CONF-770625--3

THE USE OF RELIABILITY IN THE LMFBR INDUSTRY

J. R. Penland, A. M. Smith, D. K. Goeser

THE USE OF RELIABILITY IN THE LMFBR INDUSTRY

J. R. Penland, A. M. Smith, D. K. Goeser

ABSTRACT

This mission of a Reliability Program for an LMFBR should be to enhance the design and operational characteristics relative to safety and to plant availability. Successful accomplishment of this mission requires proper integration of several reliability engineering tasks--analysis, testing, parts controls and program controls. Such integration requires, in turn, that the program be structured, planned and managed. This paper describes the technical integration necessary and the management activities required to achieve mission success for LMFBR's.

1. Introduction

The development and application of reliability engineering techniques in the nuclear power industry to date have been primarily directed at evaluation of safety-related systems and events. These evaluations have utilized not only quantitative aspects of reliability analysis but also significant areas of qualitative analysis. These studies have addressed subjects such as common cause failure and human operator error. The study objectives have been to enhance safety design features and related decisions and, thus, to improve licensability. The Reactor Safety Study[1] was performed to enhance the ability to make decisions. Numerous examples of studies aimed at licensability exist (see references 2, 3 and 4, for example).

The Liquid Metal Fast Breeder Reactor (LMFBR) industry has proceeded toward commercialization only very recently and has had the ability to learn from the experience of the Light Water Reactor (LWR) industry and from other industries utilizing realiability engineering techniques. These experiences indicate that the role of reliability engineering should also include design and operation enhancement to realize the most effective use of the technology.

The goal of design and operation enhancement is applicable to licensability, safety, and plant availability and is being used in varying degrees in each of the areas by the LMFBR industry. Addressing this goal effectively requires the use of the full spectrum of reliability engineering techniques. For reliability engineering to achieve enhancement of design and operation, organizational elements other than reliability specialists must be an integral part of the reliability program.

This paper describes a suggested approach to utilize the full scope of reliability engineering technology in an integrated manner with the total design and operational cycle. This approach reflects the results of the current learning process (including trial and error) in the LMFBR industry as well as the experience in other industries.

In the following sections, the objectives of an LMFBR Reliability Program are described, the basic approach to achieving the objectives are delineated, key technical elements are defined and conclusions are reached.

2. Objectives of an LMFBR Reliability Program

The objective is to achieve reliability enhancement of design and operation for safety, plant availability and licensability. Although functional and technical interdependencies exist, these areas are described below.

In the area of reactor safety, the greatest emphasis is applied to prevention of the Core Disruptive Accident (CDA). Accidents of lower consequence but of higher probability are not excluded; but at this stage of LMFBR development, primary emphasis must be placed on the CDA. Breeding of new fuel and utilization of a fast neutron spectrum produces core configurations which have the potential, albeit probabilistically remote, for the Core Disruptive Accident. It is theoretically possible that the LMFBR CDA can cause core disassembly, partially vaporize fuel and produce severe structural loadings.

In applying an approach to reduce the probability of the CDA, the LMFBR industry is taking additional precautions relative to normal reactor safety practice. Although LWR safety indirectly treats reliability[5,6], the principal LWR emphasis has been placed upon mitigation of consequences of hypothetical accidents. This approach is used for LMFBRs[7] but is augmented by direct programs to decrease the probability of such occurences.

To minimize the CDA probability, major emphasis is placed upon two systems -- the Reactor Shutdown System (RSS) and the Shutdown Heat Removal System (SHRS). Although other systems are involved in CDA event sequences, all involve failure of one or both of the RSS and SHRS[8]. The most effective treatment of the CDA is through concentration on these systems.

Treatment of RSS and SHRS reliabilities is directed at reducing their failure probabilities in fact, and establishing via numerical analysis that these probabilities are vanishingly small for all known failure modes. Although regulatory authorities endorse this approach[9], the lack of convincing statements hampers the use of reliability technology directly in the licensing process. Quantitative reliability estimates are an important part of the process but other aspects of qualitative analysis, testing program results, reliability controls and engineering judgement must be an integral part of the program.

The LMFBR reliability program approach to licensability is, therefore, to concentrate on those activities and items which will produce enhanced safety. Many of these activities, by their very nature, are not amenable to generating absolute proof of conservatism. As these activities mature and confirm the ability to enhance safety, the licensing process must endorse those activities and give appropriate credit.

