N72-25981

# FAULT TREE APPLICATIONS WITHIN THE SAFETY PROGRAM OF IDAHO NUCLEAR CORPORATION

By

Dr. W. E. Vesely
Senior Technical Specialist
Computer Science Branch
Idaho Nuclear Corporation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1 '1

## INTRODUCTION

At Idaho Nuclear*, a system safety analysis program is in existence for the routine safety and reliability analysis of control and safeguard (backup) systems. Though the systems analyzed are generally peculiar to the reactor industry, the methods employed, and their applications, are generally utilizable in any safety program. In Idaho Nuclear's safety program, a diverse assortment of techniques are employed, such as fault hazard analysis, failure mode analysis (FMEA and FMECA), failure matrix methods, block diagram modeling, and fault tree methods. The fault tree method and its applications in particular are discussed in this paper, since this technique enters into a large portion of the safety analysis performed at Idaho Nuclear.

Fault tree methods are used to obtain both qualitative and quantitative information about the safety and reliability of the system analyzed. For the analysis, the fault tree depicts all the primary causes for a particular system failure (or accident occurrence). The system failure or accident occurrence is the top event of the fault tree. The primary causes are usually component failures, administrative errors or environmental conditions; in general, the primary causes depict the resolution desired for the causes of the system failure or accident occurrence. By use of the standard "AND" gate and "OR" gate symbology, the fault tree depicts the logical relationships of the primary causes, and their consequences, which led to the specified system failure (or accident). Figure 1 at the end of this paper summarizes the basic fault tree representations. For a discussion of the fault tree method, the reader is referred to Haasl(1) or Crosetti(2).

At Idaho Nuclear the fault tree analyses are performed for the following objectives:

1. To represent in an objective and communicative manner the causes of the system failure or accident occurrence.
2. To obtain the modes by which the system failure or accident occurs. These modes are termed "critical paths" in fault tree terminology.
3. To determine the relative importances of the individual critical paths.
4. To determine the qualitative and quantitative impact on safety or reliability due to proposed design modification or component upgrade.
5. To determine the quantitative response of system availability with regard to particular maintenance schemes.
6. To determine the quantitative safety, reliability, or availability with which to compare to established standards.

The fault tree itself satisfies the first objective since it portrays in a lucid manner the logical chains of events which lead to the system failure or accident. The fault tree, once drawn, is an effective implement by which management, reliability or safety engineer, and design engineer can communicate.

From the fault tree, a simple qualitative-type evaluation determines all the modes, or critical paths, for the system failure or accident. A critical path is a group of primary causes which must all occur in order for the system failure or accident to occur; if one of these primary causes does not occur then the system failure or accident will not occur by this mode. The complete set of critical paths for the fault tree gives all the combinations of primary causes which give rise to the top event. If one or more of these combinations occurs, then the system failure (or accident) occurs.

A few simple illustrations may serve to best clarify the critical path definition. Assume a fault tree has been drawn and its critical paths have been obtained. If one of these critical paths is "Resistor 1 Failure in Mode A" and "Resistor 2 Failure in Mode B" then Resistor 1 must fail in Mode A and Resistor 2 must fail in Mode B in order for the system failure or accident to occur. If either resistor does not fail, or fails in modes other than A and B, then the top event (system failure or accident) will not occur by this particular route. If one of the critical paths obtained is "Resistor 3 in Mode A", then only Resistor 3 failing in Mode A is sufficient for the top event to occur, and Resistor 3 in

* As of July 1, 1971, Idaho Nuclear will be under the Aerojet Management and will be known as Aerojet Nuclear Company.

Mode A" is termed a single failure. The set of critical paths obtained for this fault tree represent all those primary cause combinations, and only those combinations, which will cause the top event to occur.

The critical paths are obtained from the fault tree by means of a number of existing safety and reliability computer programs; at Idaho Nuclear the programs PREP and KITT(3) are used. The critical paths are an important class of information since they directly tie the system failure or accident to the primary causes. If improvement is desired, the critical paths identify the specific areas which are the weakest and which would have greatest response to an improvement. In general, optimal improvement consists of increasing the size of the smallest critical paths. If the fault tree has one component critical paths (single failures) improvement should be centered such that these paths become two component (a redundancy added), if two component critical paths are the smallest that exist for the fault tree, then they should be designed into three component critical paths and so forth.

