N72-25986

RELIABILITY TECHNIQUES
IN
THE PETROLEUM INDUSTRY

By

Mr. Henry L. Williams
Chief
CFE Engineering Branch
of
Reliability Division

NASA
Manned Spacecraft Center

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

PRECEDING PAGE BLANK NOT FILMED

INTRODUCTION

Every taxpayer has an investment in the U.S. space program. A complete list of the many returns from U.S. manned and unmanned space programs would not be appropriate for this paper; however, the following examples are cited as being indicative of the number of benefits that have been obtained. In terms of domestic impact, the returns range from national pride to better paints. Early warnings of hurricanes discovered by satellites have saved lives and millions of dollars in property damage. The development of rechargeable batteries, stimulated by the space program, has brought remarkable changes in the design and use of portable power tools and appliances.

In addition to the domestic impact, the space program has also provided technology applicable to many industrial processes. Fireproof Beta cloth has been developed and is already being used for fire-fighter suits in municipal departments and on board aircraft carriers. The requirements for deep-space operations demanded major improvements in the state of the art of computer technology. The chemical industry is already using these advanced computers in large data centers.

The rigorous efficiency and performance requirements of the space age led to the development of new technologies for achieving the required reliability in the millions of complex components in space equipment. These rigorous requirements are particularly true for the Apollo spacecraft with its complex mission of taking men to the moon, landing them, and returning them safely to earth. The NASA Manned Spacecraft Center (MSC) at Houston, Texas, has responsibility for the development of the command module, the service module, and the lunar module. At MSC, the reliability and quality assurance organization is at the highest level within the center, and the Director of Reliability and Quality Assurance reports to the center Director. It is a basic philosophy within the center that reliability and quality assurance personnel have direct access to top management for resolution of problems. Reliability and quality assurance activities are so closely related that some activities can be classified as either reliability or quality assurance. Some of the reliability activities described in this paper may be considered re quality assurance tasks, as in fact they are elsewhere in NASA. If some reliability concepts appear to be missing, it is because they have been classified at MSC as quality assurance activities. Since the Apollo spacecraft constantly evolves to accommodate changing mission requirements, the reliability analysis of each spacecraft is affected. That is, the prohibitive cost of reliability demonstration, coupled with limited production runs, has caused NASA to emphasize a qualitative rather than quantitative analysis approach to reliability. Quantitative reliability evaluation depends on statistical information that requires large sample sizes such as those experienced in the automobile and chemical industries. This characteristic in the Apollo Spacecraft Program is precluded by the limited production. These qualitative techniques applied in achieving Apollo goals also have application to the chemical industry. Effective translation of this technology to the chemical industry requires that special attention be given to differences in (1) industry definitions, terms, and acronyms; (2) industry goals and motivations such as performance, cost, schedules, and safety; and (3) repeatability of product or process. The technological advances in reliability are concerned particularly with offsetting reliability demonstration costs and limited production runs.

Part I of this paper describes the qualitative disciplines, the definitions and criteria that accompany the disciplines, and the generic application of the disciplines to the chemical industry. Part II translates the disciplines into proposed definitions and criteria for the chemical industry, into a base-line reliability plan that includes these disciplines, and into application notes to aid in adapting the base-line plan to a specific plan or operation.

PART I - APOLLO SPACECRAFT RELIABILITY PROGRAM ELEMENTS

The basic objective of the Apollo Spacecraft Reliability Program was the development of a spacecraft that would safely carry man to the surface of the moon and back. The Apollo Spacecraft Program Manager and the Design Engineers were committed to this objective, which was reached by strict attention to details throughout the Apollo Spacecraft Program.

