FEB 05 '03 12:52 2023583007 PAGE.02

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

<u>Phase 1:</u>

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)

December, 1990

FEB 05 '03 12:57 2023583007 PAGE.03

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.

NASA HQ Program Fax:2023583007 Feb 5 2003 15:44 P.03

FEB 05 '03 12:57 2023583007 PAGE.04

TABLE OF CONTENT

FEB 05 '03 12:58 2023583007 PAGE.06

FIGURES

PAGE.07 2023583007 FEB 05 '03 12:58

NASA ODIN Program Fax:2023583007 Feb 5 2003 12:45

TABLES

FEB 05 '03 12:58 2025832007 PAGE.09

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.

NASA ODIN Program Fax:2025832007 Feb 5 2003 13:45 P.03

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

Phase 1:

<u>Risk-based priority scale and preliminary observations</u>

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 orbiters 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 this 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 edge 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. <u>Background information:</u> 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

FEB 05 '03 13:01 2023583007 PAGE.18

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

FEB 05 '03 13:01 2023583007 PAGE.19

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.)

NASA ODIN Program Fax:2023583007 Feb 5 2003 13:48 P.19

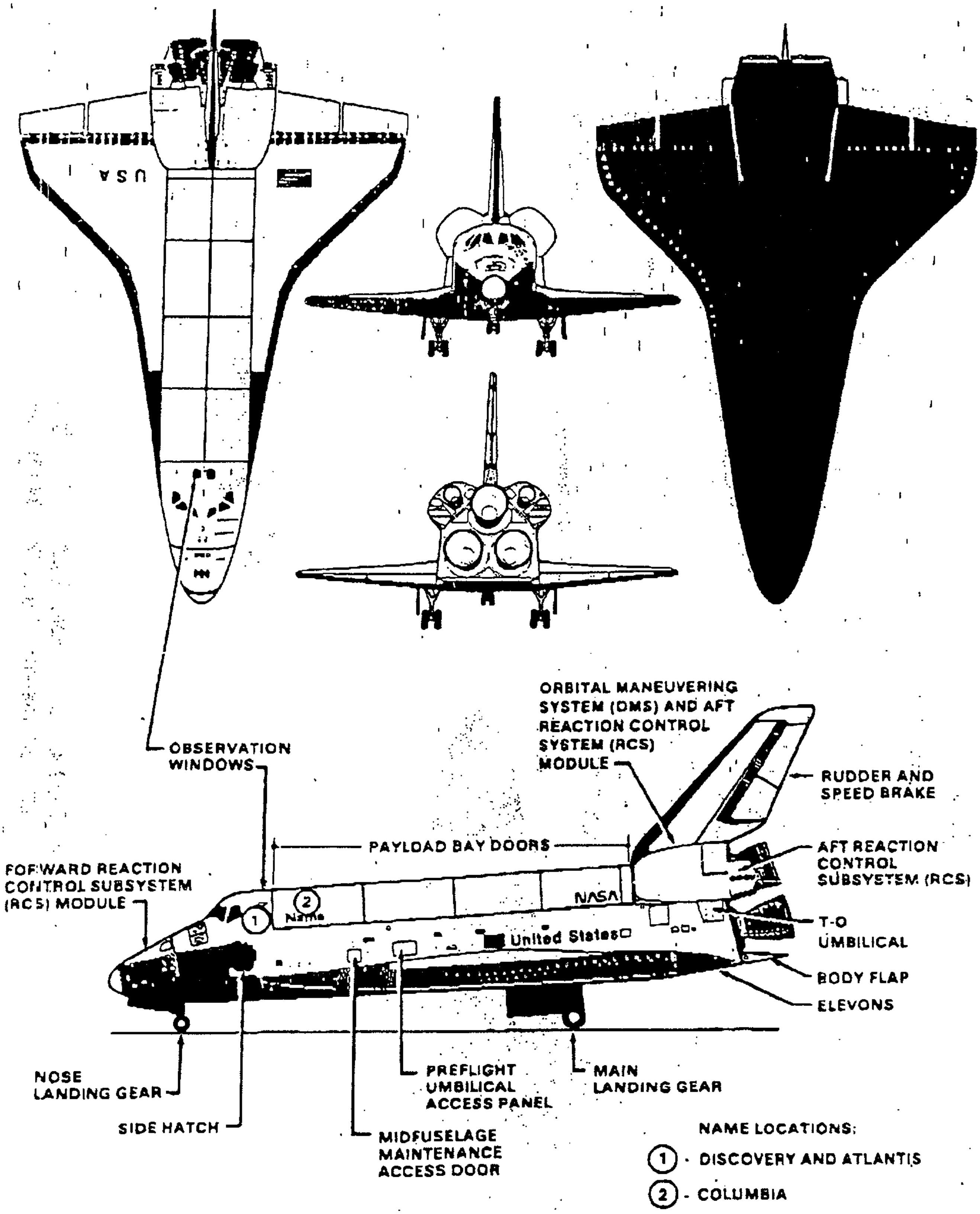


Figure 1: The space shuttle orbiter

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

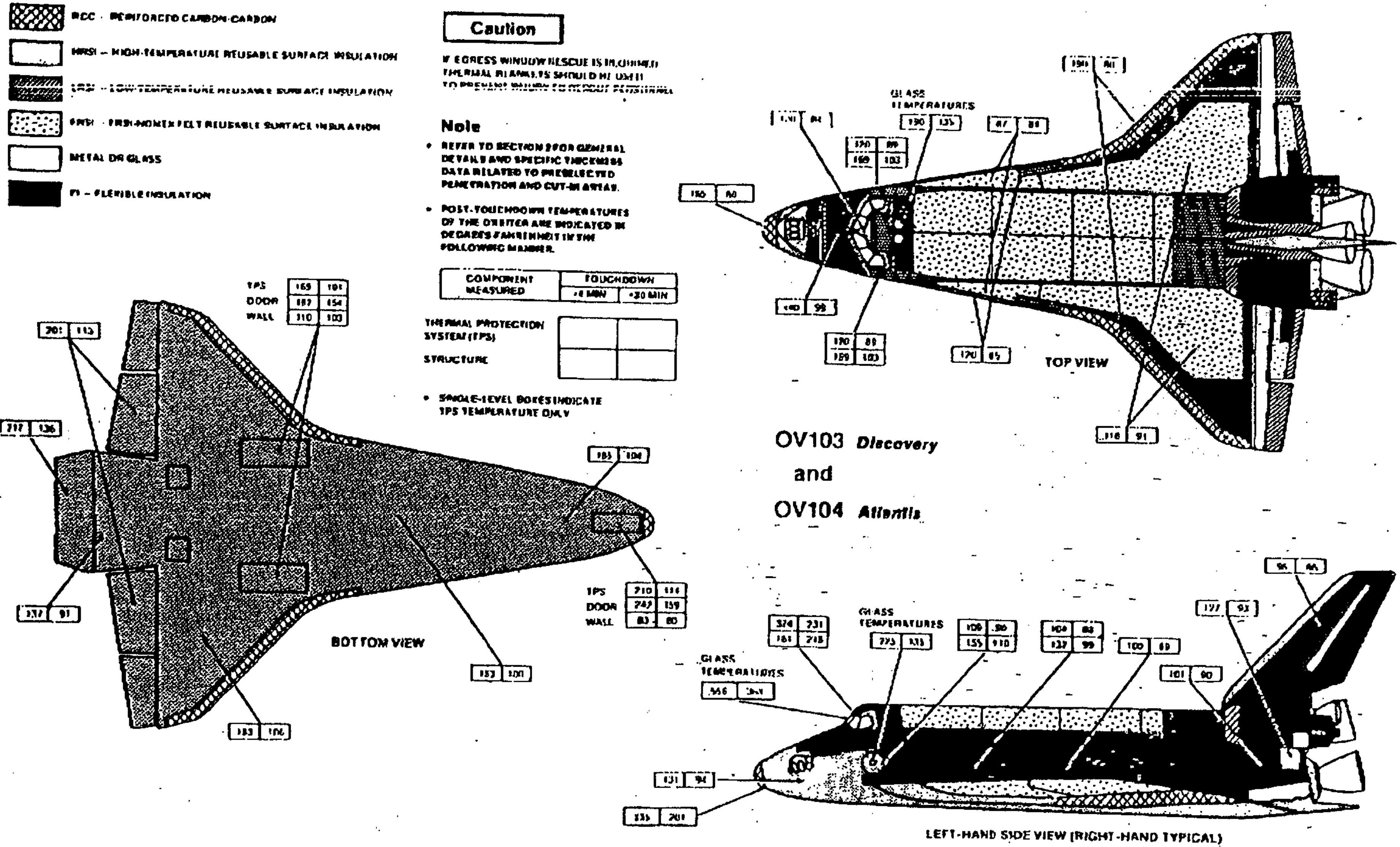


Figure 2: The thermal protection system (TPS) for OV 103 (Discovery) and OV 104 (Atlantis)

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

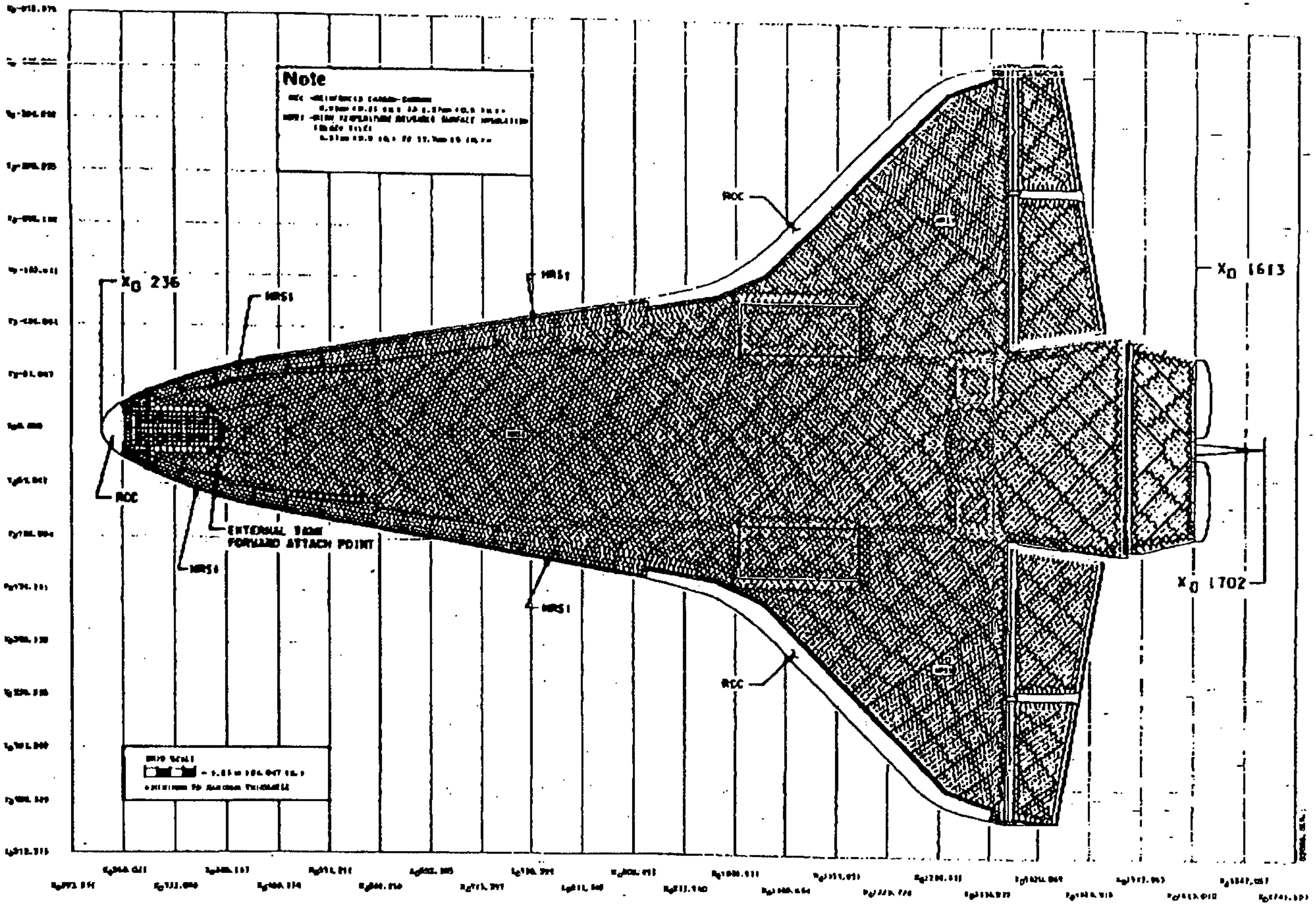


Figure 3: The black tiles (all vehicles)

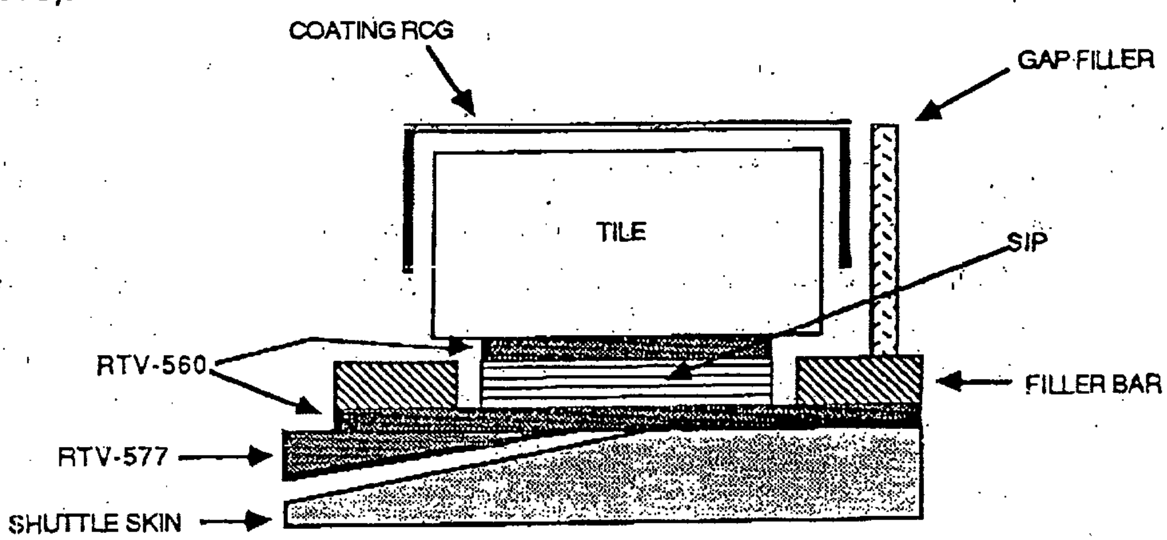
Source: Shuttle Operational Data Book, JSC 08934 Vol. 4

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).

FEB 05 '03 13:04 2023583007 PAGE.26

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

FEB 05 '07 17:04 2023583007 PAGE.27

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, 1988, 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

NASA OIG Program Fax:2023583007 Feb 5 2007 15:31 P.27

° 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 0.10 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	MajorDebris 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	Dicovery	11/22/89	21	118
33	32R	Columbia	01/09/90	15	120

Table 1: Summary of orbiter flights and debris damage

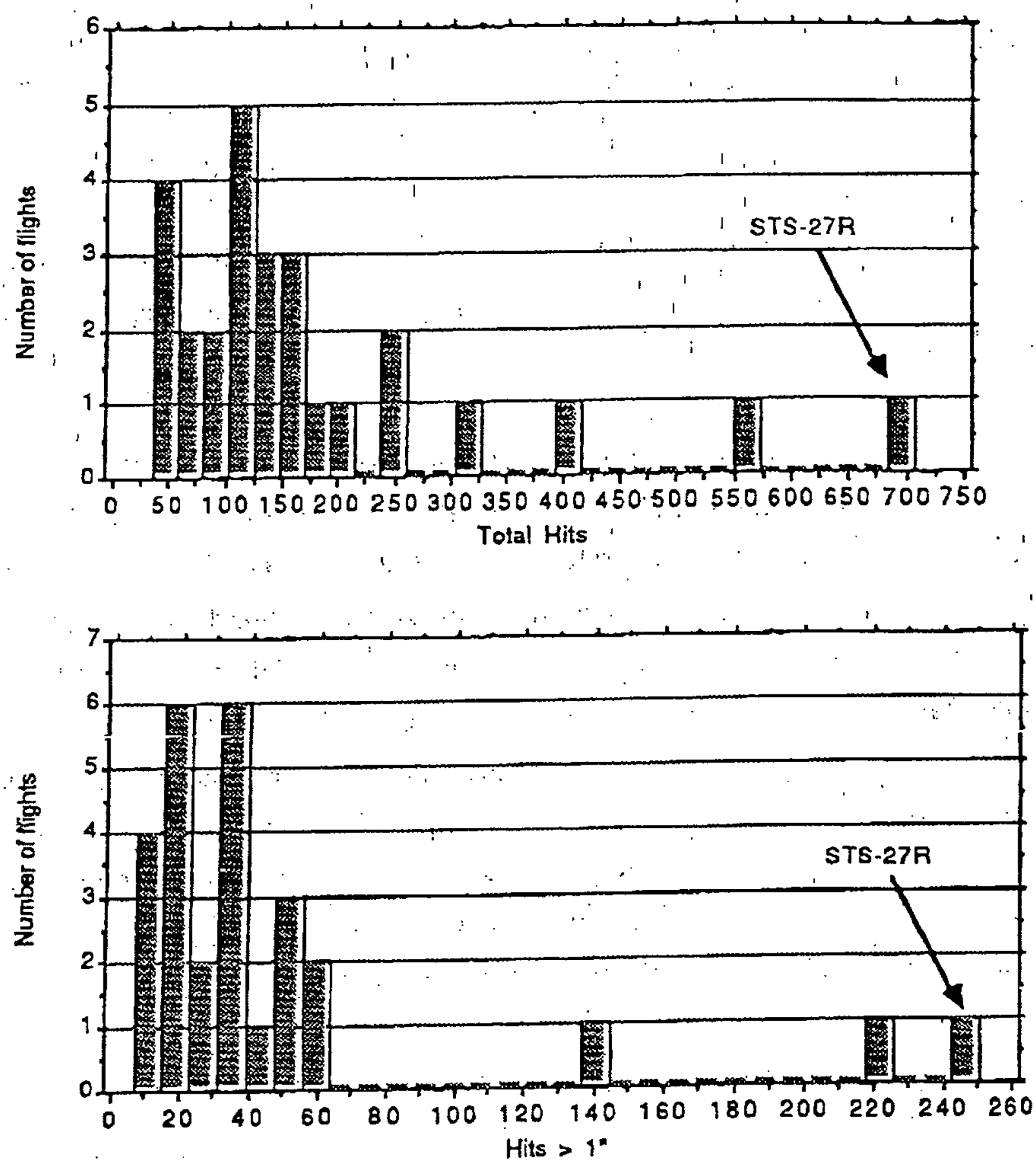


Figure 5: Histogram of tile damage due to debris.