For the quantitative information in the preceding list of objectives of the fault tree analysis, the computer programs PREP and KITT are utilized. PREP and KITT employ the Kinetic Tree Theory approach to obtain quantitative information about the fault tree. The Kinetic Tree Theory technique has been described in a number of articles (4,5,6) and the details of this approach will not be discussed here.

The fault tree as drawn by the engineer is simply input into PREP and KITT. The only other data needed as input are the failure rates or probabilities for the primary causes (i.e., for the components and any environmental effects) and the average repair times for those primary causes that are repairable. With this input data, PREP and KITT obtain the critical paths of the fault tree and the following quantitative information:

1. The probability that the failure or accident will not occur at all to time t.
2. The probability of the failure or accident existing at time t.
3. The expected number of times the failure or accident will occur to time t.
4. The failure or accident frequency at time t (the integral of this quantity is simply the previous characteristic (3)).
5. The failure rate (lambda) at time t.

This information is obtained for any series of time points t desired by the user, and hence time dependent curves are obtained which portray the time history of the reliability or safety. From these curves one is able to discern, for example, the degradation of reliability or safety with respect to time; lifetime-type information is thus included in the results obtained. If a particular time is of interest, then one point from these curves is simply used.

This time dependent information is obtained for each primary cause of the fault tree (i.e., for each component or environment effect), for each critical path of the fault tree, and for the top event of the fault tree (the accident or system failure of interest). As applied to a particular primary cause, the information gives the frequency at which the primary cause occurs, the probability of the primary cause not occurring at all, the probability of the primary cause existing at time t, and the expected number of times the particular primary cause will occur. If the primary cause is a component, the information thus gives the detailed reliability and availability of the component and shows, for example, the detailed effects of repair or environment stresses on that particular component. Since this information is obtained for every primary cause, those primary causes, such as particular component failures or environment effects, which are most critical are readily identified.

The information obtained for a particular critical path gives the frequency, expected number of times, etc., the top event (i.e., system failure or accident) will occur by this particular mode. The primary causes in the particular critical path are solely responsible for the system failure or accident and the obtained information describes how often this particular critical path, or mode, will cause the failure or accident. The information is obtained for each of the critical paths of the fault tree, and hence the most important critical paths are identified, those by which the failure or accident will most likely occur.

Any safety or reliability improvements will be directed to these "weak links".

In addition to being obtained for each primary cause and critical path, the five time dependent characteristics are also finally obtained for the top event of the fault tree. The characteristics give the frequency at which the system failure or accident will occur, the number of times it is expected to occur, and the probability of it not occuring at all. If the system analyzed is a safety backup-type system, this information gives, for example, the availability of the system, that is, the probability that the system will perform correctly when an accident condition exists. For an on-line operating system, the information gives the percentage of time the system will operate without failure in any time period. The information obtained is a complete characterization of the failure or accident for any particular situation analyzed; effects of repair, environmental stress, and administrative procedures are explicitly obtained. Since the information is time dependent, a complete history of the safety and reliability characteristics is yielded.

The PREP and KITT codes obtain the time-dependent characteristics by an analytical technique which does not entail any Monte Carlo simulation. The codes require little computer time, for example, approximately two minutes of IBM 360/75 computer time is needed to completely analyze a 1000 component fault tree. For smaller trees the computer time is considerably less*. Because of the small computer time, sensitivity studies and design modification studies are practically performed. The failure rates, repair times, or particular portions of the tree are simply modified and the programs run again to assess these possible deviations.

## PARTICULAR APPLICATIONS

This section describes particular fault tree analyses which have been performed at Idaho Nuclear. The specific, technical details of the systems are not described so that the reader is not encumbered with jargon with which he may not be familiar. The aim of this section is to demonstrate, as straightforwardly as possible, practical applications of fault tree analyses. By describing the results which have been obtained from these analyses, this section will hopefully illustrate the power of fault tree analysis and the role it can play in a system safety program.

