N93-26976

Nuclear Electric Propulsion Operational Reliability and Crew Safety Study

NEP Systems / Modeling Report

22 October, 1992

Presented By:

James Karns
Science Applications International Corporation
8 W 40TH ST, 14TH Floor
New York, NY 10018
(212) 764-2820

Presented At:

1992 Nuclear Propulsion - Technical Interchange Meeting
NASA Lewis Research Center
Sandusky, OH

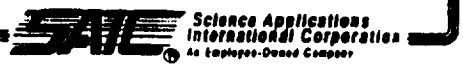
This work was accomplished under contract NAS3-25809, Mod 22 for the NASA Lewis Research Center Nuclear Propulsion Office, and under the technical direction of Michael Doherty.

The project manager for this contract was Michael Stancati. The technical work effort was led by Joseph R. Fragola, Vice President and Manager, Advanced Technology Division. James J. Karns led the reliability analysis task and overall systems engineering effort. Dennis Pelaccio was responsible for nuclear and propulsion systems engineering, Lloyd Kahan for reliability modeling, Peter Appignani and Richard McFadden for identifying and developing surrogate reliability data bases, and Darrel Walton for administrative support.

We would like to thank Mike Doherty and Jim Gilland of the Nuclear Propulsion Office for their invaluable expertise and assistance in performing this task.

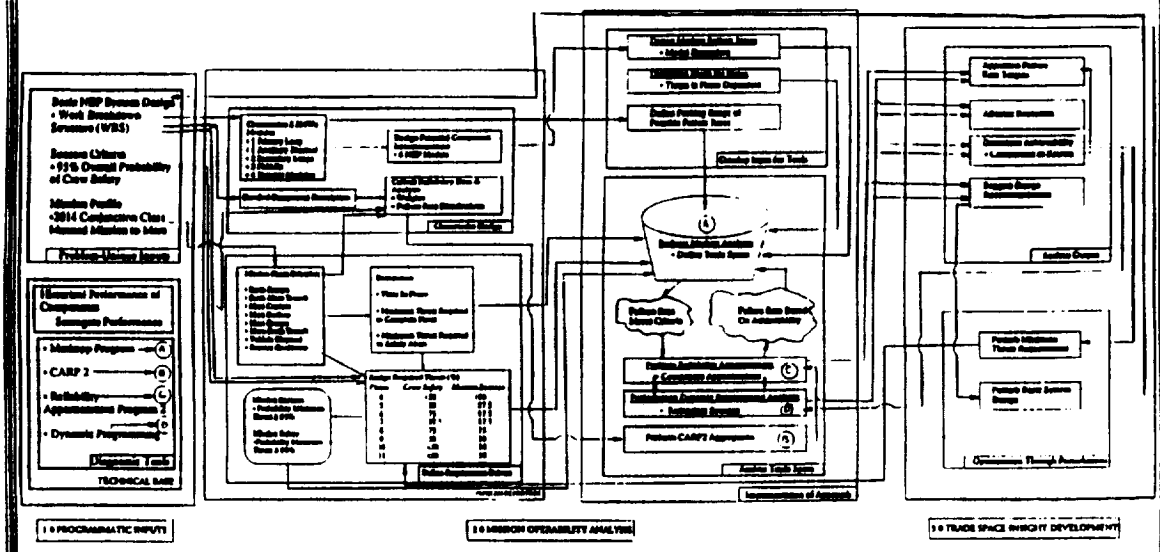
STUDY OBJECTIVES:

- Determine the range of reliability figures of merit required for a successful NEP manned Mars mission.
- Provide design insights:
  - design achievability, given existing technology;
  - alternative design approaches or concepts to enhance reliability, crew safety;
  - allocation of research and development resources.



The objective of this study was to establish the initial quantitative reliability bounds for nuclear electric propulsion systems in a manned Mars mission required to ensure crew safety and mission success. Finding the reliability bounds involves balancing top-down (mission driven) requirements and bottom-up (technology driven) capabilities. In seeking this balance we hope to: (1) provide design insights into the achievability of the baseline design in terms of reliability requirements, given the existing technology base; (2) suggest alternative design approaches which might enhance reliability and crew safety; and (3) indicate what technology areas require significant research and development to achieve the reliability objectives.

STUDY OVERVIEW



Science Applications International Corporation
An Employee-Owned Company

This study was broken down into three broad areas: the processing of programmatic inputs; performing the mission operability analysis; and analyzing the trade space for design insights. The processing of **programmatic inputs** began with identifying, soliciting, obtaining, and processing the required *program unique inputs*. These included the basic NEP system design, the top-level mission and crew safety success criteria, and the mission profile. Next, the existing *technology base* was examined to identify and obtain data on the historical performance of NEP and NEP-related (surrogate) components, and to determine the set of diagnostic tools appropriate to this analysis.

The **mission operability analysis** consisted of problem definition and implementation of the selected analysis approach. *Problem definition* included characterizing the design in terms appropriate to the selected diagnostic tools, and defining the reliability requirement drivers in the NEP system for the selected mission. *Implementation of the approach* consisted of developing the input for the various diagnostic tools, and analyzing the reliability trade space developed by the tools. The process of **trade space insight development** included *analyzing the trade space output* and seeking design insights by looking for improvements in system reliability when the basic design is altered, or *optimization through perturbations*.

CONCEPT OF ACHIEVABILITY

- Achievability: The ratio of required performance to achieve performance.
  - Measures how far a design has to go.
    - Achievability Index = 1: Design is achieved.
    - Achievability Index = 0: Design cannot be achieved with existing technology.
- Incorporates uncertainties in:
  - Particulars of design,
  - Relevance of historical performance.
- Should therefore be presented as a range of values.

A core concept in this analysis is the idea of achievability -- how well the existing technology base will support the NEP mission and design as given. Achievability is formally the ratio of the required performance to the readily achieved performance, given the state of the technology base. Since there are uncertainties in both the particulars of the design, and in the relevance of historical performance to NEP - Manned Mars Mission performance; and since there is significant variability in the measured performance of historical (surrogate) elements, the achievability should be presented as a range of values.

Due to time and funding limitations on this study, a rigorous development of the distribution of achievability values is not presented. Instead, point values of the limits on achievability are found.

ACHIEVABILITY DEFINITION

$$\phi\,(AchIcomponent) = \frac{\phi\,(\lambda pportioned\ Component)}{\phi\,(\lambda Surrogate\ Component)}$$

$$\Phi\,(AchISystem) = Aggregate\,(\phi\,(AchIComponent))\,\Big|_{All\ Components}$$

$\phi\,(AchIComponent)$ Distribution of achievability index (AchI) for a component.

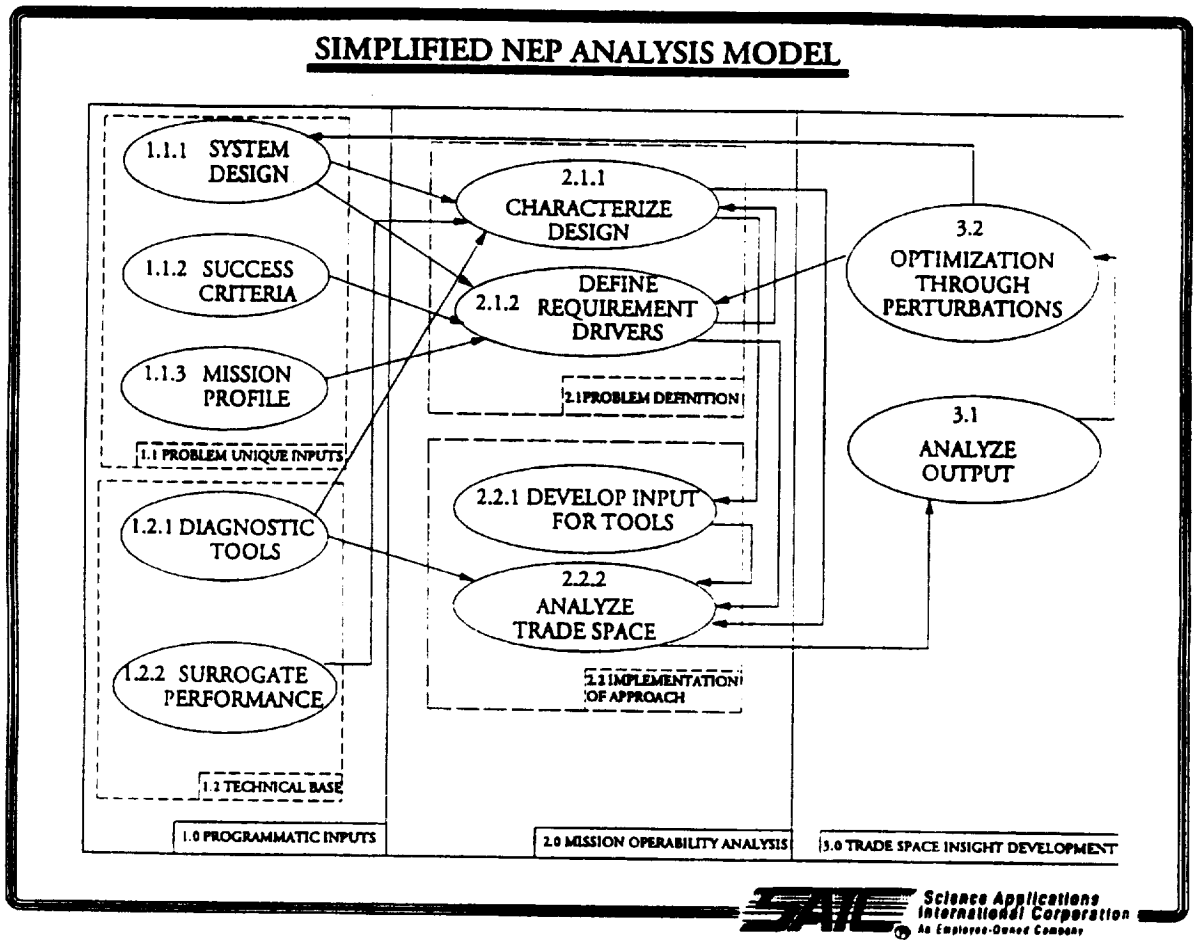
$\Phi\,(AchISystem)$ Distribution of AchI for a system.

$\phi\,(Apportioned\ Component)$ Distribution of apportioned failure rates required for component.

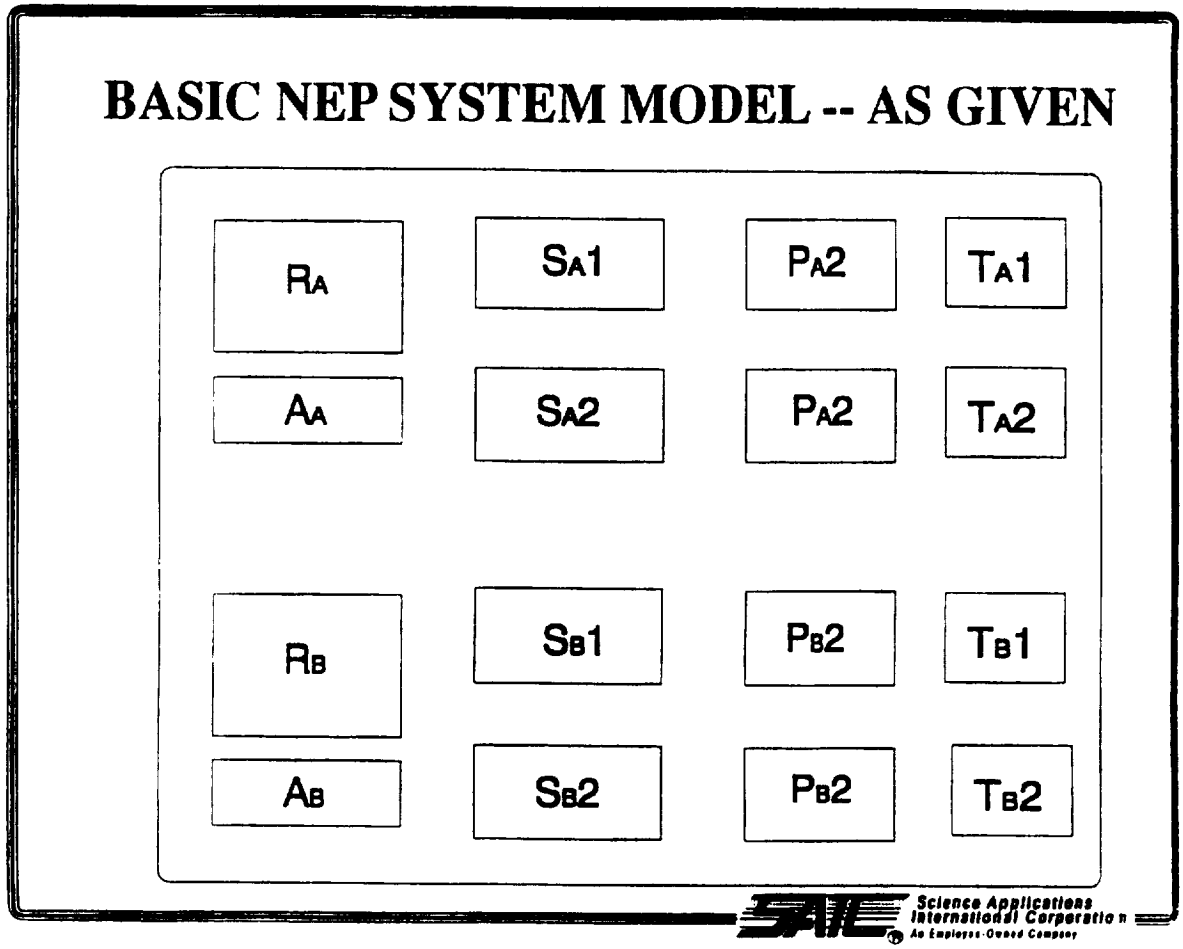
$\phi\,(Surrogate\ Component)$ Distribution of likely failure rates for component based on surrogate performance.

SAIC Science Applications International Corporation An Employee-Owned Company

Achievability is measured in terms of an achievability index (*AchI*), which is measured in terms of the measurable figure of merit for this study, random failure rate (λ). The distribution of *AchI* for a component is the ratio of the distribution of failure rates apportioned to the component based on design and mission requirement parameters, and the distribution of failure rates associated with surrogates of the component from the technology base. The distribution of *AchI* for the entire NEP system is the aggregate of component *AchI* distributions.



The analysis process began with characterizing the system design at a high level in terms appropriate to the analysis tools.



We were provided a simple model of the NEP system, consisting of two essentially independent modules. Each module consisted of a Primary Heat Source Loop (R), an Auxiliary Thermal Subsystem (A) two Secondary Loops (S), two Power Management and Distribution Assemblies (P), and two Thruster Assemblies (T).

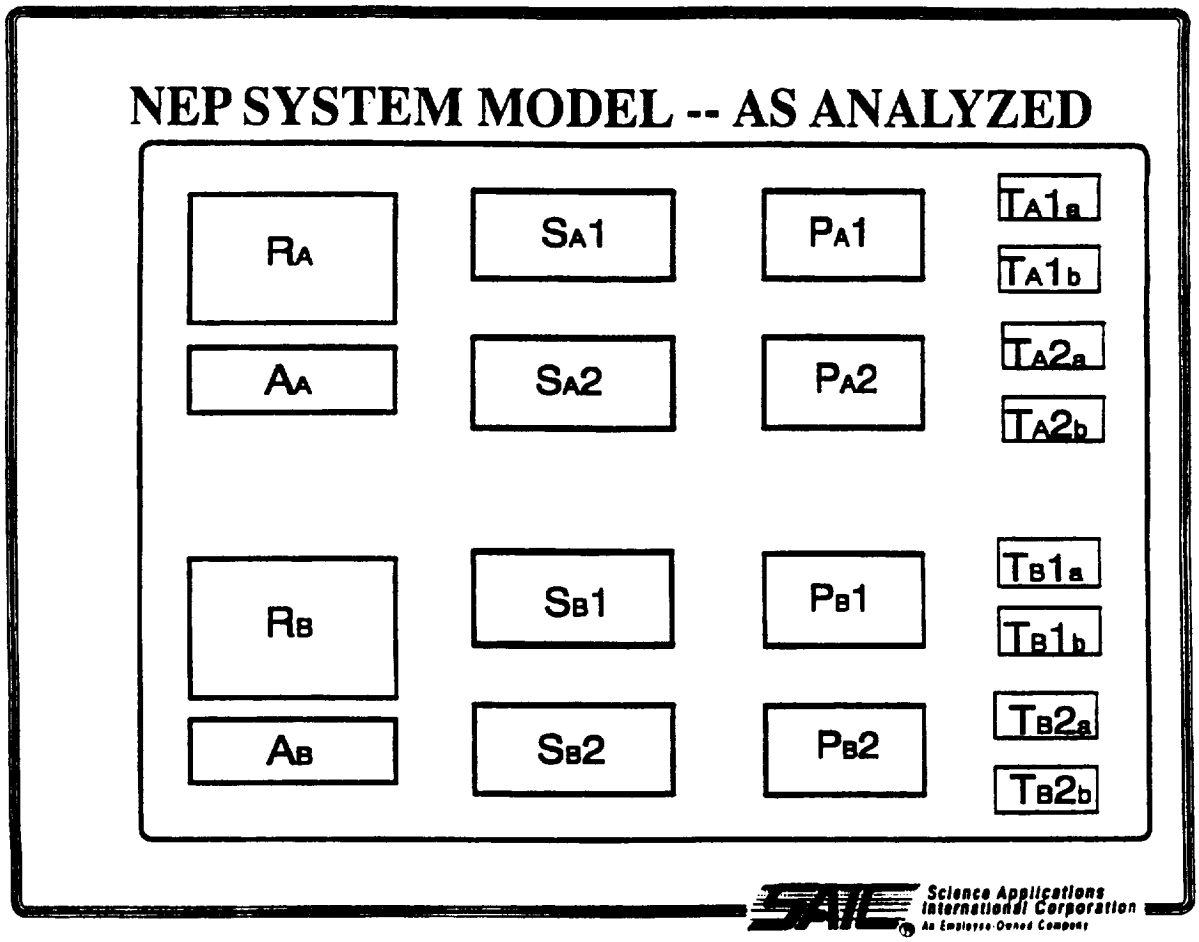
This basic top level design representation was extended and altered somewhat to provide various design concept bases for analysis.

NEP SYSTEM MODEL

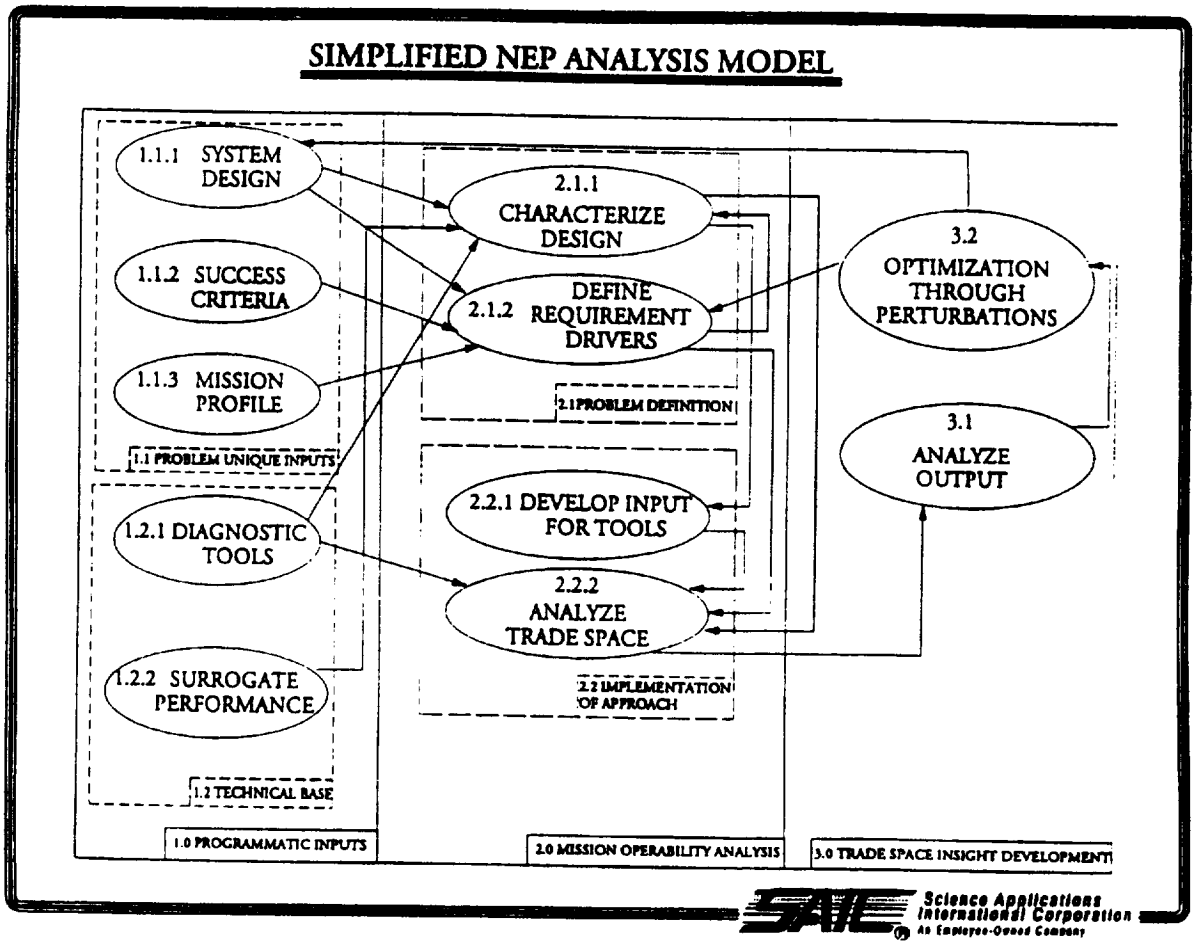
- Two 5MWe NEP Modules:
  - Each 5MWe NEP module:
    - 1 Primary heat source subsystem (R)
    - 1 Auxiliary thermal management system (A)
    - 2 Secondary subsystems (S)
    - 2 Power Management And Distribution (PMAD) subsystems (P)
    - 4 half-Thruster module subsystems (T)
      - The "given" thruster modules were split, as analysis indicated two halves essentially independent.

Science Applications International Corporation
An Employee-Owned Company

No comment required.