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

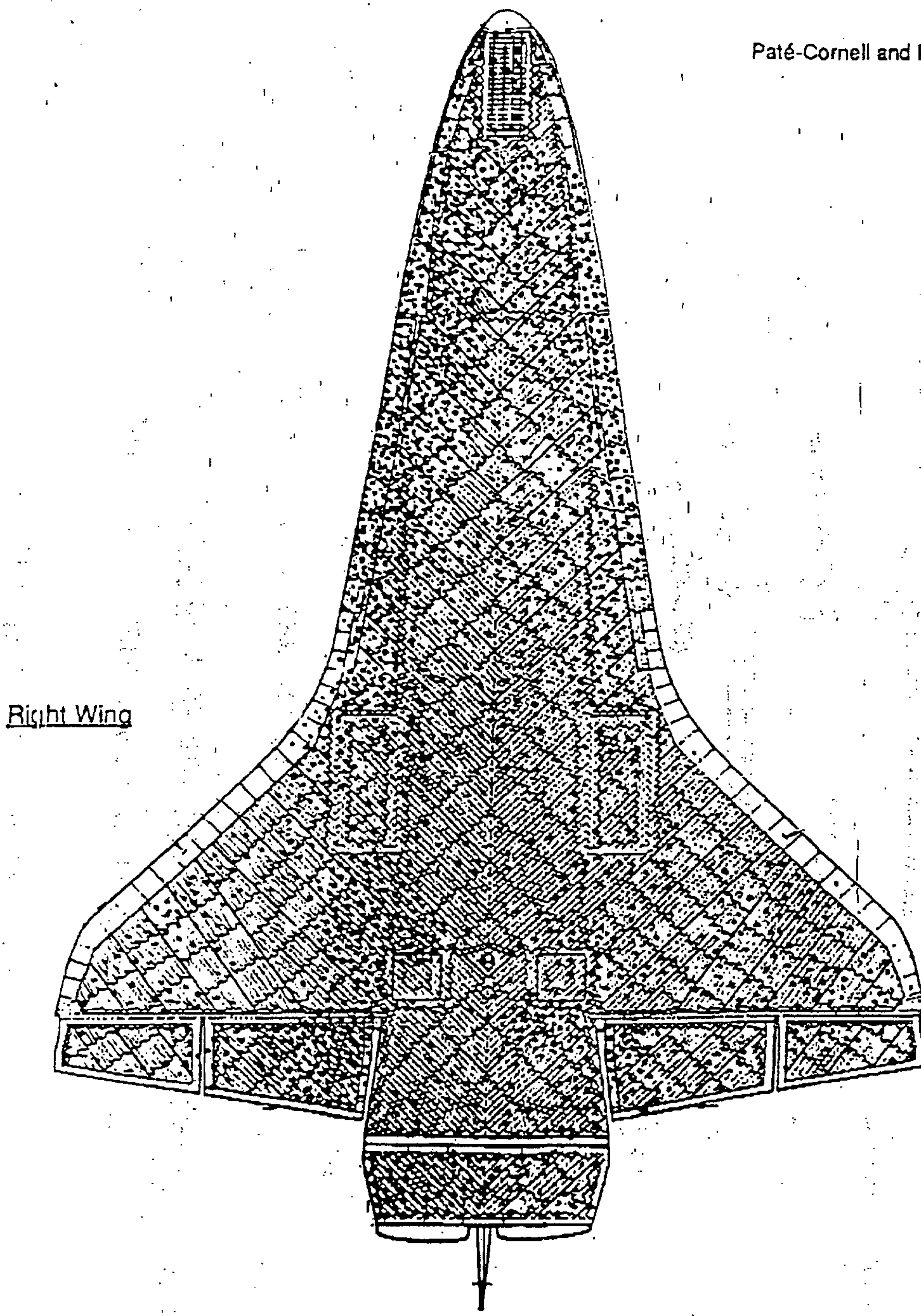


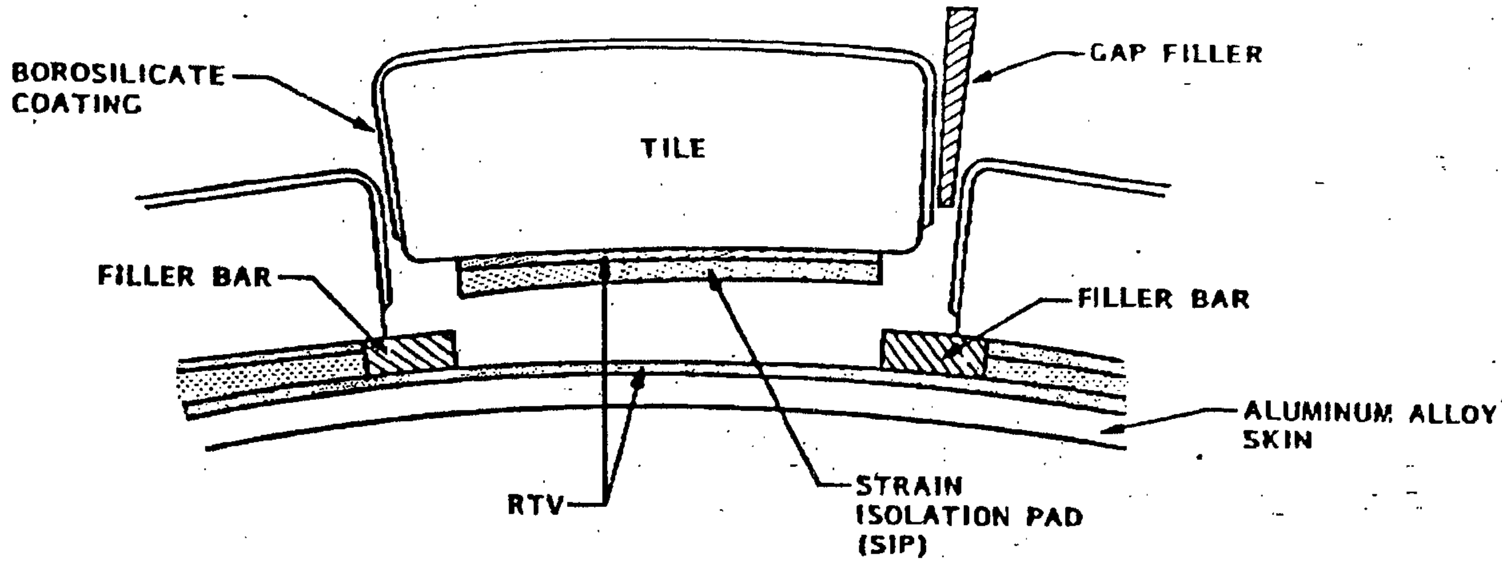
Figure 6: Accumulated major debris hits (lower surface) for flights STS-6 through STS-32R

Source of data: J. McClymonds, Rockwell International

Feb 5 2003 13:54 P.37
Fax:2023583007 NASA ODIN Program
PAGE.37 2023583007 FEB 05 '03 13:08

Lockheed

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

FEB 05 '03 13:09 2023583007 PAGE.40

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

FEB 05 '03 17:09 2023583007 PAGE.43

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

NASA ODIN Program Fax:2023583007 Feb 5 2003 15:56 P.43

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.

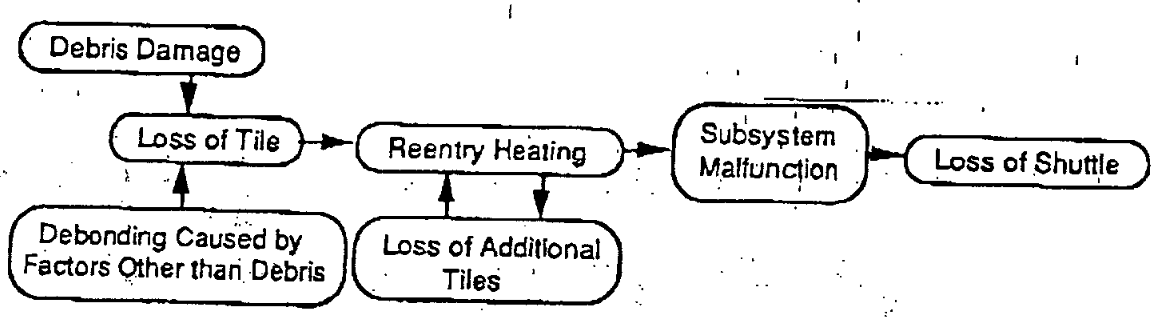
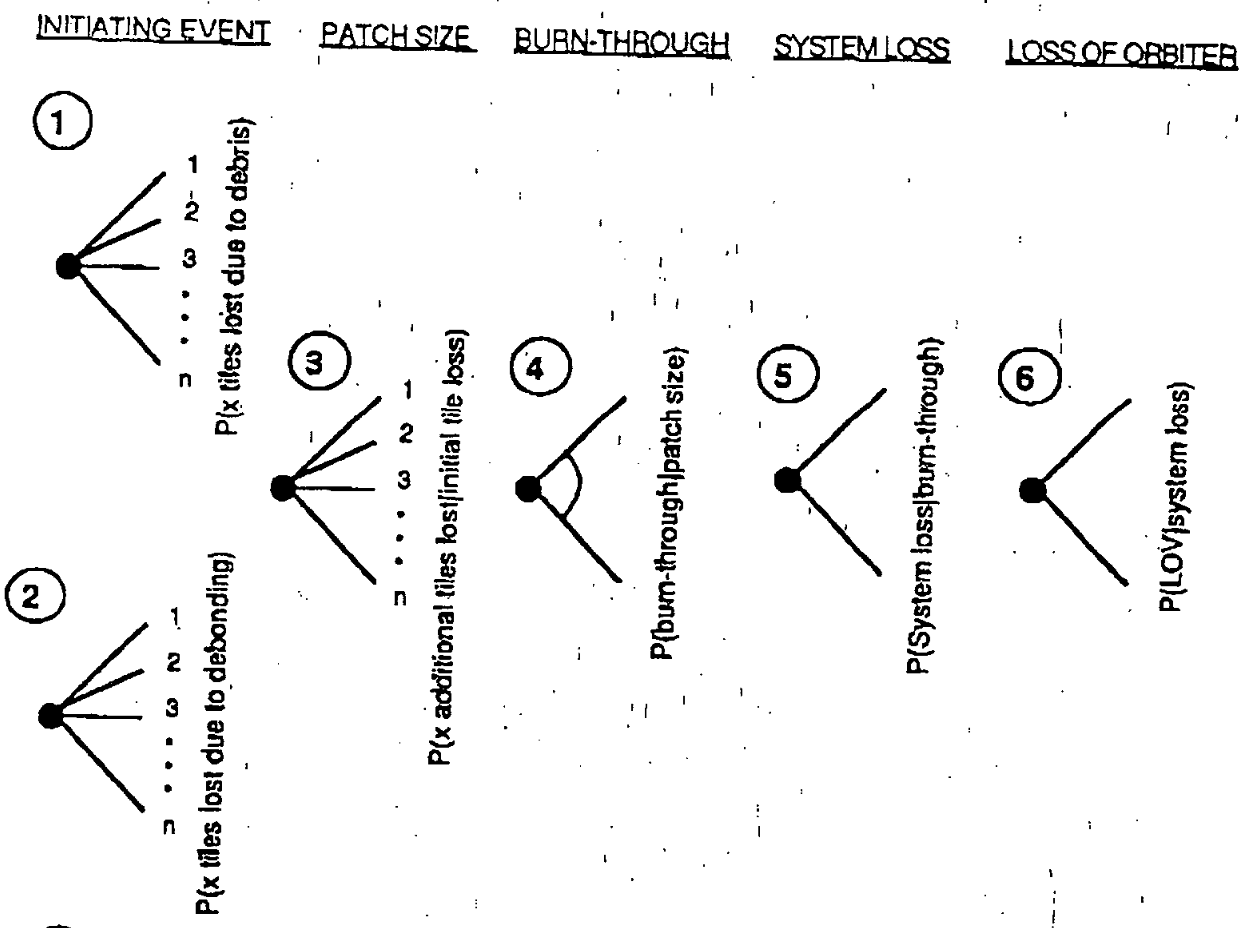


Figure 8: Event diagram: failure of the TPS leading to LOV

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.

FEB 05 '03 13:10 2023583007 PAGE.45



(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.)

FEB 05 '03 13:11 2023583007 PAGE.47

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".

NASA ODIN Program Fax:2023583007

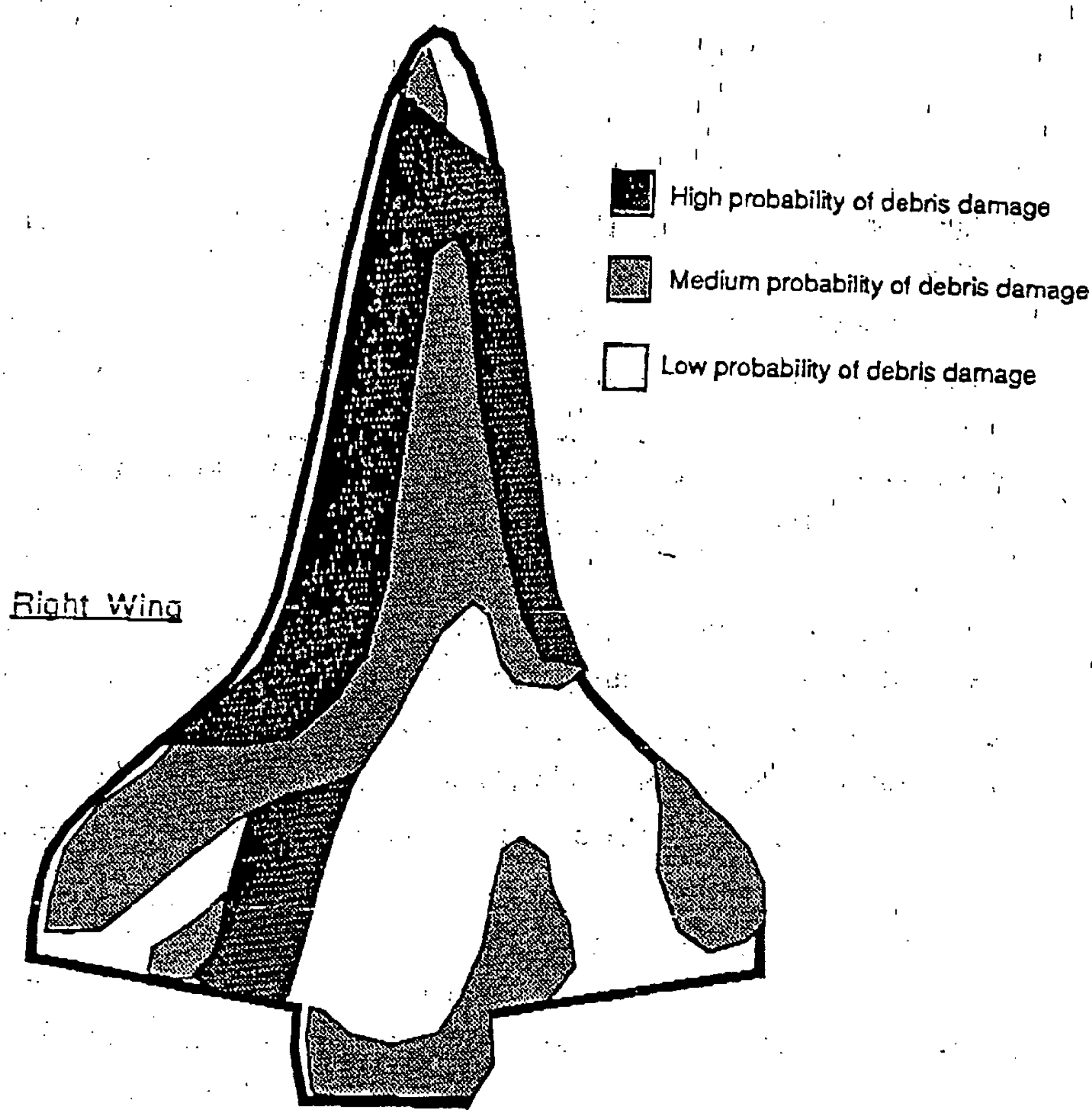


Figure 10: Partition of the orbiter's surface into three types of debris zones (index: h)

