A Dynamic Risk Model for Evaluation of Space Shuttle Abort Scenarios

Source of Acquisition
NASA Johnson Space Center

E.M. Henderson
National Aerospace and Space Administration (NASA), Lyndon B. Johnson Space Center, Houston TX, United States

G. Maggio, H.A. Elrada, S.J. Yazdpour
Science Applications International Corporation, New York, NY, United States

ABSTRACT: The Space Shuttle is an advanced manned launch system with a respectable history of service and a demonstrated level of safety. Recent studies have shown that the Space Shuttle has a relatively low probability of having a failure that is instantaneously catastrophic during nominal flight as compared with many US and international launch systems. However, since the Space Shuttle is a manned system, a number of mission abort contingencies exist to primarily ensure the safety of the crew during off-nominal situations and to attempt to maintain the integrity of the Orbiter.

As the Space Shuttle ascends to orbit it transverses various intact abort regions evaluated and planned before the flight to ensure that the Space Shuttle Orbiter, along with its crew, may be returned intact either to the original launch site, a transoceanic landing site, or returned from a substandard orbit. An intact abort may be initiated due to a number of system failures but the highest likelihood and most challenging abort scenarios are initiated by a premature shutdown of a Space Shuttle Main Engine (SSME). The potential consequences of such a shutdown vary as a function of a number of mission parameters but all of them may be related to mission time for a specific mission profile.

This paper focuses on the Dynamic Abort Risk Evaluation (DARE) model process, applications, and its capability to evaluate the risk of Loss Of Vehicle (LOV) due to the complex systems interactions that occur during Space Shuttle intact abort scenarios. In addition, the paper will examine which of the Space Shuttle subsystems are critical to ensuring a successful return of the Space Shuttle Orbiter and crew from such a situation.

1
2
3 INTRODUCTION

The Dynamic Abort Risk Evaluation (DARE) model is a dynamic risk assessment model that evaluates the risk of intact Space Shuttle abort scenarios, namely, Return To Launch Site (RTLS), Trans-Atlantic Landing (TAL) and Abort To Orbit (ATO).

The DARE model was developed by Science Applications International Corporation (SAIC) under the sponsorship of the NASA Johnson Space Center (JSC). DARE is being used to:

- Assess the risks of each of the abort scenarios and identify their major risk contributors
- Identify the abort scenarios with the least risk in the event that one of three Space Shuttle Main Engines (SSME) benignly shuts down during ascent
- Perform various design and operational trade studies

4 SPACE SHUTTLE INTACT ABORT OPTIONS

As the Space Shuttle ascends to orbit, it transverses various intact abort regions planned before the flight to ensure that the Space Shuttle Orbiter, along with its crew, may be returned to either one of the following: the original launch site (RTLS), a transatlantic landing site (TAL), or from a substandard orbit (ATO) in the event that an abort is initiated. Each of these options is shown in Figure 1. If a failure should occur late in the trajectory, mission control may opt to simply continue on to the planned orbit (Press to MECO – PTM). If a significant failure during an intact abort occurs, then a contingency abort is executed.