To accomplish this basic objective, the Apollo Spacecraft Program Manager was required to emphasize qualitative goals such as the following: (1) safe transport of man to the moon and back, (2) minimization of critical single-point failures, and (3) development of a spacecraft system that could be launched into earth orbit by a Saturn launch vehicle. These goals were attained through the imposition of reliability requirements on all three phases - design, manufacturing, and operations - of the Apollo Spacecraft Program. Attention to detail is achieved through the accomplishment of the following 10 disciplines, which will be discussed further:

1. Program management
2. Failure mode and effect analysis
3. Problem reporting and corrective action
4. Design specification review
5. Design review
6. Quantitative reliability analysis
7. Reliability test requirements
8. Maintainability
9. The parts program
10. Reliability documentation

These disciplines constitute a reliability program with the fundamental purpose of identifying and removing problem-causing elements from the design and, ultimately, from the equipment selected to implement the design. This approach to identification and removal of problem elements is summarized in Figure 1.

Program Management

Basic NASA reliability requirements are contained in the NASA reliability publication NPC 250-1, entitled "Reliability Program Provisions for Space System Contractors," July 1963. These requirements are further defined and modified for use at MSC by MSC document MSCM 5315, entitled "Supplemental Reliability Requirements and Implementation Instructions for Manned Spacecraft Center Equipment," May 1969. These documents provide the basis for the Apollo Spacecraft Reliability Program, which is implemented primarily by the contractors that have responsibility for major hardware elements. Management of the reliability portion of a contract is the responsibility of the Reliability Division of the Reliability and Quality Assurance Office at MSC.

Reliability provisions in contracts and supporting reliability program plans are the primary tools of reliability program management. Each contractor develops a reliability program plan to detail how the provisions of the contract will be implemented. This plan, which is reviewed and approved by MSC, establishes the scope, applicability, and organizational responsibilities of the contract. The development of each contractor's or each subcontractor's program plan is guided by the Reliability Division, which considers factors such as the following: (1) the complexity of the equipment, (2) the functional criticality of the equipment, and (3) the procurement size. In the plan, the 10 reliability tasks previously discussed are described in terms of their basic requirements, definitions, implementation, procedures, exceptions, and data generation. The plan also establishes guidelines for scheduling the analyses, reporting the results, and distributing the necessary information to user agencies.

The Reliability Division continuously monitors the contractor's progress and conducts periodic meetings with the contractor to resolve implementation and scheduling problems. These meetings are based on the continuous interactions of the two organizations and on periodic formal audits of the contractor's performance with respect to the program plan requirements. The Reliability Division of MSC also places requirements on the contractor concerning the management of subcontractors and the reliability data to be generated by the subcontractors. Personnel from MSC may participate periodically with the contractor in his audit of the subcontractor.

The application of the Apollo Spacecraft Reliability Program concept to the chemical industry consists of developing a plan (1) that establishes division or corporate policy on reliability requirements such as (a) reporting failures and (b) criteria for accepting new equipment from vendors and (2) that establishes reliability requirements for turnkey plant design and construction.

Failure Mode and Effect Analysis

A designer usually evaluates his design by a thought process in which he examines possible

5-5

failure mechanisms, and protection for the failure mechanisms thus identified is provided. In the Apollo Spacecraft Reliability Program, this mental exercise is documented, put into a logic format, and complemented with the "what if" logic of the test, operations, and reliability engineers. This documentation affords the designer an evaluation of the design concept in which the complete set of requirements for the equipment is considered. This analysis is known as the Failure Mode and Effect Analysis. Inputs to the analysis include a description of the function the equipment is to perform and historical performance data on similar equipment. The analysis is oriented toward discussion of how items will fail rather than of how to make them work. The analysis consists of (1) an examination of each component of the system or function and (2) identification of the modes in which each component could fail. The effect component failure has on the system or function is then determined. Where interrelated functions exist, it is also necessary to evaluate the effect the failure has on other elements of the equipment. The failure effects are evaluated against established criticality definitions, with attention focused on major problems requiring design modification or procedural workarounds. Equipment (such as power, air conditioning, and structural support) that has service functions is included in the analysis.