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}	3×10^{-3}	5×10^{-4}
P(One of two tiles hit)*	8×10^{-4}	2×10^{-4}	4×10^{-5}
P(One of three tiles hit)	7×10^{-5}	2×10^{-6}	3×10^{-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 (5×10^{-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

FEB 05 '03 13:12 2023583007 PAGE.51

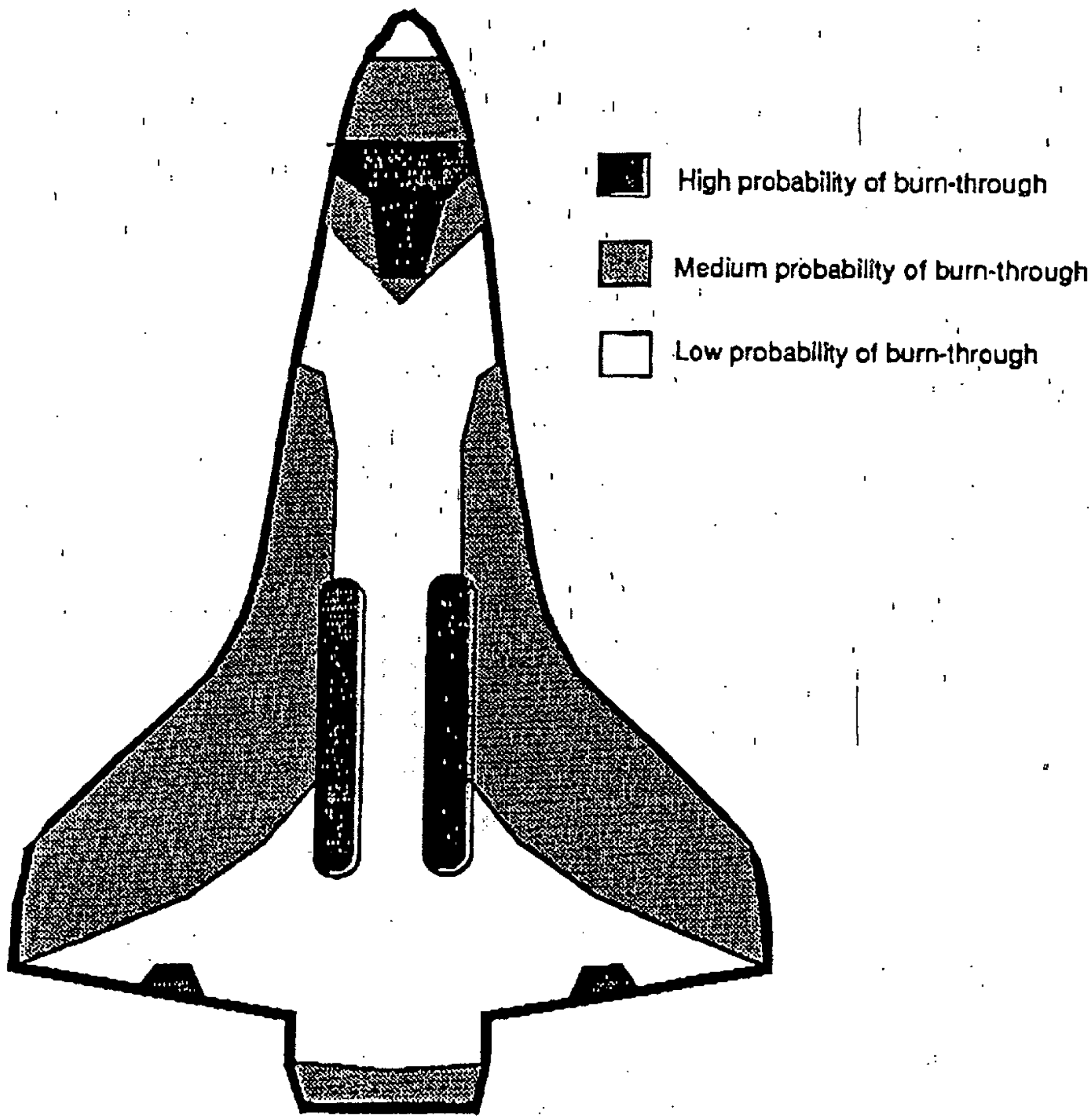


Figure 11: Partition of the orbiter's surface into three types of burn-through zones (index: k)

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 600°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 at 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.

FEB 05 '03 13:12 2023583007 PAGE.53

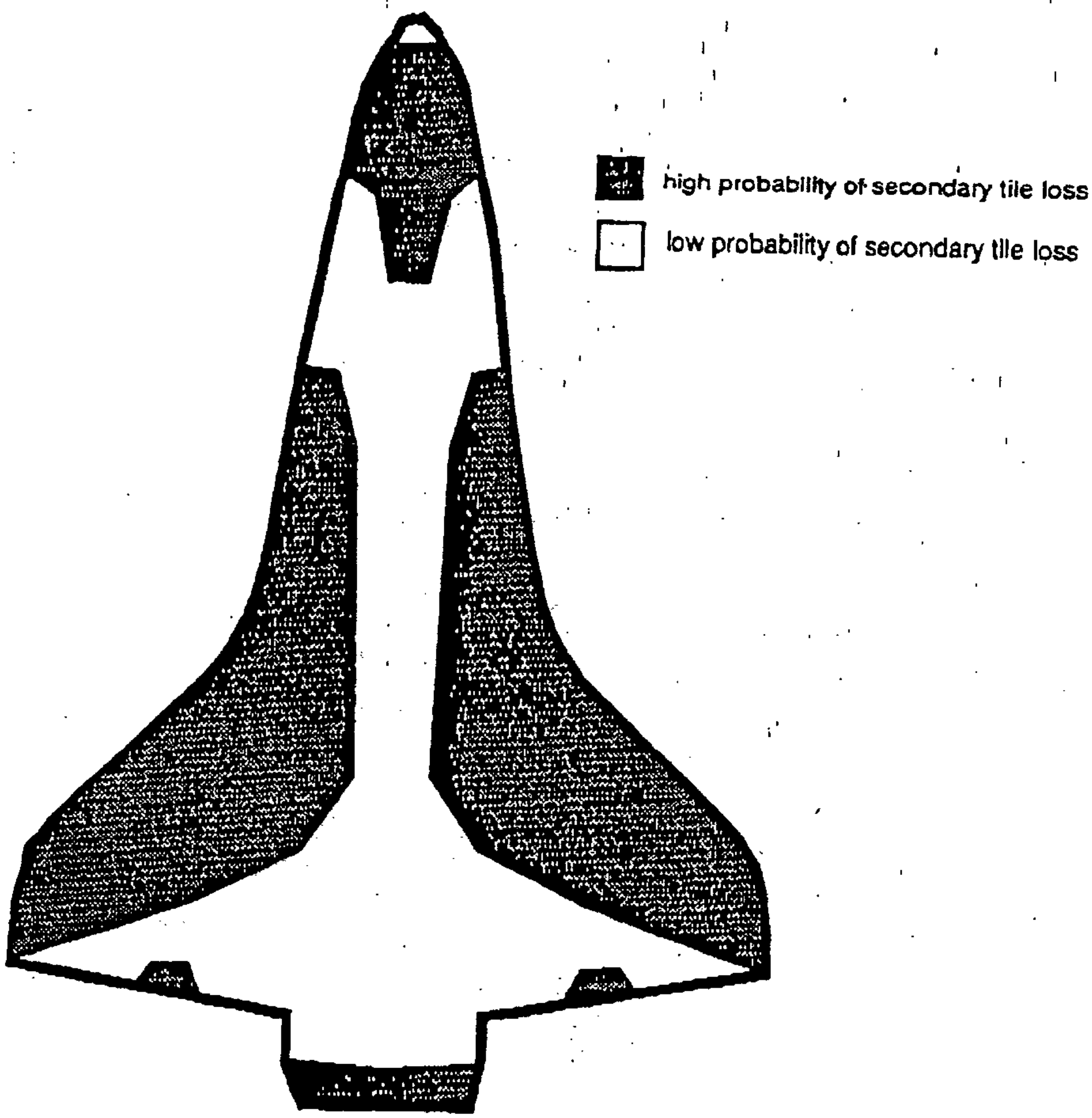


Figure 12: Partition of the orbiter's surface into two types of secondary tile loss zones (index: I)

NASA OIG Program Fax:2023583007 Feb 5 2003 13:59 P.55

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

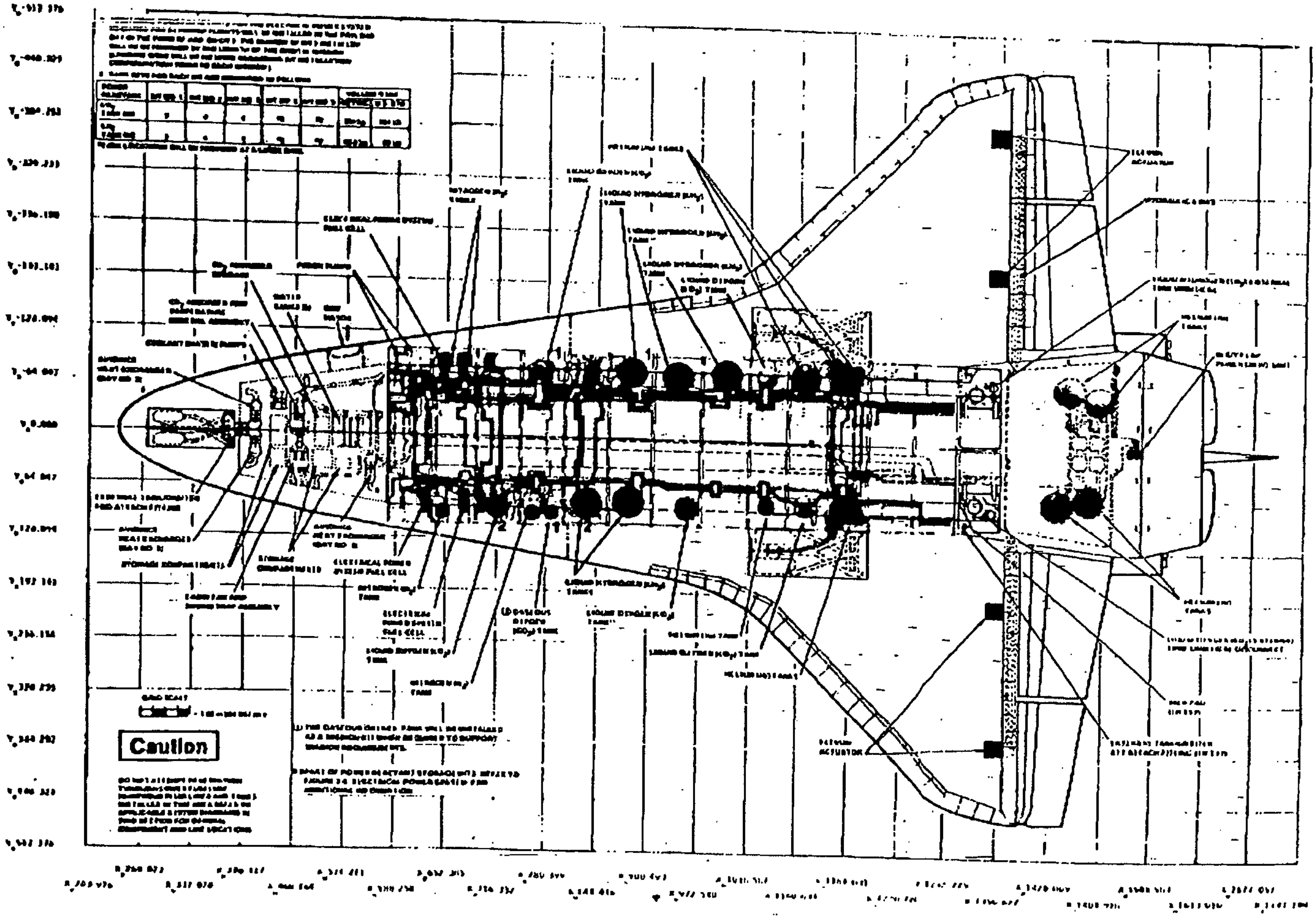


Figure 13: Component and systems location

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

FEB 05 '93 13:13 2023583007 PAGE.55

FEB 05 '03 13:15 2023583007 PAGE.02

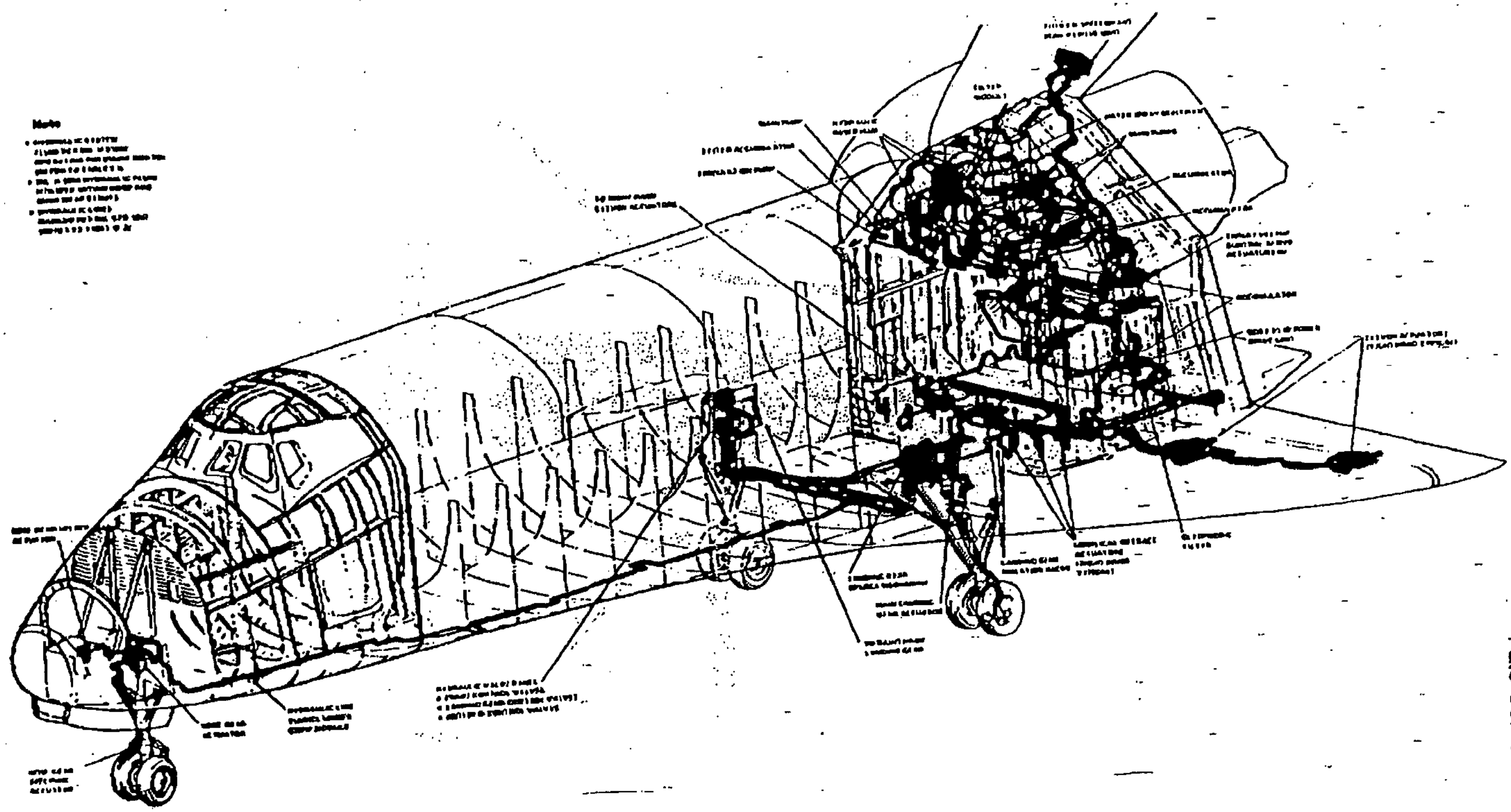


Figure 14: Hydraulic system components and line locations

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

FEB 05 '03 13:15 2023583007 PAGE.03

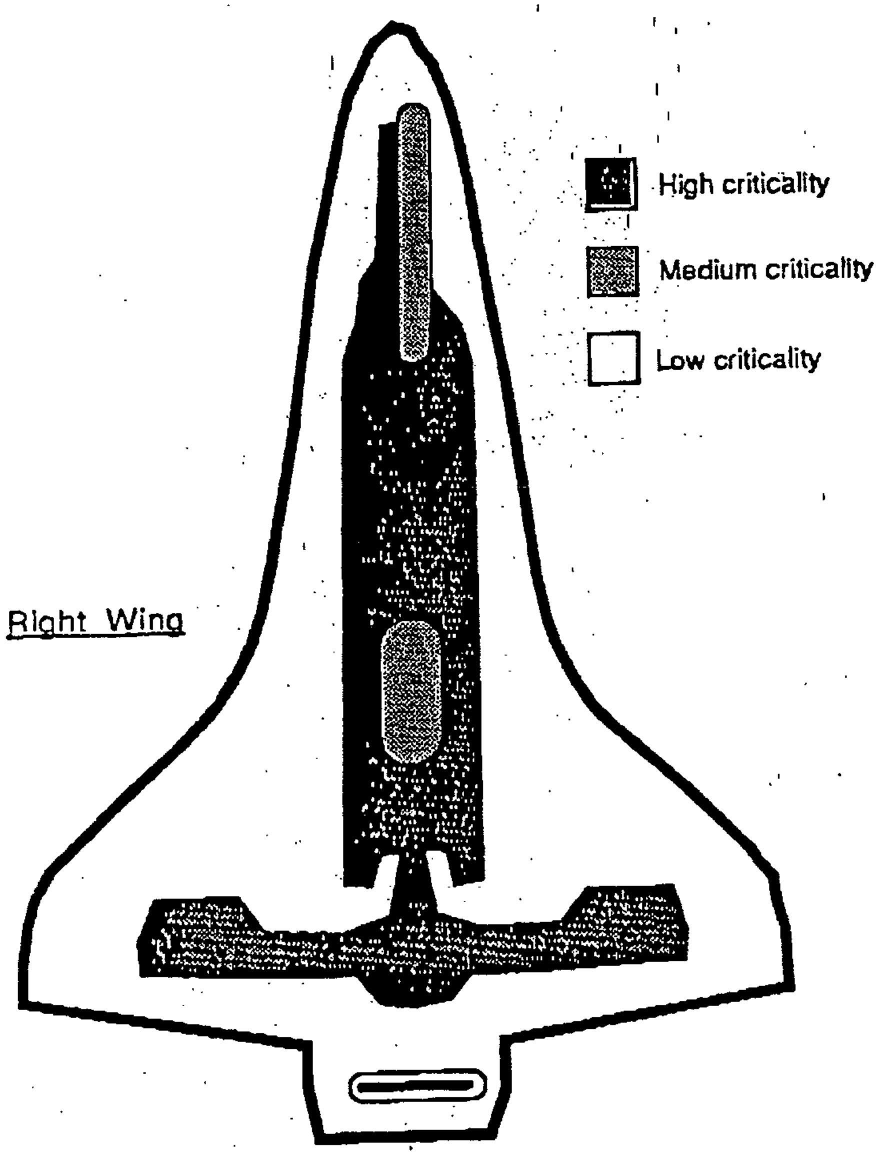


Figure 15: Partition of the orbiter's surface into three types of zones of functional criticality (index: j)

FEB 05 '03 13:16 2023583007 PAGE.04

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 x10^{-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 x 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

NASA ODIN Program Fax:2023583007 Feb 5 2003 14:02 P.04

RDD

Lockheed

TILE BOND VERIFICATION

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/AI 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 0.50. 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 fall. The probability that the final patch size reaches M depends on the secondary loss index of the min-zone (l_i) and is given by the following geometric distribution (which means that M-1 additional tiles fail and no adjacent tile afterwards:)

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

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:

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

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:

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

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

$$EV(M) = 1 / [1-P_i(Fa|Ft)] \quad (4)$$

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:

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

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

$$\ldots$$

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

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.

