ORNL-TM-3935

cy. 96

RELIABILITY EVALUATION OF THE FORT ST. VRAIN EMERGENCY ENGINE–GENERATOR SYSTEM

Paul Rubel

[redacted]

OAK RIDGE NATIONAL LABORATORY
OPERATED BY UNION CARBIDE CORPORATION • FOR THE U.S. ATOMIC ENERGY COMMISSION

ORNL-TM-3935

Contract No. W-7405-eng-26

Nuclear Safety Information Center

RELIABILITY EVALUATION OF THE FORT ST. VRAIN EMERGENCY ENGINE-GENERATOR SYSTEM

Paul Rubel
Instrumentation and Controls Division

DECEMBER 1972

OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37830
operated by
UNION CARBIDE CORPORATION
for the
U.S. ATOMIC ENERGY COMMISSION

CONTENTS

INTRODUCTION

One stated objective of the HTGR Safety Program is to add discipline to the assessment of potential accident causes and the effectiveness of engineered safeguards. This requires establishment of a logical framework in which to view plant contingencies with regard to their expected frequencies, other related or coincident events, consequent plant conditions, and responsibilities placed on various systems. The methods proposed include those of formal reliability and risk analysis, emphasizing the logical aspects. By so placing events in perspective, it is hoped to gain guidance not only in ranking the safety research priorities but also in systems design and quality assurance.

The subject analysis of the reliability of the Fort St. Vrain reactor plant emergency engine-generators was undertaken mainly as a pilot study to cultivate a major data and experience source which could be helpful in promoting the larger program objective. That source is the UKAEA Systems Reliability Service (SRS), to which ORNL subscribed in 1971 in anticipation of limited use. Accordingly, the SRS was requested to carry out the formal analysis based on information furnished by Gulf General Atomic Company (GGA) through ORNL.

Of immediate concern was the reliability of an unusual arrangement at Fort St. Vrain, whereby two full-capacity generators (1400 kW) each are driven by tandem half-capacity engines (900 hp). Since a failed engine is automatically disengaged by actuation of a clutch, the system can deliver adequate emergency power with any two engines out of service. However, the arrangement entails added complexity due to the controls which sense engine failure and initiate clutch operation, and the engine speed governors which also apportion load between engine pairs. Qualitative phases of the study concentrated on these design features while reviewing the system overall. Other phases included construction of the system response logic model and numerical evaluation of the system reliability on the basis of accumulated experience for similar components. The study results indicate that the system design should achieve reliability comparable to that of conventional systems employing generators driven by single engines. The problem specifics were set forth in a

letter to SRS, a copy of which is included here as Attachment 1. On completion of the task, SRS presented their conclusions and commentary with supporting data and calculations in a report, principal sections of which comprise Attachment 2.

In light of the exploratory nature of the arrangement, the present report reviews the specific tasks performed by SRS with particular regard to those aspects reflecting on possible future problems. The comments go beyond the immediate study to consider the general procedure in performing the work, the demonstrated ways by which practical insights can be drawn from analysis, and the SRS approach in setting reliability goals. A few points of the study are expanded upon from the author's experience with engine-generators and from his conversations with A. A. Schmudde of the Caterpillar Tractor Company, the engine manufacturer.

Among the broad conclusions drawn from the pilot study is that the validity of the SRS methods and data is not diminished due to differences in design practice between U.S. and British systems, the latter providing the main basis for the SRS experience. Particularly impressive about the study were the many significant engineering interpretations derived from the analysis logic as well as from the numerical results. The exercise of submitting the problem to SRS, discussing the work in progress, and reviewing the results served to develop the desired working relationship between ORNL and SRS.

PROBLEM SELECTION AND EXECUTION

A system reliability analysis traditionally is carried out in two phases: (1) a logic model of the system function is devised in terms of the component contributions, and (2) the probability that the system will perform its function adequately is evaluated, based on the nonfailure probabilities of the components. While these basic procedures are more or less routine, they allow individual analyses to vary widely in depth, interpretation, and execution. Methodical qualitative analyses such as failure mode and effect and common-mode failure usually bridge the gap between the models and the actual systems.

In placing a pilot problem with SRS, it was intended to obtain a conventional reliability evaluation of a safeguard system, along the lines described but with the advantage of a substantial data base of reactor plant experience. There was also incidental interest in the details of the problem execution, particularly interpretations of the components data. Moreover, we wished to learn how and to what extent the SRS exploited analysis so as to add perspective in the review of system designs. With these factors in mind, discussions between GGA and ORNL led to the selection of the engine-generator problem for the following reasons:

1. The system design was available and the system installation essentially completed.

2. A performance reliability objective had been established, and the AEC Division of Reactor Licensing had requested tests to substantiate statistically that the goal could be met.

3. The reliability of emergency engine-generator systems for reactor plants is a continual subject of discussion and controversy.

4. The equipment is familiar enough to afford a basis in practical understanding from which to assess the analysis results.

Arrangements for performing the study according to the ORNL subscription contract were made by letter from D. W. Cardwell to A. E. Green on December 6, 1971. The scope letter (Att. 1) followed, at which time system and equipment information were forwarded. Work was begun by SRS promptly upon receiving the problem information and was completed ahead of the requested date, February 15, 1972. One request for additional information was handled by TWX without delay.

Follow-up discussions of the study were held at ORNL with John Bowen of SRS. Bowen indicated that a large portion of the analysis effort had been devoted to gaining an adequate understanding of the system functions from the drawings and descriptive literature.

TECHNICAL EVALUATION

Study Scope and Methods

Interest in the unusual tandem engine arrangement in the Fort St. Vrain system was the main reason for placing the arbitrary boundaries on

the analysis problem, shown in Fig. 1 of Att. 2. Economy with regard to the demonstration problem was another important factor. The latter consideration also limited the exercise in level of detail; however, the depth had to be sufficient to evaluate essential system features and to demonstrate the SRS problem approach adequately. Suitable depth was achieved by grouping many minor components into subsystems, for example, the engine starting controls and the engine governors. The grouping, shown in Fig. 2, is further justified in that detailed examination requires detailed familiarity with the particular equipment and hence is best done by the component manufacturers.

The SRS analysis report brings out at several points why it is difficult or unrealistic to draw reliability conclusions about such artificially bounded systems. In this particular problem, for instance, the ultimate concern is whether the plant protection features respond in emergencies; to evaluate those probabilities is not only a more complex problem, but one which emphasizes engine-generator responses somewhat different than those in the present analysis. Perhaps the most important single factor disregarded in defining the problem (but not overlooked in the SRS report) is that the availability of emergency power for a gas-cooled reactor may be delayed, permitting time for minor repairs or operator intervention when automatic sequences fail. The report further points out potential common-mode factors beyond the problem boundaries, such as the cooling water supplies to the engine heat exchangers. The latter consideration further involves the problem definition in regard to required running time; in the case of the water supply, interruptions may be unimportant for the specified 4-min cycle, but likely critical with regard to realistic longer cycles.

The SRS carried out the study as a straightforward system reliability analysis, observing the constraints and emphasizing other aspects as requested. Component reliability data were obtained from the Syrel information system, which is associated with SRS and derives most of its input from operating records of UKAEA reactor plants. Where the available data were inadequate or not directly applicable to the problem, they were supplemented by engineering evaluations.

A system logic model was developed from the system description provided to SRS. Since the model was fairly simple, the initial reliability calculations were done by hand, with the usual discarding of trivial terms to simplify the process. The system was then modeled and evaluated more rigorously using the computer program NOTED; in this step, SRS obtained problem solutions over ranges of parameter values in order to determine the effects of, or sensitivity to, the input variations. Several natural questions regarding effects of component data uncertainties were answered by the sensitivity analysis.

A major part of the problem assignment was to demonstrate practical engineering interpretations of the input data, the logic model, and the numerical results. The SRS report indicates how this was done at each stage. Considerable attention is given to those factors determining the effectual conduct of system tests.

Incidental to the main study, SRS had been requested to comment on the setting of reliability goals. Their response was based on application of the Farmer risk criterion[1] and included examples combining demand frequency with failure consequence to determine the required response probability.

System Reliability Criteria

The problem statement to SRS indicated a system target reliability of 0.9999 with 95% confidence, for every trial and meeting any of the several "success" combinations. Section 2.2 of the SRS report states that the target should be allowed to vary depending on different initiating conditions. One practical aspect of such variation is brought out in the discussions of system testing, Section 5.7, where it is shown how dependence on the system changes over the plant commissioning phases and with later operation.

---

[1]F. R. Farmer, Siting Criteria — a New Approach, in *Containment and Siting of Nuclear Power Reactors*, Symposium Proceedings, Vienna, 1967, pp. 303–329, International Atomic Energy Agency, Vienna, 1967 (STI/PUB/154).

Appendix 2 describes via a series of simple examples how the "frequency risk approach" can be applied in setting protection system reliability targets. In brief, the method postulates situations in which the protection system is called upon and estimates their frequency (i.e., demand frequency). The consequence of protection system failure is expressed in terms of ultimate fission product release, which is then referred to a general "risk limit line" to find the "acceptable" frequency of that release magnitude. The allowed failure probability of the system is determined as that value which, when multiplied by the demand frequency, yields the acceptable release frequency. Different probability values will be found for the various demand situations, the highest response probability requirements generally providing the basis for system design. The examples further demonstrate how the method may be used to determine the reliability requirements on parts of a protection system with redundancy, for example, by including partial failures of that system as contributions to the demand on other portions of the system. To use the method effectively requires careful analysis of the overall plant, which seems desirable for other reasons as well.

Section 2.2 (b) points out that a system design reliability target of 0.9999 is too high where manual operation is required within 1 or 2 min of the system demand; hence the problem statement is inconsistent. This criticism is proper; however, it is based on incorrect information furnished to SRS. Provisions are made in the Fort St. Vrain Plant to switch the vital loads automatically; only after several coincident failures is operator action called for to select and apply loads. Even then, the time allowed is more like 15 to 30 min rather than the criticized 1 to 2 min.

Components Reliability

In illustrating the iterative nature of reliability studies, particular attention was given to the engine speed governors after a preliminary system evaluation had identified them as critical items. Sections 3.1 through 3.8 of the report provide both failure mode and effect and common-mode failure analyses of the governor systems. In particular, the

possibility was examined that a failure could disable both engines of a tandem unit or even all four engines of two tandem units when operating in parallel. The discussion of failure mechanisms suggests several points for design review and for special test or maintenance attention. The exercise further illustrates how an engineering evaluation may exploit generic reliability data on similar equipment as a means to develop reasonable estimates of the reliability of specific components for which no direct experience data are at hand.

Sections 3.9 and 3.10 treat the reliability of the basic engines and some auxiliaries. Considerable experience data were available from Syrel; however, the statistics were mainly for overall failures of engines to start and run, with no separate accounting for component contributions. Since the reliability effects of the speed governors, redundant starting systems, and other component groups were explicit in this study, it was necessary to estimate what portion of the experienced failures were due to the engines themselves or to auxiliary equipment lumped with them in the logic model.

Available reliability figures for the generator and excitation systems were for units in continuous operation. Somewhat higher values were estimated for standby units, as described in Section 3.11, since the rate of deterioration of the windings depends on operating conditions such as temperature and vibration.

The preliminary system analysis indicated minor dependence on the clutch disengaging function. Additional attention was given in Sections 3.12 and 3.13 to failure modes whereby the clutch could not transmit power.

Only limited information on the reliability of air starting motors is claimed in Section 3.14. However, the redundancy of these motors results in only minor dependence on individual units. Section 6.1 (a) suggests the possibility of a common-mode failure in which the starter pinion jams the engine flywheel ring gear; this is indicated by the engine manufacturer to be very unlikely.

A very small failure probability was attributed to the engine fuel supply facilities for the short operating cycle. However, Sections 3.15 and 6.2 [(b) iii and iv] highlight several possible common-mode failures of the fuel system. These involve such diverse factors as improper fuel

furnished to the main tank, fuel in the main tank chilled so that it cannot be pumped to day tanks, and failure in engine supply piping from the common (i.e., to one pair of engines) day tank. Moreover, operating the engines over longer cycles (i.e., the real emergencies) would involve more of the fuel system equipment, in particular, all of the fuel transfer facilities and the main storage tank. This area requires careful attention in design and operation.