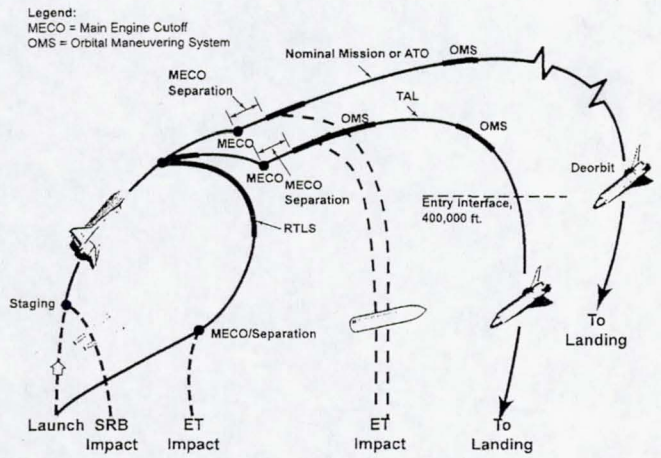


Figure 1. Space Shuttle Intact Abort Options

As the Space Shuttle climbs to orbit, the consequences of a single engine shutdown become less severe. More specifically, as the vehicle gains momentum and altitude it is better situated to maneuver and conduct aborts. The most challenging of the aborts available to a Shuttle pilot are the return to the launch site (RTLS) or a trans-atlantic abort landing (TAL). Both of these abort modes require the Shuttle to have a minimum altitude and velocity providing sufficient energy (kinetic and potential) to enable the spectrum of vehicle state vectors. This spectrum is necessary to allow for the successful completion of either of these difficult landing approaches. These minimum energy profiles require that the remaining two engines continue firing for the length of time necessary to ensure that the proper profile is attained to attempt an abort.

5 DARE MODELING CONCEPT

The DARE modeling concept is shown in Figure 2. It begins with an initiating event, and terminates with an end state. This methodology was designed to handle time-dependent conditional failure probabilities for the pivotal events, and conditional failure probabilities based on pivotal events interdependencies (i.e. failure of the Orbital Maneuvering System/Reaction Control System (OMS/RCS) to dump propellant would affect the weight of the Orbiter at landing and thereby increase the Loss Of Vehicle (LOV) risk). For the DARE model, pivotal events represent failures of systems or conditions that might result in a failure to successfully abort a mission.

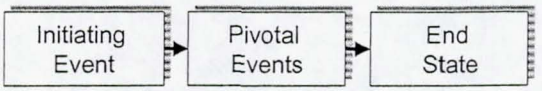


Figure 2. DARE Modeling Concept

6 DYNAMIC MODEL DEVELOPMENT

Figure 3, shown below, represents the outline for the DARE model development process. The DARE modeling approach involves a disciplined time dependent analysis of scenarios.

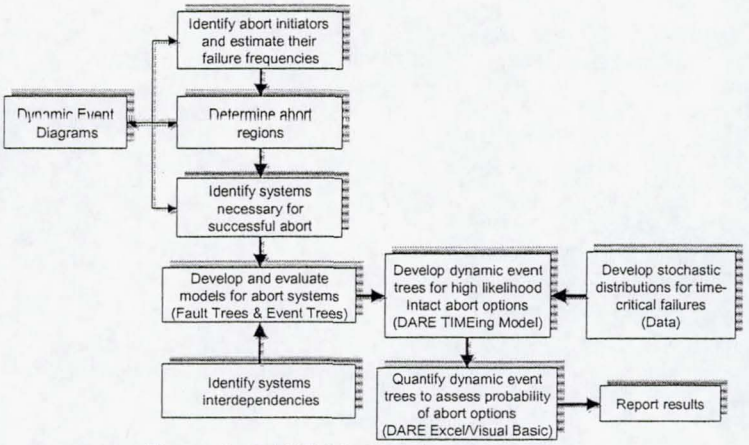


Figure 3. DARE Methodology Process

The process begins with the Dynamic Event Diagram (DED) and ends with producing the report of results. A brief description of the steps that were taken to develop DARE are outlined in the following subsections.

6.1 Dynamic Event Diagrams (DED)

In a conventional PRA practice, an event sequence diagram (ESD) is developed to represent the successes/failures of the systems required for a successful abort. Reaching beyond the limits of the ESD, the DED was developed to show the *time* at which these systems are required to initiate and function. DEDs, developed for each abort scenario (RTLS, TAL and ATO), represent the systems that must function to accomplish a successful abort. These systems can be considered pivotal events as defined above. Simply, the DED is used as a map to further investigate the initiating events, the abort region, and the systems to be modeled and analyzed. Figure 4, shown below, represents a non abort-specific DED.