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

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

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:

$$\begin{aligned} P(L|\text{min-zone } i) &= \sum_{q=0}^{\infty} P_i(L|N_i=q) \times P_i(N_i=q) \\ &= \sum_{q=0}^{\infty} p'_i \times q \times P_i(N_i=q) \\ &= p'_i \times EV(N_i) \\ &= p'_i \times n_i \times P_i(Ft) \end{aligned} \qquad (9)$$

FEB 05 '03 13:17 2023583007 PAGE.10

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:

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

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:

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

If three tiles are damaged initially:

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

If four tiles are damaged initially:

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

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:

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

3.5 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:

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

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

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

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:

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

FEB 05 '03 13:18 2023583007 PAGE.13

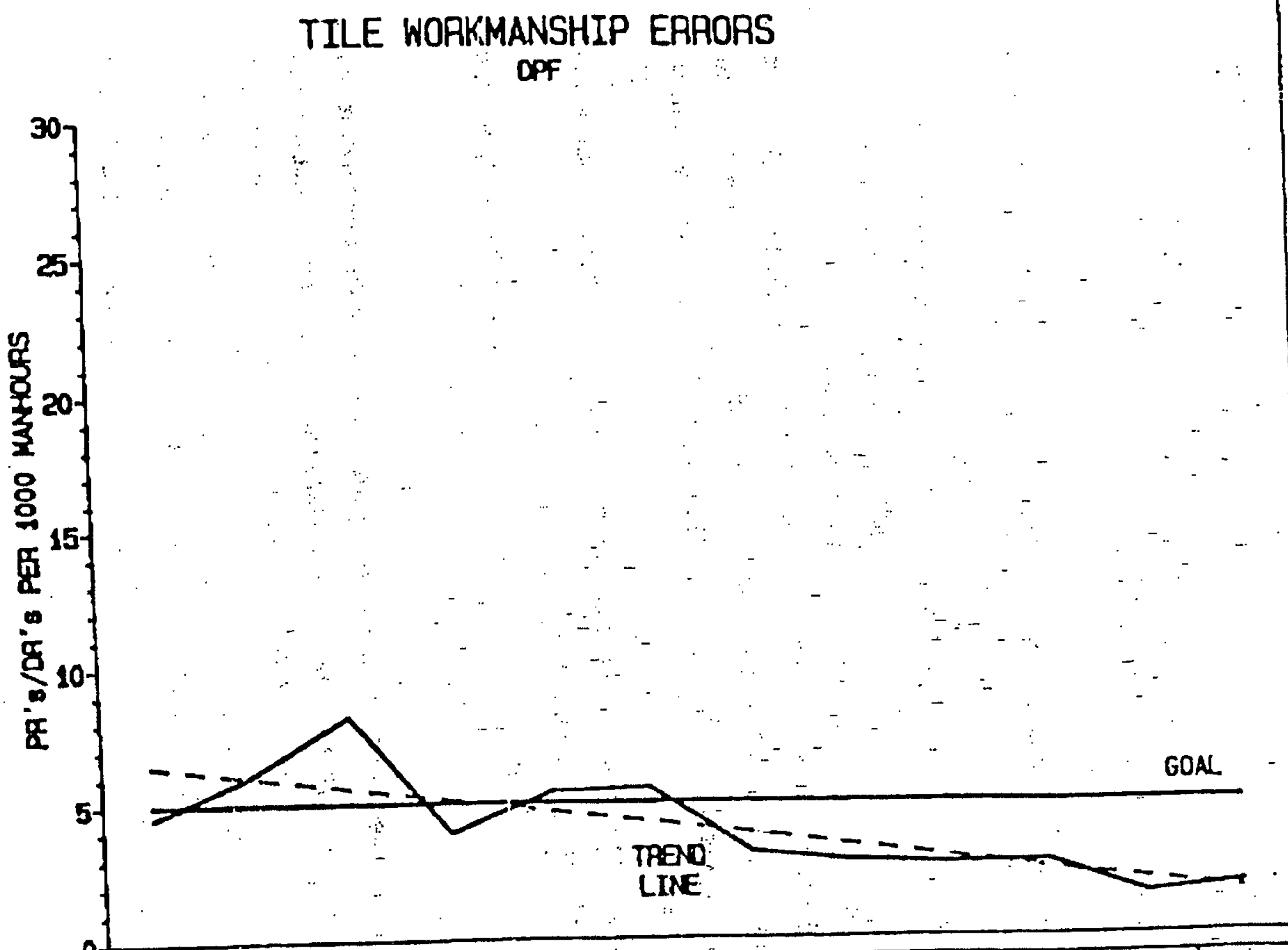
3.7 Additional Information and data

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;

NASA ODIN Program Fax:2023583007 Feb 5 2003 14:05 P.14



ERRORS/1000 MH WORKMANSHIP PR's MANHOURS	4.51 80 17757	6.03 162 26860	8.20 92 11216	3.83 109 28472	5.39 67 12426	5.52 159 28787	3.07 122 39689	2.74 84 30694	2.61 88 33690	2.69 111 41338	1.46 32 21968	1.79 31 17310
DATE	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	8/11

Figure 17: Tile workmanship errors

Source: D. Weber, Lockheed Corporation (1989)

FEB 05 '03 13:18 2023583007 PAGE.14

- 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.

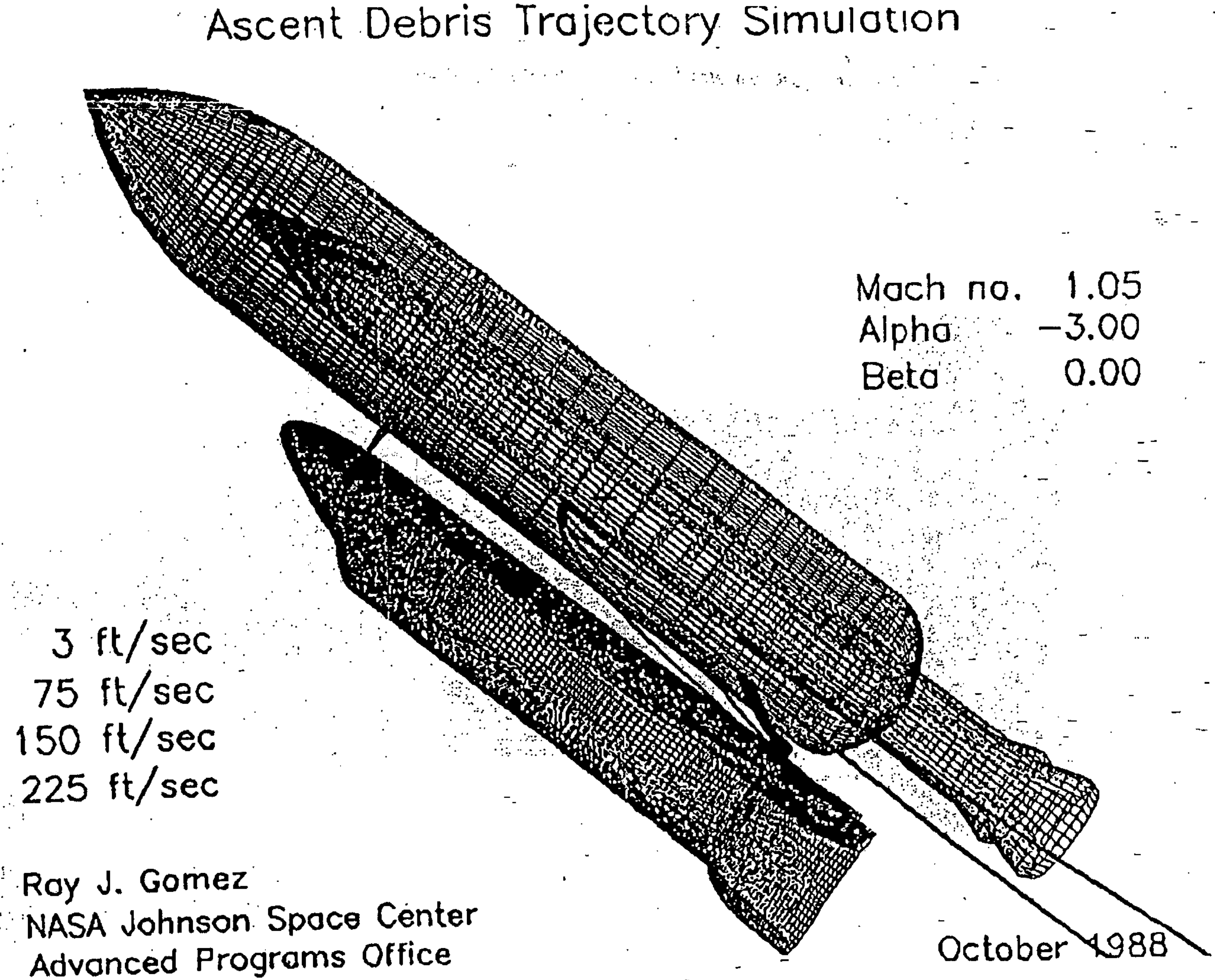


Figure 18: Ascent debris trajectory simulation (side view)

Source: R. Gomez, NASA JSC (1988).

PAGE.16 2023583007 FEB 05 '03 13:19

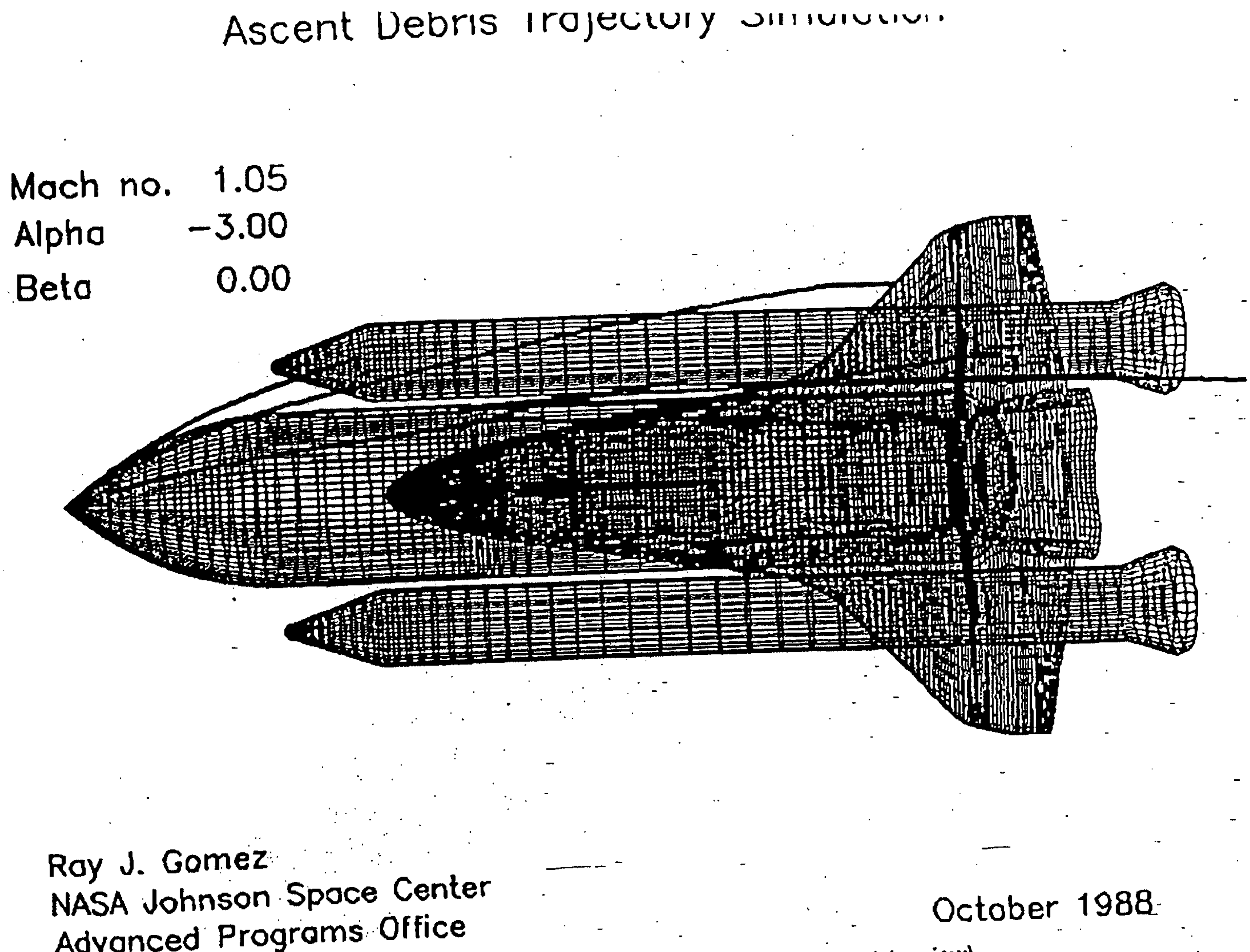


Figure 19: Ascent debris trajectory simulation (plan view)

Source: R. Gomez, NASA JSC (1988)

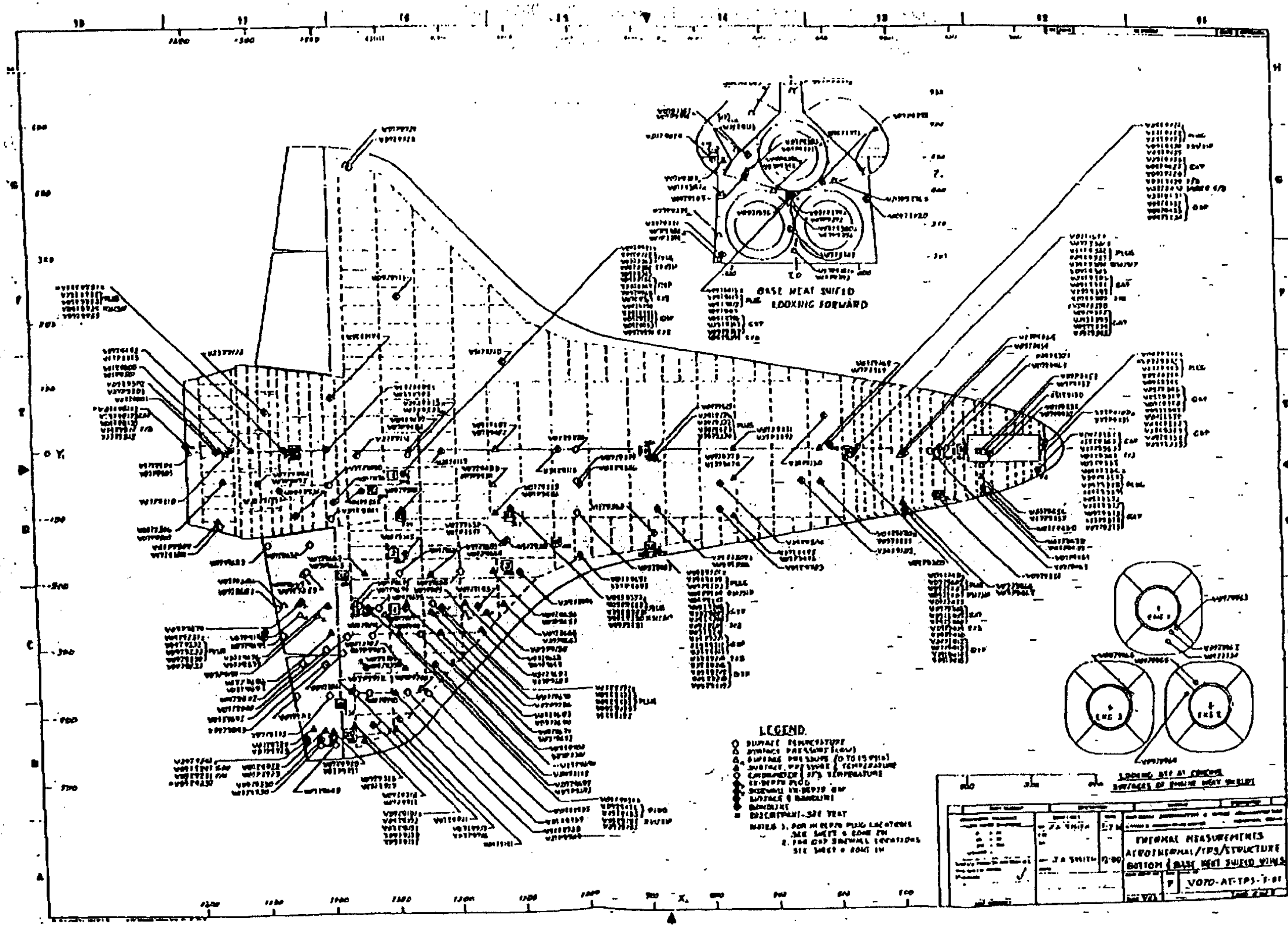


Figure 20: Thermal measurements (bottom view)

