IAEA-TECDOC-591

Case study on the use of PSA methods: Backfitting decisions

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,– in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

IAEA-TECDOC-591

Case study on the use of PSA methods: Backfitting decisions

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

CASE STUDY ON THE USE OF PSA METHODS:
BACKFITTING DECISIONS
IAEA, VIENNA, 1991
IAEA-TECDOC-591
ISSN 1011–4289

Printed by the IAEA in Austria
April 1991

FOREWORD

Probabilistic Safety Assessment (PSA) is increasingly being used to complement the deterministic approach to nuclear safety. From the traditional discipline of reliability engineering, PSA developed as a structured method to identify potential accident sequences from a broad range of initiating events and to quantify their frequency of occurrence.

PSAs use inductive (event tree) and deductive (fault tree) logic and plant specific as well as generic component failure rates and frequencies of initiating events. Plant specific test and maintenance schedules, human errors and common cause failures are also considered in the probabilistic models.

PSA is nowadays a fundamental tool that provides guidance to safety related decision-making. By its very nature PSA recognizes the uncertainties associated with the logic models used to represent reality and quantifies the variability in the data of the parameters in the models.

The IAEA is promoting the conduct of PSA studies through standardization of the methodology, co-ordination of research, assistance through its Technical Co-operation Programme, and development of PSA software (PSAPACK). In addition it offers International Peer Review Services (IPERS) to review PSAs at various stages of completeness.

Emphasis at present is concentrated on "level-1" PSAs which quantify accident sequences up to estimates of core-damage probability. Level-2 (releases of radioactivity) and level-3 (off-site impacts) will be addressed at a later stage.

The work described above on the conduct of PSA is complemented by a programme on how to use the results of PSA in nuclear safety. For this purpose a series of CASE STUDIES has been prepared. The objective is to provide those who have performed PSAs with practical examples on how PSA results have been used. Those authorities and utilities still reluctant to request or perform PSAs will find convincing evidence on the benefits of such studies for nuclear safety.

With these objectives in mind, the IAEA requested a number of internationally recognized experts to document, in a uniform and suitable format, actual experience with the use of PSA for safety decisions. The documents were peer reviewed by an Oversight Committee for quality and completeness.

It is hoped that this series of CASE STUDIES will significantly contribute to the use of PSA to improve nuclear safety.

EDITORIAL NOTE

In preparing this material for the press, staff of the International Atomic Energy Agency have mounted and paginated the original manuscripts and given some attention to presentation.

The views expressed do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

The use in this book of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of specific companies or of their products or brand names does not imply any endorsement or recommendation on the part of the IAEA.

PREFACE

A series of CASE STUDIES has been prepared to summarize practical examples on how the results of PSA studies have been used in nuclear safety. They draw from the experience of major studies and, to the extent possible, use a similar format to guide the reader. The studies illustrate the range of applications in a specific topical area. It is the objective to take examples which are using level-1 PSAs rather than individual accident sequences or systems reliability. Emphasis is given to a logical step-by-step description of the analysis and documentation of calculational procedures and data. The interpretation of the results explicitly addresses the problem of uncertainties and limitations of the studies, and includes the results of Peer Reviews.

This case study addresses the problem of assessing different options of increasing safety by reducing the unavailability of safety systems. Using the example of a Low Pressure Injection System, the study compares the impact of three alternative options to improve unavailability. Using PSA techniques it is possible to quantify the reduction in unavailability in comparison to the original design. This information and cost estimates for the different options allow a rational decision which option to choose. Such a decision has to consider the uncertainties associated with the estimates.

The purpose of this CASE STUDY thus is to provide a practical example on how PSA can be used to determine the best options to improve the unavailability of a safety system.

The following additional Case Study documents are available:

IAEA-TECDOC-522	A Probabilistic Safety Assessment Peer Review: Case Study on the Use of Probabilistic Safety Assessment for Safety Decisions (1989)
IAEA-TECDOC-543	Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment (1990)
IAEA-TECDOC-547	The Use of Probabilistic Safety Assessment in the Relicensing of Nuclear Power Plants for Extended Lifetimes (1990)
IAEA-TECDOC-590	Case Study on the Use of PSA Methods: Determining Safety Importance of Systems and Components at Nuclear Power Plants (1991)
IAEA-TECDOC-592	Case Study on the Use of PSA Methods: Human Reliability Analysis (1991)
IAEA-TECDOC-593	Case Study on the Use of PSA Methods: Station Blackout Risk at the Millstone Unit 3 (1991)

CONTENTS

CONTENTS

Proposed plant and system design backfitting generally emanate from either of two distinct sources. Regulatory bodies may propose design backfits which are intended to enhance plant safety by improving equipment operability. Backfits of this type are often proposed in response to safety issues which have become newly recognized or which are believed to have recently become better understood and can, thus, be addressed in a more effective way. The second major source of proposed design backfits is the utilities which own and operate nuclear power plants. Backfits proposed by the operating utilities may be intended to address specific safety concerns, to achieve greater economy or operating efficiency, or, in some cases, may be developed as alternatives to more costly backfits proposed by regulatory bodies.

Whether proposed by a regulatory agency or by operating utilities, proposed design backfits can be, and frequently are, objectively evaluated using PRA techniques. In using PRA techniques to evaluate proposed backfits, one of three types of conclusions regarding the necessity or advisability of the backfit may be reached. First, applications of PRA techniques may indicate that the proposed backfit would result in attaining the desired effect in terms of plant safety levels and thus, should in fact be implemented. Secondly, use of PRA techniques may show that a proposed backfit would have no appreciable effect on plant safety and, therefore, should not be implemented. Lastly, the use of PRA techniques can, in some cases, be used to demonstrate that a similar level of safety can be achieved by implementing an alternative backfit which is less costly than the one which was originally proposed. Some examples of situations in which PRA techniques have been used to address backfit issues at operating nuclear power plants are summarized in Table 1.

When utilizing PRA results to determine the necessity or desirability of a backfit, it is first necessary to determine which quantitative measures of safety are appropriate to support the design process. Many potential safety indices can be developed from application of the set of PRA techniques to the assessment of plant and system designs. Selection of the appropriate measures should be linked to the initial motivation for the backfit. However, additional measures may also be appropriate to provide an improved view of the potential impact of the backfit.

The potential measures of safety are as follows:

Level of Resolution	Safety Measure(s)
a) System/Function	System Unavailability
b) Accident Sequence(s)	Sequence Frequency
c) Plant	Plant Damage State Frequency Core Damage Frequency Release Category
d) Site	Population Dose Early Fatalities Latent Cancer Fatalities Property Damage

TABLE 1. PRA RESULT UTILIZATION WITH RESPECT TO PLANT MODIFICATIONS

PRA Study	Impetus for Utility Involvement	Impact of PRA Findings on (Proposed) Plant Modifications
Zion PRA	Utility undertook study to verify the adequacy of the plant design, in response to NRC recommendations for design changes.	Based on calculation of offsite consequences, the utility was able to show they did not need a filtered vented containment, hydrogen recombiners, a core catcher, or core spray system modifications. No design changes are documented to have occurred as a result of the PRA.
Indian Point PRA	Same as Zion	Based on calculation of offsite consequences, the utility was able to show they did not need a filtered vented containment, hydrogen recombiners, or a core catcher. The utility did change the power supplies of the diesel generator fuel oil transfer pump, block a vent valve in the Diesel Generator (DG) Service Water System (SWS), replace manual isolation valves in the fan cooler SWS with Motor Operated Valves (MOVs), and upgraded the control building walls at Unit 2.
Big Rock Point PRA	Sought relief from NRC directives.	As a result of TMI and the Systematic Evaluation Programme (SEP) NRC required Big Rock Point to make plant modifications that would cost $49M; two times the estimated worth of the plant. The PRA was used to identify the cost-effectiveness of each modification. The utility was able to get exemptions on requirements totaling $46M based on the results of the PRA study. The major exemptions were on plant shielding, in-vessel instrumentation, and control room habitability. The utility implemented changes totaling $2.9M. The major modification was an alternate shutdown panel. Since the PRA was completed, the utility has used it as an ongoing management activity to request exemption from NRC directives; $2.4M of directives have been exempted and only $63K have been installed.

TABLE 1. (cont.)

PRA Study	Impetus for Utility Involvement	Impact of PRA Findings on (Proposed) Plant Modifications
Utility ATWS Study	Response to the NRC proposed rulemaking for ATWS	Utilities performed a detailed probabilistic evaluation of ATWS and cost-benefit analysis of ATWS rule options. Results showed that the proposed NRC rule was not cost-effective and that the utility rule was not only cost-effective, but provided adequate safety. The study was very instrumental in getting the NRC to compromise on its proposed rule.
Palisades PRA	Utility made commitment to have PRA models on all plants.	Study is presently incomplete, but partial findings were adequate to gain deferment of MSIV backfit modification imposed as result of SEP.
Browns Ferry Utility Study	Utility desired their own PRA model to parallel the IREP model.	Study is not complete yet, but partial findings were adequate to show that no modifications were required to the scram discharge volume.

Selection of the particular safety measure(s) will allow assessment of the potential benefit or adverse impact of a proposed backfit from a safety point of view. However, recognition of the level of uncertainty associated with each measure listed previously is least uncertain at the system level and becomes increasingly uncertain as the level of resolution becomes more global. In addition, site level safety measures include many factors not affected by plant design such as meteorology and demographics.

As mentioned previously, the safety measure chosen should be related to the backfit notification. If the backfit is to improve system availability, then system unavailability should be chosen as the safety measure.

However, when core damage frequency is the safety measure of interest, simply improving the availability of a particular safety system may not have the desired effect. This is because not all plant safety systems are equally important relative to core damage frequency. In attempting to achieve reductions in the calculated core damage frequency through backfits, it is necessary to first determine the relative importance of each safety system with respect to core damage frequency. Only by determining the relative importance of plant systems with respect to core damage frequency and, on that basis, proposing backfits which first improve the availability of the most important systems, can the overall core damage fequency be most effectively reduced.

A basic assumption of this backfit assessment process is that existing design criteria provide valid limits of acceptable design practices. Given that the analysis has not shown particular backfit requirement to be unnecessary, each backfit alternative must at least meet applicable functional and operability requirements and display features to satisfy existing safety and reliability requirements to some degree.

It is helpful to have some initial screening criteria to begin the process of selecting the optimum course of action in response to a specific regulatory, licensing or other proposed backfit requirements. A search for definitive safety criteria for either design or operation of LWR facilities in the United States resulted in the following general findings:

(1) So far, LWR technology has not been provided with firm numerical safety criteria at plant, system or component levels that could be used for design decisions. This is not critical, since failure to have quantitative criteria does not obviate the design optimization process.

(2) The existing qualitative safety criteria are scattered into many different documents with more or less legal import ranging from federal regulations (10CFR-20, -30, -50, and -100) to industry standards (ANSI, ASME, ASTM and ANS, etc.).

(3) The system level safety criteria found are subjective and qualitative and are solution oriented rather than requirement oriented. The guidance found is best illustrated by the following set of solutions that attempt to dictate dsign directions.

    (a) suitable redundancy
    (b) reasonable isolation
    (c) sufficient diversity
    (d) sufficient independence
    (e) sufficient margin to assure

Any backfit solution must, of course, comply with the applicable qualitative design criteria.

When quantitative plant safety criteria are established, the tools used to quantitatively assess design safety in backfit decisions may also be used to allocate these top requirements to lower and lower levels of detail. These allocated requirements could then be used as the preliminary screening criteria for competing backfit design solutions (or subcontracts and vendors, as applicable). All alternatives that can be predicated to meet the initial selection criteria can be compared by refined estimates of safety (or reliability, depending on application) and cost impact.

2. OVERVIEW OF THE ANALYSIS

Many methods and techniques are utilized in the performance of PRAs. Selection of the appropriate techniques for a particular backfit situation depends on not only development of the safety measures desired but also other factors.

The method that would best provide the desired safety measure(s) would:

(a) Measure the specific design features that are intended to provide safety in a particular backfit situation.

(b) Be proven form of analysis.

(c) Be able to analyze different types of designs (i.e., electrical, mechanical, structural, etc.) and provide comparable results.

(d) Be able to analyze a plant or system design at the appropriate level of resolution.

(e) Provide a permanent record of the reasons that particular backfit decision was indicated.

The decision process [1] depicted in Figure 1 begins with a determination that some type of backfit is required and the proposal of a specific backfit design. In evaluating the proposed backfit, it must first be positively determined that it meets the functional and operational requirements established by the design. If these requirements are not met, the backfit must be redesigned until they are. Once the functional and operability requirements are met, the backfit becomes a candidate for implementation and will be subject to the cost/benefit evaluation which is the basis of the design decision methodology.

In performing the cost/benefit evaluation, parallel efforts are initiated to thoroughly investigate both the real change in safety which would result from the backfit, and the total costs associated with a particular backfit. If the design being evaluated is considered to be the baseline design, this cost and safety information is established as a point of comparison against which alternative designs will be examined.

