquartz, commonly called Q-felt). These materials have replaced most of the 5,000 thin white tiles on the upper surface of the orbiters, originally designated low temperature reusable surface insulation (LRSI). Their replacement has reduced the complexity of the TPS at the cost of a slight weight increase (see Figures 1 and 2.)

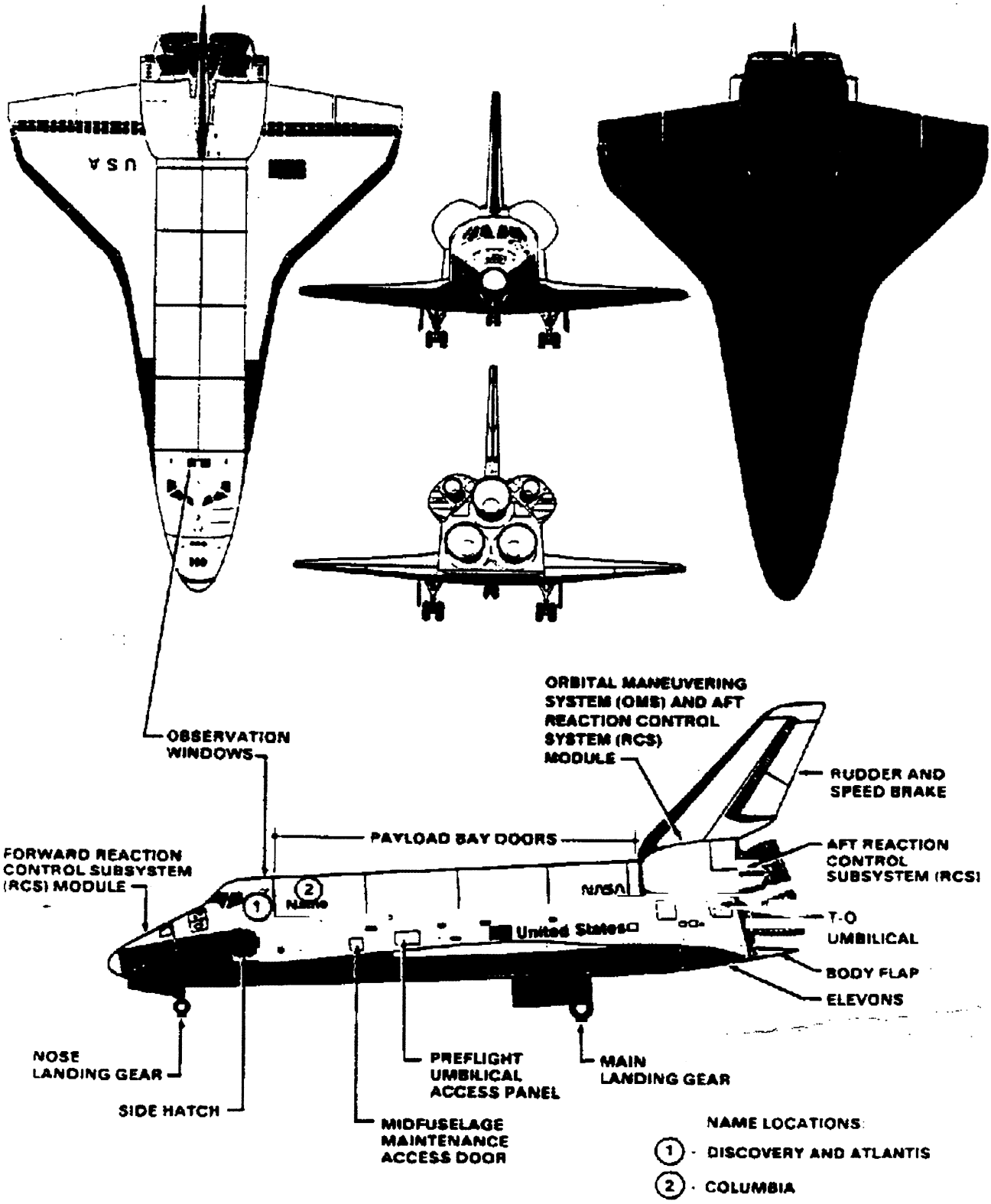


Figure 1: The space shuttle orbiter

Source: Shuttle Operational Data Book, JSC 08934, Vol. 4

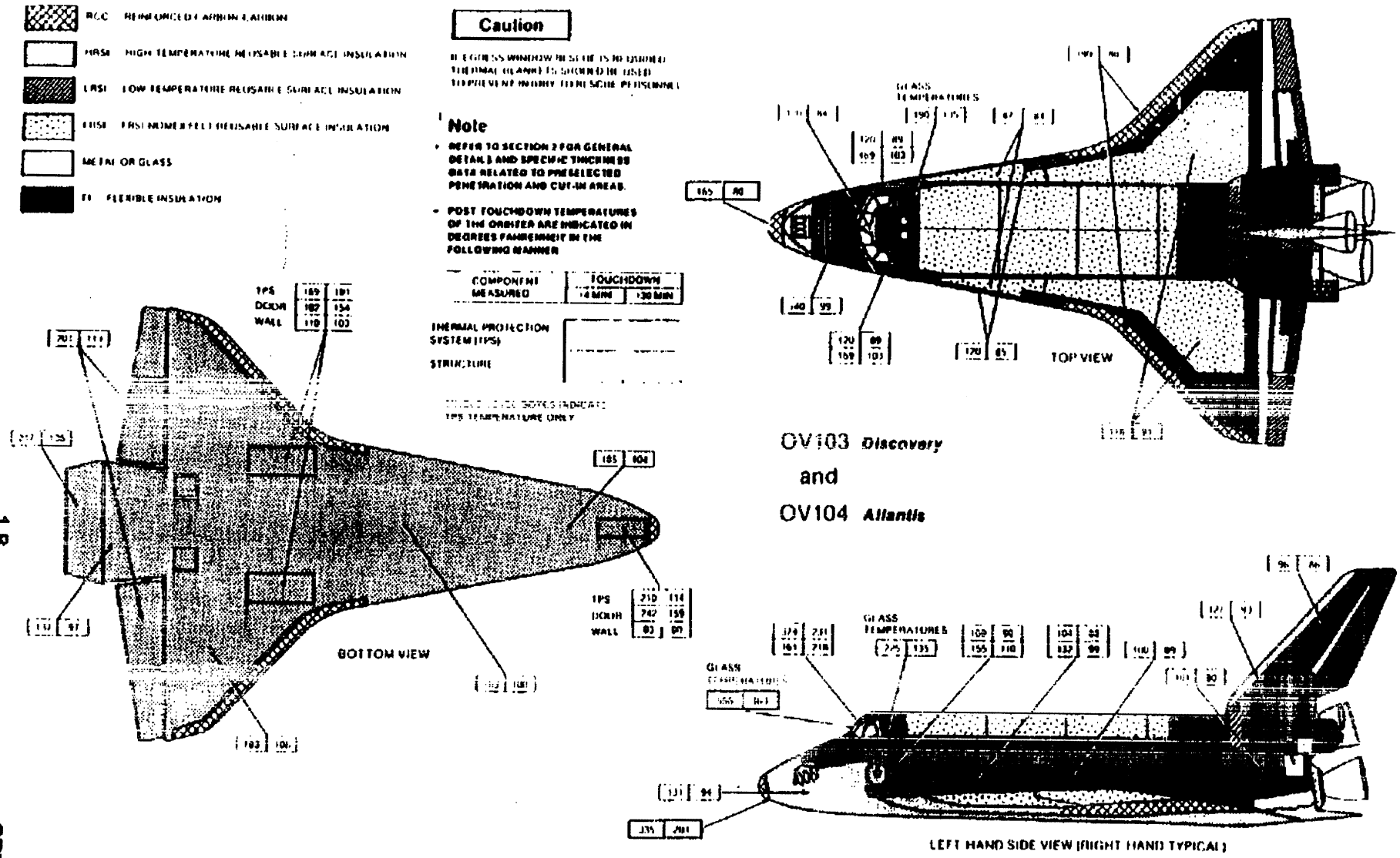


Figure 2: The thermal protection system (TPS) for OV 103 (Discovery) and OV 104 (Atlantis)

Source: Shuttle Operational Data Book, JSC 08934 Vol. 4

The tiles that are of primary interest in this report are designated *high temperature reusable surface insulation* (HRSI) (see Figure 3.) These tiles are coated with black reaction cured glass (RCG) and are certified for 100 missions up to a maximum surface temperature of 2300°F. Approximately 20,000 of these tiles are used to cover the bottom of the orbiter. Among them, approximately 17,000 have a density of 9 pounds per cubic foot (pcf). The remaining 3,000 tiles are of higher density (12 and 22 pcf). They are used in areas where higher strength is needed, primarily around doors and hatches, and where it is required by structural deflections. The 22 pcf tiles are capable of withstanding surface temperatures as high as 2700°F without shrinkage.

These tiles, being highly brittle, have a strain-to-failure performance that is considerably less than the aluminum skin of the orbiter. In addition, the tiles have a much lower coefficient of thermal expansion. Therefore, if they were bonded directly to the aluminum, thermal and mechanical expansion and contraction would cause the ceramic material to crack and fail. To protect the ceramic material, the sizes of the individual tiles were kept small (nominally 6 inches square). These numerous designed gaps allow for relative motion of the tiles as the aluminum skin expands and contracts and the substructure deforms under loading. However, this allowance is not sufficient to protect the integrity of the tiles. In order to further isolate the tiles from local forces, a strain isolation pad (SIP) is secured between the tiles and the skin. The SIP is a felt pad constructed of Nomex fibers and comes in three different thicknesses (0.09, 0.115, and 0.16 inch).

The tiles are bonded to the SIP and the SIP to the aluminum skin using a room temperature vulcanizing silicon rubber adhesive (RTV-560). In certain areas where the aluminum skin is particularly rough and disjointed, a screed or putty (RTV-577) is used to smooth the surface. In order for the SIP and tiles to vent during ascent and to protect the aluminum structure from gap heating, filler bar strips (RTV-560 coated heat-treated Nomex felt material) secured only to the aluminum

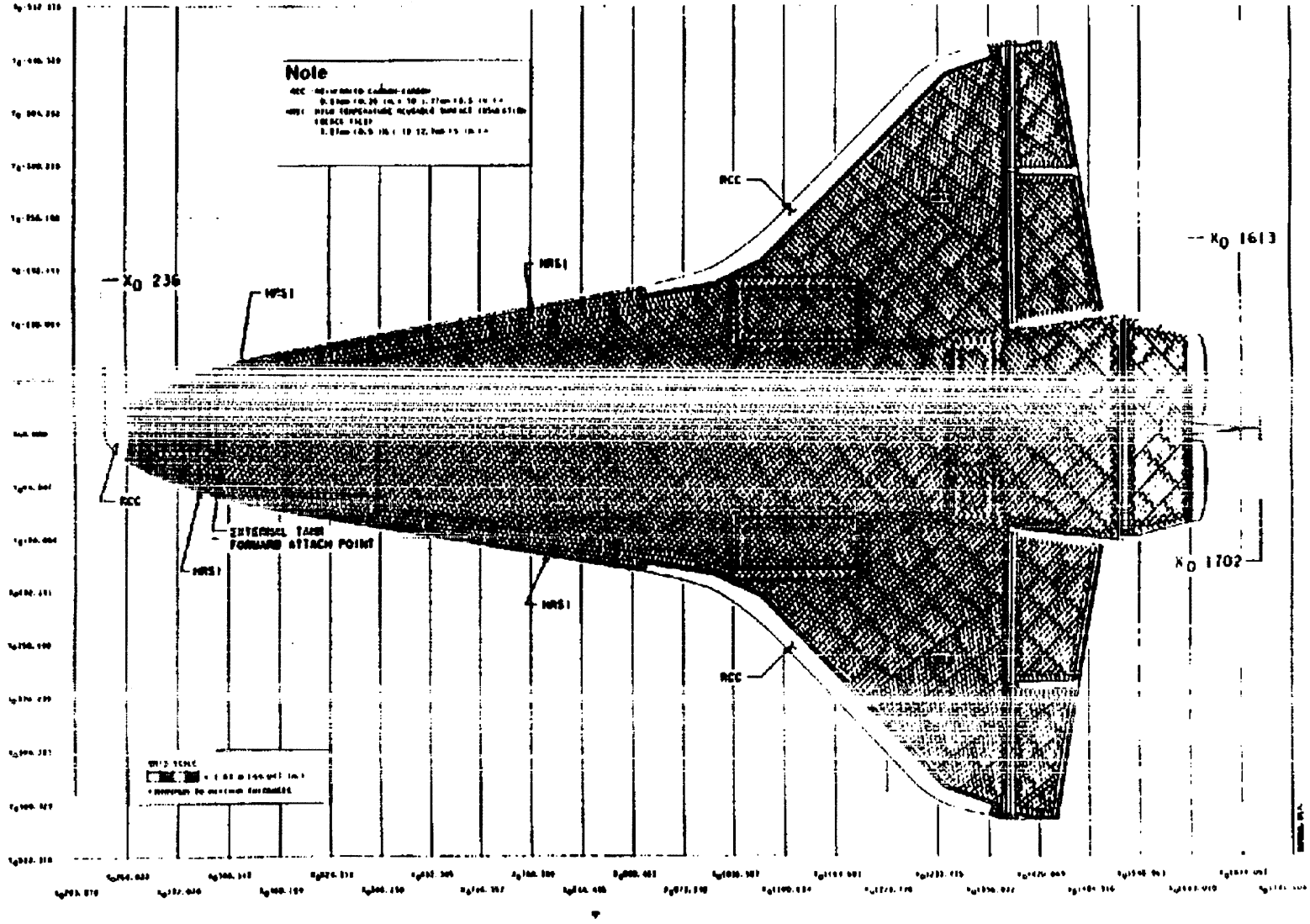


Figure 3: The black tiles (all vehicles)

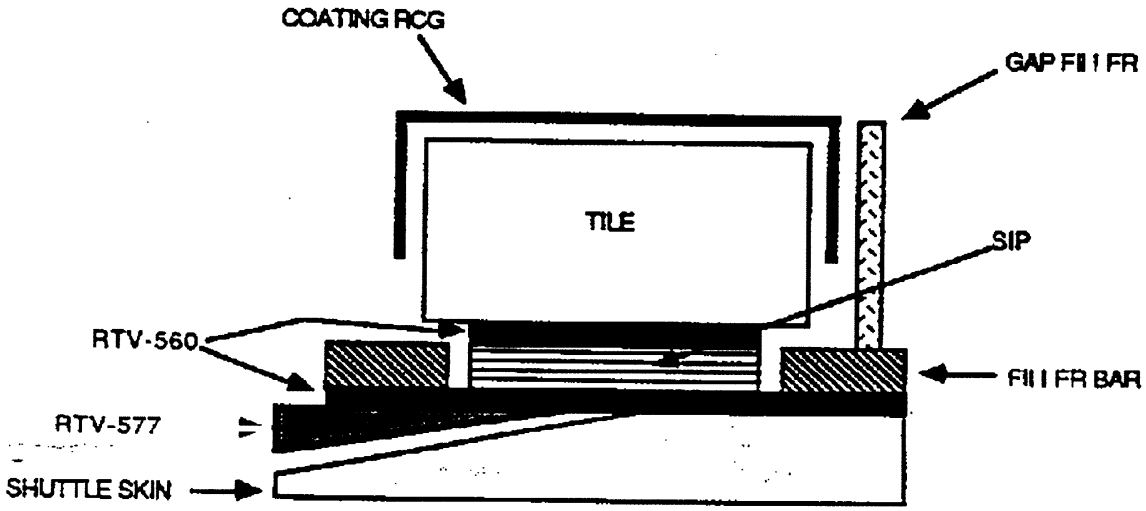
Source: Shuttle Operational Data Book, JSC 08934 Vol. 4

skin are placed around each piece of SIP. The porous tiles are allowed to vent since the RCG coating does not extend to the filler bar. Between tiles in the hotter areas (approximately 4,500 locations), gap fillers are used in addition to the filler bars to prevent gap heating damage during reentry. The gap fillers are secured in place with RTV. Figure 4 shows a typical black tile with all the related components.

2.2 Life cycle and maintenance operations

2.2.1 Tile manufacturing and installation

Because of the extreme environment in which the orbiter operates, the TPS must be made of only the purest materials. Contamination of the tiles during fabrication could lead to failure of the TPS well before meeting its 100 mission requirement. Raw material (amorphous silica fiber) has to be 99.7% pure (AW & ST, 1976).



Note: Thickness exaggerated for clarity; Screed (RTV-577) only where needed

Figure 4: The tile system

The fabrication process starts with a slurry of water and 1.5 micron diameter silica. The water is drained and binder added. This mixture is compressed into blocks slightly smaller than 1 cubic foot. After the binder sets up in 3 hours, the blocks are dried in a microwave oven. The sintering process which locks the fibers

together requires tight heat tolerances. The blocks are baked at 2,375°F for two hours. Next, they are cut into rough tiles (four to eight per block). Tile density and density gradient are verified using X-rays. Since each tile is different, the tiles are trimmed to specification using automated milling machines. A second quality check assures that the tiles are fit for coating. The coating is sprayed on and then glazed. A third quality check verifies the integrity of the coating. These tiles are then internally waterproofed with a silane material. During original construction, the tiles were next placed in arrays that matched their placement on the orbiter's surface. Each array consisted of approximately 35 tiles. The bottoms of the arrays were then shaved to match the shape of the orbiter. A fourth quality check verified the dimensions of randomly selected tiles from each array. All current replacement tiles are machined individually.

The original installation of the tiles at time of construction was done an array at a time. The SIP was first bonded to the tiles using RTV, while a lattice of filler bars were bonded to the orbiter. After these bonds had set, the entire array was bonded to the orbiter. Difficulty arose in aligning the tiles/SIP array with the grid of filler bars. If the tile/SIP array is partially resting on the filler bars instead of directly to the orbiter's skin, the strength of the TPS bond is greatly reduced. The arrays are held in place with 2-3 psi pressure while the RTV dries. Bonds are verified using a pull test on each tile. The strength of each test varies based on the location of the tile and the expected in-flight loading (2 to 13 psi). Once a tile has passed this initial pull test, it is unlikely that it will be checked again during its life cycle of 100 flights unless an anomaly is detected.

2.2.2 Flight profile loading

During a typical mission, the tiles are subjected to a wide range of loads and temperatures. These must be considered in order to determine the limitations and life cycle of the TPS. The description below summarizes a report by Cooper and Holloway (1981).

Ignition of the orbiter's main engines creates an oscillatory pressure wave that loads the tiles in the aft region of the orbiter. Though strong, this wave should dampen rapidly. In addition, acoustic pressure created by the engines can directly load the tiles and the aluminum skin. Any motion of the aluminum will, in turn, cause inertial pressure on the TPS. The amount of inertial pressure depends on the local response of the aluminum substructure, but noise levels up to 165 dB are attained during lift off. During ascent, the tiles experience a wide range of aerodynamic loads including: pressure gradients and shocks, buffet and gust loads, acoustic pressure loads caused by boundary layer noise, inertial pressure caused by substructure motion and deflection, and unsteady loads coming from vortex shedding from the connecting structure to the external tank. Almost every tile will experience loads of 160 dB during this phase of a mission.

Since the tiles are highly porous (90% void), it is during the ascent that any internal pressures must be vented in order to equalize with the external environment. Because of this, both the SIP and the tiles may experience varying degrees of internal pressure. Vent lag can cause tensile forces to build up. In addition, small residual tile stresses are caused by differences in the thermal expansion rates of the tiles and the coating. Also, any water that was absorbed will cause internal pressure as it expands and contracts with the temperature changes.

During re-entry, a second series of stresses are placed on the TPS including: substructure deformation, boundary layer acoustic noise, steady aerodynamic loads, unsteady aerodynamic loads caused by boundary layer separation and vortices, and loads from aerodynamic maneuvering. The *boundary layer transition* from laminar to turbulent flow always occurs, but the time of this transition (for the same entry trajectory) depends primarily on *vehicle roughness*. This roughness is divided into two types: discrete (one single large protuberance) or distributed (many small protuberances.) Early time of transition results in higher turbulent flow peak temperatures and higher total heat loads that depend on temperature and time of

exposure (Smith, 1989). Nearly one third of the tiles on the lower surface of the orbiter reach temperatures in excess of 1900°F and are subjected to problems of uneven thermal expansion.

The TPS has been rigorously tested and has withstood thousands of test cycles of limit load without failure. The system has then been certified for at least 100 flights. However, repeated exposure to the stresses and strains that accompany a space mission can affect the integrity of the individual components. The tiles can weaken, for example, above the densification boundary layer, the SIP can stretch as fibers pull out of the matrix, and the RTV can creep under very high loads. It is only through rigorous maintenance procedures and quality-control verifications that the true life cycle of the TPS can be determined and that acceptable system safety can be achieved.

2.2.3 Tile maintenance procedure

The maintenance procedure is guided by the Rockwell specifications (Rockwell International, 1985, 1989). It involves (1) a sequence of tile-damage inspections and assessments after landing to decide which ones can be mended and which ones must be replaced; (2) tile replacement; (3) bond verification using pull tests; (4) step and gap measurement; (5) decision to install or not a gap filler.

The steps involved in the replacement of a tile are the following:

- First prefit
- Densification
- Second prefit
- Bonding of the SIP to the tile
- Cleaning of the cavity (inspection point)
- Priming of the cavity
- Mixing (and testing) of the RTV
- Application of the RTV to the tile/SIP system

° Bonding of the tile/SIP to the cavity

° Verification of the bond.