It was beyond the problem scope to perform elaborate analyses of the engine starting, clutch actuating, and other control circuitry. However, preliminary estimates of the circuit reliabilities were made using numbers and types of elements provided and generic failure rate data from Syrel. The data used appear in Tables 1 to 3 of the SRS report. Various comments on features of the control circuits are given in Section 4.4 (number of contacts in series in starting control), Section 4.5 (unnecessary dependence of the clutch actuator circuit on a master relay), Section 6.1 (c) (dependence on common dc control power supply), Section 6.1 (d) (control panel protection against common accident involvement), and Section 6.1 (e) (operator error which defeats controls).

System Analysis

Chapter 4 of the report, with Appendices 3 and 4, presents the details of the problem execution, as summarized earlier under "Study Scope and Methods." Clearly shown are all steps of the model construction and its numerical evaluation, along with the component reliability values used. The problem is solved first by hand calculations using "best estimates" of the component values and is then repeated by computer to determine the effects of varying the component reliability values and the test intervals.

The main conclusion of the analysis is that the system reliability is between 0.999 and 0.9999, disregarding the probability of common-mode failures. Two other salient factors are demonstrated: (1) the speed governors, common to each pair of engines, are relatively important to the overall system reliability; and (2) the capability to disengage a failed engine is relatively unimportant. Sections 4.11 to 4.14 draw additional engineering interpretations from the analysis results.

Regarding the apparent unimportance of the clutch disengaging function, it appears to the author that this may be partly an artificial conclusion, due to the problem rules. In the actual long-term operating situation there is reason to believe that the clutches could enhance the system reliability somewhat. The benefit suggested, however, is difficult to quantify since it involves operator intervention.

Section 4.11 (f) points out that the system reliability depends heavily on the reliability of the monitoring and alarm facilities. The desirability of locating readouts and annunciators at manned stations is also highlighted.

Testing to Substantiate Reliability Predictions

A test regime to demonstrate the reliability of the engine-generators, planned and initiated before undertaking the SRS study, is now completed. Briefly, it consisted of repeated start and short run cycles, sufficient to establish the individual generator unit reliabilities of 0.99 at 95% upper confidence level. In requesting SRS to recommend a test procedure, it was felt that the tests in progress were not entirely consistent with the required duty of the system and that some vital capabilities were not being adequately demonstrated.

Chapter 5 of the SRS report explores the test problem thoroughly from both theoretical and practical standpoints. The theoretical discussion points out that various statistical criteria may be applied, leading to much different test requirements. Several practical substitutes for accelerated "statistical" testing are offered, emphasizing careful engineering review of the test experience and allowing system conclusions to be drawn from satisfactory performance of the components.

The practical test regime proposed is attractive in an engineering sense, less rigorous statistically than the one in progress, and properly concerned with the ultimate system duty. By the time the reactor is ready for startup, a substantial body of experience has accrued. A careful review of that experience could then establish whether (1) all evidence of systematic trouble had been resolved, (2) wear-in difficulties were no longer appearing at an appreciable rate, and (3) the equipment

identified with potential common-mode system failures showed no sign of unreliability. With the system satisfactory on all the above counts, it could tentatively be judged reliable enough to permit the reactor startup. Statistical confirmation that the reliability goal was being met would be realized after about one year of reactor operation, assuming no significant failures were experienced in that time.

Common-Mode Failures

The SRS numerical analysis model did not include common-mode failures since these are individually improbable. Chapter 6 comments, however, that the overall frequency of common-mode faults in "reliable" systems is expected to be of the same order as the system failures due to random component faults. The remaining discussion in Chapter 6 concerns particular common-mode failure mechanisms for this system; faults disabling one generator are considered first, then faults affecting both units. Events and conditions beyond the problem boundary are covered. A number of suggestions are developed which should prove valuable, not only with regard to system design but also to long-term system operation.

Comparison with More Conventional Arrangements

Appendix 5 of the SRS report essays a rough comparison between the reliabilities of the Fort St. Vrain engine-generator system and of the more conventional system proposed for the TVA Sequoyah plant. According to the Preliminary Safety Analysis Report for Sequoyah, the latter system has three independent single-engine single-generator units, each capable of supplying one-half of the total emergency load. The theoretical results show the systems to be about equivalent, although the Fort St. Vrain system reliability is much more sensitive to the reliability of the speed governors. Unreliable governors (i.e., in both cases) would weight the comparison in favor of the Sequoyah arrangement; but since this is a threshold effect, the converse is not true.

CONCLUSIONS

The SRS study fulfilled all the basic analysis requirements and addressed each of the specific requests set forth in the scope letter. A careful reading of the SRS report is urged, since it brings out clearly by example how theoretical and practical considerations can be combined to gain realistic reliability insights. In this respect, the report is perhaps more instructive than most of the current literature on the subject (and a great deal more concise). The many engineering interpretations placed on the components data, the model, and the numerical results are in welcome contrast to the unrelieved statistics often associated with reliability analysis; a desirable impression is conveyed of a methodical engineering evaluation with the added perspective of logic and probability.

The present depth of the analysis seems adequate to assess the potential reliability of the engine-generator arrangement and to identify possible system weaknesses. It also suffices to exploit the principal relevant experience data from the UKAEA reactors. However, some further detailed review of certain system parts appears desirable; this could be accomplished by the designers and equipment manufacturers more economically than by SRS, given the present guidance of the SRS report.

Several of the technical points raised in the analysis pertain to tandem engine operation in a general way. Since that arrangement is attracting interest for other reactor plant applications, these questions have been referred to the engine manufacturer for comment.

Other issues in the report concerned the role of the emergency power supply in the overall plant protection scheme. Although such matters are beyond the scope of the immediate study, it is hoped that the HTGR Safety Program and similar efforts will define the system requirements satisfactorily in the near future.

ATTACHMENT 1

OAK RIDGE NATIONAL LABORATORY
OPERATED BY
UNION CARBIDE NUCLEAR COMPANY

POST OFFICE BOX Y
OAK RIDGE, TENNESSEE

December 13, 1971

Mr. A. E. Green, General Manager
Systems Reliability Service
United Kingdom Atomic Energy Authority
Risley, Warrington, Lancashire
England

Subject: Request by Oak Ridge National Laboratory (Subscriber) for Reliability Analysis Service

Dear Mr. Green:

In his recent letter to you, Mr. D. W. Cardwell indicated that we wish to submit a pilot reliability problem to the Systems Reliability Service for analysis. The desired study concerns the reliability of the emergency electric power supply for the Fort St. Vrain gas-cooled reactor plant. This letter and the accompanying material (under separate cover) describe the problem in detail.

The main purpose of the exercise is to allow us to become familiar with SRS practice, e.g., in matters of problem approach and communication with clients. However, the trial problem itself is an important one in several respects. First, the system represents a departure from the usual reactor emergency power supply safety requirement (in the U.S.) that a single engine/single generator unit be capable of handling the largest transient demands imposed by the vital loads. The AEC in this case has required the reactor license applicant to justify the arrangement, that is, to show that it represents no significant compromise relative to the conventional scheme. This explains the seemingly arbitrary choice of problem system boundaries. The fact that the AEC desires the justification via numerical analysis is a significant milestone; we hope it portends further adoption of such methods. Finally, the AEC has requested tests to substantiate the system reliability. The applicant has already proposed a test program which we believe does not adequately demonstrate all of the features vital to system reliability in degraded modes (e.g., one or two engines do not start).

Our interest in the trial problem extends considerably beyond the numerical results. In particular, we wish to see whether, or to what extent, SRS reduces the problem conclusions to engineering considerations. These could take various forms such as qualifications on the component data, recommendations regarding system improvement, practical advice on component selection, etc.

Main components of the system to be analyzed are outlined in Figures 1 and 2, which also show the boundaries of the numerical analysis problem. Additional details are given in the design drawings and literature descriptive of the components.

We recognize that reasonable limits need to be chosen with regard to extent of detail that shall be considered in the analysis. Overall, we hope to remain within the amount allowed by the service subscription plus about $3000; as Mr. Cardwell's letter pointed out, we would need to have an estimate of any anticipated expenditure beyond $3000 in order to request a special authorization for additional funds.

In keeping with the above, I have indicated in Figures 1 and 2 what I believe to be a minimum level of detail for a satisfactory analysis. That is, many "minor" components have been grouped as subsystems. The additional detailed information provided may suggest areas where some expansion is worthwhile; otherwise, this information will help you to gain a background knowledge of the system.

The problem system has all components of U.S. manufacture. Nevertheless, we prefer that you apply generic reliability data from Syrel for comparable components or subsystems; if Syrel makes any distinction by component origin or manufacturer, such refinement may be included and highlighted to us. We would like to have listed separately the individual component or subsystem reliability values which are used in the system analysis. Some of these values will be predicated on reasonable test intervals, which assumptions should then be indicated. Equipment outside the problem boundary shall be regarded as having perfect reliability, i.e., R = 1.0.

For the formal analysis, reliability is equated to mission success probability. The mission is defined: System starts automatically on demand and delivers at least 1200 kw (i.e., 50% of total combined nominal capacity) for 4 minutes thereafter. Allowed combinations include:

a) all engines and generators
or
b) engines 1 and 2 with generator A
or
c) engines 3 and 4 with generator B
or
d) generators A and B with one engine each at full power to drive them and disabled engines disengaged from generators by automatic clutch (PTO) actuation.

We believe that a failure-mode-and-effects analysis in great detail is beyond the scope of the present task. However, we hope that you will comment informally on the system arrangement and engineering features, in regard to reliability as well as other practical engineering aspects. Additional comments on portions of the system outside the formal boundary would also be welcome, e.g., fuel storage and transfer, generator paralleling, engine secondary heat rejection, etc.

The target reliability for the system, i.e., for portions within the problem boundary and according to the mission success criterion defined above, is 0.9999 for each trial with 0.95 confidence. It is desired to demonstrate this reliability via a suitable test regime. The procedure now being proposed consists of repeated trials of one unit, i.e., two engines with one generator, until the numbers of simple successes and failures yield the desired binominal success/failure ratio and confidence. Even presuming the system initial defects to have been corrected before the main test is begun, the procedure could require a large number of trials. Moreover, the tests tend to de-emphasize the vital contribution of the clutch disengaging function to the system reliability.

We feel that it should be possible to devise a test procedure more effective than the one proposed, perhaps via separate demonstration of a few vital sybsystem reliabilities, e.g., engine, clutch, speed governor, generator, etc. But unfortunately we at ORNL have had no experience at combining reliability data for several components so as to carry the confidence concept into a system reliability prediction. In requesting SRS to recommend a test procedure, we are interested in finding whether any of your previous work bears on this matter of an acceptable test-by-parts.

The test considerations thus far are of an initial demonstration. We are also interested in your views and/or recommendations regarding a long range test program to assure continued system reliability.

In view of the system commissioning schedule, it would be desirable to complete the analysis by about February 15, 1972.

Feel free to contact me concerning any questions of system detail or conduct of the analysis. If you anticipate that the work outlined will exceed the indicated limit, please advise both Mr. Cardwell and me before proceeding; it would also be desirable at the same time for you to suggest ways of adjusting the task to within the limit.

We are looking forward to your response on this pilot problem. We also are in hopes that the present effort will promote further use of and participation in the SRS program.

Sincerely yours,

Paul Rubel

PR:vcf

Paul Rubel

ATTACHMENT 2

[redacted]

DRAFT

SYSTEMS RELIABILITY SERVICE

(on behalf of:

OAK RIDGE NATIONAL LABORATORY
POST OFFICE BOX Y
OAK RIDGE
TENNESSEE
U.S.A.

SRS/ASG/1017

AN IN PRINCIPLE RELIABILITY ASSESSMENT OF THE FORT ST VRAIN H.T.R. EMERGENCY ELECTRICAL SUPPLY SYSTEM

Systems Reliability Service,
U.K.A.E.A.
Risley
Nr. Warrington
Lancashire

February 1972

[redacted]

SUMMARY

This report contains the results of an "in principle" assessment of the Fort St Vrain Emergency Electrical Supply System which has been carried out by the Systems Reliability Service of the United Kingdom Atomic Energy on behalf of the Oak Ridge National Laboratory.