Source: Structural & Aerodynamic Pressure Measurement Locations JSC 17889

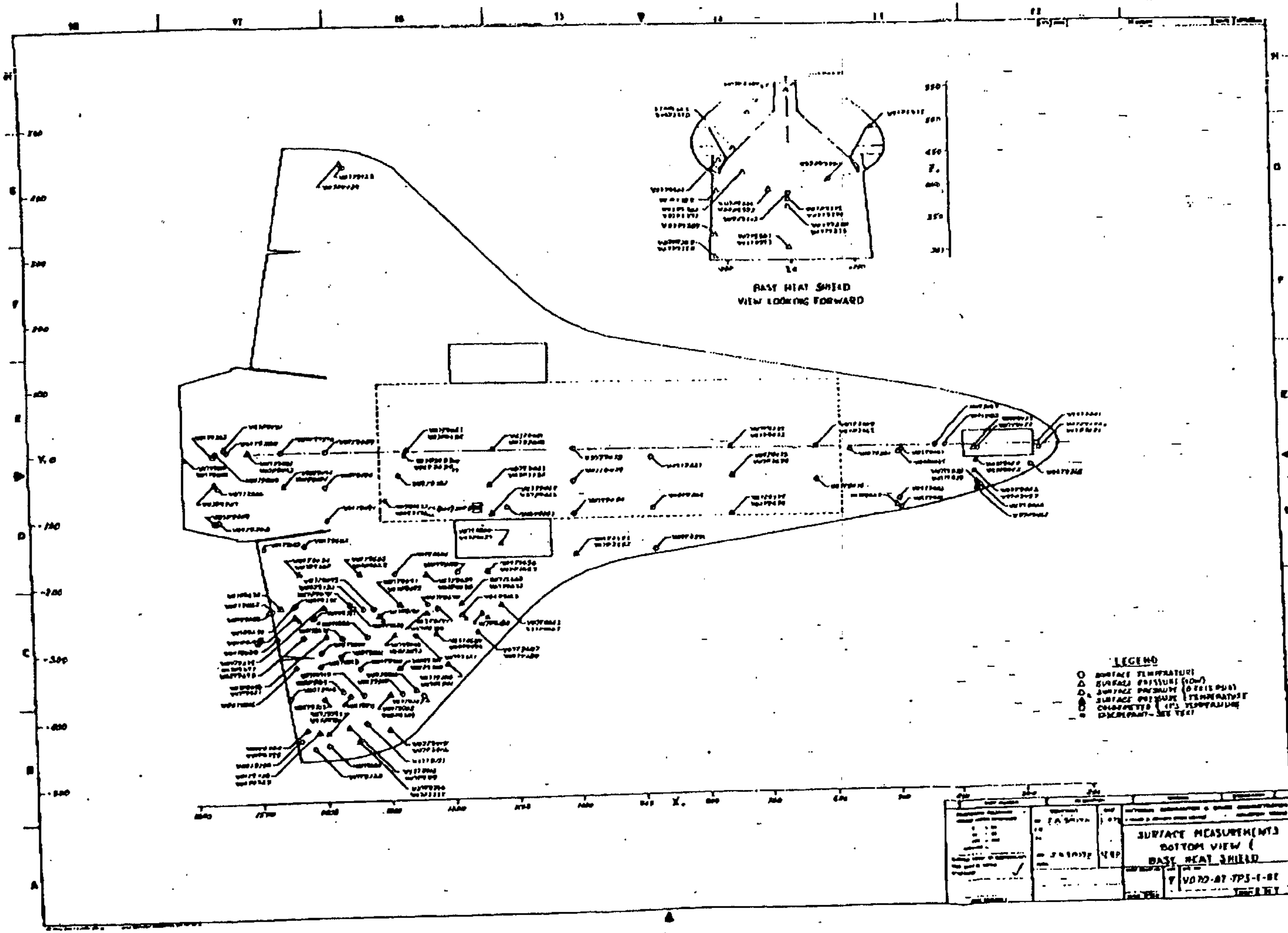


Figure 21: Surface measurements (bottom view)
Source: Structural & Aerodynamic Pressure Measurement Locations JSC 17889

FEB 05 '93 13:20 PAGE.19

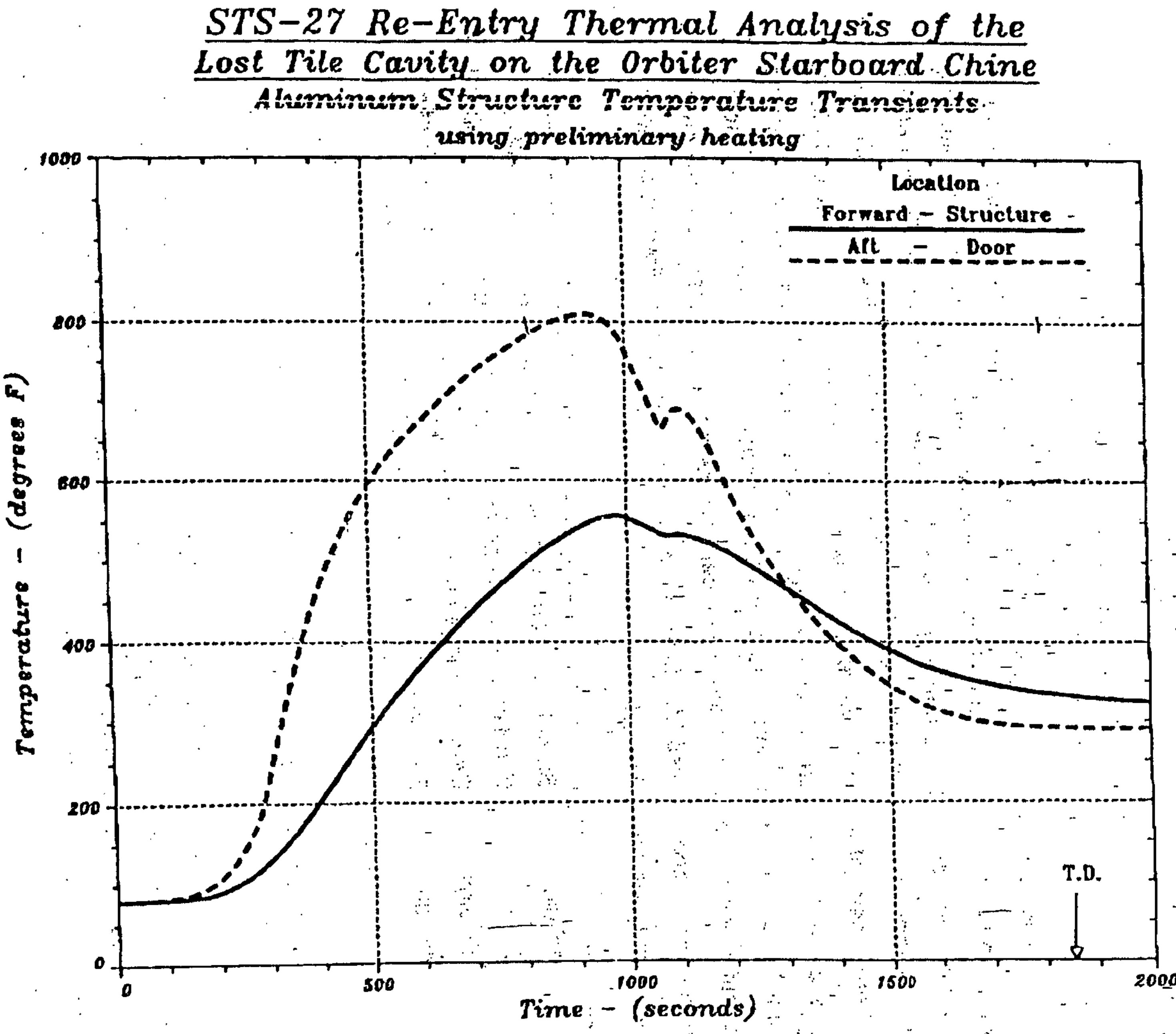


Figure 22: Re-entry thermal analysis of lost tile cavity

Source: R. Maria, NASA JSC (1988)

FEB 05 '03 13:20 2023583007 PAGE.20

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

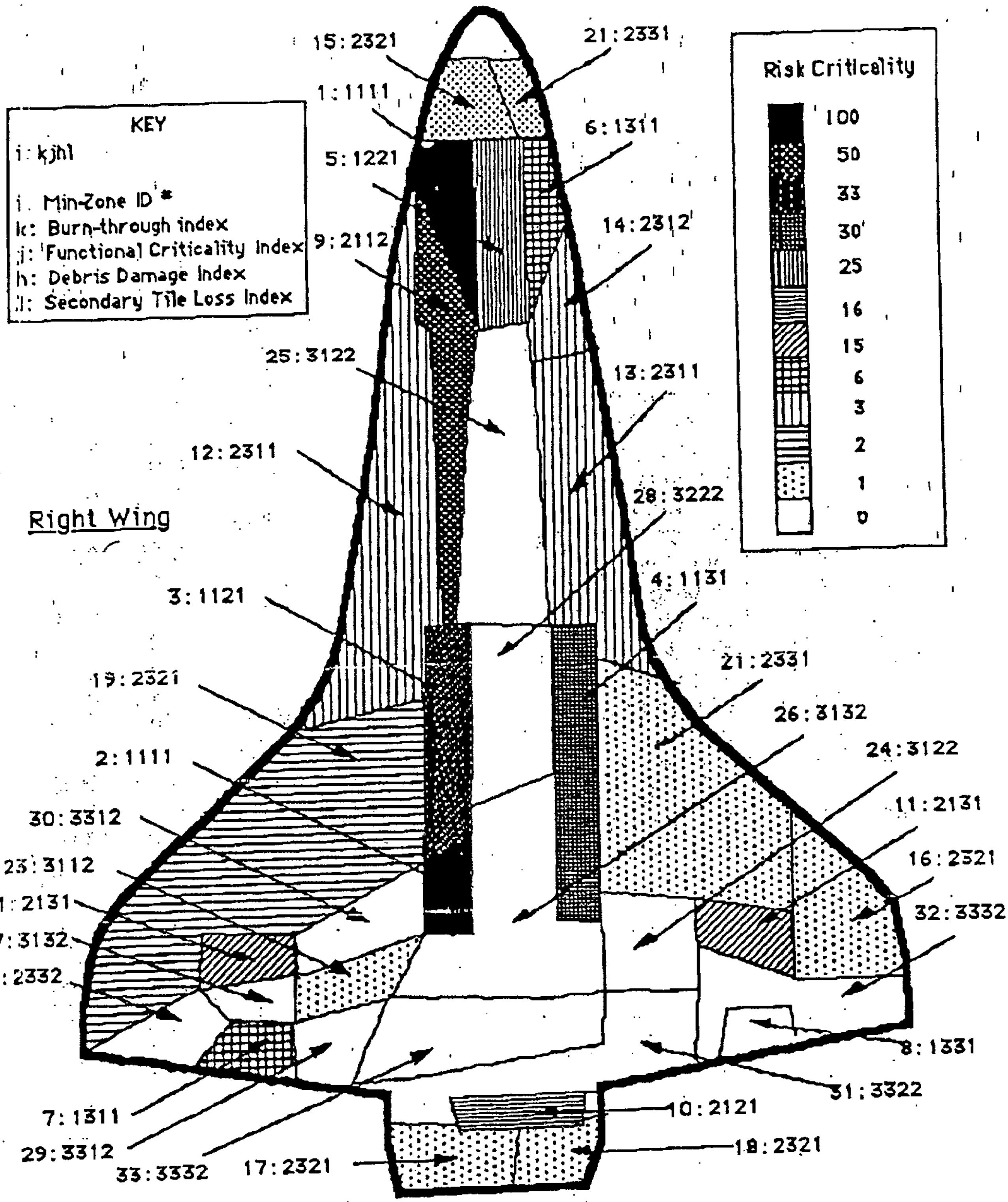


Figure 23: Partition of the orbiter's surface into 33 min-zones (index: i)

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

FEB 05 '03 13:22 2023583007 PAGE.24

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

NASA ODIN Program Fax:2023583007 Feb 5 2003 14:08 P.24

FEB 05 '03 13:22 2023583007 PAGE.25

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	0.870	55.770	4	1.870	24.000
2	0.870	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	0.185	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

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}).