The criticality definition for the Apollo Spacecraft Program had three categories: (1) personnel safety, (2) mission termination, and (3) all others. For the chemical industry, this definition is translated directly to (1) life/property loss, (2) plant shutdown/product contamination or loss, and (3) all others. When the selected set of definitions is used, the analysis provides a list of equipment elements whose failure could cause an undersired event. In the Apollo Spacecraft Program, these elements are referred to as single-failure points, which implies that the list does not contain combinations of failure points which could cause an undesired event. This list of equipment elements is the basis for a management function to force either redesign of these elements, provision of a workaround to offset the failure of these elements, or location of a different way to perform the function. In cases where no corrective action is available for a single-failure point, program management approves launch commitments after assessment of remaining risks.

The discussion up to this point has been focused on design activity. The Failure Mode and Effect Analysis is used in other ways such as to provide an input to the test requirements by identifying elements that require functional acceptance testing. Inputs are provided to the prelaunch checklist by identifying backup elements and workarounds which should be verified. The Failure Mode and Effect Analysis also serves as a working tool for the operations engineer by providing him with an aid in fault isolation. The Failure Mode and Effect Analysis is a design tool which has application throughout the life cycle of the equipment.

Figure 2 presents an example of the Failure Mode and Effect Analysis format used at MSC. The format in Figure 2 is simpler than the one actually used for the spacecraft, but is a good example for illustration purposes. The Failure Mode and Effect Analysis format might might be used in the chemical industry in the following ways:

1. As a joint analysis performed by plant designer and customer to check the design concept against the operating procedures to be used.
2. As an analysis performed as a design tool and then charted in summary form as a fault isolation aid during startup.
3. As an analysis performed as an aid in selecting instrument points for supervisory control of a plant or process.

The Failure Mode and Effect Analysis is considered to be a major factor in achieving trouble-free performance. This analysis is particularly useful where complex operations with interrelated functions required design detail by serveral designers.

The single-failure-point list resulting from the Failure Mode and Effect Analysis provides the designer with an action-item list of problems to be solved. When documented for the final design, the Failure Mode and Effect Analysis traces the effects back to the causes.

Problem Reporting and Corrective Action

Many unscheduled repairs, equipment failures, and catastrophic losses are avoidable if constant attention is given to prevention of their occurrence. Recurrence of a problem can

be avoided if effective corrective action is taken the first time the problem occurs. Recurrence control depends on communication among all users of the problem-causing equipment. A problem-reporting and corrective-action system is used by NASA in the Apollo Spacecraft Program Program to report problems, monitor the application of corrective action, and implement recurrence control.

Using a carefully selected problem definition, personnel concerned with the life cycle of a piece of equipment report the occurrence of any problems. These problems are recorded in a permanent record for that piece of equipment. Each reported problem is checked for previous occurrence and for the adequacy of previous corrective action. A solution must be found for all reported problems; that is corrective action must be identified and implemented. The corrective action must be based on a sound engineering solution to the problem. Failure analysis is the basis for the solution and may range from simple inspection of the failed equipment to special tests that duplicate the conditions of failure. Sufficient engineering effort is applied to clearly identify the cause and to understand the conditions which influence failure occurrence. The organization responsible for the reporting system verifies the corrective action before the problem is officially considered to be solved. This problem-reporting and corrective-action system prevents inferior elements or concepts from reaching the operational status. Also, when used along with the Failure Mode and Effect Analysis, this system provides a dual approach to reducing the occurrence of problems throughout the life cycle of the equipment.

The important elements of problem reporting are (1) the basic problem definition, (2) the basic critical-function definition (should be the same as the Failure Mode and Effect Analysis), (3) effective reporting techniques, (4) well-planned corrective action, and (5) careful correlation of the recurrence control history.