It was noted that each Thruster assembly had two essentially independent halves, so the model was modified slightly to make this apparent.

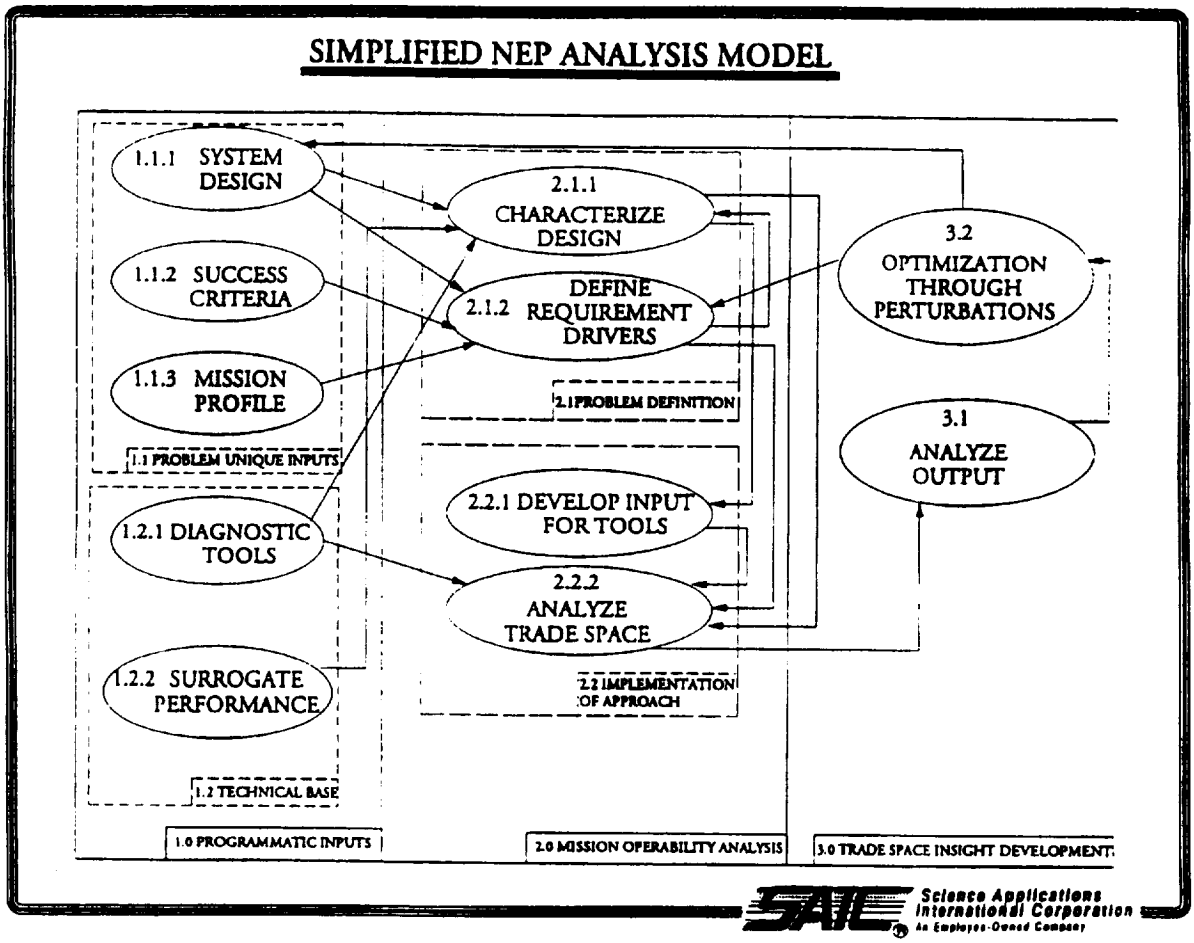


The next step in the analysis process was to identify and characterize the measurable success criteria for the mission.

NEP MANNED MARS MISSION SUCCESS CRITERIA

- 99% Probability of Crew Safety.
  - Aborts possible,
  - System need not reach Mars, but
  - Must return to Earth in or before nominal mission time frame.
- 95% Probability of Mission Success.
- Criteria applied to NEP System Only!
  - Overall mission probabilities must account for all other systems:
    - Life Support,
    - GNC, EPS (distribution), Thermal, TT&C, C&DH, etc.,
    - Ascent / Descent modules,
    - Earth Crew Capture Vehicle.

At a top level, the success criteria was given as 99% probability of crew safety, and 95% probability of mission success. It should be noted that this criteria was interpreted to apply only to the NEP system, not to other, equally vital, systems.

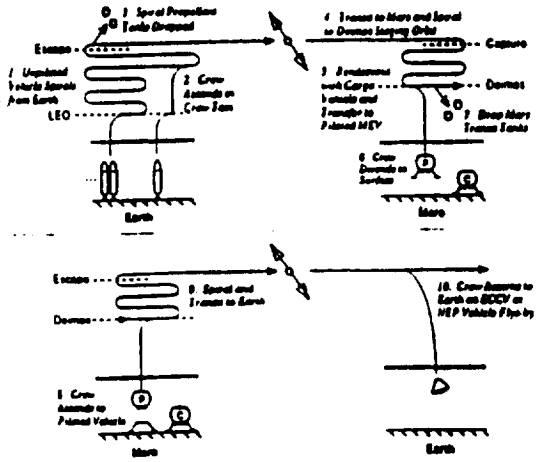


The last aspect of the Problem Unique Inputs portion of the analysis problem was to identify and define the Mission Profile.

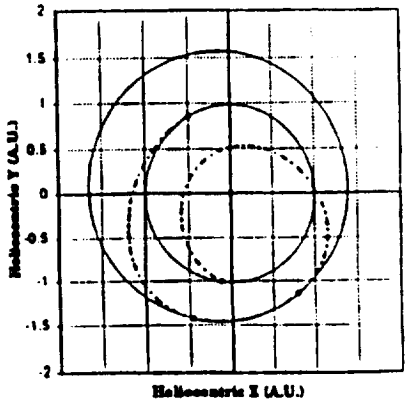
C-5

BASELINE MISSION CHARACTERISTICS

Mission Profile

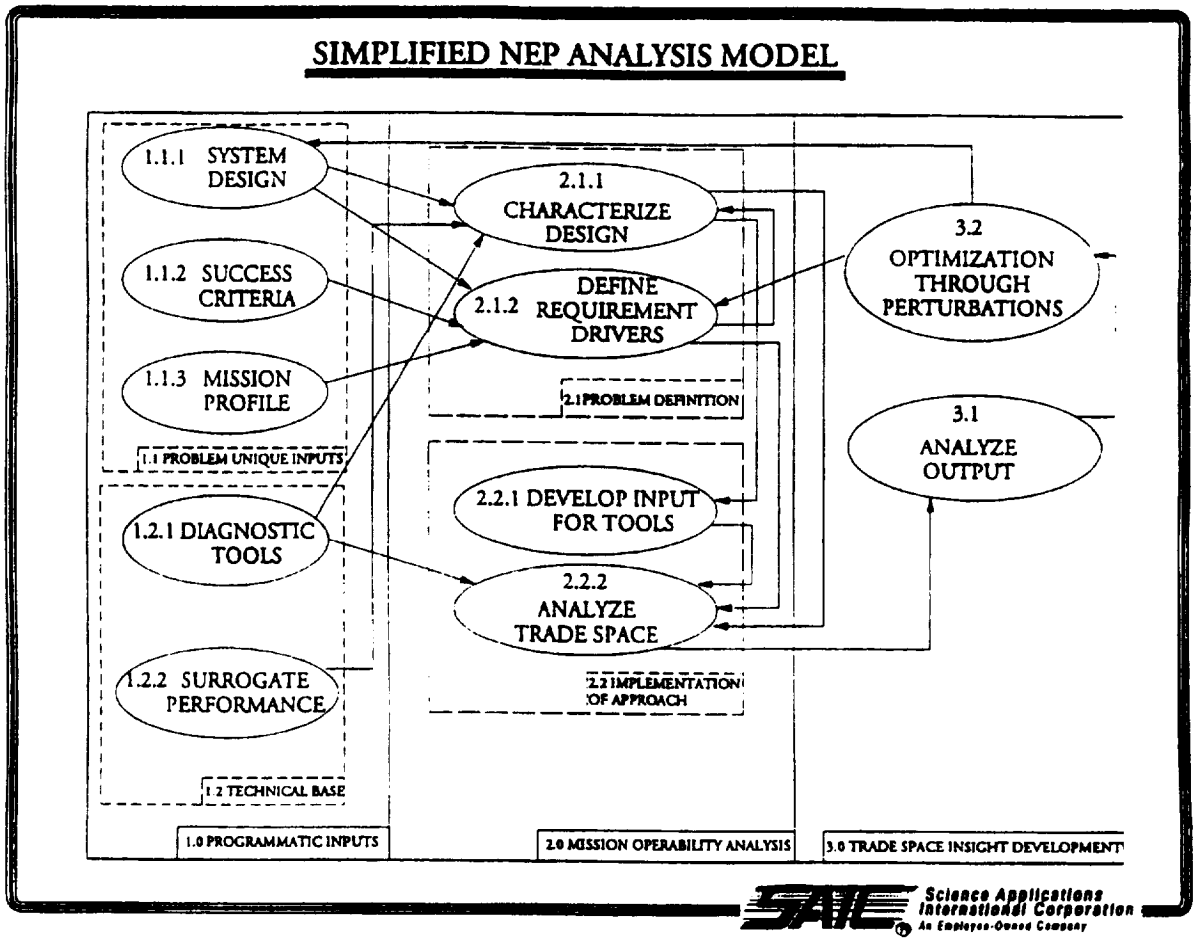


Orbit Plot



- Imelco - 350 MT
- Minimum Heliocentric Distance- 0.50 - Air

The mission analyzed was a 2014 conjunction class Manned Mars Mission.



After obtaining and characterizing the Program Unique Inputs, the technology base was then examined to determine the diagnostic tools appropriate to the analysis problem.

DIAGNOSTIC TOOLS

- Markapp(TM) -- Dynamic Markov Chain analysis program.
  - Determine top-level reliability figure(s) of merit (FOM).
- RAP2(TM) -- Reliablity Approtionment Program.
  - Apportion top-level FOM to component level.
- Dynapro(TM) -- Dynamic Integer Programming
  - Non-linear "optimization" of redundancy complement.
- CARP(TM) -- Computerized Aggregation of Reliability Parameters.
  - Combine historical reliability performance data from multiple sources.

The analytical tools selected were Markapp™, RAP2™, Dynapro™, and CARP™.

Markapp™ is a dynamic Markov-Chain analysis program. This tool allows the system to be modeled as a set of discrete states, based on the number and types of components that will fail. The probability of the system being in each of the states at any time in the mission can be calculated based on the failure rates associated with the components. This tool is used to determine what set(s) of top-level failure rates will result in achieving the mission success criteria.

RAP2™ apportions top-level reliability goals to lower-level components based on a variety of apportionment strategies. Dynapro™ is a Dynamic Integer Programming tool used in conjunction with RAP2™ to determine optimum allocations of, and limits on, spare allocation.

CARP™ -- Computerized Aggregation of Reliability Parameters is used to combine or aggregate distributions of failure rates from components similar to NEP components to define an appropriate surrogate distribution for each of the NEP components.

MARKAPP$_{(TM)}$ MARKOV CHAIN ANALYSIS

- The Markov chain is a discrete state - continuous time analytical model.
  - Used to determine sets of functional element failure rates that meet success criteria.
- A state is a unique configuration of NEP functional elements
  - 2 Pri, 2 AuxTherm, 4 Sec, 4 PMAD, 8 Thruster
- Transition between states *i* and *j* occurs at transition rate λ_{ij}.
- Markapp(TM) calculates probability that the system is in each state -- a function of:
  - Previous state of the system,
  - Failure rates of functional elements,
  - Time in mission.

The Markov model is comprised of a description of the NEP system in terms of its functional elements, a list of operational states of the system in terms of whether each of the components is operational or failed, and the rate at which the system transitions from one state to another. The transition rates are expressed in terms of the failure rates of the functional elements of the system.

Markapp™ solves the Markov model for the probabilities that the system is in each defined operational state as a function of time in the mission. These probabilities can be combined with the knowledge of which states meet the mission success criteria at each phase of the mission to determine the probability of the system meeting the success criteria. That information, in turn, indicates whether the input (trial) failure rates for the functional components will meet the mission objectives.

THE MARKOV PROCESS

$$\mathbf{x}(t + \Delta t) = \Delta t \begin{bmatrix} \lambda_{11} & \lambda_{12} \cdots & \lambda_{1N} \\ \lambda_{21} & \lambda_{22} \cdots & \lambda_{2N} \\ \vdots & \vdots & \vdots \\ \lambda_{N1} & \lambda_{N2} \cdots & \lambda_{NN} \end{bmatrix} \mathbf{x}(t)$$

$\mathbf{x}(t) = [x_i(t)] =$ Vector of probabilities that system is in state i.

$\lambda_{ij} = a_{ij}\lambda_{\text{Primary}} + b_{ij}\lambda_{\text{AuxTherm}} = c_{ij}\lambda_{\text{Secondary}} + d_{ij}\lambda_{\text{PMAD}} + f_{ij}\lambda_{\text{Thruster}}$

λ_{Primary}, $\lambda_{\text{AuxTherm}}$, $\lambda_{\text{Secondary}}$, λ_{PMAD}, $\lambda_{\text{Thruster}}$: Failure rates of functional elements.

N, a_{ij}, b_{ij}, c_{ij}, d_{ij}, f_{ij},: Parameters determined by the system design.

Science Applications International Corporation
An Employee-Owned Company

These equations describe the mathematics of the Markov Process.

RAP2$_{(TM)}$ RELIABILITY APPORTIONMENT

- RAP2(TM) apportions reliability from top-level to component level.
- Simplified apportionment equation:
  - $R_i\text{Apportioned} = R_{Goal}^{\frac{W_i}{\Sigma W}}$
- 3 apportionment methods:
  - Simple -- based on history of like components:
    - $W_i\text{Simple} = R_i\text{Surrogate} = e^{-\lambda i_{Surrogate}}$
  - AGREE -- based on part count (complexity) and criticality:
    - $W_i\text{Agree} = \#\text{Parts}_i * \text{Criticality}_i$
  - Weighted Nth-Root -- based on physical characteristics of component:
    - $W_i\text{NthRoot} = a_1 W_i\text{Complexity} + a_2 W_i\text{StateofArt} + a_3 W_i\text{Type} + a_4 W_i\text{Quality}$

Science Applications International Corporation
An Employee-Owned Company

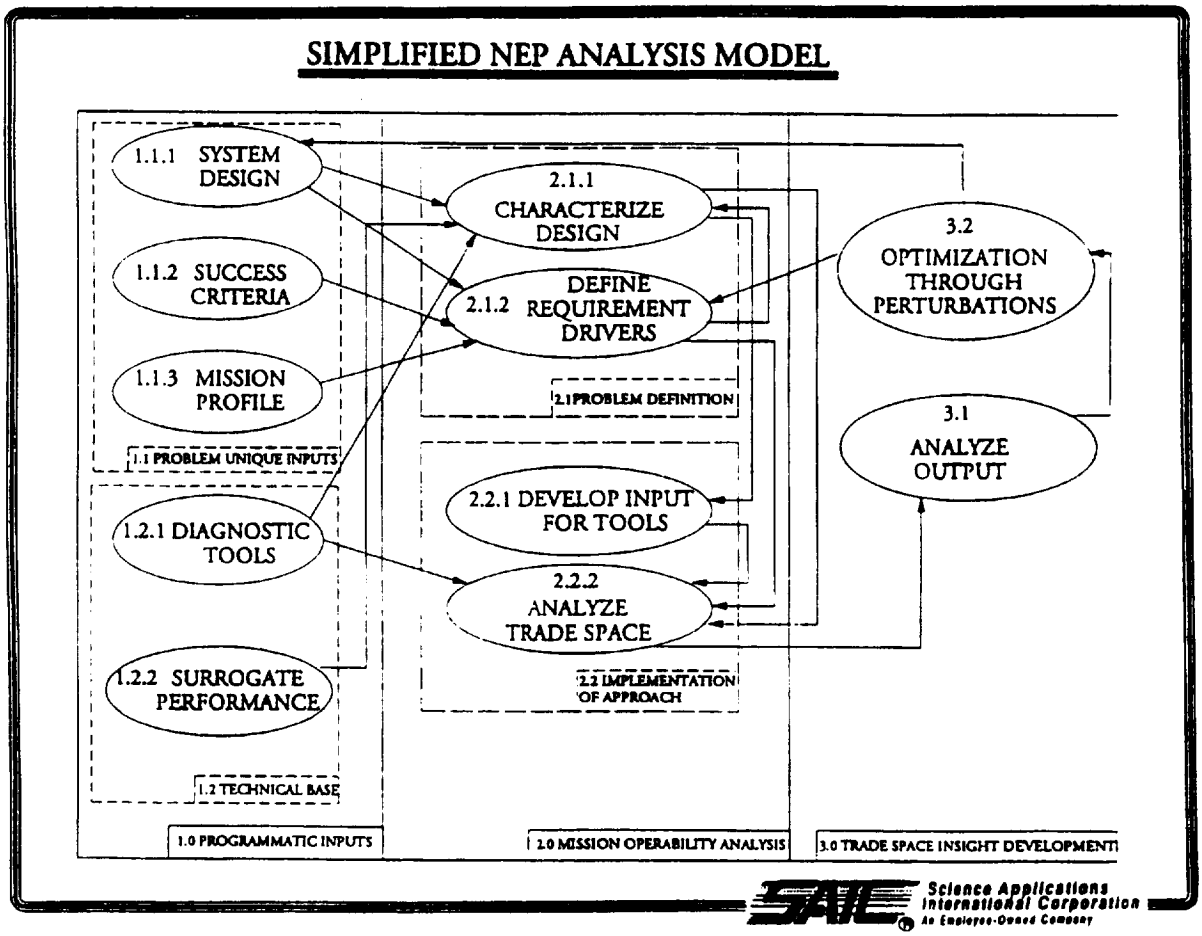
The RAP2™ Reliability Apportionment Program is used to apportion the top-level (functional-level) failure rates arrived at using the Markov analysis to the lower level components of the NEP system. The program uses three algorithms, each of which provide unique insight into the apportionment problem. The Simple apportionment algorithm is based strictly on the historical performance of like components, and indicates most directly how much the system reliability requirements will push the technology base. The AGREE algorithm is based on subjective assessment of the component relative importance, and on the component complexity. AGREE therefore provides a simple and much less rigorous way of apportioning based on mission requirements (criticality) than the Markov model. The weighted Nth Root method apportions reliability based on subjective evaluation of the relative difficulty in achieving high reliability for the components. Comparing relative differences between the Simple and Weighted Nth Root algorithms provides a first approximation of what is available versus what the analyst believes ought to be available.

CARP(TM) SURROGATE AGGREGATION

- Identify likely failure rate range of new component based on aggregation of similar components:
  - Similar in function;
  - Similar in application;
  - Similar in stress environment.
- Failure rate distribution incorporates:
  - Inter- and Intra-source Variability;
  - Uncertainty in similarity of function, application, or environment.
- Surrogate data sources:
  - NPRD-91, DSR-4, IEEE 500, CREDO, various NUREGs.
- No similar historical surrogate => establish range by "reality boundary".

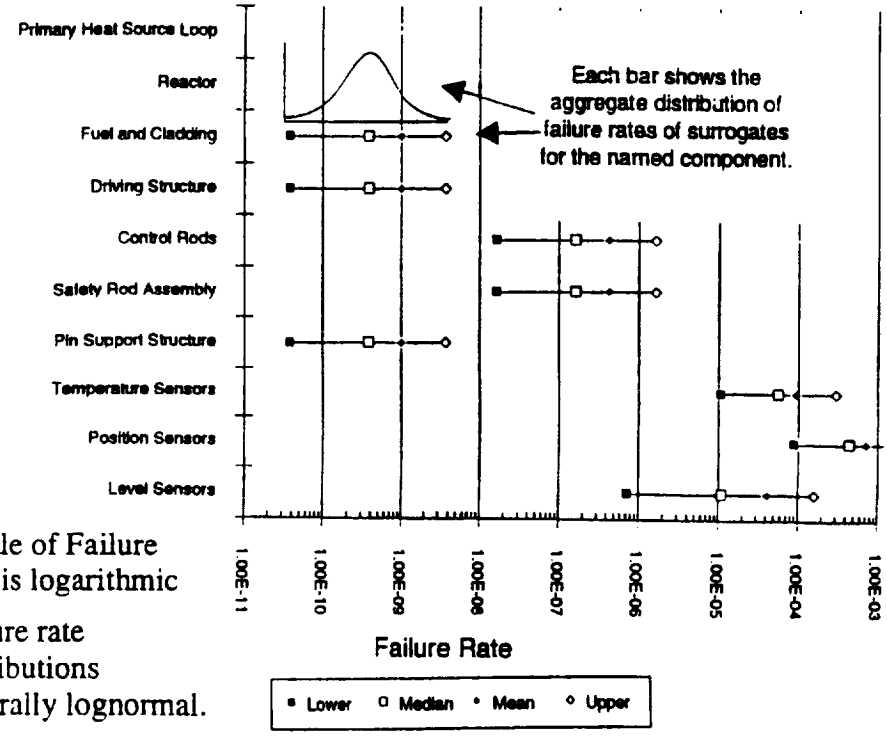
Finding the failure rates of components similar in function, application, and environment to the NEP components involves searching multiple sources. From each source a distribution of failure rates reflecting the variability in the historical components is obtained. CARP combines a number of these sources into a single, surrogate distribution representative of the anticipated performance of similar components in the NEP system.

If sufficiently similar components cannot be found in historical data references, a surrogate distribution for the NEP component is obtained by estimating the bounds within which the failure rate must fall, based on the physics of the component and the comparison of the unknown component with well-known components.



The selection and analysis of surrogates for NEP component performance was the next step in the analysis of the technology base.