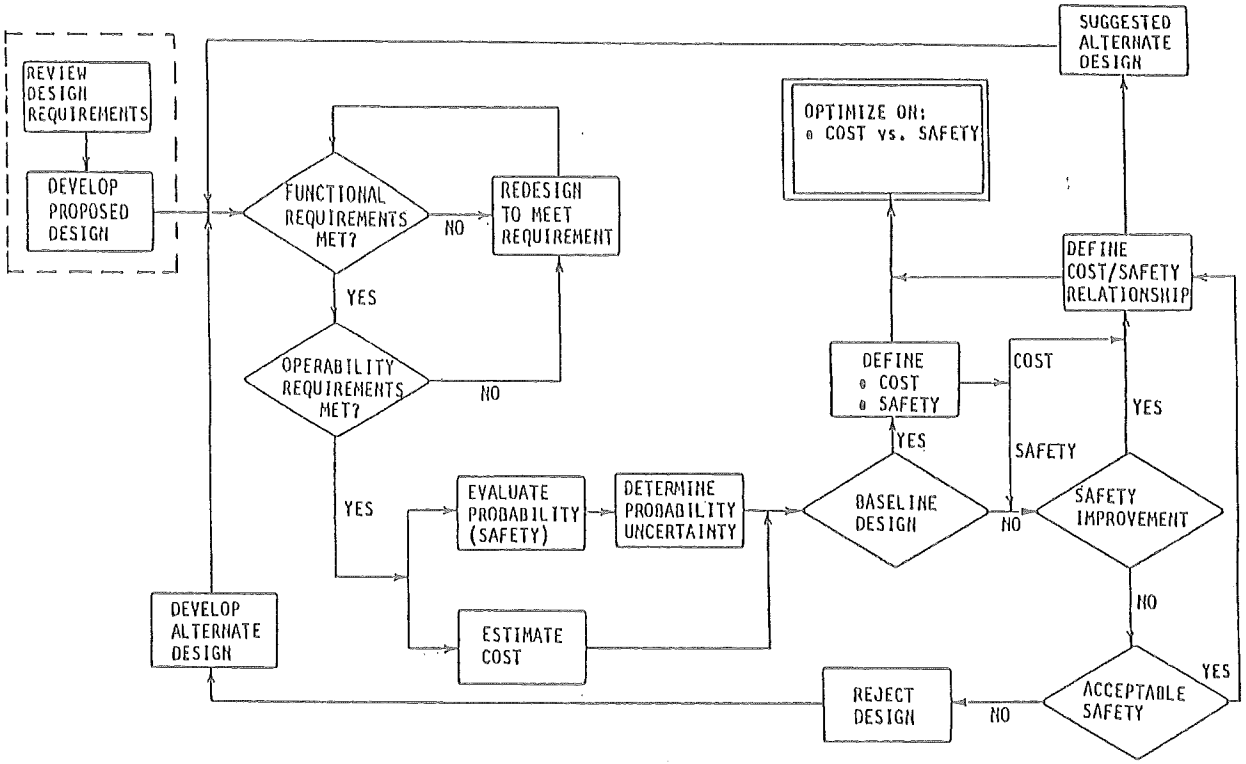


FIG. 1. Backfit design decision methodology flow chart.

Each alternative design backfit is examined to determine whether or not its associated level of safety is either an improvement over the baseline safety level or is at least minimally acceptable. If the safety level is not acceptable, the design is rejected and a new alternate design may be developed. If the safety level is an improvement over the baseline, or if it is at least minimally acceptable, the cost/safety relationship will be formally defined. Out of this definition of the cost/safety relationship comes a basis for cost/safety optimization. In addition, this cost/safety definition may suggest design alternatives which will be subjected to this design decision process.

When no quantitative statement of acceptable safety exists, three decisions are possible in each potential backfit situation:

(1) Provide the best possible safety evel for the cost implied by the initially required backfit design;

(2) Provide the level of safety implied by the initially required backfit design at the least cost; or

(3) Argue that the required backfit design does not materially improve the level of safety.

Each one of these decisions is addressed in the context of a hypothetical system backfit situation in an example include in this discussion.

The specific details of the decision flow can be tailored to the needs of the user and the user's design process. The essential ingredients of the process are:

(1) Quantification of the level of safety for the existing design;

(2) Quantification of the level of safety for the backfit design alternatives;

(3) Cost estimated of the backfit design alternatives;

(4) Optimization of cost and safety considerations, and

(5) Development of the above information in a timely fashion concurrent with the design process to support decision making.

Although an acceptable level of safety for plant system designs does not explicitly exist, a de facto safety requirement can be implied from an assessment of either the existing design or the initially required backfit design. This de facto quantitative safety requirement is used in the design process to assure that suggested alternatives meet the implied improvement of the initially required backfit and do not degrade the level of safety below the existing situation.

In some backfit situations, the potential exists for a given backfit to successfully achieve its intended effect relative to a particular safety consideration but in so doing, to degrade the level of safety in some unintended way. This situation will likely arise only when intersystem dependencies are effected by a proposed backfit. The design decision team must, therefore, take particular care to investigate how design backfit alternatives may effect these baseline intersystem dependencies.

The process of developing alternate designs is augmented by utilizing probabilistic system analysis techniques. This is because the analytical technique will identify which features of each design contribute the most to system failure. By concentrating on design solution which "fix" these problems, alternative designs are often "suggested" as a by-product of the analysis process.

3. ANALYSIS PROCESS

3.1. Scope of analysis activity

The scope of analysis must be tailored to the decision and trade-offs that are required. This is done in two ways, once at the beginning of analysis, and periodically when sensitivities to analysis factors are uncovered. The scope of the analysis depends on the level(s) of resolution of the safety measure(s).

3.1.1. Scope definition for a system level analysis

The purpose of the system analysis is to identify and evaluate significant contributors to the potential failure of systems and provide a quantitative measure of system unavailability. Definition of the top event to reflect the system's failure is the first step in fault tree analysis.

The top event definition includes consideration of the level of operating equipment failure which constitutes loss of system function, the operating mode of the system, the time frame of the failure and postulation of any other considerations which would impact fault tree development. The system operating modes to be included must be defined as operating within a defined environment or set of environments. Two main environments that must nearly always be considered are the normal environment (or ambient) and the environment during the accident that the safety system is designed to protect against. Other evironments may be included as dictated by special needs of a particular backfit.

The system to be analyzed is defined at two levels for the fault tree analysis. The first level of definition is a function one which is directly related to the system role that must be accomplished to successfully respond to an accident or transient condition (i.e. reactor protection, safety, injection, post accident heat removal). The second level of definition is a physical one which identifies the combination of hardware which is designed to provide the required function. This hardware definition provides the bounds for the system fault tree. It is important to identify the system bounds for the fault tree, as they may be different from system bounds as more traditionally described.

The system definition is such that all systems or functions which interface with the system of interest and could impact its intended operation are accounted for and described. Certain interfaces may be complex (i.e., instrumentation and control) and require specific definition of system limits as considered for a particular analysis. Some components may be identified as being within the bounds more than one system.

Rationale associated with the selection of each top event should be documented along with all basic considerations and assumptions made regarding system boundaries, performance and timing constraints.

As each system is examined in detail, faults are postulated consistent with the level of existing data and with providing visibility of the potential interaction between systems. The analysis developed is with iteration and reorganization as necessary to meet the demands of increased system understanding by the analyst and integration in the overall design decision process.

3.1.2. Special considerations for a system level analysis

The fault tree process allows the representation of common cause failures within individual systems. In addition, as a part of the fault tree process, elements common to more than one system and the various system interfaces are identified. These elements and interfaces are examined for common cause failures within each system fault tree.

When performing a system level analysis, it is important to note that a particular system may perform more than one safety function, especially under different postulated accident conditions. It is imperative that all pertinent functions of the system of interest be identified and that the system level analysis give due consideration to how the various system design backfit alternatives will effect each of these functions. The objective of this examination of various system functions is to verify that in achieving a desired effect in terms of a chosen system function, a proposed backfit is not unintentionally resulting in the degradation of some other function which is also performed by the system. In the case where multiple system functions are important to safety, an integrated

measure of plant safety, such as core damage frequency, should be considered.

The potential for human error must be considered as part of the detailed fault tree development process. Human errors should be considered as they might impact individual components as well as their potential impact on subsystem/system operation. Each individual should be evaluated to determine the potential for a human error to result in component failure. These errors include failure to take a required action or commission of an erroneous act. Human errors are included in the fault tree directly and are evaluated as part of the hardware contribution to system unavailability. Operator actions and errors may also impact system unavailability through test and maintenance activities.

Other potential human errors may result from a combination of hardware related actions, and activities related to test, calibration or improper procedural response which may affect an entire system as well as interfacing systems. The potential for those types of human errors are identified as part of the overall analysis process and are included in the common cause contribution to system unavailability.

3.1.3. Cost model scope

Typical models which have beendeveloped to describe plant life cycle costs contain many parameters and variables. In general, proposed plant design backfits will significantly effect only a few of these parameters and variables, thus making the task of estimating the total costs associated with a particular backfit relatively straightforward. A rational basis for comparing costs can be developed by examining the cost factors related to only those variables which are determined to be significant. In identifying significant cost variables associated with a particular design backfit, it should be noted that the various plant life cycle phases imply at least some differences in terms of which variables are likely to be of concern. For example, a backfit which is proposed during the plant construction phase may result in costs associated with plant construction delays, while the same change considered during plant operation may result in lost revenues due to plant down time. For most plant design backfits, significant cost variables are likely to include:

- Capital costs of hardware procurement, including spares.
- Labour costs associated with backfit implementation.
- Construction delays.
- Lost revenues due to plant shutdown or decreased power production during backfit implementation.
- Changes in maintenance costs.
- Engineering costs associated with backfit design.
- Cost of financing backfits.

Although additional variables will also impact the total costs associated with a particular backfit, these other variables will tend to be insignificant compared with those listed above. In addition, other variables such as operator training costs, system operational testing, health physics costs, security costs, and the like will tend not to vary significantly from one backfit alternative to another. For these reasons, consideration of cost variables listed above generally ensures that a reasonable basis for comparing the costs associated with various proposed design backfit alternatives has been developed.

3.1.4. Level of design detail

The level of detail that must be included in the analysis depends on what information is available and on what details is needed to make the decision. This further depends upon whether a backfit or a new plant requirement is under study. The backfit situation is explained herein and the new system decision data requirements can be extrapolated from, the tupes of data referred to.

When a requirement for backfit is being analyzed, there may be many ways to satisfy the requirement or there may be only two or three ways. If there are many candidate solutions, the detail about each candidate should include basic functional descriptions, simplified schematics, envelope drawing, general application information, experience data and acquisition cost. If there are only two or three candidates, more detail may be eventually needed to distinguish between them. As distinctions are made between closely competing alternatives, details, schematics and application drawings, specific test requirements, and operating procedures may be needed.

When the competition is close between the final alternatives, the unavailability of data forces some level of estimating based on engineering judgement and experience. It is important that, although this situation is not desirable, those aras where judgement had to be used to make the final decision must be documented for later traceability. Each place where judgement had to be used contributes to the uncertainty of evaluations for the decision being made and for any future modification proposals that are affected by the present decision.

It is important that the data used is as accurate and current as possible. In backfit evaluations, as-built Piping and Instrumentation Drawings (P & ID's) and schematics are needed, latest versions of operating procedures and technical specifications are essential, and if possible, some measure of the strictness with which Operating and Maintenance (O & M) procedures are implemented is helpful to assess any of the human factors that may contribute to design optimization. It is also desirable that the best possible component field experience and failure data be available.

3.2. Alternative system design generation

In actual practice, the credible options to satisfy a new requirement can come from many independent sources and can be categorized as follows:

(a) Do nothing, the proposed design change provides no improvement.

(b) Improve personnel training requirements or discipline.

(c) Change the operational and/or maintenance procedures.

(d) Change the operational envelope of some systems or of the whole plant.

(e) Change the operational envelope of some systems or the whole plant.

(f) Change component suppliers.

(g) Modify the application of some components.

(h) Modify some system design (added redundancy, monitors, etc.).

(i) Add a totally new system (including removal of an old system as needed).

(j) Remove, replace, rearrange or redesign groups of systems.

The decision methodology can handle any or all of the option categories in any combination and make distinction on safety versus cost of any number of options within category or group of categories.

In applying the design decision process, it is important that the process be recognized as an integral and essential part of the overall design activities. The design decision process cannot be regarded as a more peripheral element of the design task. It must be a central element.

As more is learned about the safety (functionally and probabilistically) and the cost impact of the different options, this is quickly fed back into the design process, whether on a new plant or on a backfit development. From this feedback, new options can be created that are expected to improve the cost or safety. When accompanied by appropriate analysis results, these new modifications can often be adopted in the design immediately depending on their impact on the overall modification.

Many options can result from the process itself, for example:

(a) add a redundant logic train,

(b) reverse the unpowered state of a relay or valve from normally open to normally closed, or vice versa, or

(c) use integrate solid state components in place of electro-mechanical, or use a hydraulic actuator rather than pneumatic.

3.3. Quantitative design criteria

Quantitative design criteria are a subject of considerable discussion and debate. Assignment of quantitative criteria infers an acceptable level of safety associated with the level at which the criteria are assigned.At the present time, there are no commonly accepted numerical measures of safety at any level plant, system, component, which can be used to guide the design and development process. This is partly due to problems associated with regulatory or other decision makers determining how safe is safe enough and confirming that quantitative criteria have been met. The concerns noted above are indicative of those generally associated with the numerical safety measures when used inon absolute sense.

For the purposes of design decisions, particularly at the system level, it is not necessary to utilize absolute numerical values for safety. The numerical values are to be used only in a relative sense. However, some notion of existing or acceptable values is desirable when screening alternative solutions. In that regard, for system level considerations it is assumed that the existing designs of currently licensed operating reactor safety system are acceptable.