An equally important application of LMFBR reliability technology is plant availability. The current utility atmosphere requires high plant availability as the most effective manner of achieving high utilization of capital. The LMFBR is a new type of plant for commercial power production and, as such, must demonstrate the capability to produce reliably.

While safety and availability have many areas of common interest and interface, availability encompasses additional considerations and, therefore, must be explicitely addressed in a comprehensive Reliability Program.

Reliability engineering is a vital ingredient in assuring economic competiveness. Without a sizeable base of operating plants from which to learn, reliability technology must be more inclusive in scope for LMFBR's than would be appropriate for LWR or fossil plants. Analysis, testing and reliability related design controls must perform functions which use of operating plant data would perform for LWR's and fossil plants.

3.0 Basic Approach

3.1 Program Strategy

The need for product reliability is universally accepted. In viewing an overall product cycle from inception through operation, reliability is often thought of as everybody's job. It is true that a large percentage of the personnel involved in designing, producing and using a product contribute directly to its reliability, but to set specific reliability objectives -- and achieve them -- requires a deliberate and structured effort. As the product complexity increases, and as the economic and/or safety consequences of unreliability become more severe, the necessity for a structured reliability effort becomes a primary consideration.

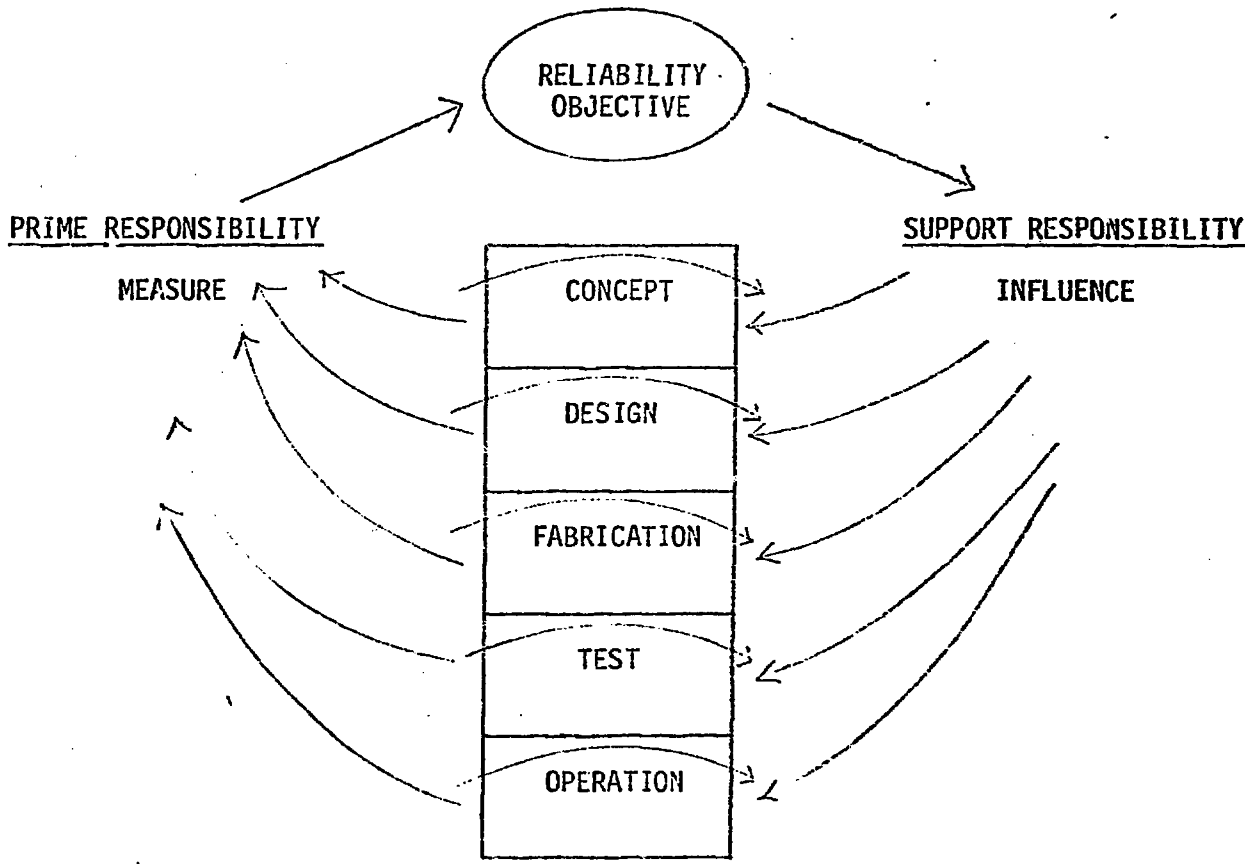
Structuring a formal reliability effort for a complex product is no mean task. Given that specific reliability objectives have been selected, a cost-effective reliability program that permeates the product cycle must be developed. While different approaches can be envisioned, a strategy that is simple and effective is illustrated in Figure 3.1. An organized Reliability Engineering operation provides the focus and technical expertise required to accomplish specific reliability tasks. These tasks, in turn, involve two categories of activities:

1. Reliability Engineering provides a support role to the line organizations responsible for design, fabrication, test and operation. In this support function, their role is to influence the product to achieve the specified reliability objectives. This is done in several ways, ranging from evaluations for system configuration selection to detailed reliability analyses that may be essential to decisions for inspection techniques, sampling plans and the formulation of operational procedures.

2. As a direct and prime responsibility, Reliability Engineering is charged with the independent and objective measurement and evaluation of reliability status versus the specified reliability objectives. It is essential that the responsible design organizations are not held accountable for such measurements; they play an important support role in this case, but cannot be held both responsible for design and independent of its assessment.

FIGURE 3.1

THE ROLE OF RELIABILITY ENGINEERING



Thus, Figure 3.1 shows a typical closed loop situation. The reliability objective guides the degree of influence that should be fostered by Reliability Engineering. The measurement activity provides the status of reliability achievement. Feedback occurs when the status and goal are not properly matched. This is a very important cycle and is the essence of the cost-effective reliability program. When further attention is required, the cycle so indicates; or conversely, it becomes clear when further effort (and dollars) are unwarranted. Without this definitive cycle, management must, at best, intuitively judge the necessity for further effort.

3.2 Program Elements

Implementation of the strategy requires the development of key program elements which can be used to effectively structure a formal reliability effort. Four such elements are suggested.

1. Reliability Objectives. Specific reliability objectives are essential to the conduct of a meaningful reliability program. These objectives most often are stated in quantitative terms and may be numerical goals defined at the plant level. These numerical values must be allocated down to specific systems and components so that each responsible design engineer will know that part of the reliability objective which is his to meet and satisfy. These objectives may have qualitative aspects to

provide proof or confirmation of reliability factors which have been appropriately treated. Without these quantitative and qualitative objectives, reliability studies tend to be meaningless.

2. Reliability Program Plan. This is the "road map" of how the objectives will be achieved. It is a specific definition of the tasks to be performed, the level of effort required to do them, the schedular milestones for their accomplishment, and the assignment of responsibilities to do them. It includes organizational definitions and interface relationships (including those with co-contractors, customers and vendors, as appropriate). Any good management approach requires a meaningful planning effort and a reliabilty program is no exception.

3. Reliability Control. Since reliability tends to be everybody's job, the question of control becomes very difficult. While the measurement and evaluation role of Reliability Engineering discussed in Section 3.1 is an important facet of overall control, other, more discrete, control points throughout a product cycle should also be exercised. Four such control points where Reliability Engineering becomes an integral part of the mainstream process are noted.

   a. Reliability approval of Final Design Review before drawings are released for prime hardware manufacture. If the Reliability Engineering support role has been properly accomplished, there should be no problem with such approval. If a reliability problem does exist, that problem must not proceed downstream into the prime hardware where its correction becomes more expensive and time consuming.

b. Reliability control and approval of a master parts, materials and process (PMP) list. The PMP list controls should require that all product specifications and drawings adhere to the disciplined usage of only those items that have been scrutinized and technically adjudged as suitable for the product. The haphazard usage of parts, materials and processes has proven to be the Achilles heel of more than one product.

c. The placement of reliability objectives (or their allocation) on all first-tier vendors. It is virtually impossible for a prime manufacturer to achieve his reliability objectives if he cannot obtain the same degree of reliability achievement from his first-tier vendors. To affect this element of control, Reliability Engineering should have approval or concurrence authority on procurements to assure the continuity of reliability objectives to the first-tier vendors. Reliability requirements placed on vendors must reflect the technical feasibility of measuring compliance with the requirements.

d. Reliability control of failure analysis and reporting activity on all reliability-critical components. Data on failures of critical components is perhaps the most important information that will develop over the course of the product cycle. It indicates the true reliability status and must be addressed and resolved with meticulous attention to detail. Reliability Engineering is not necessarily the group embodied with the expertise to perform this technical evaluation, but they are in the proper position to control and administer this function independently.