### SPERT IV Protection System Analysis*

The SPERT protection system is an electrical control system which has the function of shutting the reactor down when certain safety criteria are exceeded. In this particular instance, the system consisted of an automatic control (time triggered) and a manual backup control. If the automatic control system failed, a signal was relayed to an operating personnel who was then to initiate the manual control system (by pressing a control button).

A fault tree was drawn for this system, in which the system failure (top event) was defined to be both the automatic control system failing and the backup manual control system failing, when accident conditions existed. In this case, an analysis was performed on an already existing system; the SPERT control system (automatic and backup) was operating, but an upgrade was desired. In order to upgrade this system, the following information had to be obtained:

1. An identification of all credible component failures and/or fault conditions that could result in the designated system failure.
2. An identification of the most critical weaknesses in the existing system (termed the "base-line" system).
3. A determination of the impact on system safety due to proposed design modifications.

The fault tree was decided upon as the most practical method of obtaining this information. The fault tree analysis was performed independently of other safety analyses and was the major effort for this particular system study.

The fault tree, once it was drawn, consisted of approximately 300 component failures

*The computer time is insensitive to the number of time points desired by the user.

*SPERT IV is the name of a particular reactor.

and fault conditions (primary causes). The primary causes (the "bottom ends" of the fault tree) were basic component failures such as particular resistor failures, relay failures, and wire failures. Adverse environmental conditions on these components were also included in the primary causes. The resolution of the fault tree was therefore on a basic component level.

A correct input to the automatic and backup control systems was assumed and the fault tree analyzed the causes for no output or incorrect output. Hence, the analysis isolated the "signal-passing function" of the control system. No human errors were considered in the fault tree. Certain subsystems of the control system were periodically checked and this scheduled maintenance was included in the analysis. To draw this fault tree, a total time of approximately two man-weeks was required. This task thus required little time and effort.

The fault tree itself and the critical paths determined by PREP and KITT yielded the first class of information in the preceding list. In the PREP and KITT computer run, failure rates (lambdas) were assigned to the components on the fault tree to determine the most import critical paths, i.e., to identify the most severe weaknesses in the system. The results of this run are shown below.

Table 1

COMPONENT FAILURE CONTRIBUTIONS TO A SYSTEM FAILURE

Manual Control Failure

| Component | Failure Contribution |
|---|---|
| Relays (8) | 0.6477 |
| Console Switches (2) | 0.3076 |
| Terminals and Connectors (27) | 0.0262 |
| Wires (76) | 0.0185 |

Automatic Control Failure

| Component | Failure Cont. ibution |
|---|---|
| Timer (1) | 0.9927 |
| Relays (14) | 0.0071 |
| Terminals and Connectors (26) | 0.0001 |
| Wires (71) | 0.0001 |

The above table lists only the major contributors to system failure; the numerous other components not listed had negligible contribution. From the table, if the automatic control system failed, 99% of the time it would be due to the automatic timer mechanism itself failing, while only 0.01% of the time it would be due to one of or more of the 76 wires failing. If the manual backup system failed, 65% of the time it would be caused by one or more of the eight relays failing and 31% of the time would be caused by one or both of the console switches failing. The critical area in the automatic system was thus the timer mechanism while the critical areas in the manual backup system were the eight relays and two console switches.

From the identification of these critical areas, and from the critical paths and fault tree itself, which showed the interconnections these critical areas had within the system, modifications become evident which might upgrade the safety of the system. The modifications were quite simple and consisted of 1) placing a second relay in parallel with an existing one ("Modification 1"), and 2) inserting a manually set timer in the automatic control circuit ("Modification 2"). The impacts of these modifications were determined by two additional PREP and KITT computer runs which analyzed the fault tree with the modifications inserted. The total IBM 360/75 computer time required for these two runs plus the original run was three minutes, which was neglible. The result of the impact evaluations is shown in Figure 2 at the end of this paper.