The main conclusion is that the system has a success probability of 0.999 - 0.9999 to deliver at least 50% of the total system capacity, on demand, for four minutes.

The assessment consists of a qualitative and quantitative engineering analysis.

The predominant item in the overall reliability of the system is shown to be the engine governor unit which is a common element between two engines. Recommendations are made for testing arrangements with a view to substantiating that the system approaches the target reliability figures.

Constructive comments are also made regarding parts of the system, outside the boundary of work assessed, which could affect the overall system reliability.

[redacted]

LIST OF CONTENTS

APPENDICES

TABLES

FIGURES

[redacted]

SYSTEMS RELIABILITY SERVICE

Reliability Assessment of the Emergency

Electrical Power Supply System for the

Fort St Vrain High Temperature Gas Cooled Reactor Plant

1. AIMS AND METHOD OF ASSESSMENT

Introduction

1.1 The Systems Reliability Service of the United Kingdom Atomic Energy Authority, at the request of the Oak Ridge National Laboratory[1,2], has carried out an "in principle" reliability appreciation and outline reliability analysis for the Emergency Electrical Power Supply for the Fort St Vrain High Temperature Gas Cooled Reactor Plant. This appreciation and analysis has been completed in accordance with the Contract Letter[3] and the following extract of Clause 2 of the Contract Letter details the aim of the assessment.

Aim of Assessment

1.2 "Subject to the availability of information as under Clause 1 and subject to the provisions of Clause 7, S.R.S. will carry out work so as to:

a) highlight any significant areas of unreliability on any specific parts of the system which may significantly affect the overall reliability of the system;

b) list the data used in the work and comment on its appropriateness for the particular application;

c) comment on aspects of system capability and such other aspects related to engineering considerations as may arise during the course of the work;

d) make suggestions with regard to means for confirming any appropriate reliability estimates which arise from the work, means for improving reliability and areas where further work would be desirable."

[redacted]

Method of Assessment

1.3 The basic details of the system design and operation were obtained from the letter Paul Rubel/A. E. Green dated 13 December 1971[2] and from accompanying drawings and literature describing various system components and the system boundary[4]. Further information was requested by S.R.S. on system initiation and of its starting (or dormant state) and this was provided in a telex Paul Rubel/E. A. White dated 27 December 1971[5] and which enabled S.R.S. to build up a further understanding of the system design and operation.

1.4 The following procedure has been adopted:

a) Generic failure rate data from the SYREL Data Bank has been used for components e.g. contacts, relays, in start up and trouble circuits.

b) An engineering appraisal has been made of the functioning of the Woodward Governor system and failure rates ascribed to this from a comparison of similar electronic equipment. The clutch or Power Take Off Unit has been dealt with in a similar manner.

c) Generic failure rate data from SYREL has been used for the complete diesel engine unit, air motors, solenoid valves etc. The above are discussed in detail in section 3.

d) In some instances specific failure rate values are not available. For such cases a failure rate or failure probability has been assumed based on information for similar equipment. Where the assumed value is shown to represent a sensitive area with regard to the overall system reliability then upper and lower mean values have been used to demonstrate the overall effect of the different fault rates. Similarly in using this "boundary approach", where it is seen that the various values for a component do not have a significant effect on the reliability of the complete system, then this is stated

e) A mathematical model, covering the system, for use in hand calculations has been evolved in Appendix 3.

[redacted]

f) The system has also been set up for the NOTED programme as in Appendix 4 and in which the importance of reliability values for different parts of the system has been examined. The system assessment, taking in account the above is discussed in Section 4 which also discusses the engineering interpretation of the results.

g) Testing of the system, both initial and operational, is discussed in Section 5.

h) (a) to (f) will enable the random failure rate of the system to be evaluated. There are a number of areas, some outside the system boundary, in which the possibility of systematic failures arises. These are discussed specifically in Section 6.

j) Since it is stated in Ref 2 that the Fort St Vrain System represents a departure from U.S. practice a simple comparison has been made in Appendix 5 between the Fort St Vrain System and the Sequohah P.W.R. system. It is not known if Sequohah is typical or whether rule changes have been made since Sequohah, but information was to hand for Sequohah and this was therefore used as a comparison.

2. SYSTEM DESCRIPTION AND OPERATION AND TARGETS

2.1 The system consists of:

a) Two a.c. Generators A & B each of 1400 kW.

b) Four 900 h.p. Diesel Engines Nos 1, 2, 3 and 4.

c) Engines 1 and 2 drive Generator A through a clutch or power take off unit with the speed and power being controlled through a governor system common to both engines. The same arrangement applies to engines 3 and 4 with Generator B.

d) The system boundary is shown in Figs. 1 and 2 which also shows the duplicate air starter motors, air tanks etc.

[redacted]

e) For the formal analysis, reliability is equated to mission success probability. The mission is defined: system starts automatically on demand and delivers at least 1200 kW (i.e. 50% of total combined normal capacity) for 4 minutes thereafter. Allowed combinations include:

i) All engines and generators, or

ii) engines 1 and 2 with generator A, or

iii) engines 3 and 4 with generator B, or

iv) generators A and B with one engine each at full power to drive them and disabled engines disengaged from generators by automatic clutch (PTO) actuation.

f) The target reliability for the system as defined above is 0.9999 for each trial (or demand) with 0.95 confidence.

g) Transfer of protected distribution buses to emergency power is automatic, one to each generator. If a large load is connected to an emergency bus prior to the transfer, e.g. for a test, it is dropped automatically. Cross connection between the two buses is manual including synchronisation.

h) Starting of major emergency loads is manual.

Comments on 2.1

2.2 It is appropriate to comment on 2.1(f) and 2.1(e) and (h).

a) The target reliability, i.e. 0.9999 success with 95% confidence, is given as applying for every demand. In the U.K.A.E.A. approach to reactor safety the system reliability required would vary depending on the different initiating demands. Appendix 2, which is included for information, gives a simple outline of the U.K.A.E.A. frequency/risk approach to reactor safety. Possible changes in target requirements are also discussed in Section 5.

b) The statement at 2.1(h) that the starting of major emergency is manual does not appear to be consistent with 2.1(e and f) i.e. that the system

[redacted]

starts on demand, and is required to run for four minutes with a reliability of 0.9999 and 95% confidence. The U.K.A.E.A. would only ascribe success in the range 0.3 - 0.9 for a manual operation on a timescale which must be of the order one to two minutes. This item is outside the boundary of the present analysis but is drawn to the attention of O.R.N.L. for further consideration.

3. ENGINEERING COMMENTS AND RELIABILITY OF SYSTEM COMPONENTS

Woodward Governor and Actuators

3.1 A significant fact about the Woodward Governor is that it consists essentially of a single unit shared between two diesel engines. The governor is operated by a single magnetic pickup for generator speed measurements. A single output from the governor operates the two diesel fuel supply actuators. The actuator coils are connected in series so that they are energised by the same electrical current.

Any fault affecting the governor output will thus affect both diesel engines. The governor also senses the voltages and load currents supplied by the generator by means of a part of the circuit called the load sensor. Faults within the load sensor can also affect the output to the actuators.

3.2 The governor is essentially a d.c. (direct current) device and it is known that for d.c. circuits, about 50% of the failure rate will generally cause an output decrease, the other 50% generally causing an output increase. A decrease in the governor output will cause reduction or loss of fuel to the diesels and hence a loss of the electrical supply. An increase in the governor output will cause the diesels to overspeed: the overspeed trip will then be expected to shut the system down, again causing a loss of electrical supply.

3.3 It would appear that during standby conditions, the governor is permanently connected to the 24V supply and is therefore continuously energised, ready for

[redacted]

a start demand. However, the governor output current does not seem to be monitored except indirectly during periodic routine checks of the diesel generator system. Hence, unrevealed faults could occur between checks. Then, at start up, the behaviour of the diesels would depend upon the condition of the output from the faulty governor: the diesels may not start at all; they may fail to accelerate after having been started; they may overspeed and cause a trip.

From the point of view of system failure, the governor together with all the input sensors and transducers and also together with the two actuator coils, can be considered as a single "block": (an open circuit fault on an actuator coil will stop both diesels).

3.4 For the purposes of this short exercise, it is not intended to analyse in detail the failure rates for the governor "block". A sample of electronic equipment used in land based nuclear installations have shown failure rate from $6f/10^6h$ up to about $200f/10^6h$, in 95% of cases, the figures being dependent upon the degree of equipment complexity, operating conditions, etc.

These figures are based on a sample of 19×10^6 equipment hours giving a mean failure rate of $82f/10^6h$. Based on this experience, a tentative mean failure rate of 0.7 faults/year has been allocated to the Woodward Governor with possible lower and upper values of this mean of 0.2 and 2.0 faults/year.

3.5 The actuators are hydraulic/mechanical items. The following conditions are assumed:

1. The actuator coils are always energised from the governor
2. The hydraulic supplies to the actuators are normally off during standby conditions and only come on when the diesels are cranked.

Each actuator will only affect one diesel when a fault occurs (not counting open-circuit actuator coils). The actuator can be considered as a "direct coupled" device (analogous to a d.c. electronic equipment) where approximately 50% of the failure rate will cause a fuel loss, the other 50% causing a fuel increase. However, because of the presence of the overspeed trip facility on

[redacted]

the diesel engine, all actuator faults will have the same final effect; i.e. loss of drive from the corresponding diesel engine.

3.6 Field failure rates for hydraulic actuators have shown values of 2.4 to $23f/10^6$ the aboverage being $7.6f/10^6h$ (based on history time, not operating time). The actuators were operational for about 3.3% of their total history time. For the purpose of this exercise, the history failure rate for the actuator is assumed as 0.07 faults/year. The actuator is not in use for much of its time so that faults due to wear are expected to be minimal. However, this advantage could be off set by such factors as variations in environmental conditions and siezing of sliding seals during standby. The possible range of mean failure rate values for the Woodward actuators are assumed to be 0.02 and 0.2 faults/year, for the purposes of this report.

3.7 It has been noted both in the Woodward specifications and in the circuit diagrams for the diesel generator system that provision is made for paralleling the generators. The load sharing facilities of both governors would be operable under these conditions. At the instant of paralleling, an earth fault on the common line between the two governors would cause all 4 diesels to shut down. In addition, if the generators are successfully paralleled, then a subsequent fault affecting the load sensor circuit in either governor would again cause all 4 diesels to shut down. Obviously, in any reliability analysis of these standby supplies, the adverse effect of even occasional paralleling of the supplies should be taken into account. The reduction in system reliability will be a function of the proportion of time used in the parallel mode of operation.

3.8 <u>Calculations, Fractional Deadtimes due to Failures</u>

(i) <u>Failure of any 1 diesel to start (due to actuator faults)</u>

Actuator Failure Rate	Mean .07	Lower .02	Upper .2	Unit faults/yr
Fractional deadtime (weekly checks)	7×10^{-4}	2×10^{-4}	2×10^{-3}	
" " (monthly ")	3×10^{-3}	8×10^{-4}	8×10^{-3}	

[redacted]

(ii) Failure of both diesels on one set to start (due to governor faults)

	Mean	Lower	Upper	Unit
Governor "block" failure rate	.7	.2	2	faults/yr
Fractional deadtime (weekly checks)	7×10^{-3}	2×10^{-3}	2×10^{-2}	
" " (monthly ")	3×10^{-2}	8×10^{-3}	8×10^{-2}	

Diesel Engines

3.9 Each diesel engine has two associated air motors any one of which will successfully crank the engine. Each air motor has its own independent air supply via a solenoid control valve and this is energised to open when a demand arises. Both solenoid valves are energised to operate from the same start up circuit shown in Fig 3(a). In considering the overall reliability of a diesel engine to auto-start and run, on demand, the majority of field information available to S.R.S. gives the number of occasions that a unit has failed to start when required. This fault rate, however, is for the complete system i.e. from the starting signal to the engine operating - hence it includes starting circuits, control relays and valves and the engine itself. For this system the individual parts are being separately assessed and thus a value is required solely for engine faults. Our data indicates a value not higher than 5×10^{-3} and so this figure will be used.