4. Reliability Visibility. Management, engineer and technician alike must know what the objectives are, where the product stands against those objectives, and what their role is. Reliability Engineering must institute written and oral reporting procedures to assure that the reliability message is properly conveyed. As a part of the Reliability Program Plan, a structured reporting cycle should be established. This should be augmented throughout the cycle with special presentations and reports to keep management well advised of the reliability status and activities.

A fifth element should be noted to avoid any misconceptions. All the strategy and planning in the work is for naught unless there is solid top management backing and support for an effective Reliability Program.

4.0 Key Technical Elements

Although safety, availability and licensability differ in reliability missions, the applicable tasks to the three areas have much in common.

To identify the required tasks, consider the ideal--having systems which never fail to perform their required functions. For the system never to fail either (a) the system must be defect free (b) the system must be able to perform its function with failed components.

If the system is to have no defects, then it must embody

1. perfect design and
2. perfect parts.

For the system to function in spite of faults

3. the system must be fault tolerant, and
4. there must exist the ability to monitor the system and repair or replace failed components.

None of the items 1 through 4 are absolutely achievable. To produce a system approaching the ideal, items 1 through 4 must each be pursued.

In the following sections, each of these areas are examined. The two areas related to design -- assuring the design can perform its function and assuring that the design can tolerate failures -- are combined.

4.1 Design Considerations

Reliability techniques appropriately combined with design activities are an essential element of the conceptual design phase. Their role is to analyze the plant concept to identify (a) critical systems for safety, (b) critical systems for availability, and (c) interrelations of systems for each of the safety and the availability missions. This analysis is qualitative and semi-quantitative in nature, first in the form of system level failure modes and effects analysis (FMEA) and, second, in the form of quantitative evaluations to select between various alternate configurations. Inputs are deterministic systems analyses, initial systems requirement and engineering specifications, LWR history and data and engineering judgment. An example of the impact such an evaluation may have is that the need for two separate, redundant and diverse shutdown systems may be identified. Evaluations leading to this conclusion rely on operational histories from other reactors and estimates of the effect of such failures. In addition to forming an early identification of critical systems, results of the analyses can be fed back into the design process as design requirements. At this early stage in which no detailed design information exists, the impact, and therefore the importance, of reliability evaluations is significant.

A top-level analysis of identified critical systems should be performed as a cooperative effort of design and reliability engineers. This analysis should identify system configuration problems and define a Reliability-Critical Items List (RCIL). The RCIL is a tool to maintain visibility and cognizance of the status, actions required, results of tests, etc. of components, subsystems, or systems which are either critical to success of the overall system or which are subject to significant uncertainties.

System analysis should be performed by reliability engineers and design engineers acting as a team. This coordination is necessary since: (1) The reliability engineer is trained to evaluate in a systematic manner from a potential weakness viewpoint as opposed to the designer's more direct "here is how it works" perspective. (2) Without the detailed knowledge of the design engineer, the results of the reliability evaluation may be incomplete or, in cases, incorrect. (3) The combined effort assures reliability feedback into design at the earliest possible time.

The top level system evaluation should identify areas for more detailed evaluation. From this definition, the reliability engineer should develop guidelines or criteria for design of these areas. Typically, these will take the form of qualitative requirements such as modified single failure criteria[10]. Formal mechanisms for imposition of these guidelines into design should exist.

After completion of the initial system evaluation, more detailed analysis and initiation of testing programs should begin. This second level of analysis is generally quantitative in nature. To impact design, the most realistic portrait of the system is necessary in order to accurately pin-point system weakness. If overly conservative data or assumptions are utilized, the introduced conservatism may mask real problems.

For quantitative reliability studies impact design and operation, their use must be carefully selected. Applications can be misleading in which data is non-existent or where common cause failure (CCF) considerations are controlling and cannot be described analytically. The weaknesses, as well as the strengths, of quantitative reliability analysis must be recognized and the use of this tool concentrated in areas where meaningful and effective results can be produced.

As design details and testing results on system components are developed, component level reliability evaluations should be performed. Results of these studies, both qualitative and quantitative, are used to "build-up" to updated system evaluations. In this sense, the system reliability evaluation process is dynamic in order to support design through the full evolution process.

Based upon qualitative and quantitative reliability studies, testing programs may be advisable. It is often not economically feasible to test to demonstrate failure probabilities at a given confidence level. Effective testing should generally be directed at identification of failure inducing parameters, definition of failure modes, characterization of failure effects and experimental searching for unsuspected failure factors. Appropriate statistical treatment of the data should be performed to achieve full utilization of experimental information.