In accomplishing the demonstration phase of this study, fault tree analyses were conducted of an existing system design and a measure of the level of safety determined. The numerical input data was applied consistently to the proposed alternative designs and the system level safety measures are evaluated on a comparative basis.

3.4. Uncertainty evaluation

Both the probability and cost estimates for a set of alternatives are defined over a range of possible values for each alternative due to uncertainties in the analysis models and the supporting experience data. When safety and cost estimates for each alternative are compared, it is necessary to know if these estimates differ by more than the probable error in each.

Four possible outcomes could occur when comparing an alternative design to the existing or baseline design. The combinations are:

(a) The system point estimate unavailabilities differ by more probable error, but the cost point estimates cannot be distinguished.

(b) The unavailabilities cannot be distinguished, but the cost estimates are very different.

(c) Both unavailability and cost are significantly different.

(d) Neither the unavailability nor costs are significantly changed by the alternative.

In the first combination, the most available design is chosen; in the second situation, the least cost design alternative is chosen. In combination (c), the correct decision is based on the following groundrules:

(1) The backfit must improve system availability, so any alternative displaying lower availability is rejected.

(2) If more than one candidate is compared to the baseline, the most available at the least proportional cost increase is selected.

(3) If only one backfit candidate is being compared to the baseline, the cost must be commensurate with the amount of improvement in system availability, and with the significance to plant safety of losing the system in the event of the initiating accident(s).

In the last combination (d), it would be usual to conclude that the backfit would not be cost effective to implement. If the uncertainty limits on the unavailability and cost point estimates are large compared to the mean estimate, some effort may be worthwhile to identify the main contributors to the uncertainty and attempt to make the input data more accurate. By narrowing the bounds on the leading contributors the statistical significance of the point unavailability and cost estimates can be improved, perhaps to a degree that allows some distinction between designs.

Cost estimating data, such as component purchase cost ranges or labor rates, can be treated as equally probable within maximum and minimum estimates. Economic factors such as the potential cost of capital or inflation need not be used (and therefore their uncertainties are avoided) as long as constant dollars can be used for all of the design alternatives. In some cases where trade-offs involve costs over widley differing time periods, monetary and economic factors may be required. For example, one option may incur a large cost in a very short imminent period and competing option may use the same money but spread over a larger period. If interest rates were not considered in this trade-off, a large error and uncertainty could be inadvertently introduced. In so far as possible, the total cost of backfit should be considered so that cost model uncertainties are kept to a definable minimum.

Component failure data is traditionally thought to be normally, lognormally, or binomially distributed. This is generally true if the components have simple binary internal failure mechanisms. If there are internal redundancies, the normal distribution of mean times between failure may not be accurate. For trade-off purposes, the normal, log normal, or Possion distributions well be accurate enough because the existing small samples of failure data will usually introduced more uncertainty than using the wrong distribution. There are several techniques for tracing failure rate uncertainties though the fault tree (e.g., SMAPLE was used for WASH-1400). There are thorough mathematical treatments of uncertainty and error in many texts on statistics and the interpretation of experimental data. These texts explain the principles and possible applications of error estimation that are almost directly applicable to fault tree analyses.

Ideally, of course, it would be most desirable to employ plant specific data derived from actual operation of each of the components for which failure rates are required. When the use of such data is feasible, the uses of relatively narrow uncertainty bounds may be justified. Very often, however, usually because of limited plant specific operating histories, generic data must be used to characterize component failure rates, thereby implying the use of somewhat wider uncertainty bounds.

In general, trade-off studies to optimize a series of choices in selcting the best design do not require that error bounds be determined very accurately. As a result, simplifying assumptions and approximations can be used (i.e. adopting some general distribution as representative of the component failure data). If the failure rates for the fault tree are treated as random variables, themselves having upper and lower bounds, then calculating the effects on the probability of the top event by varying the input variable failure rates provides a reasonable estimate of the uncertainty of the point estimate of safety system unavailability.

3.5. Optimization of factors

The engineering process of deciding on the "best" design relative to a set of requirements involves comparison of different designs with each other and comparison to predetermined criteria or measures of merit. In this context, the term "measure of merit" refers to some predefined target value for a selected measure of system operability or, in some cases, plant safety. Perhaps the most frequently used parameter for expressing a measure of merit in terms of system operability is system availability. The design that most nearly satisfies all of its requirements is the best choice (given that the requirements have been logically derived from overall

objectives). Quantitative measures are essential to determine which option "most nearly satisfies" the established criteria and requirements. Before defining the best set of factors to use to optimize the design, it is necessary to provide a brief rationale for the units selected.

Within the existing LWR design decision process there is a dichotomy between the reactor (and its associated power controles) and the safety systems such as containment, emergency core cooling, reactor protection and auxiliary feedwater systems. The Nuclear Steam Supply System (NSSS) is designed to minimize accident whereas the safety systems are designed to mitigate the effects of an NSSS accident, should it occur. Within this framework, the design optimization of a given system (or set of safety systems) can be accomplished by measuring the probability that each safety system will perform its functional requirements, given that those requirements are effective in containing (in a functional sense) the effects of an NSSS accident. Therefore, a safety system measure of safety merit can be its availability and dependability (which includes the system's demand reliability). Within this framework of present approaches to assuring system and LWR plant safety, the most available safety system at the least cost, can be defined to be the "best" system.

Although cost and safety issues can be expected to be the major factors in selecting a backfit alternative, it should be recognized that in any particular situation, a number of other considerations may influence the decision process. A requirement to satisfy deterministic design criteria or a determination that a certain type of computer software must be used in a system are both examples of additional constraints which may effect the decisions which are made. Such peripheral constraints must be recognized, and the safety/cost optimization process must be accomplished within them.

4. SYSTEM LEVEL BACKFIT EXAMPLE

In order to illustrate the potential application of a quantitative safety measure in the design process, a demonstration of the methods at the system level was in the design process, a demonstration of the method at the system level was performed. The system selected for this demonstration was the Surry Low Pressure Injection System (LPIS). The LPIS is designed to provide high flow, low pressure emergency coolant to the reactor core under certain loss of coolant accident conditions. The Surry system was selected because on analysis of its level of safety (unavailability) already exists in WASH-1400 [2] along with an appropriate data base for evaluation of alternate designs.

Three possible "backfit" options were postulated for the Surry LPIS. Each design alternative was reviewed for compliance with existing design criteria. An assumption was made that the present LPIS design in WASH-1400 [2] represents an acceptable level of safety. The demonstration is designed to simulate the following likely backfit scenario:

(a) A review by NRC of all emergency core coolant systems for potential weaknesses identifies the LIPS (Figure 2) as requiring modification to provide redundant pump discharge paths with redundant block valves in each path (Figure 3).

(b) The utility or architect engineer estimates the cost impact of the proposed change.

(c) The level of safety (unavailability) of the existing system and the required modification are derived.

(d) An alternate design (Figure 4) with redundant pump discharge and partially redundant pump suction lines is developed by the utility or architect engineer.

(e) The alternate design is assessed for its cost impact and level of safety.

(f) Based upon the safety and cost assessments of the previous three desings (baseline, required modification, and proposed alternative) a cost effective alternate design (Figure 5) which provides the same level of safety as the required modification is proposed.

This demonstration is illustrative of the approach which can be utilized in the backfit situation described above. The quantitative measure of the safety level for each system is obtained using the fault tree analysis technique considering only failure of the low pressure system to perform its injection function on demand. The cost estimate for each backfit alternative includes only material acquisition and installation costs. In a more detailed investigation the other cost variables listed in Section 3.1.3 would also be considered.

Each system design, including the baseline LPIS, is briefly described along with the point estimate of this level of safety in Section 4.1. A cost estimate is also described for each alternate backfit design. Section 4.2 summarizes the results of the safety and cost assessments for each system. The selection of the optimum design is described in Section 5.

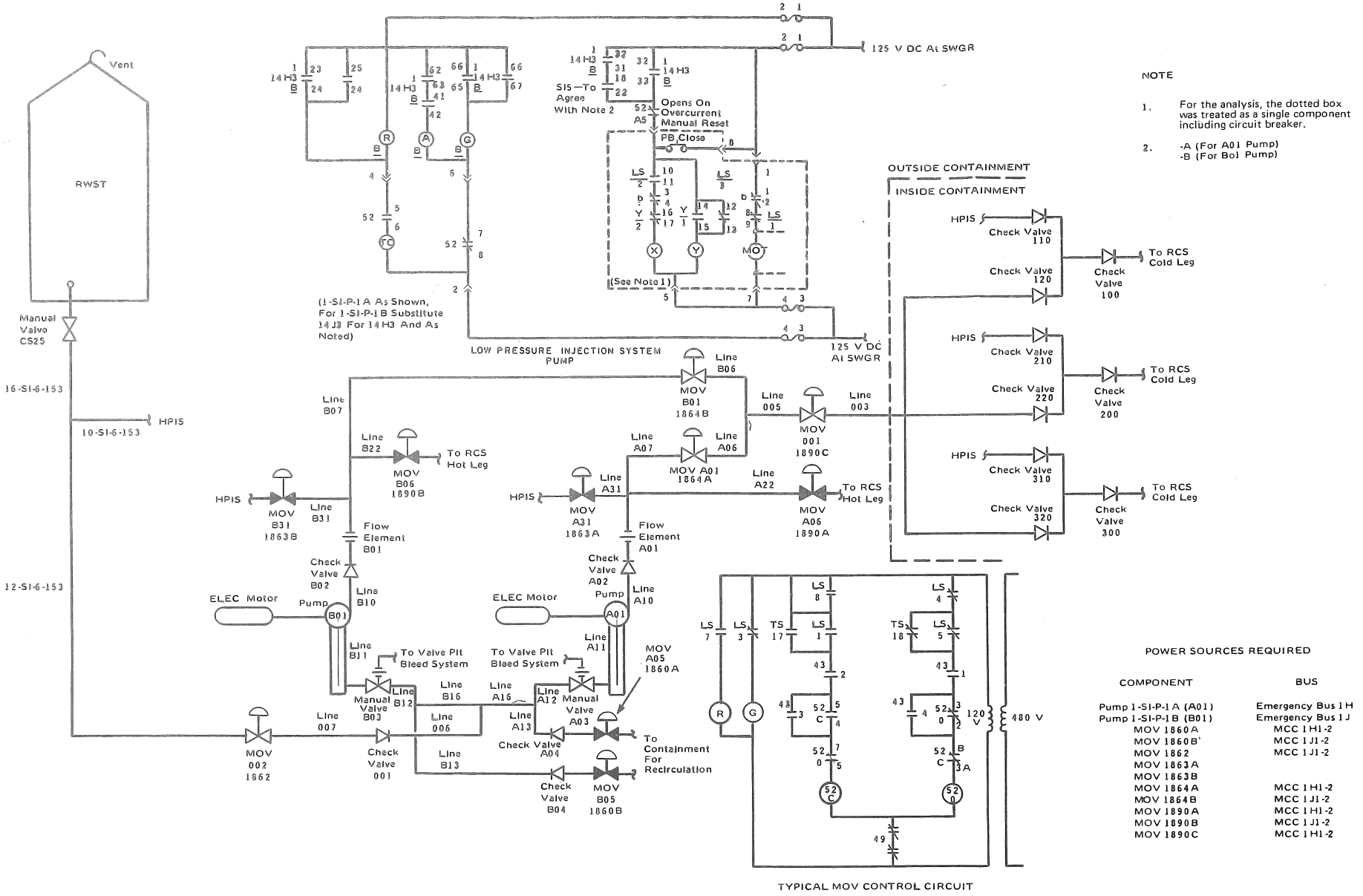
4.1. Design description

4.1.1. Baseline design description

Figure 2 is a flow diagram of the PWR of the Low Pressure injection System as analyzed in WASH-1400. The purpose of the LPIS is to provide a large volume of water to the reactor pressure vessel during the early post-accident period following a large loss of coolant accident (LOCA). The LPIS pumps are automatically activated by a Safety Injection Control System (SICS) signal whenever a combination of low pressure and low fluid level in the Reactor Coolant System (RCS) occures, or if high pressure in the containment is sensed. The following sections provide a brief description of the LPIS and the results of the WASH-1400 fault tree analysis.

Major Component Operating Characteristics

The LPIS includes the 350,000 gallon Refueling Water Storage Tank (RWST), two pumps in parallel redundancy and associated valves and piping. All block valves between the RWST and the reactor coolant system are local and/or remote controlled valves and are in the normally open position. Check valves in the cold leg injection lines are installed to preclude backflow from the high pressure (2000 psi) RCS to the pressure LPIS (600 psi).