3.10 Having stated this we feel that some of our own experience with complete auto-start diesel engine systems should be recorded. During a total of 340 engine test starts (8 engines) 16 failures to start were recorded. On another installation (2 engines) 6 failures were recorded dueing 256 test starts. Thus a mean failure rate to start of approximately 2×10^{-2} emerges. These installations consisted of a single air start valve, de-energised on loss of normal supply to admit air to the engine and the majority of failures were associated with this auto-start control device. For current installations having duplicate air start devices we have demonstrated 10^{-2} probability of failure per demand. However, in our opinion this can only be maintained with a high standard of maintenance, proof checks and no operator adjustment to controls without justification and prior approval.

[redacted]

Generator

3.11 Available failure rates for generators are associated with running units and these give a value of 0.7 faults/year. For the generator on this particular system, which is normally dormant, one would expect a lower value for any unrevealed failures and for these to be associated with excitation and other control systems. In the absence of a detailed investigation it is considered reasonable to assume an initial fault rate for the generator of 0.07 faults per year, and then consider the effect on the overall system reliability of a higher fault rate.

Clutch - Twin Disc Type SP321-P00

3.12 In this installation the clutch is a normally closed, dormant device. It is only required to operate (i.e. open) in the event of an engine failure, hence in looking at the clutch operation one is interested in determining those faults which in the event of a demand, would prevent it from opening e.g. due to mechanical stiction or failure. However, brief attention has also been given to the possibility of it failing to transmit power due to inherent failure.

It is a mechanical, self-sustaining clutch, i.e. it remains engaged or disengaged after the actuating force has been removed. It is simple, and with correct adjustment and lubrication should be very reliable. Only two failure modes need be considered here:

(a) Slip due to mal-adjustment. The number of demands on the clutch will be small and after correct initial adjustment, failure from this cause would be very unlikely.

(b) Failure of the thrust collar and yoke. This has a metal to metal grease lubricated bearing which would wear rapidly if the solenoid pneumatic valve failed to release the actuating force after engagement. Even where the collar is completely lost, the clutch would still transmit power, but it could not be disengaged in the event of one engine failure.

[redacted]

Failure Rates

3.13 Assuming that the clutch functioned satisfactorily at the last test and that a warning is provided if the clutch is not left in the "engaged" state, then the probability of it not transmitting torque at start-up is considered to be less than 10^{-4} per demand. This failure has not been taken into account in the analysis in view of the low rate compared with other components in the system.

The duty requirement of the clutch relative to its effect on system reliability is its capability to open on demand. Hence its probability of failure to open on demand is required to be known. This probability of failure, assuming air is admitted to the actuating mechanism is considered to be 10^{-3}. Detailed consideration has not been given to further substantiate this value since the analysis in Section 4 shows it to be not critical.

Air Motors

3.14 These units are not in continuous operation but only in intermittent use following a demand. A fault rate per year parameter may not therefore be the most appropriate. The parameter required is the probability of failure per demand and this could best be demonstrated by a test programme as discussed in Section 6. For this exercise a failure probability for an air motor of not greater than 10^{-2} is considered realistic, based on limited information and is therefore used. The effect of a higher failure probability is however also shown in Section 4 to have little effect on the overall system reliability.

Engine Fuel Supplies

3.15 The diagrammatic arrangement of the engine generator system - Fig. 1 - shows a "fuel day tank" and an associated fuel transfer pump for each engine. However, it is obvious, from Drg. P1-92 and Drg. No. 683982 that each pair of engines e.g. engines 1A and 1B, have a common "day tank" and a single electrically driven fuel transfer pump. A pipe fracture, blockage or union leakage in the feed line from the day tank to the engines, could thus prevent operation of both engines.

[redacted]

Similarly in the event of low level in the day tank requiring operation of the fuel transfer pump and/or the low level alarm, then failure of either of these could result in loss of both engines. This is not seen as a failure which is likely to inhibit starting and running for a short period and the probability of such failure due to this fault is considered not greater than 10^{-4}. It would thus have no significant effect on the overall system reliability.

However, if the reliability of the engines to run for a period of some hours was of safety significance then we would recommend that the reliability of this part of the installation, the pump starting arrangements, low level alarms and fuel checks by the operatior, be all examined in some detail.

General Components

3.16 Failure rates for other system components are listed in Table 1. As previously stated some have been obtained from the SYREL data bank but other values e.g. that for the time delay relay, are those derived from a detailed assessment of a specific device in use on systems which we have examined.

4. SYSTEM ANALYSIS

General Arrangement

4.1. A logic flow diagram for a single unit i.e. two engines and one generator is shown in Fig. 3. This shows each individual component in the start up chains and also in the clutch opening circuit. From this diagram and using the fault rate values listed in Tables 1 and 2 the probability of failure of the operating circuits and of an engine unit to start on demand is determined.

Engine Starting Reliability

4.2 Considering therefore a single engine unit and assuming the rules when dealing with small probability values:

The probability of failure to start an engine on demand

[redacted]

= Probability of failure of the starting circuit + probability of failure of the air motors + probability of failure of actuator + probability of failure of engine.

The probability of a system failing on demand (i.e. due to unrevealed faults) is the fraction of the time that it could be in a failed state due to such dormant faults.

Hence, probability of failure = Mean fractional deadtime

$$= \frac{\theta\tau}{2}$$

where θ = fault rate per year

τ = test interval in years

The assumption is made that each engine will be automatically test started on a weekly basis.

∴ From Table 2 and Fig 3(a)

the probability of failure of the engine starting circuit due to component faults $= \frac{\theta\tau}{2} = \frac{0.016}{104}$

$\approx 1.65 \times 10^{-4}$

Probability of failure of the starting air solenoid valve $= \frac{\theta\tau}{2}$

$\approx \underline{\underline{5 \times 10^{-4}}}$

Probability of failure of a single air motor $= 10^{-2}$

∴ Probability of failure of a single valve and motor $= 10^{-2} + 5 \times 10^{-4} \approx \underline{\underline{10^{-2}}}$

Using redundancy arguments then the probability of failure of both motors $= (10^{-2})^2 = \underline{\underline{10^{-4}}}$

Probability of failure of engine to start and run $= 5 \times 10^{-3}$

Probability of failure of actuator (mean value) $= 7 \times 10^{-4}$

[redacted]

Hence the probability of failure of a single engine to start and run on demand $= 1.65 \times 10^{-4} + 10^{-4} + 5 \times 10^{-3} + 7 \times 10^{-4}$

$\approx \underline{\underline{6 \times 10^{-3}}}$

Note: If a failure probability of say 3×10^{-2} per demand was used for each air motor then this would increase the overall probability of failure to start and run on demand to approximately 7×10^{-3}. This is shown from para 4.9, where a value of 10^{-2} per engine is additionally considered, to have a small effect on the overall system reliability.

4.3 From Fig. 3(b) and Table 3 the probability of failure of the clutch opening circuit is $\underline{1.55 \times 10^{-3}}$ (assuming weekly testing)

and $\underline{6.5 \times 10^{-3}}$ (assuming monthly testing)

Having derived these figures the following observations and qualifications are pertinent and should be considered in using these values in the assessment of the overall system reliability.

Starting Control Circuit

4.4 It will be noted that the calculated probability of failure value for the initiating circuit i.e. 2×10^{-4}, is small compared with the overall value of 6×10^{-3}. Nevertheless its reliability is dependent on several relays, associated contacts and switches, either operating or being in the correct closed stated at the time of a demand. Failure of any single component would result in failure of the start signal to the engine. However it is noted that several are continuously monitored for correct state as they form part of the "IL Ready to Start" indication circuit and thus any open circuit contact would nullify this indicating circuit.

Nevertheless there are certain contact states which are not monitored and it is against these that a failure rate has been allocated. Regular testing will of course reduce the "fractional deadtime" or probability of the system being in the failed state, but following such tests it will be necessary for an operator

[redacted]

to restore the system to its correct starting state e.g. operation of the reset switch and CS/C AUTO/MAN Switch. Again it is noted that these are alarmed to indicate the healthy position but a single contact failure could still inhibit the starting circuit. Thus although the calculated failure probability for this part of the system is low it is an overall recommended principle that the number of series components, events and pre-requisites in any initiating circuit be kept to a minimum. As an example we do not see the virtue in having series contacts in the engine starting circuit from the Trouble Relays - even though they are monitored.

Clutch Opening Circuit

4.5 It is noted that the clutch opening circuit, for an engine failure to start fault, is dependent on energising of the IR relay, which itself is dependent on the success of the whole of the start-up circuit. Thus if an engine start circuit failed the clutch opening circuit and overcrank timer circuit would also fail. The argument for this arrangement could be that in such an event the cranking of the other engine would in fact crank both engines with still some chance of successful starting of both machines and hence nullifying the requirement to disconnect the clutch. However if the engine with the faulty starting circuit failed to start then it would not be de-clutched and would fail the whole unit. This again points to the need for a direct initiating circuit, e.g. why supply the OCT/TDE timer via the IR relay contact?

4.6 Paragraphs 4.1 to 4.8 discuss the reliability considerations and values relevant to operating a single engine and/or clutch. Consider now the reliability of an overall unit (i.e. two engines and a generator) and then of the overall installation of two independent units.

Appendix 3 shows a diagrammatic arrangement of a complete unit and considers firstly the probability of achieving 100%, 50% and zero output for the single unit. It then considers the overall probability of failure to obtain the minimum requirement of 50% output from the complete installation.

[redacted]

4.7 Considering a single set only, it is seen, as would be expected, that the overall failure probability equation contains a term for all components shown in the diagram. From the truth table compiled for the two complete units, the overall system failure is represented by sum of the probabilities of failure for States 6, 8 and 9 and the equation is derived on Page 3 of Appendix 3. Since the failure probability values derived for redundant units (e.g. engines) are low (i.e. $\not< 10^{-2}$) then it is considered reasonable to neglet terms above p^2.

Making this assumption, therefore, the overall probability of failure to achieve 50% output on demand:

$$\bar{P} = (\bar{p}_5 + \bar{p}_6)\,(4\,\bar{p}_7 + \bar{p}_5 + \bar{p}_6)$$

where $\bar{p}_5$ = probability of failure of a generator

$\bar{p}_6$ = probability of failure of a governor

$\bar{p}_7 = \bar{p}_1 = \bar{p}_2$ = probability of failure of an engine to start (including the starting circuit)

4.8 The overall system reliability is thus a function of the governor reliability and engine reliability and this can be understood when it is realised that failure of a governor, which is common to, and hence affects, two associated engines, coupled with failure of a single engine on the other unit, results in system failure.

4.9 It will be observed that the clutch term $\bar{p}_8$ (where $\bar{p}_8 = \bar{p}_3 = \bar{p}_4$) and represents the probability of failure of a clutch to open (including the initiating circuit) is not represented in the final formula - hence implying that it does not influence the overall reliability value. This is in fact the case for low probability values (e.g. $\not< 10^{-2}$) and again will be understood when it is realised that for failure of a single clutch to result in overall system failure, requires it to be coupled with simultaneous failure of two diesel engines. This will be observed from the Appendix, where the symbol for the clutch failure probability $\bar{p}_8$ is associated with a cube term e.g. $4\,\bar{p}_7\,\bar{p}_8\,(\bar{p}_5 + \bar{p}_6)$ and hence neglected as insignificant compared with squared terms.

[redacted]

4.9 From the failure rates in Table 2, Section 3 and paragraph 4.2 the following probabilities of failure are derived:

Test Period	Component			Total System Failure Probability $P = (\bar{p}_5 + \bar{p}_6)(4\,\bar{p}_7 + \bar{p}_5 + \bar{p}_6)$
	Generator $\bar{p}_5$	Governor $\bar{p}_6$	Engine $\bar{p}_7$	
Weekly	7×10^{-4}	7×10^{-3}	6×10^{-3}	2.36×10^{-4}
Monthly	2.9×10^{-3}	3×10^{-2}	8.8×10^{-3}	2.25×10^{-3}

The dominant terms in the overall failure probability value are those for the engine and governor (i.e. $4\,\bar{p}_6\,\bar{p}_7$) and if fixed value of 10^{-2} per engine was used (this being the best substantiated value available in the UKAEA), then the overall failure probability would be 3.7×10^{-4} for weekly testing of the governor and generator and 2.4×10^{-3} for monthly testing.