The application of the problem-reporting and corrective-action system to the chemical industry can be related to the development of new equipment and to the distribution of problem histories to other plants and divisions within the user company. If a valve jams in the open position and cannot be closed, all other plants in the organization should be notified if they are using the same valve in the same application. If a minor problem occurs when an engine is in a noncritical application, an audit can be made to determine if the engine is used elsewhere in a more critical function and whether corrective action is necessary. This system can also be used (1) to provide inputs to inventory control systems, (2) in maintenance planning, and (3) in the support of unit turnarounds. In addition, this system can be used by management to maintain an overview of program problems and their status.

Design Specification Review

Reliability considerations should form an integral part of the preparation, review, and approval of all design specifications, vendor-change requests, specification drawings, purchase orders, and subsequent revisions or amendments or both. A design specification is not adequate until the reliability requirements are clear to the designer. The reliability requirements include qualitative reliability goals, reliability procurement goals, and reliability documents goals. The same requirements must also be applied to vendor-deviation requests. This approach to design specification review is directly applicable to the chemical industry.

Design Review

The entire reliability program represents a continuous design review effort. From conceptual configuration studies to eventual design freeze, reliability continually evaluates the systems and updates analyses. Design reviews are conducted at the following hardware levels: (1) component, (2) subsystem, and (3) system. Each contractor has his own method of conducting design reviews, but participation by representatives of all disciplines (such as engineering, quality, reliability, manufacturing, and purchasing) is required. Some of the primary purposes of the design review are to determine the following: (1) Have all potential failure mechanisms been eliminated? (2) Is the item manufacturable? (3) Can the item be inspected? (4) When put together as a subsystem or system, will all components work together as specified?

Reliability personnel have a prime role to play in the major system design reviews, which are the Preliminary Requirements Review where the spacecraft requirements are established; the Preliminary Design Review where the conceptual design is reviewed and approved; the Critical Design Review where final design approval, along with the go ahead for the manufacturing phase, is granted; and the Flight Readiness Review where approval for launch is given after a review of all data associated with the spacecraft. Table I correlates the system design reviews to equivalent events in the development of a chemical process.

Quantitative Reliability Analysis

The Apollo Spacecraft Reliability Program consists primarily of qualitative disciplines. As stated previously, limited production quantities, extremely high reliability requirements, and evolutionary changes to the spacecraft preclude the use of statistical inference to assess the numerical reliability of the spacecraft. Reliability predictions using historical data of similar equipment have been accomplished for the purpose of comparing alternate approaches. These design studies that have a common historical base are valuable for comparison of different configurations of equipment selected from the data base.

Differences among the equipment in the data base and the actual Apollo hardware preclude accurate predictions of the total spacecraft reliability. However, statistical analysis of test results, performance parameters, and physical properties are performed by other organizations.

Reliability Test Requirements

The reliability organization functions as an integral part of the contractor's test program and is required to ensure, through analysis and proof, that all equipment will perform to the design intent. The reliability organization concurs in all test plans, specifications, and reports. The responsibility of the reliability organization is to evaluate all performance aspects to ensure that all parameters (thermal, vibration, environment stress, etc.) are properly applied and that the results demonstrate the design competence.

Test planning and monitoring are continuous disciplines covering programs on design concept, design verification, prototypes, thermal or environmental (or both) conditions, qualification or certification (or both), acceptance, parts and materials, subsystems, systems, and end-items. Each program requires unique analysis and evaluation to ensure prompt correction to design concepts for a progressive evolution to product reliability. Special emphasis is placed on monitoring the qualification test program which tests the equipment in the actual usage environment including vibration and thermal conditions.

In development and qualification tests, the objectives are related to verification of the design approach. During acceptance test and checkout, the emphasis shifts to verification of the manufacture and assembly of the equipment. Reliability supports these activities with design information and test histories.