READING SURROGATE DATA

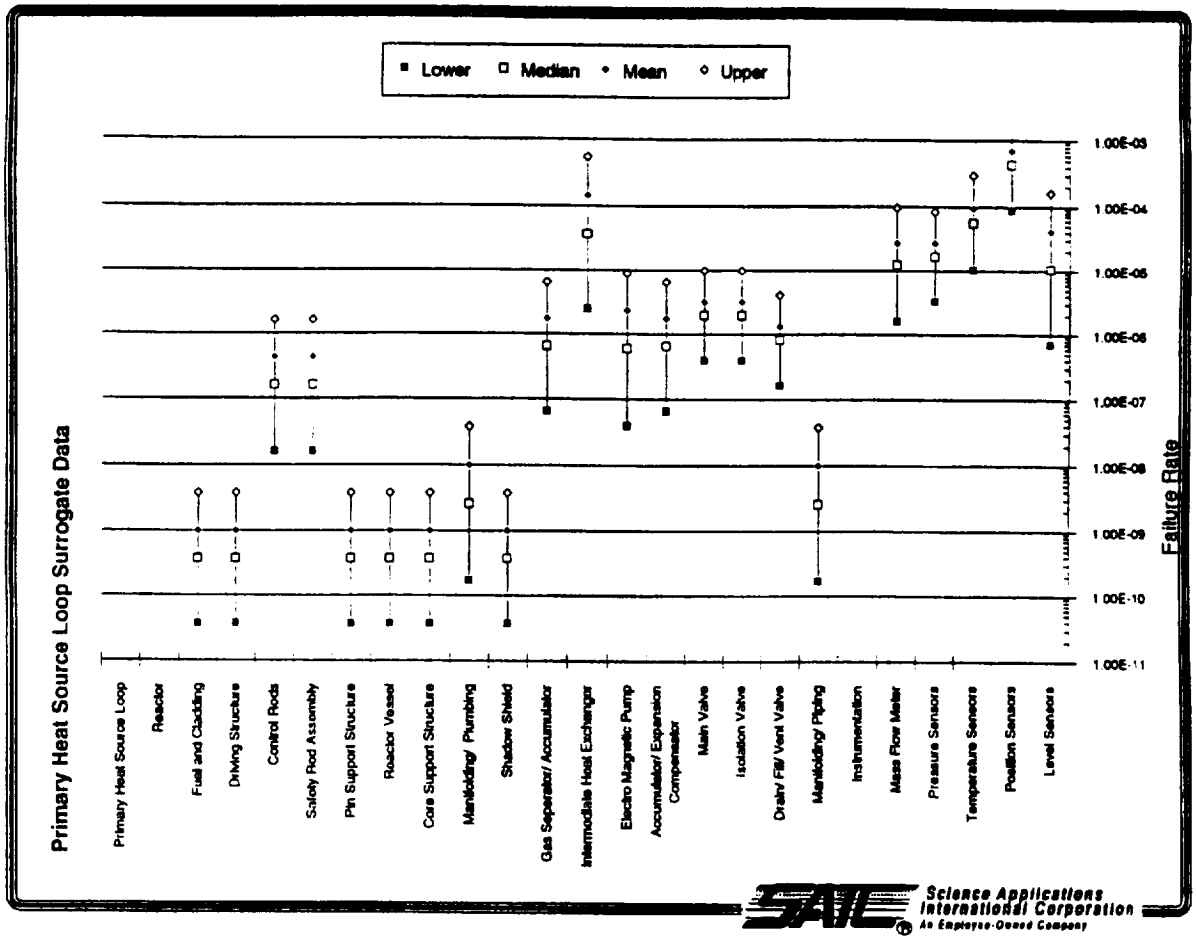


- Note: Scale of Failure Rate axis is logarithmic
  - Failure rate distributions generally lognormal.

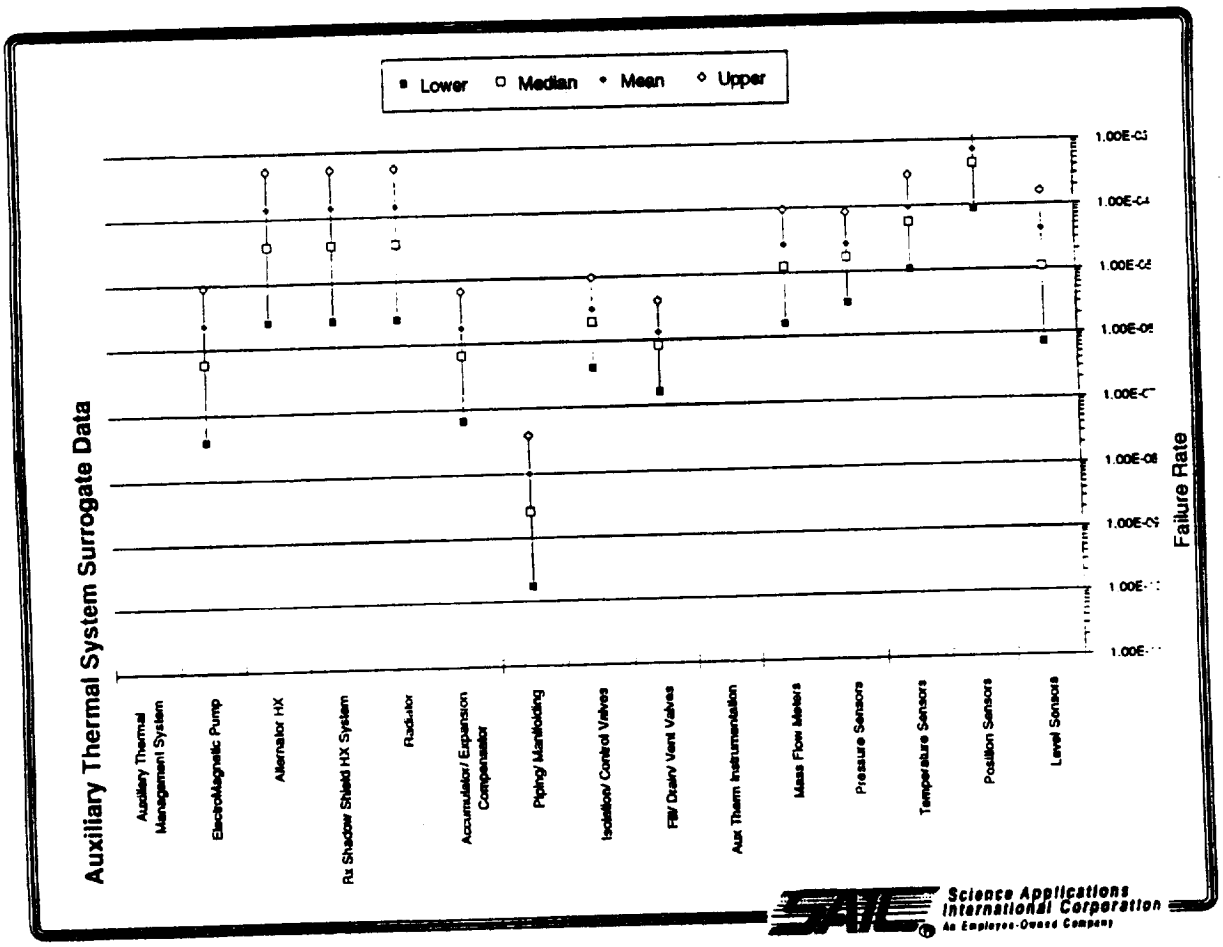
Science Applications International Corporation
An Employee-Owned Company

For each component, the distribution of representative (surrogate) failure rates is depicted as indicated. The upper and lower bounds of the indicated distributions are in fact the 5th and 95th percentiles. The mean and median are both shown because these distributions are generally left-skewed rather than normal, so the mean and median are different.

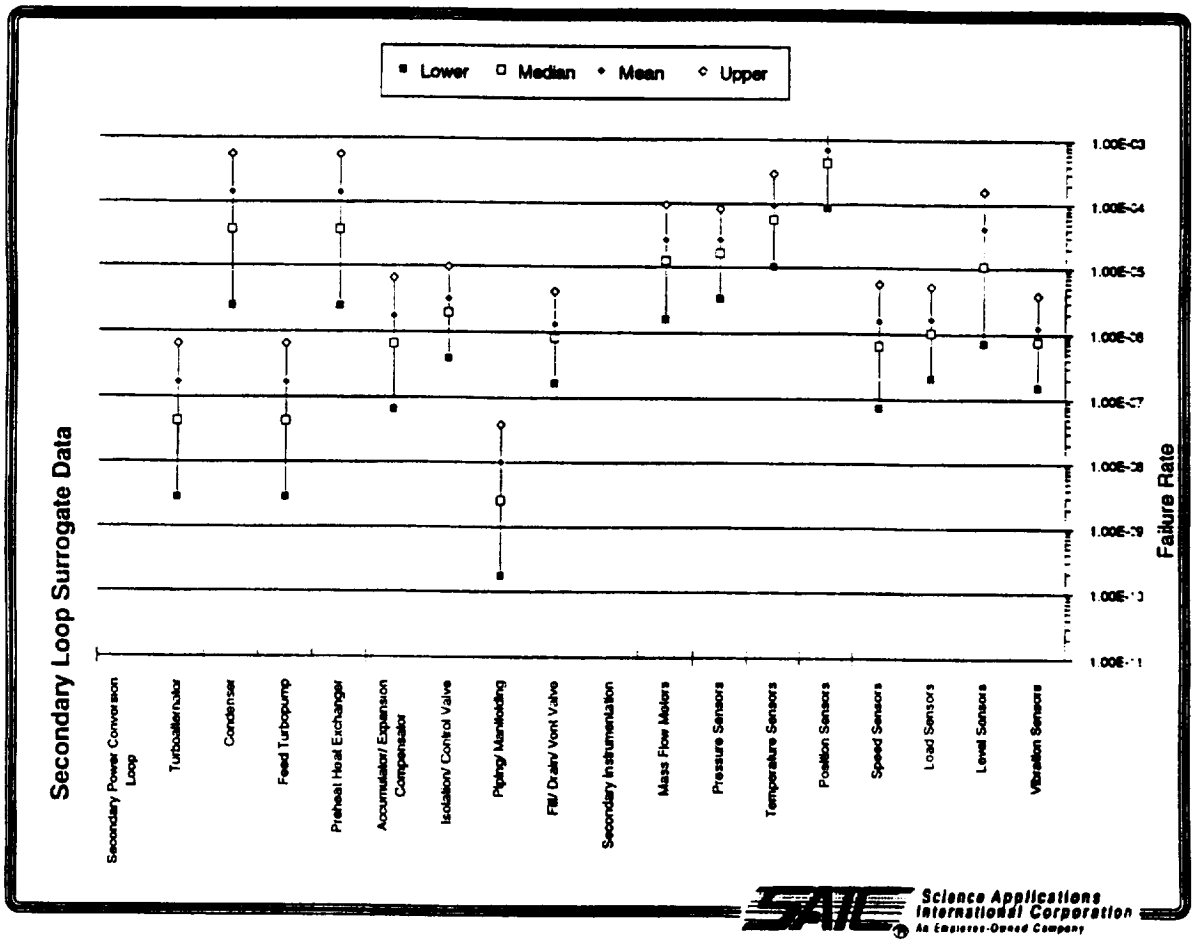
The x axis of this plot is logarithmic, so the distributions (which appear symmetric on this graph) are in fact lognormal.



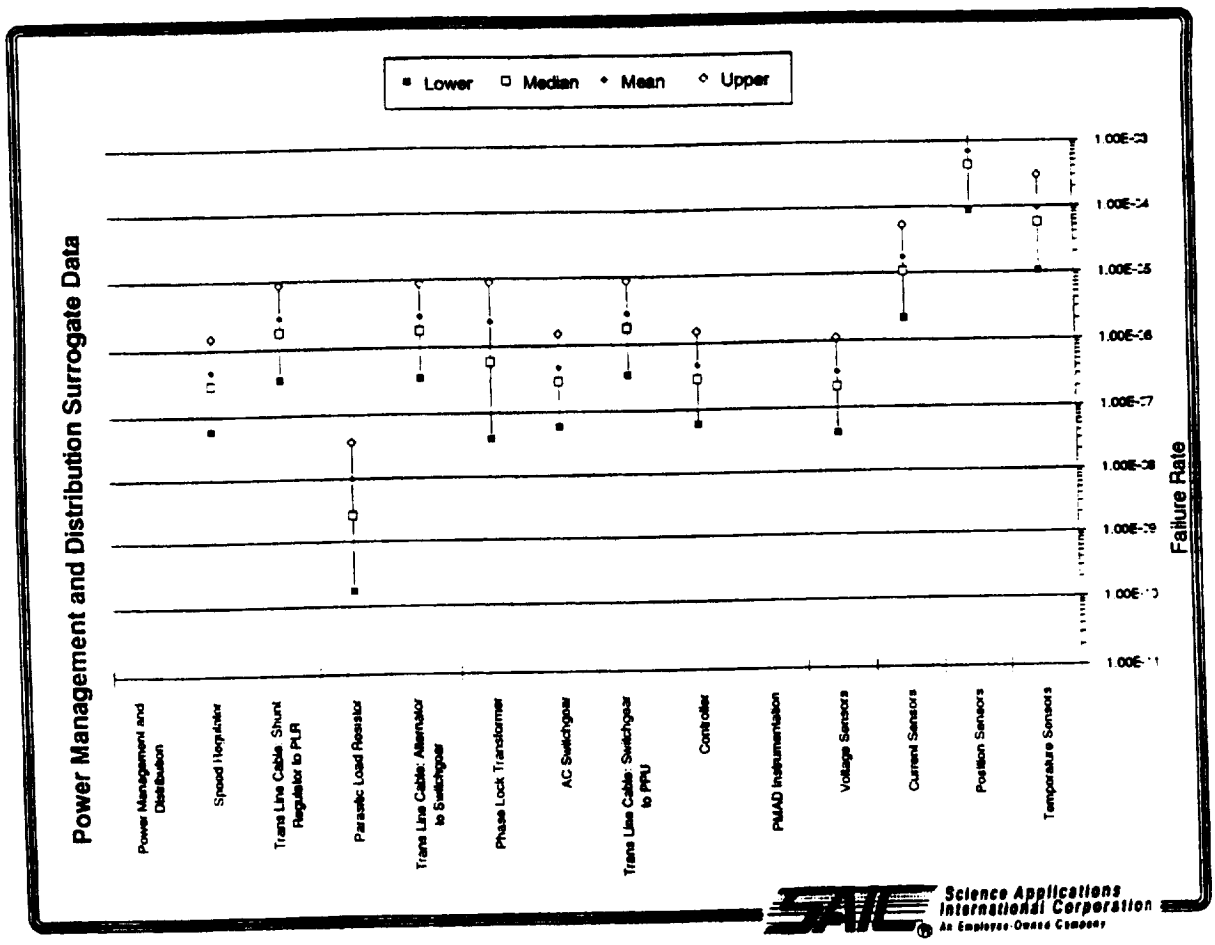
Surrogate failure rate distributions for components in the primary heat source loop.



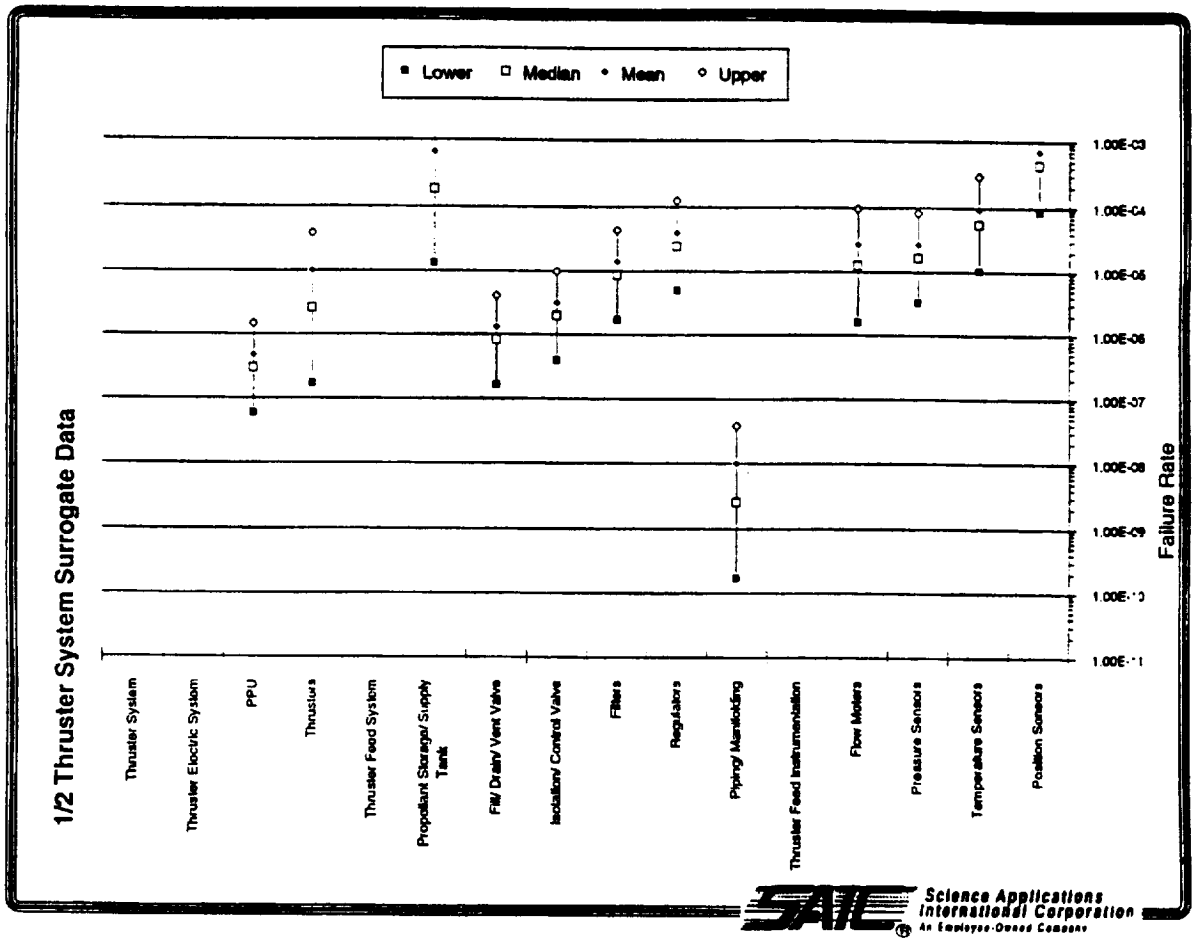
Surrogate failure rate distributions for components in the Auxiliary Thermal Management system..



Surrogate failure rate distributions for components in the Secondary Loop system.



Surrogate failure rate distributions for components in the Power Management and Distribution system.



Surrogate failure rate distributions for components in the Thruster module.

INTERPRETATION OF SURROGATE DATA NARROW SURROGATE DISTRIBUTIONS:

- Cause:
  - Little variability among components in class;
  - Little uncertainty in similarity between surrogate class and NEP application.
  - Generally mature, well understood component.
- Implication:
  - These components unlikely to change their nature through evolutionary design or wishful thinking.
- Candidate NEP components:
  - Valves, Cables, Switchgear, Sensors, Regulators, ...
- Required performance > attained performance?
  - Fundamental redesign of function.

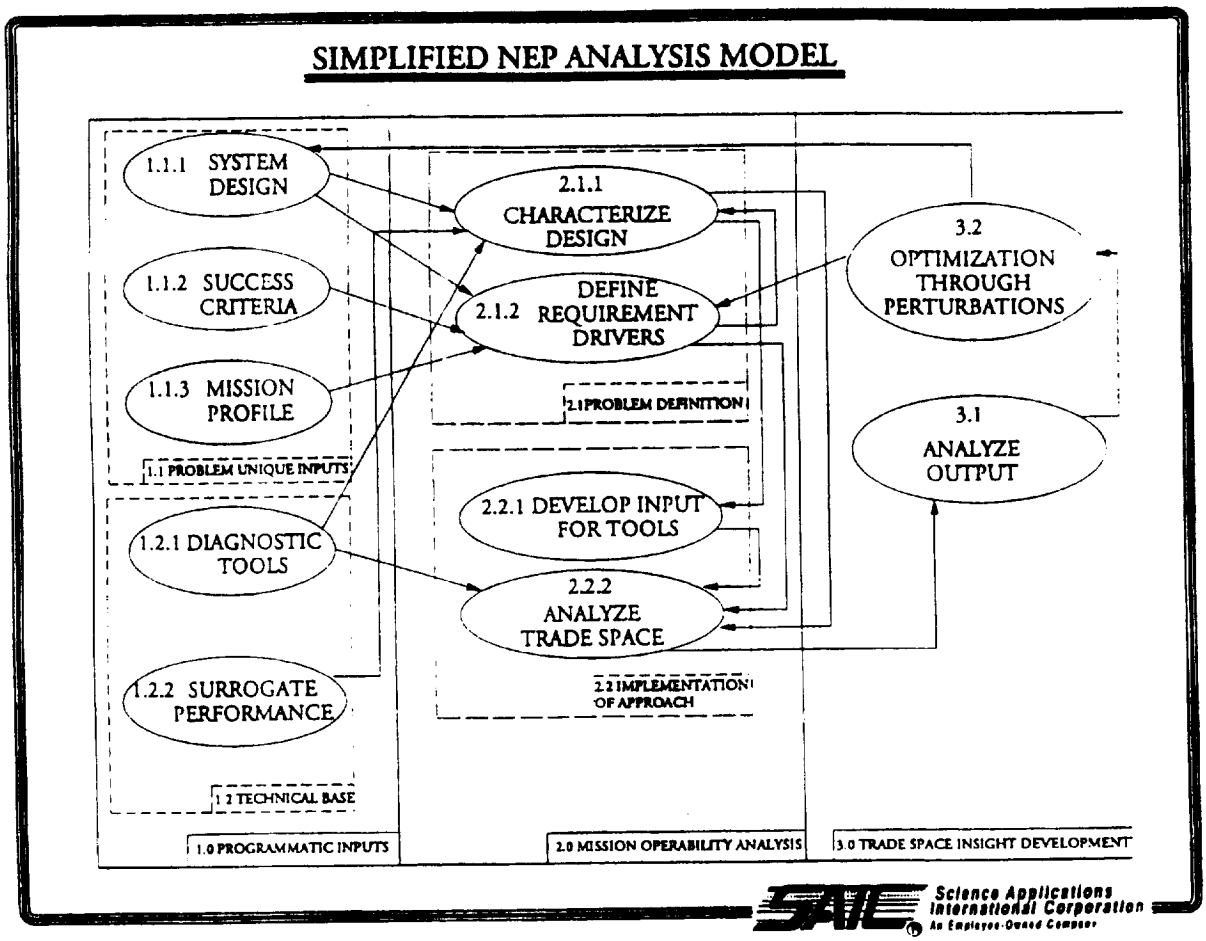
Narrow distributions in the surrogate data indicate that the component exhibits little variability in historical applications, and that there is little uncertainty in the application of this surrogate to the NEP application.