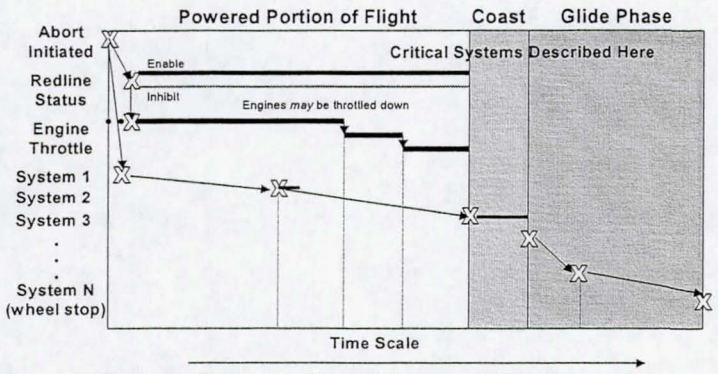


Figure 4. Dynamic Event Diagram (DED) Example

6.2 Identification of Abort Initiators

An intact abort may be initiated due to a number of system failures, but the most likely abort scenarios are initiated by a premature benign shutdown of one of three SSME (Maggio G. et al. 2000). Therefore, this was the abort-initiating event that was chosen for further in-depth dynamic probabilistic risk assessment.

6.3 Determine Abort Region

As shown in Figure 5, different intact abort options are available and chosen depending on the time a benign engine shutdown occurs. The dynamic probabilistic risk model for intact aborts uses abort region estimates from flight dynamicists that include the time of a benign engine shutdown and its associated available abort options. The actual abort boundaries are calculated prior to each flight based on a number of complex mission time-dependent parameters such as vehicle weight, orbital inclination, and available landing sites, etc.

There are cases where these abort regions might overlap. If this occurs (where performance loss is the only factor), the next available abort option would be chosen (i.e. if both are available, a TAL is always chosen over an RTLS) when the initiating event is a benign engine shutdown.

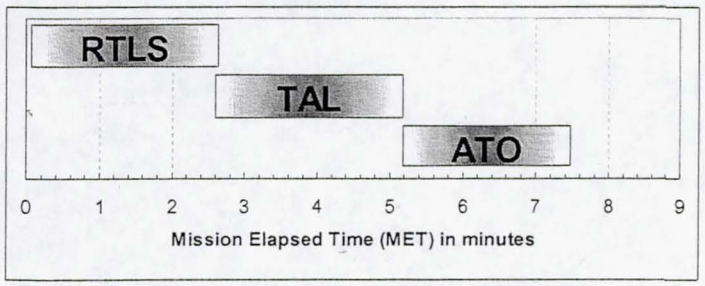


Figure 5. Typical Abort Boundaries used in DARE

Exercising any one of the abort options will depend upon the time at which the first engine benignly shuts down. For example, an RTLS due to an engine out at lift-off is selected at the earliest time, approximately two minutes, twenty seconds into the mission (after solid rocket booster separation). The probability of a benign shutdown of the second engine or the probability of a catastrophic failure of either one of the remaining two engines will vary depending on when the first engine shutdown occurred.

The STS101 and STS111 are the missions that are currently being evaluated by the DARE model. The baseline DARE model uses 104.5% as its throttle level of the Block II SSMEs. However, the model has the capability to evaluate the risk of elevated power levels as well as evaluating the LOV risk for various other planned missions.

6.4 Identification of Systems Necessary for a Successful Abort

The following is a list of the modules that make up the DARE model. These modules represent the systems that must function during an abort in order to accomplish a safe landing.

SSME: As the Space Shuttle ascends to orbit, the severity of the consequences of a single engine shutdown changes with time. The DARE model evaluates the LOV risk due to a second SSME shutdown and the LOV risk due to catastrophic failure of one of the remaining two SSMEs.

External Tank (ET) Separation: When the SSMEs are shutdown, the ET is jettisoned and it breaks up as it enters the Earth's atmosphere. Successful ET separation depends on the success of the Reaction Control System (RCS) to perform its intended function.

ET Debris Hit: During a TAL abort, subsequent to Orbiter/ET separation, the ET may be in relatively close range of the Orbiter when it ruptures during entry. This increases the risk of the Orbiter being struck by ET debris.