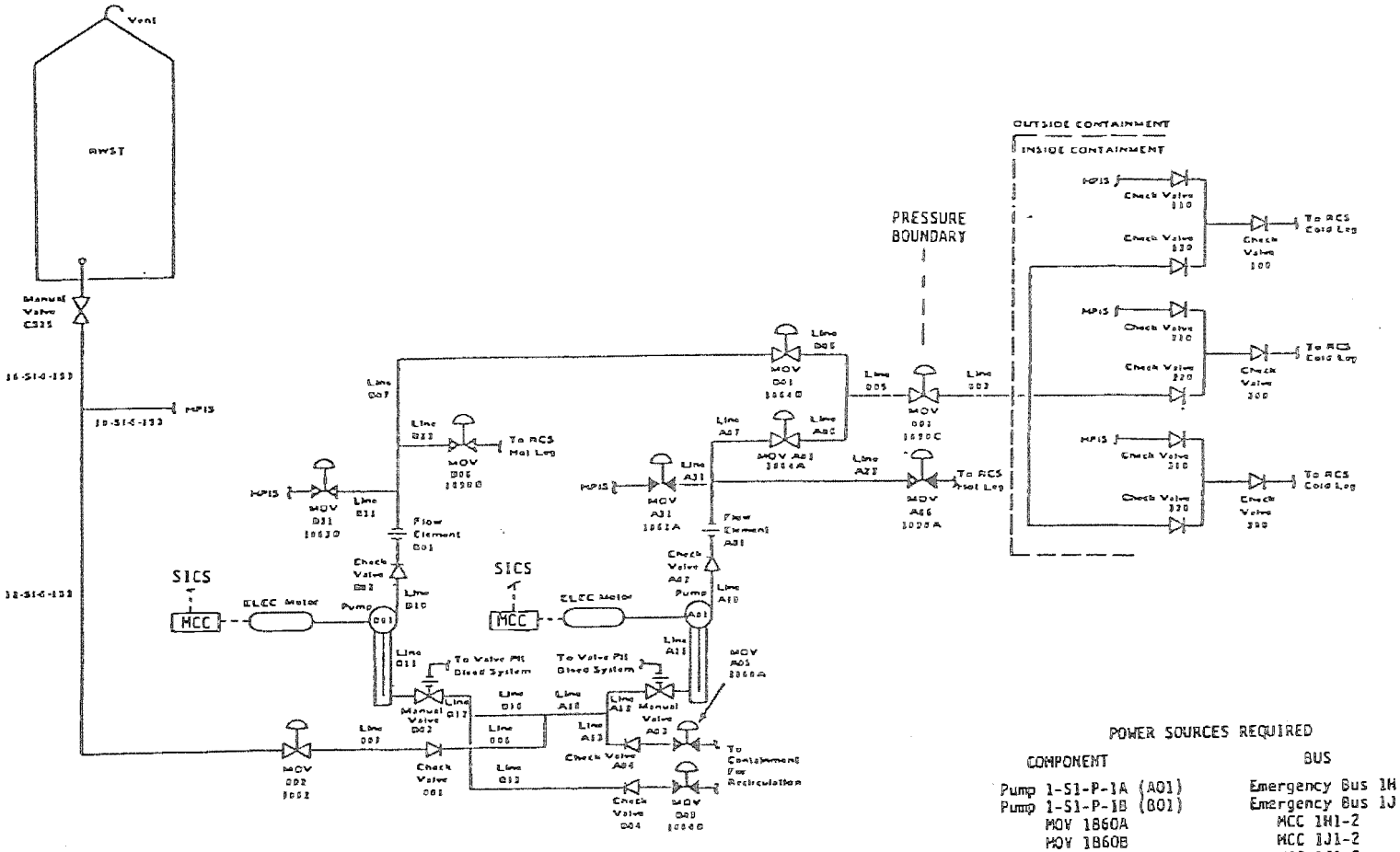
NOTE

1. For the analysis, the dotted box was treated as a single component including circuit breaker.
2. -A (For A01 Pump)
   -B (For B01 Pump)

POWER SOURCES REQUIRED

COMPONENT	BUS
Pump 1-SI-P-1A (A01)	Emergency Bus 1H
Pump 1-SI-P-1B (B01)	Emergency Bus 1J
MOV 1860A	MCC 1H1-2
MOV 1860B	MCC 1J1-2
MOV 1862	MCC 1J1-2
MOV 1863A	
MOV 1863B	
MOV 1864A	MCC 1H1-2
MOV 1864B	MCC 1J1-2
MOV 1890A	MCC 1H1-2
MOV 1890B	MCC 1J1-2
MOV 1890C	MCC 1H1-2

FIGURE II 5-34 Low Pressure Injection System Flow Diagram



POWER SOURCES REQUIRED

COMPONENT	BUS
Pump 1-SI-P-1A (A01)	Emergency Bus 1H
Pump 1-SI-P-1B (B01)	Emergency Bus 1J
MOV 1860A	MCC 1H1-2
MOV 1860B	MCC 1J1-2
MOV 1862	MCC 1J1-2
MOV 1863A	
MOV 1863B	MCC 1H1-2
MOV 1864A	MCC 1J1-2
MOV 1864B	MCC 1H1-2
MOV 1890A	MCC 1J1-2
MOV 1890B	MCC 1H1-2
MOV 1890C	

FIG. 2. Baseline low pressure injection system.

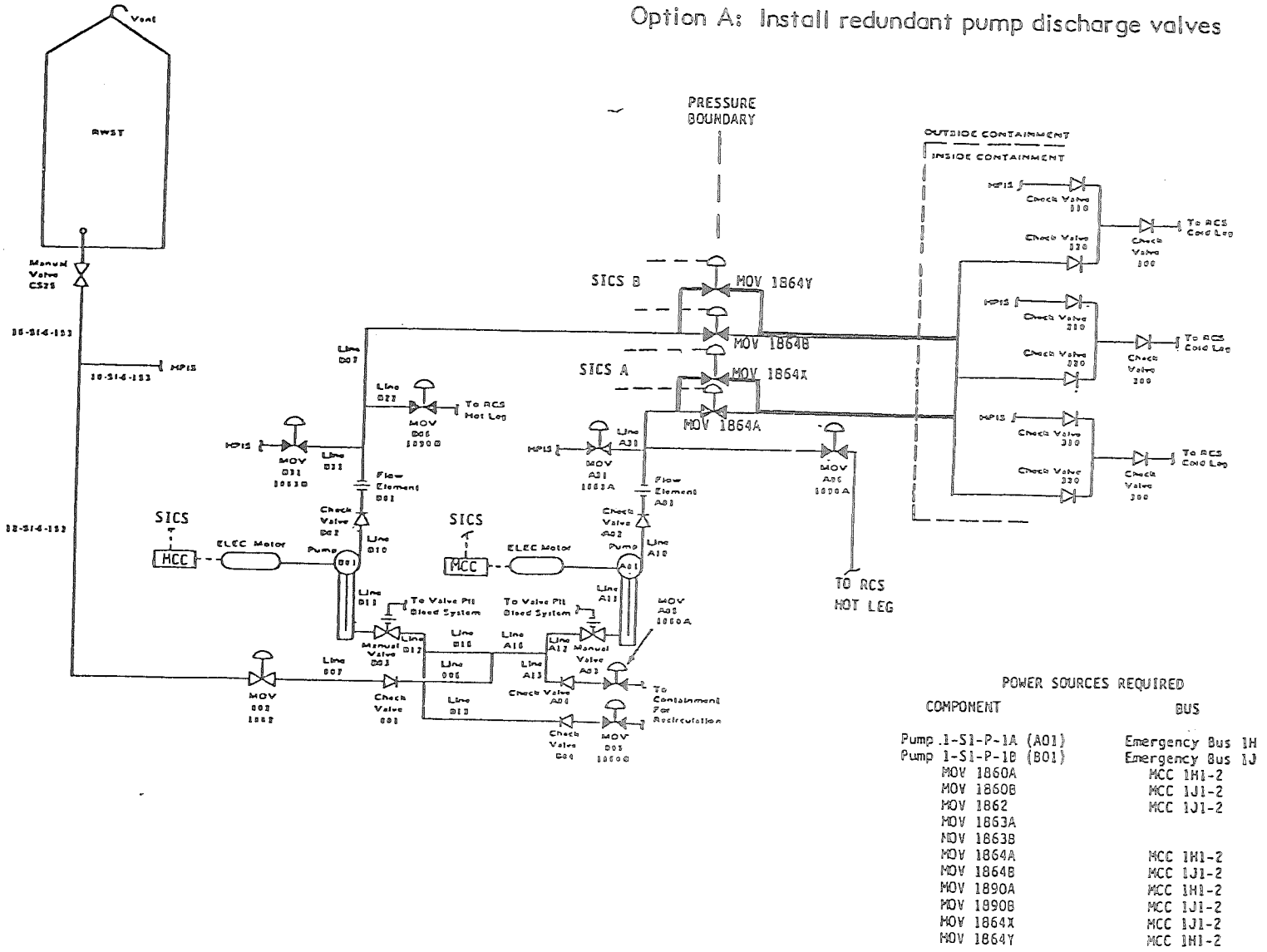
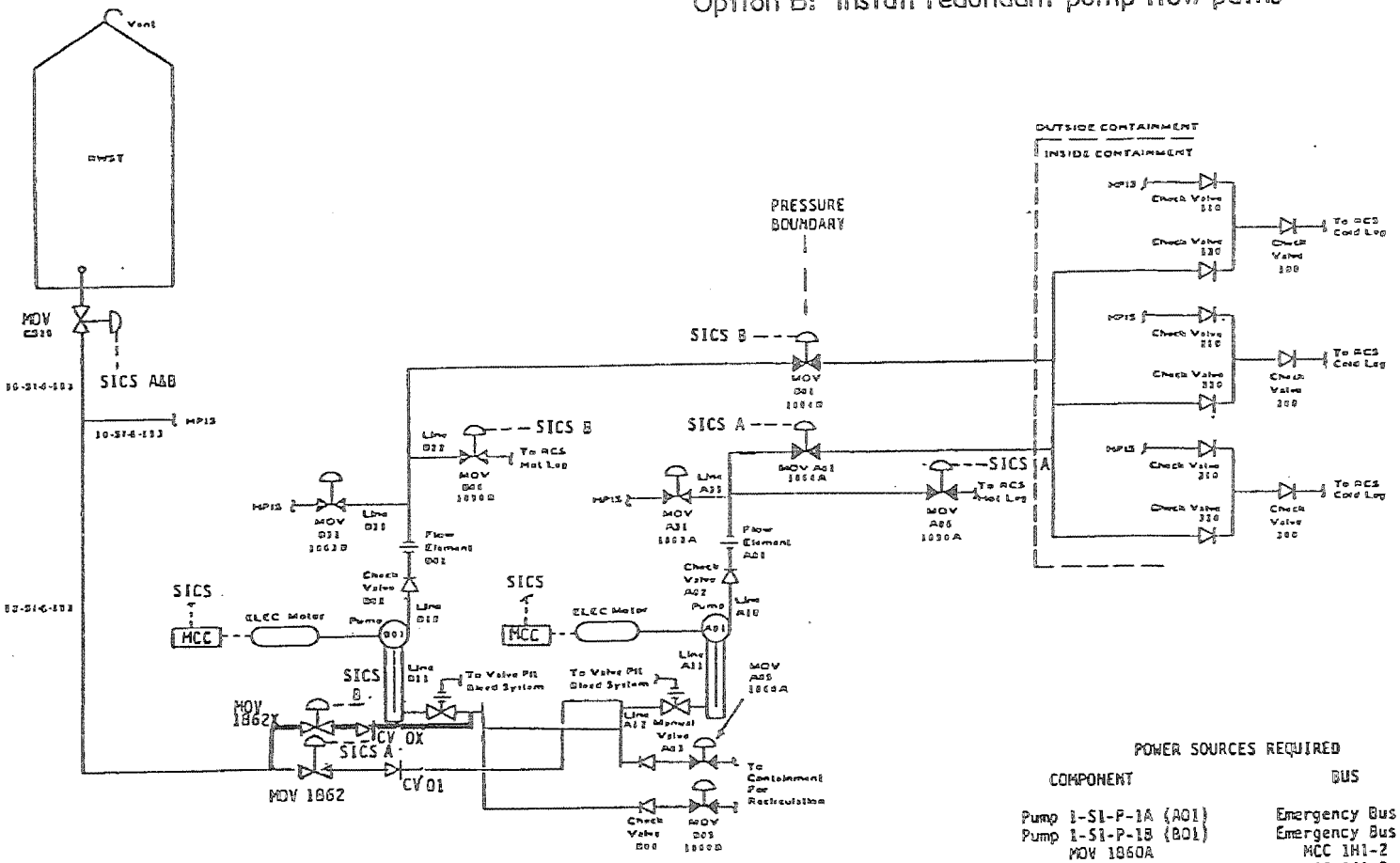


FIG. 3. Option 'A' low pressure injection system.