A narrow distribution is generally indicative of a mature component whose essential nature is well understood and generally not a good candidate for improvement in reliability, except through very fundamental redesign.

INTERPRETATION OF SURROGATE DATA BROAD SURROGATE DISTRIBUTIONS:

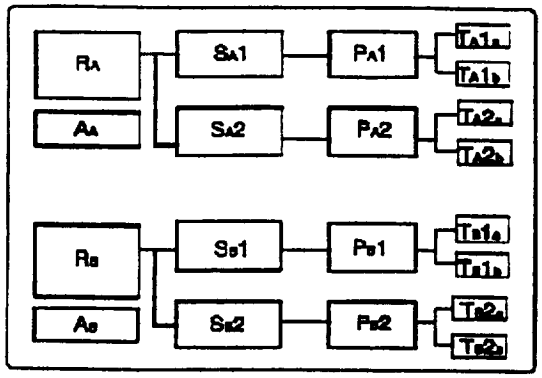
- Causes:
  - High variability in surrogate component population.
  - Significant uncertainty in applicability of surrogate data to NEP.
- Implication:
  - Requires close attention in design, specification, and selection.
  - High developmental risk.

Conversely, wide distributions of surrogate failure rates indicate significant variability, uncertainty, or both. Wide distributions indicate that this component may be a high risk item.

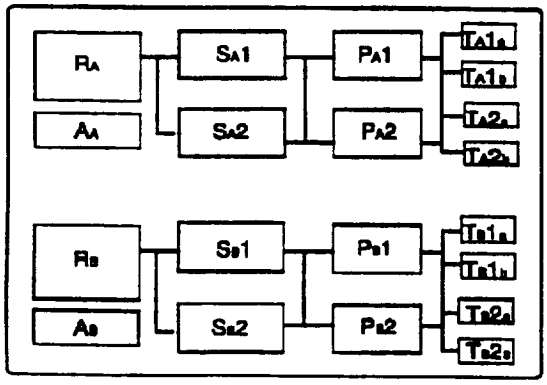


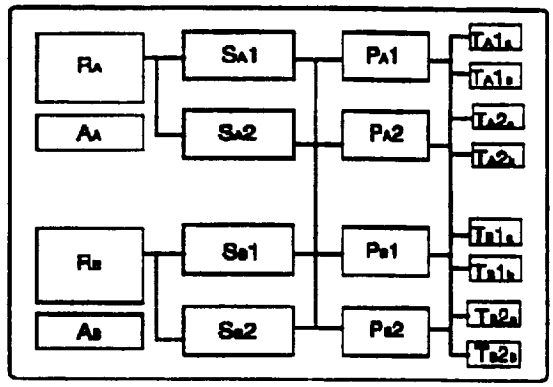
In the problem definition phase of the analysis, the first step was to characterize the design.

NEP MARKOV MODELS - PHYSICAL CONFIGURATION

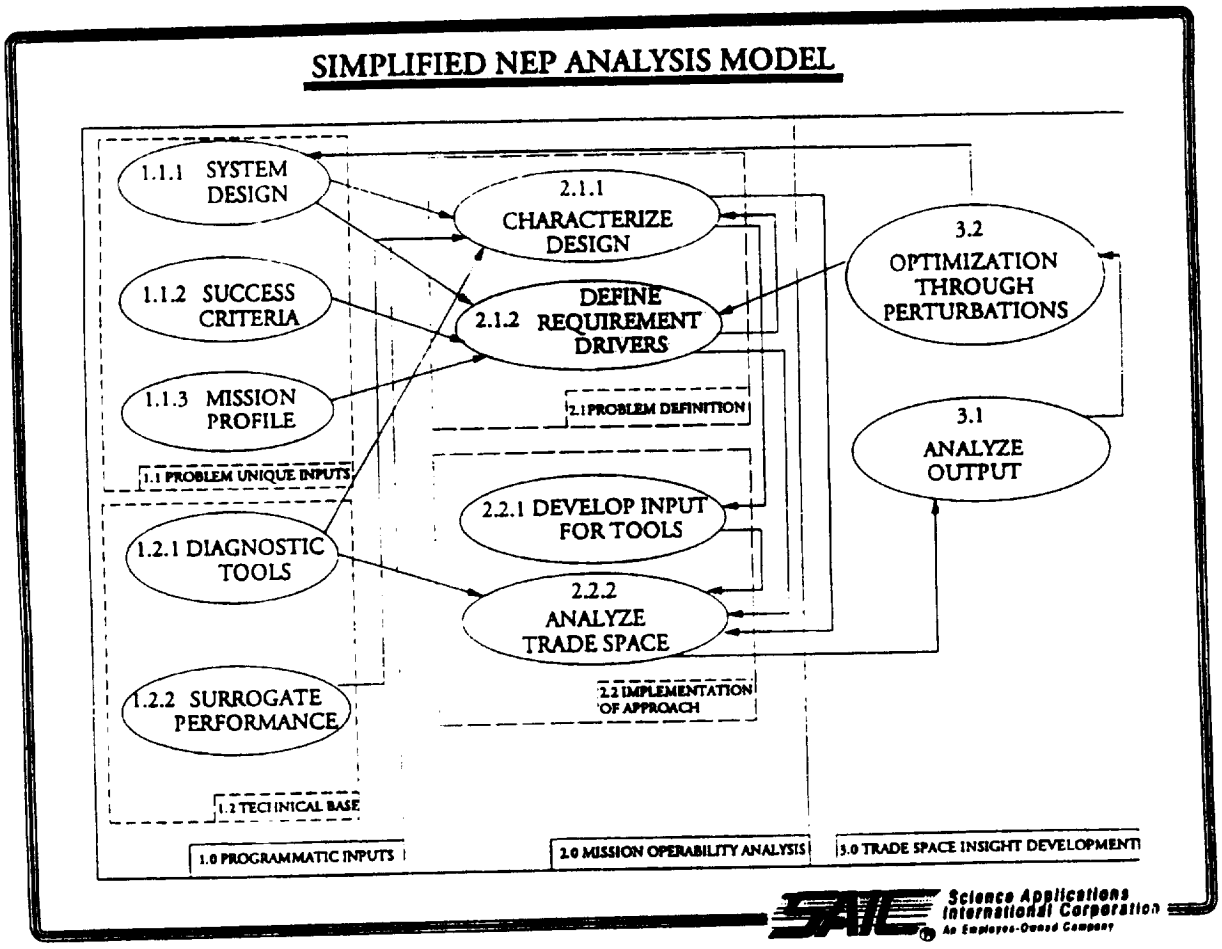


- Three physical configurations of basic model examined:
  - No Cross-Connection
  - Electrical Cross Connection w/in 5MWe module
  - Electrical Cross Connection accross 5MWe modules





There were essentially three different ways to functionally connect, or "wire" the basic design we were provided in the program input phase. Each of the connection strategies embodied a different level of inherent resiliency.



The next step in problem definition was to define the requirement drivers within the context of the model.

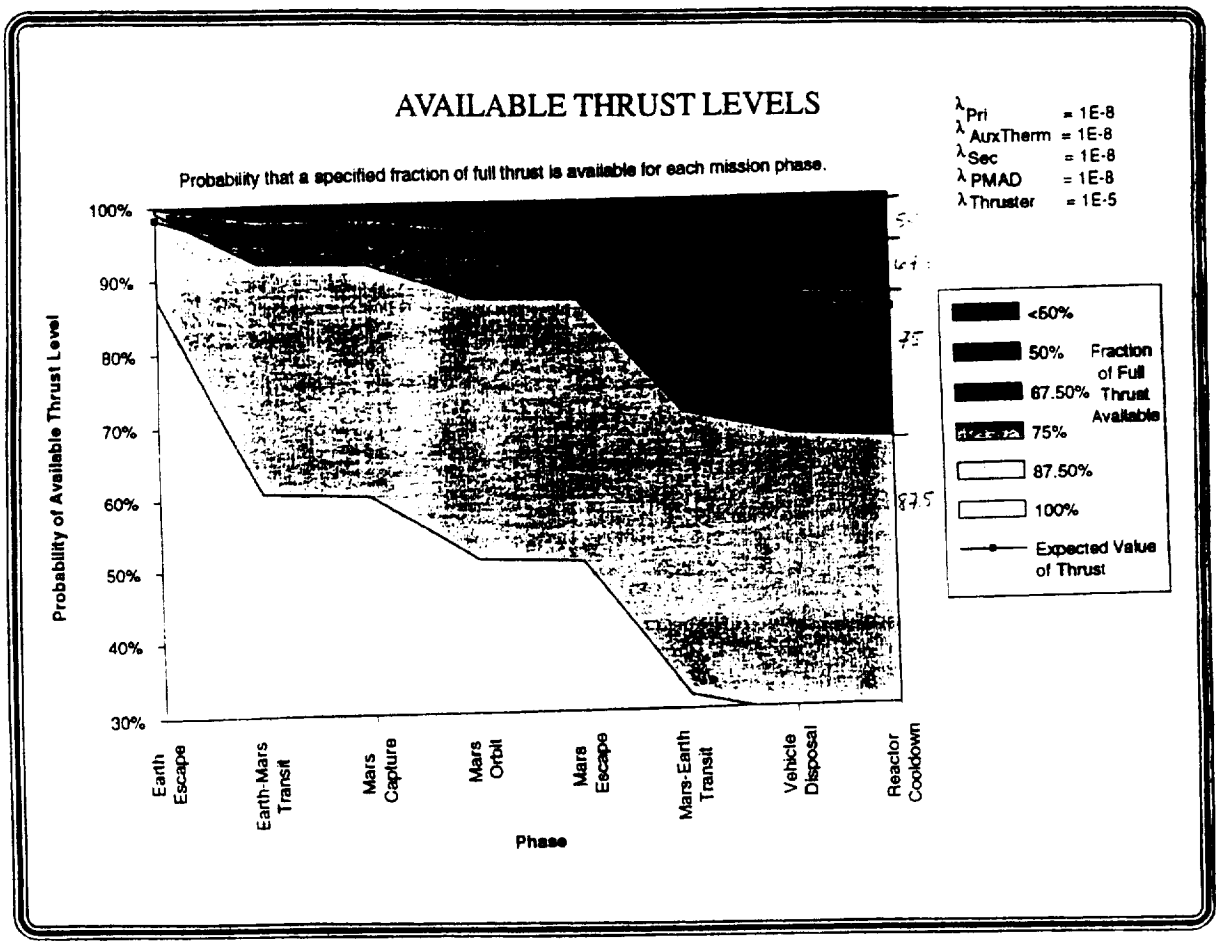
QUANTIFY SUCCESS CRITERIA

- Possible quantitative interpretations of success criteria:
  - Simple Reliability -
    - Probability that NEP system performs to specified capacity throughout mission > 0.99.
    - Specified capacity = Full capacity
    - Mission success and crew safety equivalent.
  - ⇒ Probability of available thrust > minimum thrust required.
    - Minimum thrust required varies with mission phase.
    - Minimum thrust to complete mission generally not equal to Minimum thrust for crew safety (abort).
  - Expected value of thrust.

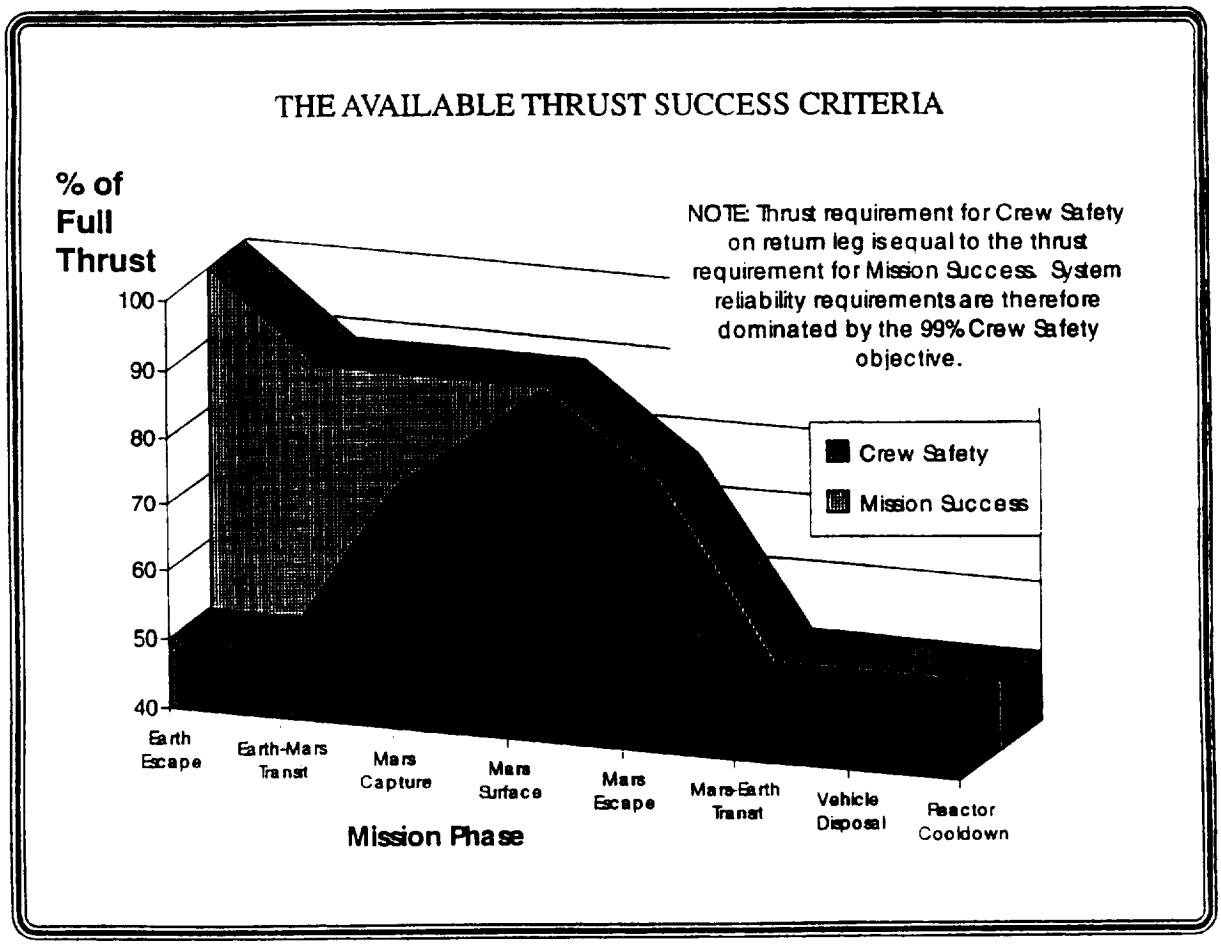
Science Applications International Corporation
An Employee-Owned Company

At least three different interpretations could be applied to the basic mission success criteria. The interpretation applied in this study was to determine the minimum thrust required in each phase of the mission for crew safety and for mission success, and to select reliability parameters so that the probability of achieving those levels of thrust was greater than 0.99 (crew safety) and 0.95 (mission success).

An important element of this interpretation is the idea that the thrust required to complete the mission successfully is not necessarily equal to the thrust required to return the crew safely.



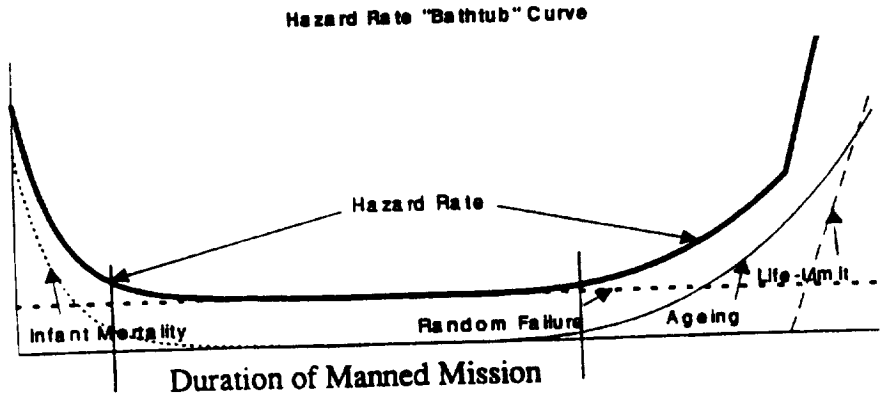
This graph depicts the probability that the NEP system will be able to deliver at least the indicated fraction of full thrust (100%, 87.5%, 75%, ...) as a function of mission phase, given the subsystem failure rates indicated in the upper right corner. These failure rates were chosen to produce an exemplary graph, not because the are realistic.



The preceding graph provided the probability that discrete levels of thrust would be available during each mission phase, half of the information required to determine the probability of meeting crew safety and mission success objectives. This curve show the other half of the information required -- specifically, what level of thrust is required in each phase to complete the mission and to ensure crew safety.

While these values were selected with some care, they are not the result of rigorous mission and orbit analysis. They are intended to represent a starting point for further investigation. Note that the values selected imply that the thrust required to ensure crew safety is the same as the thrust required for mission success throughout the return leg of the mission. The implication of this, if it correctly reflects the actual system, is that for most combinations of subsystem reliability parameters the 99% crew safety requirement dominates the 95% mission success requirement.

SELECTING RELIABILITY FIGURE OF MERIT

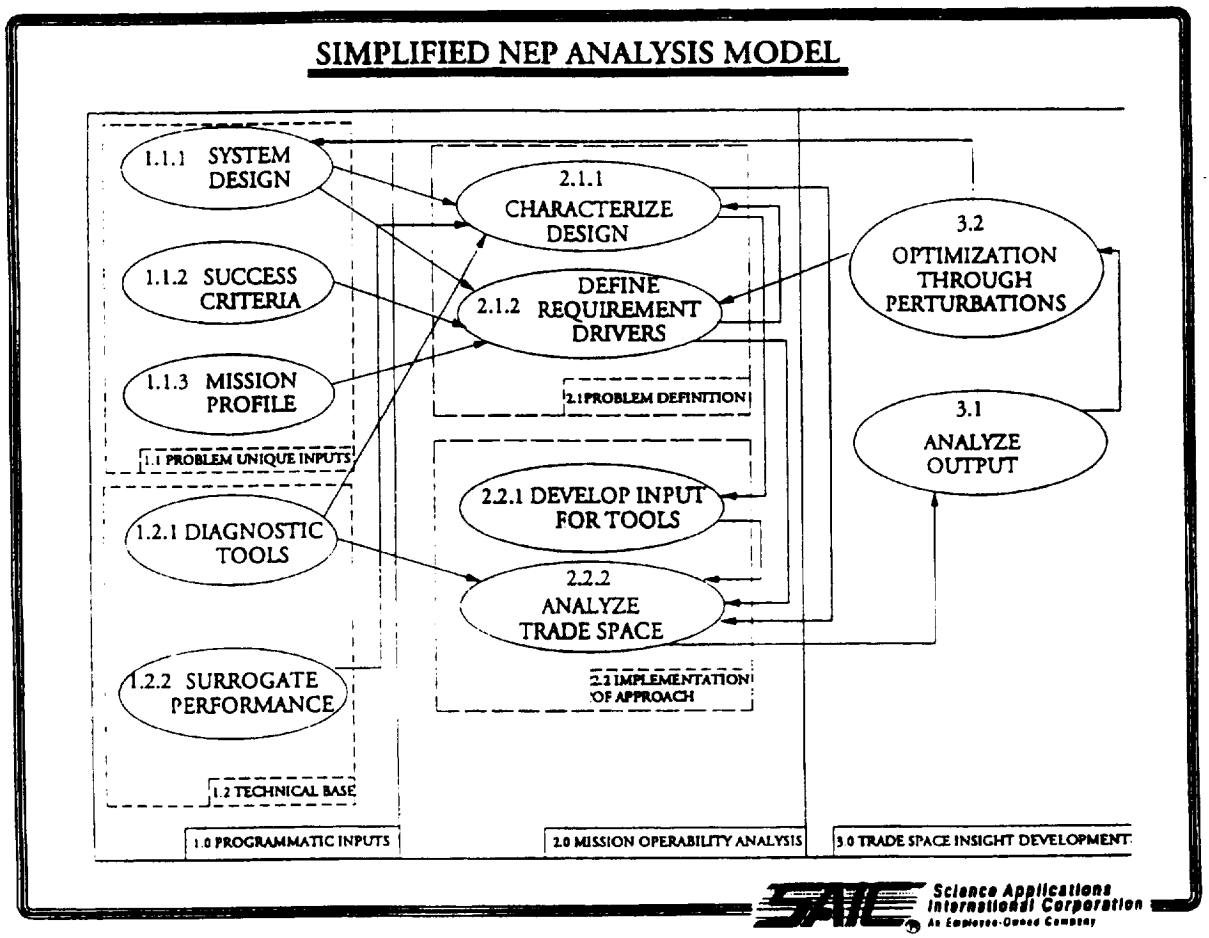


- Manned mission phases occur after Earth escape spiral "shakedown".
  - Infant mortality not an issue during manned phases.
- Sound design practice is assumed:
  - Crew return before ageing becomes issue.
- Reliability Figure of Merit = Random Failure Rate.

Science Applications International Corporation
An Employee-Owned Company

The rate at which failures occur is referred to as the hazard rate. In general, hazard rate is a time-varying quantity and is frequently separated into components which reflect the behavior of the hazard rate over time. These components are: (1) infant mortality, the hazard rate starts high and decreases over time as latent defects are "shaken out" of the new system; (2) random failure, the hazard rate is approximately constant; (3) aging, hazard rate increases as components weaken; and (4) life-limit, hazard rate increases rapidly (to 1) for components with a deterministic, observable depletion mechanism.

The constant random failure rate was the only component of hazard rate analyzed in this study based on the assumption that the manned portion of the NEP mission would occur in that domain.



The next phase in the analysis was to develop the inputs for the selected tools.