Powered Pitch Around (PPA): The PPA maneuver is performed only during an RTLS abort. The PPA maneuver changes the Orbiter's attitude from heads-down going away from the launch site to heads-up pointing toward the launch site by an approximately 60 to 70 degree maneuver Failure to perform this maneuver within a specific period oftime would lead to landing short of the runway or missing it completely which was assumed to result in LOV.

Powered Pitch Down (PPD): This is an RTLS specific critical maneuver. During the powered portion of an RTLS abort, in order for altitude and flight path angle constraints to be met at Main Engine Cut Off (MECO), a positive angle of attack

(~30 degrees) is required. However, an angle of attack of –2 degrees is necessary to ensure a safe ET separation. This transition is what is referred to as powered pitch down and must be completed rapidly by properly gimbaling the engine thrust to avoid large sink rates, which may cause overheating and overstressing. Failure to perform the PPD maneuver was quantified by modeling the inability to gimbal one of the remaining two SSME.

Control Surfaces: Control surface failures were assumed the driving risk factor in maintaining control of the vehicle during the glide phase of RTLS and TAL intact aborts. A streamlined model based on aircraft parts reliability was developed to account for this risk.

Thermal Protection System: The failure modes of the TPS during a TAL abort are assumed similar to those that might occur during a nominal mission. These failure modes include: debris damage with subsequent tile debonding (external tank, right solid rocket booster nosecone or orbital debris) and debonding from other sources (heating loads, high temperatures, aero-acoustic loads, cycle degradation of bonding materials and maintenance errors).

Touchdown Associated Failures: This includes the risk due to: excessive sink rate, tire failure(s) or runway under/overshoot, misalignment.

Orbital Maneuvering System/Reaction Control System (OMS/RCS) Dumps: Similar to the MPS, the OMS/RCS is modeled in DARE for its ability to dump propellant to reduce the likelihood of LOV. The amount of OMS propellant onboard the Shuttle during launch is mission specific. During an abort, the OMS propellant is dumped by burning it through both OMEs and possibly through the twenty-four aft RCS thrusters. This improves the performance during the abort and enables the Orbiter to achieve an acceptable landing weight and center of gravity (C.G.) location.

Main Propulsion System Dump: The MPS is modeled in DARE for its ability to dump propellant to reduce the likelihood of LOV. If the MPS fails to dump enough propellant, it would result in violating the Orbiter C.G. envelope, which in turn, could lead to loss of control of the vehicle.

6.5 System Interdependencies

Tremendous amounts of interdependencies exist among the modules listed above. For example, failure of the OMS/RCS to dump propellant during an abort would increase the risk at touchdown because an excessively heavy Orbiter will have too high a sink rate, possibly causing the Orbiter to slap down onto the runway. Furthermore, a high sink rate is likely to cause collapse of the landing gear and/or tire blowout.

6.6 Develop and Evaluate Models for Abort Systems

The DARE modeling process included the development of risk models for each of the systems discussed above. Some of these risk models used conventional risk methodology that include fault tree and event tree type models. For example, the PPD was modeled and quantified using fault tree analysis and was later incorporated into the DARE model. The OMS/RCS uses an event tree to both display and quantify the different failure scenarios of the OME and RCS jets. Some of these sequences resulted in end states that violate the Orbiter's C.G. limits affecting flight stability and were assumed to result in LOV. Other systems, such as the SSME time dependent risks are modeled using dynamic event trees and quantified using MS Excel and Visual Basic programming.

6.7 Data Analyses

Statistical distributions representing the pivotal event failures were constructed and used as input into the DARE model to quantify the abort risks. For example, lognormal distributions for both the likelihood of the orbiter getting hit by debris due to the breakup of the external tank in the Earth's atmosphere and the mean time-between-failure for the benign shutdown and catastrophic failure probabilities for the SSMEs were developed and used to evaluate the LOV risk. The Weibull distribution was used to evaluate the time dependent SSME risks.

6.8 Quantification

The DARE model has a graphical user interface (GUI) which employs complex MS Excel and Visual Basic macros to perform a Monte Carlo simulation to evaluate the abort risks.