Option B: Install redundant pump flow paths

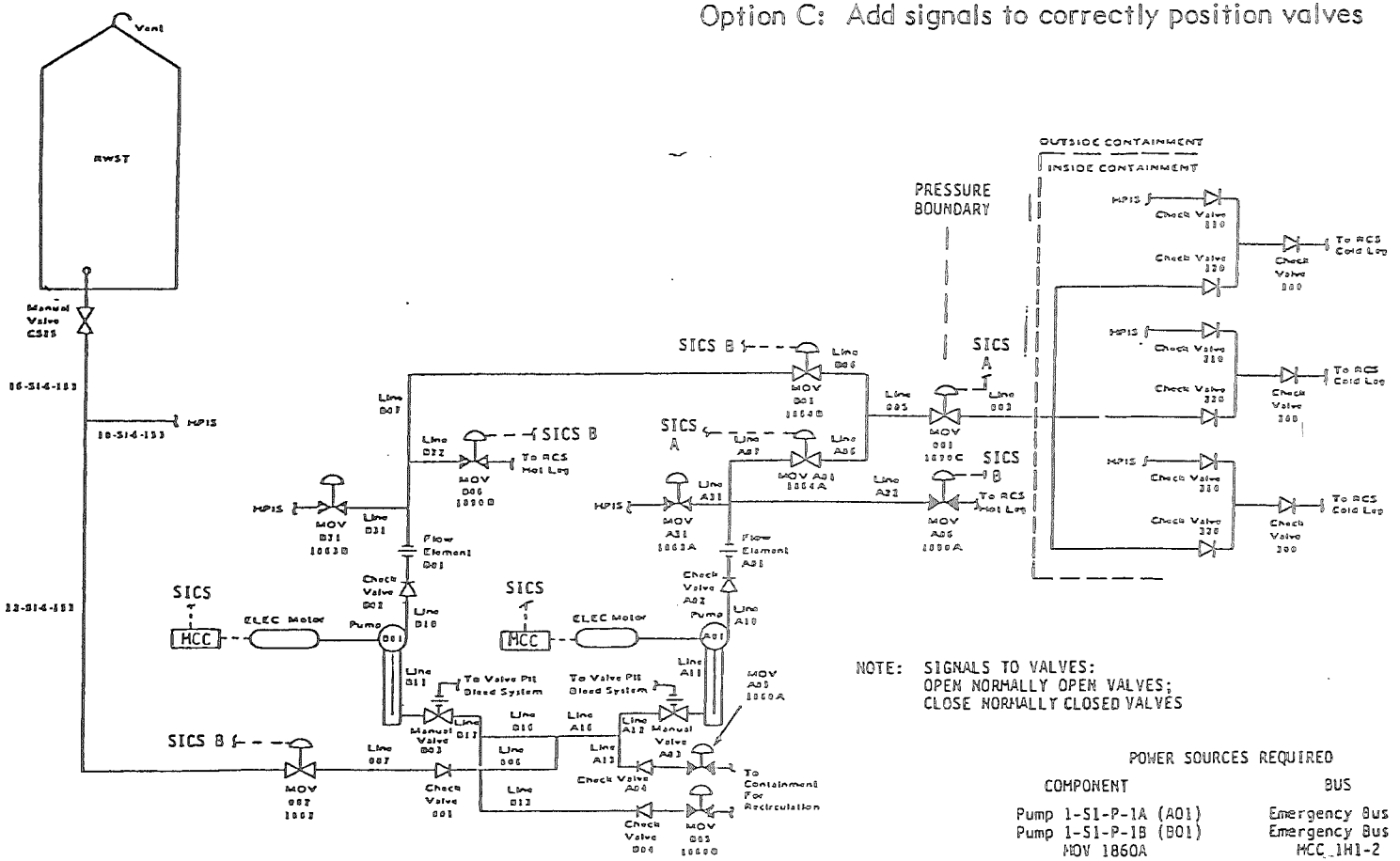


POWER SOURCES REQUIRED

COMPONENT	BUS
Pump 1-SI-P-1A (A01)	Emergency Bus 1H
Pump 1-SI-P-1B (B01)	Emergency Bus 1J
MOV 1860A	MCC 1H1-2
MOV 1860B	MCC 1J1-2
MOV 1862	MCC 1J1-2
MOV 1863A	
MOV 1863B	
MOV 1864A	MCC 1H1-2
MOV 1864B	MCC 1J1-2
MOV 1890A	MCC 1H1-2
MOV 1890B	MCC 1J1-2
MOV 1862X	MCC 1H1-2
MOV CS25	MCC 1H1-2

FIG. 4. Option 'B' low pressure injection system.

Option C: Add signals to correctly position valves



NOTE: SIGNALS TO VALVES:
OPEN NORMALLY OPEN VALVES;
CLOSE NORMALLY CLOSED VALVES

POWER SOURCES REQUIRED

COMPONENT	BUS
Pump 1-SI-P-1A (A01)	Emergency Bus 1H
Pump 1-SI-P-1B (B01)	Emergency Bus 1J
MOV 1860A	MCC 1H1-2
MOV 1860B	MCC 1J1-2
MOV 1862	MCC 1J1-2
MOV 1863A	
MOV 1863B	
MOV 1864A	MCC 1H1-2
MOV 1864B	MCC 1J1-2
MOV 1890A	MCC 1H1-2
MOV 1890B	MCC 1J1-2
MOV 1890C	MCC 1H1-2

FIG. 5. Option 'C' low pressure injection system.

Operability

The LPIS is initiated automatically by the SICS following a large LOCA. The pumps start upon receipt of the SICS and continue to supply fluid to the RCS until the RWST water supply is depleted (approximately 30 minutes). The output of either pump to the cold of the RCS is sufficient to provide adequate low pressure coolant injection.

Successful operation of the baseline LPIS design is defined based on the following two criteria:

(1) Either pump path A or B must provide sufficient flow, and
(2) Emergency coolant injection into only one of the three cold leg flow paths is required.

Criterion (1) is met if emergency coolant is delivered through either of the two redundant LPIS flow paths. Because the baseline design is normally aligned for injection, that is to say, no valves are required to change position prior to system operation, criterion (1) is met if one LPIS pump starts as required, continues to run for the duration of the injection phase, and if no faults exist in the non-redundant portions of the system.

Criterion (2) is satisfied if emergency coolant is delivered through either of the two remaining cold leg flow paths assuming a LOCA has occurred in one cold leg. The baseline design actually consists of three cold leg injection flow paths. Flow path success includes losing fluid out the broken cold leg.

A complete discussion of the LPIS failures which may render the system incapable of satisfying the criteria for successful system operation is presented in the Safety Level discussions.

Test and Inspection Specifications

The test and inspection frequency for major system components is based on a monthly or yearly cycle. The pumps and their drivers are tested monthly. In order to perform their test, no valve positions need to be changed. The pumps are simply started and water from the RWST is pumped back to the RWST via a two inch diameter test line on the pump discharge. The flow through this two inch line is instrumented by an orifice-plate type flow instrument. As can be seen from Figure 2, the pump will be delivering its discharge pressure up to check valves 110, 210, and 320. However, since the pump deadhead pressure is approximately 350 psi, no RWST water will be injected into the RCS cold leg during normal operation because the RCS normal operating pressure is 2000 psi. This pump test, therefore, provides and indication that a pump will start upon demand and provide reduced flow (through a two inch line).

The other major system components, the Motor Operated Valves (MOVs), are tested on a yearly basis. These valves are in a normally open position which provides the required flow path to the RCS without valve operation. The test consists of cycling the valve to ensure its opening and closing. The other MOVs (to HPIS, RCS hot leg, and Containment for Recirculation) and normally closed valves and are tested yearly as well. It is assumed that when the above major components are tested, their associated instrumentation and power is verified by successful operation.

Safety Level

The LPIS system chosen for the baseline design has been analyzed by the WASH-1400 study to determine its unavailability on demand. This unavailability is utilized in this demonstration as the measure of the safety level of the LPIS design. The point estimate of the LPIS safety level from WASH-1400 is:

$$Q_{total} = 4.2 \times 10^{-3}$$

The following is a brief description of the major contributors to this unavailability.

The fault tree model of the baseline design identified eleven quantitatively significant single faults which would constitute system failure. Of the total point estimate of 3.2×10^{-3} unavailability due to just LPIS hardware faults, these eleven single faults account for 3.2×10^{-3}. All of these singles are faults either of MOV 1890C or 1862 or erroneoulsy opening MOV 1890A or B fail the system and, collectively, account for 2.2×10^{-3}. In addition, the operator error of erroneously closing the manually operated RWST outlet valve, CS25, contributes 3.0×10^{-4}. The remaining single faults are all hardware faults associated with valves. Specifically, these include the internally failed open condition of MOV 1890A or B, or the internally failed closed condition of MOV 1890C, MOV 1862, manual RWST outlet valve CS25, or check valve 1890C. Collectively, these account for 6.0×10^{-4}.

Jointly, test and maintenance activities contribute 9.6×10^{-4} to the total LPIS system unavailability. It was determined that maintenance activities account for the entire test and maintenance contribution and that the system testing contribution to unavailability is negligible. This conclusion was reached by determining that during system testing, each pump is manually started by the operator in the control room and a limited amount of fluid is pumped through a test line. This test does not require isolation of the pump. If the LPIS is required during a system test, the pump is automatically returned to operating status. The motor operated valves are tested annually during refueling shutdowns when the LPIS is not required to be operable. Hence, pump and valve contributions to LPIS unavailability are negligible and $Q_t = E$.

Maintenance activites constitute a significant LPIS unavailability contributor. Maintenance of pumps and valves comprise the entire test and maintenance contribution. Pump maintenance times may range from 0.5 hours to 24.0 hours, with a log normal mean duration of 7.0 hours. The mean pump maintenance interval is estimated to be 4.5 months, yielding a main maintenance frequency of 0.22 maintenance/month. Utilizing the equation

$$Q_m = \frac{(\text{duration})(\text{frequency})}{\text{interval}},$$

the unavailability of one pump path due to pump maintenance is:

$$\frac{(7.0)(0.22)}{720} = 2.14 \times 10^{-3}$$

In accordance with the procedures set forth in the WASH-1400 study, the same values were used to calculate the unavailability of one pump path due to maintenance of the pump discharge motor operated valve. The total

unavailability of one pump path due to maintenance is, thus, $(2.14 \times 10^{-3})(2) = 4.28 \times 10^{-3}$. The contribution of the two redundant pump paths due to maintenance is obtained by multiplying the maintenance unavailability of one path by the fault unavailability of the other path and multiplying this project by two because two pathways exist. The LPIS unavailability due to maintenance of the two redundant pump paths is, thus, $(4.28 \times 10^{-3})(9.6 \times 10^{-3})(2) = 8.2 \times 10^{-5}$.

In addition to the maintenance contribution of the redundant pathways, four non-redundant motor operated valves may be subject to maintenance insofar as an operator may be required to verify the position of one of these valves. The four non-redundant valves subject to this verification are MOV 1862, MOV 1890A, MOV 1890B, and MOV 1890C. It was estimated that the mean verification time for this act is 0.72 hours and that the associated frequency is 0.22/month. Thus, the LPIS unavailability due to maintenance of these four valves is given by:

$$\frac{(4.0)(0.22)(0.72)}{720} = 8.8 \times 10^{-4}$$

The total LPIS unavailability due to test and maintenance, Q_{tm}, is given by:

$$Q_{tm} = Q_{test} + Q_{redundant} + Q_{non\text{-}redundant}$$

$$= E + 8.2 \times 10^{-5} + 8.8 \times 10^{-4}$$

$$= 9.6 \times 10^{-4}$$

In addition to the hardware and test and maintenance contributions, the evaluation of the baseline LPIS identified a common mode type contributor. The failure of both Safety Injection Control System (SICS) signal trains would result in LPIS unavailability and is estimated to have a probability of 4.5×10^{-5}. For the assessment of the design alternatives, common cause failure of both trains of the SICS was combined with the hardware failure of SICS for a total point estimate of 9.9×10^{-5}, and included in the hardware contribution to LPIS failure.

4.1.2. Option A design description

Figure 3 is a flow diagram of the hypothetical required modification to the LPIS based upon correction of an apparent weakness in the existing system. The Option A design is based upon the original Surry 1 FSAR LPIS design. The original design was the same as Option A (FSAR design) except that the LPIS was tied into the RCS hot-leg. During the design phase, prior to construction of Surry 1, it
was not acceptable and the design had to changed to reflect cold-leg injection with the capability for hot-leg injection. However, because the materials have been ordered based upon the "original" design, and the new requirements for both hot-leg and cold-leg injection, the decision was made to proceed with the design known here as the baseline design. As can be seen from Figure 3, the Option A design is the same as the baseline design except that (1) MOV 1890 C is removed, (2) Parallel MOVs are added to MOV 1864A and MOV 1864B, (3) a separate line from each pump train tie into the RCS header inside containment, and (4) MOV 1864A & B and their new parallel valves are changed to normally closed valves and open automatically upon receipt of the SICS.

Major Component Operating Characteristics

The LPIS Option A will operate in the same manner as the baseline design. The major system difference is that the RCS isolation valves, MOV 1864A, B, X and Y are normally closed and open upon the receipt of SICS. The Option A equipment configuration is very similar to the baseline design. The addition of parallel valves for MOV 1864A & B and elimination of MOV 1890C require that MOVs 1864A, B, X and Y ensure that the valves will open when required. The new penetration through the containment provides a separate path to the RCS for each pump train.

Operability

The Option A LPIS is initiated in the same manner as the baseline design. The SICS automatically starts pumps A01 and B01 and at the same time opens MOVs 1864A, B, X and Y. The Option A design meets the design criteria of (1) either pump A01 or B01 providing sufficient flow and (2) acceptable system performance will be achieved with only one of the three cold-leg providing flow into the RCS.

Successful operation of the Option A LPIS design is defined based on the same two criteria as for the baseline case.

Criterion (1) is met if emergency coolant is delivered through either of the two redundant LPIS pump flow paths. The Option A design has incorporated two normally closed redundant motor operated valves in both pump discharge lines, one of which must open upon receipt of an SICS signal in order for operation of that pump path to be successful. These redundant MOVs are 1864A, X, B and Y. Of course, successful operation of the pump paths depends on the successful start and continued operation of the LPIS pumps for the duration of the injection phase.