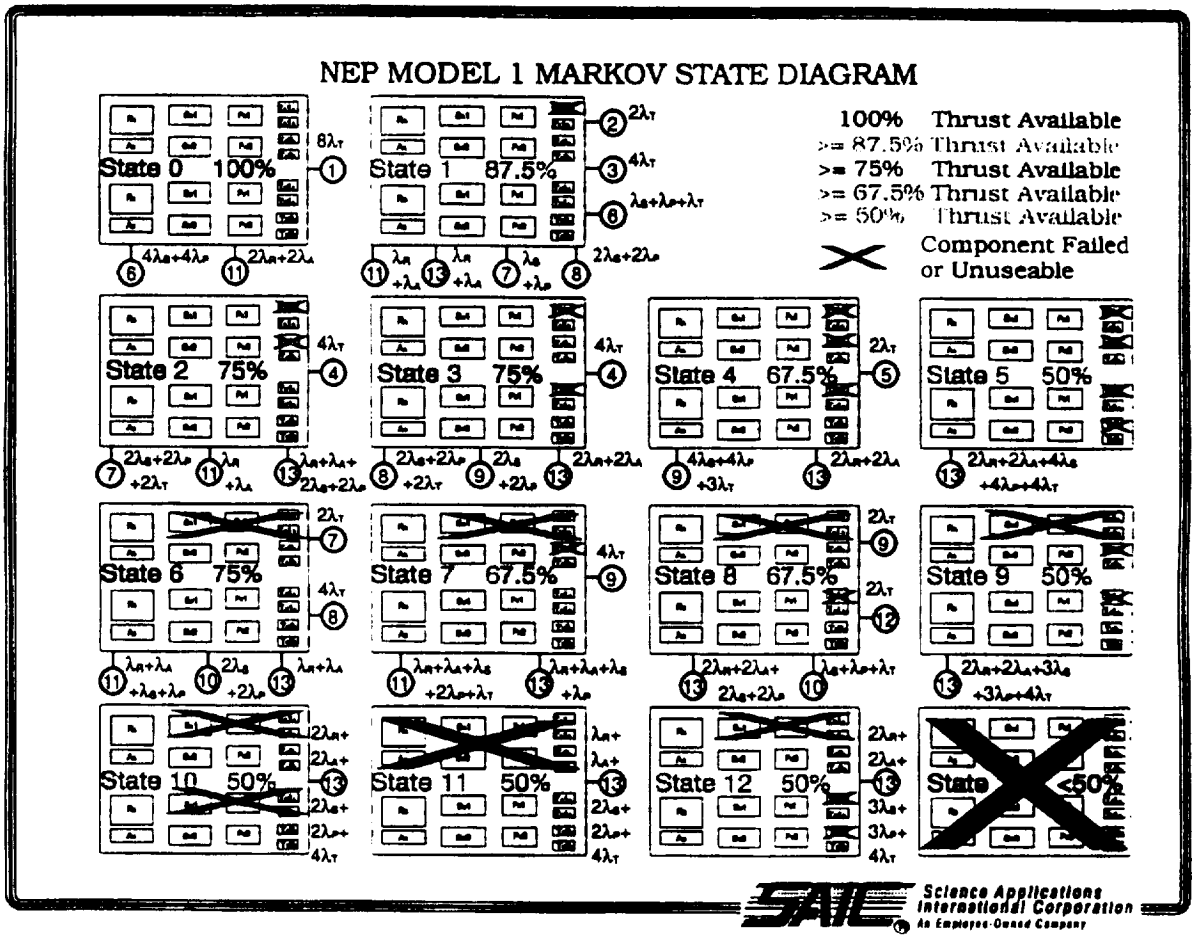
DESIGN ALTERNATIVES TESTED

NEP Model Number Achi Static Reliab	Minimum Thrust Required in Limiting Phase				Min Equip. List	Repair / Salvage
	87.5%	75.0%	67.5%	50.0%		
No Cross Connection	1	2	-	-	1MEL	4
Electrical Cross Connection Within 5 MWe Module	5	5T	-	-	-	-
Electrical Cross Connection Between 5 MWe Modules	6	6T	-	-	-	-
Fluid / Mechanical Cross Connection Between 5 MWe Modules	-	-	-	-	-	-
Minimum Equipment List Approach to Safety	1MEL	-	-	-		
Reparable / Salvageable System	4	4T1	4T2	4T3		

- Matrix of achievability analysis experiments.
- Cells contain:
  - Experiment Number

Science Applications International Corporation
An Employee-Owned Company

Although the analysis was limited to a single core design concept, a wide variety of perturbations or interpretations of the design could be applied. This matrix depicts the alternatives that were analyzed.

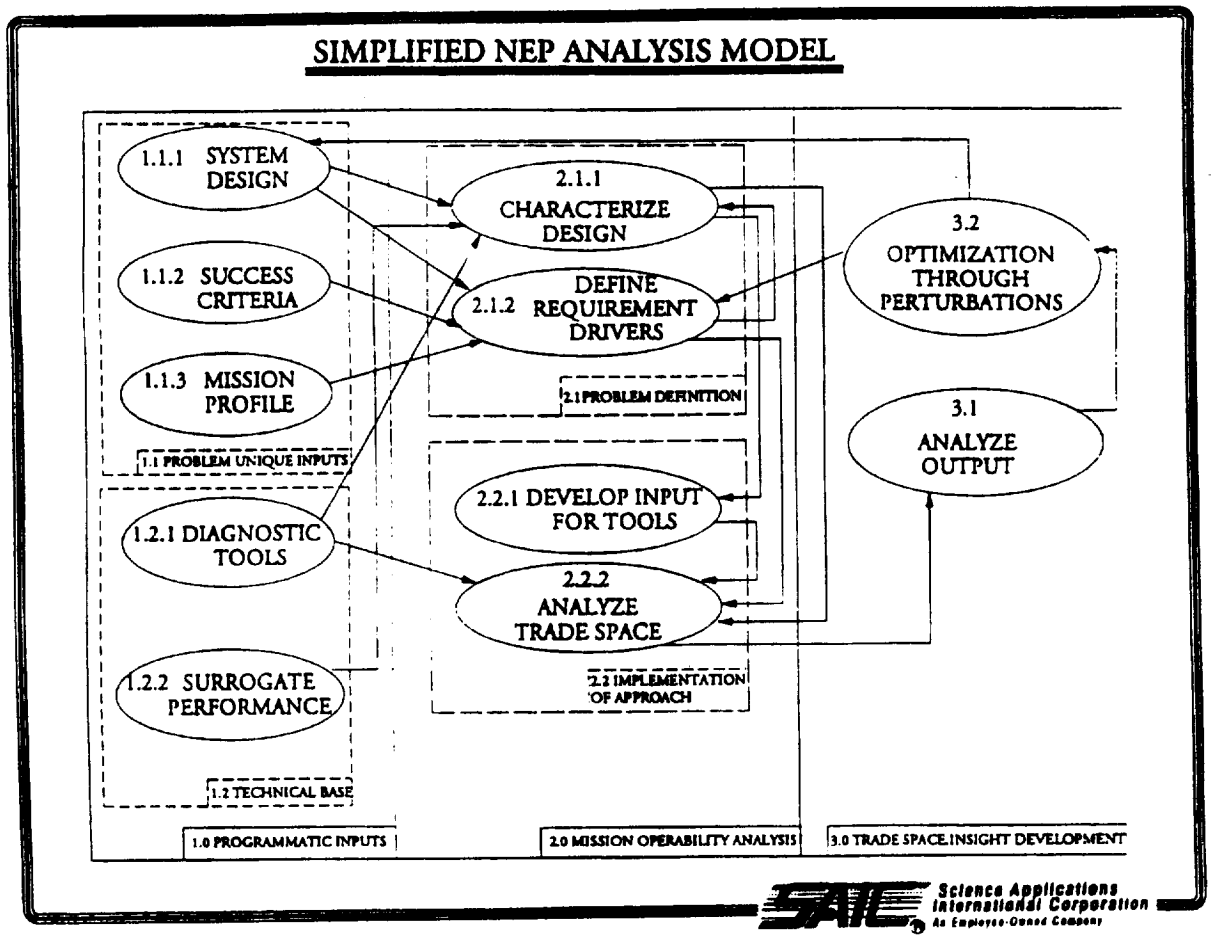


The simplest analytical model of the system allowed no cross connection between subsystems on different legs within a 5MWe module, or across modules. This diagram depicts the system states used in the Markov analysis for this model.

State 0 depicts the system with all modules operational. State 1 is the system with a single failed thruster module, state 2 has two failed thrusters - one in each leg of the same 5MWe module. For this analysis all conditions resulting in less than 50% of total thrust available were lumped into the same state, since we assumed that all such states led to mission failure and loss of the crew.

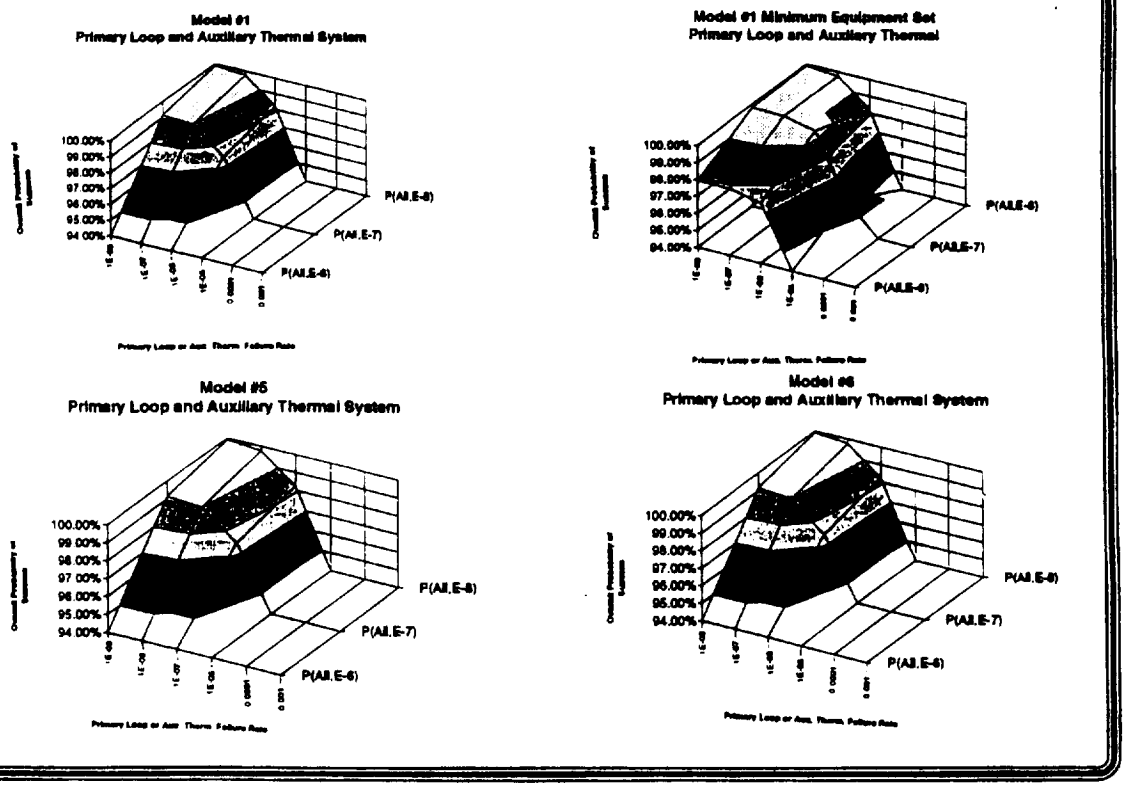
The rate at which this system (model) transitions from one state to another is indicated in terms of the failure rates of the subsystems. Ultimately, the Markov analysis is used to find the set subsystem failure rates that result in the success criteria being met. The thrust levels associated with each system state are also indicated on this diagram.

The other models are not depicted in this fashion because the number of states was too high.



The final step in implementing this study approach was to analyze the subsystem failure rate trade space resulting from the Markov analysis.

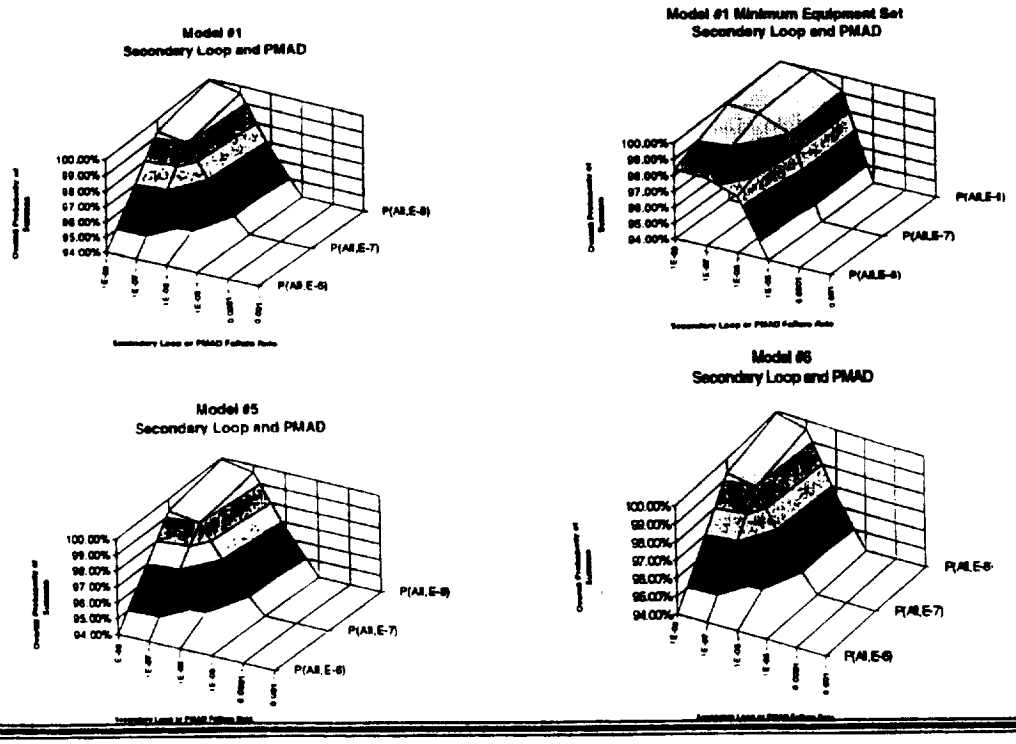
Primary and Auxiliary Model Comparison



The Markov model associates sets of failure rates with the probabilities that the system will be in each state at any time in the mission. Combining this with the knowledge of the thrust available in each state, and the thrust required for mission success and crew safety, we can determine the probability that the system will meet the success criteria as a function of the subsystem failure rates.

These graphs depict the "success probability" of the system as a function of the failure rate of the Primary Loop and the Auxiliary Thermal subsystems versus the failure rates of all other subsystems. Primary Loop and Auxiliary Thermal are lumped together because if either fails, the system is reduced to 50% thrust capacity -- a failure in any mission phase. This means that the Primary Loop and Auxiliary Thermal subsystems are equally important to the system -- from the success requirements point of view their failures are indistinguishable -- therefore the successful failure rates associated with them are the same. The different graphs depict different models which vary primarily in the arrangement of interconnections. Note that the failure rates required for the Primary and Aux. Thermal subsystems is essentially independent of the degree of interconnection, since any failure of these systems results in mission failure.

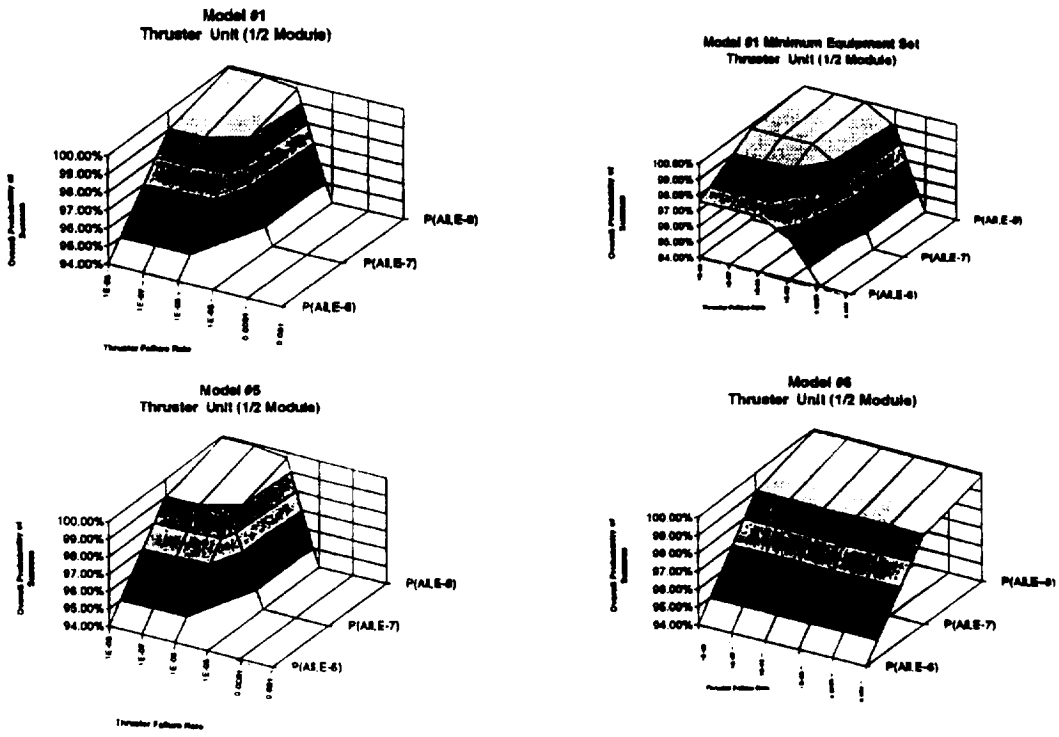
Secondary & PMAD Model Comparison



Like the Primary and Aux. Thermal subsystems, the PMAD and Secondary subsystems are of equal importance. Since a failure of either of these subsystems would reduce available thrust to 75%, and since (for these models) the thrust required for crew safety and mission success is 87.5% during the Mars escape spiral, any PMAD or Thruster failure prior to Mars escape would result in mission failure and generally (given the model assumptions) loss of the crew. The required failure rates for PMAD and Secondary given these model assumptions are therefore essentially the same as those required for the Primary and Aux. Thermal subsystems, very high, and independent of degree of interconnection. We will show in other models which assumptions need to be relaxed to permit more reasonable failure rates for these subsystems.

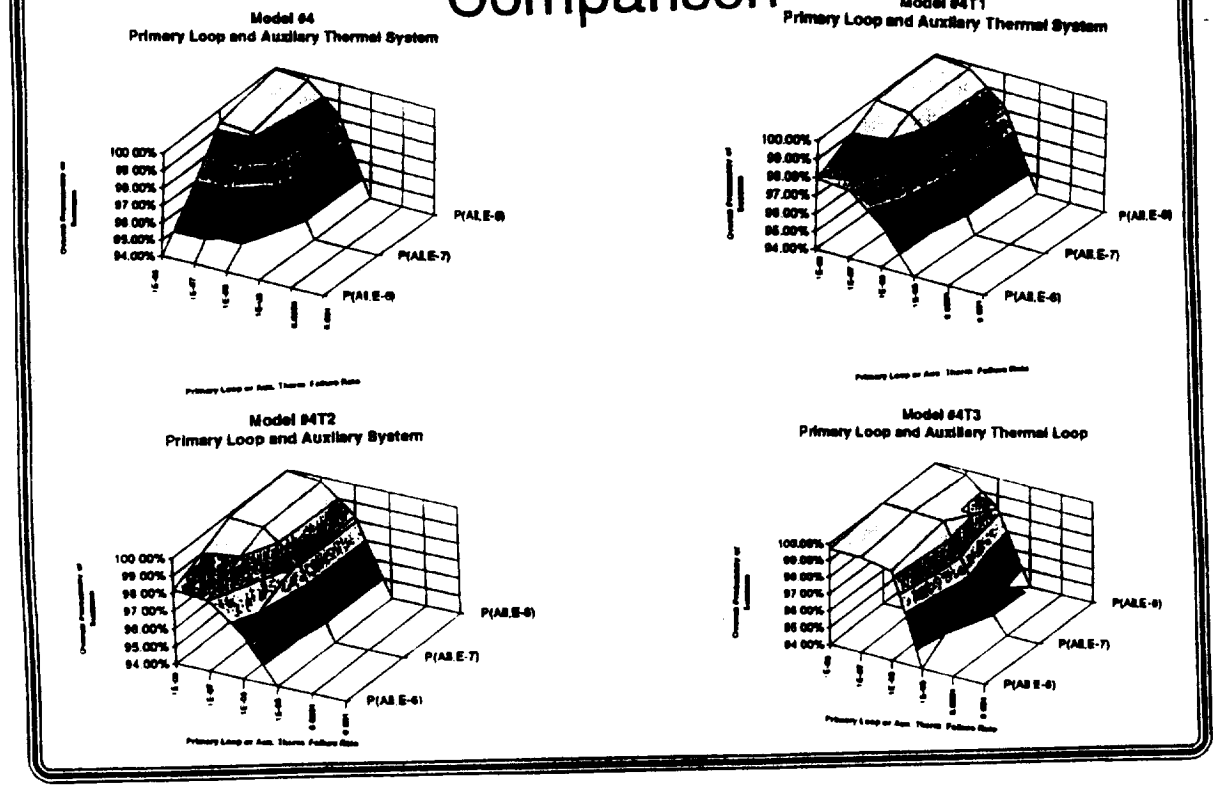
The Minimum Equipment Set model will be described later, but it should be noted here that in that model the 95% mission success criteria generally dominates the 99% crew safety requirement, so the set of "successful" failure rates in that model are those that result in "Overall Success Probability of >95%, rather than 99% which is the case in the other models.