The verification of the bond at the end of this process involves a *pull test* of variable strength. One problem that has been reported is that this pull test may not allow detection of tiles that are only partially bonded because bonding to the adjacent gap fillers may provide sufficient strength to pass the test. Though these partial bonds pass the initial pull test, they tend to be more susceptible to deterioration over time and slumping.

Step and gap measurement is meant to ensure the smoothness of the orbiter's surface and avoid the excessive heat loads due to vehicle roughness. It is currently a time-consuming procedure involving 24 measurements per tile, done manually by insertion of plastic gauges to a certain depth in the space between tiles. The result of this inspection often leads to a decision to install standard gap fillers. Several problems have been reported in this part of the work, including inaccurate measurements due to misplacement of the plastic gauges. A laser system is currently being developed to automate step and gap measurement, making it both quicker and more reliable (Lockheed Research and Development Division, 1989; SIORA, 1990). Clearly, the corresponding reliability gain for the whole TPS depends on the initial contribution of wrong steps and gaps and orbiter's roughness to the probability of failure of the TPS.

Note that this maintenance procedure is mostly *maintenance on demand.* The only random testing that occurs is in select areas where a small number of tiles are pulled to determine if there has been any weakening of the original screed caused by initial and subsequent exposures to waterproofing materials. In the absence of a non-intrusive test of the bond, the fear is that the tests themselves may weaken the tile/SIP/RTV system.

2.3 Failure history: incident recording and data bases

2.3.1 Failure history and incident recording

A history of the tile problems can best be described by grouping the difficulties into three broad categories: (1) *design problems*, (2) *processing and maintenance induced problems*, and (3) *damage caused by external debris*. This information is summarized from data compiled by Carlos Ortiz at Johnson Space Center (JSC) in Houston, Texas. It should be remembered that to date, *only two black tiles have been lost prior to or during re-entry*: one due to RTV failure caused by chemical reaction with a waterproofing agent (Challenger, Flight 41-G) and one due to debris impact (Atlantis, Flight STS-27R). Even then, there was some remaining material in the tile cavity prior to entry. In both cases, there was neither catastrophic secondary tile damage, nor burn-through of the orbiter skin. This good fortune was due in part to the location of the missing tiles and the structure under the skin. Similar losses in different locations could have been far more costly. Nonetheless, the TPS has done very well and proven to be far more robust than anticipated.

With any complex system, the design process does not stop with the initial product. Improvements occur as the system is used and weaknesses are detected. The orbiter's TPS is no different. Revisions to the original design started before the first launch, and have continued ever since. These properly redesigned components have greatly increased the reliability and maintainability of the overall system. Deficiencies that have, as of yet, gone undetected will be solved in a similar fashion providing that they are uncovered prior to a major system failure.

Design

During the initial design of the TPS, each component (tile, SIP, and RTV) was certified individually; but it was not until they were combined during the construction of the first orbiter, Columbia, that a "weak link" in the bond between the tile and SIP was indentified. Tests of the tile/RTV/SIP/Koropon as a system revealed that the

combined tensile strength was weakest at the tile-to-SIP interface. This was caused by the RTV not impregnating enough the basic tile material to insure adequate attachment. The President of Rockwell Space Systems Group stated: " I think that it is a fair criticism that we didn't define the problems more clearly as far as the tile/strain isolation pad capabilities are concerned. We worked too hard on the quality of the material alone and waited too long for the thermal analysis." (AW&ST, 25 February 1980.) Because of this oversight, many of the already installed tiles had to be retested, pulled, *densified*, and replaced. To eliminate the "weak link", the tiles are densified by applying a mixture of Dupont's Ludox AS and silica slip to the underside --or inner mold line-- of the tile to an approximate thickness of 0.010 inches. The result of this procedure is to move the "weak link" up into the tile material itself. Since the minimum strength of the basic 9 pcf material is 13 psi, the majority of the tiles now satisfy the maximum induced-load requirements. Many of the installed tiles were known to have greater than the minimum 13psi strength and could be shown to have positive margins for flight loads. The tiles that could not be shown to meet flight loads with a positive margin were replaced with 22 pcf tiles whose minimum strength far exceeds the maximum flight loads. This additional work meant that the 30,000 tiles on Columbia required more than 50,000 tile installations before the first flight. Even so, not all the tiles were densified prior to the first launch, but were deemed acceptable based on proof load testing to 1.25 times the limit stress. For all the orbiters after Columbia, the tiles were densified during installation.

Even though the overall temperatures reached during re-entry were less than the maximum allowable, tiles in three areas were found by flight experience to be subjected to local thermal degradation and/or unacceptable thermal gradients resulting in a negative margin for the mid-fuselage structure. Three redesign solutions were used to resolve these area-related problems. Tiles inboard and forward of the main landing-gear doors (denoted as "location A" tiles) were knowingly made thinner than the initial thermal design thickness to minimize weight and to retain the aerodynamic mold line. The thin tiles were able to maintain the

structural temperature limits because the initial flights were flown from the Eastern Test Range at Kennedy Space Center, while the "thermal" design trajectory was based on launches from the Western Test Range, which put a greater heat load on the structure. However, extensive analyses, both thermal and stress, showed unacceptable negative structural margin due to thermal gradients. These negative margins were initially resolved by internal structural modifications and by installing internal heat sink material. Later, the "location A" tiles were replaced with slightly thicker tiles (approximately 1/10 inches thicker) which still provided an acceptable aerodynamic outer mold line based on flight data evaluation. Tiles between the nose cone and nose landing gear were receiving excessive heating, which caused tile slumping and subsurface flow. These tiles were eventually replaced with a much more durable RCC chin panel. A similar problem occurred with the elevon cove tiles. In this case, the size of the tiles was increased, thus reducing the number of troublesome gaps. All three modifications have proven successful.

Processing and maintenance.

The most critical TPS problems related to processing and maintenance have occurred with various waterproofing agents that have affected the strength of the RTV by reacting chemically with the bond. However, in addition, a significant set of other problems have arisen because of maintenance errors. Initial waterproofing was done with an external application of Scotchgard to the tile surfaces. This was not totally effective because the waterproofing degraded with exposure to rain and sunlight. On the second flight, tiles that had absorbed and trapped water, fractured when ice formed in orbit. This defined a need for an internal waterproofing agent. In addition, the Scotchguard was found to chemically attack the RTV-560. Fortunately, this was discovered immediately after an accidental overspray. The first internal waterproofing agent, HMDS, was found to react with the screed (RTV-577), slowly reverting it from solid to liquid. This interaction between waterproofing and screed was not immediate, and eventually led to the loss of a black tile. Fortunately, the other nearby tiles affected by the softened screed did not fail during reentry. A

second generation of waterproofing, DMES, has been developed and proven successful. However, the long-term, residual effects of the outdated HMDS are still causing concern.

Several chemical spills during tile installation have necessitated the removal and rebonding of nearly 1,000 tiles. These spills, involving an oxidizer on Columbia and hydraulic fluid on Challenger, demonstrate the sensitivity of the tiles and their bonds to their maintenance environment. Another incident involved the mislabeling of a container of the bonding agent. RTV-566 was labeled as RTV-560 which has a shorter drying time. The bonds were not allowed to cure for the appropriate time and thus were weaker than allowed. This discrepancy was caught during final pull testing. Finally, during a return flight from California to Florida on the back of a 747, the orbiter Columbia was flown through a rainstorm, damaging over 1,000 tiles of which 250 needed replacement.

Debris

Since the first flight, the orbiter has always been exposed to external debris damage. Table 1 summarizes the damage by listing total number of hits and major hits (greater than 1 inch). Simple statistical analysis demonstrates the great variation that has occurred (Total Hits: mean = 179, standard deviation = 157; Hits ≥1": mean = 51, standard deviation = 60). This variability is further highlighted in Figure 5, which shows histograms of the debris damage (for the upper graph, number of flights as a function of the total number of debris hits; for the lower graph, number of flights as a function of the number of hits greater than one inch). For the first flights (until STS-27R), the actual major source of debris was found to be from portions of SOFI insulation from the External Tank (ET). During STS-27R, the orbiter's TPS experienced significantly more debris damage than on any previous flight, including the loss of a large portion of one black tile (Orbiter TPS Damage Review Team, STS-27R, 1989). Based on the pattern of damage and the recovery of actual debris material lodged in the tiles, AFRSI, and gaps, it was possible to

Sequence	Designation	Orbiter	Date	Major Debris Hits > 1"	Total Debris Hits
1	1	Columbia	04/12/81	•	•
2	2	Columbia	11/12/81	•	•
3	3	Columbia	03/22/82	•	•
4	4	Columbia	06/27/82	•	•
5	5	Columbia	11/11/82	•	•
6	6	Challenger	04/04/83	36	120
7	7	Challenger	06/18/83	48	253
8	8	Challenger	08/30/83	7	56
9	41H	Columbia	11/28/83	14	58
10	41B	Challenger	02/03/84	34	63
11	41C	Challenger	04/06/84	8	36
12	41D	Discovery	08/30/84	30	111
13	41G	Challenger	10/05/84	36	154
14	51A	Discovery	11/08/84	20	87
15	51C	Discovery	01/24/85	28	81
16	51D	Discovery	04/12/85	46	152
17	51B	Challenger	04/29/85	63	140
18	51G	Discovery	06/17/85	144	315
19	51F	Challenger	07/29/85	226	553
20	51I	Discovery	08/27/85	33	141
21	51J	Atlantis	10/03/85	17	111
22	61A	Challenger	10/30/85	34	183
23	61B	Atlantis	11/26/85	55	257
24	61C	Columbia	01/12/86	39	193
25	51L	Challenger	01/28/86	•	•
26	26R	Discovery	09/29/88	55	411
27	27R	Columbia	12/02/88	250	707
28	29R	Discovery	03/11/89	23	132
29	30R	Atlantis	05/04/89	56	151
30	28R	Columbia	08/08/89	20	76
31	34R	Atlantis	10/18/89	18	53
32	33R	Discovery	11/22/89	21	118
33	32R	Columbia	01/09/90	15	120

Table 1: Summary of orbiter flights and debris damage

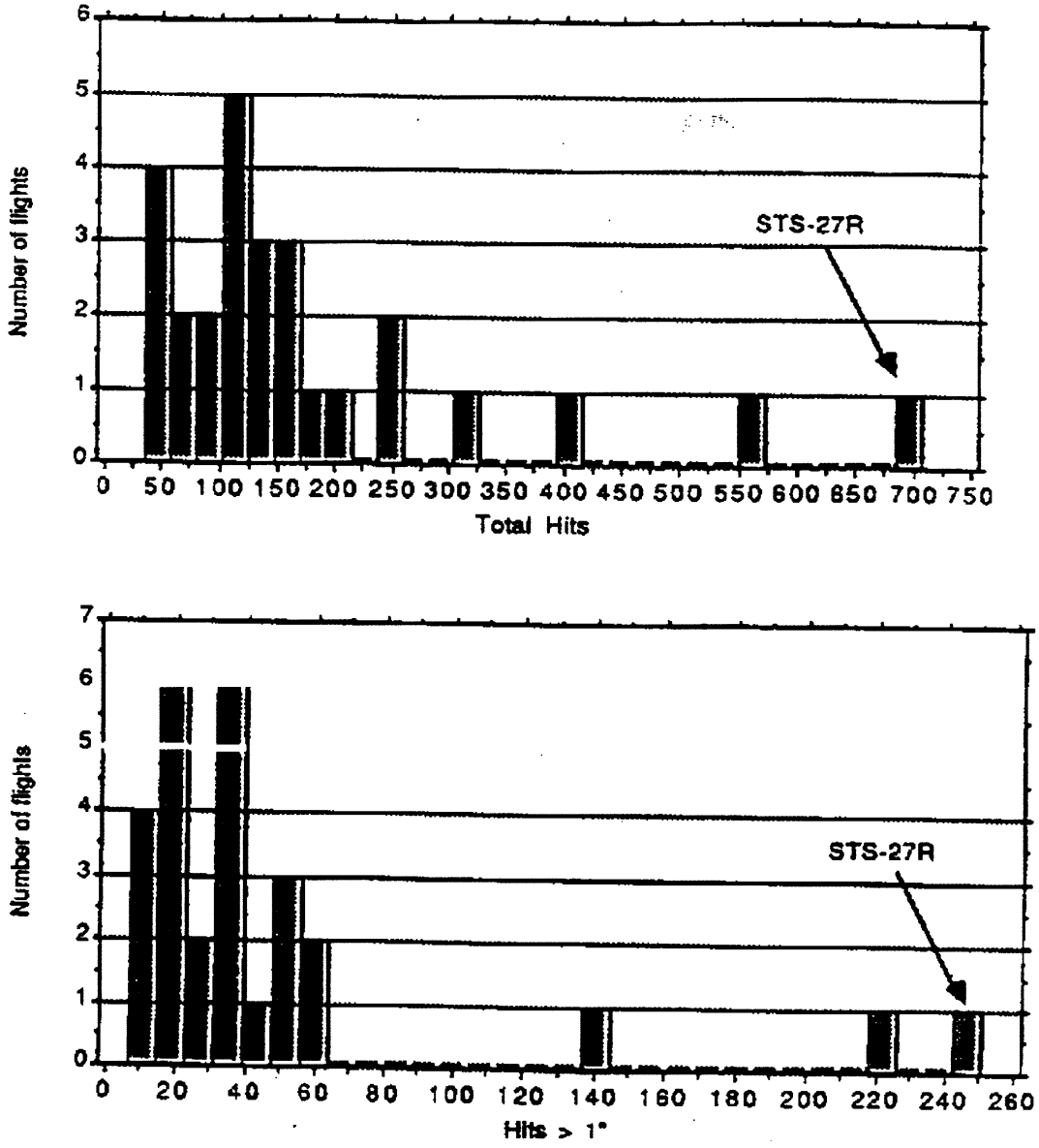


Figure 5: Histogram of tile damage due to debris.

Indicates the number of flights that experienced a specified amount of debris damage (i.e. four flights had 40-60 total hits, two different flights had 60-80 total hits, etc.) based on available data for the first 33 flights (missing: first five missions and STS-51L)

determine that much of the severe damage was caused by insulation from the cone area of the right SRB. Other damage, minor but more extensive than usual, was caused by the insulation of the ET. This was similar to the type of damage that had been experienced in previous flights. In addition, an in-depth analysis done at the time concluded that there was no obvious correlation between tile damage and launch conditions that might affect ice formation, which was considered earlier a possible source of tile impact damage (Orbiter TPS Damage Review Team, STS-27R, 1989).

Figure 6 displays on one orbiter surface a cumulative recording of all significant tile damage from all flights and all orbiters (through STS-32R.) The damage is obviously not uniformly distributed, and certain tiles are much more likely to be damaged than others. Computer models developed by Ray Gomez at JSC have been able to show how insulation from both the SRBs and the ET could cause such damage (see Figures 18 and 19 in Section 3.) The complexity of the problem does not currently allow for a direct and focused backtracking from a tile on the orbiter to a particular spot of insulation because the trajectory depends on many factors (e.g., the velocity of the orbiter and the angle of attack.) It may be possible, however, to determine roughly the initial location and the size of loose insulation necessary to inflict specific damage (location and severity) to the tiles.

Debonding of tiles due to factors other than debris impact

To date, as mentioned above, only one black tile has been lost due to factors other than debris impact (in that case, chemical reversion of the screed). There are several reasons for unsatisfactory bonds: 1) improper alignment during installation, 2) failure to comply with RTV drying limitations, 3) chemical reversion of the screed or RTV, and 4) possible weakening of various components in the TPS under repeated load cycles. An initial investigation of a small discrete set of tiles showed that a high proportion of the bonds that had pssed the pull test were later found to be unsatisfactory (see Figure 7). Since then, however, this number has been found to

Paté-Cornell and Fischbeck

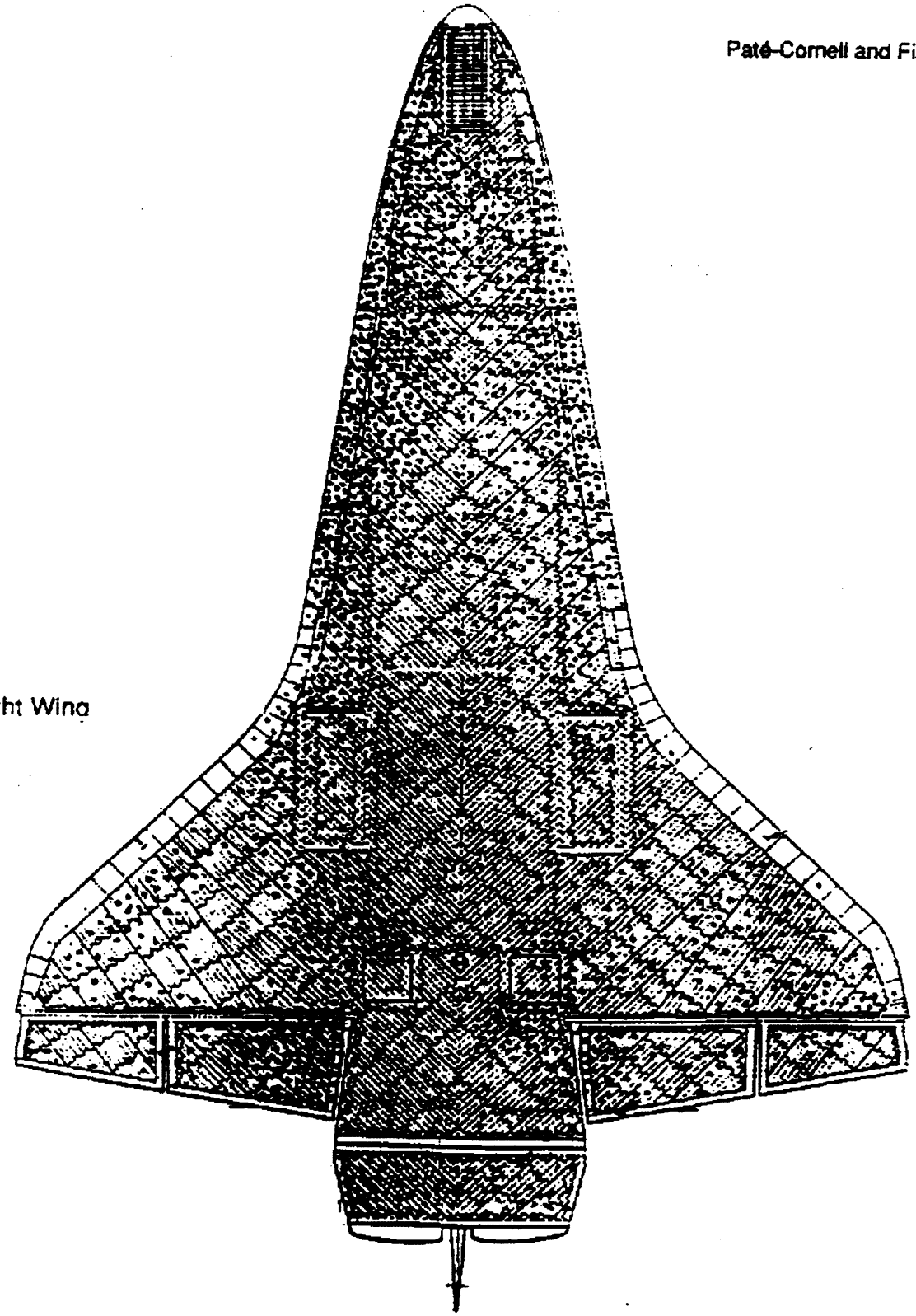
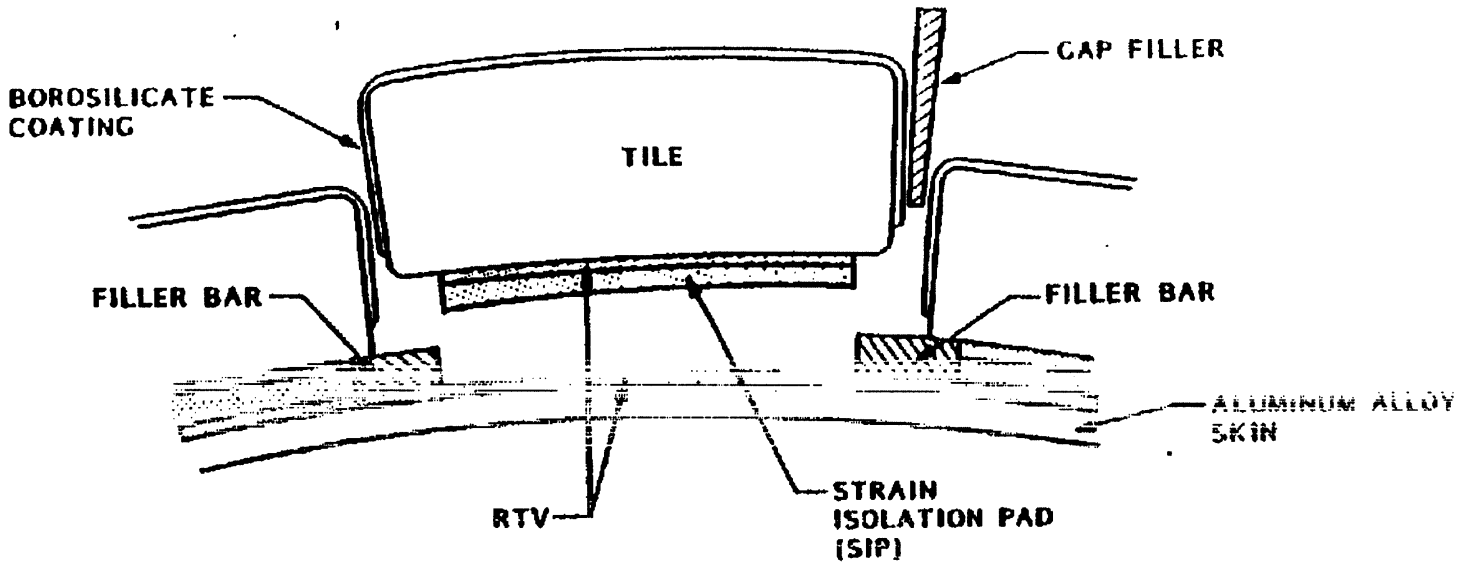


Figure 6: Accumulated major debris hits (lower surface)
for flights STS-6 through STS-32R

Source of data: J. McClymonds, Rockwell International

PROBLEM OVERVIEW



PROBABLE CAUSE OF BOND PROBLEMS

- POOR ADHESION BETWEEN SIP AND RTV
- POOR ADHESION BETWEEN RTV AND ORBITER SKIN
- PHYSICAL INTERFERENCE IN CAVITY; SIP RESTS ON EDGE OF FILLER BAR

CURRENT BOND CERTIFICATION METHOD IS A PULL TEST

- INADEQUATE: >20% CERTIFIED BONDS LATER FOUND UNACCEPTABLE

Figure 7: The tile system and bond verification

Source: Lockheed Corporation (1989), R. Welling. Reproduced by permission

be much smaller. A recent and on-going evaluation of all 9,045 tiles using the 0.090 and 0.115 inch SIP has shown that of the 6,517 tiles evaluated to date, only 8 showed anomalous conditions (most of which, but not all, were subnominal bonds). So far, during normal maintenance and the replacement of debris-damaged tiles, 12 tiles have been found to have no bond between the SIP and the orbiter's skin. These tiles were only held in place by the gap filler's bond to adjacent tiles.