The DARE model uses a set of inputs provided by NASA flight dynamicists. These parameters are mission specific and include the following items:

- Abort Landing Site
- Inclination (deg)
- First Engine Shutdown Time (sec)
- Solid Rocket Booster Staging (sec)
- OMS Assist On and Off (sec)
- Abort Initiation Time (sec)
- RCS Ignition Time (sec)

- OMS/RCS Dump Stop (sec)
- OMS Dump Duration Time (sec)
- RTLS Turnaround Time (sec)
- Powered Pitch Down Time (sec)
- Main Engine Cutoff Time (sec)
- External Tank Separation Time (sec)
- Orbiter center of gravity at lift off (x and y (in))
- Second stage lift off weight (lbs)
- Orbiter lift off weight (lbs)

The results for each specific trajectory are generated and output within the MS Excel environment.

The DARE model evaluates the LOV risks due to failure of any of the systems described above
During the quantification process, DARE selects conditional failure probabilities for the systems components based on: 1) time of the first engine shutdown; and 2) other systems failures during a specific abort scenario. For example, failure of the OMS/RCS to dump propellant during an abort increases the LOV risk at touchdown due to an excessively heavy Orbiter. The DARE model assigns touchdown failure probabilities depending on whether the OMS/RCS is successful in dumping propellant.

Another example of how the DARE model evaluates the dynamic risk is illustrated below in Figure 6. This figure represents a conceptual diagram for the evaluation of the LOV risk due to a catastrophic failure of either one of the two remaining SSMEs.

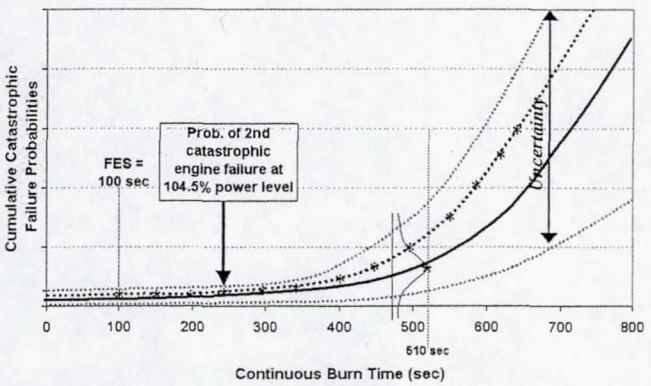


Figure 6. Estimation of Catastrophic Failure (conceptual)

Given a first engine shuts down at 100 seconds, the probability of a second engine catastrophically failing is given by the dotted line (with 'stars'). This is a function of the continuous burn time and the lognormal distribution as it marches through the time segments along the Weibull curve. This represents the SSME failure probability given that the power level is at 104% following the first engine shutdown.

7 APPLICATIONS OF THE DARE MODEL

The primary application of the DARE model is to evaluate the Loss of Vehicle (LOV) risk due to an abort given a benign engine shutdown. The DARE model has been used to perform sensitivity analyses and trade studies that include:

- Evaluating the abort risk of the SSME Block II vs. Block IIA
- Assessing the risk of being in a black zone given a second engine shutdown
- Assessing the probability of crew bailout given a second engine shutdown
- Assessing the probability of having to perform an East Coast Abort Landing (ECAL) given a second engine shutdown
- Evaluating the abort risk given higher SSME throttle levels

The DARE model is being used, and will continue to be used in the decision-making process to assess and improve the Space Shuttle operation, maintenance, and emergency procedures for the nominal and the abort scenarios.