Use of Computer Programme NOTED

4.10 In addition to the foregoing calculation of overall system reliability the system reliability has also been calculated used the NOTED[7] programme. Although the programme has its real virtue in considering more complex networks and systems nevertheless it is useful in this instance for comparing the difference in overall system reliability for varying values of fault rates for system components. The method of application to the problem is discussed in Appendix 4. Several values were calculated using the NOTED programme and these are as follows:

(a) The standard case considered was using the component fault rates listed in Table 1 and assuming weekly testing for all components except for the clutch opening which was considered as a monthly test. The mean probability of failure is calculated to be 2.53×10^{-4}

[redacted]

b) Using a fault rate of 0.7 for the generator instead of 0.07 with all otherconditions the same, the mean probability of failure is calculated to be 5.59×10^{-4}

c) Using the upper fault rate of 2 faults/year for the governor instead of 0.7 faults/year with all conditions as in the standard case the mean probability of failure is calculated to be 9.8×10^{-4}

d) Using a clutch failure probability of 10^{-1} instead of 10^{-3} and all other conditions the same, the mean probability of failure is calculated to be 2.78×10^{-4}

e) Assuming monthly testing for the standard case instead of weekly tested the mean probability of failure is calculated to be 2×10^{-3}

4.11 The following comments, observations and recommendations arise as a result of the foregoing study

a) The results from NOTED programme confirm those derived by hand calculation. The mean values quoted from the NOTED runs are in fact obtained from the mean of five computer runs. In each case the probability of failure was calculated assuming a demand arose immediately following a test, immediately prior to a test and at intermediate time intervals. This enables the effect of maintenance of various components on the overall system reliability to be studied.

b) From the calculated values obtained the overall reliability is shown to be determined by the reliability of the engines and the governor and generator. The important and yet obvious point to emerge is that redundancy arguments cannot be used for this system of four engines - since they are not truly independent. They have a very strong common link in the governor and its calculated probability of failure of 7×10^{-3} (weekly testing) or 3×10^{-2} (monthly testing) becomes in fact the failure probability of a unit (i.e. two engines).

[redacted]

c) The dependence on the governor means that it must have a demonstrated high reliability to operate on demand i.e. its fractional deadtime due to unrevealed faults must be kept to a minimum. The reduction in reliability for monthly instead of weekly testing is very significant and dictated by the governor failure probability. Hence a frequency of testing of not less than once a week is recommended for both the governor and the engine. The subject of testing is discussed in detail in Section 5 of the report but it is here emphasised that this test frequency for these components be maintained throughout the operating life of the plant.

d) A high reliability requirement is also seen to be essential for engine starting and hence again a regular testing programme is necessary. The calculated failure probability for the starting of each unit is approx 6×10^{-3} of which a value of 1×10^{-4} is associated with the starting circuit. Although this is low it is considered that attention should be given to this part of the system with a view to reducing the number of contacts and interlocks in this circuit. Because of the limited timescale it has not been possible to give this detailed consideration but our experience has been that "failures to start" have generally been associated with the initiating circuits. Our operating experience with auto-start diesel generator units is discussed in Section 3.

e) The clutch assembly whilst having an important influence if considering only the success of a single unit (i.e. two engines and generator) has an insignificant effect on the reliability of the whole installation and a test period of not less than 1 month would be adequate. This negligible effect is clearly demonstrated from the NOTED results where if a high probability of failure for the clutch of 10^{-1} is used the overall probability of system failure is 2.78×10^{-4} compared with 2.53×10^{-4}, when a value of 10^{-3} is used. In the limited time available it has not been possible to examine the Drg E-1208 in detail but it is noted that a "clutch relay CR/S" is

[redacted]

energised if a clutch is open and that it has a contact in the TR/TDE trouble relay circuit. Hence it is assumed that there will be indication if a clutch is ever left in the open position.

f) Paragraphs (d) and (e) above show that a high reliability is also required of the indication and alarm circuits for giving the operator indication that all pre-requisites for start up are satisfied. Position of alarms, type of alarms and dependence on the operator therefore form part of the start up reliability which have not been quantified.

It is recommended that alarm annunciators be located at a manned position. It is noted that the ready to start relays JL, TR/TDE and G will normally be energised - hence an annunciator will be illuminated. Thus a dark panel would indicate a fault. This requires that an operator observes and remedies any suspect faults immediately since any unattended fault represents an inhibiting of start up procedures.

g) It should be noted that because of the limited operation of the system, say two hours per week during testing, it is assumed that the system is not age dependent and that a regular testing and maintenance programme ensures that no deterioration occurs in operating performance.

4.12 The foregoing generally discusses the reliability and engineering requirements of items within the system boundary. The following comments refer to parts of the system outside the defined boundary. They arise because of our lack of knowledge of the design arrangement and system operation but are nevertheless pertinent to the overall system capability and reliability.

4.13 Since 1200 kW of power is required, i.e. 1 complete generator unit or 1 independent engine associated with each generator (2 single engine driven generators) this could necessitate that either (a) the generators must either be connected to 1 bus-bar or (b) that essential loads are duplicated. Condition (a) is understood not to be the case and furthermore it would not be expected - on reliability grounds - to have auto-synchronising since any such facilities would represent an unreliable feature. Hence, it both diesel generator units are successfull it would be assumed

[redacted]

that they would each close on to an independent essential bus-bar, and remain independent in operation.

If, however, only one unit (i.e. 2 engines with 1 generator) is successful and closes on to its busbar - how is the other busbar of the unsuccessful unit supplied - or again are the loads fully duplicated.

Alternatively if a single engine of each generator functions - do they operate independently on separate bus-bars and what determines the essential load item to be started. It is stated that operator action is necessary to connect essential loads, but this could be irreconcileable with the early requirement for essential loads, i.e. < 4 mins and in an emergency we would not normally expect to rely on operator action in less than 15 minutes.

4.14 Summarising, it is desirable for high reliability that the diesel generator units operate independently, and we would not recommend auto-synchronising, or parallel operation; nor would we consider manual starting of loads possible in a short time scale. Hence, with the present design, we assume that each unit is 100% for the reactor, and that if each unit only operates at 50% capacity then loads are 100% duplicated on each essential bus, and operate in a selected running/auto-start stand-by mode.

5. TESTING TO SUBSTANTIATE RELIABILITY PREDUCTIONS

Introduction

5.1 The system has been designed against a target reliability criterion of 0.9999 chance of success per demand at a 95% upper confidence level. The complementary required probability of system failure per demand is 10^{-4} at the same upper confidence level.

The problems of substantiating whether the system is likely to meet this type of reliability criterion fall into two main parts. The first are those dealing with the statistical theory of making estimates from limited sample data and the

second are those associated with the practicalities of the corresponding test procedures.

Theoretical Arguments

5.2 If it were possible to carry out a large number of realistic and independent trials of the complete system under all the true conditions, then this would theoretically be the most direct and realistic solution to the problem. Because of the large number of trials involved in such a theoretical approach it is legitimate to work with the Poisson approximation to binomial sampling distribution. On this basis, it would be necessary to carry out at least 30,000 trials with no overall system failure in order to begin to substantiate a probability of failure per demand of 10^{-4} at a 95% upper confidence level. If failures occurred during the trials the number of trials would rise to at least 47,000 with one failure, to at least 63,000 with two failures and so on according to the Poisson sampling distribution law. It is almost certain, of course, that such an approach could never be adopted because of the practical difficulties of the large number of trials involved and the need to make each trial representative of the true conditions.

5.3 Since the system is designed to achieve a high reliability on the basis of redundancy, the reliability requirement for each of the redundant components in the system is not as high as the overall system. The substantiation of the reliability for each of the individual components may, therefore, be easier if the overall system reliability can then be deduced from this component part reliability knowledge. If the system is considered as a simple two-set redundant arrangement then the required mean probability of failure per demand per set is 10^{-2} provided that the two sets are truly redundant and completely independent. Using similar arguments to those in the previous paragraphs, the substantiation of the figure of 10^{-2} at a 95% upper confidence level for a single set would require at least 300 single-set trials with no failure, 470 trials with one failure and so on. But

[redacted]

if this is done, the question arises as to what confidence can now be ascribed to the estimated figure of 10^{-4} for the complete system. An example may help to illustrate the difficulties. Suppose that the complete system, made up of two identical, independent and redundant sets A and B, has been subjected to 470 trials. During these trials, one failure occurred on set A and one failure occurred on set B but these two failures were not concurrent so that the complete system suffered zero failures in the 470 trials. If the evidence is taken only from the trials on set A or only from the trials on set B, then either of these results yields an estimate of 0.01 failures per demand at the 95% upper confidence level. The corresponding system estimate then looks as though it should be $(0.01)^2 = 0.0001$. If the evidence for an individual set is taken from the combined data associated with both sets A and B, then the test yields two failures in 940 set-trials which gives a figure of about 0.007 failures per demand at 95% confidence and a corresponding estimated system figure of $(0.007)^2 = 0.000049$. If, as another aspect, the individual set performances are ignored and estimates are made from the evidence for the complete system, then the test shows zero failures in 470 trials or a system probability of failure of about 0.006 at a 95% upper confidence level. The three system estimates are totally different and it is abvious, even in this simple example, that combining estimates associated with confidence levels is by no means straightforward. It can be resolved for the simple example just quoted, but if the number of trials alters, the number of failures alter or the system configuration alters then so does the relationship between the confidence estimates. As far as the SRS is aware, there is no simple solution or, in some cases, no solution at present available at all, to the generic problem.

5.4 The approaches so far adopted by SRS in connection with this problem in redundant systems have been to:

a) empirically increase the required confidence levels associated with the tests on the individual element;

[redacted]

b) continue the tests on the individual elements until the sample size of the failures reaches at least 20, or

c) to test the complete system, monitoring all the individual elements, and then make estimates based upon all the available information.

It is felt that some combination of these approaches, particularly with the inclusion of approach (c), is to be preferred. This is commented upon further in the next section.

Practical Approaches

5.5 It has been seen in the previous section that the number of trials needed, even at the component level of a redundant system, may be of the order of several thousand in order to substantiate a system reliability criterion of 0.9999. Nevertheless, this is only a deterrent if a definite substantiation is required in a short period of time from some special test programmes. SRS feel, in this type of situation, that reliability substantiation is a growth process which should start from tests on units leaving the production line, proceed through organised tests of the system during commissioning and early reactor operation and continue throughout the reactor life from the accurate and systematic recording of fault data. In this way, the reliability estimates start with tentative values at lower confience and become firmer at higher confidence levels as the system proceeds through its life. This, in any case, is probably what is required. It is presumed, for instance, that the system reliability criterion of 0.9999 is not required during system or reactor erection and commissioning. Also, during the first phase of reactor operation, the requirement may not need to be as high as 0.9999 since the consequences of failure, based on such things as fission product inventory, may not be as severe. In addition, a lower substantiated reliability in the early years of reactor operation may be capable of being balanced against a higher substantiated value during the latter years of operation.

If the above philosophy is complemented with procedures for rigorously recording and analysing all available information during each operation phase then the case may be demonstrated in a satisfactory, but progressive, fashion.

[redacted]

The idea is to use planned fault recording and analysis as a reliability monitor. If at any state or at any time, the analyses show that the current reliability criterion is not being met then extra tests or different operational procedures can be implemented until the situation is rectified.

5.6 The other important factor is that the practical tests and recording of information should be continually compared with the original theoretical reliability analysis of the system. The practical and theoretical approaches should be used to maximum advantage during all phases by cross-fertilisation of the results of the two approaches.