Due to the large costs, testing must be concentrated on unproven systems. Furthermore, advantage must be taken of existing tests. For nuclear plant components these could include design verification tests, prototype tests, acceptance tests and pre-operational tests. In certain instances specific reliability testing beyond these tests may be a good return on investment. This should be considered in the case of new designs or where potential failure modes warrant the accumulation of more detailed data. In addition, Reliability Engineering should have strong input to all phases of testing.

4.2 Parts Controls

Reliability analysis and the initial phases of testing will identify components critical to system reliability. These parts should then be entered into the Reliability-Critical Items List (RCIL). The RCIL by itself accomplishes nothing, but the controls applied to RCIL items are the key to an effective means of improving reliability.

Controls for RCIL components should address initial specifications through system operation. Major points at which parts controls come into play are specifications, procurement, development testing, acceptance testing, installation, pre-operational testing and operations.

For electrical parts, a detailed structure for grading of parts exists from military and aerospace experience. Grading levels reflect not only manufacturing procedures but also differing levels of inspection and burn-in. Data[11] indicate that reductions in component unreliability of factors of five to ten are achievable by more rigorous specifications. Although these data primarily reflect random failure rates, reduction in susceptability to random failures also reduces sensitivity to common cause failures. More rigorous parts specification impacts safety and also aids plant availability by reducing the probability of spurious activation of back-up systems.

While existing specifications cover several aspects of electronics reliability, mechanical component controls are more complicated. For mechanical components, reliability engineering should have a direct, formal input into detailed engineering specifications, manufacturing procedures, installation procedures and QA requirements. It may become necessary to perform qualitative analyses of manufacturing and installation procedures to identify and eliminate elements which could degrade the inherent design reliability. Further effort to evaluate historical failures in like equipment may be necessary as a reliability grading system comparable to that for electrical parts does not exist.

Procurement of RCIL components must be monitored closely by reliability engineering. Although specifications may be established to perfection, the real world of procruement produces exceptions to the specifications. These exceptions must be analyzed to determine their effects on component reliability.

A failure reporting, analysis and corrective action program must be implemented. This system consists of the following elements.

1. A procedural system must detect and report failures which occur during development, acceptance, pre-operational testing and operations.
2. Sufficiently detailed information must be collected on reported failures to guide failure analysts.
3. In many cases, special failure analysis must be performed to identify the failure causes.
4. Parts traceability must exist in order to implement corrective actions or like or similar components.
5. A positive corrective action system must exist.

The failure reporting, analysis and corrective action system is one of the most critical aspects of a reliability engineering program. This system is the dynamic means for insuring feedback into future equipment.

4.3 Maintainability and Repairability

For even a system of high order redundancy to achieve high reliability, that system must be capable of being effectively maintained and efficiently repaired. From a quantitative analysis point-of-view, the repair time is as important a parameter as failure rate.

Maintainability and repairability considerations should permeate design and operational procedures. The following summarizes key tasks and elements which should be considered prior to operation.

1. Design. The design should be analyzed to evaluate ability to perform maintenance or repair when the plant is "on-line".
2. Diagnostics. Analysis should be performed to assure that key failures are annunciated to the operations staff. Consideration should be given to special diagnostic systems for incipient failure detection.
3. Accessability. Analyses and tests, if feasible, should be performed to assure that repair or replacement can be performed with a minimum of strain on personnel or equipment. Plant scale models are an invaluable tool for this effort.
4. Spare Parts. Analysis and historical experience should be used to determine what spare parts should be on-site to expedite repair.
5. Tools. Special tools required for maintenance and repair activities should be identified.
6. Manpower. Human resource requirements should be identified. Not only the number of men, but also their necessary skills should be identified and training programs established.

7. Time Line Studies. For critical operations such as refueling, detailed time line studies should be performed to identify possible problems and to identify means of accelerating the operation. Contingencies for generic types of problems should be identified. As a part of the time-lining efforts, logistics problems should be analyzed.

After operation of the facility, repairability and maintainability programs should stay in effect. Key elements for this phase are maintenance and analysis of repair operations and feedback of this information into on-going efforts.

5.0 Conclusions.

This paper has presented descriptions and recommendations based upon current LMFBR and other related industrial experience. Based upon this information, the following conclusions are reached.