As mentioned earlier, the SIP is bonded to each tile using RTV while the filler bars are bonded to the skin. After all these bonds have firmed, a layer of RTV is placed on the skin in the hole defined by the filler bars. The tile/SIP combination is then held in place completing the installation. If the tile/SIP combination is not aligned correctly with the filler bars, the SIP may rest on the filler bars and never touch RTV or skin. Obviously, these tiles will have very poor bonds. In several cases the tiles were placed correctly between the filler bars, but directly over exposed sensor wires. These wires prevented complete contact between the SIP and the RTV and thus made for a weak bond. It should be noted that even with no primary bond between the SIP and the skin, tiles have still passed the pull tests (because of the gap filler bonds) and that, as of yet, no tile has been lost due to poor installation.

If the RTV is allowed to dry before the tile/SIP combination is placed on it, the bond will not develop to its full potential. This can happen when several tiles are been placed at one time, and a single batch of RTV is mixed for the several prepared sites. If the installersare not careful, the RTV may exceed its "pot life", i.e., the age beyond its safety margin, before the last tile is placed.

The chemical transformation of the RTV is very sensitive to temperature and humidity and must be monitored carefully during installation. In several cases, the curing time of the RTV has been reduced by the installers using water (or saliva). Such a procedure, which is explicitly forbidden, is not believed to affect the immediate strength of the bond, but may reduce its life. A similar class of problems

has occurred when the aluminum surface has not been properly prepared. In this case, the RTV bond may fail at the interface with the orbiter's skin.

The only black tile that has been lost due to debonding not caused by debris occurred when the first internal waterproofing agent, HMDS, reacted chemically with the screed causing it to soften and revert back to its more viscous form. The formula of the waterproofing agent has since been changed so that it will not affect the screed. This new waterproofing agent has completed 50 mission cycles on combined-environment testing, and no weakening of the TPS system was found. Yet, careful monitoring is required to ensure that no residual amounts of the old HMDS agent are causing a very slow reversal reaction and, eventually, loss of tiles. The current HMDS testing procedures involve removing two or three tiles after each flight to check the chemical composition of the screed. To date no additional problem has been found.

In the long term, repeated exposure to load cycles and environmental conditions of heat and humidity on the ground may weaken some of the TPS components and, eventually cause tile failure. The most vulnerable tiles are those with no bond or very little bond (e.g., less than 10% of the surface) between the SIP and the orbiter's skin, and that are held primarily by the gapfiller's RTV bond to the adjacent tiles. RTV bonds, so far, have not shown visible signs of deterioration over time and load cycles. It is known, based on extensive testing, that the hundred-flight certification is justified for well-bonded tiles. What will happen in the future, however, is uncertain.

After some flights, several cases of slumping (sagging) tiles have been observed. These are easily identified visually since they break the smooth surface of the orbiters. According to David Weber at KSC, the most common cause of slumping is a weakening of the SIP's fibers due to repeated load cycles. Pre-densification testing showed that the part of the tile located right above its

interface with the SIP was the weakest part and was most likely to be affected by repeated load cycles. With densification, this weakest zone has moved, on one hand, further up into the tile, and on the other hand, down into the SIP itself. A problem in either location is difficult to detect if there is not overt visual clue. Yet, once again, to date no tile has been lost due to repeated load cycles.

2.3.2 Data bases:

Three data bases have been identified and described by Ellen Baker and Bonny Dunbar as part of their TPS Trend Analysis Survey (March, 1988). They are:

- **PRACA** (Problem Reporting and Corrective Action) which is managed by NASA. Tile problems constitute only a subset of these data. The information regarding the tiles can be accessed at KSC.
- **TIPS** (Tile Information Processing System) which is managed by Rockwell (Downey, California). The specialist is Ms. B. J. Schell, supervisor of the TPS Data Systems at Rockwell International, Downey, California. The information can be accessed at Downey, JSC, and KSC.
- **PCASS** (Program Compliance Assurance and Status System) which is part of a NASA (agency-wide) System Integrity Assurance Program Plan.

PRACA and TIPS are described in Appendix 2. The survey conducted in 1988 by Baker and Dunbar showed that a trend analysis was judged highly desirable:

1. To monitor the performance of the TPS in order to ensure conformance with design requirements
2. To ascertain long term effects of TPS-related procedures (repairs, etc.).
3. To enable engineering design changes to system failure.

The participants to the survey indicated that there was a need for a single user-friendly data base including all useful data and, in particular, results of trend analysis. They would want to have routine access to this data via a local PC or

terminal. As we show in section 4, the risk-criticality index that we have developed can be an important part of the record for trend analysis because it represents the relative contribution of each tile to the probability of LOV due to TPS failure. These probabilities can be updated on the basis of new information and the results can be encoded for all tiles that share similar characteristics.

Section 3:
DESCRIPTION OF THE PRA MODEL FOR THE TILES

3.1 Susceptibility and vulnerability

Our probabilistic risk assessment (PRA) model for the black tiles of the thermal protection system (TPS) of the space shuttle is based on two major factors: *susceptibility* of the tiles to damage and *vulnerability* of the shuttle once tile damage has occurred. The terms susceptibility and vulnerability have been standardized in the study of aircraft combat survivability; their use in the space shuttle context may facilitate the understanding of the problem.

Susceptibility of the tile system to damage is determined by the combination of *loads* on the tile and its *capacity* (strength) to withstand them. Failure occurs when the loads exceed the capacity. The problems can generally be divided into two categories: (1) tile loss caused by excessive external loads and (2) tile loss under regular loads caused by weaknesses in the tile system (debonding due to factors other than debris impact). A third possibility (a combination of the two) is the case where external loads not severe enough to cause the loss of a well-bonded tile, causes the loss of a weakened tile. In this study, this case is treated as a subset of the first category. Historically, the vast majority of excessive external loadings has been from *debris*, mostly from the external tank and the solid rocket boosters (defective insulation and ice). Also included in this category is space debris. Depending on the size and energy of the debris hitting the orbiter, several tiles can be damaged simultaneously. It is also conceivable that the reentry *temperature* may exceed the designed capabilities of the tiles, leading to tile failure or burn-through (for example, due to severe malfunction of the guidance system).

Capacity reduction caused by weaknesses of the tile system account for tile losses caused by long-term deterioration of the RTV, defective bonds not caught

during installation, and tile bonds weakened due to improper maintenance procedures, waterproofing, and spills. These weaknesses could affect a single tile (tile resting on its filler bar) or a group of tiles (use of a weak batch of RTV). Tile susceptibility can therefore be reduced by controlling the external debris, improving tile installation and maintenance procedures, and developing new tests (non-destructive pull tests and other types of tests) to ensure bond verification. Another approach to reducing the susceptibility of the tile system that will not be considered in this study would be to harden the tiles so that the impact of external debris would not cause any damage. Extensive use of RCC would be one such solution, but at the cost of a significant increase of weight and design complexity, as well as an enormous additional expense.

The vulnerability analysis starts with the premise that a tile has been lost for whatever reason, then proceeds to analyze the effects of this loss on the shuttle's performance and safe return. Of primary concern in this phase is the layout of the shuttle systems immediately below the shuttle's skin. A heating or burn-through of the skin could cause the loss of various hydraulic lines, computers, fuel tanks, or even a weakening of the structural integrity of the spacecraft. Also included in the vulnerability analysis is the effect of an initial loss on the surrounding tiles. When the TPS was developed, it was feared that one hole could lead to adjacent tiles peeling off because of reentry heating (the so-called zipper effect). This phenomenon has not occurred in the two instances where tiles have actually been lost. Yet, the loss of a tile clearly causes a local turbulence and exposes directly the side of the next tile/SIP/RTV system to high loads (forces and heat). The probability of loss of a secondary tile, although obviously not equal to one, is still higher than the probability of loss of the first tile in a patch. If not checked, the loss of subsequent tiles could lead to exposure of a much larger patch of the shuttle's skin. The vulnerability of the orbiter could be reduced by moving, hardening, or increasing the redundancy of various critical control systems. If the tile damage can be discovered prior to reentry, then, in some cases, the vulnerability of the shuttle could be reduced (either by

protecting the exposed patch or by rerouting, draining, or securing exposed lines and tanks.) In addition, by changing the reentry flight profile of the shuttle, it may be possible to reduce the temperature of some weak, vulnerable areas. The sequence of events that is studied in this analysis is shown in Figure 8.

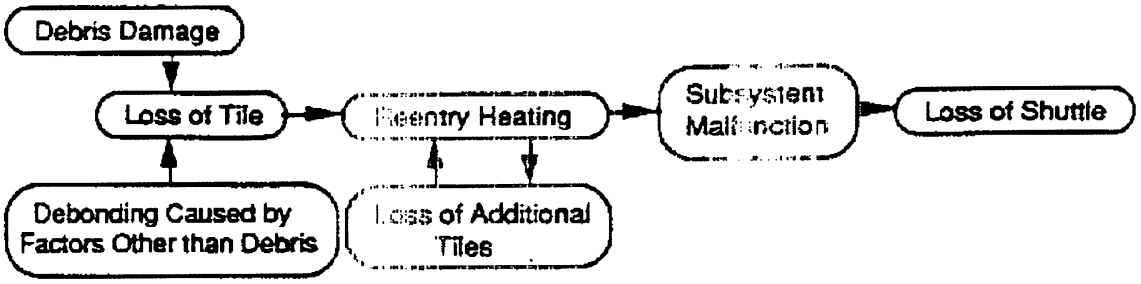
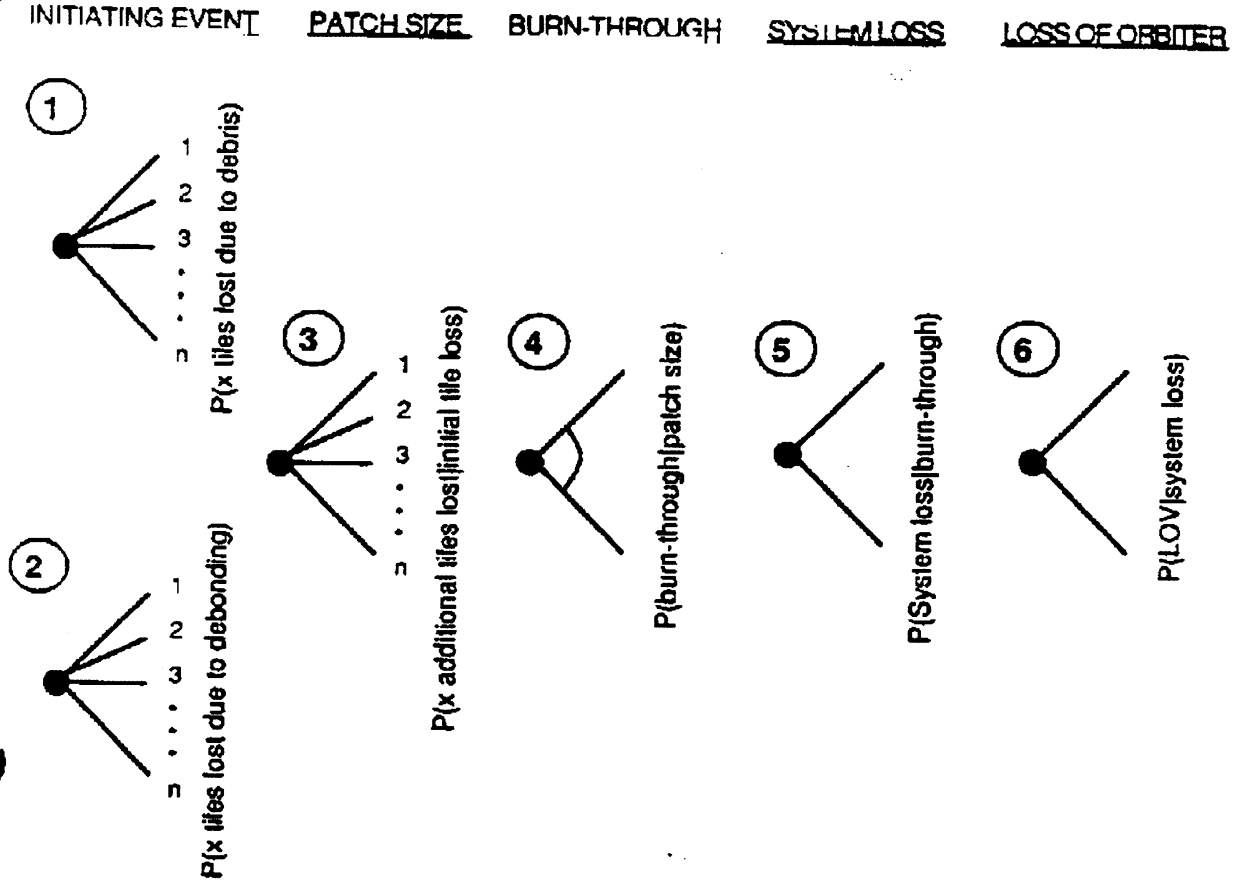


Figure 8: Event diagram: failure of the TPS leading to LOV

The structure of the probabilistic model used in the analysis (Figure 9) follows closely that of the elements presented in Figure 8. It includes: (1) *initiating events* (probability distributions for the number of tiles initially lost due to debris and to debonding caused by other factors), (2) *final patch size* (probability distribution of the number of adjacent tiles lost conditional on the loss of the first tile), (3) *burn-through* (probability of burn-through conditional on a failure patch of a given size), (4) *system loss* (probability of failure of systems under the skin conditional on a burn-through), and (5) *loss of orbiter* (probability of LOV, conditional on failure of subsystems due to burn-through.) The analysis is thus done using the usual mix of probabilities estimated through frequencies, and of subjective probabilities when needed (e.g., for the probabilities of failure of subsystems under the skin for which no formal PRA studies have been done). Bayesian formulas were used to compute the probabilities of different scenarios as described further in this section.

Note that, in this study, we did not account for excessive heat loads (above the design criteria) causing the burning of a tile due, for example, to tile design problems or to a malfunction of the guidance system and/or the control surfaces.



1. Discrete random variable: number of initial tiles lost due to debris
2. Discrete random variable: number of initial tiles lost due to debonding
3. Discrete random variable: number of additional tiles lost given initial tile damage
4. Continuous random variable: severity of burn-through given a patch size of missing tiles
5. Binary random variable: subsystem failure occurs given level of burn-through
6. Binary random variable: LOV occurs given loss of subsystems

Figure 9: Event tree of LOV due to TPS failure

Although this failure mode may contribute to the overall risk of failure of the orbiter's TPS, it was considered here that these initiating events now have a much lower probability than the loss of a tile due to debris damage and/or debonding caused by other factors.

We did not account for dependencies among the probabilities of failures of subsystems under the skin due to TPS failure; for example, two redundant elements of the hydraulic system could be crippled during the same flight by loss of tiles in two different locations. The probability of such simultaneous failures was considered to be too small. Finally, we did not account for dependencies among tile failures caused by the repetition of the same mistake (e.g., from the same technician) which becomes a common cause of failure (for example, addition of water to the RTV mix and treatment of several tiles). This concern will be part of the second phase of the study.

3.2 Definition of min-zones

Because of the factors described above, the black tile system cannot be treated as a uniform structure. Debris is more likely to hit some parts of the orbiter than others, different bonding materials are used in different areas, temperatures vary considerably over the surface, and critical subsystems are located only in a few areas. Therefore, for this analysis, the entire tile protection system is subdivided into smaller areas, called here *min-zones*, such that *all tiles of a specific min-zone have the same level of susceptibility and vulnerability*. Depending on the number of discriminating characteristics, the number of tiles in each min-zone could conceivably vary from a single tile to thousands. (An alternative approach would be to categorize each tile individually with regard to susceptibility and vulnerability, but since most adjoining tiles have identical characteristics, this level of detail is not needed.)

The definition of min-zones is critical to the analysis. The number of factors used to delineate the min-zones determines the complexity of the problem. As an initial cut, we define a min-zone by four factors: (1) susceptibility to debris impact, (2) potential for loss of additional tiles following the loss of the first one (depending on heat and aerodynamic loads), (3) potential for burn-through given one or more missing tiles (heat loads), and (4) criticality of underlying systems. For this study, it is assumed that the probability of debonding caused by factors other than debris impact is uniform over the orbiter's surface and does not require a separate partition of this surface. As mentioned above, it is also assumed that flight profiles will not expose the entire TPS to severe temperatures that would exceed their specifications.

3.2.1 Debris classification

In order to account for the fact that debris damage during ascent is not uniformly distributed across the underside of the orbiter, the black tiles are partitioned into three *debris areas* such that all tiles in a particular area have roughly the same probability of being initially damaged by external debris. The definition of these debris areas also accounts for the fact that some areas are more susceptible to being hit by large pieces of debris that will damage several adjacent tiles simultaneously.

To define the debris zones, we plotted all known debris damage from the first 33 flights on a single shuttle layout (see Figure 6.) These data came from J. W. McClymonds (1989) at Rockwell in Downey. Areas with similar damage intensity were grouped together into high, medium, and low debris damage areas (see Figure 10.) An estimated probability of tile damage due to debris per flight was determined by dividing the number of hits by the number of tiles in each area and by the number of flights. A similar plot and calculation was done for all damage to black tiles over one inch in size. (Historically about one fourth of the damage has been greater than one inch in size.) It should be noted that the only missing tile to date caused by debris is in one of the "high debris damage areas".

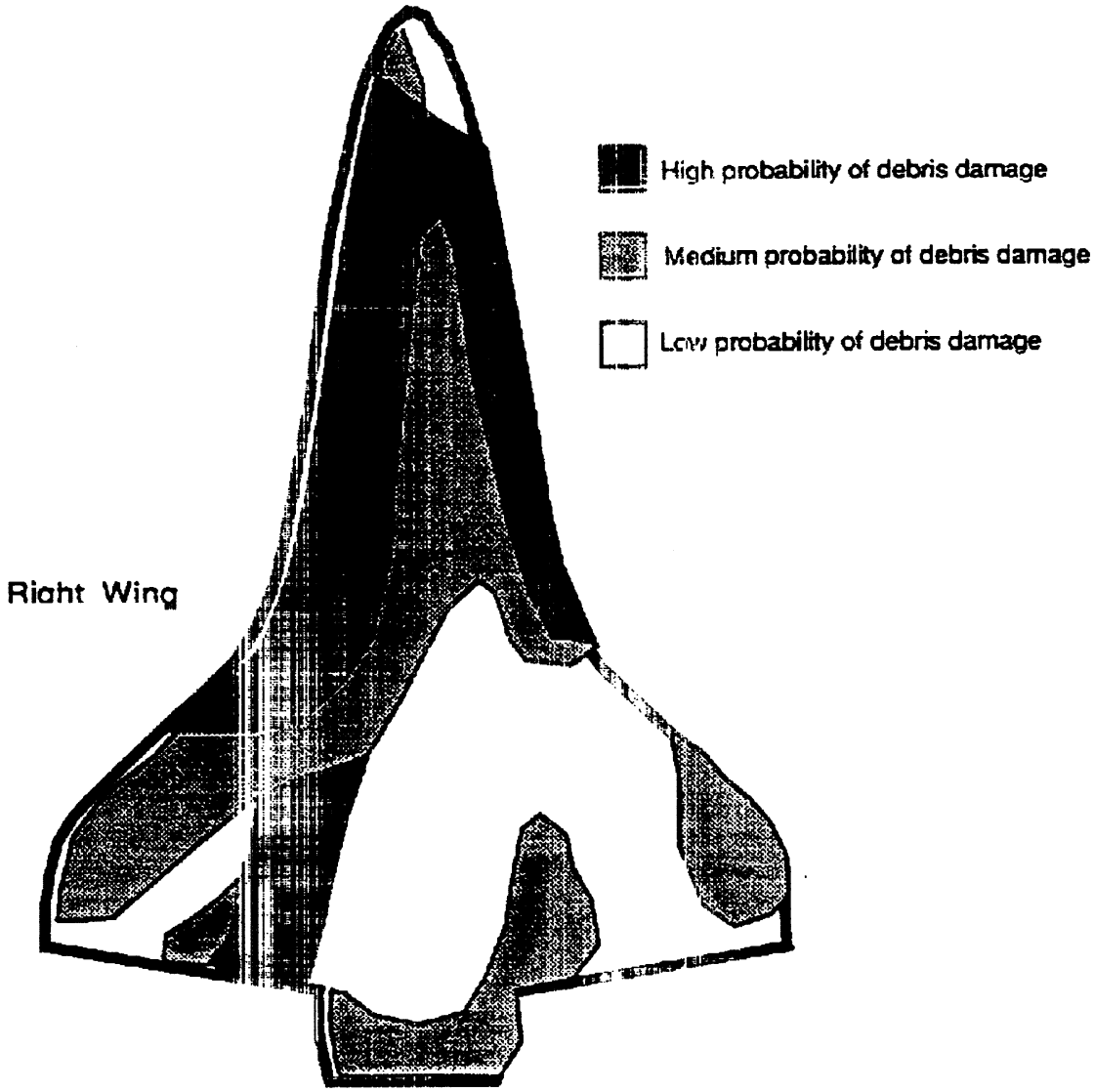


Figure 10: Partition of the orbiter's surface into three types of debris zones (index: h)

Based on this analysis, the probabilities of a specific tile receiving *any debris damage* were assessed as shown in Table 2. The probability of multiple tile damage was calculated using a typical six-inch by six-inch square tile and estimating the percentage area, within a 1/2 inch border, that would allow for other tiles to be hit simultaneously with sufficient energy to cause significant damage.