Criterion (2) is met if emergency coolant is delivered through either of the two remaining cold-leg flow paths in which a LOCA has not occured. The Option A design actually consists of three cold-leg injection flow paths. However, for the purposes of this analysis, a LOCA is assumed to occur in one of the three paths, leaving only two cold-leg injection flow paths intact.

A complete discussion of the LPIS failures which may render the system incapable of satisfying the criteria for successful system operation is presented in the safety level discussion.

Test and Inspection Specifications

The Test and Inspection procedures and frequency of Option A for the pumps and their drivers remain the same as the baseline. The test procedures also remain the same for the motor operated valves, but the frequency is increased to once per month for the valves which are now normally closed and must open for successful operation of the LPIS. The test frequency for the normally open valves is the same as considered in the baseline design, i.e., once per year.

Safety Level

The safety level of Option A was determined by utilizing the same analysis method and data that was used in WASH-1400. The fault tree analysis of the Option A design results in a total unavailability point estimate of:

$$Q_{total} = 2.9 \times 10^{-3}$$

Eleven quantitatively significant single faults were identified in the course of the fault tree analysis of the Option A design. Collectively, these eleven single faults accounted for an unavailability contribution of of 2.1×10^{-3} out of a total point estimate of hardware unavailability of 2.2×10^{-3}.

Nine of the eleven single faults are faults which are associated with system valves. Four of the nine are operator errors, three are mechanical failures of the valves in the closed position, and two are mechanical failures of the valves in the open position.

Specifically, the operator errors of erroneously closing the manually operated RWST outlet valve CS25, motor operated valve 1862, or erroneouly opening MOVs 1890A or B accounts for 1.5×10^{-3} of the system unavailability. Mechanical failures of valves in the improper position account for 5.0×10^{-4}. Valves which are subject to this failure mode are the manually operated RWST outlet valve, check valve 1890C, MOV 1862, and motor operated valves 1890A or B. In addition, the common cause type failure of both SICS signal trains was estimated to contribute 9.9×10^{-5} and plugging of the RWST vent contributes 4.4×10^{-7}.

Test and maintenance activities contribute an unavailability factor of 7.7×10^{-4}. It was assumed that monthly testing would be performed on the two LPIS pumps and on the normally closed motor operated valves MOV 1864A, X, B and Y. However, because opening the valves and starting the pumps for testing do not render the system unavailable, testing of these components does not constitute an unavailability contributor. MOVs 1862, 1890A, and 1890B are tested annually and do not contribute to the unavailability of the Option A design. Testing of the system components, then, has no effect on system unavailability.

Maintenance activities, however, do constitute an unavailability contributor. Pump maintenance times are estimated to have a log normal mean duration of 7.0 hours. The mean pump maintenance interval is estimated to be 4.5 months, yielding a mean maintenance frequency of 0.22 maintenance/month. The unavailability of one pump path due to pump maintenance is, thus:

$$\frac{(7.0)(0.22)}{720} = 2.14 \times 10^{-3}$$

Each of the two pump paths may also be unavailable due to maintenance of the MOVs in that path. Specifically, path A includes MOVs 1864 and 1864X and path B includes MOVs 1864B and 1864Y. The same maintenance durations and frequencies which were used to calculate pump unavailability were used to calculate the MOV unavailability due to maintenance. Thus, for each pump path, the unavailability due to MOV maintenance is,

$$\frac{(4.0)(0.22)(0.72)}{720} = 8.8 \times 10^{-4}$$

The total maintenance unavailability of each pump path is the sum of the pump maintenance unavailability and the MOV maintenance unavailability:

$$(2.14 \times 10^{-3})(4.28 \times 10^{-3}) = 6.4 \times 10^{-3}$$

The total Option A LPIS unavailability which results from maintenance of components in the redundant paths is obtained by multiplying the maintenance unavailability of one path by the fault unavailability of the other path and multiplying this product by two because two pathways exist. The unavailability due to maintenance of the two redundant pump paths is, thus,

$$(6.4 \times 10^{-3})(8.5 \times 10^{-3})(2) = 1.1 \times 10^{-4}$$

In addition to the maintenance contribution of the redundant pathways, three non-redundant valves may require maintenance in the form of operator verification of their position. These three valves are MOV 1862, 1890A, and 1890B. It was estimated that the mean verification time for this act is 0.72 hours and that the associated frequency is 0.22 per month. Thus, the Option A design unavailability due to maintenance of the three non-redundant valves is given by:

$$\frac{(3.0)(0.72)(0.22)}{720} = 6.6 \times 10^{-4}$$

The total Option A design unavailability due to test and maintenance, Q_{tm}, is given by:

$$Q_{tm} = Q_{test} + Q_{redundant} + Q_{non\text{-}redundant}$$

$$= E + 1.1 \times 10^{-4} + 6.6 \times 10^{-4}$$

$$= 7.7 \times 10^{-4}$$

Estimated Costs

The estimated capital costs for Option A are based upon the general costing, design guidelines and assumptions as identified in Section 3.1.3. The actual implementation of this option would require the following (refer to Figures 2 and 3):

(1) Remove MOV 1890C
(2) Re-use MOV 1890C for MOV 1864B
(3) Install (3) new 10 inch MOVs for MOVs 1864A, X, and Y
(4) Fabricate and install spool piece from MOV 1864A and X to line 003
(5) Fabricate and install spool piece from MOV 1864 and Y to RCS header through existing unused containment penetration
(6) Install new conduit, fittings, and cable to MOVs 1864A, B, X and Y

The material and labor costs for modifying the LPIS to the Option A configuration are detailed in Table 4. The total cost is US $376,360. Engineering, licensing, quality assurance and operating costs are not included in this cost estimate.

4.1.3. Option B design description

The initially considered utility alternate to the required modification is shown in Figure 4 and referred to as Option B. The Option B design was selected for consideration because of its apparent cost advantages over the Option A design and qualitative improvements in unavailability over the baseline design.

The design changes consist of eliminating MOV 1890C, adding a separate penetration through containment so that each pump has a separate path to the RCS header, changing MOVs 1864A and B to normally closed valves and increasing their pressure rating, providing parallel pump suction lines including new valves MOV 1862X and CVOX, adding a motor operator to manual valve CS25, and adding SICS signals to all valves to ensure their proper position in the event the SICS is initiated.

Major Operating Characteristics

The Open B design will operate in the same manner as the baseline design. The major system difference is that the RCS isolation valves, MOV 1864A and B are normally closed and open upon receipt of the SICS. The equipment configuration for Option B is similar to the baseline design with the major difference being the elimination of MOV 1890C. This charge necessitates the upgrading of MOV 1864A and B to a higher pressure rating. The addition of SICS to MOV 1864A and B ensure that the valves will open when required. The new penetration through containment provides a separate path to the RCS for each pump train.

Operability

The Option B LPIS is initiated in the same manner as the baseline design. The SICS automatically starts pumps A01 and B01 and at the same time opens valves MOV 1864A and B, gives MOVs CS25, 1862X, 1862 "stay open" signals.

Successful operation of the Option B LPIS design is based on the same two criteria as the baseline case.

Criterion (1) is satisfied if emergency coolant is delivered through either of the two LPIS pump flow paths. Normally closed motor operated valves 1864A and 1864B are required to open upon receipt of an SICS signal in order for the operation of their associated pump paths to be successful. As in the case of the baseline design, once all valves are properly aligned, the LPIS pumps are required to start on command and continue operation for the duration of the injection phase.

Criterion (2) is satisfied if emergency coolant is delivered through either of the two cold-leg injection flow paths which are not effected by the postulated LOCA. No deviations from the baseline design inside containment were incorporated into the Option B design.

A complete discussion of the LPIS failures which may render the system incapable of performing its intended function is presented in the safety level discussion.

Test and Inspection Specifications

The test and inspection procedures and frequency of Option B for the pumps and their drivers remain the same as the baseline design. The test procedures also remain the same for the motor operated valves but the frequency is increased to once per month for the valves which are now normally closed (MOVs 1864A and B) and must open for successful LPIS operation. The test frequency for the normally open valves is the same as considered in the baseline design, i.e., once per year.

Safety Level

The safety level of Option B was determined by utilizing the same analysis method and data that was used in WASH-1400. The fault tree analysis of the Option B design results in a total unavailability point estimate of:

$$Q_{total} = 1.2 \times 10^{-3}$$

The fault tree analysis of the Option B LPIS design revealed that of a total design hardware unavailability point estimate of 4.8×10^{-4}, five single faults account for 4.0×10^{-4}. Three of these five single faults are the mechanical failure of system valves in the improper position. Specifically, the RWST outlet valve MOV CS25 in the closed position or MOV 1890A or B in the open position contribute 3.0×10^{-4} collectively. The remaining two single faults are the common mode failure of both SICS signal trains which contributes 9.9×10^{-5} and plugging of the RWST tank vent which contributes 4.4×10^{-7}.

The remainder of the Option B LPIS design point estimate of hardware unavailability derives from 40 double cut sets.

Test and maintenance activities constitute the largest unavailability contributor for the Option B LPIS design, accounting for 7.3×10^{-4}. Pump maintenance in each of the redundant pump paths is assumed to occur with a frequency of 0.22 per month. The log normal mean ppump maintenance duration is estimatd to be 7.0 hours. The option B unavailability of one pump path due to pump maintenance is, thus,

$$\frac{(7.0)(0.22)}{720} = 2.14 \times 10^{-4}$$

One motor operated valve in each pump path will also require maintenance. This is MOV 1864A or B. The same frequency and duration values were assumed for valve maintenance that were used in calculating pump maintenance unavailability. Thus, the unavailability of each path due to valve maintenance is 2.14×10^{-3}. The total system unavailability due to maintenance of the redundant path by the fault unavailability of the other path and multiplying this product by two to represent the two pathways. The total system unavailability due to maintenance of the redundant pump paths is:

$$(2)(4.3 \times 10^{-3})(8.6 \times 10^{-3}) = 7.4 \times 10^{-5}$$

In addition to maintenance performed on components in the redundant pump paths, maintenance is also performed on the three non-redundant MOVs, CS25, 1890A, and 1890B, in the form of verification of their positions. This is assumed to occur 0.22 times per month with a log normal mean duration time of 0.72 hours per occurrence. Unavailability due to verification of the position of these three valves is given by:

$$\frac{(3)(0.22)(0.72)}{720} = 6.6 \times 10^{-4}$$

Maintenance must also be performed on MOVs 1862 and 1862X. Unavailability due to maintenance on these valves is obtained by multiplying the maintenance unavailability of one valve by the fault unavailability of the other and multiplying this product by two because

there are two of these valves. This maintenance unavailability contributor is given by:

$$\left[(2)(1.0 \times 10^{-4})\right]\left[\frac{(7)(0.22)}{720}\right] = 4.28 \times 10^{-7}$$

The total Option B LPIS design unavailability due to maintenance is given by:

$$Q_m = Q_{m\ \text{redundant}} + Q_{\text{non-redundant}} + Q_{1862}$$

$$= (7.4 \times 10^{-5}) + (6.6 \times 10^{-4}) + (4.3 \times 10^{-7})$$

$$= 7.3 \times 10^{-4}$$

It was determined that testing activities do not contribute to the Option B design unavailability. The entire test and maintenance contribution is therefore due to maintenance activities.

Estimated Costs

The estimated capital costs for Option B are base dupon the following tasks:

(1) Add SICS signals to seven valves, (MOV 1864A, B; 1890A, B; 1862, X; CS25) including the additional conduit, fittings, and cable.
(2) Remove MOV 1890C
(3) Remove 1864B and install MOV 1890C
(4) Install new 10 inch MOV for MOV 1684A
(5) Install new 12 inch MOV for MOV 1862X including two 12 inch diameter tees and 150# check valve for CVOX
(6) Install new actuator for MOV CS25 including new power hook-up
(7) Fabricate and install new piece from MOV 1864A to line Q03
(8) Install tee in RCS header and tie in new fabricated spool piece from MOV 1864B through existing unused penetration.

The total material and labor cost for modifying the LPIS to the Option B configuration are detailed in Table 4. The total cost ist US $354,665. Engineering, licensing, quality assurance and operating costs are not included in this cost estimate.

4.1.4. Option C design description

Based upon the fault tree evaluation of the baseline and Option A, a possible "fix" is suggested which involves providing signals to motor operated valves to reduce the contribution to LPIS unavailability due to some human errors. Option C, shown in Figure 5, was selected as an example of a design alternative which may become evident as a result of the safety assessment process. The Option C design is a simple improvement of the existing baseline design, consisting of only the addition of SICS signals to MOVs to ensure their proper operation.

Major Component Operating Characteristics

The Option C design will operate in the same manner as th baseline design. Upon initiation of the SICS, the pumps A01 and B01 will start and supply water from the RWST to the RCS via all normally open valves. The

major system difference is that the normally open valve will receive a "stay open" signal and the normally closed valves will receive a "stay closed" signal.

Operability

The Option C LPIS operates in the same manner as the baseline design and meets the original design requirements. The successful operation of the Option C LPIS design is dependent on satisfying the same two criteria as in the baseline case.

Criterion (1) is satisfied if emergency coolant is delivered via either of the two LPIS pump flow paths. As all system valves are normally aligned for injection, only the start and continued operation of the LPIS pumps is required.

Criterion (2) is satisfied if emergency coolant is delivered through either of the two cold leg injection flow paths which are not effected by the postulated LOCA. No deviations from the baseline design inside containment were incorporated into the Option C design.