1. The need for reliability programs directed at safety and at availability exists in the real world and should become a more direct part of the licensing process.
2. A haphazard approach to a reliability program will not produce desired results. In order to achieve design and operation enhancement, many complex tasks must be integrated to achieve the synergistic benefits. An overall "systems" approach to building reliability into nuclear

plants must be adopted.

3. For a large project a formalized and structured approach is necessary and should be appropriately considered in the contractural aspects of the project. This is required to assure uniformity, viability and management support and also to assure that the results of reliability technology are fed back into design.

4. A balanced program relative to design, parts and maintenance is required. Omission of one down grades the effectiveness of the others.

REFERENCES

1. "Reactor Safety Study: An Assessment of Accident Risks in U. S. Commercial Nuclear Power Reactors", WASH-1400 (NUREG-75/-14), U.S. Nuclear Regulatory Commission, October 1975.

2. J. F. Scott, V. J. Galan, L. R. Cartin, W. R. Heldenbrand, J. R. Penland, "Analysis of Anticipated Transients Without Trip", BAW-10016, Babcock and Wilcox, September 1972.

3. W. C. Gangloff, W. D. Loftus, "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients", WCAP-7706, Westinghouse Electric Corporation, July 1971.

4. B. M. Tashjan, "Sensitivity Analysis of a Two-Out-of-Four Coincidence Logic Reactor Protection System", Nuclear Science Transactions, vol. NS-18, Feburary 1971, pp. 455-464.

5. IEEE Standard 279-1971 (ANSI N42.7-1972), "Criteria for Protection Systems for Nuclear Power Generating Stations."

6. "Technical Report on Anticipated Transients Without Scram for Water-Cooled Reactors", WASH-1270, U.S. Atomic Energy Commission, 1973.

7. "Third Level Thermal Margins in the Clinch River Breeder Reactor Plant: Updated Analysis for the First 24 Hours, November 1976. An enclosure

to ERDA letter S:L:1820, A. R. Buhl to R. S. Boyd, "CRBRP - 24-Hour Non-Venting Criteria", dated November 5, 1976.

8. "Clinch River Breeder Reactor Plant Preliminary Safety Analysis Report; Appendix C: Safety-Related Reliability Program", Docket Number 50-537.

9. Letter, Richard P. Denise to Lochlin W. Caffey, Docket No. 50-537, dated May 6, 1976.

10. IEEE Standard 379-1972 (ANSI N41.2-1972), "Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection Systems."

11. "Reliability Prediction of Electronic Equipment", MIL-HDBK-217B, 20 September 1974.

RELIABILITY ENGINEERING SHOULD ENHANCE DESIGN AND OPERATIONAL CHARACTERISTICS RELATIVE TO:

- SAFETY
- PLANT AVAILABILITY
- LICENSABILITY

LMFBR SAFETY RELATED RELIABILITY DECREASES "CDA" PROBABILITY BY CONCENTRATING ON CRITICAL SYSTEMS

- REACTOR SHUTDOWN SYSTEM
- SHUTDOWN HEAT REMOVAL SYSTEM
- INTERFACING SYSTEMS

PLANT AVAILABILITY ACTIVITIES ACCELERATE THE MATURATION OF LMFBR COMMERCIALIZATION

- REDUCE FORCED OUTAGE RATE
- DECREASE RESTORATION TIME
- ACCELERATE PLANNED OUTAGES

ENHANCED LICENSABILITY RESULTS FROM DEMONSTRATED SAFETY ENHANCEMENT

- RELIABILITY ANALYSIS PROVIDES ONE MEASURE OF SYSTEM ADEQUACY
- ENGINEERING EXAMPLES MUST PROVIDE BASES FOR CREDIT
- RELIABILITY MUST DEMONSTRATE WORTH

DESIGN AND OPERATION ENHANCEMENT REQUIRES SYSTEMATIC APPROACH

- IDENTIFY APPLICABLE TECHNICAL TASKS
- DEFINE ROLE OF RELIABILITY ENGINEERING
- IMPLEMENT PROGRAMMATIC ELEMENT TO ASSURE PROPER INTERACTION

RELIABILITY ACTIVITIES ARE DESIGN-RELATED FUNCTIONS WHICH IDENTIFY AND CONTROL FAILURES

- QUALITATIVE ANALYSIS
- QUANTITATIVE ANALYSIS
- REPAIR AND MAINTAINABILITY
- PARTS PROGRAM
- TEST PROGRAM
- FAILURE ANALYSIS AND CORRECTIVE ACTIONS