Debris Area	High	Medium	Low
P(Single tile hit)	10^{-2}	$3x10^{-3}$	$5x10^{-4}$
P(One of two tiles hit)*	$8x10^{-4}$	$2x10^{-4}$	$4x10^{-5}$
P(One of three tiles hit)	$7x10^{-5}$	$2x10^{-6}$	$3x10^{-6}$

*P(one of x tiles hit) = probability that a particular tile is in a group of x adjacent hit tiles

Table 2: Probabilities of debris hits in the different areas shown in Figure 10

Translating this information into the probability that a specific tile will be knocked off or so significantly damaged as to burn off during reentry is a more difficult task. It is logical to assume that the probability of this level of damage is the ratio of the number of destructive hits to the total number of hits in the past. Since one tile has been lost out of roughly two thousand significant debris hits, it is proposed, in this study, to use an initial estimate of 1 in 2,000 ($5x10^{-4}$) for the probability that large hits would destroy a tile's insulating capability in the high debris areas. Slightly smaller probabilities were used in the medium and low debris areas. The probabilities of tile loss due to debris hits for each tile in each area of Figure 10 have been further allocated as shown in Table 3. For example, the probability of a single tile loss in "high" debris area is the product of (1) the probability that the tile is hit by a debris, (2) the probability that the size of the hit is greater than 1" conditional on a hit and (3) the probability that the tile is knocked-off given a large debris hit.

Debris Area	High	Medium	Low
P(Single tile lost)	1.3×10^{-6}	10^{-7}	10^{-9}
P(One of two tiles lost)*	10^{-7}	10^{-8}	0
P(One of three tiles lost)	10^{-8}	10^{-9}	0

*P(one of x tiles lost) = probability that a particular tile is in a group of x adjacent lost tiles

Table 3: Probabilities of tile loss due to debris in the different areas shown in Fig. 10

3.2.2 Burn-through classification

In a similar fashion the tiles are partitioned into three *burn-through areas* (see Figure 11.) The probability of a burn-through is dependent on two factor: the temperature that the surface reaches during reentry (and for how long), and the ability of the unprotected aluminum skin to dissipate the heat build up. The denser and stronger the structure under the skin, the greater the capacity to resist burn-through. In both cases where tiles have been lost, burn-through has not occurred in part for this reason. The larger the patch of missing tiles, the greater the likelihood of burn-through. The probabilities shown in Table 4 were estimated from information provided by Robert Maria of NASA Johnson Space Center in Houston. Once again, these are only coarse estimates.

Burn-through Area	High	Medium	Low
P(Single tile lost)	0.2	0.1	0.001
P(One of two tiles lost)*	0.7	0.25	0.01
P(One of three tiles lost)	0.95	0.7	0.1

*P(one of x tiles lost) = probability that a particular tile is in a group of x adjacent lost tiles

Table 4: Probabilities of burn-through due to tile loss in areas shown in Fig. 11

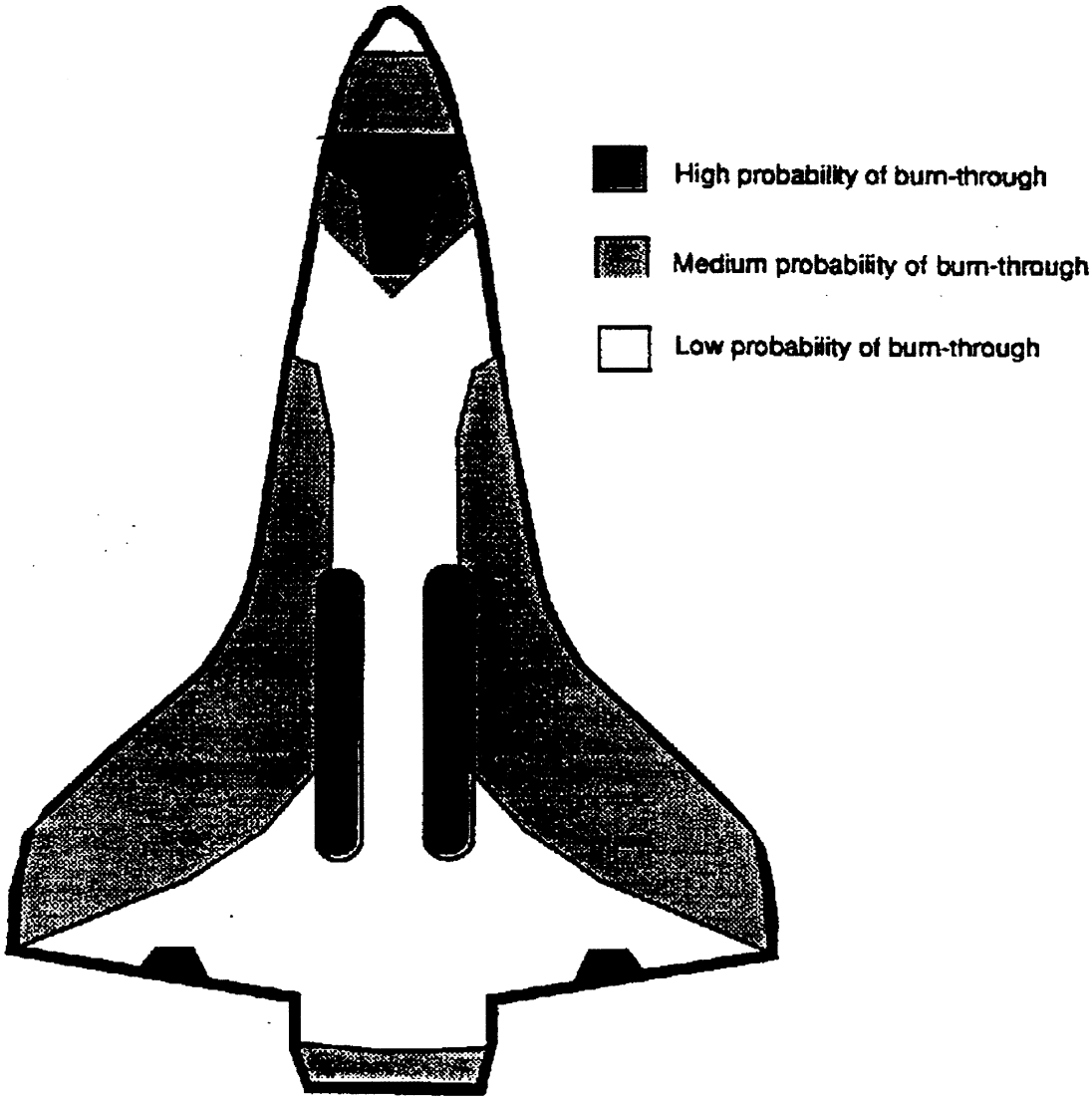


Figure 11: Partition of the orbiter's surface into three types of burn-through zones (index: k)

Note that the two areas just in board of the main landing gear have been notated as being in the high burn-through area. This is not, strictly speaking, a burn-through problem. The structure in those areas is extremely sensitive to temperature differences and would fail even without a burn-through. However, because of their sensitivity to temperature, these two areas were grouped in the high burn-through category.

3.2.3 Secondary tile loss classification

In order to account for the potential of a single tile causing the loss of adjacent tiles, the orbiter is divided into two *secondary tile loss areas* (see Figure 12.) The probability of additional tile loss depends on the aerodynamic forces and on the magnitude and duration of the increased reentry temperatures that occur around a missing tile due to the disruption of the laminar flow. This increase of temperature also depends on the ability of the skin to dissipate the heat build-up. The RTV bond will fail above 500°F. Because of this, the secondary tile loss areas are related to the temperature areas used in the burn-through analysis above. In this study, the two secondary tile loss areas will be defined by the probability of adjacent tile loss shown in Table 5. These values were estimated from information provided by Robert Maria from NASA in JSC.

Zone 1 (high loads): P(Additional tile lost | One tile lost) = 10^{-2}

Zone 2 (low loads): P(Additional tile lost | One tile lost) = 10^{-3}

Table 5: Probabilities of losing adjacent tiles
due to initial tile loss in areas shown in Figure 12

A *failure patch* is defined as a group of lost tiles that started from one initiating event (initial tile loss) and has reached its maximum size. The size of a failure patch depends on the number of tiles initially damaged and on the subsequent vulnerability of the adjacent tiles.

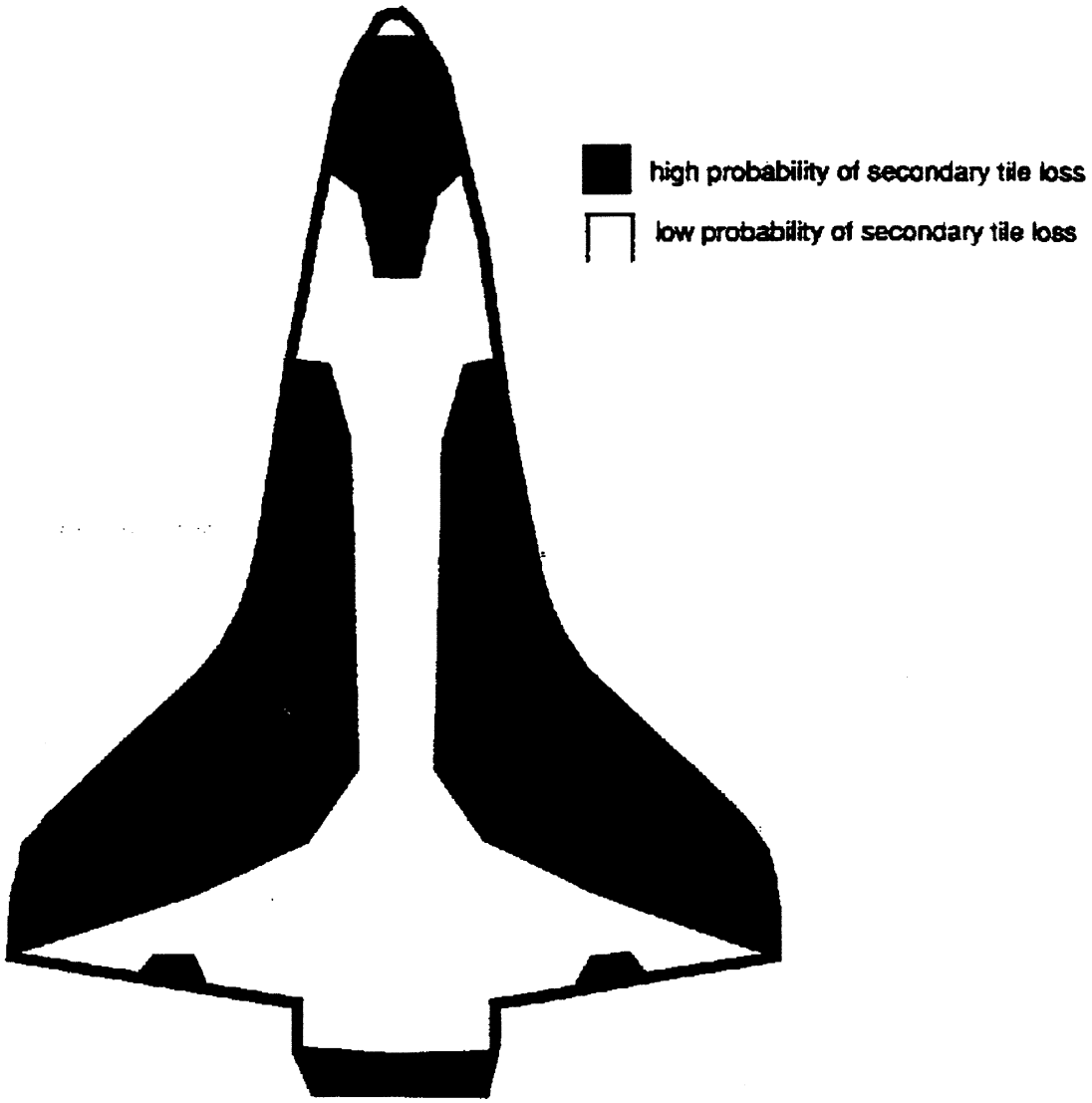


Figure 12: Partition of the orbiter's surface into two types of secondary tile loss zones (index: *i*)

3.2.4 Functional criticality classification

The varying criticality of the subsystems of the orbiter located under the aluminum skin is handled by partitioning the tiles into three *functional criticality areas.* Once a burn-through has occurred, various systems would be exposed to extreme heat and would fail. If those systems were essential for flight, their failure could lead to the loss of the orbiter. By examining the location of critical systems (electrical, hydraulic, fuel, etc. as shown in Figures 13 and 14), three areas were identified (Figure 15). The following probabilities were estimated by assuming that a burn-through would cause an area of four square feet around the hole to be exposed to hot gases.

Area of high functional criticality:	P(Loss of orbiter | Burn-through) = 0.8
Area of medium functional criticality:	P(Loss of orbiter | Burn-through) = 0.2
Area of low functional criticality:	P(Loss of orbiter | Burn-through) = 0.05

Table 6: Probabilities of LOV conditional on burn-through in functional criticality areas shown in Figure 15

3.2.5 Debonding caused by factors other than debris impact

In this model, it is assumed that the probability of debonding caused by factors other than debris impact is the same for all tiles. In reality, the location of screed, thin SIP, and gap filler as well as the age of RTV, and the temperature and pressure zones would affect the probability of debonding. Short of conducting considerable additional research, this simplification should be adequate. Again, the probabilities used for illustration are only coarse estimates that are intended to provide an idea of the relative magnitude of the debonding problem to the debris problem. Another relationship not considered directly in this analysis is the effect of weak bonding on the susceptibility of a tile to debris impact. A weakened tile is much more likely to be dislodged by a medium-sized debris hit. For the purposes of this