Maintainability

The Apollo spacecraft was designed with standby and redundant systems to free the crew from inflight maintenance tasks which might interfere with critical crew functions. Maintainability for the spacecraft consists primarily of fault isolation and switching to backup systems. Because of the need to control the operating time which accumulates on certain equipment prior to launch, equipment with limited operating life time is identified and carefully monitored during ground tests and checkout. If insufficient operating lifetime remains, the equipment is replaced prior to launch. The Failure Mode and Effect Analysis, which was discussed previously, provides inputs to the ground-support-equipment maintenance program by identifying critical equipment for which rapid repair or replacement is required during launch operations.

Parts Program

The NASA reliability publication NPC 250-1 establishes parts criteria for space system contractors. This document requires contractors to implement a program covering selection, specification, qualification, and application reviews of parts for all items to be used in a system. A parts program plan

must also be submitted as part of the reliability program plan. By review and approval of the plan, NASA assures that an acceptable parts control program is implemented by Apollo contractors. The elements of an acceptable control program include qualification, lot acceptance, parts screening and burn-in, and derating.

When departures from program criteria are identified, a detailed technical review of the critical part applications is accomplished to ensure that an adequate rationale for such usage is provided. The assessment activities also include the evaluation of part failures in equipment, the corrective action taken, and an evaluation of the possible impact of problems reported by the NASA ALERT system and other sources. The NASA ALERT system is a program which requires that all NASA installations exchange information on significant parts and materials quality or application problems of general concern. A computerized parts master file provides the identification and applications of all spacecraft electrical, electronic, or electromechanical part. The use of this file permits a rapid evaluation of the potential impact of a problem with any given part type. Significant electrical, electronic, and electromechanical part problems receive particular program management attention. Effective resolution and closeout are verified progressively at major milestone reviews.

The Apollo parts program has concentrated on electrical, electronic, and electromechanical parts because of their predominance in the space program. The program outlined previously was based on acceptance of each part. The high design margin of mechanical parts used predominantly in the chemical industry suggests a program which emphasizes the rejection of bad parts. This control can be accomplished through a system similar to the NASA ALERT program.

Reliability Documentation

The quantity of documentation of the Apollo Program is very large. Yet, the complete, clear story that can be retrieved concerning problem history and equipment tests serves a purpose in such an immense program as Apollo, with approximately 40,000 companies involved in the program. Clear, concise information concerning results from reliability activities is necessary, and a level of documentation to support this requirement is necessary. Documentation requirements adjust as the associated program evolves from its design conceptual phases through design maturity and product operational phases. The necessity for accuracy and technical excellence is obvious when the impact on crew safety or mission success is considered. Reliability design analysis is made available for use by operational personnel in a large program or company only through documentation.

PART II - APPLICATION TO CHEMICAL INDUSTRY

Introduction

With careful attention to economic factors, the techniques discussed in Part I can be applied successfully to the chemical industry. This paper describes the qualitative program elements which are the basis of the Apollo Spacecraft Reliability Program. The application of the techniques to the chemical industry requires careful attention to economic feasibility. Failure Mode and Effect Analysis and problem reporting are the basis for a sound qualitative reliability program in the chemical industry.

The high reliability of the Apollo spacecraft is a demonstration of the effectiveness of qualitative reliability requirements. On the Apollo 8 mission, only five of 5,000,000 parts failed to perform their function. If a level of 99.9 percent had been achieved for the reliability of these parts, then one part in a thousand might be expected to fail. Thus, on each flight, approximately 5,000 parts could be expected to fail.

Reliability Program Implementation

The reliability program elements described previously have been effectively applied to large and small procurements. Procurement size influences the associated reliability plan in two ways. Most smaller procurements are accomplished by a prime contractor on a subcontract basis. The reliability program of the

prime contractor is extended to cover the subcontracted equipment. In other small procurements, the function of the equipment may be completely noncritical to the mission objectives. In this case, minimal reliability requirements are implemented.