QUALITATIVE METHODS IDENTIFY HOW A SYSTEM AND ITS COMPONENTS CAN (NOT "WILL") FAIL AND WHAT THE EFFECTS ARE

- FAILURE MODES AND EFFECTS ANALYSIS (FMEA)
- FAULT TREE ANALYSIS
- COMMON CAUSE FAILURE ANALYSIS

QUANTITATIVE ANALYSES YIELD SYSTEM DESIGN INFORMATION NECESSARY TO ENHANCE RELIABILITY

- NUMERICAL MODELING IDENTIFIES THE MOST RELIABILITY IMPORTANT COMPONENTS
- SENSITIVITY STUDIES INDICATE EFFECTIVENESS OF COMPONENT REDUNDANCY, INDEPENDENCE, ETC.
- ASSESSMENT YIELDS ONE MEASURE OF SYSTEM ADEQUACY
- REALISM REQUIRED TO IDENTIFY REAL PROBLEMS

REPAIR AND MAINTAINABILITY ACTIVITIES MINIMIZES DOWN TIME

- ON-LINE MAINTAINANCE CAPABILITY
- DIAGNOSTICS
- ACCESSABILITY
- SPARE PARTS
- TOOLS
- MANPOWER
- TIME LINE

PARTS PROGRAM ASSURES THAT COMPONENTS SUPPORT SYSTEM OBJECTIVES

- INFANT MORTALITY MINIMIZED BY SCREEN AND BURN-IN
- TRACEABILITY ALLOWS ELIMINATION OF FAULTY PARTS
- UNIFORM RELIABILITY PARTS IMPROVE COST EFFECTIVENESS OF DESIGN

TEST PROGRAMS SHOULD BE DESIGNED FOR MAXIMUM RELIABILITY BENEFIT

- DEVELOPMENT TESTS
- ACCEPTANCE TESTS
- DESIGN ENVELOPE TESTS
- RELIABILITY TESTS
- PRE-OP TESTS
- START-UP TESTS

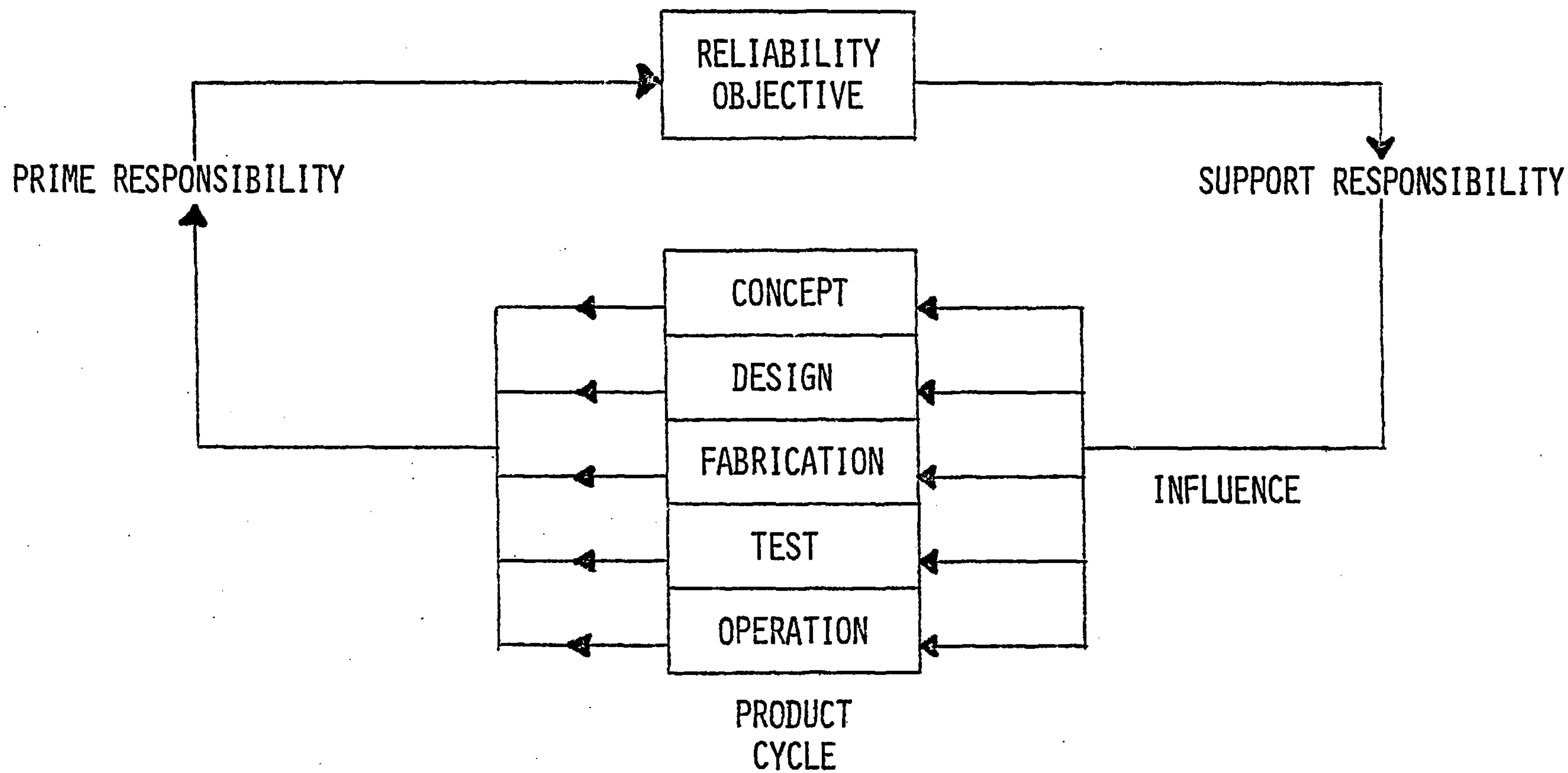
FAILURE REPORTING/ANALYSIS/CORRECTIVE ACTION REMOVES HARDWARE AND DESIGN DEFICIENCIES