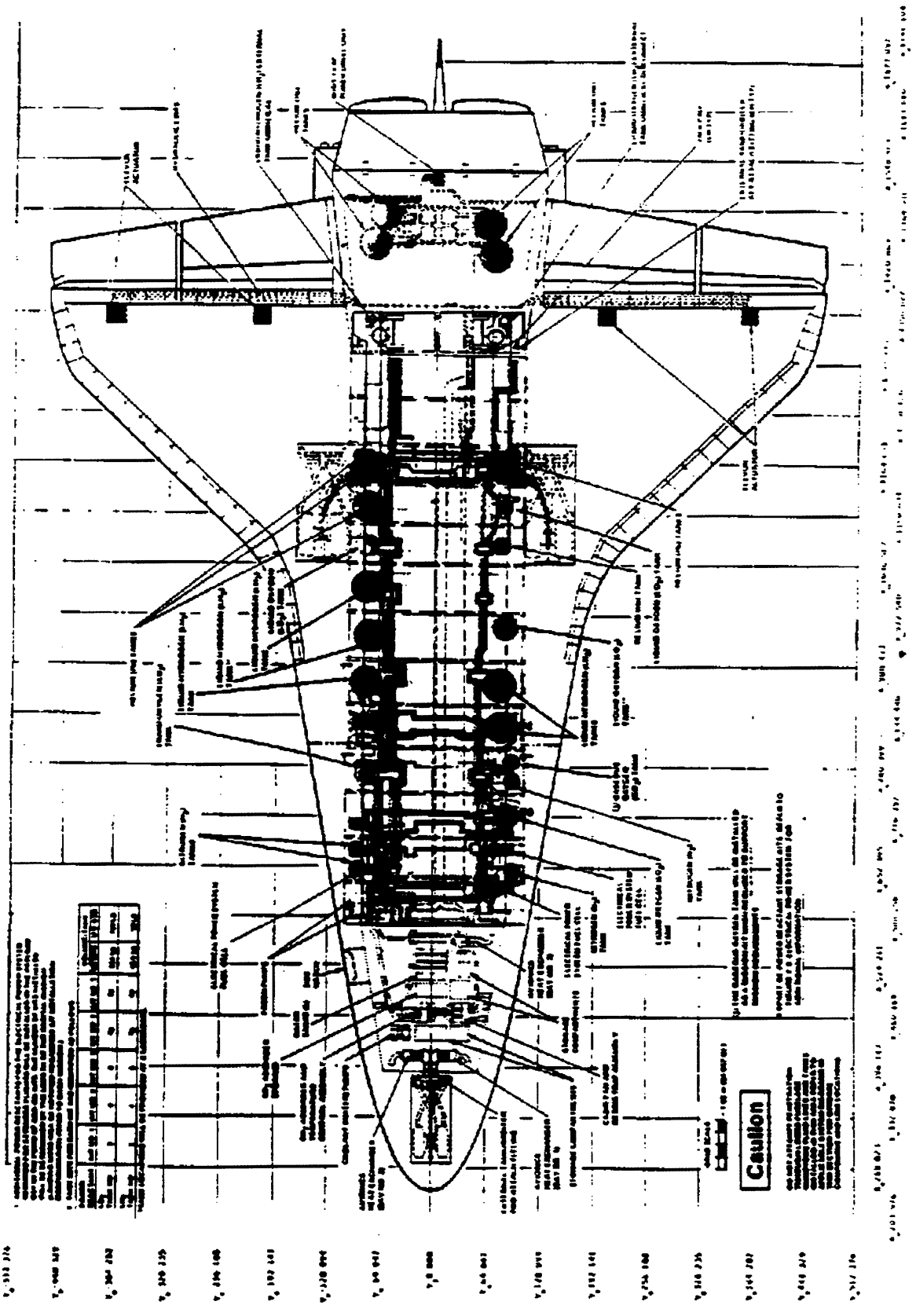


Figure 13: Component and systems location

Source: Shuttle Operational Data Book, JSC 08934 Vol. 1

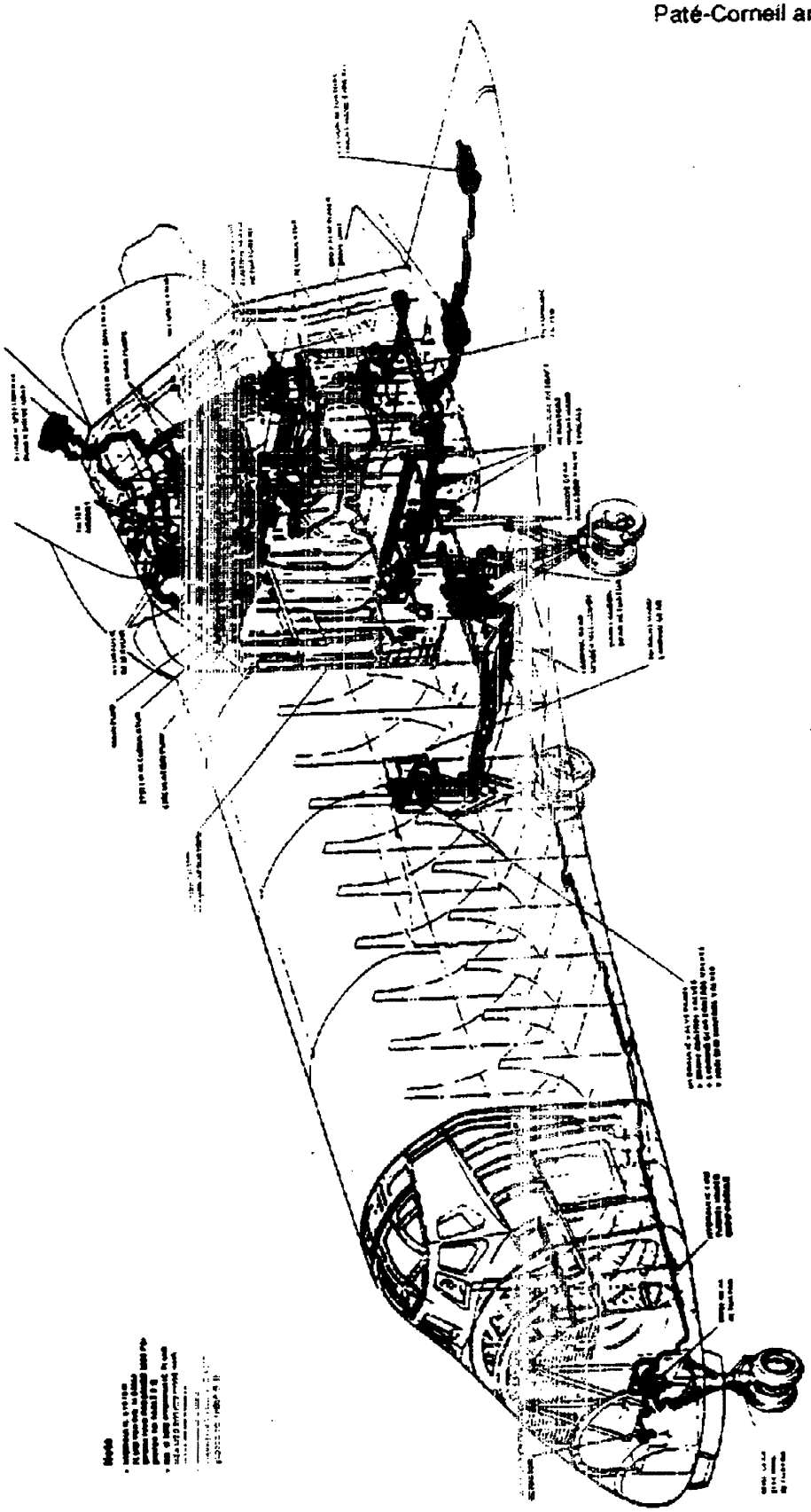


Figure 14: Hydraulic system components and line locations

Source: Shuttle Operational Data Book, JSC 08934 Vol 4

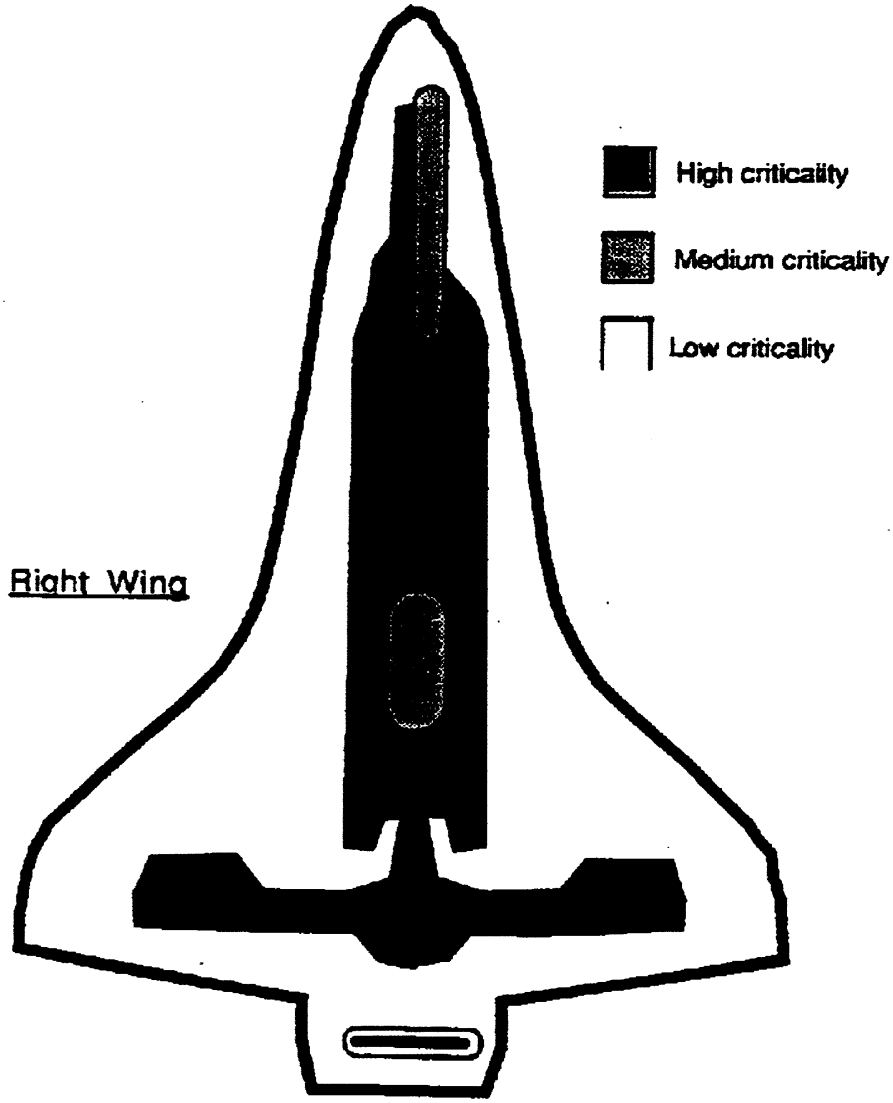


Figure 15: Partition of the orbiter's surface into three types of zones of functional criticality (index: j)

model, with its uniform distribution of debonding, this factor is included in the debris analysis.

Of the approximately 130,000 black tiles that have been installed at various times on all the orbiters, 12 have been found during maintenance to have no bond other than through the gap filler. A complete analysis of tile capacity, as revealed by the maintenance observations, will be part of the second phase of this work. We assumed, for the moment, that about half of the unbonded tiles that are held in place by the gap fillers have been detected by now, either because of visible slumping or because they have been replaced for other reasons such as debris damage (about 25% so far have been replaced.) Those with no bond that have not been detected so far are those that have not yet shown visible signs of weakness and have not needed replacement.

David Weber from KSC estimated that a tile with this weak a bond would have a probability of failure of one in a hundred (10^{-2}) per flight, making the probability of debonding of this kind, for any tile, to be approximately 9.0×10^{-7} per flight. Estimating the probabilities for the other types of debonding (excluding those caused by debris impact) is more subjective. We used a previous Lockheed study of bond verification (see Figure 16) and confirmed the results during discussions with David Weber. This study gives relative values of the probabilities of different debonding modes. Following these results, we assumed that chemical reversion of the screed and weakening due to repeated exposure to load cycles are less likely to cause debonding, and we used a probability of failure of 2×10^{-7} per tile and per flight. As a further simplification, these two probabilities (weakening due to repeated exposure to load cycles and insufficient bonding) are assumed to be independent and can thus be added. In actuality, poorly bonded tiles or tiles resting on soft screed are likely to be much more susceptible to this kind of weakening. Using these values, the probability of losing at least one of the tiles due to debonding caused by other factors than debris impact, on any flight, would be a little more than 0.02, which

FOUR MAJOR DEBOND PROBLEM TYPES

DEBOND TYPE	FREQUENCY-OF-OCCURRENCE FACTOR (1-10)	RISK FACTOR (1-10)	PRIORITY	SAMPLE PREPARED
GAP BETWEEN SIP AND RTV				
• DRIED RTV	9	10	1	X
• SIP RESTS ON EDGE OF FILLER BAR	4	10		X
GAP BETWEEN RTV AND KOROPON/Al SKIN				
• SURFACE PREPARATION	8-9	5	2	X
"FUZZ BOND" - PARTIAL PENETRATION OF RTV INTO SIP	7	3	3	
• RTV CURE RATE				X
• MISMATCH OF SIP AND FILLER BAR				X
RTV CHEMICALLY REVERTS	3	8	4	

Figure 16: Four major debond problem types

Source: R. Welling, Lockheed Corporation (1989) Reproduced by permission

then implies that over 35 flights, the probability of losing at least one tile on one of the flights is a little less than 1 50. This appears reasonable based on historical events and the one missing tile.

3.3 PRA model: definition of variables

Throughout the rest of the analysis, the areas defined in the previous section are indexed as follow:

- **i:** Index of min-zones
- **h:** Index of debris areas
- **j:** Index of functional criticality areas
- **k:** Index of burn-through areas
- **l:** Index of secondary tile loss areas

Note that a double subscript (e.g., ji) represents parameter j (criticality in this case) of min-zone i and that the term "debonding" refers to "debonding due to factors other than debris impact"

- **n:** Total number of black tiles on the orbiter
- **n_i:** Number of tiles in min-zone i.
- **N:** Total number of min-zones
- **N_i:** Number of failure patches in min-zone i.
- **q:** Index for the failure patches in any min-zone
- **M:** Final number of tiles in any failure patch
- **m:** Index for the number of tiles in a failure patch
- **Ft:** Initiating failure of a tile
- **Fa|Ft:** Failure of any adjacent tile given initiating failure
- **D:** Number of adjacent tiles in initial debris area
- **S:** Number of adjacent tiles in initial debonding area
- **L:** Loss of vehicle (LOV)
- **P(X):** Probability of event X
- **P(X|Y):** Probability of event X conditional on event Y
- **P(X,Y):** Joint probability of event X and event Y
- **EV(Z):** Expected value of random variable Z

This analysis follows closely the structure of variables described in Figure 9. Two types of initiating events are considered: those caused by debonding, and those caused by debris impact. A third category, failure of the tile itself due to heat loads,

may be added later.) It is assumed that the two types of initiating events are probabilistically independent. Since each min-zone has its own set of characteristics, they are treated as separate entities. Tiles in each specific min-zone have the same probability of being initially damaged and of causing a larger failure patch, burn-through, damage to a critical system, and the loss of the vehicle. Because of these assumptions, the analysis determines first the probability of losing the vehicle for each type of initiating event and each min-zone. The overall failure probability is the sum of the failure probabilities for all zones and initiating events. Debris impacts are considered first.

3.4 Initiating event: initial debris impact on one tile only (D=1)

To determine the probability that a specific tile in min-zone i starts a patch due to debris impact, it is also necessary to consider the size of the initial damage. We consider first the case where a single tile is initially damaged. Throughout section 3.4, it should be remembered that the probability of initial tile failure in min-zone i, $P_i(Ft)$, should be read as $P_i(Ft|D=1)$. Next sections consider $P_i(Ft|D=2)$ and $P_i(Ft|D=3)$. These additional levels of initial damage (two and three tiles simultaneously) are combined later.

Once the first tile in min-zone i is lost due to debris, there is the potential for adjacent tiles to also fail. The probability that the final patch size reaches M depends on the secondary loss index of the min-zone (I_i) and is given by the following geometric distribution (which means that M-1 additional tiles fail and no adjacent tile afterwards:)

$$P_i(M \mid Ft) = P_{ii}(Fa|Ft)^{M-1} \times [1-P_{ii}(Fa|Ft)] \qquad (1)$$

Note that M must be at least equal to 1. This equation assumes that the probability that adjacent tiles debond does not change as the patch grows.

In each min-zone, there is the possibility of several patches starting. The probability that the number of patches reaches N_i in min-zone i is:

$$P_i(N_i) = \frac{n_i!}{N_i!\,(n_i-N_i)!} \cdot P_i(Ft)^{N_i} \times [1-P_i(Ft)]^{n_i-N_i} \qquad (2)$$

This formulation assumes that the initial tile failures are independent, and that there will be no overlapping of patches because the probability of an initiating event (Ft) is small compared to the number of tiles in each min-zone (n_i). The product $EV(N_i) \times EV(M)$ which equals the total number of tiles lost in each min-zone is considered negligible compared to n_i. Also, N_i (number of patches) and M (size of patches) are considered independent random variables. Based on these assumptions, the expected number of patches is approximately:

$$EV(N_i) = n_i \times P_i(Ft) \qquad (3)$$

and the size of each patch is given by the mean of the distribution of M:

$$EV(M) = 1 / [1-P_i(Fail\ Ft)] \qquad (4)$$

Given this result, it is now possible to calculate the probability that the orbiter will fail due to debris that impact one tile only. Remembering that j is the index of the criticality areas and k is the index of the burn-through areas, we define the probabilities of orbiter failure due to a patch of size M, in min-zone i, initiated by debris impact (D=1) as follows:

$$P_i(L|\ M=1) = p_{jki,1}$$

$$P_i(L|\ M=2) = p_{jki,2}$$

...

$$P_i(L|\ M=m) = p_{jki,m} \qquad (5)$$

It must be remembered that any given min-zone could have several patches in it, and each patch could be of a different size. To calculate the probability of orbiter loss due to specific number of patches (N_i) in min-zone i, the following definition is necessary. Let p'_i be the probability that an arbitrary patch in min-zone i causes a failure.

$$p'_i = \sum_{m=1}^{\infty} p_{jki,\,m} \times P(\text{patch size} = m) \qquad (6)$$

$$p'_i = \sum_{m=1}^{\infty} p_{jki,\,m} \times P_{ji}\,(Fa|Ft)^{m-1} \times [1-P_{ji}(Fa|Ft)] \qquad (7)$$

Therefore, q being the number of patches in a given min-zone, the failure probability for a specific number of patches in a min-zone is:

$$P_i(L|\,N_i=q) = p'_i \times q \qquad (8)$$

Once again, this assumes that the probabilities are small and that the patches will not interfere with each other (they are assumed to be separate and independent). These assumptions are valid providing that each min-zone has a sufficiently large number of tiles and that the size of the patches is relatively small.

Based on Equation (8), the probability of orbiter failure given all patches that occur in min-zone i becomes:

$$P(L|\text{min-zone i}) = \sum_{q=0}^{\infty} P_i(L|N_i=q) \times P_i(N_i=q)$$

$$= \sum_{q=0}^{\infty} p'_i \times q \times P_i(N_i=q)$$

$$= p'_i \times EV(N_i)$$

$$= p'_i \times n_i \times P_i(Ft) \qquad (9)$$

This result represents only the cases of debris impact causing the initial failure of a single tile. A more complete rewriting of Equation 9 highlights this fact:

$$P(L|\text{min-zone } i, D=1) = g'_i(D=1) \times n_i \times P_i(Ft|D=1) \qquad (10)$$

3.5 Initiating event: initial debris impact on several tiles (D=d)

In order to expand this model to include the possibility that the initial debris impact damages more than one tile, it is necessary to modify some of the above equations. It is assumed that if a large enough piece of debris hits the orbiter, several adjacent tiles may be knocked loose at once. Each of these missing tiles may in turn cause their adjacent tiles to fail and a specific number of additional tiles can fail in multiple ways. Therefore, additional summations are required in order to account for the increased number of exposed tiles. This compounded problem requires that Equation (1) be rewritten to account for this potentially larger patch growth rate. If the initial damage involves two tiles, the probability that the final patch reaches size M is:

$$P_i(M|Ft, D=2) = (M-1) \times P_{ii}(Fa|Ft)^{M-2} \times [1 - P_{ii}(Fa|Ft)]^2 \qquad (11)$$

If three tiles are damaged initially:

$$P_i(M|Ft, D=3) = \left[\sum_{k=1}^{M-2} k\right] \times P_{ii}(Fa|Ft)^{M-3} \times [1 - P_{ii}(Fa|Ft)]^3 \qquad (12)$$

If four tiles are damaged initially:

$$P_i(M|Ft, D=4) = \left[\sum_{k=1}^{M-3} \sum_{i=1}^{k} i\right] \times P_{ii}(Fa|Ft)^{M-4} \times [1 - P_{ii}(Fa|Ft)]^4 \qquad (13)$$

This set of equations can be extended to include greater initial damage; historical evidence, however, supports limiting the analysis to this level. It must be remembered that the value M of the final patch size must always be at least equal to the size of the initial damage area, D. Equation (2) in its most general form is written:

$$P_i(N_i|D=d) = \frac{N_i!}{n_i!\,(N_i-n_i)!} P_i(Ft|D=d)^{N_i} \times [1-P_i(Ft|D=d)]^{n_i-N_i} \qquad (14)$$

and Equation (3) becomes:

$$EV(N_i) = n_i \times P_i(Ft|D=d) \qquad (15)$$

Equations (5) and (6) do not change except for the indexing of the summation since their results depend only on the final patch size and the functional criticality index. Equation (7) would change as Equations (11) to (13) are integrated to account for the various debris damage areas. The final probability for each initial damage area and min-zone is computed using a variant of Equation 10:

$$P(L|\text{min-zone } i, D=d) = p'_i(D=d) \times n_i \times P_i(Ft|D=d) \qquad (16)$$

Because all the initial damage probabilities are very small, it is possible to approximate the probability of debris causing loss of an orbiter for all damage areas in a particular min-zone by:

$$P(L|\text{min-zone } i, \text{debris}) = \sum_{d=1}^{\text{Max } d} P(L|\text{min-zone } i, D=d) \qquad (17)$$

Once this probability is determined, the probability of orbiter failure for all min-zones due to debris impact is simply the sum of the probabilities of failure for all min-zones since all min-zones and initiating events are assumed to be independent:

$$p(L|debris) = \sum_{i=1}^{N} P(L|min\text{-}zone\ i, debris) \qquad (18)$$

3.6 Initiating event: debonding caused by factors other than debris impact

The same procedure and basic formulas are used to determine the probability of orbiter failure due to debonding caused by factors other than debris impact. Again, the probability of orbiter failure due to failure of the TPS is computed from the probability of tiles spontaneously debonding in groups of various sizes in each min-zone. The problem is slightly easier since it is assumed that the likelihood of such debonding is uniform across all tiles. The probability of secondary tile failure $P_i(Fa|Ft)$ is the same as for the debris problem. The probability of orbiter failure based on all patches in min-zone i that started from a damage area of initial size s is given by:

$$P(L|min\text{-}zone\ i, S=s) = p'_i(S=s) \times n_i \times P_i(Ft|S=s) \qquad (19)$$

The other equations follow accordingly. The total probability of shuttle failure for damage initiated by debonding caused by factors other than debris impact is:

$$P(L|debonding) = \sum_{i=1}^{N} P(L|min\text{-}zone\ i, debonding) \qquad (20)$$

Finally, assuming independence of initiating events (debris and debonding due to other causes), the overall probability of shuttle failure per flight due to tile damage is:

$$P(L|tile\ problem) = P(L|debonding) + P(L|debris) \qquad (21)$$

3.7 Additional information and data

A PRA model like the one described above needs to be constantly updated to reflect information that may have existed before but had not been uncovered at the time of this initial study, and information from new experience including recent inspections, tests, evaluations, studies, and in-flight performance data. In this implementation phase, more refined data may thus be used and additional information available at NASA can be introduced in the analysis. One important part of the problem at that stage will be to capture the evolution of the failure probability of the orbiter. Clearly, *the system is not in a steady state*. On one hand, the quality of the maintenance work appears to improve (Figure 17). Initial defects of the installation work that resulted in a decrease of the tile capacity are progressively being discovered and corrected during successive maintenance operations. Existing problems, such as the impact of chunks of insulation from the ET and the SRBs or the elevon-cove design problem, are resolved as they are discovered. On the other hand, the possibility of long-term deterioration of the TPS clearly increases the probability of tile failure (even if slowly) and the rate of deterioration is a major unknown. Of specific concern are: the possibility of degradation of the bond over time, of slow chemical reaction due to water proofing agent, and of weakening of the SIP/tile system under exposure to repeated load cycles. Additional data regarding the initial test results used in the certification procedure from JSC and from the manufacturers of the tiles, the SIPs, and the bond are needed to update the model. Therefore, this updating should be based not only on statistical data on tile performance during each flight, but also on basic information about the components of the TPS.

A complete analysis of the distribution of tile capacities will require additional data from maintenance operations including:

- The numbers of tiles replaced so far on each orbiter;
- A statistical distribution of the percentage of the surface of the tile/SIP system that was found to be actually bonded to the orbiter's skin;

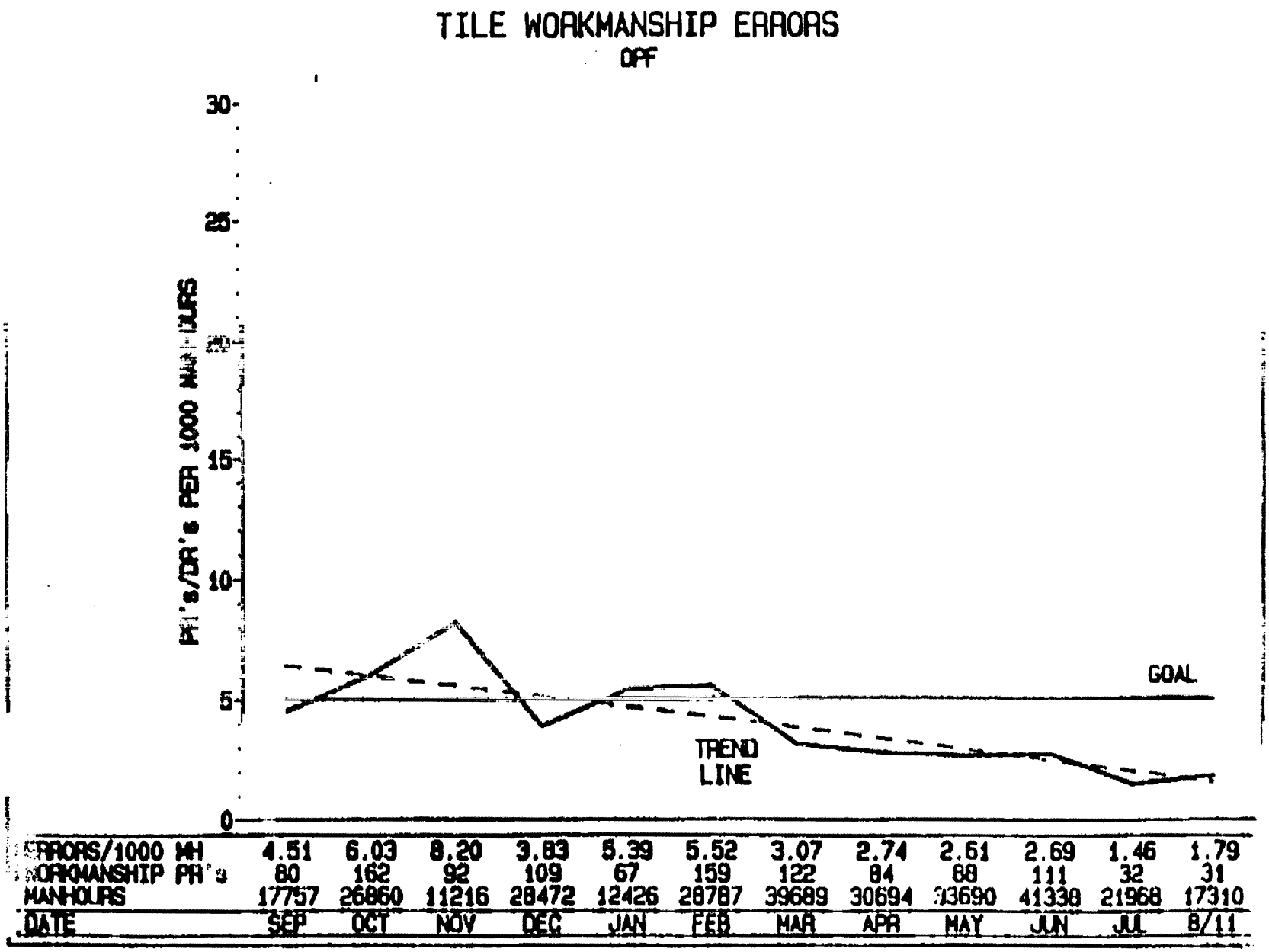


Figure 17: Tile workmanship errors

Source: D. Weber, Lockheed Corporation (1989)

- Estimates of the probability of failure of a tile of given capacity (e.g., 10% bonded) under different kinds of load (e.g., debris hit >1").