In the figure, the "Failure Probability" is that both the automatic control system and the manual control system will fail in any one or more of the number of tests performed (a "test" here is simply an operation of the control system). For example, the failure probability at 200 tests denotes the probability of control failure in one or more of these 200 tests. The "BASE-LINE" curve depicts the failure probability for the existing automatic and backup system, the "MOD-1" curve is for this system incorporating Modification 1 (described previously), and the "MOD-2" curve is for the system incorporating both Modification 1 and Modification 2.

As evident from the figure, the proposed modifications significantly increased the safety of the control system. These modifications were made evident from the fault tree analysis and the impacts of these modifications were then able to be objectively determined from the PREP and KITT computer runs. Modification 1 (corresponding to the MOD-1 curve) was consequently decided upon as a change to be incorporated in the system which would be practical in cost and which would substantially upgrade system safety.

## Plant Protection System Pilot Study

The system analyzed in this study is an on-line control system. Critical plant parameters are continuously monitored and if any of these parameters exceeds safe operating limits the control system rapidly reduces the reactor power. The fault tree analysis was performed during the conceptual phases of system development. Three possible designs were proposed for the control system, and the fault tree analysis served the role of determining the "best" system design out of the three proposed. The analysis investigated both the safety and reliability of the designs; in fact, in this instance, if the system safety was the only characteristic examined the wrong design would have been chosen.

The fault tree analysis of the three designs was conducted on a functional level; the minimum components required to provide a discrete and separate function were considered as the basic building blocks of the system. This level of analysis was sufficient to define the primary causes of failure on the fault tree. Any further detail was inappropriate in this conceptual design phase and the functional level of resolution provided adequate information with a minimal expenditure of time and effort.

Six fault trees were drawn for the three proposed designs, one fault tree considering reliability and one fault tree considering safety for each design. The studies were performed by system design engineers who were familiar with the concepts of fault tree analysis. Each fault tree consisted of approximately 70 components (primary causes) and the six fault trees required two man-weeks to complete (two engineers working five days).

Each of the three designs possessed redundancies in the electrical circuits. All the designs utilized two out of three coincidences to insure against spurious, undesired action, and all three designs were of the same order of cost. It was not obvious from the design as to which one design was the best and a fault tree analysis was the only method deemed practical, and of sufficient power, to solve this problem.

For the safety fault tree of each design, the system failure (top event of the tree) was defined to be "failure of the system to respond when protective action is necessary". For the reliability fault tree the system failure was defined as "system responds when protective action is not necessary". For the safety study the failure thus investigated was the system not working when accident conditions existed; accident conditions were input to the system, but the system did not respond. For the reliability study, the failure was the system acting as if accident conditions existed when they did not; normal, nonaccident conditions were input to the system, but the system responded as if accident conditions were input. In the safety failure, the system gave no protection to an accident and in the reliability failure, the system gave unwanted protection which shut the plant down.

The fault trees, once drawn, were input to the PREP and KITT programs to obtain the quantitative system safety and reliability characteristics. Component failure rate data, gathered from existing reports, was also input to the programs. The same failure rate data was used for all the fault trees in order to obtain valid comparisons. The six computer

runs required a total of four minutes computer time, which was inconsequential. The results of the analyses are shown in Figures 3 and 4 at the end of this paper.

In Figure 3, the probability of a safety failure is plotted versus total operating time (hours). A point on a curve gives the probability of the system failing during a particular operating period. If, for example, the time period of 1200 hours is chosen (the x value) then the probability that the system will fail during this 1200 hour operating period is obtained from the curves. (The curves in Figure 3 are only plotted to 2000 hours since this is the proposed maximum continuous operation time for the system.)

The system failure investigated in Figure 3 is a safety failure, i.e., the failure of the system to respond when protective action is necessary. Each of the three safety fault trees for the three designs investigated this particular safety failure (had this as the top, undesired event on the fault tree). "System I", "System II" and "System III" in Figure 3 represent the three individual design proposals. From the figure, System I and II are the safest designs with System II being a bit safer than System I. If safety was the only consideration, then System II would be chosen as the best design since it was simpler and slightly cheaper than System I.