- COVER ACCEPTANCE TESTING THROUGH PLANT OPERATION
- IDENTIFY CAUSES OF DEFICIENCIES
- ASSURE RECTIFICATION OR RATIONAL ACCEPTANCE OF RISK

COMPLEX, INTER-RELATED TASKS REQUIRE THAT ROLE OF RELIABILITY ENGINEERING BE INTEGRATED WITH DESIGN ACTIVITIES

- PRIME RESPONSIBILITY FOR MEASUREMENT OF RELIABILITY STATUS
- SUPPORT RESPONSIBILITY TO DESIGN FOR DESIGN FABRICATION, TEST, OPERATION

ROLE OF RELIABILITY ENGINEERING



PROGRAMMATIC ELEMENTS INTEGRATE TASKS AND RELIABILITY/DESIGN ORGANIZATIONS

- RELIABILITY OBJECTIVES
- RELIABILITY PROGRAM PLAN
- RELIABILITY CONTROLS
- ORGANIZATIONAL VISIBILITY

RELIABILITY OBJECTIVES PROVIDE "AIMING POINTS" AND RATIONAL MEASURE OF RELIABILITY IMPORTANCE OF SYSTEMS AND COMPONENTS

- OBJECTIVES MAY BE QUANTITATIVE OR QUALITATIVE
- EX: SAFETY - 10^{-6}/YR OF EXCEEDING 10CFR100
- EX: AVAILABILITY - 82%

RELIABILITY PROGRAM PLAN IS THE IMPLEMENTATION DOCUMENT FOR THE PLANNING FUNCTION

- DEFINES TASKS
- DEFINES LEVEL OF EFFORT
- ESTABLISHES SCHEDULES
- DELINEATES RESPONSIBILITIES

RELIABILITY CONTROLS ENFORCE PROPER INTERFACE FUNCTIONS

- DESIGN REVIEWS
- PARTS, MATERIALS, PROCESS LIST
- REALISTIC ALLOCATION OF RELIABILITY OBJECTIVES TO VENDORS
- FAILURE REPORTING/ANALYSIS/CORRECTIVE ACTION

VISIBILITY OF THE RELIABILITY ENHANCEMENT PROCESS ASSURES THAT EACH CONTRIBUTOR UNDERSTANDS HIS ROLE AND RESPONSIBILITIES

- STRUCTURED REPORTING CYCLE
- PROBLEM ESCALATION ROUTE

EFFECTIVE RELIABILITY ENHANCEMENT PROGRAM REQUIRES INTEGRATION OF COMPLEX TASKS AND DIVERSE ORGANIZATIONS

- BENEFITS IN SAFETY, AVAILABILITY, LICENSING EXIST
- "SYSTEMS APPROACH" TO PROGRAM IS NECESSARY
- FOR LARGE PROJECT, FORMALIZED STRUCTURE MUST BE IMPLEMENTED
- A BALANCED PROGRAM OF TASKS MUST BE DEVELOPED