Thruster Model Comparison



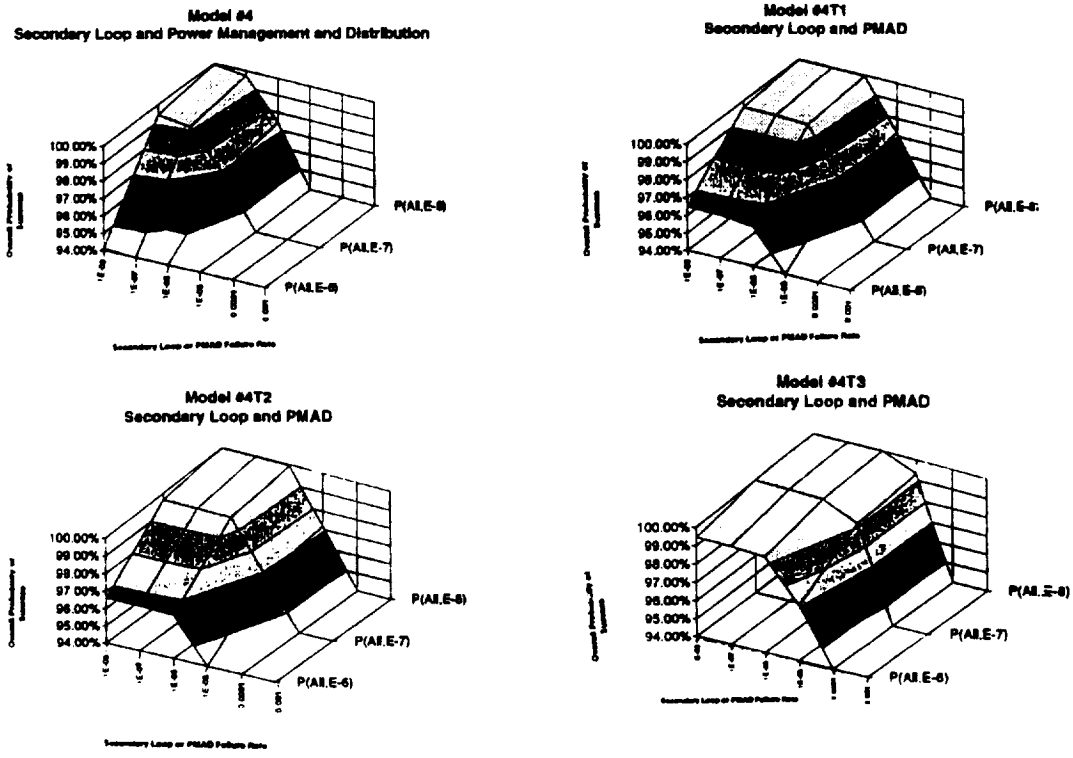
Thruster failures only remove 12.5% of the full thrust capacity, so a single failed thruster results in a successful system state at any phase of the mission, and in most phases, several Thruster failures can occur and still result in mission success. Thrusters are also very sensitive to the degree of interconnection between components.

Model 4 Primary and Auxiliary Thermal Comparison



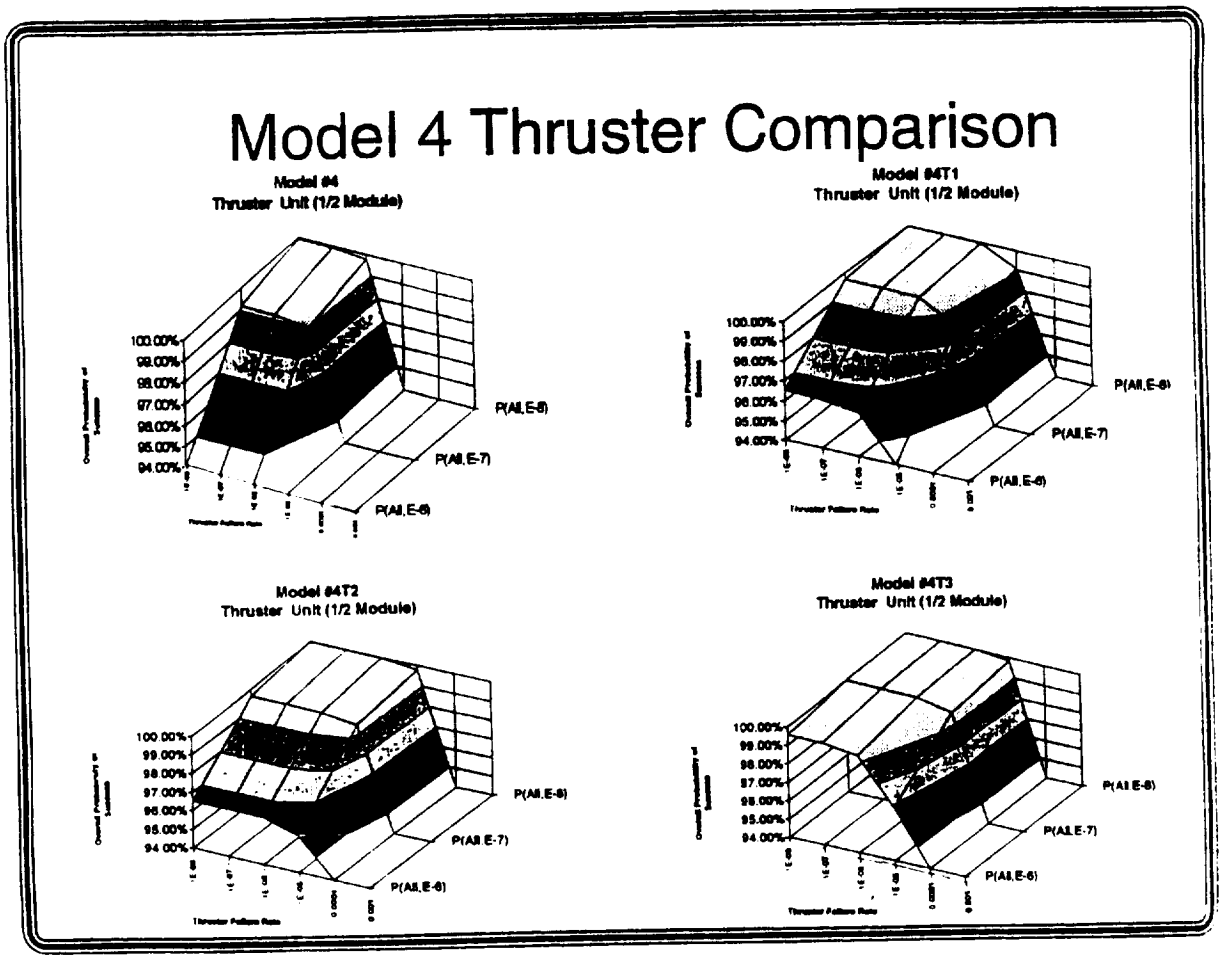
In Model 4 some degree of repair or salvage is allowed in systems other than the Primary, specifically, 25% of the first failures that occur in those subsystems are assumed to be repairable, and all the second failures are repairable, since one of the two failed systems could be used to salvage the other. The different models depicted here show the impact of lowering the highest minimum thrust requirement from 87.5% (Model 4) to 50% (Model 4T3) in 12.5% increments.

Model 4 Secondary & PMAD Comparison



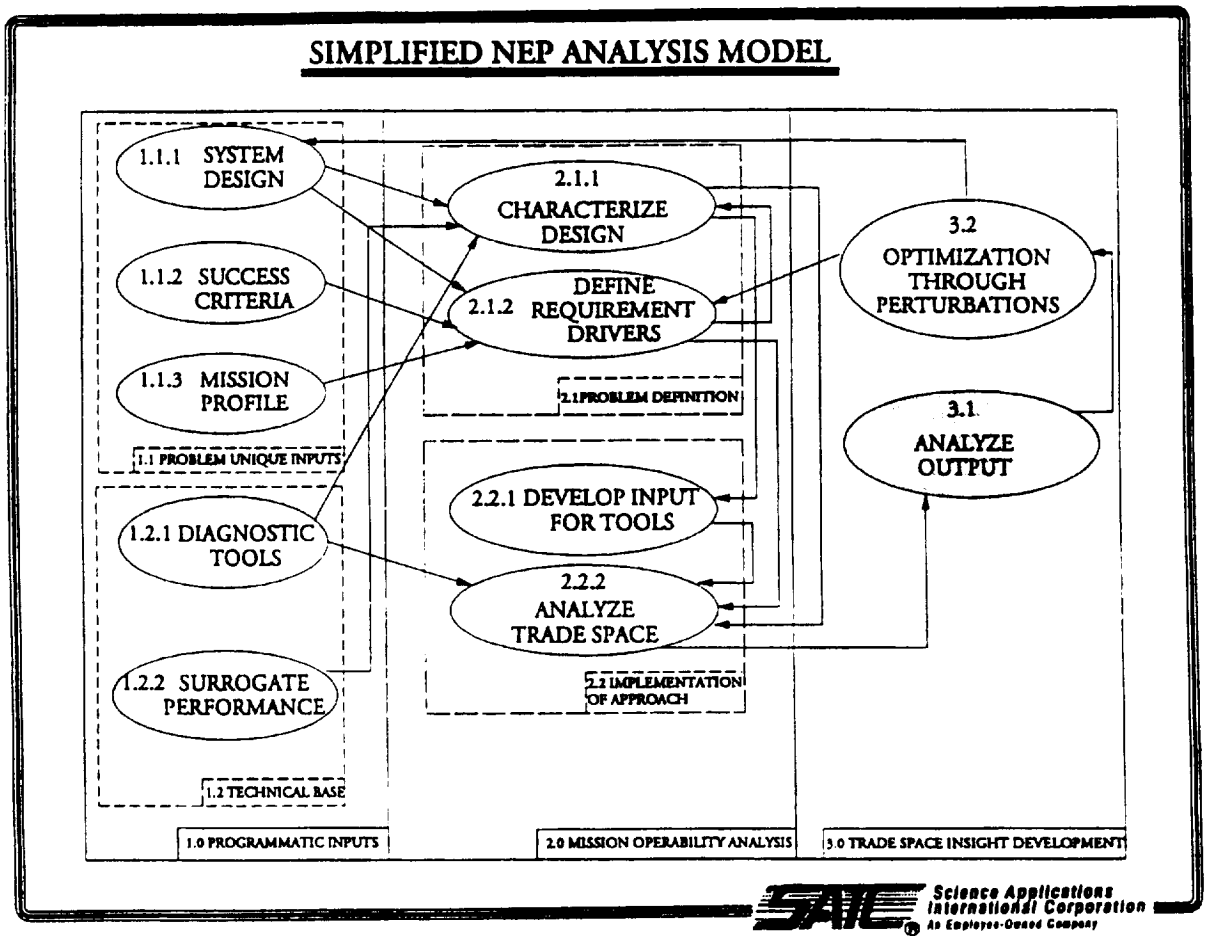
The benefit of reducing the minimum thrust requirement to thresholds which allow the failure of a subsystem without causing system failure are evident in these graphs. When the required thrust is reduced from 87.5% to 75% the required failure rates for Secondary and PMAD subsystems are reduced by an order of magnitude. Further reduction to 67.5% results in no change since Secondary and PMAD failures reduce available thrust in 25% increments. Reducing the required thrust to 50% gains another order of magnitude in required failure rate.

Model 4 Thruster Comparison



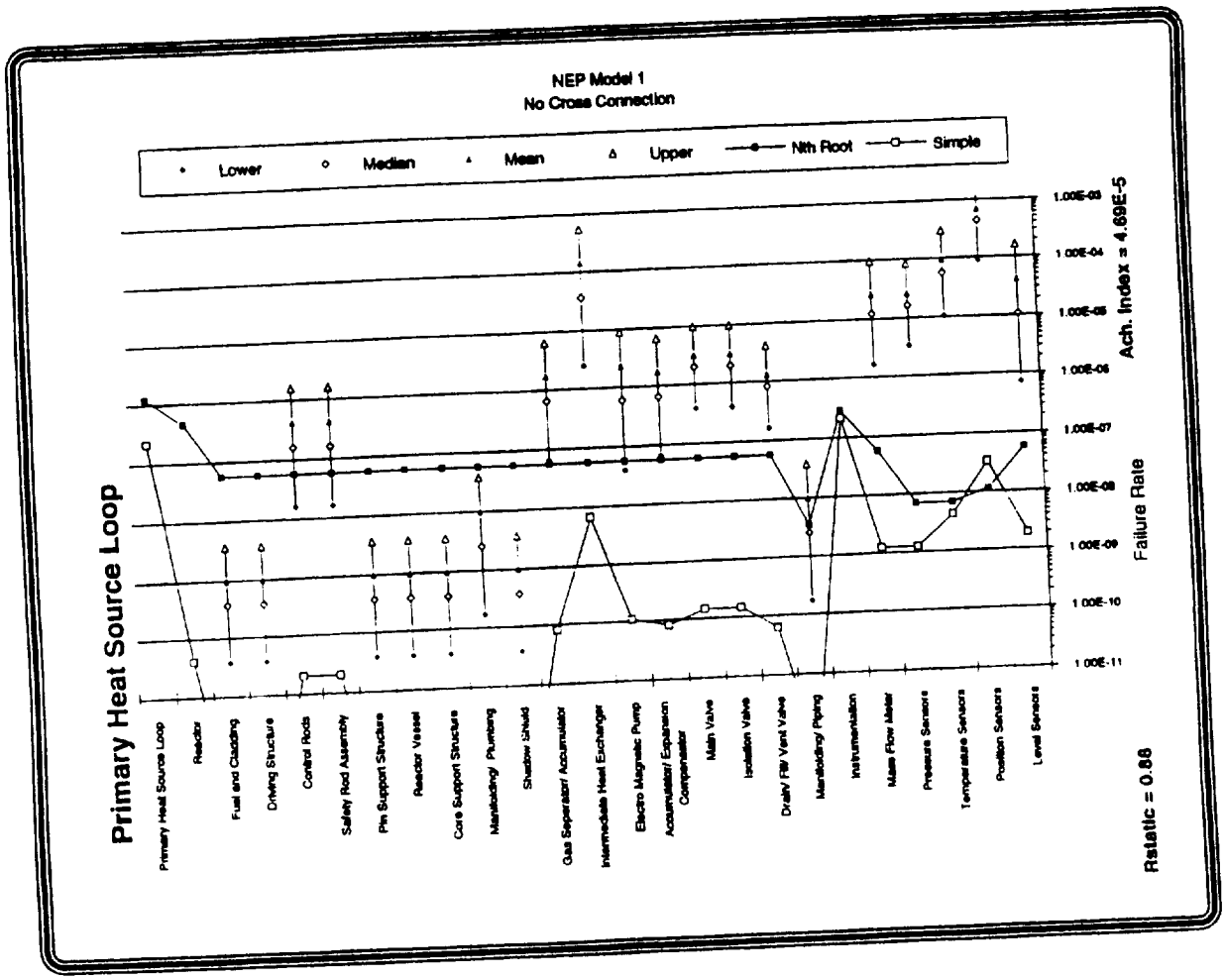
Like the Secondary and PMAD, required Thruster failure rates are significantly reduced as the maximum required thrust is reduced. Since Thruster failures only remove 12.5% of the total thrust capacity, each 12.5% reduction in required thrust has an associated relaxation of Thruster failure rate requirements.

Physically the effect of reducing the maximum required thrust in the model can be achieved without increasing the total power of the system. The reduction of thrust requirements corresponds to designing the Secondary, PMAD, and Thrusters so that they can operate at higher nominal loads. For example, if the Secondary and PMAD were designed to operate at 150% of nominal capacity, half of the failure impact of a unit could be absorbed by the other unit in the 5MWe module. Instead of reducing the thrust capacity of the system by 25%, the failure of a Secondary or PMAD would only reduce the capacity by 12.5%. Similar gain is achieved by designing the Thruster module to operate at 125% of nominal capacity. This effect is enhanced by maximizing the cross-connectivity between subsystems.



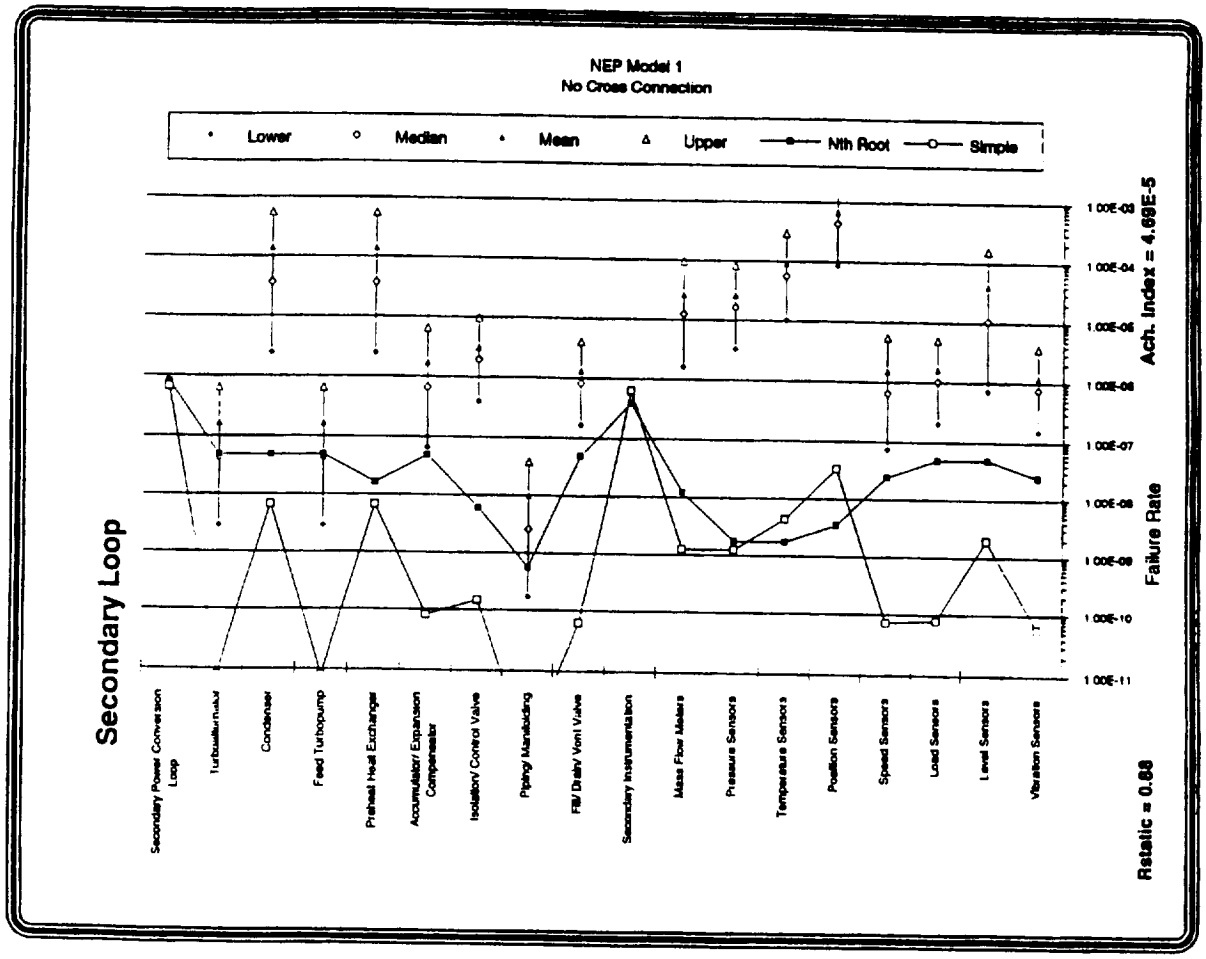
To complete the analysis the sets of subsystem-level failure rates which meet the success criteria are apportioned down to the component level for comparison with surrogate data. The RAP2™ computer code is used to accomplish this apportionment. Only two of the RAP2™ apportionment algorithms (the Simple algorithm and the Weighted Nth Root algorithm) were applied in this analysis to establish the bounds within which component failure rates would need to lie in order for the system to achieve the success criteria. The Simple algorithm establishes the worst case bound, and the Weighted Nth Root method, the best case.

A complete analysis would extend the material presented here in two respects. First, an "optimum" set of component failure rates would be sought by seeking the set of requirement driven subsystem level failure rates which minimize the aggregate achievability index (AchI). This would require extensive iteration which was not possible in this analysis. Second a distribution of apportioned failure rate and AchI would be developed, rather than the mean values presented here. The apportioned failure rates presented here are a solution, but by no means the best solution, to the problem.

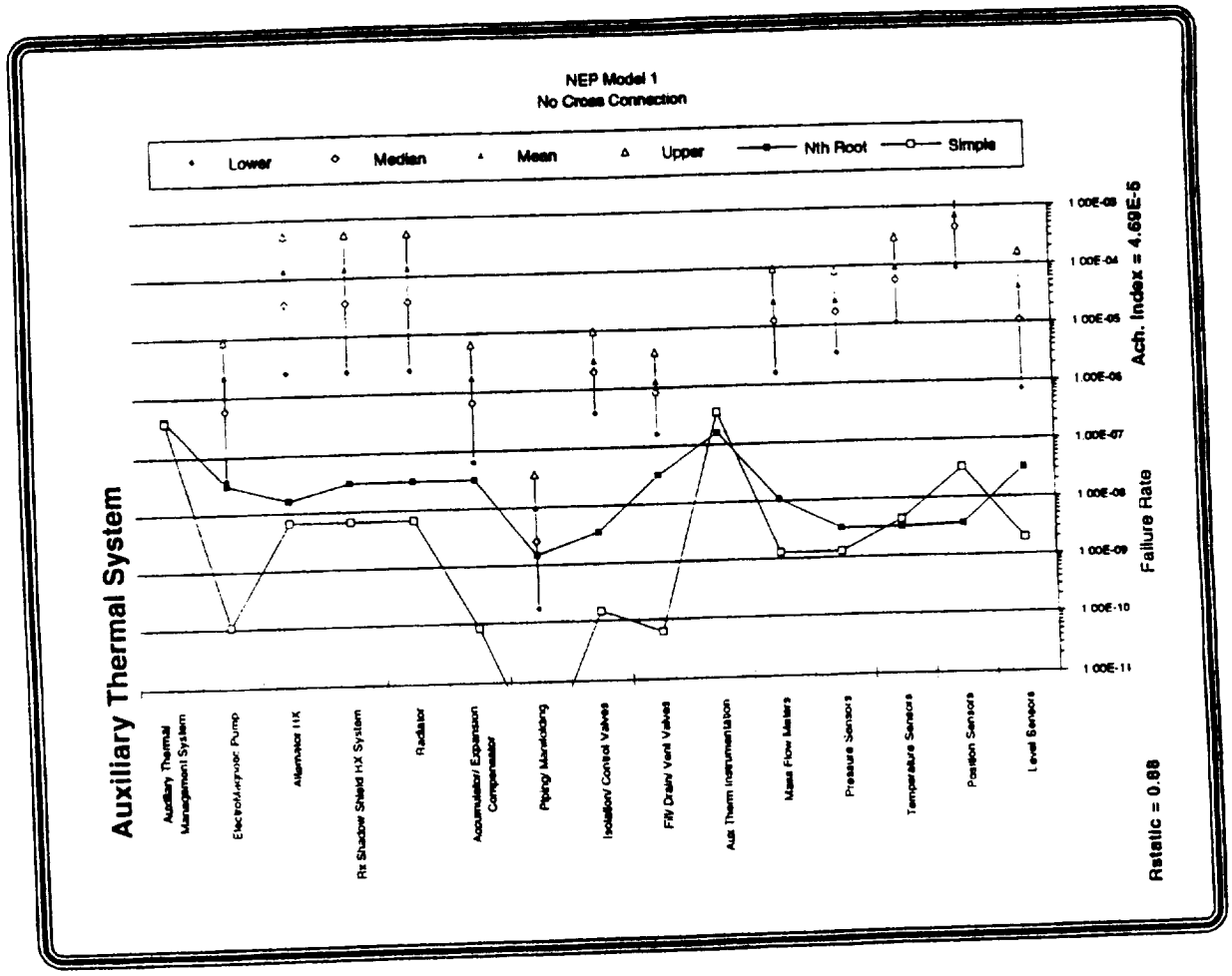


This graphic depicts the apportioned failure rate values for the Primary Loop subsystem along side the surrogate distributions obtained from the historical performance of similar components. The achievability index (AchI) is represented by the distance between the surrogate distributions and the apportioned values. The point estimate of AchI for this model in the upper right corner is the ratio of the Simple method apportioned values to the mean of the surrogate distributions. This value is essentially an outer bound on the achievability of the system for Model 1.