Figure 4 illustrates the reliability of each of the three designs. The probability of a reliability failure (the y-axis) is the probability that the system responds when protective action is not necessary. Total operating time is again depicted on the x-axis. From the figure, System I is the most reliable, while Systems II and III are highly unreliable and cause numerous unwarranted shutdowns.

Investigating both Figures 3 and 4, that is investigating both safety and reliability, System I is clearly the best design. The safety of System I is acceptable with regard to the established program standards and in fact the difference between the safety of System I and the safest design is insignificant. The reliability of System I equals its safety ($\sim 10^{-3}$ after 2000 hours) and far exceeds the reliability of the other two designs. Because of this analysis, System I was the design chosen and is presently progressing through the finalized design stages.

For this study, the fault tree analysis thus allowed the best design to be chosen with little effort and cost expenditure. System III was the simplest design and had the fewest components, while System I, the design chosen as the best, was the most complex. The fault tree analysis showed that in this case, a small amount of added complexity bought large returns in safety and reliability. As an added verification, the present finalized design studies of System I substantiates completely the results of the performed fault tree analyses.

## PBF Poison Injection System Analysis

The final study discussed in this paper is an investigation of a backup emergency system. The poison injection system is used as an emergency reactor shutdown system; it is essentially a two out of three type control system which is manually initiated. A correct input to the system was assumed and no response was the system failure examined (i.e., this was the top event of the fault tree). Resolution was on a basic component level and human errors were not considered. The fault tree analysis was performed again during the conceptual design stage. The fault tree consisted of approximately 200 components and, as in the previous cases, required approximately two man-weeks to complete.

The analysis is different from the previous two in that the injection system is solely a backup system and system availability is the primary safety concern. ("Availability" here is the probability the system will function when called upon at any particular time. Conversely, the "unavailability" is the probability the system will not function when called upon.) The fault tree analysis was performed to investigate the following:

1. Possible weaknesses in the system design (the base-line system). These would be determined from the fault tree itself and from the critical paths obtained by PREP and KITT.
2. The response of system availability with regard to various maintenance checking intervals used for the components. This would be determined from the quantitative characteristics obtained by PREP and KITT.

3. Differences that would result in system availability due to particular design modifications. The quantitative characteristics from PREP and KITT would again be used here.

The fault tree analysis was one part of a larger safety analysis performed on this system.

The fault tree, having been drawn for the base-line system design was input to the PREP and KITT codes to obtain the critical paths and quantitative characteristics. The input also included the component failure rates and a range of checking times for those components that would have maintenance (not all components would be checked and this was taken into consideration). From the fault tree and critical paths, possible weaknesses in the base-line system were uncovered. A second and third computer run was then performed to analyze two possible design modifications; in these additional runs, the same component failure rates and checking times were used. The total computer time required for the three runs was five minutes IBM 360/75 time.

Figure 5 at the end of the paper shows the system availability versus component checking interval for the base-line system design and for the two proposed design modifications. The quantity actually plotted on the y-axis is the failed probability, or system unavailability, which is one minus the availability. The "NO REDUNDANCY" curve is the based-line system, the "PARTIALLY REDUNDANT" curve is for a design modification making certain portions of the system redundant, and the "COMPLETELY REDUNDANT" curve is for a second design modification making the system completely redundant.

From the figure, for example, if the maintainable components of the base-line system were checked every 100 hours ($10^2$ on the x-axis) then the system unavailability would be $6 \times 10^{-2}$ (the corresponding y-value on the NO REDUNDANCY curve). Thus, for this design and checking interval, 6% of the time the system would not function when called upon.* Again, for the base-line system, if the maintainable components were checked every 1000 hours, then the system unavailability would be $4 \times 10^{-1}$, i.e., there is a 40% probability that the system would not function when it was called upon at any particular time, (when accident conditions existed). The unavailability for the PARTIALLY REDUNDANT design or the COMPLETELY REDUNDANT design, for a particular component checking interval, would be read from the figure in a similar manner as above.