8 REFERENCES

Fragola J.R., Maggio G., et al. 1995. Probabilistic Risk Assessment of the Space Shuttle, A Study of the Potential of Losing the Vehicle during Nominal Operation, SAIC/NY 95-02-25, New York

Heydorn, R., Railsback J., Nguyen C. 1998. *Shuttle Abort Probabilities for Redline Limits Management*, JSC White Paper

Maggio G. & Fragola J.R. 1995 Combining Computational Simulations with Probabilistic Risk Assessment Techniques to Analyze Launch Vehicles, Reliability and Maintainability Symposium Proceedings

Maggio G., et al. 1997. *A Dynamic Probabilistic Assessment of the Premature Shutdown Risk for the Space Shuttle Main Engine*, SAIC/NY 97-12-01, New York

Maggio G., Heydorn R.P., Railsback J.W. 1998. *A Risk-Based Assessment of the Space Shuttle Main Engine Redline Management Philosophy*, AIAA 98-3207

Maggio, G., Railsback J.W., Heydorn, R.P., Safie, F. 2000. *A Dynamic Risk Assessment of Space Shuttle Intact Abort Scenarios*, Probabilistic Safety Assessment and Management (PSAM5) Proceedings

Assessment of Space Shuttle Abort Risk for Varying In-flight Vehicle Management Scenarios
Modification to Statement of Work (121202)

I. Introduction

A study was undertaken by SAIC under Purchase Order T-6398W to quantify the risks associated with the Return-To-Launch-Site (RTLS) and Transoceanic-Abort-Landing (TAL) intact abort scenarios. SAIC developed The Space Shuttle Dynamic Abort Risk Evaluator (DARE). DARE is a computer code that uses the dynamic stochastic risk assessment methodology to assess the intact abort risk encountered during Space Shuttle missions. DARE is being utilized to assess the following phases of this project:

Phase I: Develop and implement a DARE model for RTLS and TAL intact aborts
Phase II: Develop and implement a DARE model for ATO
Phase III: Develop and implement a DARE model for contingency aborts (2EO)
Phase IV: Incorporate the Shuttle PRA results into DARE
Phase V: Independent DARE Assessment

Phase I has been further subdivided into three phases, Phases IA, IB, IC and ID. In Phase IA, modifications to the DARE were made to facilitate the unique requirements of this assessment and to streamline the evaluation of any future in-flight scenarios. Specifically, the DARE model was modified to output risk estimates for point abort boundary conditions rather than statistically generated data. The results for RTLS and TAL intact aborts were differentiated to facilitate comparative assessment of the risk associated with each option. Phase IB included the development of additional DARE modules as well as modifications to existing modules to address areas identified during Phase IA. Under Phase IC, updated the SSME risk probabilities and compared the risks between BKII and BKIIA SSME engines and provided support to the JSC Technical Panel Reviews

The specific tasks completed in both of the previous sub-phases are as follows:

- Phase IA
  - Modify DARE to Analyze Point Input Conditions
  - Differentiation of RTLS and TAL Risk Results
  - Produce Results for Defined RTLS and TAL cases
- Phase IB
  - Review NASA RTLS and TAL Risk Concerns
  - ET Separation Risk Model Review
  - Meeting with SSME Reliability Experts
  - Expand DARE to Include RTLS and TAL Glide Phases
  - Produce Interim Results for Modified RTLS and TAL DARE Model
  - ET Debris Impact Risk Model Review
  - Two-Engine Shutdown LOV/LOC Assessment
  - Produce Final Results for Modified RTLS and TAL DARE Model

- Phase IC
  - Update SSME Risk Probability
  - SSME Block II and Block IIA Risk Comparisons
  - Comparisons of RTLS and TAL Risk for Varying Power Levels
  - Comparisons of RTLS Risk with varying Q-bar at ET Separation
  - Prepared and delivered presentation to Flight Technique Panel
  - Prepared and delivered presentation to Integration Control Board
  - Prepared and delivered presentation to Space Shuttle Risk Assessment Team

Phase II
  - Developed and integrated risk modules for ATO
  - Produced Results for defined ATO

Phase IV task IV-1
  - Incorporate SPRAT Preliminary models/results into the DARE model
  - Obtain Abort Trajectories from JSC and perform sensitivity analyses to evaluate the LOCV for a number of Abort scenarios for different engine shutdown times and related abort types.
  - Aggregate DARE results with SSME shutdown estimates to provide a single abort risk input for SPRAT
  - Prepare presentation and report findings

Phase V
  - Prepare a document describing the DARE model mechanics and probabilistic methodology and its application

This modification is proposed to amend the existing statement of work with Phase VI. Phase VI will provide support to the Independent Peer Review team.