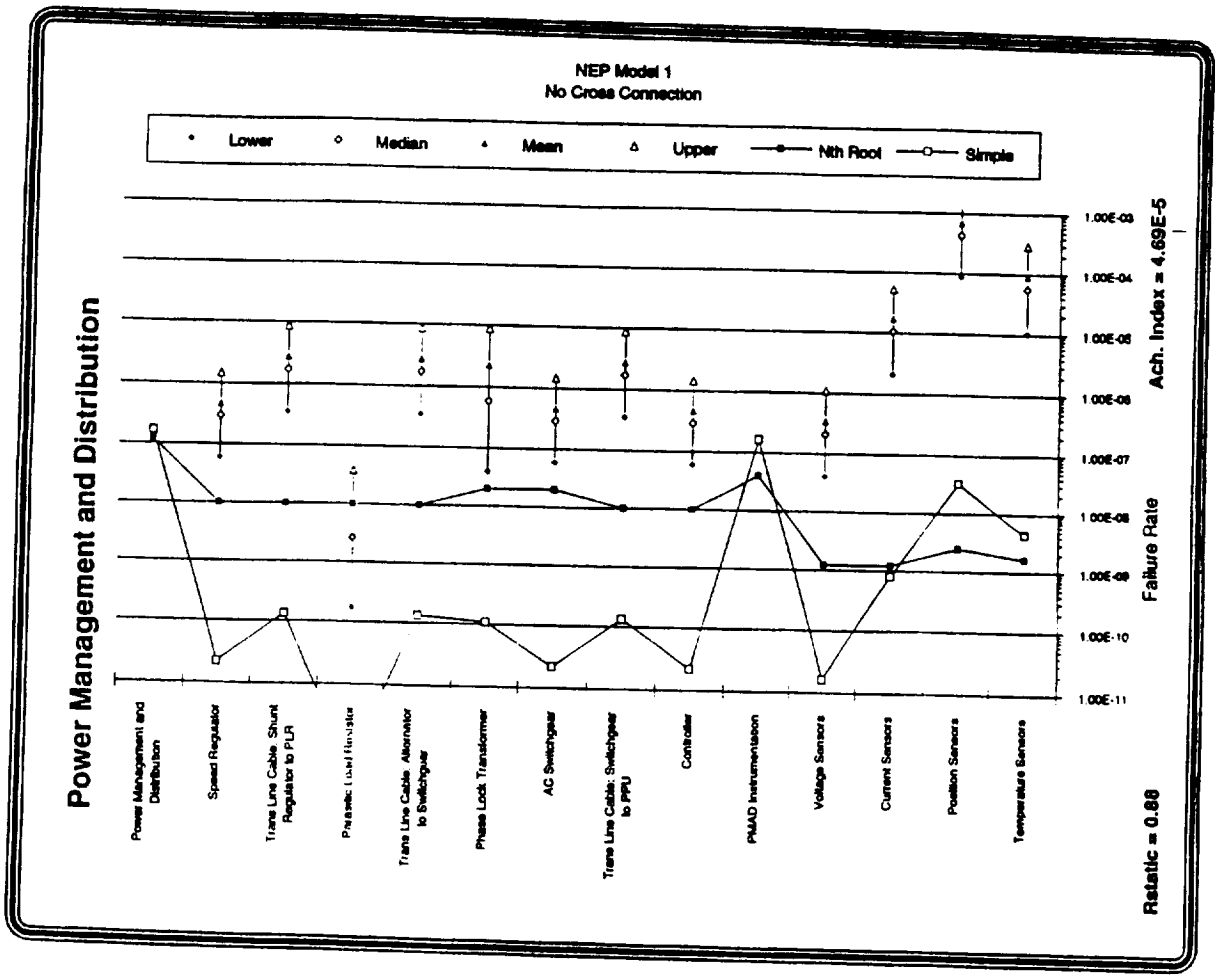
Model 1 was the simplest configuration analyzed, with no resiliency through subsystem cross-connection, and using the worst case (87.5%) required thrust criteria.



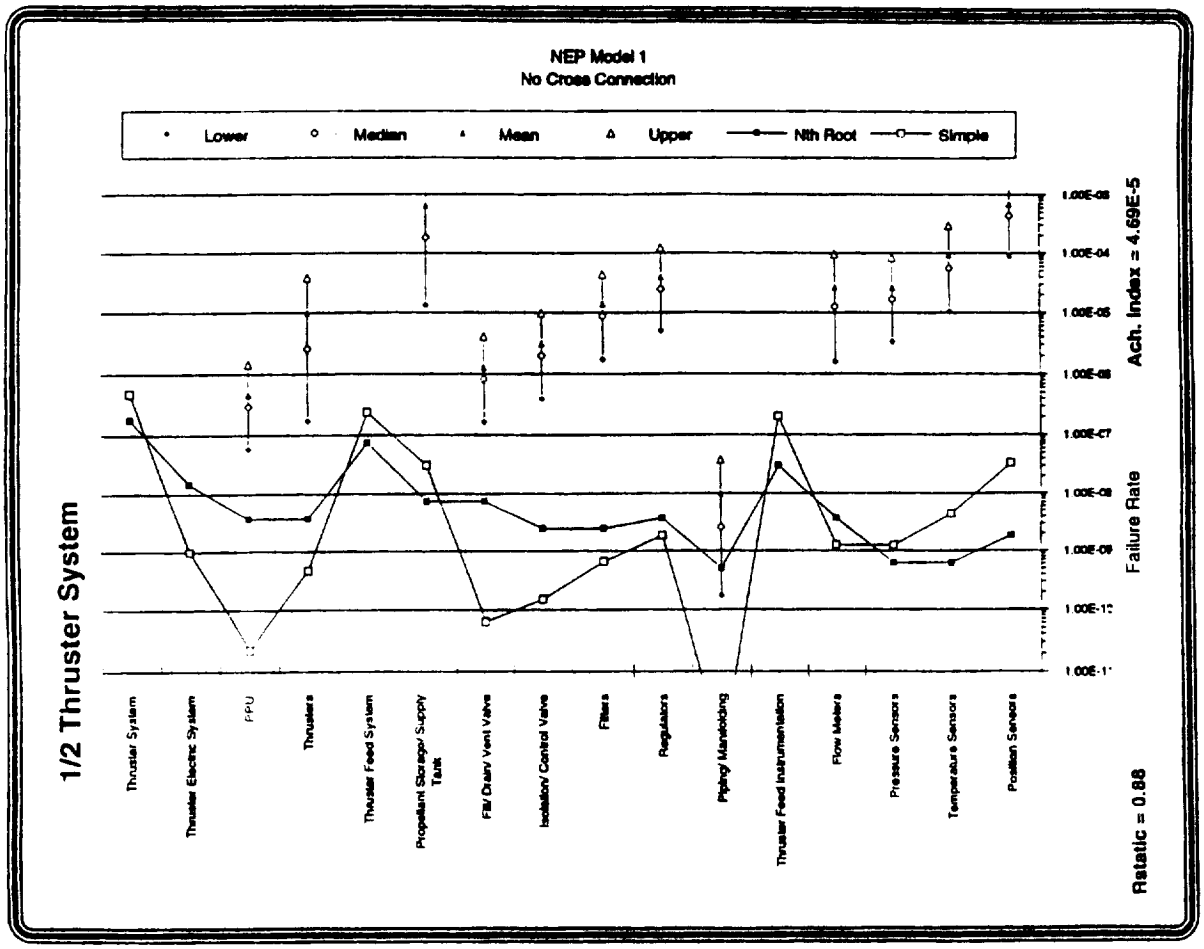
This graphic depicts the achievability of the Secondary system for Model 1. The distance between the Simple apportionment values and the surrogate distributions (the mean values of the surrogate distributions) is the same as it was for the Primary Loop subsystem. This will be true of all components because of the nature of the Simple algorithm. The Weighted Nth Root apportioned values are farther from the surrogates. This is a result of selecting a priori weighting values which indicated that, in general, high reliability would be more difficult to achieve in the Primary subsystem than in the Secondary.



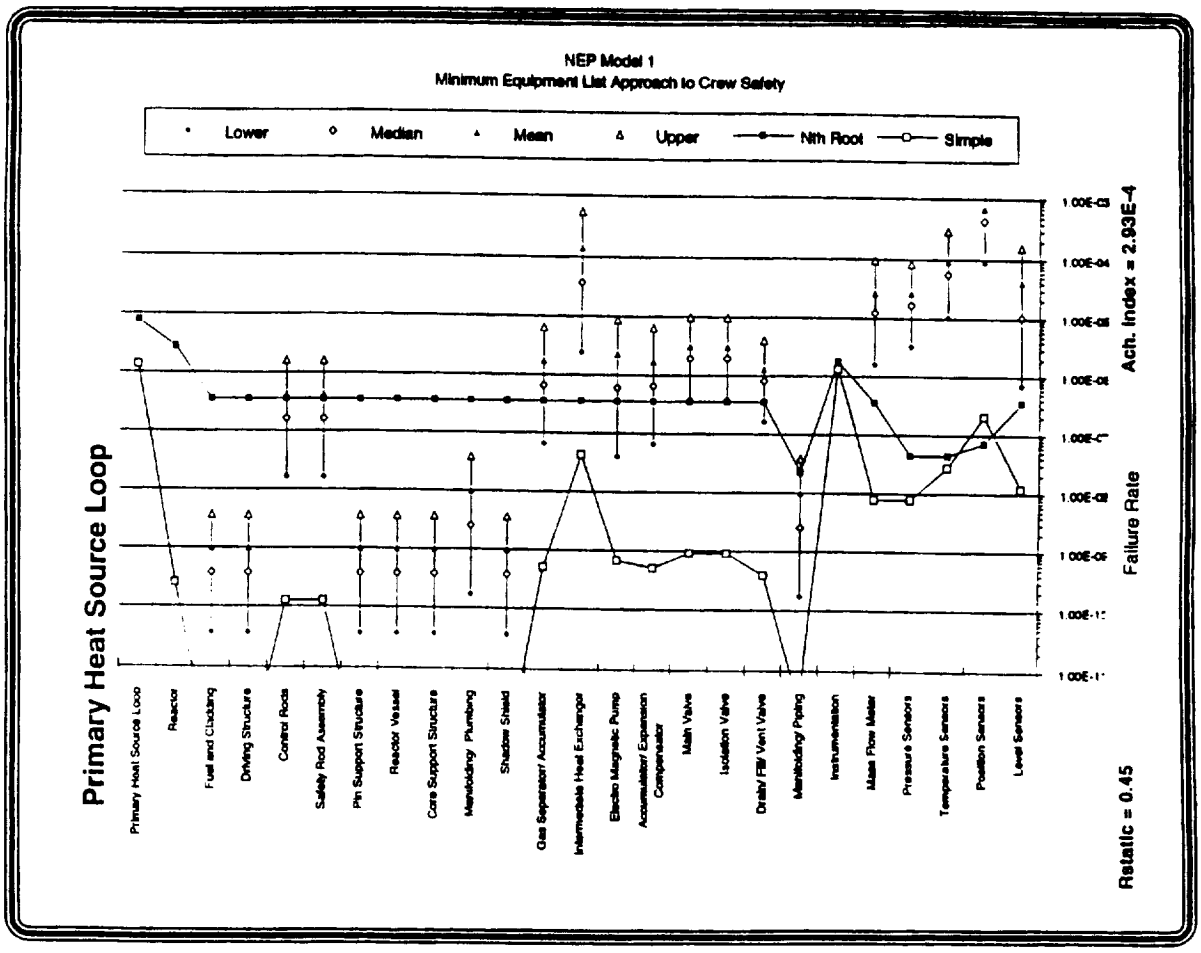
Note that the heat exchangers and the sensors in the Auxiliary Thermal system have significantly higher surrogate failure rates than is required. Also, the sensors have fairly tight distributions, indicating that these are probably fairly mature components with little variance or uncertainty in applicability. These factors indicate that these components should receive special attention. This is particularly true of the sensors, which are found in every subsystem. Sensors are discussed in more detail later.



Sensors, particularly the position sensors, appear to be the limiting PMAD component.



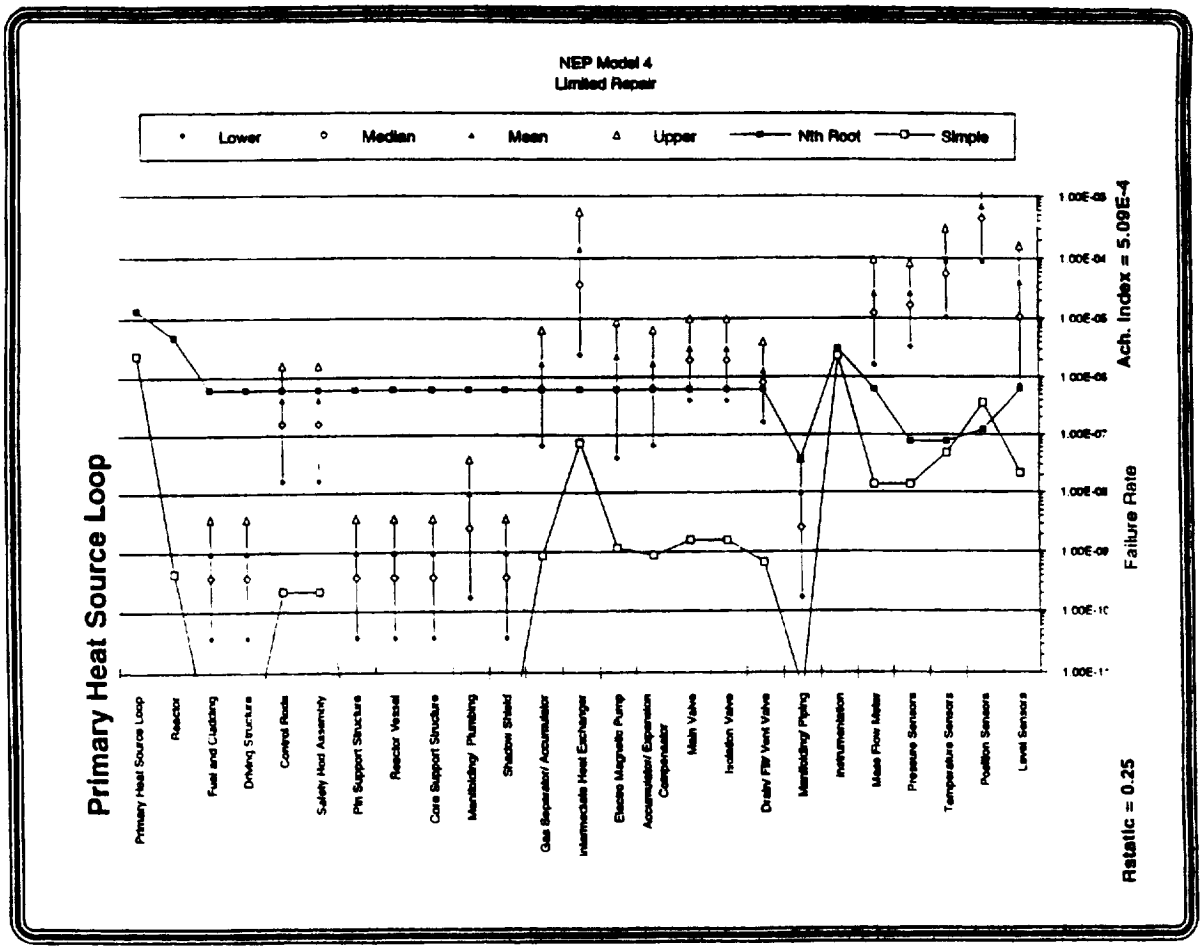
The Thruster Feed System, sensors, filters and regulators are the limiting Thruster components.



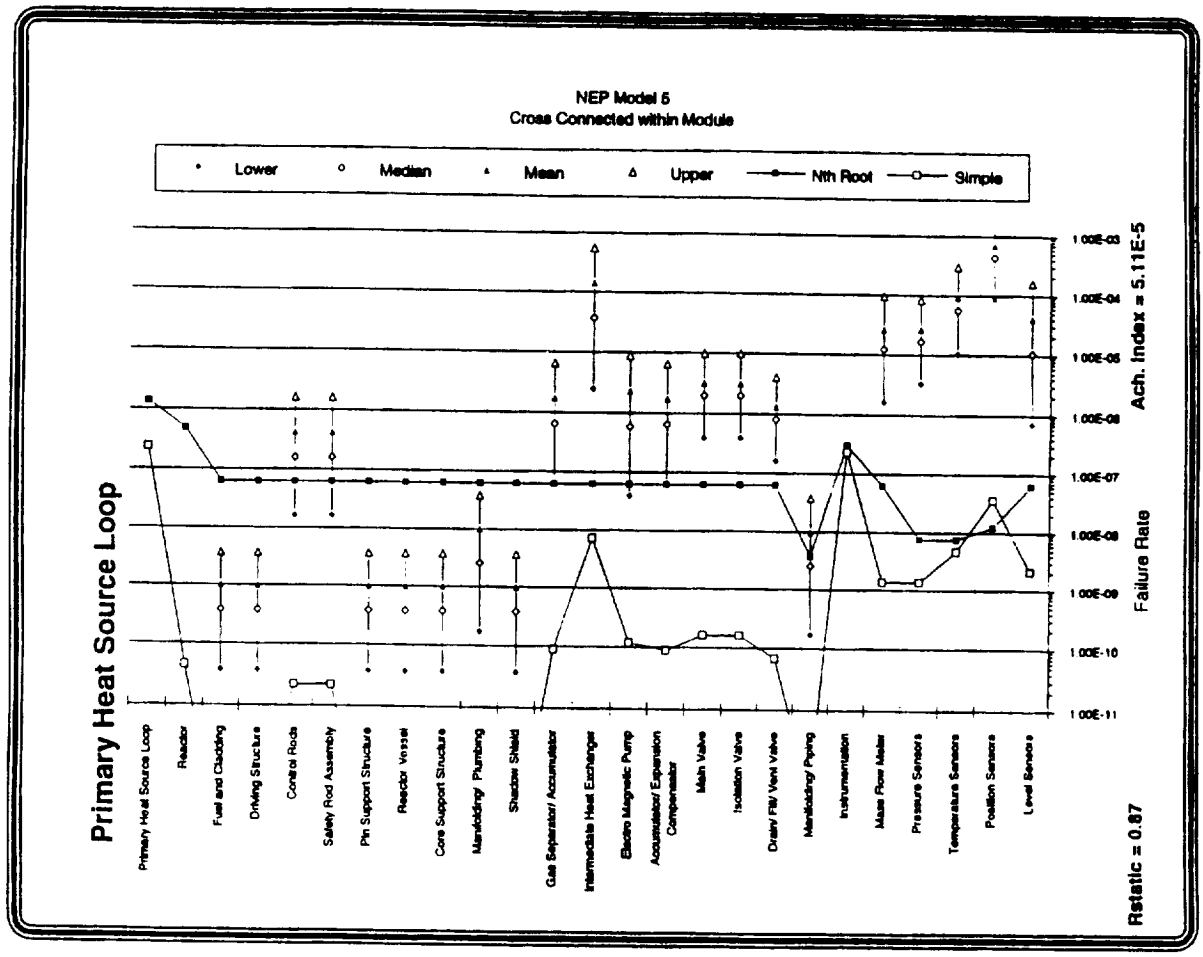
This diagram depicts the apportionment results using a model which reflects a "Minimum Equipment List" approach to crew safety. In this model, it was assumed that the decision to abort would be continuously analyzed based on the operability of a Minimum Equipment List for the NEP system. In this approach, if the system does not have sufficient operating equipment at the start of a phase to complete the mission with a 99% probability of crew safety, then an abort would occur. The set of equipment required to ensure crew safety varies from phase to phase, and is referred to as the Minimum Equipment List.

Applying this standard allows "restarting" the reliability clock with respect to crew safety at the start of each phase. The mission success reliability clock continues to run, so the 95% mission success criteria generally dominates the 99% crew safety criteria in this model.

Note that this approach improves the achievability index by a factor of almost 20 -- from $4.7 * 10^{-5}$ to $2.9 * 10^{-4}$.