For all procurements for the Apollo spacecraft, the definitions "loss of life" and "mission termination" are used to judge the criticality of the function. For the chemical industry, it may be necessary to use a variable definition of critical function. For example, an automatically controlled process which has a throughput capability in excess of demand is not sensitive for loss of life or of productive time. But, the process may have an economic hazard of much consequence such as contamination of a catalyst, spillage of an expensive feedstock, or destruction of property. Although this example oversimplifies safety considerations, it is obvious that variability of definitions is necessary. The following are the major factors which influence the degree of implementation of a reliability program for a given plant or process.

1. Scope - Plant size, number of similar plants, procurement size
2. Contract tier - Turnkey designer, equipment supplier, volume component supplier
3. Criticality of function - Obvious critical functions, unknown or obvious lack of critical functions
4. Definition of criticality - Safety, facility loss, production schedules, economics

The following are the steps in implementing an effective reliability program utilizing the Apollo disciplines:

1. Use the disciplines previously described to structure the basic reliability requirements for a plant, division, or corporation. More extensive commitment to the basic requirements means more success in the individual applications. The basic requirement should include a definition of problem and definition of criticality categories coordinated with the intended users.

2. Perform the following for each segment of the organization, plant, or process:

a. Extend or subdivide the definitions of problem and criticality to fit special conditions. Definitions need not be changed, only supplemented.

b. Examine each reliability requirement in terms of the implementation factors (scope, contract tier, criticality of the function, and criticality definitions). Judge the effectiveness of the requirement in supporting overall objectives (schedules, minimum nonproductive time, reduction, effective turnarounds, and product quality).

c. Develop a procedure for each basic reliability requirement which is economically feasible when the factors in items a and b are also considered.

d. Document the procedures in item c as a plant reliability plan.

e. Develop the forms, data flow, and signature approvals to support the plan.

f. Implement the plan, and train personnel. (The importance of proper training in reliability requires careful planning for this step.)

Implementation for Equipment Suppliers

Equipment suppliers should consider the elements of the baseline plan in development of new product lines. However, the Failure Mode and Effect Analysis and design specification review techniques can strengthen the sales brochure or application guides. Documenting the results of environmental tests and other demonstrations of specification requirements aid the customer in his design review. The Failure Mode and Effect Analysis can be used to define configurations of instrumentation power sources and physical position which offset potential failure modes. This acknowledgment of possible failure modes does not detract from the qualifications of the equipment to the customer who is reliability oriented.

Implementation for Turnkey Design Companies

The base-line reliability plan can probably be most effectively adapted for use by an organization having total responsibility for development of a process facility. Reliability requirements can be implemented at the beginning of the project. The Failure Mode and Effect Analysis proves its value in the selection of the best equipment configuration. Problem report summaries provide an effective way of directing project management and

customer attention to the critical problems of the development cycle, and the customers feel less inclined to oversee the details of the project. An effective set of milestone reviews can be established in which the major problems and corrective actions are reviewed in detail and in which the majority of the project is reviewed in summary format. The problem-reporting system must be good enough to provide confidence that the important problems will stand out. The criticality categories sort all problems into tiers of importance, which allows effective audits of lower tiers. This procedure, which is "management by exception" in the basic form, requires dependence on accurate reporting of events.

Implementation for Startup and Operation

The qualitative approach to reliability as described in this paper focuses attention on designing reliability into a system. Requirements for replacement of limited-lifetime equipment and for preventive maintenance are translated into operational requirements. Problem reporting continues into the operational phase and becomes the focal point of operational reliability. Qualitative reliability documented analysis performed during the development program benefits this phase. The Failure Mode and Effect Analysis provides a basis for fault isolation diagnosis during startup and operations. Review of the Failure Mode and Effect Analysis and of corrective action for problems provides a list of items to be given special attention or checks prior to startup. These data also provide inputs to supervisory control instrumentation points and control functions. The later addition of equipment such as supervisory control to the process requires that the new equipment be subjected to the total requirements of the reliability plan.