The phases of this contract are described in detail below:

The tasks in each of these subsequent pre-approved phases are as follows:

- Phase ID
  - RTLS Risk Reduction Investigation

- Phase III
  - Develop and Integrate Risk Model for Contingency Aborts
  - Produce Results for Defined Contingency Case

Phase IV
  - Review SPRAT Preliminary and Final Models and results
  - Update DARE with SPRAT Results
  - Prepare presentation and report findings

Note that only Phase VI is discussed in the subsequent sections since Phase ID, Phase III and Phase IV are part of the existing purchase order.

II. Task Descriptions

A. Phase VI – Independent Assessment Review and Independent Peer Review Support

The following tasks are required to support the Independent Review Team:

- Arrange meeting with IPR team and provide written information
- Prepare presentation on DARE technology
- Present DARE technology to NASA –JSC, NASA risks analysis management and the Independent Reviewers.
- Provide IPR team with any additional information
- Solicit and review IPR comments.
- Prepare response to IPR comments and submit to IPR for approval.
- Resolve any IPR comments or disagreements that might result from item described above
- Develop a plan to implement IPR recommendations and make modifications if funding allows

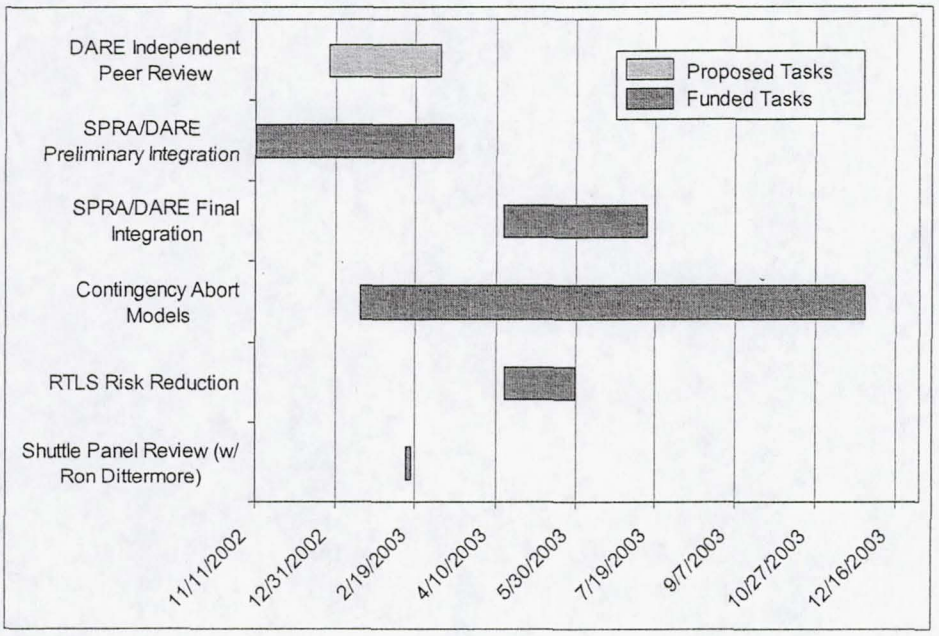
III. Deliverables

The following describes the deliverables required by this SOW.

Report of Results
SAIC shall deliver a report (in the form of a presentation) on the results at the end of each phase of the DARE project. For each phase, the report will describe the data, assumptions, and analysis methods used to produce the results. The report shall be delivered to NASA in an electronic form. Each report shall be delivered no later than 1 month after completion of the technical requirements.

IV. Period of Performance

The funded period of performance will not change and remains September 1, 2000 to December 31, 2003.



V. Cost

These are rough-order of magnitude (ROM) estimates and are not official estimates:

	Description	Cost
Phase VI	**Independent Peer Review Support**	**$30,891**

Official estimates shall be provided in the final proposal.