A more refined partition of the orbiter's surface can be obtained using data such as:

- Effect of excessive step and gap on the heat load in different locations;
- Possibility of partial failure of the guidance system or control surfaces at re-entry and corresponding increase in the heat load;
- Trajectories of debris from the ET and the SRBs. Computer simulations done at JSC (see Figures 18 and 19) could give better information about the vulnerability of the orbiter's TPS, in particular in the most risk-critical areas;
- Measurements of temperatures and aerodynamic forces on the surface of the orbiter (see Figures 20 and 21);
- Effect of tile loss on the orbiter's surface temperature in the cavity (Figure 22).

The analysis itself can be refined in several ways. A major unknown is the performance of the subsystems under the orbiter's skin once they are exposed to excessive heat loads due to TPS failure. The only alternative, short of a systematic PRA of these individual systems, is to use subjective estimates. Finally, it seems that the availability of a kit for in-orbit repair of the tiles might provide a significant reliability gain. An assessment of its effectiveness will be included in Phase 2 of this study.

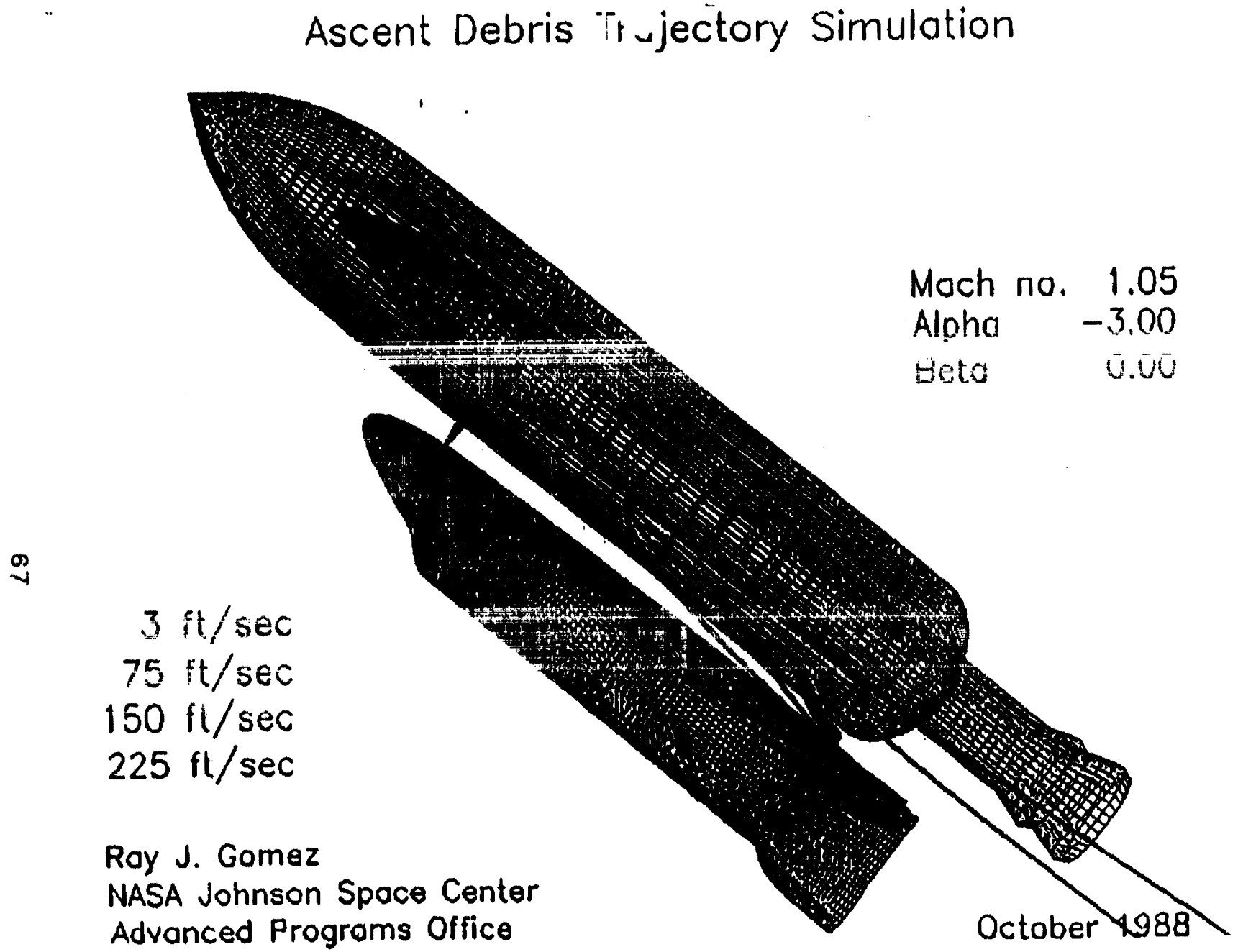
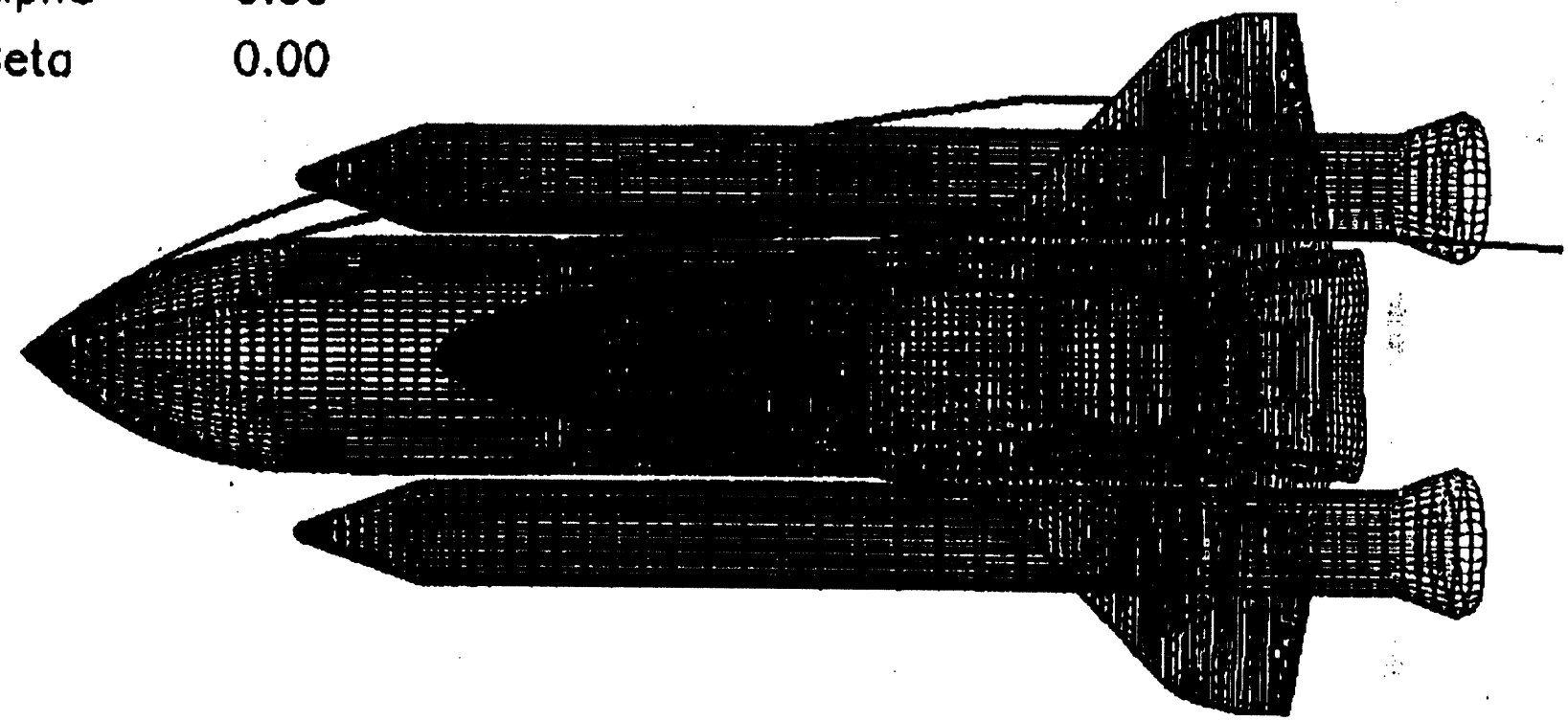


Figure 18: Ascent debris trajectory simulation (side view)

Source: R. Gomez, NASA JSC (1988)

Mach no. 1.05
Alpha −3.00
Beta 0.00



Ray J. Gomez
NASA Johnson Space Center
Advanced Programs Office

October 1988

Figure 19: Ascent debris trajectory simulation (plan view)

Source: R. Gomez, NASA JSC (1988)

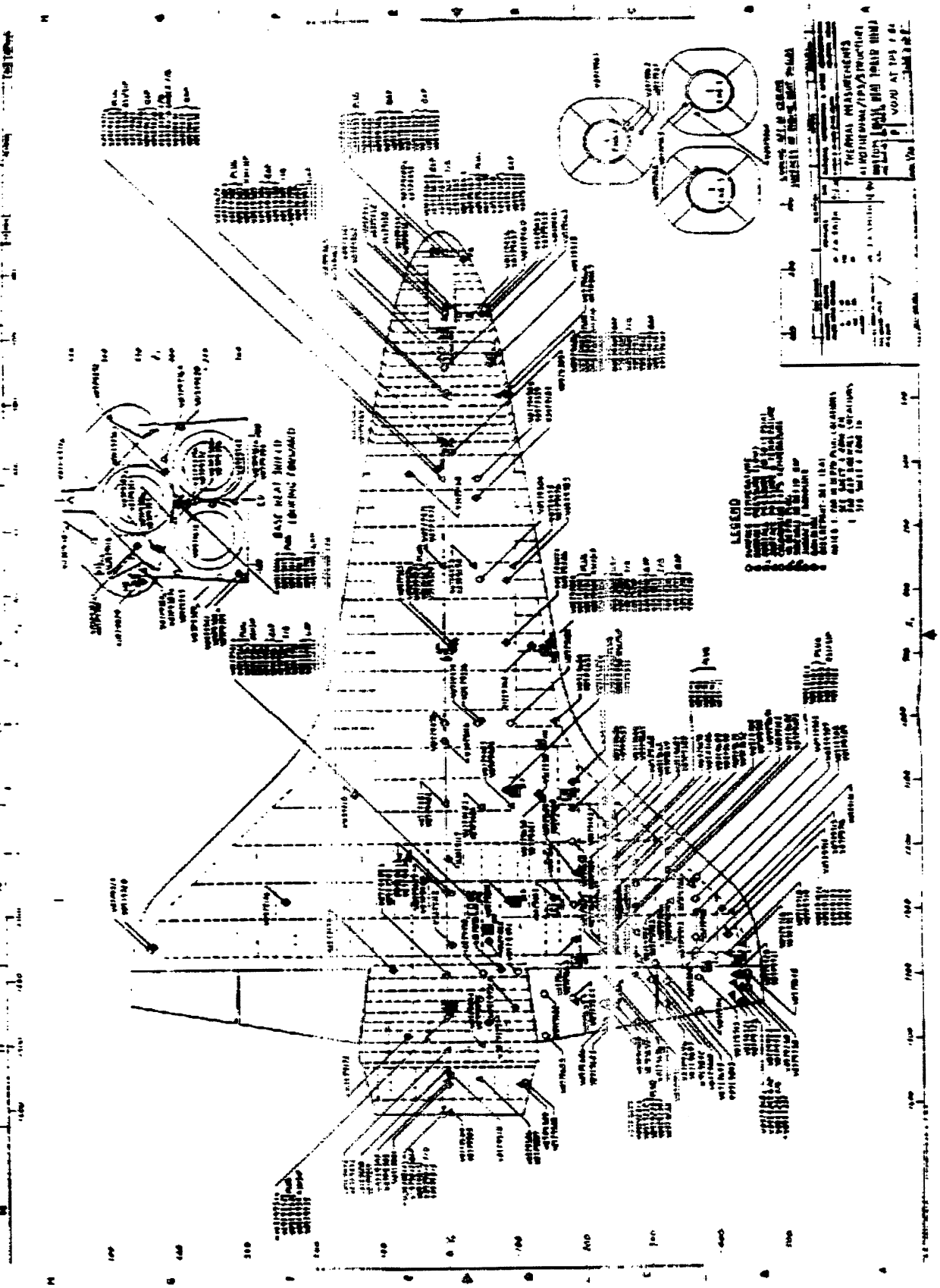


Figure 20: Thermal measurements (bottom view)
Source: Structural & Aerodynamic Pressure Measurement Locations JSC 17889

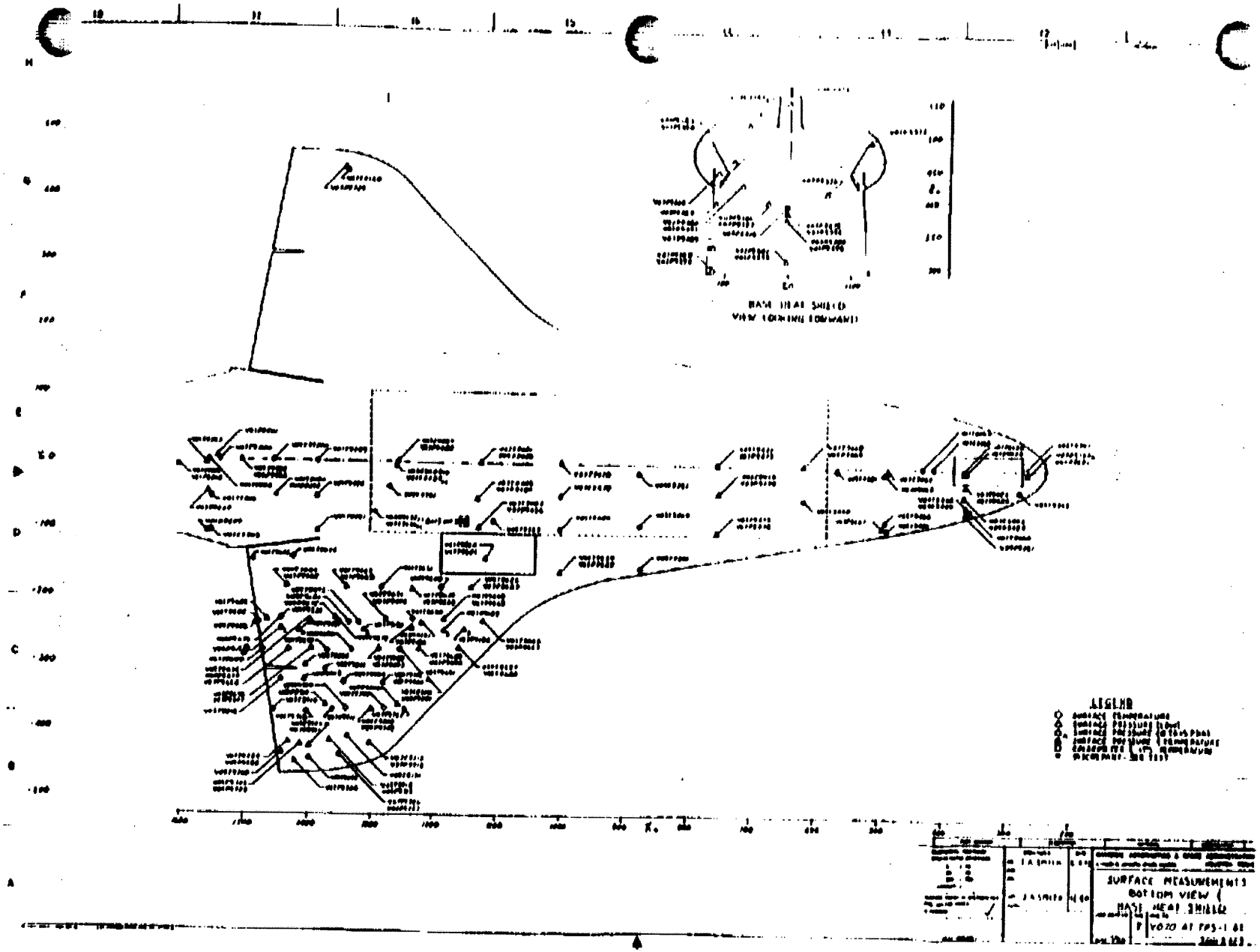


Figure 21. Surface measurements (bottom view)
Source: Structural & Aerodynamic Pressure Measurement Locations JSC 17889

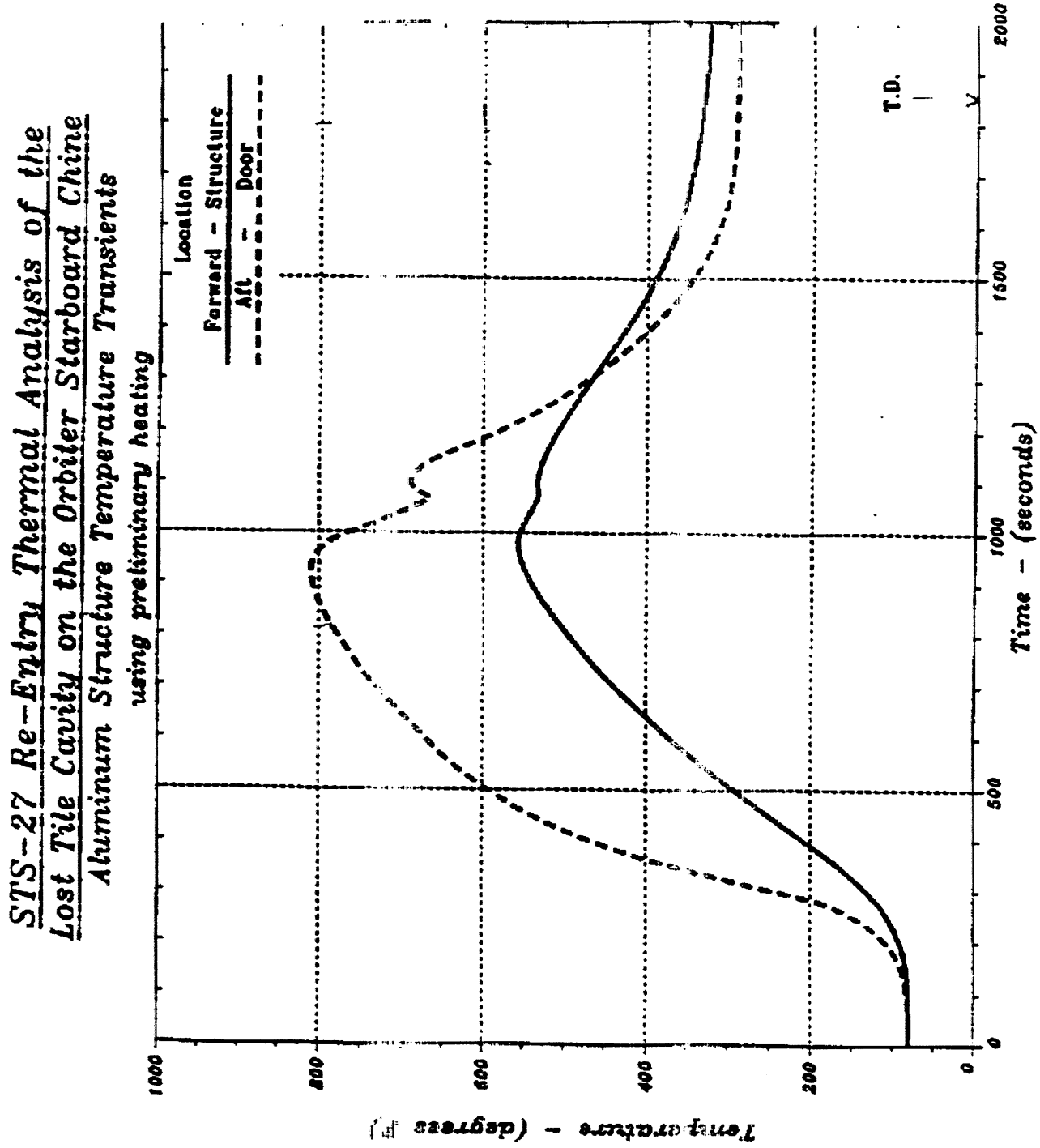


Figure 22: Re-entry thermal analysis of lost tile cavity

Source: R. Maria, NASA JSC (1988)

Section 4:
ILLUSTRATION OF THE MODEL

The illustration of the model presented here is based on coarse numbers whose relative values are more significant than their absolute values. By overlaying the functional criticality, burn-through, debris damage, and secondary tile loss areas, 33 min-zones were established. Of these, 21 are unique zones (i.e., that have different sets of indices). Several zones with the same combinations of indices appear on different locations on the orbiter. Figure 23 shows the final layout of the min-zones and the numerical results of the model. Each zone is assigned an identification number. The lower numbers are generally assigned to more critical areas. Each zone is also identified by an index number whose digits relate to the four area types shown in Table 7:

1st digit:	Burn-through areas (1 high, 2 medium, 3 low, probabilities)
2nd digit:	Functional criticality areas (1 high, 2 medium, 3 low, criticality)
3rd digit:	Debris damage areas (1 high, 2 medium, 3 low, probabilities)
4th digit:	Secondary tile loss areas (1 high, 2 low, probability)

Table 7: Structure of the indices of the min-zones shown in Figure 22 and Table 8.