The results from the fault tree analysis and the subsequent PREP and KITT runs shown in Figure 5 are significant since they show not only the response of availability with respect to various maintenance schedules for a particular design, but also show the impact of design modifications on the system availability. If a given availability is desired (or equivalently if a given failed probability, or unavailability, is desired), then either the base-line system design with a given component checking interval may be used or a modified design with a larger checking interval may be used. The design modifications have their chief impact on the checking interval, allowing the same availability to be attained with less maintenance.

The modifications which made the system completely redundant (the COMPLETELY REDUNDANT curve in Figure 5) consisted of incorporating more piping redundancy into the system. These modifications increased the independence of the flow circuits as verified in Figure 5. The modifications have been taken into consideration in the final design of the system.

Finally, Figure 6 shows the failed probability (unavailability) for the completely redundant design when possible errors in component failure rate data are taken into account. The "MOST PROBABLE VALUE" curve in Figure 6 is the same as the COMPLETELY REDUNDANT curve in Figure 5, but is plotted on a different scale. The MOST PROBABLE VALUE curve represents the best value for the completely redundant system unavailability. The "90% Upper Bound" and "90% Lower Bound" are the 90% confidence bounds for the system unavailability (i.e., the curves represent 90% error bars when possible errors in data are taken into account). These upper and lower bound curves were computed by

*Checking every 100 hours means a periodic maintenance check is performed after every 100 hours of operation.

assuming a possible error of a factor of 10 in each component failure rate (to 90% confidence). These error curves serve to show the effect errors in component failure rate data have on the system computed safety characteristics. As observed, the possible errors did not significantly affect the system results. Even accounting for these possible component failure rate errors, the relative differences between the curves in Figure 5 remained the same (i.e., the possible failure rate errors merely shift all the curves in Figure 5 up or down the y-axis without changing their relative separations). The completely redundant system thus still showed the same gain in availability when possible errors in component data were taken into account.

For this study of a stand-by emergency system, the fault tree analysis thus showed, in an objective manner, the effect of maintenance on the system availability and the effect of proposed design modifications on the availability. As for the previous studies, the fault tree effort required minimal time and cost, with returns greatly exceeding the investment.

## SUMMARY

The fault tree methods that were used for the described analyses are not peculiar to any particular system; the methods can be used on any electrical or mechanical system in any industry. Furthermore, the methods need not only be applied to systems, but can be applied to any event or incident, such as an accident occurrence, for which the primary causes are desired. The same kinds of results as were illustrated in this paper will be obtained for any fault tree, regardless of its particular nature. Any fault tree will yield, among other information, the critical paths, i.e., the modes by which the system failure or accident will occur, the most critical areas likely to cause the failure or accident, detailed failure probabilities, and the response of safety or reliability to design modifications and maintenance schemes. The fault tree itself is a significant result since it objectively defines the failure or accident and is valuable tool for communication. The fault tree analysis has most application in the design phases, but it can be used on already existing systems. Finally, the fault tree can be as detailed as desired, however, the fault tree need not be elaborately complex in order to yield useful and significant information.

## REFERENCES


(1) D. F. Haasl, "Advanced Concepts in Fault Tree Analysis", System Safety Symposium, June 8-9, 1965, Seattle: The Boeing Company, 1965

(2) P. Crosetti, "Fault Tree Analysis with Probability Evaluation", in IEEE Transactions on Nuclear Science, Vol. NS-18, (1), February, 1971

(3) W. E. Vesely and R. E. Narum, PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree, IN-1349, August, 1970

(4) W. E. Vesely, "Reliability and Fault Tree Applications at the NRTS", in IEEE Transactions on Nuclear Science, Vol. NS-18, (1), February, 1971

(5) W. E. Vesely, "A Time Dependent Methodology for Fault Tree Evaluation", Nuclear Engineering and Design, 13 (1970) pp. 337-360

(6) R. E. Narum, "A Rapid and Exact Methodology for Fault Tree Analysis", Proceedings of the Semiannual AEC Computer Information Meeting, 1969