Reliability Program Plan

Appendix A contains a base-line reliability program plan for a multiple-plant division or corporation. The plan defines requirements, including procurement of equipment or turnkey plants, for the total life cycle of plants within the division. Implementation of the plan for a division should be accomplished by coordination of the requirements with managers, operators, and engineers from each plant and by modification of the requirements until practical implementation is possible. The plan should then become official procedure, subject only to periodic review and update, as necessary for solving operational problems.

CONCLUSIONS

The reliability program at MSC is basically qualitative in nature, with major emphasis on the disciplines of problem reporting and corrective action and Failure Mode and Effect Analysis. This qualitative approach is most appropriately applied to complex, one-of-a-kind projects. Several chemical industry segments meet this criterion.

Success in implementation of this approach will depend on implementation of each discipline, using definitions and criteria derived separately for each application. Carefully planned and correctly scoped, a reliability program and increase profitability of many chemical operations through reduction of downtime, reduction of equipment losses, and reduction of contingent liability. Implementation of the reliability program for effective management and control is best accomplished by development of a program plan that has been coordinated with all organizational elements involved.

APPENDIX A

BASE-LINE RELIABILITY PROGRAM PLAN

INTRODUCTION

The purpose of this document is to set forth the basic reliability requirements for the_____Division of_____Chemical Company. Management directive_____ authorizes this document and necessitates implementation of the requirements for all processes put into operation after___(date)___. All processes put into operation prior to ___(date)_____must implement the requirements which have operational application. (See implementation guide, page____.) Requirements for safety, quality assurance, maintenance, and testing should be considered in implementing these requirements in order to avoid duplication of effort.

RELIABILITY REQUIREMENTS

The_____Division reliability program consists of the following activities which take place during the development and operation of processes.

Reliability Program Plans

A reliability program plan shall be developed for each plant or operation in this division. Each requirement shall be implemented by a plant procedure or operating rule. Any procedure or rule which conflicts with this plan must be approved by division management. Requirements shall be implemented to the extent appropriate for each of the following cagegories of equipment:

1. Equipment previously installed
2. Standard off-the-shelf equipment procured on a lot basis
3. Special procurements of major equipment items
4. Multiple equipment procurements (turnkey plants)

Design Specification Review

Each design specification shall be reviewed in order to accomplish a correlation between the design and the operating plan functional requirements. Each specification will be reviewed for performance requirements, safety, human factors, test criteria, maintainability, environmental requirements, and equipment that has a limited operating lifetime. The specification shall be reviewed against the basic operating plan and appropriate emergency and standby procedures.

Failure Mode and Effect Analysis

The Failure Mode and Effect Analysis shall be accomplished for each new process facility. The analysis shall identify possible failure modes, the effect on the process, and the criticality of the effect. A control list of the equipment which has Criticality I and II failure modes shall be established and shall be maintained as a major status document during the development of the process. The list shall contain the equipment name, the critical failure mode, the effect, and the proposed corrective action. A process cannot be put on line until all Criticality I failure modes have been eliminated and until all Criticality II items have adequate workarounds. The following are the criticality categories:

I. Destruction of life or process facility
II. Interruption of the process
III. All other critical factors

Problem Reporting and Corrective Action

A problem is defined as the failure of an equipment to perform its intended function when required. A problem may be caused by design inadequacy, quality defect, procedural error, or human error. Problems are categorized as Criticality I, Criticality II, or Criticality III. A system will be developed for reporting problems which occur in any equipment during or subsequent to acceptance testing. A list of Criticality I and II problems and the associated corrective actions will be established and maintained as a major status report during the development and operation of a process. Any problem on this list for which corrective action has not been taken is considered to be an open problem. A process will

not be put on line if any equipment has open problems. The following are other features of the system:

1. Reporting of open problems to management will be scheduled so that timely knowledge of risks will be provided.

2. Each problem reported will be correlated with the Failure Mode and Effect Analysis to determine the criticality category. If the problem has not been identified in the Failure Mode and Effect Analysis, the criticality category shall be identified through analysis, and the data shall be added to the Failure Mode and Effect Analysis.