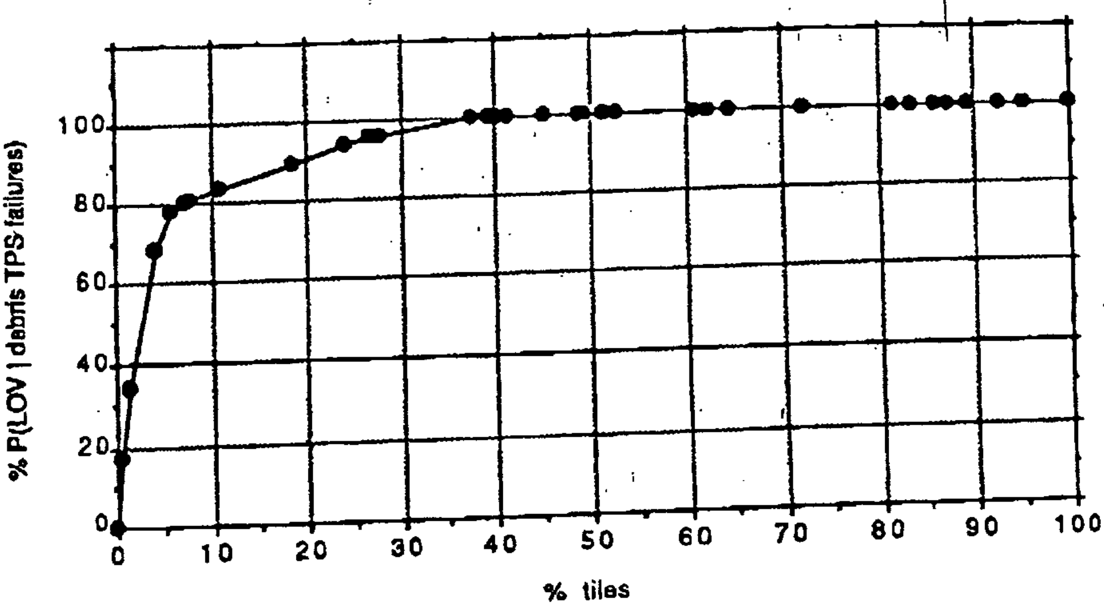


Figure 24: Relative risk of LOV due to debris-initiated TPS damage

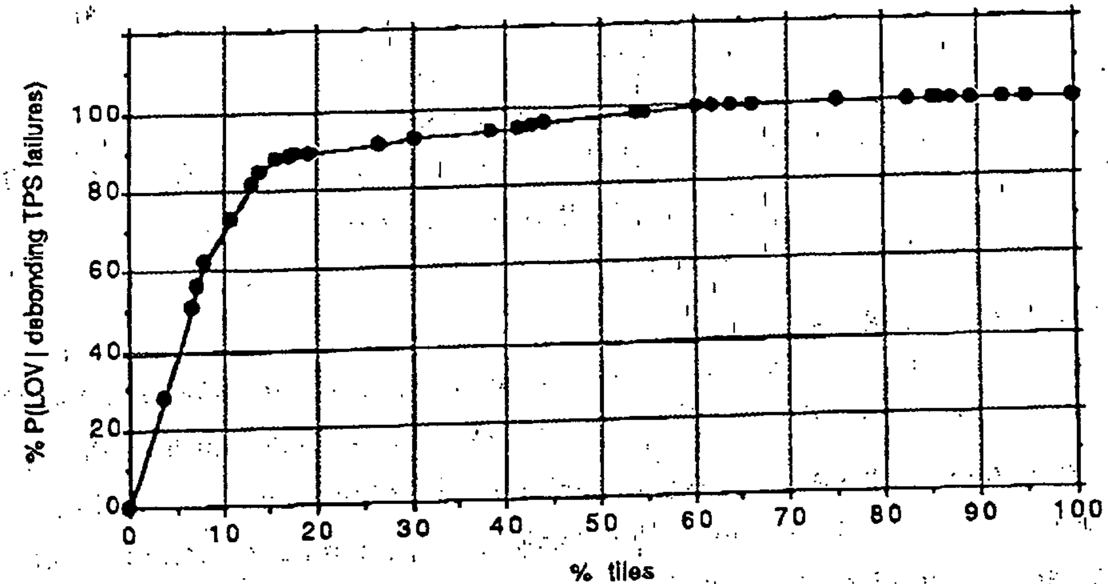


Figure 25: Relative risk of LOV due to debonding-type TPS damage

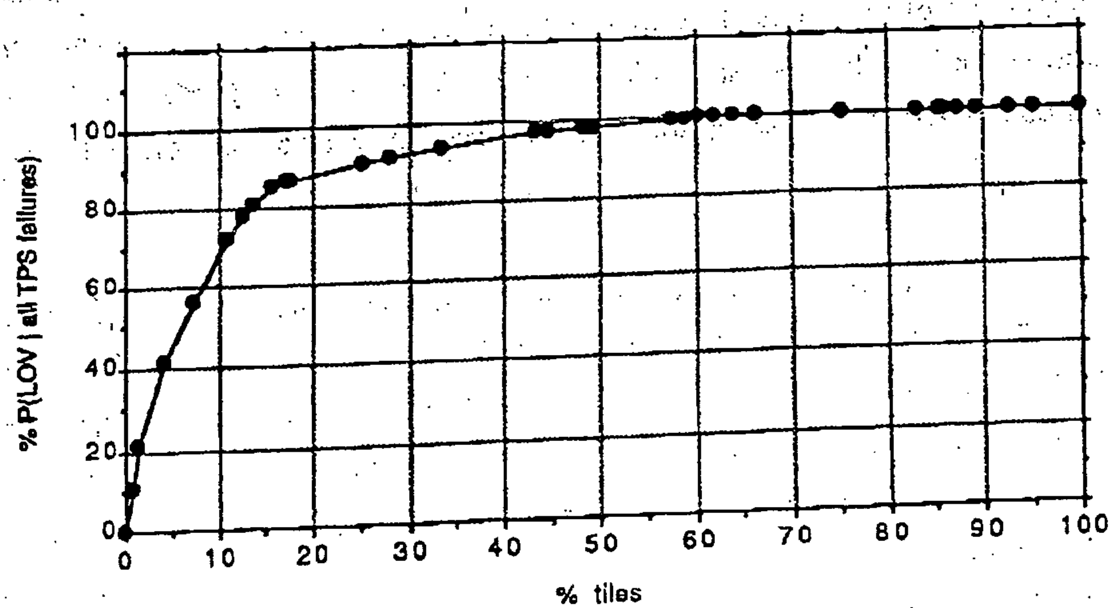


Figure 26: Relative risk of LOV due to both types of TPS damage

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

FEB 05 '03 13:23 2023583007 PAGE.30

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

NASA ODIN Program Fax:2023583007 Feb 5 2003 14:10 P.30

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

FEB 05 '03 13:24 2023583007 PAGE.33

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 the 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.

FEB 05 '03 13:25 2023583007 PAGE.36

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

NASA OUTR Program Fax:2023583007 Feb 5 2003 14:12 P.36

FEB 05 '03 13:25 2023583007 PAGE.37

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 R. 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.

Section 8:

APPENDICES

Appendix 1

Organizational Extensions of PRA models and NASA Application

Nuclear

GPU Nuclear Corporation
One Upper Pond Road
Parsippany, New Jersey 07054
201-316-7000
TELEX 136-482
Writer's Direct Dial Number:

May 18, 1990

Prof. Elizabeth Paté-Cornell
Department of Industrial Engineering
Stanford University
Stanford, CA 94305

Dear Professor Paté-Cornell:

On behalf of the American Nuclear Society Nuclear Reactor Safety Division, I am pleased to inform you that your paper, "Organizational Extension of PRA Models and NASA Application" (which was presented at the PSA '89 Conference in Pittsburgh, Pennsylvania), has been selected for a Best Paper Award. This award was determined on the basis of an evaluation by the Technical Program Committee members for the PSA '89 Conference.

As I mentioned to you on the phone, arrangements are being made to recognize you at the NRSD Annual Luncheon on Wednesday, June 13, 1990 in Nashville, Tennessee (in conjunction with the ANS annual meeting). At that time you will be presented with a certificate. The luncheon will begin at 11:30 a.m., you will be seated at the head table, and your luncheon ticket will be complimentary.

Congratulations again on receiving a Best Paper Award.

Yours truly,

Donald N. Grace

Donald N. Grace
Chairman, Honors & Awards Committee, NRSD

cc: Dr. Raymond DiSalvo

Proceedings of PSA '89
Pittsburgh, Pennsylvania
April 1989

Best Paper Award
American Nuclear Society
Nuclear Reactor Safety Division
PSA '89

ORGANIZATIONAL EXTENSION OF PRA MODELS AND NASA APPLICATION

Elisabeth Paté-Cornell
Department of Industrial Engineering
and Engineering Management
Stanford University
(415) 723-3823

ABSTRACT

This paper describes a probabilistic method which extends classical PRA to include some characteristics of the organization that processes or manages an engineering system. A taxonomy of errors is presented and their organizational roots are examined. An assembly model is proposed for the analysis of the resulting spectrum of capacities of the system. The management of the Thermal Protection System of the Space Shuttle is used as an illustration. : The model allows assessment of the benefits of organizational improvements of the orbiter's processing.

PROCESS ANALYSIS IN RELIABILITY MODELS

The quantitative analysis of the reliability of an engineering system such as a nuclear power plant or the space shuttle allows identification of its different failure modes and computation of their probabilities. Therefore, it permits a decision maker to choose technical solutions that maximize an objective function (including reliability) under resource constraints. This means, for instance, the choice of design characteristics that minimize the probability of failure during the lifetime of the system under constraints of costs, time, and performance.

Technical modifications, however, represent only one class of risk management strategies. When a system's failure is studied *a posteriori*, it is often pointed out that what resulted in a technical failure was actually rooted in a structural or functional failure of the organization. This was the case, for example, of the accident of the space shuttle Challenger where a number of organizational factors contributed to NASA's decision to launch under unacceptable temperature conditions.[1] These organizational factors include, for example, geographic dispersion (thus, sometimes, poor communications), time constraints, and pressures of public relations. Modifications and improvements of the organization itself may address some of the reliability problems at a more fundamental level than strengthening the engineering design alone.[2] Such modifications include, for example, improving communications, setting effective warning systems, and ensuring consistency of standards across the organization.[3]

The object of this paper is to discuss a quantitative approach to the analysis of the effects of organizational features on system reliability. The principle is to compute the probability of occurrence of the basic events in greater depth than it is generally done in classical PRA by linking this probability to the industrial process itself.[4] The method involves explicit assessment of the effect of managerial procedures on the probability of technical failures and, therefore, allows extension of the value of information of conventional PRA. By assessing explicitly the reliability benefits of organizational improvements along with technical ones, the results allow setting priorities among safety measures that go beyond technical modifications alone.

The National Aeronautics and Space Administration (NASA) presents some organizational features that influence its mode of operations and thus the reliability of its space systems. NASA is a high-visibility organization, uncertain about its future funding and, therefore, dependent on public relations. It is also fragmented in two ways: geographically among space centers, and operationally among space programs. In the early 1960's, NASA decided against probabilistic risk analysis, thus avoiding the issue of "how safe is safe enough" in what is generally recognized as a high-risk operation. Yet, following the Challenger accident in January 1986 and faced with a long list of potential corrections, NASA is beginning to complement its qualitative methods of identification of the failure modes by quantifying probabilities and dependencies as recommended by the Slay Commission.[5] A current objective is clearly to increase the effectiveness of the organization and the efficiency of resource allocation by setting priorities among the technical solutions to existing problems. Yet, as the Rogers Commission pointed out,[1] it is clear that some of NASA's reliability problems cannot be resolved by design modifications alone because their roots are organizational. The fragmentation of the organization, the apparent buffering between engineers and managers and the divergence of their risk perceptions,[6] difficulties of learning given the scarcity of usable trend records, all these factors have contributed to the vulnerability of space systems operations. These effects, however, vary among the different subsystems according to their physical and functional characteristics and to the features of the managing organizations.

The Thermal Protection System (TPS) of the space shuttle provides an example of the coupling between technical and organizational problems. It is a complex system that is designed, manufactured, processed, and maintained by several organizations. It is made of black and white tiles (about 24,000 on the orbiter Discovery), reinforced carbon-carbon in the hottest zones, thermal blankets in colder zones, and flexible insulation. The tiles themselves are attached by a special bond (RTV) to a flexible pad designed to absorb the bending of the orbiter's surface. The pads are bonded to the aluminum skin (itself covered with a primer) by the same RTV. The TPS can fail in three ways: debonding, burn-through, and damage by impacts. It is subjected to a set of external loads, some of them mostly predictable (like vibrations and heat under normal operating conditions), some of them more random like debris. Important features of the PRA model for the tiles are the potential failure dependencies from tile to tile, and the coupling between failure of the TPS and failure of the subsystems located directly under the aluminum skin of the orbiter.

The management of the TPS presents many characteristics that are typical of the linkage between organizations and reliability. It involves several organizations and contractors in different places (including Rockwell, Lockheed, and NASA, at Kennedy Space Center and at Johnson Space Center) and procedures that were mostly developed for the initial shuttle construction and not for a long term maintenance program. The TPS inspection and maintenance procedures are extremely labor intensive and time consuming, and are often on the critical path to the next launch. The training, dedication and motivation of the personnel involved in this process is critical to the reliability of the system. The current procedure relies mostly on maintenance on demand. Although destructive pull tests are performed for a small sample of tiles, in most places, the problems posed by the aging of the bonding are not addressed directly. The recording of operations involves a mass of paper documents. Furthermore, the procedure involves some prioritization among the TPS elements based on qualitative judgments, but no systematic priorities based on a quantitative assessment of the risks of failure due to tiles' location with respect to other critical systems.

A new method to automatize the inspection of the tiles is currently being implemented.[7] An important aspect of this method is that it greatly simplifies the current tasks of observing, communicating, storing, and retrieving information concerning the current state of the tiles and their past performance. It should, therefore, increase the reliability of the inspection and maintenance operations. By accelerating the process, automation may also, in many instances, take the tiles off the critical path to the next launch. The gain in shuttle reliability between manual inspection and automation is a function (1) of the initial contribution of the TPS to the overall failure risk and (2) of the gains made in TPS reliability. One specific issue that can be addressed by the extension of PRA described here is the benefit of accounting for the relative criticality of the tiles in different locations on the orbiter's surface in the management of the TPS. This may result in increasing maintenance efforts in key areas such as the surface covering the hydraulic command system, but also, perhaps, special monitoring of the installation operations for these most critical areas. Another issue that can be addressed by extension of PRA as described here is the relative importance of the management of the TPS itself and of the management of other systems that are sources of debris (e.g., the external tank insulation) in the overall reliability of the thermal protection function.

INTEGRATION MODEL

Probabilistic risk analysis (PRA) for engineering systems allows identification of their weakest parts through quantification of the probabilities of the different failure modes (see, for example, Henley and Kumamoto).[8] Extension of the PRA model permits more explicit consideration of major organizational characteristics[9] (structure, procedures, and culture[10]) that affect the reliability of operations, specially in situations of distributed decision making.[11] The method extends the scope of PRA through a Bayesian analysis of the sequence of tasks to be performed in the process of design, manufacturing, inspection, maintenance, and operations, and the computation of the probabilities of technical as well as organizational failures that can affect the system's reliability. The reasoning involves analysis and extension of errors to include not only the classical operators errors but also errors that are due to the procedures and structure of the organization. An essential distinction is made here between gross errors and errors of judgment because remedial actions to address these two types of problems may be of different nature.[12]

The first phase is an analysis of the process[13] (e.g., engineering, maintenance, and operation) in order to identify what constitutes "normal performance" and potential problems with their probabilities or base rates per time unit or per operation, which depend, among other factors, on the organization's culture and incentive structure. Given that a basic error occurs, the next phase is an analysis of the organizational procedures and incentive system to determine the probability that it is observed, recognized, communicated, and corrected in time (i.e., before it causes a system failure). The results of these two phases is a computation of the probabilities of the different system's states corresponding to possible types of structural defects and, therefore, to different levels of system's capacity. The third phase is a probabilistic risk analysis of the physical system that allows computation of the overall failure probability (1) under normal circumstances, and (2) given potential weaknesses of the different elements and increase of their failure probabilities. These three models (process, organization, and PRA for different levels of system's capacity) are integrated using an event tree (or an influence diagram) to compute the overall failure probability and the relative contribution of different scenarios (e.g., occurrence and correction of a given problem). Figure 1 provides a schematic illustration of the structure of this integration model.

PRA FOR THE THERMAL PROTECTION SYSTEM OF THE SPACE SHUTTLE: MODEL STRUCTURE

A PRA model currently under study for the TPS of the space shuttle relies on a partition of the surface along several dimensions: (1) the external loads (mainly heat and debris) to which the orbiter can be subjected and that vary according to the location on the orbiter's surface and (2) the criticality of the different subsystems located immediately under the aluminum skin. In order to allow recommendations regarding the management of the relevant subsystems, the model is divided into two parts: the first part is a study of debonding and burn-through due to weaknesses of the bond, heat loads, vibrations, etc.; the second part is a separate study of the impact of debris, their sources, and their effects on the TPS reliability. In this paper, the scope of the PRA model is limited to the tiles located on the underneath surface of the orbiter.

First part: debonding and burn-through (excluding the effect of debris)

Figure 2 provides a schematic illustration of the partition of the orbiter's underneath surface for the first part of the analysis (there is no attempt at this stage to locate realistically the different zones according to temperature and criticality). A minimal zone (or min. zone) is an element of the final partition of the surface. Each min. zone of index i is thus characterized by a heat index (k(i)) and a criticality index (j(i)).

The basic notations are the following:

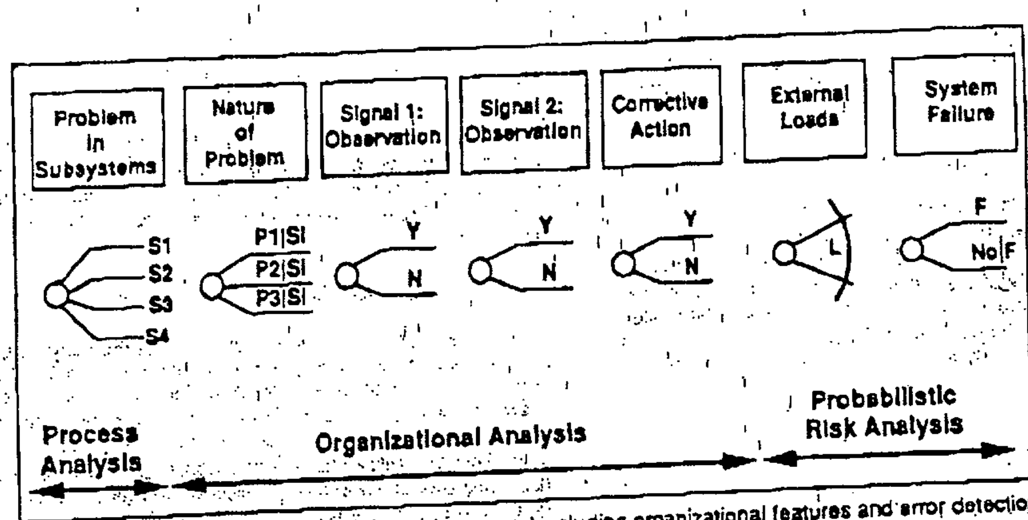


Figure 1: Structure of the generalized reliability model including organizational features and error detection

$F(t)$:	Failure of the orbiter: loss of vehicle and crew (LOV/C) at launch t primarily caused by failure of the TPS
n:	Total number of tiles on the orbiter
j:	Index of criticality area (ex: criticality of the min. zones covering the hydraulic system)
k:	Index of temperature area
i:	Index of min. zones (j, k) => j(i); k(i)
N_i:	Number of failure patches in min. zone i.
n_i:	Number of tiles in min. zone i.
$F1$:	Failure of the "first tile" (initiating failure) in a failure patch
$F'\|F1$:	Failure of any adjacent tile given initiating failure

<u>Initiation of a failure patch:</u>

It is assumed in this phase of the analysis that any failure patch (of size one or more) develops by the loss of a first tile (F1: initiating failure for the patch), followed or not by the failure of adjacent tiles (F'|F1). The probability of losing the first tile in a patch depends on the failure mode (debonding or burn-through):

$$p_i(F1) = p(F1, \text{debonding}) + p_{s|i}(F1, \text{burn-through})$$

The probability of debonding is assumed to be independent of i (the location on the orbiter) whereas the second term (burn-through) depends on the temperature component of the min.zone descriptor k(i).

<u>Development of a failure patch of size M given that it starts in min. zone i:</u>

$$p_i(M \mid F1) = p_{s|i}(F' \mid F1)^{M-1} \times [1 - p_{s|i}(F' \mid F1)]$$

This probability depends on the temperature of the min. zone (index k(i)).