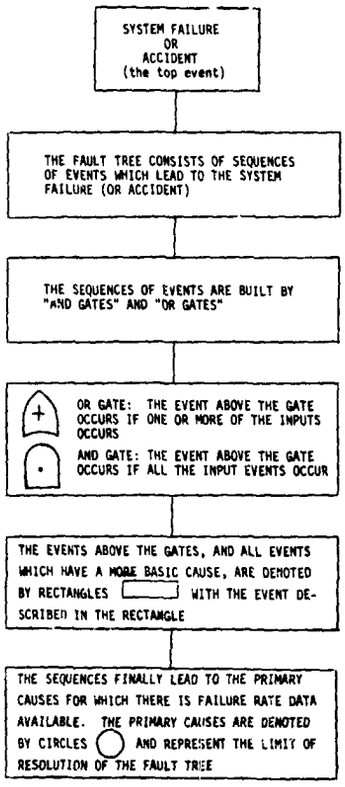


FIGURE 1

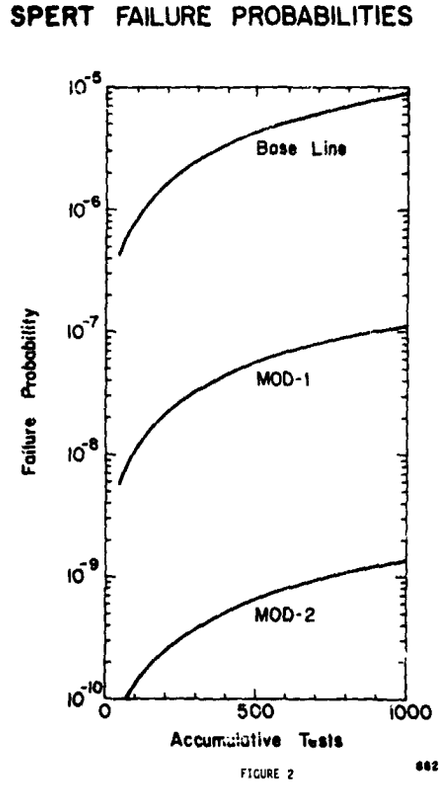


FIGURE 2

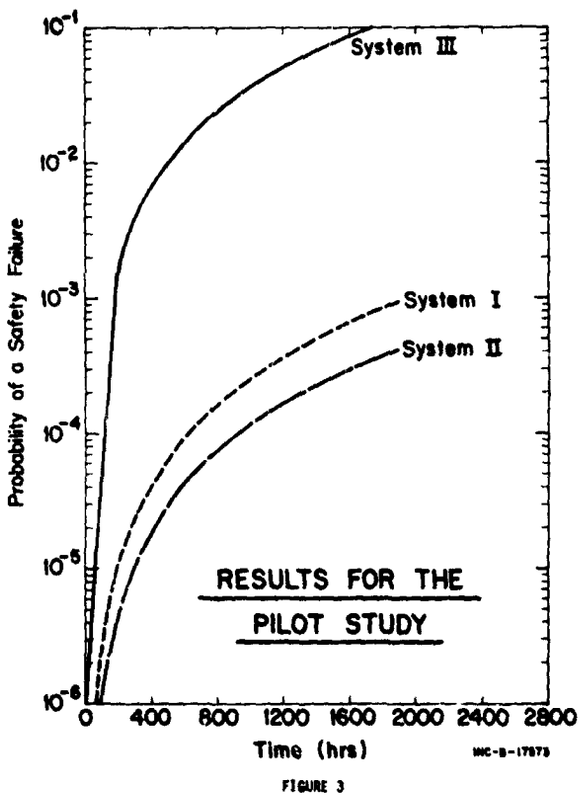


FIGURE 3

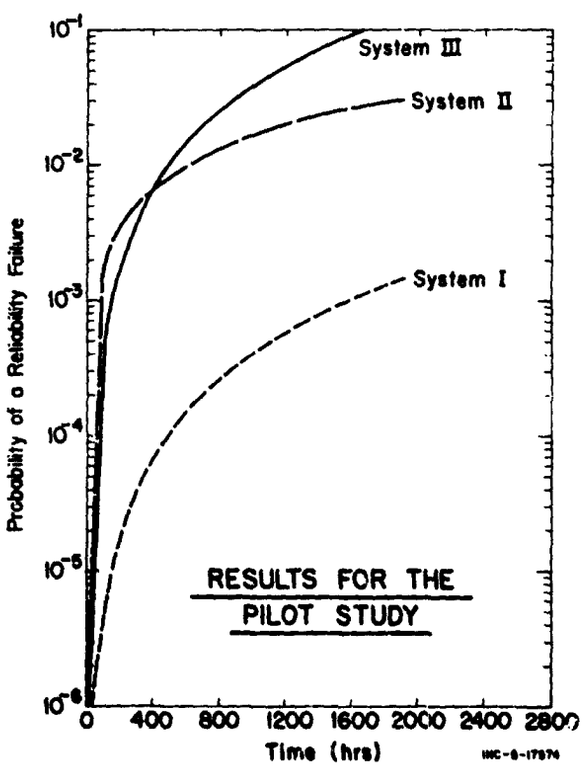


FIGURE 4

FAILED STATE PROBABILITY