3. Each problem report of a limited-lifetime item shall include the operating time at the time of failure.

Parts Program

Equipment with basic design proven inadequate for a process is defined as an ALERT item. Each item will be reported to the _____ Division headquarters for distribution to other plants. If Division headquarters receives an ALERT concerning lot-procured items, a procurement stoppage will result until the ALERT can be investigated. An ALERT report from a plant should include identification of the successful substitute.

Reliability Test Requirements

For test under the cognizance of this division, problems encountered during testing must be reported as defined in the section entitled "Problem Reporting and Corrective Action." Problems must be reported during and subsequent to acceptance testing for equipment which is intended for use in this division. If the test is conducted prior to transfer to this division, problem reporting requirements will be included in the specification or procurement document. The acceptance test for equipment to be assigned to this division must include a functional demonstration in the specified environments of pressure, temperature, atmosphere (salt water, etc.), vibration, and compatibility with process feedstocks and products for lot-procured items. Previously documented tests of three or more units satisfy this requirement.

TABLE I

CORRELATION OF INDUSTRY MILESTONES

AEROSPACE INDUSTRY MILESTONE	CHEMICAL INDUSTRY MILESTONE
PRELIMINARY REQUIREMENTS REVIEW	REVIEW OF PRELIMINARY SPECIFICATION
PRELIMINARY DESIGN REVIEW	MANAGEMENT APPROVAL TO RELEASE DESIGN SPECIFICATION
CRITICAL DESIGN REVIEW	MANAGEMENT APPROVAL TO RELEASE DRAWINGS TO MANUFACTURING
FLIGHT READINESS REVIEW	MANAGEMENT APPROVAL TO START UP PLANT

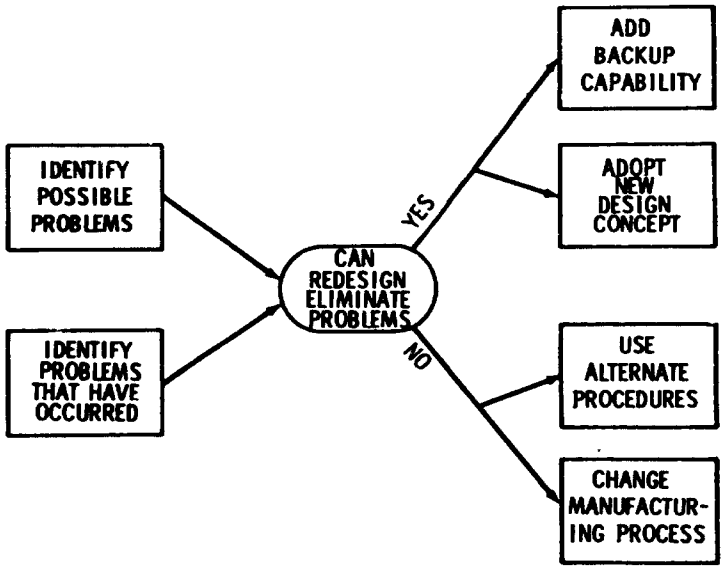

Fig. 1. Basic reliability approach.

ITEM IDENTIFICATION, FUNCTION, AND QUANTITY USED	FAILURE MODE	CRITICALITY	FAILURE EFFECT (a) MISSION (b) SPACECRAFT (c) SUBSYSTEM (d) RELATED SUBSYSTEM (e) INTERFACES	FAILURE DETECTABLE BY		ALTERNATE MEANS OF OPERATION	POTENTIAL HAZARDS RESULTING FROM FAILURE OR FAILURE PROPAGATION DURING CHECKOUT THROUGH RECOVERY	REMARKS OR RECOMMENDATIONS
				SC CREW	GROUND CREW			

FIGURE 2