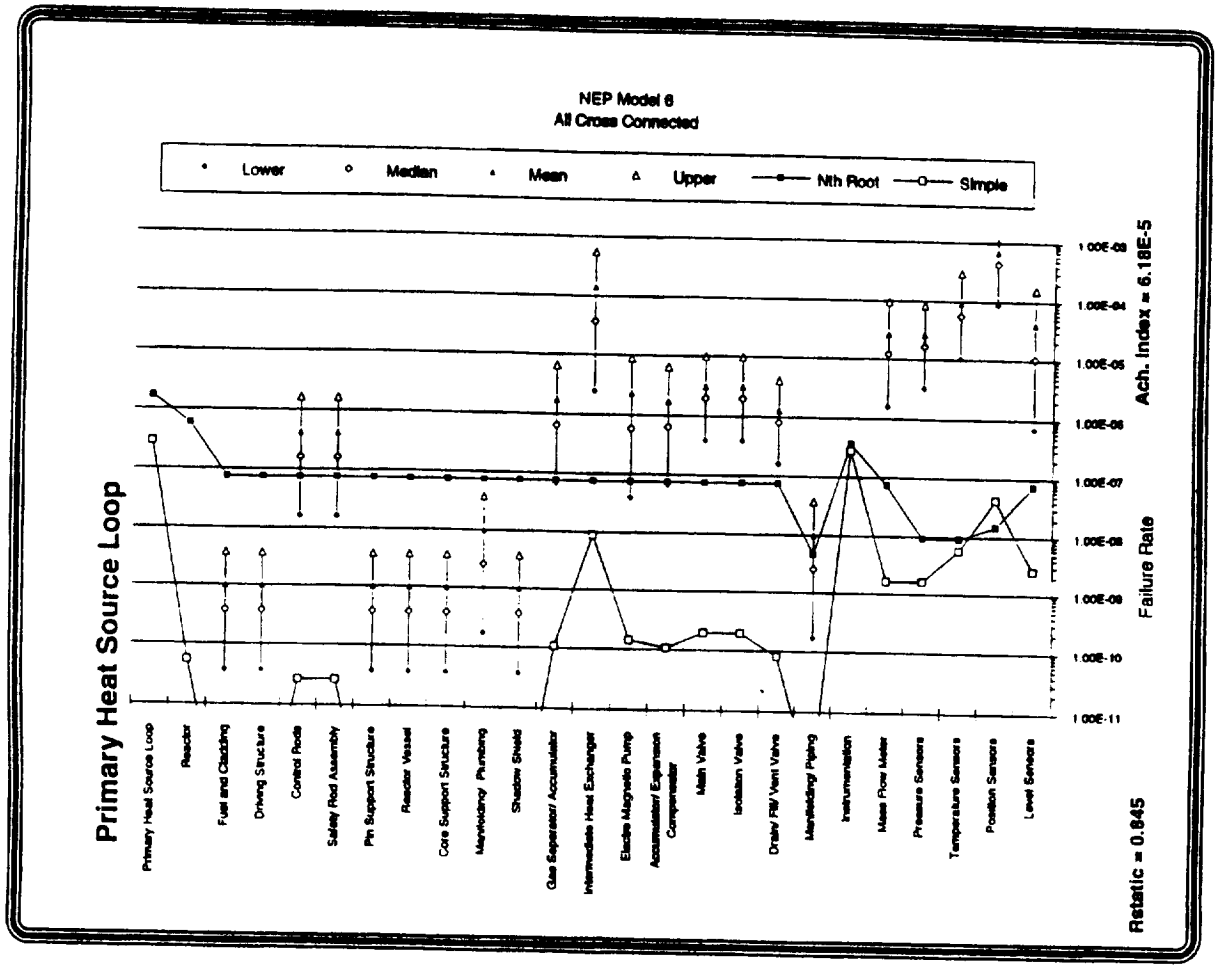


Model 4 (discussed previously) allowed limited repair / salvage. Note that the achievability index is approximately a factor of 10 better than the base case (model 1).



This model allowed cross-connection of the subsystem elements within a 5MWe module. This approach affords little improvement in achievability for these models because of the high importance of the subsystem modules. Any failure other than a Thruster resulted in the system producing less thrust than was required for the Mars escape spiral (87.5%). Therefore, no amount of interconnectivity compensates for a subsystem failure.

Limited cross-connection examined in this model is expected to provide significant benefit if the importance of the subsystems is lowered, either by requiring a smaller minimum thrust, or by providing excess capacity in the components as discussed previously.



This model, which allows for cross-connection of all electrical components -- even across 5MWe modules -- suffers from the same problem that the more limited cross-connection model does. The minimum thrust requirement is set too high to allow the resiliency of the design to have any real impact. What improvement there is in achievability ($6.2 * 10^{-5}$ versus $5.1 * 10^{-5}$) is due to the fact that the thrusters are operating in a six out of eight redundancy configuration for the portion of the mission requiring 75% thrust or less for crew safety.

ACHIEVABILITY OF NEP DESIGN

- Achievability is related to distance between apportionment curves and surrogate distributions.
- Simple and NthRoot Methods provide very different results:
  - NthRoot apportions to function
  - Simple apportions to individual component
  - Where a function has many identical components, Simple lies farther from surrogate.
- Actual solution lies between curves.

Science Applications International Corporation
An Employee-Owned Company

To recap, the achievability index is the measure of the distance between what is required of the system, and what is demonstrably attainable. The surrogate date indicates what is attainable, and failure rates apportioned from top-level reliability requirements establish what is required. The two apportionment methods used here were selected to bound (at least to first order) the failure rates that would actually be required for the NEP system components.

DESIGN ALTERNATIVES ACHIEVABILITY MATRIX

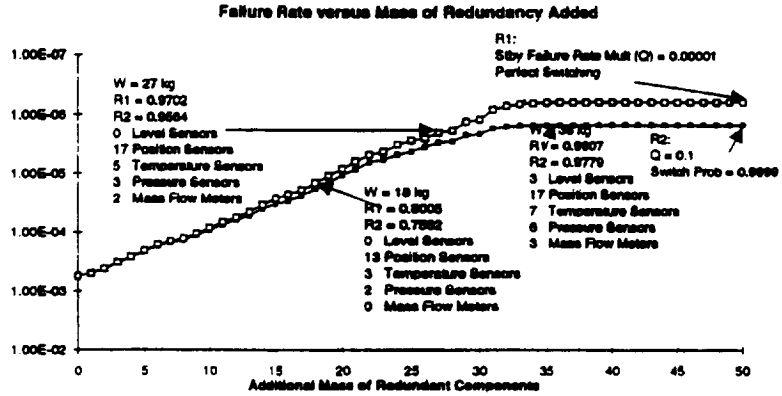
NEP Model Number Achl Static Reliab	Minimum Thrust Required in Limiting Phase				Min Equip. List	Repair / Salvage
	87.5%	75.0%	67.5%	50.0%		
No Cross Connection	1 4.7E-5 0.88	2 6.8E-5 0.83	-	-	1MEL 2.9E-4 0.45	4 5.1E-4 0.25
Electrical Cross Connection Within 5 MWe Module	5 5.1E-5 0.87	5T	-	-	-	-
Electrical Cross Connection Between 5 MWe Modules	6 6.2E-5 0.84	6T	-	-	-	-
Fluid / Mechanical Cross Connection Between 5 MWe Modules	-	-	-	-	-	-
Minimum Equipment List Approach to Safety	1MEL 2.9E-4 0.45	-	-	-		
Reparable / Salvageable System	4 5.1E-4 0.25	4T1	4T2	4T3		

- Matrix of achievability analysis experiments.
- Cells contain:
  - Experiment Number
  - Central Value of Simple method achievability index.
  - Equivalent reliability for a static system.

Science Applications International Corporation
An Employee-Owned Company

This matrix shows again the different models that were compared, along with the associated achievability index (AchI), and the equivalent static reliability value which would result if the apportioned failure rates for that model were used in a static reliability model of the NEP system.

ADDING RELIABILITY THROUGH REDUNDANCY



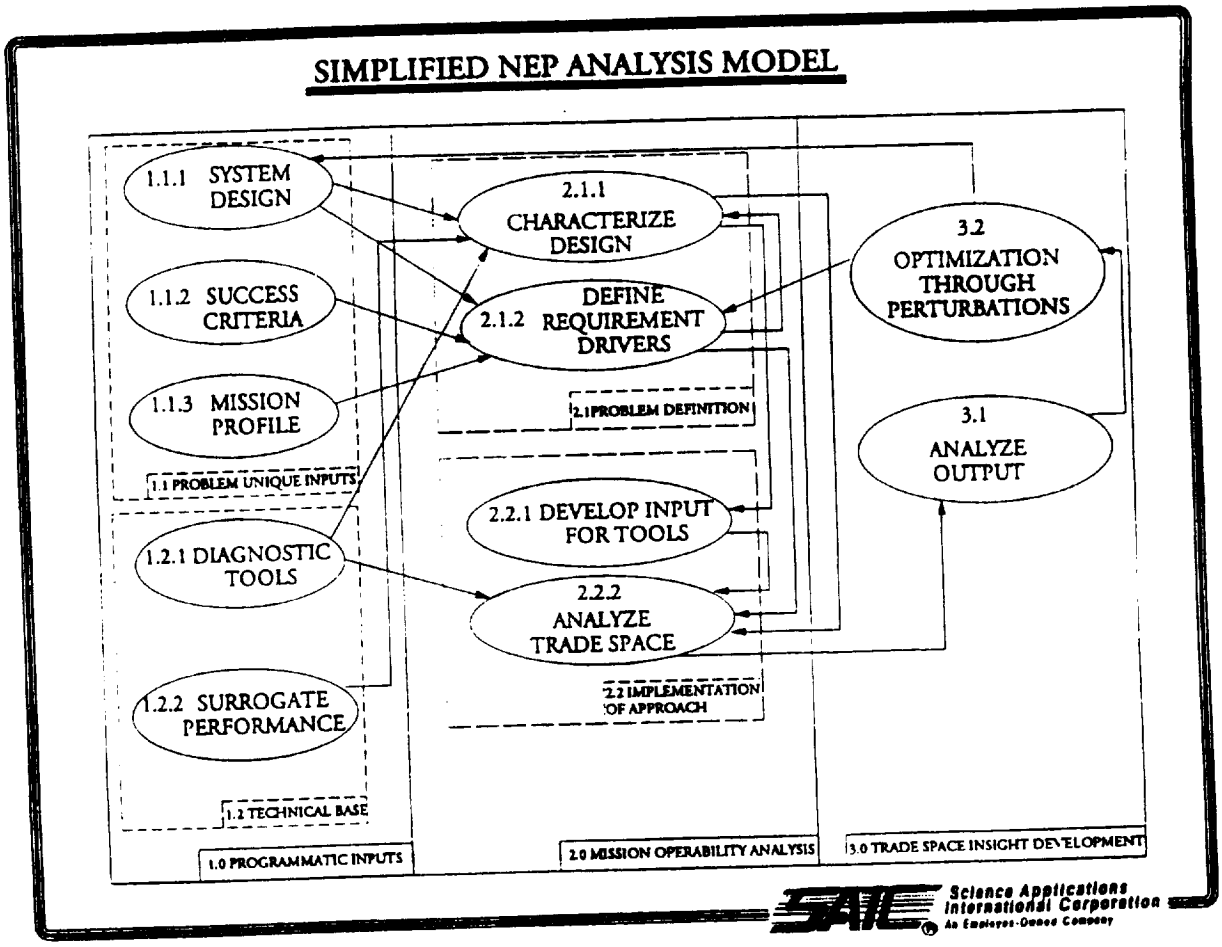
- "Optimal" failure rate versus mass of redundancy for Primary Loop Instruments found using Dynapro(TM).
- Note that there is a limit to the reliability that can be added through redundancy.
- Typical levels of redundancy improve functional failure rate by factor of 2.

Science Applications International Corporation
An Employee-Owned Company

A common fallacy is that any level of reliability can be achieved by adding enough redundancy. To determine the extent to which this true we used Bellman's dynamic integer programming algorithm as implemented in Dynapro™ to find the mathematical "optimum" redundant combinations of sensors in the Primary Loop. Here "optimum" is the highest reliability that can be obtained in a "M out of N" configuration for a specified increase in mass. We added up to 50 kg of mass for redundancy, almost an order of magnitude more than the mass of the single-string sensor suite, and checked the reliability for the "optimum" combination of sensors at that mass increment.

The curve illustrates that, while a very significant improvement in reliability -- three orders of magnitude -- can be obtained, there is a limit. Moreover, the mass penalty for improving reliability solely through redundancy is excessive.

Typically, double or triple redundant systems improve functional failure rate by a factor of two.



Finally we examine the various models to determine what lessons were learned from this analysis.

DESIGN INSIGHTS

- Design for Salvage / Repair is the single best strategy to maximize Probability of Crew Safety, Mission Success.
- Design & plan for refurbishment prior to Mars transfer orbit.
- Design to maximize robustness:
  - Maximize element interconnection.
  - Size system so return is possible with major element failure -- keep element importance < mission threatening.
  - Design to remain operating after major failures -- "Post-*Thresher*" approach to system safety.
- Use Minimum Equipment List approach to mission and abort planning.

Science Applications International Corporation
An Employee-Owned Company

The first order conclusions of this study are fairly simple. (1) In a manned environment where there is a need for the system to operate near its capacity at very high reliability even late in the mission, no single reliability strategy is more effective than designing the system to allow for salvage and repair. (2) Since radiological concerns will probably preclude full scale operation of the system and "burn in" prior to launch, infant mortality will be a factor. (3) Within the basic design parameters specified there are a number of ways to combine the system components to maximize the robustness of the system. (4) The Minimum Equipment List approach to mission and abort design can be used to prevent the very stringent requirement for probability of crew safety from setting unrealistic reliability goals.

DESIGN FOR SALVAGE / REPAIR

- Ability to salvage / repair improves achievability by an order of magnitude or more.
- Keys to salvage are:
  - Modular, repairable design;
  - Element importance < mission threatening.
- Parts on hand governed by:
  - Element importance;
  - Failure probability -- Pareto rule;
  - Commonality.

Designing the system for salvage and repair does not mean that the crew should be able or required to replace any failed part in the system. It does mean that, as a last resort, the crew should be able to replace critical, highly stressed parts, and should be able to change connections or move modules to jury rig a single working element from two or more that have failed.

PLAN FOR REFURBISHMENT

- Infant mortality failures will occur during Earth escape spiral "shakedown".
  - Take advantage of the shakedown opportunity, rather than be victimized by it.
    - Infant mortality is excellent predictor of random failure performance.
      - 1st month failure rate = 4 to 20 times random (mean = 7 * Random failure rate)
      - Distribution of failures among subsystems / component type approximately constant.
  - Factor in time for minor redesign and on-orbit refurbishment prior to heliocentric transfer.

Science Applications International Corporation
An Employee-Owned Company

Early failures attributed to infant mortality have played a role in nearly every space system. Since the manned portion of the NEP Mars mission does not begin until after the NEP system has accumulated significant operational time, it is highly probable that some failures will have occurred before the crew boards. By designing and planning for minor refurbishment prior to the start of the manned portion of the mission, NEP planners can minimize the possibility that the crew will start the mission with less than a full redundancy complement. Moreover, since infant failures are predictors of the types of failures which will occur during the operational phase, the unmanned "shakedown cruise" can actually be used to significantly enhance the probability of mission success -- through procedure development, work-around strategies, and possibly even minor component redesign -- prior to the actual start of the mission.

MAXIMIZE ROBUSTNESS

- Element interconnection
  - Reduce / remove probability that element failure will prevent use of other elements in string.
- Element importance -- impact of element failure on system.
  - Size system elements so major element failure does not jeopardize crew return.
- "Post-*Thresher*" approach to safety -- System response to component failure determined solely by maximizing probability of returning the crew alive.
  - "Safeing system" generally = leave it alone / operating.
  - e.g.: Reactor may continue operation w/ open control loop (no instrumentation) -- but restart w/out instrumentation difficult or impossible => no shutdown (SCRAM) on instrument / control failure.

Maximizing the robustness of the NEP system involves three elements. First, minimize the extent to which the failure of one element in a string impacts the other elements in the string. Second, maximize the extent to which an operating element can compensate for the loss of a like element. Third, ensure that no element in the system is made more important to the system than is absolutely required. For example, an irrecoverable failure in the Primary instrumentation which results in the shutdown (SCRAM) of the reactor would result in the loss of the crew in most mission phases. Almost any level of risk associated with continuing to operate the reactor, despite the failure of a critical sensor, is preferable to that alternative.

MINIMUM EQUIPMENT LIST

- Minimum Equipment List (MEL) -- the minimum set of equipment required to complete mission.
  - Varies with time in mission.
  - Points where MEL changes are abort decision points.
    - Determined by Markov or other dynamic analysis:
      - MEL state = minimum state vector that accomplishes success criteria?
    - Actual system state < MEL state => abort.
- In general, changes limiting reliability criteria from 99% $P_{(CrewSafety)}$ to 95% $P_{(Mission\ Success)}$.
  - Improves achievability by factor of 5 or more.
- May have other mission planning benefits -- staging, etc.

Applying the Minimum Equipment List approach to the mission and system design will enhance crew safety while limiting the burden of very high system reliability goals associated with crew safety.

IMPACT OF DESIGN INSIGHTS ON ACHIEVABILITY

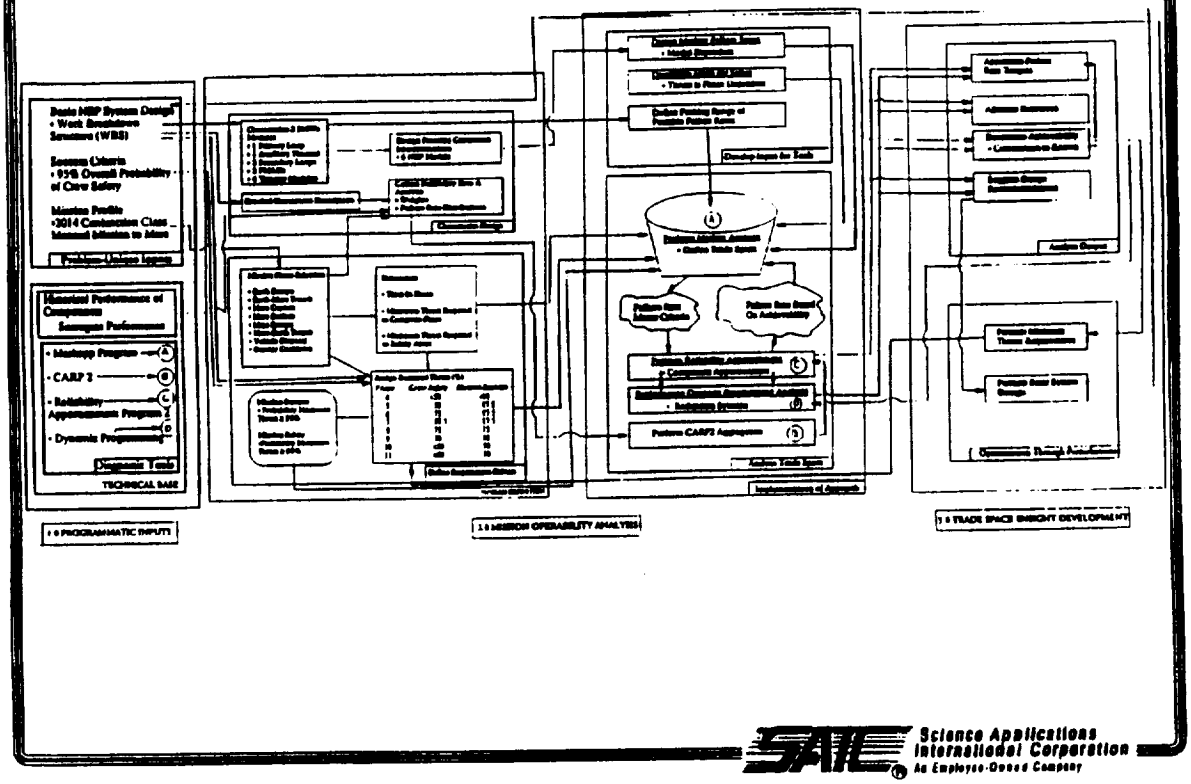
	AchISimple	Cummulative
· Baseline (No Cross Connection)	· $4.7*10^{-5}$	$4.7*10^{-5}$
· Redundancy (*2)	· $9.5*10^{-5}$	$9.5*10^{-5}$
· Salvage / Repair (*10)	· $5.1*10^{-4}$	$9.5*10^{-4}$
· Element Importance < Mission Threatening (Primary and Auxiliary Thermal not included)	· $6.8*10^{-5}$	$1.5*10^{-3}$
· Remain Operating After Failure (No instruments, sensors in critical failure path)	· $2.4*10^{-4}$	$7.5*10^{-3}$
· Minimum Equipment Set (*5.1)	· $2.9*10^{-4}$	$3.8*10^{-2}$

Science Applications International Corporation
An Employee-Owned Company

The design insights gained from analyzing the different models (design concepts) are generally not correlated, so to a significant degree their effect (if applied) is cumulative. This table shows that, taken together, the reliability enhancing design alternatives analyzed here improve the outer boundary of overall achievability for the NEP system by three orders of magnitude. Since the range of achievability index spans at least two orders of magnitude, the final AchI value of 4 * 10-3 is within the range of achievable using current technology.

This conclusion does not imply that meeting the quantitative operational reliability goals for this system will be easy, or that new technologies should not be examined for potential reliability improvements. On the contrary, several critical functions, notably heat exchangers / radiators, and sensors should be examined carefully to determine if there is an intrinsically more reliable way to accomplish the function than using existing technology.

SUMMARY



Science Applications International Corporation
An Employee-Owned Company

The process and conclusions of this study have been discussed at some length. This study deliberately only examined the boundaries of the problem and the conclusions should be considered more qualitative (with extensive quantitative backup) than quantitative. We did not attempt, for example, to find optimal or near optimal component failure rate requirements. To do so would require refinement and extensive recursion of the models and tools we have demonstrated.

CONCLUSIONS
CONCEPT OF ACHIEVABILITY:

- Quantifies how far a design has to go with respect to success criteria.
  - A powerful method for
    - assessing design alternatives;
    - assessing developmental risk;
    - directing R&D effort.

The concept of achievability was used in this study to measure the distance between the required and the attainable. This concept proved to be very powerful and is recommended for use in quantitative analyses of any performance dimension which pushes the state of the art.

CONCLUSIONS
DESIGN ALTERNATIVES:

- Several promissing design strategy alternatives were analyzed.
  - Repair / Salvage.
  - Maximizing Robustness:
    - Cross-Connection
    - Reducing element importance < mission threatening.

This study examined only a few design alternatives within a fairly rigid basic design envelope. While several promising reliability-enhancing strategies were identified and examined, there is clearly more that could be done.

CONCLUSIONS
DESIGN ACHIEVABILITY:

- Overall achievability for simple, no cross-connection design is very low ~ 10-4 even with redundancy factored in.
- However, simple design alternatives presented here give a cummulative 3 order of magnitude increase in achievabiliity.
- While challenging, NEP achievability is within striking distance of realization.

It is the conclusion of this study that the existing technology base could support the quantitative reliability requirements of a manned Mars mission.

NUCLEAR ELECTRIC PROPULSION

TECHNOLOGY