5.7 It is not possible, in this short survey, to work our any detailed implementation of the approaches generally suggested above, but the following guide lines come immediately to mind:

a) From the theoretical analysis, choose the items of the system which make the most significant contribution towards system unreliability. These could be, for instance, the reliability of the governor and the reliability of an engine starting on demand.

b) For the items selected in (a), plan a pre-installation test programme at the manufacturer's works. For the engines, this could involve a specified number of trial engine starts under specified and controlled conditions. The conditions would need to be carefully specified and any element of accelerated testing would need to be examined most critically. Each system has four engines, so it is possible that one hundred or so engine starts could be examined at this stage. Provided that failures were few or non-existent, this would give an initial reliability estimate of about 1 in 25 failures per demand at 95% confidence. For items like the governor, which in practice will be continually energised, the probability of failure per demand can be evaluated from the mean time to failure (m.t.t.f.) and the periodicity of testing decided upon for the installation. With a weekly test routine, the required m.t.t.f. is going to be of the order of 20,000 hours. Ten governor

units on test for about three months without failure would establish an estimate of about 7,000 hours m.t.t.f. with 95% confidence.

c) From the site installation of the system up to commencement of reactor operation, test the complete system comprehensively at the time intervals that will be dopted during operation, for instance, once per week. The tests should exactly simulate a real demand situation and every item of the system should be monitored and their faults recorded, even if these faults do not lead to complete system failure. The intention, at this stage, being to continue the test procedures on the parts of the system and also to begin tests on the complete system. This latter is important as a first step in substantiating the system's freedom from any common fault modes which could well be the predominant influence on overall system reliability. If this commissioning procedure involving the complete system lasts for, say, a year, then there will have been about a further 200 test starts of individual engines and a further 20,000 hours of governor running times. With complete successes on all occasions the engine reliability estimate could now stand at about 1 in 100 failures per demand at 95% confidence and the governor m.t.t.f. at about 13,000 hours at the same confidence level. At the complete system level, however, the direct test information will only yield an estimate of about 1 in 20 failures per demand at 95% confidence. Hence, the substantiation of system freedom from common faults will have to depend heavily, at this stage, on the results of the engineering appraisal and theoretical analysis of the system.

d) Continue the tests described under (c) during the years of reactor operation. Within one year, however, if the previously suggested programme has been followed, there should be enough data available to substantiate the required reliabilities for the system components such as the engines and governors. Also, any indications of the system's proneness to common faults may now be coming to light. Direct substantiation in this area will never be

[redacted]

possible and the case will have to rest on a combination of test results, theoretical and engineering analysis and strict adherence to appropriate operational and maintenance procedures.

Conclusions

5.8 The substantiation of overall system reliability involves certain theoretical and practical difficulties but it appears perfectly feasible to substantiate reliabilities of the order of those required for some of the main and important components of the system. The reliability information derived for such components may, with care and appropriate safeguards, be used to demonstrate a reasonable case for overall system reliability. System common faults will be the main problem but the chance of these occurring can be minimised by rigorous design appraisals and by maintaining throughout the system life appropriate operational procedures. All tests on which information is based should simulate true conditions and carry appropriate safeguards for not leaving the system in a failed state. A smaller number of realistic tests are considered more worthwhile than a larger number of unrealistic or accelerated tests. The complete case for substantiation, at any state, should preferably be based on a combination of test results, engineering appraisal, operational procedures and theoretical analysis.

6. COMMON MODE FAILURES

6.1 The numerical analysis has considered random fault rates for system components and has used redundancy arguments for duplicated components or sections of the system. It has not quantified the frequency of occurrence of failure of the system due to common mode fault effects. Whilst these are difficult to absolutely quantify it can be stated that where failure probabilities due to random faults are low (e.g. $\not> 10^{-4}$) then common fault probabilities are likely to be of this order. An attempt must therefore be made to highlight possible sources of common mode faults and the following areas are considered.

[redacted]

a) Although there are two starting air motors per engine it is possible that any two of one machine can drive both engines and the generator and thus three would require to fail before the unit would fail to be cranked. However redundancy arguments are only valid provided each motor is independent in all respects. Since it is assumed that each motor of one engine will be operating on the same flywheel starter ring then jamming of one starter pinion could cause failure of both motors and indeed of a complete unit. One could reasonably assume the probability of such a fault (i.e. starter pinion jamming) to be not greater than 10^{-4} per demand and hence for 4 motors the probability of failure of a unit due to this type of fault would be 4×10^{-4}. It is also noted the two air motors for each engine are initiated by means of the same starting circuit. As previously stated 50% of the circuit is monitored for dormant faults but the need for this circuit to be kept to a minimum in terms of number of contacts and relays is again emphasised.

b) The effect of the common mode fault on a governor is already revealed in the analysis and in Section 3.

c) It is noted that the 125V d.c. supplies for the control circuits for both engines 1C and 1D are taken from the same distribution panel 1B. A fault in this supply thus represents a fault mode common to both machines. This common fault frequency will obviously depend on the redundancy and diversity employed in the supplies to the d.c. distribution panel and from the panel to the machine control panels. We would expect these supplies to be physically and electrically segregated.

d) Any local control panels for each generator, housing such auxiliaries as control relays, excitation and A.V.R. controls, should be installed or protected so that they are not exposed to damage due to a fault in a single engine, e.g. fractured C.W. or fuel pipe or mechancial disruption.

[redacted]

e) Operator actions - the operator always represents a common element in any plant and whilst operator error probability may be low, nevertheless, orders of 10^{-2} to 10^{-3} for normal operations and as high as 10^{-1} in emergency situations can be quoted. Therefore operator actions which can have a multiple effect should as far as possible be designed out. We have already examined such events as operator failure to operate the reset switch, failure to set the CSIC switch to AUTO or failure to ensure the clutch is closed and it is noted that these are monitored in the "Ready to Start" indication circuits. Other possible areas for operator error would require more time and a detailed knowledge of system operation and geographical layout. However this shows the need for good presentation of indication and alarms to the operator and the need for his remedying alarm faults immediately rather than ignoring them, perhaps because of continual spurious signals, or leaving them for subsequent attention.

6.2 Whereas para 6.1 discusses common mode faults affecting one unit, there are a number of other items or events which could lead to a systematic failure of the whole system. These are discussed below:

a) <u>Layout</u>

(i) Both generator units are located in the same building separated by a wall with communicating doors. If a fire or explosion starts in either side of the system it is necessary to be satisfied that the walls and doors have the necessary blast and fire proof standards e.g. it would be expected that the communicating doors are normally bolted or latched, that oil sills have been provided etc. S.R.S. cannot judge from Drg. No. M169 - 15 whether the necessary standards have been achieved, but it is apparent that the problem has been recognised by the designers. Appendix 2, Example 3(d) illustrates the principle of how the U.K.A.E.A. would derive the reliability required for the fire/explosion segregation. For this example and the assumptions made (which may not apply at Fort St Vrain) the fire/explosion segregation would need to be of 0.9 reliability.

(ii) The diesel installation could be damaged by missiles, for example, from the disintegration of a main turbo-alternator. The walls around the installation appear to be reasonably thick (about 1 foot). It would be necessary for a judgement to be made of the problem taking into account the layout of the diesels relative to the turbine, Example 3(c), in Appendix 2 illustrates, for the assumptions made, that 0.9 - .99 reliability would be required for this aspect.

(iii) If there is a loss of pressure accident on the reactor then the diesel system can be inhibited by reactor gas (or injected nitrogen) blanketing the air breathing system for the engines. This will be dependent on the layout of the diesel house relative to the reactor. This would need to be examined. Example 3(b) in Appendix 2 indicates, for the assumptions made, that the reliability required for loss of air breathing, needs to be 0.99.

b) Other Common Mode Faults

(i) Each engine has a separate heat exchanger but it is not clear from the information provided whether the cooling water supply is diversified or common to all four engines. This would need to be examined. In any event the possibility arises in either case the cooling water supplies could be affected by freezing conditions, Checks would be required to ensure that pipes are adequately protected against freezing conditions and an operational monitoring might be indicated in very cold weather.

(ii) In a similar manner to b(i) all engines could be affected if the intakes and exhausts became blocked with frozen snow. It is assumed that the design of intake and exhausts have been designed with this possibility in mind and that operational checks would be carried out in bad weather conditions.

(iii) The system could be inhibited if the wrong fuel is supplied. It is noted that on Drg. No. P1-92 that there is only one main fuel tank

[redacted]

for the system. It would be preferable if there were two tanks feeding different day tanks, and which were always filled by different supply tankers. This principle might be achieved by using the oil supply from the auxiliary boiler (shown on P1-92 as a back up).

It would also be expected that each delivery of oil is checked by the station chemist.

(iv) Does the oil supply require heating in low temperature conditions? If so the integrity of the heating system would need to be examined.

(v) All engines could be simultaneously effected if incorrect lubricating oil is used. It is assumed that supervisory checks are made when oil changes are made. In addition it would be considered good practice to stagger engine oil changes as a second precaution.

7. GENERAL DISCUSSION

7.1 The Fort St Vrain Emergency Electrical Supply system has a specified target reliability for success of 0.9999 at the .95 confidence level. Success is defined as the delivery on demand of at least 50% of the total system power and for a time of four minutes. The connection of major emergency loads is said to be manual. The latter point should receive further consideration since it does not appear to be consistent with the 0.9999 standard i.e. it is suggested that manual connection of emergency loads on a short timescale is of 0.3 - 0.9 standard.

7.2 The analysis (Section 4) has shown that the system success probability lies in the range 0.999 - 0.9999 and that the predominant items are the engines and the Woodward Governor.

7.3 The reliability of declutching has been shown not to be a critical item. This is demonstrated clearly in Section 4.10 where the system failure probability of 2.53×10^{-4} with a declutch failure probability of 10^{-3} is compared with a system failure probability of 2.78×10^{-4} with a declutch failure probability of 10^{-1}.

[redacted]

7.4 The reason for the predominance of the Woodward Governor System is that it represents a common mode failure to two engines (see Section 3). Thus in effect, instead of four independent engines whose failure probability is $4\ p^3$, there are only two engines whose failure probability is of p^2 order, since, with the assumptions used for the Woodward Governor, it has a similar failure rate to that of a single engine.

7.5 The importance of weekly testing of the system, in order to approach the target reliability, is demonstrated in Section 4.10. It will be noticed that the system failure probability is 2.53×10^{-4} for the "standard" case with weekly testing compared to a failure probability of 2×10^{-3} for the same case but with monthly testing.

7.6 Section 5 argues that complete substantiation of the system by preoperational testing is not really feasible. It is suggested that substantiation, at any stage, should preferably be based on a combination of tests results, engineering appraisal, operational procedures and theoretical analysis.

7.7 In view of the importance of the governor system, preoperational testing to establish the "failure" rate of the equipment is likely to give the greatest dividend; this should preferably be done with a few units. In addition more specific information might be obtained from Messrs Woodward. Additionally a more detailed analysis of the governor system may be undertaken. The figures used in the analysis, 0.2 to 2 failures p.a., are generic figures for similar electronic equipment, and have not been arrived at by a specific analysis of the Woodward Governor.

7.8 The analysis has concentrated on the reliability of system starting. This is due to the fact that running faults would be of low order, compared to 10^{-4}, for a running time of four minutes. If longer running times e.g. 1 day were required, then this aspect would need to be reconsidered. In a similar manner if a longer time were available to connect loads, then the system reliability could improve due to the possibility of operator action.

[redacted]

7.9 Although the reliability of declutching has been shown to be minimal (7.3) it is important that the clutch be in the "engaged" position in the dormant or starting state. The same applies to the position of the remote - manual switch. The position of alarms for these and similar items and dependence on the operator form part of the start up reliability which have not been quantified. It would however be recommended that the alarm annunciators be located at a continuously manned position.

7.10 Although weekly testing is suggested (7.5) this can bring its own dangers. For example, frequent testing of the clutch gives a greater chance of operator error in leaving the clutch disengaged. Therefore in view of the minimal importance of declutching (7.3) monthly or even longer test intervals are indicated for the clutch.

7.11 Common mode faults have been discussed in Section 6. Attention is drawn in particular to the single fuel tank which supplies fuel oil to the complete system. It is suggested that this can be improved by use of the auxiliary boiler supply for one half of the system and that this and the diesel system tank are filled by different tanker deliveries. Further investigation should also be given to the integrity and reliability of the fuel supply arrangements to each pair of engines (para. 3.15).