VERSUS CHECKING INTERVAL

(relative to design)

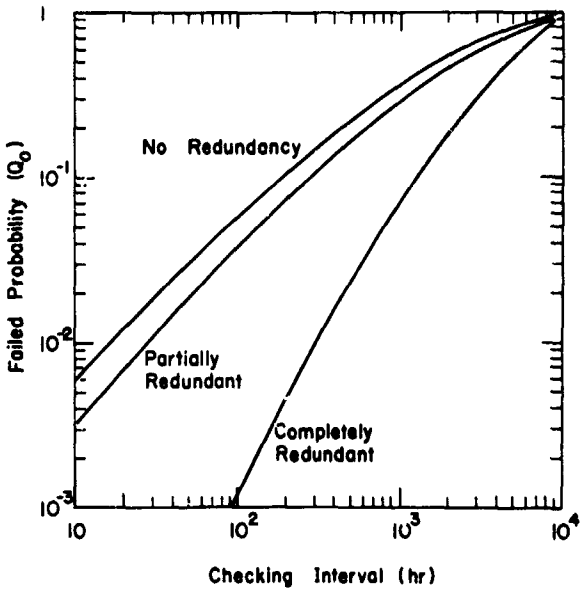


FIGURE 5

INJECTION FAILED STATE PROBABILITY
VERSUS COMPONENT CHECKING
INTERVAL

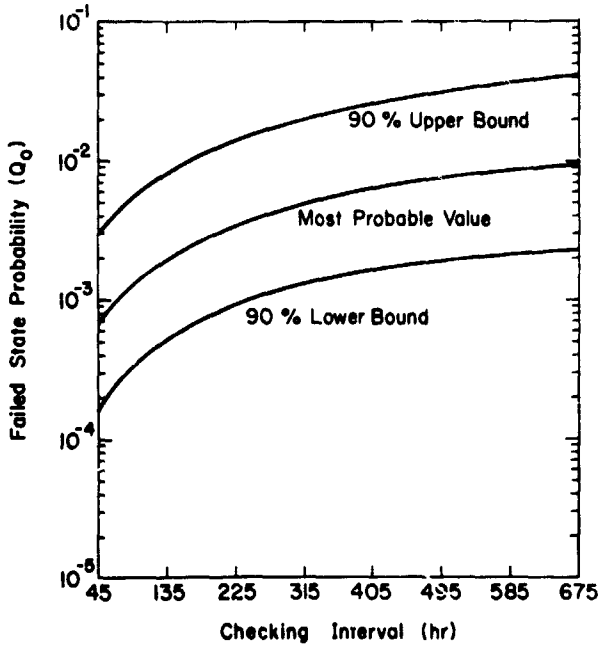


FIGURE 6