A complete Discussion of the LPIS failures which may render the sytem incapable of performing its intended function is presented in the safety level discussion.

Test and Inspection Specifications

The Test and Inspection procedures and frequency of the Option C design are the same as for the baseline design.

Safety Level

The safety level of OptionC was determined by utilizing the same analysis method and data that was used in WASH-1400. The fault tree analysis of the Option C design results in a total unavailability point estimate of:

$$Q_{total} = 2.0 \times 10^{-3}$$

The fault tree analysis of the Option C LPIS design showed that nine single fault events account for 1.0×10^{-3} out of a total hardware point estimate of 1.1×10^{-3}. Seven of the nine single faults are valve faults.

Specifically, the manually operated RWST outlet valve CS25, motor operated valve 1862, check valve 1890C, and motor operated valve 1890C may all fail mechanically in the closed position. Collectively, the failure of these four valves in this mode accounts for 4.0×10^{-4}. Motor operated valves 1890A or B may fail mechanically in the open position. These single faults contribute 2.0×10^{-4}. A postulated operator error in which an operator erroneously closes the manually operated RWST outlet valve accounts for 3.0×10^{-4}. In addition, the common mode failure of both SICS train signals accounts for 9.9×10^{-5} and plugging of the RWST tank vent contributes 4.4×10^{-7}.

Test and maintenance activities provide a total contribution of 9.5 x 10 to the Option C LPIS design unavailability. Pump maintenance in each of the two redundant trains was calculated based on an estimated

frequency of 0.22 per month and a log normal mean duration of 7.0 hours. The unavailability of one pump path due to pump maintenance is given by:

$$\frac{(7.0)(0.22)}{720} = 2.14 \times 10^{-3}$$

Each pump path also contains an MOV which is either MOV 1864A or B that required maintenance. The valves which were assumed as the frequency and duration for pump maintenance were also applied for the maintenance calculations of MOV 1862A and B. The unavailability of one pump path due to valve maintenance is thus also 2.14×10^{-3}. The total unavailability of one pump path due to maintenance of pumps and valves is 4.3×10^{-3}. The total system unavailability due to maintenance of the redundant pump paths is obtained by multiplying the maintenance unavailability of one path by the fault unavailability of the other path and mulitplying that product by two to represent the two paths. The total unavailability of the system due to maintenance of the redundant paths is given by:

$$(4.3 \times 10^{-3})(8.6 \times 10^{-3})(2) = 7.4 \times 10^{-5}$$

In addition to the maintenance which must be performed on components within the two redundant pump paths, it is expected that verification of the positions of the four non-redundant valves, MOVs 1862, 1890A, 1890B, and 1890C, will be required and that this act will assume frequencies and durations of 0.22 and 0.72, respectively. System unavailability due to maintenance of the four non-redundant valves is given by:

$$\frac{(4)(0.22)(0.72)}{720} = 8.8 \times 10^{-4}$$

The sum of the redundant component maintenance unavailability and the non-redundant component maintenance unavailability is the total unavailability of the system due to maintenance:

$$(7.4 \times 10^{-5}) + (8.8 \times 10^{-4}) = 9.5 \times 10^{-4}$$

It was determined that testing of the Option C design components does not constitute a contributor to the system unavailability. The entire test and maintenance contributor is thus due to system maintenance.

Estimated Costs

The estimated capital costs for Option C are based upon the addition of SICS signals to MOV 1890C, MOV 1864A, B, MOV 1890A, B, MOV 1862 including conduit, fittings and cable. The material and labor costs for modifying the baseline LPIS to the Option C configuration are, as detailed in Table 4, US $71,580. Engineering, licensing, quality assurance and operating costs are not included in this cost estimate.

4.2. Assessment of alternatives

After estimates of system unavailability and design modification costs have been made for each of the alternative designs under consideration, the next logical step in assessing the various alternatives is to make a comparative examination of the alternatives. Table 2 lists the major LPIS system components for the baseline design as well as for each of the three design alternatives. Table 3 provides a listing of the various

TABLE 2. MAJOR LPIS SYSTEM COMPONENTS

BASELINE	OPTION "A"	OPTION "B"	OPTION "C"
RWST	RWST	RWST	RWST
LPI pump A01	LPI pump A01	LPI pump A01	LPI pump A01
LPI pump B01	LPI pump B01	LPI pump B01	LPI pump B01
Local manual RWST outlet valve CS25	Local manual RWST outlet valve CS25	Automatically operated RWST outlet MOV CS25	Local manual RWST outlet valve CS25
Remote manual MOV 1862	Remote manual MOV 1862	Remote manual MOV 1862	Automatically operated MOV 1862
Check valve 001	Check valve 001	Remote manual MOV 1862X	Check valve 001
Remote manual MOV 1890A	Remote manual MOV 1890A	Check valve 01	Automatically operated MOV 1890A
Remote manual MOV 1890B	Remote manual MOV 1890B	Check valve 0X	Automatically operated MOV 1890B
Remote manual MOV 1890C	Automatically operated MOV 1864A	Automatically operated MOV 1890A	Automatically operated MOV 1890C
Remote manual MOV 1864A	Automatically operated MOV 1864X	Automatically operated MOV 1890B	Automatically operated MOV 1864A
Remote manual MOV 1864B	Automatically operated MOV 1864B	Automatically operated MOV 1864A	Automatically operated MOV 1864B
	Automatically operated MOV 1864Y	Automatically operated MOV 1864B	

TABLE 3. SUMMARY OF DESIGN OPTION IMPACT ON SYSTEM UNAVAILABILITY

	Event Unavailability			
Fault Event	Baseline	Option A	Option B	Option C
Valve 1890C closed (human error)	1.0E-03	Deleted	Deleted	Deleted
Valve 1862 closed (human error)	1.0E-03	1.0E-03	Deleted	Deleted
Valve CS25 closed (human error)	3.0E-04	3.0E-04	Deleted	3.0E-04
Valve 1890A open (hardware failure)	1.0E-04	1.0E-04	1.0E-04	1.0E-04
Valve 1890A open (human error)	1.0E-04	1.0E-04	Deleted	Deleted
Valve 1890B open (hardware failure)	1.0E-04	1.0E-04	1.0E-04	1.0E-04
Valve 1890B open (human error)	1.0E-04	1.0E-04	Deleted	Deleted
Valve 1890C closed (hardware failure)	1.0E-04	Deleted	Deleted	1.0E-04
Valve CS25 closed (hardware failure)	1.0E-04	1.0E-04	1.0E-04	1.0E-04
Valve 1862 closed (hardware failure)	1.0E-04	1.0E-04	Deleted	1.0E-04
Check valve 001 closed (hardware failure)	1.0E-04	1.0E-04	Deleted	1.0E-04
Failure of both trains of safety injection signal	9.9E-05	9.9E-05	9.9E-05	9.9E-05
*Maintenance contribution	9.6E-04	7.7E-04	7.3E-04	9.5E-04
*Double failure contribution	9.5E-05	7.3E-05	7.7E-05	7.7E-05
RWST vent plugged	4.4E-07	4.4E-07	4.4E-07	4.4E-07
*Total LPI unavailability point estimate	4.2E-03	2.9E-03	1.2E-03	2.0E-03

* This unavailability is the result of computations based on the system design and is recomputed for each design configuration

fault events associated with the major components as well as the correspodning fault probabilities. In addition, Table 4 summarizes the design modifications for each option and provides the cost estimate for the modifications. The paragraphs which follow provide some comparisons of cost of cost and availability of the baseline design and the three options.

The fault tree analysis of the baseline LPIS design revealed that single valve faults associated with MOV 1890C, MOV 1982, MOV 1862A, MOV 1890B, check valve CV001 or the RWST outlet value CS25 are the dominant contributors to the unavailability of the baseline LPIS system. These single faults account for 3.1×10^{-3} out of a total estimated hardware contribution of 3.2×10^{-3}. The test and maintenance contribution to the unavailability contributors, the most effective improvements to system availability might be made. Further, by proposing several alternative designs by which these improvements might be made, it was possible to compare the estimated costs of the various proposed design changes in the context of the estimated availability improvements. This process can be utilized as a preliminary screening of design alternatives.

TABLE 4. DESIGN OPTION COST SUMMARY

DESIGN	NATURE OF MODIFICATION	ACQUISITION COST	INSTALLATION COST	TOTAL OPTION COST
Option "A"	1. MOV 1090C removed.	$ —	$ 4,800	$376,360
	2. Parallel MOVs added to MOV 1864A and MOV 1864B.	128,000	112,400	
	3. Separate line from each pump train-tied into RCS header inside containment.	18,500	68,000	
	4. MOVs 1864A & B and their new respective parallel valves 1864X & Y are normally closed and open on receipt of SICS signal.	12,660	32,000	
Option "B"	1. Remove MOV 1890C	$ —	$ 4,800	$354,665
	2. Addition of a containment penetration so that each pump has a separate path to the RCS header.	18,500	68,600	
	3. MOVs 1864A and B normally closed.	40,000	28,000	
	4. Provision of parallel pump suction lines.	32,500	56,496	
	5. Motor operator added to RWST outlet valve CS25.	15,189	18,600	
	6. SICS signals provided to motor operated valves to ensure their proper position.	23,580	48,000	
Option "C"	1. SICS signals provided to motor operated valves to ensure proper position.	$23,580	$48,000	$71,580

fault events associated with the major components as well as the correspodning fault probabilities. In addition, Table 4 summarizes the design modifications for each option and provides the cost estimate for the modifications. The paragraphs which follow provide some comparisons of cost of cost and availability of the baseline design and the three options.

The fault tree analysis of the baseline LPIS design revealed that single valve faults associated with MOV 1890C, MOV 1982, MOV 1862A, MOV 1890B, check valve CV001 or the RWST outlet value CS25 are the dominant contributors to the unavailability of the baseline LPIS system. These single faults account for 3.1×10^{-3} out of a total estimated hardware contribution of 3.2×10^{-3}. The test and maintenance contribution to the unavailability contributors, the most effective improvements to system availability might be made. Further, by proposing several alternative designs by which these improvements might be made, it was possible to compare the estimated costs of the various proposed design changes in the context of the estimated availability improvements. This process can be utilized as a preliminary screening of design alternatives.

TABLE 4. DESIGN OPTION COST SUMMARY

DESIGN	NATURE OF MODIFICATION	ACQUISITION COST	INSTALLATION COST	TOTAL OPTION COST
Option "A"	1. MOV 1890C removed.	$ —	$ 4,800	$376,360
	2. Parallel MOVs added to MOV 1864A and MOV 1864B.	128,000	112,400	
	3. Separate line from each pump train-tied into RCS header inside containment.	18,500	68,000	
	4. MOVs 1864A & B and their new respective parallel valves 1864X & Y are normally closed and open on receipt of SICS signal.	12,660	32,000	
Option "B"	1. Remove MOV 1890C	$ —	$ 4,800	$354,665
	2. Addition of a containment penetration so that each pump has a separate path to the RCS header.	18,500	68,600	
	3. MOVs 1864A and B normally closed.	40,000	28,000	
	4. Provision of parallel pump suction lines.	32,500	56,496	
	5. Motor operator added to RWST outlet valve CS25.	15,189	18,600	
	6. SICS signals provided to motor operated valves to ensure their proper position.	23,580	48,000	
Option "C"	1. SICS signals provided to motor operated valves to ensure proper position.	$23,580	$48,000	$71,580

This demonstration assessment is based entirely upon the techniques (fault tree analysis, SAMPLE code) and data from WASH-1400. Subsequent to the reactor safety study, there has been a great deal of interest in evaluation techniques which account for coupled failures of hardware and human errors. These techniques include the use of factors to modify the appropriate component failure or human error rates in the evaluation process. These LPIS demonstration assessments do not include these techniques in order to allow comparison of the postulated hypothetical changes to the baseline evaluation in WASH-1400 and to avoid raising issues which might detract from the primary purpose of the demonstration.

The Option A LPS design sought to improve PLIS availability in the following ways:

(1) MOV 1890C was removed, thereby eliminating its unavailability contribution associated with its potential failure in the closed position.

(2) Parallel MOVs 1864X and 1864Y were added to existing MOVs 1864A and 1864B, respectively, to eliminate the single faults associated with these valves.

(3) A separate line from each of the two pump trains has been connected to the RCS header inside containment. This was necessary as a result of the elimination of MOV 1890C.

(4) MOVs 1864A and 1864B and their new respective parallel valves 1864X and 1864Y are normally closed and open upon receipt of an SICS signal.

These design modifications are depicted in Figure 3 and are summarized in Table 4. As a result of these design changes, the total point estimate of LPIS unavailability for the Option A design is calculated to be 2.9×10^{-3} as compared with a point estimate unavailability of 4.2×10^{-3} for the baseline design option. This unavailability improvement may be obtained for an estimated cost of US $376,360.

The Option B LPIS design attempted to improve on the baseline design in the following ways:

(1) MOV 1890C was removed, thereby eliminating its unavailability contribution associated with its potential failure in the closed position.

(2) A separate line from each of the two pump trains has been connected to the RCS header inside containment. This was necessary as a result of the elimination of MOV 1890C.

(3) MOVs 1894A and 1864B are normally closed and open receipt of an SICS signal.

(4) Parallel pump suction lines including the complementary redundant valves MOV 1862X and CVOX have been provided.

(5) The RWST outlet valve CS25 was made into a motor operated valve.