7.12 In carrying out the analysis the assumption has been made that all engines and system components are available at the time of a demand i.e. during reactor power operation. However, it can be shown that for planned outage of say, one engine week per year, the mean probability of failure over the year is relatively unaffected albeit during that period of one week the overall system reliability may be significantly affected. Hence any prolonged planned outages would require a re-examination of the overall reliability.

7.13 The U.K.A.E.A. frequency/risk approach of defining system reliabilities is outlined in Appendix 2 and this method might be used to, inter alia, define targets for the reliability of the common mode faults e.g. fire segregation etc.

7.14 The Fort St Vrain System has been compared (Appendix 5) with the Seqhohah P.W.R. System. This shows that the two systems are of the same order i.e. 10^{-4} standard, provided the Woodward Governor system has only 0.7 faults/year or less. If, however, the Woodward Governor is at the upper level considered, i.e. 2 faults/year then the Fort St Vrain system would be a factor 10 worse than Sequohah. This again emphasises the importance of the governor in the overall reliability of the Fort St Vrain system.

[redacted]

8. CONCLUSIONS AND RECOMMENDATIONS

1. The system success probability is in the range 0.999 - 0.9999 (4.15).

2. O.R.N.L. should reconsider the statement (2.1 h) that starting of major emergency loads is manual. This does not appear to be consistant with 0.9999 reliability on a short timescale.

3. Declutching reliability is of minimum importance in overall system reliability (4.10).

4. The predominant item in system reliability is the Woodward governor. It is important to establish high reliability i.e. better than 0.7 faults/year if the target reliability is to be achieved (4.10, 5, 7.7).

5. Weekly testing of the system is indicated with the exception of the declutching operation which should be monthly (4.10, 7.5, 7.10).

6. Substantiation of the system, at any stage, should preferably be based on a combination of test results, engineering appraisal, operational procedure and theoretical analysis (5.8).

7. If system operation is required for longer than four minutes e.g. 1 day, further consideration will be required for normal running faults (7.8).

8. If a longer time interval than four minutes is available to connect loads, then the system reliability could improve (7.8).

9. The fuel supply arrangement for each pair of engines should be further examined to demonstrate the low probability of a common mode fault due to fuel failure. Consideration should also be given to use of the auxiliary boiler system to feed one half of the system and the diesel tank for the other half. The tanks should be filled by separate tanker deliveries (6.2(b)iii).

10. The principle of having series contacts in the engine starting circuit from the Trouble Relays, even though monitored, is questioned (4.4).

11. It is not understood why the supply to the OCT/TDE timer is via the IR relay contact (4.5).

12. The starting circuit should be reviewed with a view to reducing the number of contacts and interlocks(4.11d)

[redacted]

13. Alarm annunciators should be located at a continuously manned position (4.11f).

14. Although outside the system boundary, clarification is needed of system operation particularly when two units are paralleled (4.14).

15. Attention is drawn to the possibility of common mode failures, some outside the system boundary. These include:

a) 125V d.c. supplies for control circuits (6.1(c))

b) local control panels (6.1(d))

c) Operator actions (6.1(e))

d) Fire segregation (6.2(a)i)

e) Missile damage (6.2(a)ii)

f) Loss of Air Breathing (6.2(a)iii)

g) Low temperature effects (6.2(b) i & ii & iv)

h) Checking of lubricating oil (6(b)v)

IN CONFIDENCE

APPENDIX 1

REFERENCES

1. Letter D. W. Cardwell/A. E. Green dated 6 December 1971
2. Letter Paul Rubel/A. E. Green dated 13 December 1971
3. Contract Letter A. J. Bourne/D. W. Cardwell dated 5 January 1972
   Ref. SRS/AM/0042
4. List of Drawings and Pamphlets provided by O.R.N.L.
   (a) Fig 1 - Engine Generator System
   (b) Fig 2 - Engine Generator Sub-System
   (c) Dwg No 683982 - Standby Generator
   (d) Dwg No M169-14 - Sectional Views
   (e) Dwg No M169-5 - Clutch Air System
   (f) Dwg No P1-92 - Oil and Air Systems
   (g) TWIN DISC PAMPHLET - Power Take Off Model SP321-P-CO
   (h) Dwg No M169-15 - Plan View of Installation
   (i) Dwg. No 1208 - Starting and Trouble Circuits
   (j) Woodward Bulletin 82517-B. Type 2301 Load and Speed Sensing Control
   (k) Woodward Bulletin 82510B - Magnetic Pickup
   (l) Woodward Bulletin 82505A - E.G. - 3P Actuator
   (m) Woodward Spec 82516A - E.G. 3P Actuator
   (n) Woodward Spec 82518 - Electric Control Systems
5. Telex Paul Rubel/E. A. White dated 27 December 1971 giving start up sequence etc.
6. Siting Criteria - A New Approach
   S.M. - 89/34 I.A.E.A. Symposium 1967 by F. R. Farmer
7. U.K.A.E.A. A.H.S.B.(S)R153 - The Programme NOTED by E. R. Woodcock

APPENDIX 2

Comments on the A.E.A. Method of Defining Reliability Targets for Safety Equipment

1. The stated reliability requirement for the Forst St Vrain guaranteed electrical supply system is that: it should start on demand and deliver at least 50% of the total combined capacity for 4 minutes with 0.9999 success and with 95% confidence. This figure would appear to apply to all fault conditions. In the A.E.A. approach there would be a different reliability requirement for each initiating fault condition. This approach is outlined below and may assist in giving a perspective of the general engineering comments giving elsewhere in the report and a general insight of the A.E.A. frequency/risk approach.

2. The frequency/risk approach to reactor safety was first suggested by F. R. Farmer in Ref. 6. The current A.E.A. safety evaluation of reactors uses a curve with a slope of -1 as shown in Fig. 4. Thus any combination of reactor incident which results in a release of 1000 curies of I_{131} would be allowed with a frequency of 10^{-3} pa, 10^{6} curies I_{131} at a frequency of 10^{-6} pa etc.

3. The following examples which are related to a guaranteed electrical system illustrate the practical implementation.

(a) (i) Initiating Faults

Complete loss of grid connection to site - frequency 10^{-1} pa.

(ii) Failure of reactor to run through and maintain "house" load to vital heat removal equipment, e.g. emergency circulator power and emergency feed pump power. Failure rate 10^{-1} per demand.

(iii) If emergency circulators or feed is not restored core melts, pressure circuit is breached; external fission product release 10^{7} curies I_{131}. Overall frequency allowed from Fig. 4 = 10^{-7} pa.

[redacted]

(iv) Failure rate required for guaranteed supply system is 10^{-5} per demand.

ie $\underline{10^{-1} \times 10^{-1} \times 10^{-5} = 10^{-7} \text{ pa as at (iii)}}$

This would demand two diverse systems each of about 10^{-3} failure probability standard. This would be provided by, for example:

(a) A diesel system and (b) a steam turbine system driven from auxiliary boilers.

(b) (i) Initiating Fault

Significant Loss of Pressure Fault and frequency 10^{-3} pa. Immediate Reactor Trip required.

(ii) Because Reactor is tripped no run through is possible. Incoming electrical supplies lost due to grid instability at frequency of 10^{-2} per reactor trip.

(iii) If emergency circulators or feed is not restored, core melts and external fission product release is 10^{7} curies. Overall frequency allowed from Fig. 4 = 10^{-7} pa.

(iv) Failure Rate required for guaranteed supply system = 10^{-2} per demand, ie $10^{-3} \times 10^{-2} \times 10^{-2} = 10^{-7}$ pa as at (iii). The failure rate of 10^{-2} per demand would be met by either of the two systems required for fault (a). The two systems at (a) would be located on either side of the reactor thus eliminating the risk of both systems being simultaneously affected by the depressurisation incident, eg reactor gas or injected gas blanketing the air supply to the diesels and auxiliary boiler unit.

(c) (i) Initiating Fault

Disintegration of Main Turbo-Alternator Frequency 10^{-3} - 10^{-4} pa.

IN[redacted]

(ii) Because Turbine has disintegrated, run through to house load not possible.

Incoming electrical supplies lost due to grid instability at frequency of 10^{-2} per reactor trip.

(iii) If emergency circulators or feed is not restored core melts and external fission product release is 10^{7} curies. Overall frequency allowed from Fig. 4 = 10^{-7} pa.

(iv) Failure rate required for guaranteed supply system = 10^{-1} 10^{-2} per demand, ie

$10^{-3} - 10^{-4} \times 10^{-2} \times 10^{-2} - 10^{-1} = 10^{-7}$ pa.

The failure rate of $10^{-1} - 10^{-2}$ pa would be met by either of the two systems required for fault (a). The different location of the two systems would reduce to a minimum the chance of both systems being simultaneously affected by missiles from the disintegrating turbine. This would need to be examined from the overall layout and the protection afforded to each system by the buildings, probable flight path and size of missiles etc.

(d) (i) Initiating Incident. Fire in Emergency Diesel Generating System completely invalidating this particular system frequency 10^{-2} pa.

(ii) Unconnected failure of incoming grid supplies for about 8 hours frequency 10^{-1} pa. Total deadtime 10^{-4}.

(iii) If emergency circulators or feed is not restored core melts external fission products release 10^{7} curies.

Overall frequency required from Fig. 4 = 10^{-7} pa.

(iv) Failure rate required from guaranteed supply system = 10^{-1} per demand, ie

$10^{-2} \times 10^{-4} \times 10^{-1} = 10^{-7}$ pa as at (iii).

This would be met by the auxiliary boiler steam turbine system.

[redacted]

(v) Note that the above case is for a "hypothetical" reactor. The following argument might be applied to Fort St Vrain.

(a) Initiating Incident. Fire or explosion in <u>one half</u> of the diesel complex, frequency 10^{-2} pa.

(b) Unconnected failure of incoming grid supplies for about 8 hours. Frequency 10^{-1} pa. Total deadtime 10^{-4}.

(c) If feed is not restored etc core "melts", vessel fails; external fission product release 10^{7} curies I_{131}. Overall frequency required from Fig. 4 = 10^{-7} pa.

(d) Failure rate required from other half of diesel system, including fire and explosion separation = 10^{-1} per demand ie $10^{-2} \times 10^{-4} \times 10^{-1} = 10^{-7}$.

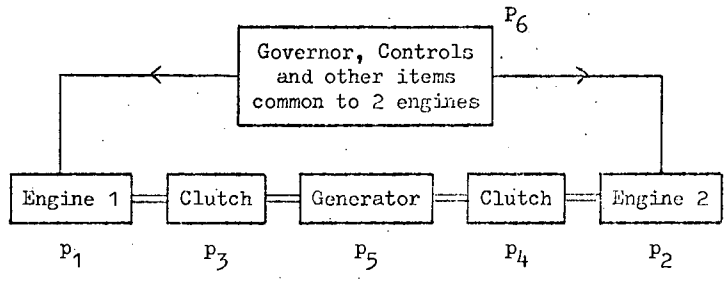
4. The above examples have been simplified to illustrate the approach. The main point to be noted is that the required failure probability for the emergency supply range from 10^{-1} per demand to 10^{-5} per demand to cover the range of the different types of initiating faults. Also that in some cases the failure probability needs to cover missile and fire damage, eg it is highly likely that the missile and fire separation of the Fort St Vrain diesel system is of 10^{-1} failure probability standard.

[redacted]

APPENDIX 3

Mathematical Model of the Fort St Vrain Emergency Electrical Supply System

Main Elements of a Typical 2-engine Set



Probabilities

p_1 = prob. of Engine 1 (+ associated starting gear and auxiliaries) being successful

p_2 = prob. of Engine 2 (+ associated starting gear and auxiliaries) being successful

p_3 = prob. of Clutch for Engine 1 successfully disengaging when Engine 1 fails

p_4 = prob. of Clutch for Engine 2 successfully disengaging when Engine 2 fails

p_5 = prob. of Generator and auxiliaries being successful

p_6 = prob. of Governor and auxiliaries being successful

States of Set

The Set may be assumed to have 3 possible states as a result of a demand, namely 100% output, 50% output and 0% output.