<u>Development of Ni patches in min. zone i:</u>

$$p(N_i) = p(F1)^{N_i} \times [1 - p_{s|i}(F1)]^{n_i - N_i}$$

This equation assumes that the development of different patches are independent events and that there is no overlap of patches, i.e., that the product $EV(N_i) \times EV(M)$ is negligible.

$$EV(N_i) \sim n_i \times p_{s|i}(F1)$$ (= expected value of the number of patches in min. zone i)

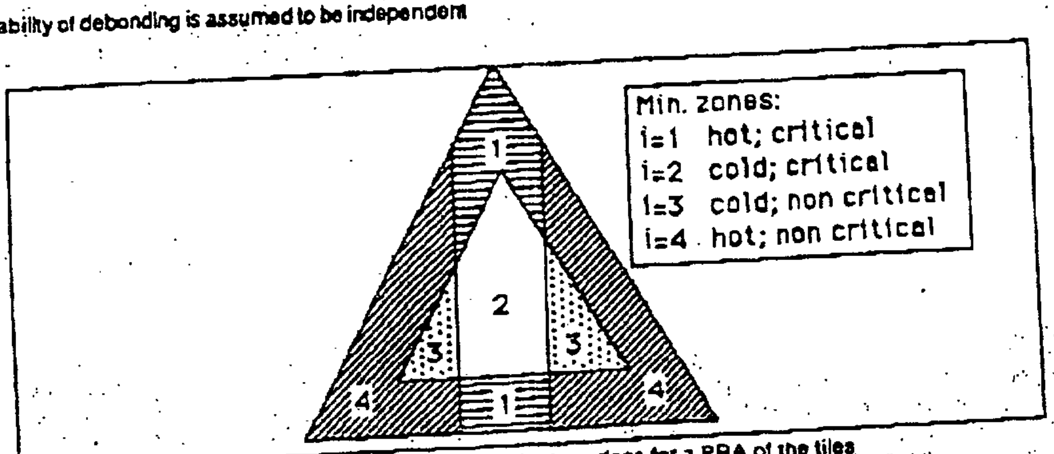


Figure 2: Double partition of the orbiter's surface for a PRA of the tiles

$$EV(M) = 1/[1-p_{s(i)}(F' \mid F1)]$$ (= expected value of the size of a patch conditional on its start)

Failure of the orbiter due to a patch of size M:

As part of the data, one needs the probability of failure of the orbiter due to the development of a failure patch of a given size in a zone of given criticality. These data may be obtained through an analysis of the reliability of the systems located under the orbiter surface and their contribution to the overall reliability of the orbiter. These probabilities can be used to define criticality itself. p(F) thus depends on j(i), the criticality index of min. zone i.

$$p_i(F \mid M=1) = p_{j,1}$$
$$p_i(F \mid M=2) = p_{j,2}$$
$$p_i(F \mid M=m) = p_{j,m}$$

Failure of the orbiter due N_i patches of random size:

A failure of the orbiter due to TPS failure in min. zone i occurs if any (one or more) of the patches of min. zone i causes failure. Given that failure probabilities p(F1) and p(F') are assumed to be small, one can write:

$$p(F \mid N_i=q) = q \times p'_i$$

in which p'_i is the probability that an arbitrary patch in zone i causes failure.

$$p'_i = \sum_{m=1 \text{ to } \infty} p_{j(i),m} \times p(\text{size } m)$$

$$p'_i = \sum_{m=1 \text{ to } \infty} p_{j(i),m} \times p_{s(i)}(F' \mid F1)^{m-1} \times [1-p_{s(i)}(F' \mid F1)]$$

Infinity is used as a convenient approximation of upper bounds when the probability of large values of the random variable is sufficiently small.

Probability of orbiter failure due to TPS failure in zone i:

p(F for all patches in min. zone i)

$$= \sum_{q=1 \text{ to } \infty} p(F \mid N_i = q) \times p(N_i = q)$$

$$= \sum_{q=1 \text{ to } \infty} p'_i \times q \times p(N_i = q)$$

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

$$= p'_i \times n_i \times p_{s(i)}(F1)$$

Failure of the orbiter for all the min. zones:

$$p(F) = \sum_{i=1 \text{ to } 4} p'_i \times n_i \times p_{s(i)}(F1)$$

Effect of external events

The probability of failure is the sum over all values of the external load X (e.g., maximum temperature if it turns out to be critical) of the probability density function for X multiplied by the probability of failure of the orbiter conditional on X.

$$p(F) = \int_x f_x(x)\; p(F \mid x)\, dx$$

In the complete analysis of the external events, it is necessary to take into account the different phases of the flight in order to obtain a distribution over time of loss of first tile and a measure of the dependence on time of the loss of subsequent tiles after loss of the first one.

Second phase: risk of failure due to debris

The analysis begins with the study of the sources of debris (e.g., insulation of the external tank, other parts of the STS, external objects) in order to obtain the probability of different scenarios characterized by the nature and the size of debris, the impact's location on the orbiter's surface, and the time of impact during the flight. This analysis leads to a description of the initial tile damage (including probability of a hit for tiles in different zones, distribution of number of tiles initially hit conditional on debris impact, severity of the damage conditional on impact). In this second part, the start of a failure patch is characterized by the possibility of multiple initial failures with different levels of severity. The study of further development of failure patches conditional on initiating failure(s) and consequent effect on the orbiter is similar to the analysis performed in the first part. The main difference is that the analysis of the effects of debris involves different levels of damage severity.

MANAGEMENT OF THE TILES AND POTENTIAL ERRORS

TPS management and reliability

The quality of the process of design, manufacturing, installation, inspection, and maintenance of the tiles affects the probability of initial and subsequent failures through burn-through or debonding (p(F1) and p(F'|F1) in the previous model). The quality of the management of other systems such as the external tank that are potential sources of debris affects the probability and the severity of damage due to debris impact in different locations of the orbiter. Given its structure, the model described above can be used to assess the gains of improvements in the management of the tiles and in the processing of the orbiter through the assessment of the changes in p(F1), p(F'), and similar variables for the case of debris impact.

For example, current maintenance of the tiles depends on the expected heat loads (with emphasis on zones such as the leading edges of wheel doors) the procedure is independent of the criticality of the systems located directly under the aluminum skin. Prioritization in the TPS processing as well as the processing of adjacent sources of debris may be designed to decrease further the probability of initiating tile failures in the most critical zones. The results can then be measured by computation of the overall risk by the previous model using new values of initiating failures. Another example of improvement that can be assessed through the model is the development and the use of non destructive testing of the RTV. The probabilities of failure p(F1) and p(F') in the first part of the model increase over time with the number of flights of the orbiter. Non destructive testing can indicate deterioration of the bonding and allow timely replacement.

In addition to conscious decisions such as ignoring the aging phenomenon or uniform inspection of the tiles, errors can occur at every step of the manufacturing of the different elements of the TPS (for example, a bad batch of RTV), of the inspection and maintenance process (e.g., wrong measurement of step and gap).

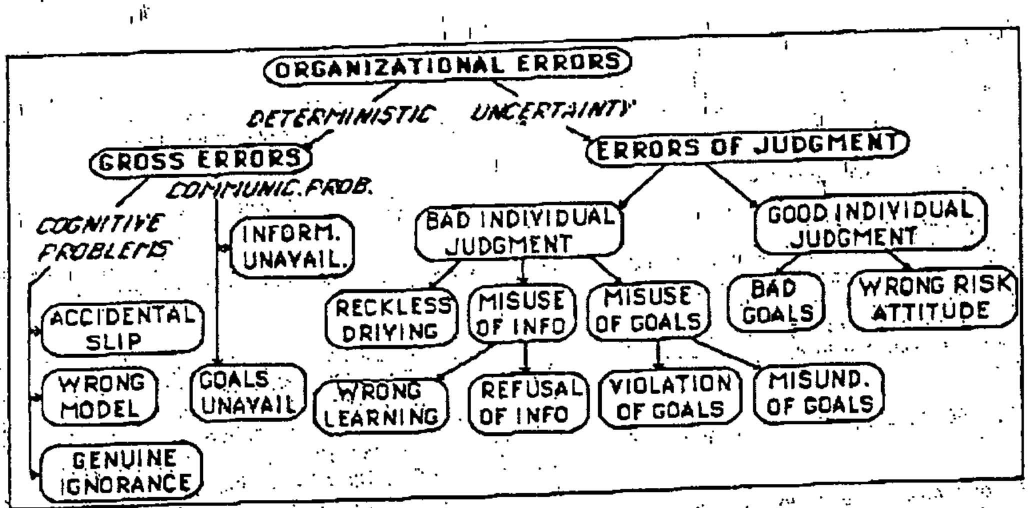


Figure 3: A taxonomy of errors in organizations

or operations (e.g., damage of the tiles during the pre-launch processing of the orbiter). In order to assess the effectiveness of organizational measures, it is necessary to relate errors to their organizational roots.

Organizational roots of errors: a general framework of analysis

Errors can result either from plain mistakes on the part of individuals, or from an inadequacy between the organization's characteristics (structure and procedures) and its expectations about human and system performances. Two major sources of mismatch between the individual and the group may be (1) the inability of the organization to make relevant information available in time to the decision makers at appropriate hierarchical levels, and (2) an incompatibility of goals and preferences between different levels of management and specific actors. The distinction between information and preferences is important because it leads to different types of remedial actions. In the first case, the problem is a cognitive one, calling for an improvement of knowledge, individual learning, and access to information. In the second case, the problem may be one of compatibility of goals, standards, and preferences. The question can then be addressed by modifying the incentive structure as well as the mechanisms by which rules and constraints are set and modified. Appropriate change of rules is a direct result of the ability of the organization (as opposed to the individual) to learn with experience.

A taxonomy of errors that can be useful in this analysis assumes a hierarchical organization in which rules, goals, and constraints ("goals" in Figure 3) are communicated by headquarters or appropriate top management down the hierarchy. This analysis focuses on actions that may lead to failure (false positives), but not on the rejection of good options (false negatives) that may result, for example, from excessive conservativeness. The proposed taxonomy relies on a distinction between gross errors based on lack of knowledge or accidental slips, and errors of judgment (see Figure 3). Gross errors are defined as errors about which everyone would agree (including the person or the group who made the mistake) and the decision would be reversed if it were reexamined. Errors of judgment occur in situations of uncertainty and involve either an interpretation of the existing evidence[14] or a value judgment concerning risk taking about which a consensus may not exist. They are defined here as decisions that could be reversed if the organization were made aware of them, for example, because the initial decision involves misinterpretation of relevant (but imperfect) information and/or because it implies a risk attitude that does not correspond to the objectives of top management. In addition, errors of judgment also include judgments and decisions by top management itself if they are incompatible with the values generally held by society at large.

A more detailed study of this taxonomy and its implications is presented elsewhere.[15] The distinction between gross errors and errors of judgment is essential because it determines the nature of the remedial actions that can be considered. Gross errors can be attributed either to cognitive problems or to miscommunication. Cognitive errors are caused mostly by information problems for which corrective actions include adequate information systems, better training, incentives to seek information when needed (and, in particular, sufficient time and resources to do so), and a thorough checking mechanism capable of observing errors in time. The organizational structure must include appropriate channels of information and functions of supervision and support. The organizational procedures must provide appropriate training and incentives not only to decision makers but also to supervisors in order to ensure that checking and quality control actually occur. A key question, for example, is how the system rewards or punishes the disclosure of problems.

Errors of judgment in the face of uncertainty are open to interpretation for two categories of reasons: uncertainty about facts and diversity of preferences. Contrary to gross errors, they cannot be easily defined by a violation of a deterministic truth such as two plus two equals four. Assessment of a probability or a probability distribution to describe, for example, epistemic uncertainties (fundamental lack of knowledge) about a variable generally requires a subjective input to interpret the evidence. As for risk attitudes and preferences in the face of trade-offs, these inputs obviously vary among individuals. Organizational problems that stem from bad judgment are, therefore, much more difficult to identify than gross errors because their detection must rely on a more precise definition of what constitutes a good decision. In retrospect, it is always easy to decide that a bad judgment is one that lead to an accident. Yet, good decisions can lead to bad outcomes. Therefore, appropriate decision processes must exist so as to balance in a satisfactory manner unknown costs and benefits involved in trade-offs such as immediate performance versus safety of operations.

In cases where there is no controversy about value judgments involved in top level decisions (considering, for example, that the opinions of Congress must prevail) the question is to ensure that relevant information is available to this top management when fundamental decisions are made, and that the organizational and individual's risk attitudes eventually reflect that of this top level. The objective is to design an incentive structure and/or a feedback mechanism that ensures this adequacy. This implies the use of appropriate information that is readily available, the acquisition of additional information when it has a net positive value given the organization's preference system, and a decision making process that leads to consistency in risk attitudes. The quality of the leadership clearly plays an essential part in the clarity and the consistency of standards across the organization.

SOME ORGANIZATIONAL PROBLEMS THAT AFFECT SYSTEM RELIABILITY

From this analysis of errors one can identify two broad categories of organizational problems that relate to the failure probability of a system because they affect the probability of process errors: *information* problems and *incentive* problems with the possibility of combination of both.

Information problems

Information problems may occur within an organization or across organizations managing the same system. They may include the following:

• Sequential engineering and lack of feedback. The engineering process may be designed in a linear manner without feedback loops to check that the design corresponds to the needs, or that resources at allocated properly for optimal reliability. For example, there may not exist any mechanism to check the shadow price of the constraints set by management, i.e., what would be the gains (e.g., in reliability) associated to different levels of relaxation of the constraints (e.g., of schedule).

• Access to relevant information. The organization's problem is to identify and communicate signals that are relevant and reliable. Organizational filters may be such that some important signals end up missing while irrelevant ones overload and confuse the system. First, the individual must be able to identify what to look for and to obtain this information in time. Communications may fail for a variety of reasons. Appropriate communication channels may simply not exist, or existing channels may not work due to accident, or impractical procedures, or deliberate retention of information. Also, the signal may be ignored because of previous false alerts (the cry-wolf effect).

• Communication of uncertainties. The information may also be distorted. For example, the organization may not be equipped (in its procedures, its culture, etc.) to communicate properly imperfect information and uncertainty. Therefore, qualifiers ("Go but...") may be dropped in the process.

Incentive problems

Incentive problems may affect the system's performance throughout the process and include the following:*

• Incentives towards optimism. In organizations whose final goal is to produce a positive product (as opposed to detecting faults) and where the risks of visible failures are sufficiently low, incentives at each level may lead to the suppression of bad news and, therefore, a bias towards optimism. This is true, in particular, when the information is incomplete and in situations of uncertainty (as described above).

• Pressures on the critical path. The technical groups whose task is on the critical path to production or operation may find themselves under pressure to cut corner. This pressure increases with the difference of total time (objective function) between them and the next critical task.

• Difficulties of learning in a high-visibility situation. It may be difficult for an organization subjected to public scrutiny to assess its own performance and learn from its mistakes. In situations of success, there may be a tendency to overlook signals of potential problems whereas in situations of difficulties, the organization may be overwhelmed by signals of problems if it does not have clear procedures to assess their relative severities and to set priorities among remedial actions. Furthermore, organizational learning and in particular change of rules may be difficult when it can be interpreted as admitting that previous procedures were inadequate.

RETURN TO THE PRA MODEL

Assembly model

The probability of failure p(F1) and of subsequent failures p(F'|F1) can be linked to the occurrence of errors of different types (e.g., a fraction of the surface only was covered with RTV) and, furthermore, to combinations of errors (e.g., insufficient quantity of bonding or inappropriate step to next tile due to mis-measurement). For each type of error, the question is to know what is its level of severity, the number of tiles that it can affect, and their location with respect to the criticality partition of the orbiter surface. In addition, it may be important to consider whether it is a gross error or an error of judgment that may be less easily identified and corrected. An error having occurred, the inspection process can be analyzed as a sequence of filters: at each step the error may be identified or missed. Finally, given that an error has occurred and been identified, it may or may not be corrected.

This analysis is described by the influence diagram shown in Figure 4. The result is a distribution for the probability of initiating failure p(F1) given possible combinations of errors and their levels of severity and the distribution of the number of tiles affected. This distribution of values of p(F1) is then entered in the previous model to obtain a spectrum of failure probabilities (LOV/C) due to failure of the TPS. The model can then be used to assess the effects of organizational improvements designed to increase the reliability of the TPS.

Examples of organizational improvements of TPS management and their analysis through the model

• Improvement in learning. Possible measures include trend analysis and feedback mechanisms. Their effect, in the model, is to decrease the probability of occurrence of errors in the first place. Also, improvement of the testing (such as the testing of RTV for aging effects) whose effect is to decrease the probability of failure itself.