(6) SICS signals were provided to motor operated valves to ensure their proper position.

The above design changes are depicted in Figure 4 and are summarized in Table 4. As a result of these design changes, the total point estimate of LPIS unavailability for the Option B design is calculated to be 1.2×10^{-3} as compared with the baseline unavailability point estimate of 4.2×10^{-3}. This unavailability improvement may be obtained for an estimated total cost of US $354,665.

The Option C LPIS design is the simplest variation on the baseline design. The only modification of the baseline PLIS design is the addition of SICS signals to all system motor operated valves. The addition of these signals helps to ensure that all MOVs will be in the proper position at the time of a LOCA. Specially, normally open valves will receive a signal fault associated with the mispositioning of receive a signal to close. All single faults associated with the mispositioning of LPIS valves are thus eliminated. This design modification is depicted in Figure 5 and is summarized in Table 4.

The addition of signals to system MOVs results in a total calculated point estimate unavailability of 2.0×10^{-3} for the Option C design as compared with a point estimate unavailability of 4.2×10^{-3} for the baseline design. This unavailability improvement could be obtained for an estimated cost of US $71,580.

5. INTERPRETATION OF THE RESULTS

Given that a system modification to improve safety must be made, inclusion of the quantitative measure of safety with the design information greatly augments the ability to make a cost effective decision. In this limited demonstration, the calculated cost and safety parameters were found to be as follows:

	Cost US $	Unavailability (Point Estimate)
Base line		4.3E-03
Option A	380,000	2.9E-03
Option B	350,000	1.2E-03
Option C	71,000	2.0E-03

Based on the point estimate of LPIS unavailability Option A, the hypothetically required modification, results in a small improvement (reduction) in system unavailability, the same dollars will "buy" a much greater safety improvement with Option B while Option C provides a slightly better improvement than the required change at about one-fifth of the costs of Option A.

With this information, one of two decisions can be made depending upon which factor (safety or cost) is of primary consideration. Although there are additional items which may be considered, such as the implications of the uncertainty in the unavailability and cost predictions, the two basic decisions implied by this data are:

(1) If the dollars for Option A are going to be spent, Option B is the design to chose because it provides the largest safety improvement for the money; or

(2) If the level of safety provided by Option A is desired, Option C is the design to chose because it provides the desired safety at one-fifth of the costs. (Actually, the costs of Option C may be a considerably smaller fraction of the other options because of minimal engineering and other uncalculated costs associated with Option C.)

The range of uncertainty associated with the predicted level of safety was derived by utilizing the SAMPLE code as in WASH-1400. The SAMPLE code is a Monte Carlo simulation to determine the error spread for the system unavailability based upon the input data errors. The results represent the 95 % and 5 % values calculated by the code. The ranges are:

Baseline	7.4E-03 to 3.1E-03
Option A	5.6E-03 to 1.3E-03
Option B	3.0E-03 to 7.9E-04
Option C	4.5E=03 to 1.5E-03

Examination of these uncertainties associated with the safety predictions does not change the basic decisions given that a change is required. However, if the requirement for the necessity of the change is to be questioned, consideration of the prediction uncertainties implies that Option B must significantly improve LPIS safety.

Without specific numerical safety criteria and given the required modification (Option A) provides the necessary safety level, the argument could be made that no change is required since there is considerable overlap in the error bounds of the baseline and Option A (the required change). Note that when there is a great deal of overlap in the error bounds associated with two alternative designs, that effectively means that the analyst cannot convincingly demonstrate that there is a significant difference between those systems in terms of their unavailabilities.

This demonstration has been purposely kept as limited and simple as possible to provide an insight into the utility of the probabilistic analysis in the design process. As powerful as these tools may be, these analytical techniques cannot be utilized to make the decisions solely based on the numerical results. Other factors such as compatibility with existing systems or procurement lead time, to identify just now, may also be considered in the decision process. Probabilistic results can, however, be used to make design decisions which are more closely related to the desire to provide cost effective designs which provide the desired level of safety.

Because of its limitations, the demonstration may leave general impressions and implications about the design decision process which require further explanation. The following issues are important:

- Cost optimization/design decision
- Resources required for implementation
- Relationship to regulatory process
- Analysis data requirements
- Acceptable level of safety
- Design criteria changes
- Safety importance of systems
- System interface impact ..... safety
- Context of the safety evaluation

Cost Optimization/Design Decision

In the absence of quantitative probabilistic safety criteria for system design, optimization of system cost is very difficult. Unlike a power plant availability situation where probability of system success can be equated to owner/operator revenues, the cost benefit of safety improvements is much more illusive. In the demonstration decision, no attempt was made to equate quantitative safety improvement to cost of the backfit. However, as noted above, a cost effective decision can still be made without a mathematically defined relationship between cost and safety.

The two possible choices raised by the demonstration were to either achive the maximum level of safety for the desired expenditure or to achieve the desired level of safety at the lowest cost. If a quantitative safety criterion existed for the demonstration system, then the second decision could be made in relation to that criteron.

A number of cost factors were not included in the demonstration. However, some of these costs could have an impact on the decisions. An additional cost with potential significant impact is engineering costs. This could be especially true in the situation where the hardware cost is small but a good deal of confirmatory analysis is necessary to demonstrate the functionability of the design. Even the cost of the probabilistic analysis of the system designs could become a factor. But, substantial savings on other design costs usually more than pays for the probabilistic analysis activities.

Resources Required for Implementation

The demonstration was purposely limited to a WASH-1400 syste to provide a good deal of visibility on the possibilities of utilizing probabilistic analysis techniques in the design process. Therefore, some of the resources required for implementation on the system level were borrowed from WASH-1400. Although significantly more than the demonstration study, the required resources for adding probabilistic analyses to the design process are not very large when examinations are limited to the type of system level decision in the demonstration.

Once the baseline safety level is established, assessment of backfit alternatives requires relatively few additional resources. Each additional assessment is primarily a modification of the initial baseline analysis. For this demonstration, the development of the fault tree analyses for the alternate designs required only two engineering weeks and evaluation of the trees another two weeks of effort and a few minutes of computer time. The cost estimating for each alternative required about three man-weeks of effort while the design criteria review and alternate design generation was accomplished with two weeks effort. The total effort required (engineering, computation, key punch) was approximately nine man-weeks.

For a system level design decision, development and assessment of three backfit alternatives can probably be accomplished for this same level of effort (nine weeks) or less. Assessment of the baseline design for a single simple system like LPIS would probably require an additional four to six weeks of analysis and evaluation effort. Of course, the more complex the design question (e.g., filtered vented containment) the larger the assessment effort. However, the potential payoff is also much larger. In some industries, safety analysis costs constitute 10 % to 15 % of engineering costs.

Relationship to Regulatory Process

The response of the industry to the regulatory process can be greatly enhanced by the utilization of the probabilistic techniques. The demonstration shows that quantitative information on the safety level can be developed to compare the existing situation and the alternatives. This information can be used in discussion with NRC justifying alternative action or no action to a system backfit request. NRC has already accepted such information in support of alternatives to NRC proposed changes to improve safety.

NRC has stated that one of the most useful applications of probabilistic techniques is the analysis of postulated accident sequences to determine their relative importance. In one case an analysis was performed to investigate the risk from seismically induced fires to determine if fire protection systems should be designed to seismic Class I requirements. The analysis performed indicated that the probability of a seismically induced fire was small compared to the probability of a randomly-induced fire occurring from causes not associated with an earth-quake. The study serverd as a basis for the NRC decision that fire protection systems should be designed to seismic Class II instead of Class I.

Probabilistic techniques were used internally by the NRC to determine the importance of a number of of safety issues raised by members of the regulatory staff. These issues were suspected to being treated inadequately in the licensing. The study showed that of those items related to plant safety, the majority involved potential accident sequences which would not have significant releases of radioactivity or which would have had lower probabilities than other accident sequences having similar releases of radioactivity. Thus, those items would not significantly affected the risks and need not to be considered further.

The demonstration information will support two basic positions depending upon the utility's desired response. The obvious response is that the same level of safety proposed by NRC can be achieved with a much less expensive backfit. An alternate response is that the requested NRC change does not significantly increase the level of safety of the system and is, therefore, not necessary.

The second position might be better rationalized on a higher level of resolution. Consideration of the impact of the system change in the context of accident response scenarious with other system failures will most likely provide a stronger argument for rebutting the necessity of the change.

Analysis Data Requirements

Application of probabilistic analysis to the design decision process for backfit situations requires data on system design, operation, component failure and maintenance. The system design and operational data consists of flow diagrams, elementary wiring diagrams, layout and evaluation drawings, operating test and maintenance procedures, and technical specifications. This information is normally available for the existing design. The same level of detail of the system information for the alternatives can be obtained by modification and assumption based on the baseline data.

The component data necessary for evaluation for the fault trees is not always part of the system design information. This data, which consists of failure rates, maintenance frequency and maintenance act duration time

should be plant specific, if possible. Failing that, generic data should be used.

Acceptable Level of Safety

If a quantitative system safety goal or requirement existed, the decision process for system design would simply be a matter of achieving that level of safety as demonstrated by analysis at the least cost.

This demonstration shows that decisions about safety levels of systems can still be made without a stated quantitative requirement. In the present situation the arguments might be made that the suggested design change is not warranted from safety improvement standpoint. However, it is quite possible that the suggested change could have a significant impact on the safety of a system with the same function and a different design. Thus, if the suggested design change came about of a changed design criterion, we could not conclude that the new criterion was generally invalid.

Similarly, the analysis of a proposed design change might suggest a new design criterion. However, it should not be assumed that this new criterion will achieve the same icreased level of protection when applied to other systems.

Safety Importance of Systems

The demonstration analysis was performed on the system level with the assumption that improved LPIS availability would lead to an increase in overall plant safety. However, the safety importance of system design changes can only be confirmed if the analyses are performed at a plant level.

System-Interface Impact on Safety

It sometimes happens that significant contributors to the unavailability of a safety system are elements of other systems. An example of this is the case in the demonstration where the Low Pressure injection System is rendered unavailable by the failure of the Safety Injection Control System (SICS). A careful search for all system interfaces and an evaluation of their potential impact must be made in the course of assessing the unavailability of reactor safety systems. In fact, this examination may make a change to the interfacing system more cost effective than the change originally contemplated. In some cases, a change to the interfacing system may be necessary because it may represent a limit of achievable safety for the systems it services.

Context of the Safety Evaluation

The demonstration analysis and decisions were limited in scope and context. The importance of these limitations have been discussed to some extent in the previous paragraphs (e.g. radiological impact on maintenance performed, effect on overall plant availability, possibility of achieving minimum requirements for safety functions) of this section. However, it is important to note that many other factors enter into making a decision about the level of safety of a design. Some of these factors are appropriately addressed by the methods utilized in the demonstration and some are not. Therefore, the context in which the design decisions are made will determine the context of the safety evaluation.

REFERENCES

[1] ENERGY INCORPORATED, LWR Design Decision Methodology Final Report, Rep. EI-81-32, Energy Incorporated, USA (1981).

[2] US NUCLEAR REGULATORY COMMISSION, Reactor Safety Study (WASH-1400), Washington D.C. (1975).

BIBLIOGRAPHY

US NUCLEAR REGULATORY COMMISSION, PRA Reference Document, Final Report, Rep. NUREG-1050, Washington D.C. (1984).

US NUCLEAR REGULATORY COMMISSION, PRA Fundamentals Training Course Notes, Rep. NUREG-4350, Washington D.C. (1985).

CONSUMERS POWER CORP., Big Rock Point PRA, Consumers Power Corp., USA (1980).

LIST OF ABBREVIATIONS

PRA -> PSA	Probabilistic Safety Assessment
NRC	Nuclear Regulatory Commission
TMI	Three Mile Island Nuclear Station
MOV	Motor Operated Valve
IREP	Interim Risk Evaluation Program
ATWS	Anticipated Transient without Scram
LWR	Light Water Reactor
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ASTM	American Society of Testing & Measurement
ANS	American Nuclear Society
LPIS	Low Pressure Injection System
LOCA	Loss of Coolant Accident
SICS	Safety Injection Control Signal
RCS	Reactor Coolant System
RWST	Reactor Water Storage Tank
WASH-1400	Reactor Safety Study
HPIS	High Pressure Injection System
FSAR	Final Safety Analysis Report

J. Young and
T. J. Leahy
1851 South Central Place,
Suite 201, Kent, Washington 98031
USA

R. J. Budnitz
Future Resources Associates Inc.
2000 Center Street
Suite 418, Berkeley, California 94704
USA

Oversight Committee for the Development of a Series of PSA Case Studies

A. Carnino
Electricité de France
32, Rue de Monceau
75384 Paris CEDEX 08
France

J. Gaertner
Electric Power Research Institute
Palo Alto
California 94303
USA

S. Hall
Safety & Reliability Directorate
UKAEA
Culcheth, Warrington WA3 4NE
UK

P. Kafka
Gesellschaft für Reaktorsicherheit (GRS)mbH
Forschungsgelände
8046 Garching
Germany

J. Villadoniga
Consejo de Seguridad Nuclear
S/Sor Angela de la Cruz 3
28020 Madrid
Spain

OECD/NEA
J. Caisely
Nuclear Energy Agency
OECD/NEA
Paris
France

IAEA
M. Cullingford — Scientific Secretary, Division of Nuclear Safety

S. M. Shah — Division of Nuclear Safety