Table 8 lists the min-zones, and shows the number of tiles in each zone and the probability of failure of the orbiter attributable to this zone. This value was determined by calculating this probability for both initiating events and then summing to obtain the results. The boundaries of the min-zones have been simplified: the number of tiles in each area is only an approximation and is not based on an actual count. The location description is only intended to provide a rough placement of the

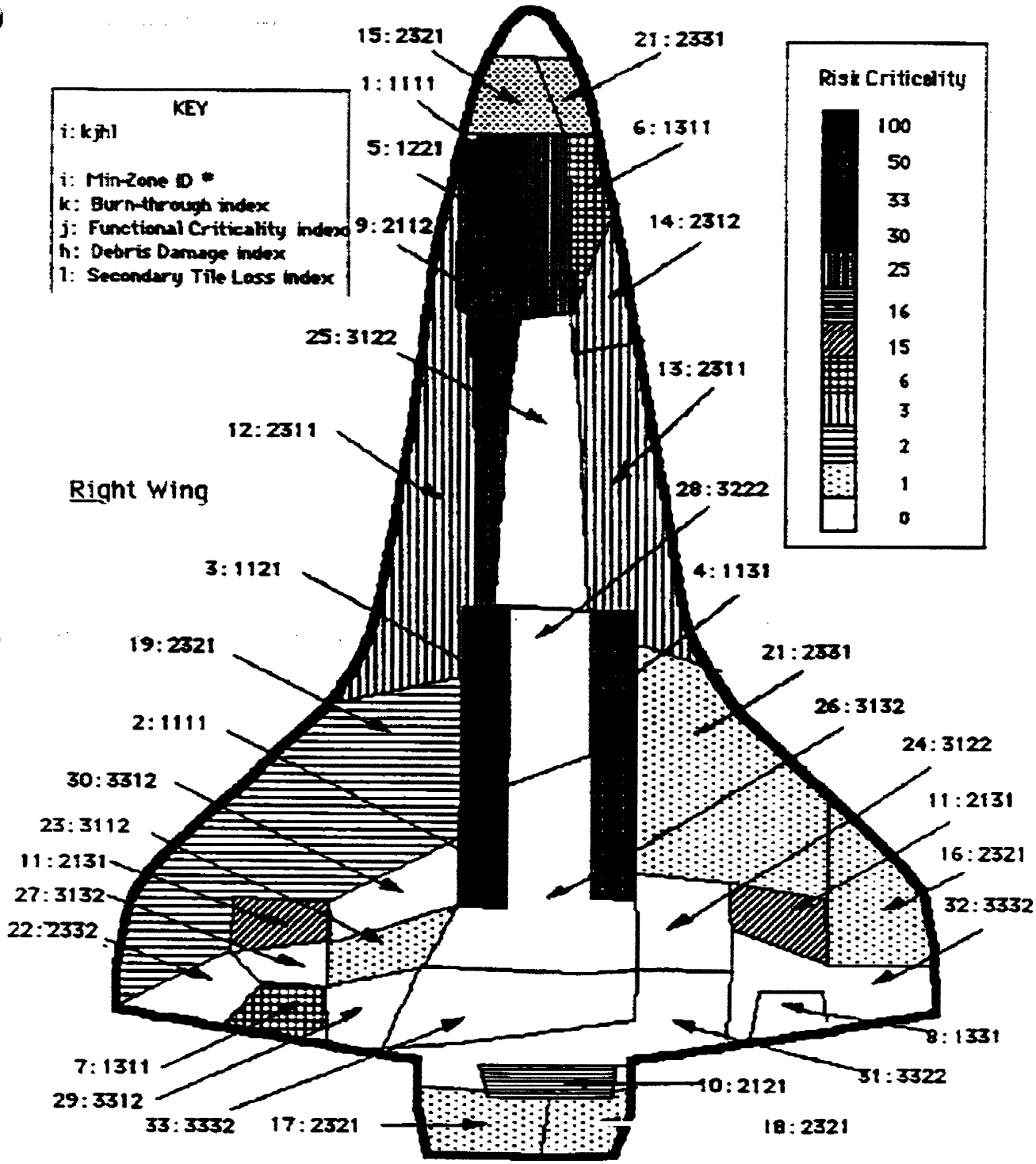


Figure 23: Partition of the orbiter's surface into 33 min-zones (index: i)

ID #	Index	Location	# Tiles	P(LOV) 10^{-4} Debris	Debond	Total
1	1111	Right side, under crew	156	0.87	0.36	1.23
2	1111	Right side, near main ldg gear (aft)	156	0.87	0.36	1.23
3	1121	Right side, near main ldg gear (fwd)	676	0.13	1.62	1.75
4	1131	Left side, near main ldg gear	780	0.00	1.87	1.87
5	1211	Centerline, under crew	364	0.51	0.22	0.73
6	1311	Left side, under crew	312	0.11	0.04	0.15
7	1311	Center of right elevon	104	0.04	0.01	0.05
8	1331	Center of left elevon	104	0.00	0.00	0.00
9	2112	Right side, fwd mid edge	624	1.73	0.75	2.48
10	2121	Center of body flap	208	0.02	0.24	0.26
11	2131	Left wing, center	468	0.00	0.56	0.56
12	2311	Right side, mid edge	1664	0.30	0.13	0.43
13	2311	Left side, mid edge	1196	0.21	0.08	0.29
14	2312	Left side, fwd mid edge	572	0.10	0.04	0.14
15	2321	Right side, nose	277	0.01	0.02	0.03
16	2321	Left wing, center	832	0.01	0.06	0.07
17	2321	Right side, body flap	104	0.00	0.01	0.01
18	2321	Left side, body flap	104	0.00	0.01	0.01
19	2321	Right wing	2132	0.18	0.16	0.34
20	2331	Left side, nose	312	0.00	0.02	0.02
21	2331	Left wing, fwd	1768	0.00	0.13	0.13
22	2332	Right elevon, outboard	312	0.00	0.02	0.02
23	3112	Right wing, center	364	0.01	0.01	0.02
24	3122	Left wing, center	468	0.00	0.01	0.01
25	3122	Center, payload bay fwd	1664	0.00	0.02	0.02
26	3132	Center, payload bay aft	1976	0.00	0.02	0.02
27	3132	Right wing, center	468	0.00	0.01	0.01
28	3222	Center, payload bay, mid	520	0.00	0.00	0.00
29	3312	Right elevon, in board	312	0.00	0.00	0.00
30	3312	Right wing, center	416	0.00	0.00	0.00
31	3322	Left elevon in / center body flap	728	0.00	0.00	0.00
32	3332	Left elevon, outboard	572	0.00	0.00	0.00
33	3332	Center, aft	1040	0.00	0.00	0.00
			Totals	5.09	6.79	11.88

Table 8. Identification of the min-zones and their contribution to the probability of LOV

min-zone. No attempt has been made to use orbiter notations. The final numerical results of the model are presented in the right-hand column as multiples of 10^{-4}. The probability values are mostly in the order of 10^{-4}. Again, it is important to remember that the importance of the numbers is not their magnitude, but their relative values when compared to each other. According to our coarse numerical analysis, the total probability of losing the orbiter on any given mission, due to TPS failure, is in the order of 10^{-3}. It is interesting to note that approximately 40% of this probability is attributable to debris-related problems and that 60% comes from problems of debonding caused by other factors. By scanning the columns, it appears that a few min-zones contain most of the risk.

Using a risk-per-tile measure, the min-zones can be ordered according to their criticality with respect to the two types of initiating events, and to the total probability of failure. The results are shown in Tables 9 and 10. Table 9 displays the contribution of each min-zone and of each tile to the probability of LOV separated into debris and debonding due to other factors. Table 10 shows the contribution of each tile and each min-zone to the overall probability of LOV. In this table, we show for each tile, *a risk-criticality factor* that is proportional to the relative contribution of this tile to the overall failure probability, accounting not only for the loads applied to this tile but also for the consequences should it fail. This risk-criticality factor is the point of reference that will be used in the second phase of the study to set priorities among different management measures designed to improve tile reliability.

A slightly different graphic representation of this table is displayed in Figures 24, 25, and 26. It is possible from our results to identify *the most sensitive min-zones* by ranking them by order of individual tile criticality. One can then plot the marginal increase of the failure probability for each added min-zone, the slope of each segment representing the (decreasing) contribution of each tile to the failure probability. Each black dot represents the addition of the next most critical min-zone. The greater the horizontal spacing between the dots, the larger the number of tiles in

Debris			Debonding		
ID#	P(LOV)/zone 0.00E-4	P(LOV)/tile 0.00E-8	ID#	P(LOV)/zone 0.00E-4	P(LOV)/tile 0.00E-8
1	0.370	55.770	4	1.870	24.000
2	0.370	55.770	3	1.620	24.000
9	1.730	27.720	1	0.360	23.100
5	0.510	14.010	2	0.360	23.100
6	0.110	3.365	9	0.750	12.000
7	0.040	3.365	11	0.560	12.000
3	0.130	1.923	10	0.240	11.500
12	0.300	1.785	5	0.218	5.990
13	0.210	1.781	6	0.045	1.440
14	0.100	1.748	7	0.015	1.440
10	0.020	0.961	15	0.023	0.829
19	0.035	0.867	12	0.130	0.781
23	0.010	0.274	16	0.065	0.781
17	0.002	0.192	21	0.133	0.752
18	0.002	0.192	14	0.043	0.752
15	0.003	0.108	20	0.023	0.737
16	0.008	0.096	22	0.023	0.737
4	0.000	0.000	19	0.156	0.673
8	0.000	0.000	17	0.007	0.673
11	0.000	0.000	18	0.007	0.669
20	0.000	0.000	13	0.080	0.137
21	0.000	0.000	23	0.005	0.128
22	0.000	0.000	24	0.006	0.128
24	0.000	0.000	27	0.006	0.121
25	0.000	0.000	26	0.024	0.114
26	0.000	0.000	25	0.019	0.038
27	0.000	0.000	28	0.002	0.000
28	0.000	0.000	8	0.000	0.000
29	0.000	0.000	29	0.000	0.000
30	0.000	0.000	30	0.000	0.000
31	0.000	0.000	31	0.000	0.000
32	0.000	0.000	32	0.000	0.000
33	0.000	0.000	33	0.000	0.000

Table 9: Probabilities of Loss of Vehicle due to tile failure initiated (1) by debris damage and (2) debonding caused by factors other than debris, for each min-zone, and each tile in each min-zone

ID #	P(LOV)/zone 0.00E-4	P(LOV)/tile 0.00E-8	Risk Criticality 0-100 scale	Number of Tiles	Location
1	1.2300	78.800	100	156	rt under crew
2	1.2300	78.800	100	156	rt main gear aft
9	2.4800	39.700	50	624	rt fwd mid edge
3	1.7500	25.900	33	676	rt main gear
4	1.8700	24.000	30	780	lt main gear
5	0.7280	20.000	25	364	center crew
10	0.2600	12.500	16	208	body flap cen
11	0.5600	12.000	15	468	lt/rt wng cen out
6	0.1500	4.810	6	312	lt crew
7	0.0500	4.810	6	104	rt elevon cen
12	0.4270	2.570	3	1664	rt side mid edge
14	0.1430	2.500	3	572	lt fwd mid edge
13	0.2930	2.450	3	1196	lt middle
19	0.3410	1.600	2	2132	rt wing
15	0.0260	0.938	1	277	rt nose
16	0.0730	0.877	1	832	lt wing outboard
17	0.0090	0.865	1	104	body flap rt
18	0.0090	0.865	1	104	body flap lt
21	0.1330	0.752	1	1768	lt wing forward
20	0.0230	0.737	1	312	lt nose
22	0.0230	0.737	1	312	rt elevon out
23	0.0150	0.412	1	364	rt wing center in
24	0.0060	0.128	<1	468	lt wing center in
27	0.0060	0.128	<1	468	rt wing cen out
26	0.0240	0.121	<1	1976	center bay aft
25	0.0190	0.114	<1	1664	center upper bay
28	0.0020	0.038	<1	520	center mid bay
8	0.0000	0.000	<1	104	lt elevon center
29	0.0000	0.000	<1	312	rt elevon in
30	0.0000	0.000	<1	416	rt wing cen
31	0.0000	0.000	<1	728	lt elev/body flap
32	0.0000	0.000	<1	572	lt elevon out
33	0.0000	0.000	<1	1040	center aft

Table 10: Risk-criticality factor for each tile in each min-zone

C-5

the zone. Several small min-zones contain a large part of the risk (those with the steepest slope), whereas several very large min-zones carry only a small part of the risk (those with zero slope). Figure 23 shows the contribution of increasing percentages of the tiles to the risk for debris-initiated damage. Note that, for failures initiated by debris, *80% of the risk is due to only 8% of the tiles.* For debonding problems that are not caused by debris, the contribution of increasing percentages of tiles are shown in Figure 24: *80% of the risk is due to 13% of the tiles.* Finally, the overall result is shown in Figure 25: for the total risk, including both initiating events, *80% of the risk can be attributed to 14% of the tiles.* It is important to remember that the same tiles do not necessarily appear in the same order in each graph. Clearly, some zones pose a much higher risk for one type of initiating event than for the other. For example, min-zone 4 located near the left main gear has not historically experienced significant debris damage and is not on the obvious trajectory of tractable debris; so, the probability of LOV due to TPS *debris* damage in that zone is basically zero. There are, however, some critical components that are temperature sensitive under the skin in that area; so, the risk of LOV due to *debonding* is non negligible (1.07×10^{-4}).

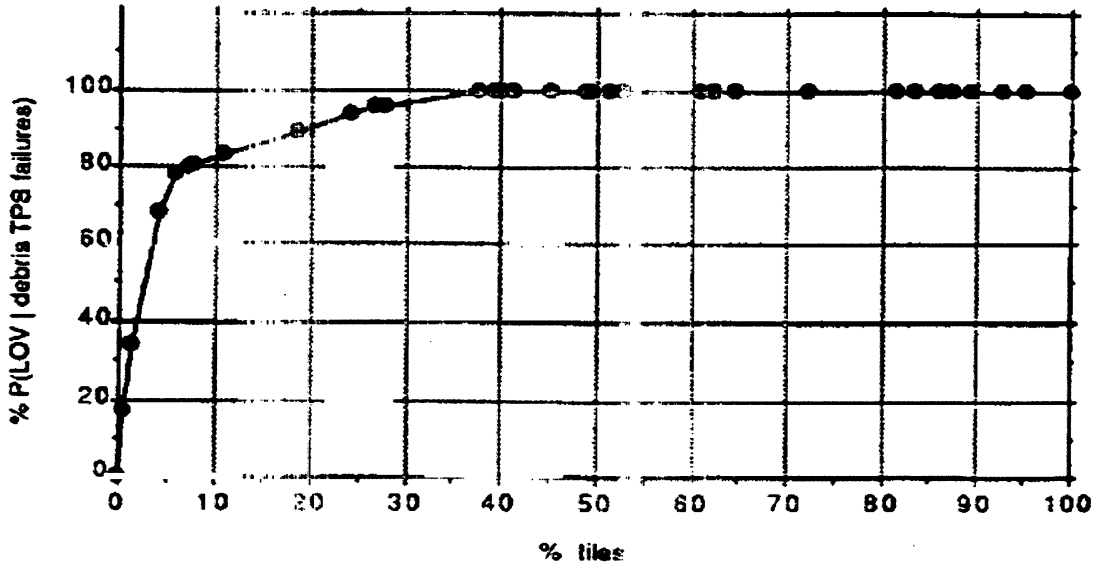


Figure 24: Relative risk of LOV due to debris-initiated TPS damage

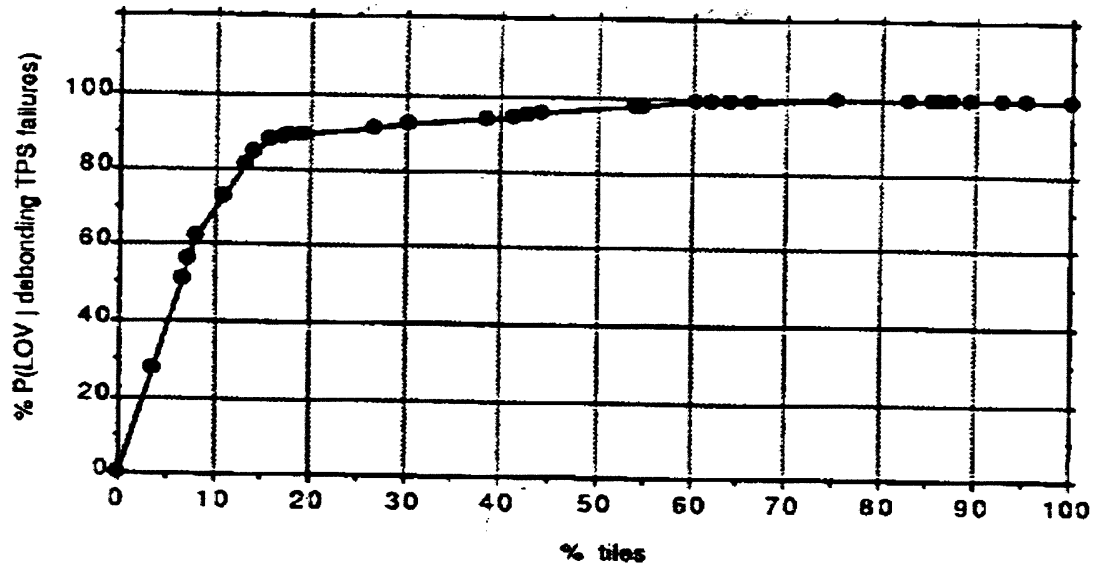


Figure 25: Relative risk of LOV due to debonding-type TPS damage

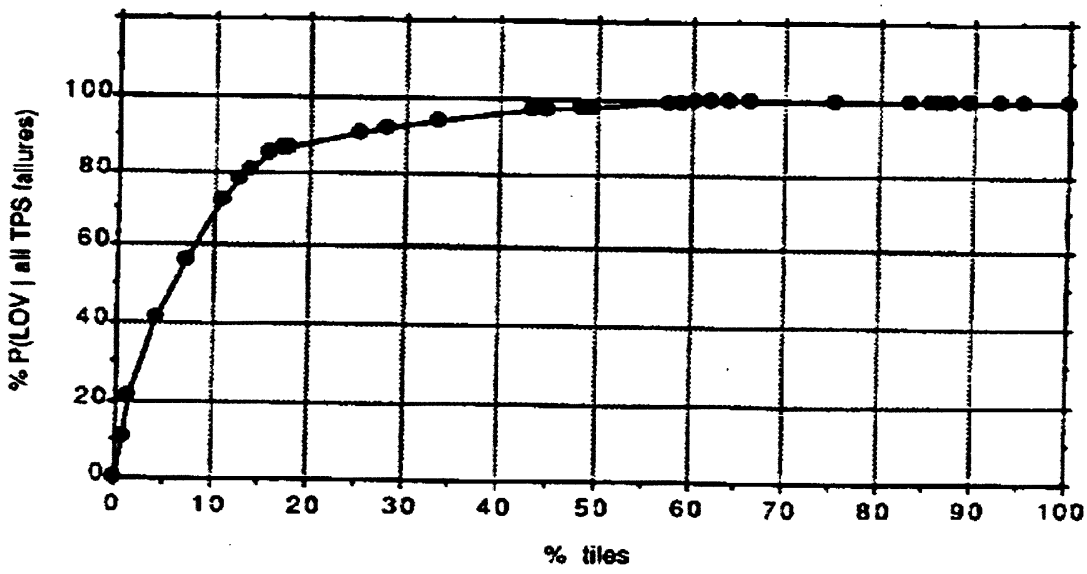


Figure 26: Relative risk of LOV due to both types of TPS damage

Section 5:
EFFECTS OF ORGANIZATIONAL FACTORS ON TPS RELIABILITY: MAIN PRELIMINARY OBSERVATIONS

5.1 Errors and risk

Well-bonded tiles are very unlikely to debond even under moderate debris loads. Given the temperature gradients measured inside the tiles during flights, it has been determined that the tiles absorb most of the heat within a fraction of their thickness and that they are very unlikely to burn, even considering a wide range of re-entry scenarios. If the tiles are to fail, it is likely to be because they have been weakened and/or hit by debris. The problem is that one does not know which ones are weak. Human errors (past and present) are at the source of at least three of the fundamental causes of tile failure: (1) decrease of tile capacity because of undetected partial or weakened bonding, (2) increase in the heat loads due to roughness of the orbiter's surface (caused, for example, by protruding gap fillers), and (3) poorly-installed and maintained insulation on the SRB's and ET that flakes off during ascent, damaging the TPS. These human errors are often the consequences of the way the organizations (NASA and its contractors) operate.