• A better allocation of resources according to the criticality of the tile location can be analyzed by the model through the

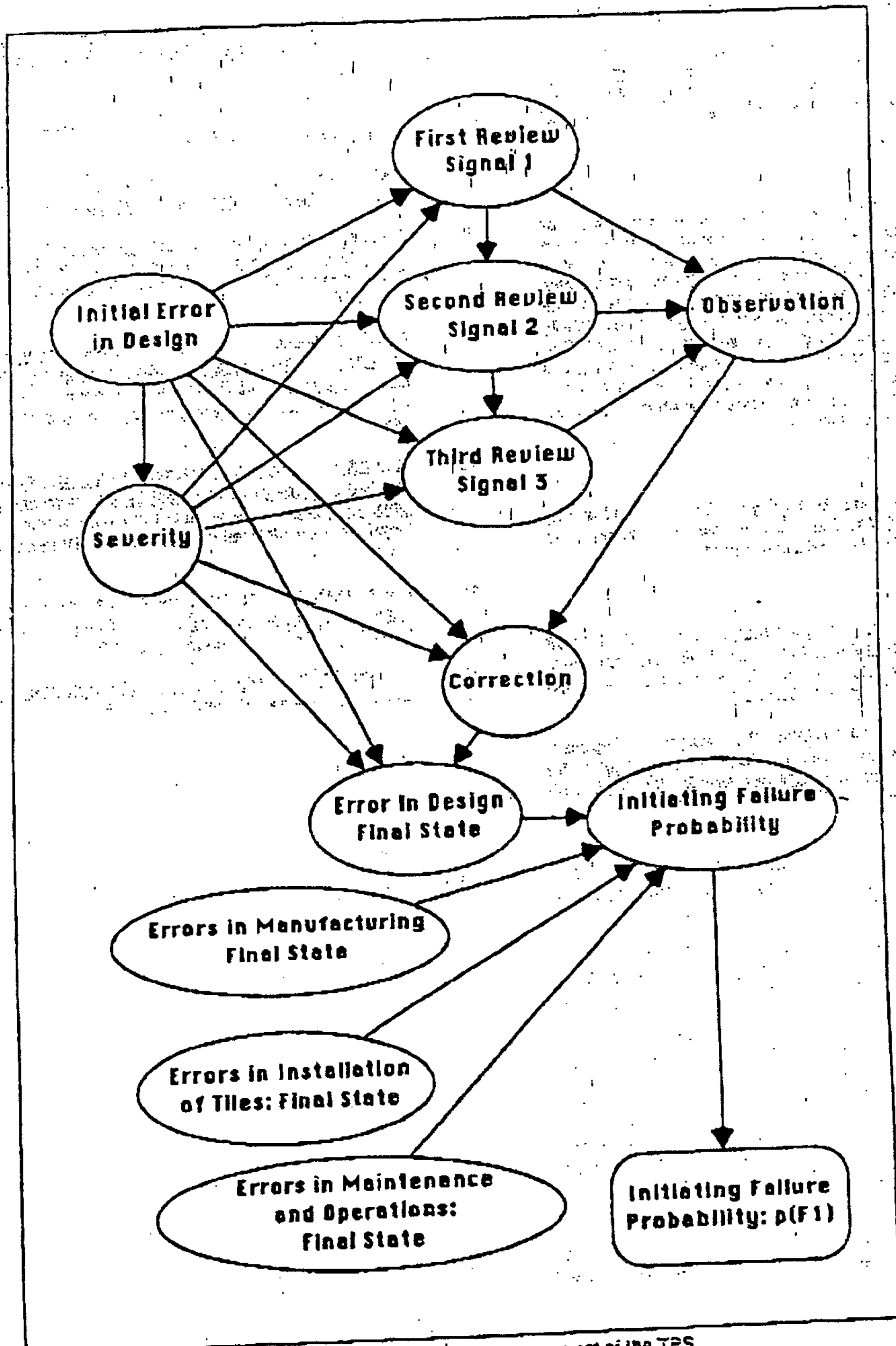


Figure 4: Analysis of errors in the management of the TPS
Influence diagram for p(F1)

decrease of the probability of initiating failure in the most critical zones.

• Better procedures for the inspection of tiles and the storage and retrieval of information increase the probability of observation of error conditional on occurrence and increase the probability of correction conditional on observation.

CONCLUSION

The extensions of classical PRA presented in this paper increase considerably the value of information of such studies because it allows setting priorities among a larger number of potential improvements. An analysis of the engineering process allows focusing attention and resources (time in particular) on the most critical tasks. Organizational aspects of engineering reliability are of interest to researchers in organizations' behavior.[11] The quantitative method outlined here allows inclusion of this body of knowledge in the decision making process by assessing the relative importance of these organizational effects through their contribution to the overall system reliability.

ACKNOWLEDGEMENT

This work was funded by NSF grant SES-8709810 and by NASA grant NCC 10-0001. The author thanks Dr M. Wiskerchen and Mr P. Fischbeck for their help in this study.

REFERENCES

1. PRESIDENTIAL COMMISSION ON THE SPACE SHUTTLE CHALLENGER ACCIDENT Report of the Presidential Commission on the Space Shuttle Challenger Accident, Washington, D.C.(1986).

2. LEWIN, A. Y. and J. W. MINTON. Determining Organizational Effectiveness: Another Look, and an Agenda for Research, Management Science, Vol. 32, No. 5, pp. 514-538, May, 1986.

3. PATE-CORNELL, M.E. and J. P. SEAWELL, Engineering Reliability: The Organizational Link, Proceedings of the 5th ASCE Specialty Conference on Probabilistic Methods in Civil Engineering, Blacksburg, VA, May, 1988.

4. PATE-CORNELL, M.E. Organizational Factors in Reliability Models, Proceedings of the 1988 Meeting of the Society For Risk Analysis, Washington D. C., November, 1988.

5. NATIONAL RESEARCH COUNCIL, Committee on Shuttle Criticality Review and Hazard Analysis Audit, Post Challenger Evaluation of Space Shuttle Risk Assessment and Management, National Academy Press, January, 1988.

6. FEYNMAN, R. P. Personal Observations on Reliability of Shuttle, Appendix F to the Presidential Commission Report on the Space Shuttle Challenger Accident, 1986.

7. WISKERCHEN, M. J. and C. MOLLAKARIMI, Training/Simulation Environment for Space Shuttle Processing, AIAA Flight Simulation Technology Conference, September, 1988.

8. HENLEY, E.J. and H. KUMAMOTO. Reliability Engineering and Risk Assessment, Prentice Hall Inc., Englewood Cliffs, NJ, 1981.

9. MARCH, J. G. and H. A. SIMON. Organizations, John Wiley & Sons, New York, 1958.

10. WEICK, K.E. Organizational Culture as a Sources of High Reliability, California Management Review, Winter, 1987.

11. FISCHOFF, B. and S. JOHNSON The Possibility of Distributed Decision Making, Workshop on Political-Military Decision Making, The Hoover Institution, Stanford University, 1986.

12. PATE-CORNELL, M. E. and R. BEA. Organizational Aspects of Engineering System Reliability and Application to Offshore Platforms, Department of Industrial Engineering and Engineering Management, Stanford University, 1989.

13. MILLER, S.M. and D. M. STRONG. A Model for Evaluating the Performance of Operational Level Information Handling Activities, Proceedings of the Seventh International Conference on Information Systems, San Diego, CA. Dec. 1986.

14. KAHNEMAN, D., P. SLOVIC, and A. TVERSKY. Judgment under Uncertainty: Heuristics and Biases, Cambridge University Press, Cambridge, U.K., 1982.

15. LA PORTE, T.R., High Reliability Organization Project, University of California Berkeley, 1988.

FEB 05 '03 13:30 2023583007 PAGE.50

Appendix 2:

Data Bases for Tile Performance

PRACA

(PROBLEM REPORTING AND CORRECTIVE ACTION)

PRACA DEFINITION

NSTS 08126C; JUNE 1987; REV. C

5.1 NASA PROGRAM OFFICE IS RESPONSIBLE FOR:

C. PROVIDING NECESSARY RESOURCES TO SUPPORT THE PRACA SYSTEM, INCLUDING THE PRACA DATA SYSTEM, COMMUNICATION SERVICES, AND COMPATIBLE HARDWARE AND SOFTWARE.

E. ASSURING THAT THE DEVELOPMENT OF A PRACA DATA SYSTEM WILL PROVIDE INFORMATION IN A FORMAT WHICH WILL BE SUPPORTIVE OF A TRENDING SYSTEM TO BE USED BY ALL ELEMENTS AS SPECIFIED IN TBD.

5.2 JSC & MSFC ELEMENT PROJECT OFFICES ARE RESPONSIBLE FOR:

B. ASSURING THAT ALL REPORTABLE PROBLEMS, INCLUDING IN-FLIGHT ANOMALIES, ARE IMMEDIATELY REPORTED INTO THE NSTS PRACA DATA SYSTEM.

D. ASSURING THAT THE INFORMATION WITHIN THE PRACA SYSTEM IS IN A FORMAT WHICH IS COMPATIBLE WITH AND SUPPORTS TRENDING ANALYSIS.

NASA Lyndon B. Johnson Space Center FLIGHT CREW OPERATIONS DIRECTORATE	SUBJECT: THERMAL PROTECTION SYSTEM TREND ANALYSIS SURVEY	NAME: CB/E. BAKER CB/B. DUNBAR	
		DATE: MARCH 2, 1988	PAGE: 15

KSC PRACA

DATA BASE

INCLUDES: ALL PR'S, IPR'S (RECENT)
SOME DR'S
FOR TPS -- TILES, T/B'S, FIB, TCS, SOME GAP FILLERS

DOESN'T INCLUDE: VEHICLE CONFIGURATION
F/B, GAP FILLER (IF NO PN)
SIP (PR WRITTEN AGINST TILE ARRAY)
SCREED MAP
CROSS REFERENCE TO CONFIGURATION CHANGES (NEW PN'S)

CAN SORT BY: PR#, PN, SERIAL #, EICN
VEHICLE, FLOW, PART NAME, SYSTEM
FAILURE MODE, FAILURE CAUSE
LOCATION (PRE FEB 86 -- FWD, MID, AFT, LWNG...)
(POST FEB 86 -- MORE SPECIFIC LOCATIONS)

PRE 41-C DATA IS ON TAPES AND IS MORE DIFFICULT TO ACCESS
SOME SUBJECTIVITY IN DATA AND PROBLEM DESCRIPTIONS
NON TECHNICAL OPERATORS ENTER THE DATA

NASA Lyndon B. Johnson Space Center FLIGHT CREW OPERATIONS DIRECTORATE	SUBJECT: THERMAL PROTECTION SYSTEM TREND ANALYSIS SURVEY	NAME: CB/E. BAKER CB/B. DUNBAR	
		DATE: MARCH 2, 1988	PAGE 16

PRACA MALFUNCTION CODES

221 - BOND FAULTY
070 - BROKEN
900 - BURNED OR OVERHEATED
910 - CHIPPED
190 - CRACKED
846 - DELAMINATED
117 - DETERIORATED
230 - DIRTY, CONTAMINATED, OR SATURATED BY FOREIGN MATERIAL
017 - DISCOLORED/STAINED
223 - GAP FILLER DAMAGED
224 - GAP FILLER MISSING
206 - GOUGES
247 - INSTALLED/ASSEMBLED IMPROPERLY
730 - LOOSE
246 - MAINTENANCE INPROPER OR FAULTY
800 - NO DEFECT. COMPONENT REMOVED OR REINSTALLED TO FACILITATE OTHER MAINTENANCE
216 - ROUGHNESS/WAVINESS
215 - SIZE IMPROPER
217 - S/G OUT OF TOLERANCE
219 - THERMAL SURFACE CRACKED
947 - TORN
020 - WORN, CHAFED OR FRAYED
207 - VOIDS
220 - WATERPROOFING FAULTY/MISSING
878 - WEATHER DAMAGE

NASA
Lyndon B. Johnson Space Center
FLIGHT CREW OPERATIONS DIRECTORATE

NAME: CB/E. BAKER
CB/B. DUNBAR

SUBJECT: THERMAL PROTECTION SYSTEM TREND ANALYSIS SURVEY

DATE: MARCH 2, 1988

KSC PRACA

ACCESS /DATA / TRENDING

- TERMINALS AVAILABLE AT NASA CENTERS
- DATA BASE COVERS ALL TPS ELEMENTS
- SOME DATA IS SUSPECT
  - INCOMPLETE
  - SUBJECTIVE
- SKILL IS REQUIRED TO ASK THE RIGHT QUESTION THE RIGHT WAY SO AS TO GET THE INFORMATION YOU WANT IN A USEFUL FORM
  - IF NOT QUERIED PROPERLY MAY MISS DATA
  - MAY GET MORE INFORMATION THAN YOU WANT
- DATA RETRIEVAL MAY BE A MANUAL TASK
- USERS HAVE PRIMARILY BEEN QE, RELIABILITY, LOGISTICS
- LIMITED USE / INPUT BY SUBSYSTEM EXPERTS
- NO FORMAL TRENDING
- VERY LIMITED GRAPHICS CAPABILITY

[illegible]

NASA Lyndon B. Johnson Space Center *FLIGHT CREW OPERATIONS DIRECTORATE*	SUBJECT: THERMAL PROTECTION SYSTEM TREND ANALYSIS SURVEY	NAME: CB/E. BAKER CB/B. DUNBAR
		DATE: MARCH 2, 1988 — PAGE 18

TIPS

(TILE INFORMATION PROCESSING SYSTEM)

NASA Lyndon B. Johnson Space Center *FLIGHT CREW OPERATIONS DIRECTORATE*	SUBJECT: THERMAL PROTECTION SYSTEM TREND ANALYSIS SURVEY	NAME: CB/E. BAKER CB/B. DUNBAR
		DATE: MARCH 2, 1988 — PAGE 19

<u>DATA BASE</u>

INCLUDES: VEHICLE CONFIGURATION (TPS RELEVANT)

- TILE AND SIP, FIB, SCREED, PVT, BV
- DESIGN GAP FILLERS (NEW)
- F/B ANOMALIES (NEW)
- S/G ON ORIGINAL BUILD PLUS ON OCCASION
- ENGINEERING DATA/REQUIREMENTS FOR LAST FLOW OF TILE

PR'S RESULTING IN TILE OR FIB REMOVAL, MR, SHAVED

DOESN'T INCLUDE: TCS, THERMAL BARRIERS
MANY TPS REPAIRS

CAN SORT BY: MULTIPLE FIELDS

INCLUDES INFORMATION BACK TO STS-4

AT THE END OF A FLOW, FLIGHT DAMAGE RECORDS ARE REMOVED FROM ACTIVE DATA BASE

ACTIVE DATA BASE FOR TILE REMOVAL GOES BACK THREE FLIGHTS

EARLIER DATA CAN BE ACCESSED ON REQUEST

TIPS

DATA FORMATS

1. TILE CHARACTERISTICS
2. ENGINEERING REQUIREMENTS
3. TILE LOCATION
4. PART NUMBER REVISIONS
5. CARRIER PLATES
6. INSTALLATION DATA (REMOVAL CODES)
7. BOND VERIFICATION (3)
8. PULSE VELOCITY TEST / SONIC DATA
9. SCREED / HEATSINK
10. TILE STEP / GAP CORNER STEP
11. TILE SIP / FOOTPRINT DATA

MALFUNCTION CODES

1. DENSIFICATION REQUIREMENT
2. FLIGHT DAMAGE (BROKEN, CHIPPED, CRACKED, GOUGE)
3. ENGINEERING EVALUATION
4. ENGINEERING CHANGE (MCR, EO, SAR)
5. CHARRED / DAMAGED FILLER BAR
6. ACCESS
7. BOND VERIFICATION FAILURE
8. GROUND DAMAGE (BROKEN, CHIPPED, CRACKED, GOUGE)
9. LOST IN FLIGHT

TIPS

MALFUNCTION CODES CONT'D

A. ENVIRONMENTAL DAMAGE (WIND, HAIL, LIGHTNING, RAIN)
B. REMOVED IN ERROR
C. HEAT DAMAGE (MELT)
D. SIP DAMAGE / PROBLEMS
E. STEP AND GAP OT (OUT OF TOLERANCE)
F. TILE EROSION (THRUSTERS)
G. FLUID CONTAMINATION (SPILLS OR LEAKS)
H. LOOSE TILE
I. TRANSFER SCRAP (FERRY FLIGHT INSTALLATION ONLY)
J. LOST DURING FERRY FLIGHT
K. TRANSFER DAMAGE (FROM PALMDALE)
L. MISCELLANEOUS
M. N / APPLICABLE TRANSFER FROM PALMDALE
N. NOT BUILT TO DRAWING
O. SONIC FAILURE
P. MISLOCATED BOND
Q. TRANSFER DAMAGE (FROM KSC)
R. RTV PROBLEMS
S. SILTS RELATED
T. SCREED PROBLEMS
U. TILE "A" MOD
V. CANNIBALIZATION
W. IMPROPER PROCESSING
X. GAP FILLER

NASA
Lyndon B. Johnson Space Center
FLIGHT CREW OPERATIONS DIRECTORATE

SUBJECT:	NAME:	
THERMAL PROTECTION SYSTEM TREND ANALYSIS SURVEY	CB/E. BAKER CB/B. DUNBAR	
	DATE: MARCH 2, 1988	PAGE 22

TIPS

ACCESS / DATA / TRENDING

- TERMINALS AVAILABLE AT DOWNEY, KSC, JSC
- DATA ENTERED BY VERY KNOWLEDGEABLE TPS OPERATORS
- DATA BASE NOT "CONTROLLED"
- WIDESPREAD USE BY TPS COMMUNITY
- NO FORMAL TRENDING
- GRAPHICS CAPABILITY IS AVAILABLE

PCASS

(PROGRAM COMPLIANCE ASSURANCE AND STATUS SYSTEM)

SYSTEM INTEGRITY ASSURANCE PROGRAM PLAN

NSTS 07700, VOL XI

APRIL 8, 1987

1.6 PROGRAM DESCRIPTION. THE SIAP ENCOMPASSES THOSE ACTIVITIES / FUNCTIONS REQUIRED TO PROVIDE COMPREHENSIVE CONFIGURATION AND MAINTENANCE PROGRAMS, CLOSED LOOP ACCOUNTING, TREND ANALYSIS AND MANAGEMENT INFORMATION.

1.7.1 THE DEPUTY DIRECTOR, NSTS PROGRAM IS RESPONSIBLE FOR MANAGING THE SIAP...

THE NSTS ENGINEERING INTEGRATION OFFICE IS THE OFFICE OF PRIMARY RESPONSIBILITY...

1.7.2 THE NSTS ELEMENT PROJECT MANAGERS ARE RESPONSIBLE FOR IMPLEMENTATION OF ELEMENT PROJECT ACTIVITIES IN SUPPORT OF THE SIAP. THIS INCLUDES BUT IS NOT LIMITED TO THE FOLLOWING:

G. DEVELOP AND CONDUCT RELIABILITY, PERFORMANCE, AND SUPPORTABILITY TREND ANALYSIS FOR FLIGHT AND CRITICAL GROUND SYSTEMS.