In the second phase of this work, we will explore to what extent *organizational procedures* (for instance, those that induce time pressure and turnover of the personnel) are at the root of these incidents. Rules that apply uniformly across tiles of widely variable risk-criticality, and rules that do not account for the possibility of system weakening over time may become major contributors to the overall risk. Furthermore, the scope of the research cannot be strictly limited to the TPS. Procedures and management decisions regarding the maintenance of the insulation of the ET and the SRBs also affect the reliability of the tiles since they are a

source of debris. Finally, in the long term, weakening of the tile system due to repeated load cycles, exposure to environmental conditions on the ground, or chemical reversion, may become a dominant factor of the failure risk. The problem of deterioration over time may not be (and is not likely to be) of immediate concern for well-bonded tiles, but may become a critical factor for those tiles whose capacities have been reduced by defective installation and maintenance. Therefore, in the second phase, we will examine closely the procedures of the organization, using our PRA model to see how the relative contributions of each of these factors affect flight safety.

In addition, the *structure of the organization* and its peripherals (NASA, plus Lockheed, Rockwell etc.) and the rules that determine the relations among these organizations (for example, in setting contracts, pay scales, and incentives, as well as schedule and budget constraints,) may also affect flight safety to the extent that they determine the occurrence and severity of human errors and their probabilities of detection. Some organizational improvements (which may have been recommended before and ignored for various reasons) may have only a minor effect on the reliability of the orbiter; others may be essential soon. Our analytical model will be used to determine which of these factors actually affect the probability of failure of the tiles (and consequently, of the orbiter) and by how much. Finally, the *culture of the organization* may also play a role. As we describe below, the low status of the tile work may induce low morale among some tile technicians. Furthermore, the behaviors of other workers towards the tile technicians may be a significant source of additional work load and time pressure.

Errors (most of which can be traced back to these organizational factors) can be classified using a taxonomy which has been designed to guide the choice of management improvements (Paté-Cornell, 1990.) Errors are categorized into two groups: *gross errors* (uncontroversial mistakes, for example, an unbonded tile) and *errors of judgment under uncertainty* (for instance, the decision to live with a

problem that seems minor --but may not be so-- until the next flight in order to decrease the work load.) Gross errors generally call for improvements of the hiring and training procedures, inspection and quality control, and information flow; errors of judgment generally require modification of incentives and rewards, improvement in the treatment and communication of uncertainties, and adaptation of the resource constraints.

5.2 Preliminary observations

In this preliminary phase, we identified the following factors as possibly affecting the efficiency of tile risk management: (1) time pressures, (2) liability concerns and conflicts among contractors, (3) turnover among tile technicians and low status of tile work, (4) need for more random testing, and (5) contribution of the management of the ET and the SRBs to TPS reliability problems. The study of these factors will be the object of the Phase 2 of this work. The foundation of this analysis will be *the risk-criticality of each tile* so that limited resources --for example, the limited number of *tile inspectors*-- can be directed first where the probability and the consequences of tile failure could be most severe.

5.2.1 Time pressures

Tile maintenance is often on the critical path to the next flight, specially after missions where tile damage has been extensive. People who find themselves under time pressures sometimes cut corners. For example, it was found in January 1989, that a tile technician had added water to the RTV mix in order to make it cure faster. Adding water at that stage (or spitting in the RTV) may decrease the long-term reliability of the bond: the catalytic reaction, which occurs during the curing, may reverse earlier and thus increases the probability of debonding under different types of loads. Time pressure is also probably the cause of more frequent errors, such as the misalignment of the tile/SIP system with the filler bar, so that only a fraction of the surface of the SIP is in contact with the orbiter's surface. Time pressures may be unavoidable, but some organizational improvements may attenuate their effects,

first, by reducing them whenever possible and second, by increasing tile quality control in the most risk-critical zones.

The time pressure under which the tile personnel operates can be reduced in several ways. First, automation of step and gap measurement (using laser devices and automatic data recording systems currently under development) may result not only in a significant reduction of the processing time, but also in a decrease of the roughness of the orbiter's surface. Second, simplifying the paper work for the tile technicians would allow them to spend more time working on the tiles and less time shuffling papers (an apparent source of frustration). Third, it seems desirable to avoid over monitoring. For example, imposing daily targets (as opposed to weekly ones) for the number of tiles to be processed may decrease the variability and the flexibility needed for optimal performance and system reliability. Fourth, time pressure may be alleviated by reducing the access time to data bases and information that is necessary for prompt maintenance decisions. The maintenance at KSC is done by Lockheed, while some of the relevant data bases are controlled by Rockwell. NASA may want to improve the transfer of information from one to the other and/or within these two organizations.

5.2.2 Liability concerns and conflicts among contractors

Relatively harmonious relations have been instituted among the people who work on the tiles. They share a common concern for the safety of the system despite obvious sources of conflicts. Rockwell and Lockheed are in a competitive situation which does not always provide incentives to make the other's work easier. Among other factors, the liabilities of the main contractors are such that they occasionally have incentives to withhold technical information (for legal and contractual reasons) that may be useful (if not essential) for the performance of the other. These decisions may be justified given the ways the contracts have been set. There are ways of writing and handling contracts that improve incentives for cooperation and encourage the sharing of relevant technical information. This implies that contracts

that affect the same subsystems (e.g., the tiles) and are signed with different firms cannot be managed independently. The positive side of this competition among contractors is that there are no incentives for complacency and strong motivations to detect and correct errors made by the other. There are, however, strong incentives to hide those made by one's own company.

5.2.3 Turnover among tile technicians and low status of tile work

The turnover among the tile maintenance personnel is high. Because tile technicians are classified in the low-pay category of material (fiberglass) technicians (a practice that NASA apparently inherited from the DoD), many of them leave their tile maintenance jobs shortly after completing the training program and obtaining certification. Organization experts generally believe that high turnover is incompatible with learning (individual and organizational) and optimal performance. Therefore, this turnover might affect TPS safety due to inferior quality work by less experienced people. Protruding gap fillers, for example, are caused by poor quality installation and are a probable cause of early boundary layer transition (Smith, 1989.) This condition may not, in itself, threaten flight safety unless it is coupled with other factors. It does decrease the overall TPS reliability and may be an adverse result of high turnover and the corresponding lack of experience of the work force. On the other hand, according to some of the technicians, the old-timers may not be as respectful of "the book" as the newcomers. Assessment of the net result of inexperience and complacency requires a study of the coupling between time on the job and occurrences of errors.

The low-paying job factor may have other indirect, negative effects on the reliability of the tiles. Because of the low consideration that other categories of technicians seem to have for tile work when doing other types of technical work on the orbiter (e.g., mechanical, or electrical) other workers do not pay sufficient attention to the integrity of the tiles. They damage tiles frequently (if not seriously) thus adding considerably to the tile maintenance work. Therefore, the low status of

the tile workers, grounded in the pay scale, may have several detrimental effects: (1) a waste of money in training tile technicians that leave the job as quickly as possible, (2) low morale for some of them, which is seldom conducive to high-quality work, and (3) the "no respect" syndrome on the part of other technicians who carelessly damage tiles. The result is an increase of time pressure for a system that is already "the long pole" a large part of the time. In the end, these factors may encourage detrimental corner-cutting in tile processing.

5.2.4 Need for more random testing:

The original tile work and subsequent maintenance work has not always been perfect. Some of the tiles have been only partially bonded and, in a few instances, not glued at all. For example, in November 1989, it was found in that one tile on orbiter Columbia had been holding for several flights by the friction of (or perhaps some RTV adherent to) the gap fillers. The fact that this tile held and did not cause an accident was called "a miracle" by the personnel who discovered the problem. How "miraculous" can be determined using this risk assessment model. (In fact, according to our estimate, the probability of debonding is 10^{-2} per flight for such a tile, making the probability of debonding in five flights in the order of 5%.) Because of these hidden weaknesses, it may be desirable to do more random, non-destructive pull tests of the black tiles between flights, focusing on the most risk-critical areas of the orbiter's surface in order to detect and replace the tiles that are far below the expected capacity.

In addition to the possibility that previous work may not have been perfect, the possibility of long-term deterioration of the room-temperature vulcanized (RTV) bond should be acknowledged and taken into account in maintenance procedures. This calls (1) for additional random testing to monitor the possible chemical degradation of the RTV after repeated heat-load cycles, and (2) for the development and implementation of non-destructive and, if possible, non-pull testing of the tiles' bond, to be applied in priority to the most risk-critical tiles.

5.2.5 Contribution of the management of the ET and the SRBs to TPS reliability:

A significant fraction of the risk of TPS failure is due to debris, in particular, pieces of insulation from the external tank and the nose cone of the solid rocket boosters. In addition, tiles are much more likely to debond under the shock of chunks of debris when they are already loose or less than completely bonded. By backtracking the computer-simulated trajectories of pieces of debris from the most risk-critical parts of the orbiter surface back to the corresponding parts of the surface of the ET and the SRBs, it may be possible to identify which parts of the surface of the ET and the SRBs should be given special attention in the treatment of the insulation. Additional testing should, therefore, be performed for tiles located in zones that are most likely to be hit by SRB and ET insulation debris.

For each of these organizational factors, the analytical procedure is to identify the decisions that they affect, the errors that they can cause, the frequency with which they occur, the nature and the severity of the resulting errors as a function of the severity of the conditions, and their effect on the probability of failure of the system using our PRA model. The efficiency of possible management improvements can then be roughly assessed so that efforts are concentrated where they can provide the greatest benefits. This assessment will be the objective of the second phase of this study.

Section 6:
CONCLUSIONS

The results of our model's illustration suggest that the probability of loss of an orbiter due to failure of the black tiles is in the order of 10^{-3} with about 15% of the tiles accounting for about 80% of the risk. If one accepts the rough NASA estimates that the probability of losing an orbiter is in the order of 10^{-2} per flight (Broad, 1989) and that a significant part of it is attributable to the main engines, then the proportion of the risk attributable to the TPS (about 10%) is not alarming, but certainly cannot to be dismissed. (Our probabilities are coarse numbers that can be refined in the second phase of the work, but they are probably in the ball park.) A critical issue is: how will these probabilities evolve in the years to come? On one hand, the quality of the tile work and the detection mechanisms for defective tiles are expected to improve. On the other hand, exposure to repeated load cycles and environmental conditions or chemical reaction may deteriorate the system's peformance capacity unless closely managed.

One of our key findings is that the most risk-critical tiles are not all in the hottest areas of the orbiter's surface. We introduced, in this study, the notion of risk-criticality and the computation of a *risk-criticality index* to account for the loads to which the tiles are subjected and the consequences of their failures given their location with respect to other critical subsystems which they protect (functional criticality). This index can serve as a guide to set management priorities, for example, for the gradual replacement of the tiles, focusing first where tile failure could be most damaging.

Well-designed, manufactured, bonded, and maintained tiles are extremely unlikely to fail. A large fraction of the risk seems to be attributable to tiles that are

only partially bonded, or to those that are not bonded at all and are held in place by the gap fillers. Management assumes unnecessary risk by denying that errors have occurred and will occur again and that, consequently, the capacity of the TPS is reduced. To assume that all work is perfect leads to a potentially gross underestimation of the risk, rendering the maintenance procedures based on this assumption of perfection suboptimal. What the actual magnitude of this part of the risk is and which organizational improvements can bring the greatest risk-reduction benefits will be studied further in the second phase of this study. This part will involve a systematic analysis of the maintenance process to identify the different types of errors (past and present), their rates of occurrences, their probabilities of detection and correction, and their severity levels (i.e., by how much they decrease the system's capacity in each case). Relating these errors to the organizational factors described in the previous section will allow us to identify management improvements, their costs, and their expected positive effects on the TPS performance.

After the completion of the first of two phases of research, our preliminary conclusions are that it is desirable: (1) to expand the current concept of criticality for the tiles (to include functional criticality, as well as the heat loads in a risk-criticality measure), (2) to adapt the inspection and maintenance procedures to focus in priority on the most risk-critical tiles, and (3) to modify the existing data bases to include the risk-criticality factor for each tile.

Section 7:

REFERENCES

Aviation Week and Space Technology. Shuttle Orbiter To Use Silica Insulation. January 26, 1976.

Aviation Week and Space Technology. Orbiter Protective Tiles Assume Structural Role. February 25, 1980.

Baker, E. and B. Dunbar. Thermal Protection System (TPS) . Trend Analysis Survey. NASA Lyndon B. Johnson Space Center. Flight Crew Operations Directorate, March 2, 1988.

Broad, W. J. NASA Now Admits It's Worried About Disasters. San Francisco Chronicle, April 10 1989.

Cooper, P. A. and P. F. Holloway. The Shuttle Tile Story. Astronautics and Aeronautics. January 1981, pp. 24-34.

Garrick, B. J. Quantitative Risk Assessment and the Space Program. Risk Analysis Seminar Series, Department of Industrial Engineering, Stanford, California, March, 1988.

Lockheed Research and Development Division Tile Bond Verification Shuttle Inspection System (Rebecca Welling et al.) Palo Alto California, March, 1989.

Lockheed Space Operations Company. Orbiter Thermal Protection System Review. Part II. Presentation by David Weber, Kennedy Space Center, November 7, 1989.

McClymonds, J. W. Records of Debris Impact and Tile Damage. Rockwell International, Downey, California, 1989.

National Research Council. Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management. (Slay Committee Report) National Academy Press, Washington D.C. 1988.

Orbiter TPS Damage Review Team, STS-27R, OV-104. Summary Report, Vol. 1, Feb. 1989.

Paté-Cornell, M. E. Organizational Extension of PRA models and NASA Application. Proceedings of PSA'89 (ANS Conference on Probabilistic Safety Assessment), Pittsburgh, Pennsylvania, April, 1989.

Paté-Cornell, M. E. and F. G. Bea. Organizational Aspects of Engineering Systems Reliability and Application to Offshore Platforms. Research Report No. 89-1, Department of Industrial Engineering and Engineering Management, Stanford University, Stanford, California, April, 1989.

Paté-Cornell, M. E. Organizational Aspects of Engineering System Safety: the Case of Offshore Platforms. Science, Vol. 250, November 30, 1990, pp. 1210-1217.

Presidential Commission on the Space Shuttle Challenger Accident. Washington D.C. June, 1986.

Rockwell International. Shuttle System Integration. Debris Damage Assessment Summary, Downey, California, 1989.

Rockwell International. Thermal Protection System. Standard Maintenance Procedures Specification. Downey, California, September, 1989.

Rockwell International. Thermal Protection System Reusable Surface Insulation (RSI) Maintenance. Specification. Downey, California, September, 1988.

SIORA. Final Report for the SIORA Program--Shuttle Tile Automation Project, Stanford University, April, 1990.

Shuttle Operational Data Book. Vol. 4, Orbiter Landing Emergency Rescue. Data Part 1. NASA, Lyndon B. Johnson Space Center, Houston, Texas, January, 1988.

Smith, J. A. STS-3, Structural and Aerodynamic Pressure and Aerothermodynamics and Thermal Protection System Measurement Locations. NASA, Lyndon B. Johnson Space Center, January, 1982.

Smith, J. A. STS-28R Early Boundary Layer Transition. Engineering Directorate, Johnson Space Center, Houston, Texas, December 1989.

X-Sender: sreidcar@mail.hq.nasa.gov
Date: Tue, 4 Feb 2003 10:38:22 -0700
To: w.p.gilbert@larc.nasa.gov, m.p.saunders@larc.nasa.gov
From: Sandra Reid <sreidcar@hq.nasa.gov>

Bill and Mark,

Attached is a copy of a report on:

Safety of the Thermal Protection System of the Space Shuttle Orbiter:
Quantitative Analysis and Organizational Factors
Phase 1: Risk-Based Priority Scale and Preliminary Observations

by

M. Elisabeth Pate-Cornell
Department of Industrial Engineering and Engineering Management
Stanford University

Paul S. Fischbeck
Department of Engineering and Public Policy
and Department of Decision Sciences
Carnegie-Mellon University

REPORT TO
THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Cooperative Research Agreement No. NCC 10-0001
between Stanford University and NASA (Kennedy Space Center)

The study was conducted in 1995 and provides a probabilistic risk-based assessment of the ramifications to the Space Shuttle given certain TPS damage states. The report clearly indicates that there is a high potential for Space Shuttle system damage resulting in a high probability of Space Shuttle Loss of Vehicle and Crew given certain TPS damage states.

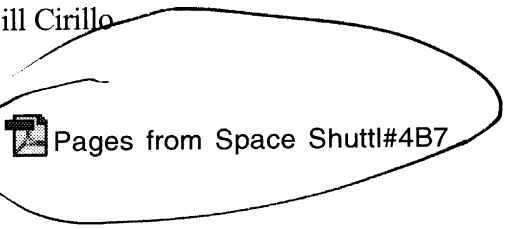
The study noted:

"...that the two areas just in board of the main landing gear have been noted as being in the high burnthrough area. This is not strictly speaking a burnthrough problem. The structure in those areas is extremely sensitive to temperature differences and would fail even without a burn-through. However, because of their sensitivity to temperature, these two areas were grouped in the high burn-through category."

If you have any questions please call me at [redacted] (cell) or send me an e-mail. I will be back in the office on Friday, February 4.

Thanks.

Bill Cirillo



Could not open

To: Jonathan Cruz <j.n.cruz@larc.nasa.gov>
From: Cindy Lee <c.c.lee@larc.nasa.gov>
Subject: Re: proposed email on ISS
Cc:
Bcc:
X-Attachments:

Jonathan,
I am going to forward your email to the person in Public Affairs handling requests for information. She will give us guidance on what to do.
C-

Remainder of page
Withheld under FOIA Exemption
(b)(5)

RF-16

Page Withheld under
FOIA exemption (b)(5)

To: "CLEGHORN, CHERYL W" <C.W.CLEGHORN@LaRC.NASA.GOV>
From: Cindy Lee <c.c.lee@larc.nasa.gov>
Subject: Fwd: proposed email on ISS
Cc: "FINNERAN, MICHAEL P" <M.P.FINNERAN@LaRC.NASA.GOV>, "CRUZ, JONATHAN N" <J.N.CRUZ@LaRC.NASA.GOV>, "BREWER, LAURA M" <L.M.BREWER@LaRC.NASA.GOV>
Bcc:
X-Attachments:

Cheryl,
In our morning meeting that Del has convened on actions from Columbia, I mentioned to Mike that Jonathan Cruz from our Competency has a standing ISS email site that has had several questions posed to it on the Shuttle incident as related to ISS. This email distribution includes the press, NASA employees, and retires. While I think Jonathan's responses are well formulated, I was not sure how we would want to handle information coming from a variety of sources that go to the press and thought it best for you to give us guidance on how to proceed with these requests.
Thanks,
Cindy Lee

Remainder of page Withheld under FOIA exemption (b)(5)

RA-7

Remainder of page withheld under FOIA exemption (b)(5)

Remainder of page withheld under FOIA exemption (b)(5)

X-Sender: c.w.cleghorn@pop.larc.nasa.gov
Date: Tue, 4 Feb 2003 12:04:24 -0500
To: Cindy Lee <c.c.lee@larc.nasa.gov>
From: Cheryl Cleghorn <c.w.cleghorn@larc.nasa.gov>
Subject: Re: Fwd: proposed email on ISS
Cc: "FINNERAN, MICHAEL P" <M.P.FINNERAN@larc.nasa.gov>,
"CRUZ, JONATHAN N" <J.N.CRUZ@larc.nasa.gov>,
"BREWER, LAURA M" <L.M.BREWER@larc.nasa.gov>

Cindy,

I have been instructed to forward any non-media questions to Evelyn Thames at HQ. We have been sending the non-media requesters a message similar to the one shown below and forwarding the actual comments/questions to Evelyn.

Thank you for your expression of sympathy over the loss of Space Shuttle Columbia and the STS-107 crew. We appreciate your interest in finding the cause of the accident. Your message has been forwarded to the appropriate organization within NASA.

You can monitor news, information, and the ongoing investigation of the Space Shuttle Columbia - Mission STS-107 at http:/www.nasa.gov/columbia.

If you like, you can forward the non-media type to me and we will forward them to HQ or you can forward them to HQ directly.

Any media questions should be directed to the Head of Langley's Public Affairs Office, Marny Skora. Marny's office specifically deals with the media.

Thanks,

Cheryl

At 10:27 AM -0400 2/4/03, Cindy Lee wrote:

> Cheryl,
> In our morning meeting that Del has convened on actions from Columbia, I mentioned to Mike that Jonathan Cruz from our Competency has a standing ISS email site that has had several questions posed to it on the Shuttle incident as related to ISS. This email distribution includes the press, NASA employees, and retires. While I think Jonathan's responses are well formulated, I was not sure how we would want to handle information coming from a variety of sources that go to the press and thought it best for you to give us guidance on how to proceed with these requests.
> Thanks,
> Cindy Lee

RE-18

Remainder of page Withheld under FOIA exemption (b)(5).

Remainder of page
Withheld Under
FOIA exemption (b)(5)

NASA Langley Research Center
Office of Public Services
PHONE: (757) 864-2497
FAX: (757) 864-7732
http://www.larc.nasa.gov