The probabilities associated with those states are:

State (% Output)	Probability
100%	$p_5\, p_6\, p_1\, p_2$
50%	$p_5\, p_6\, (\bar{p}_1\, p_2\, p_3 + p_1\, \bar{p}_2\, p_4)$
0%	$p_5\, p_6\, (\bar{p}_1\, p_2\, \bar{p}_3 + p_1\, \bar{p}_2\, \bar{p}_4 + \bar{p}_1\, \bar{p}_2)$ $+ \bar{p}_5\, p_6 + p_5\, \bar{p}_6 + \bar{p}_5\, \bar{p}_6$.

[redacted]

Only the 50% and 0% states can lead to an overall system failure. Assuming that the success probability terms can be taken as approximately unity, those two state probabilities become:

$$50\% \simeq 2\,\bar{p}_7$$

$$0\% \simeq 2\,\bar{p}_7\,\bar{p}_8 + \bar{p}_7^{\,2} + \bar{p}_5 + \bar{p}_6 + \bar{p}_5\,\bar{p}_6$$

where $p_7 = p_1 = p_2$ numerically

$p_8 = p_3 = p_4$ numerically

States for the Second Identical Set

If q is used to denote the equivalent probabilities for the second set, then the possible failure states are give by:

State		Probability
50%	$\simeq$	$2\,\bar{q}_7$
0%	$\simeq$	$2\,\bar{q}_7\,\bar{q}_8 + \bar{q}_7^{\,2} + \bar{q}_5 + \bar{q}_6 + \bar{q}_5\,\bar{q}_6$

States for 2 Sets taken together

(W = System O.K., F = System Failed)

State No	Set 1 State	Set 2 State	System State	Probability
1	100%	100%	W	
2	100%	50%	W	
3	100%	0%	W	
4	50%	100%	W	
5	50%	50%	W	
6	50%	0%	F	$\simeq 2\,\bar{p}_7\,(2\,\bar{q}_7\,\bar{q}_8 + \bar{q}_7^{\,2} + \bar{q}_5 + \bar{q}_6 + \bar{q}_5\,\bar{q}_6)$
7	0%	100%	W	
8	0%	50%	F	$\simeq 2\,\bar{q}_7\,(2\,\bar{p}_7\,\bar{p}_8 + \bar{p}_7^{\,2} + \bar{p}_5 + \bar{p}_6 + \bar{p}_5\,\bar{p}_6)$
9	0%	0%	F	$\simeq (2\,\bar{p}_7\,\bar{p}_8 + \bar{p}_7^{\,2} + \bar{p}_5 + \bar{p}_6 + \bar{p}_5\,\bar{p}_6)$ $(2\,\bar{q}_7\,\bar{q}_8 + \bar{q}_7^{\,2} + \bar{q}_5 + \bar{q}_6 + \bar{q}_5\,\bar{q}_6)$

Letting the q's be numerically equal to the p's, the overall system failure probability, $\bar{P}$, becomes:

[redacted]

$$\begin{aligned}\underline{\bar{P}} = {} & 4\,\bar{p}_7\,(\bar{p}_5 + \bar{p}_6) + 4\,\bar{p}_7\,\bar{p}_5\,\bar{p}_6 + 8\,\bar{p}_7^{\,2}\,\bar{p}_8 + 4\,\bar{p}_7^{\,3} \\ & + 4\,\bar{p}_7^{\,2}\,\bar{p}_8^{\,2} + 4\,\bar{p}_7^{\,3}\,\bar{p}_8 + 4\,\bar{p}_7\,\bar{p}_8\,(\bar{p}_5 + \bar{p}_6) + 4\,\bar{p}_7\,\bar{p}_8\,\bar{p}_5\,\bar{p}_6 \\ & + 2\,\bar{p}_7^{\,2}\,(\bar{p}_5 + \bar{p}_6) + 2\,\bar{p}_7^{\,2}\,\bar{p}_5\,\bar{p}_6 \\ & + 2\,\bar{p}_5\,\bar{p}_6 + \bar{p}_5^{\,2} + \bar{p}_6^{\,2} \\ & + 2\,\bar{p}_5^{\,2}\,\bar{p}_6 + 2\,\bar{p}_5\,\bar{p}_6^{\,2} + \bar{p}_5^{\,2}\bar{p}_6^{\,2} + \bar{p}_7^{\,4}\end{aligned}$$

or, neglecting terms above p^3

$$\begin{aligned}\underline{\bar{P}} = {} & 4\,\bar{p}_7\,(\bar{p}_5 + \bar{p}_6) + 2\,\bar{p}_5\,\bar{p}_6 + \bar{p}_5^{\,2} + \bar{p}_6^{\,2} \\ & + 4\,\bar{p}_7\,\bar{p}_5\,\bar{p}_6 + 8\,\bar{p}_7^{\,2}\,\bar{p}_8 + 4\,\bar{p}_7^{\,3} + 4\,\bar{p}_7\,\bar{p}_8\,(\bar{p}_5 + \bar{p}_6) \\ & + 2\,\bar{p}_7^{\,2}\,(\bar{p}_5 + \bar{p}_6) + 2\,\bar{p}_5^{\,2}\,\bar{p}_6 + 2\,\bar{p}_5\,\bar{p}_6^{\,2}\end{aligned}$$

or, neglecting terms above p^2

$$\begin{aligned}\underline{\bar{P}} &= 4\,\bar{p}_7\,(\bar{p}_5 + \bar{p}_6) + 2\,\bar{p}_5\,\bar{p}_6 + \bar{p}_5^{\,2} + \bar{p}_6^{\,2} \\ &= 4\,\bar{p}_7\,(\bar{p}_5 + \bar{p}_6) + (\bar{p}_5 + \bar{p}_6)^2 \\ &= (\bar{p}_5 + \bar{p}_6)\,(4\,\bar{p}_7 + \bar{p}_5 + \bar{p}_6)\end{aligned}$$

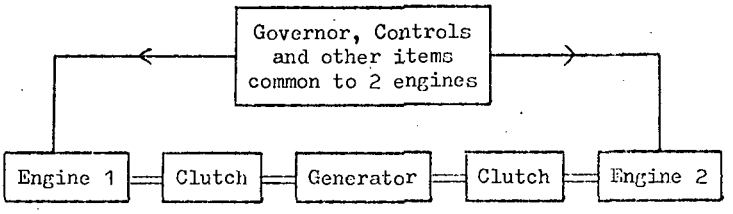
[redacted]

APPENDIX 4

NOTED Model of Fort St Vrain

Emergency Electrical Supply System

Main Element of a Typical Set



Engine 1 and Engine 2 each include the Actuator, Engine Starting Circuit and the Engine itself. The clutch includes the control circuit telling the clutch to open and the clutch itself.

For convenience define the following events:

GOV: Governor, Controls and other items common to both engines work successfully

GEN: Generator and other items common to generator work successfully

ENGINE 1: Engine 1 starting circuit, its Actuator and Diesel Engine 1 work successfully

ENGINE 2: Engine 2 starting circuit, its Actuator and Diesel Engine 2 work successfully

CLUTCH 1: Clutch associated with engine 1 and its associated opening circuit disengages successfully

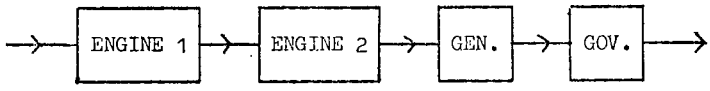
CLUTCH 2: Similarly with clutch associated with engine 2.

There are two such sets.

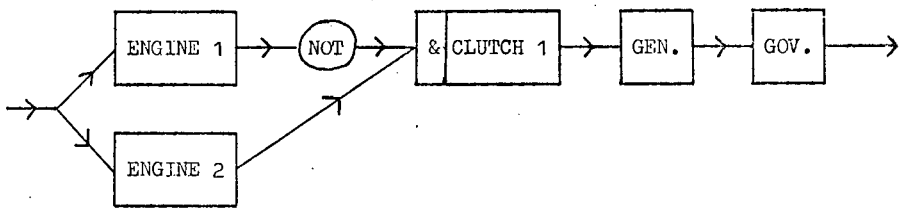
System success is defined to be 100% output on one (or both) sets, or 50% output on both sets.

[redacted]

(a) For 100% output on a set, we have the following success flow diagram:

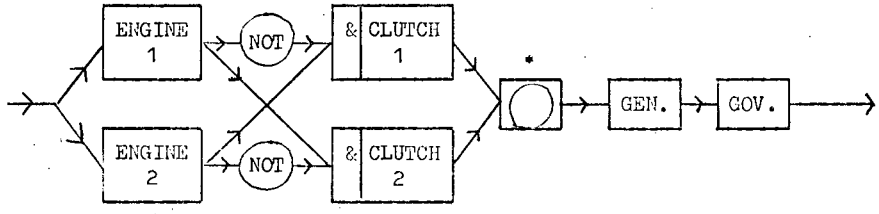


(b) For exactly 50% output on a set we require that exactly one engine fails and is successfully declutched. Assuming Engine 1 fails, we have the following success flow diagram:



Assuming engine 2 fails we have a similar success flow diagram except that 1 and 2 are interchanged.

(c) We can combine these two cases into one flow diagram where we use the 'EXCLUSIVE OR'* Box to indicate that the two cases are mutually exclusive.

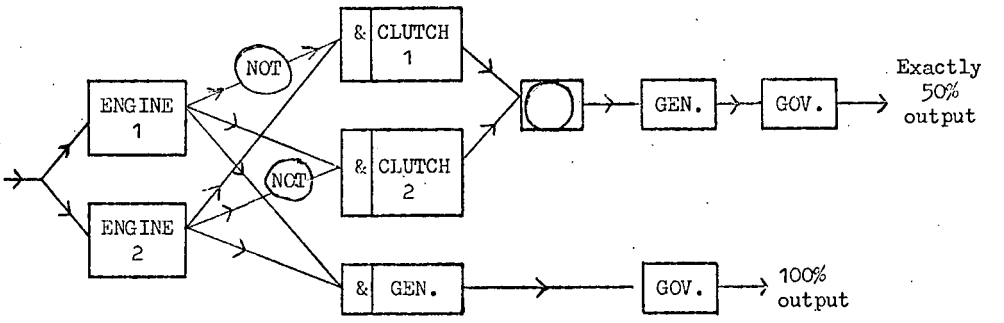


This gives us the probability of failure to get exactly 50% output from one set.

(d) The two flow diagrams in (a) and (c) may be combined to give the following flow diagram:

*Exclusive 'OR'

[redacted]



This flow diagram can be used to calculate the probabilities of failure of:

i) 100% output - We let this be event A

ii) Exactly 50% output for the one set - We let this be event B

(e) There are two such sets:

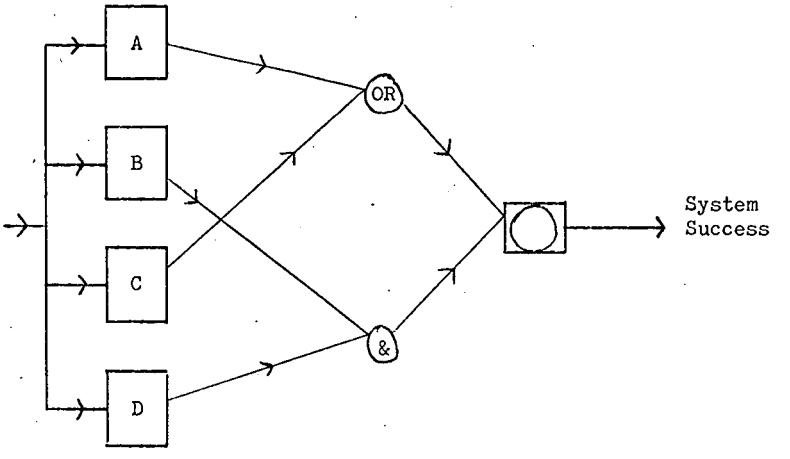
Let event C be 100% output from second set, and event D be exactly 50% output from second set.

Now system success is satisfied if one of the following occur:

Event A or Event C

or Event B and Event D

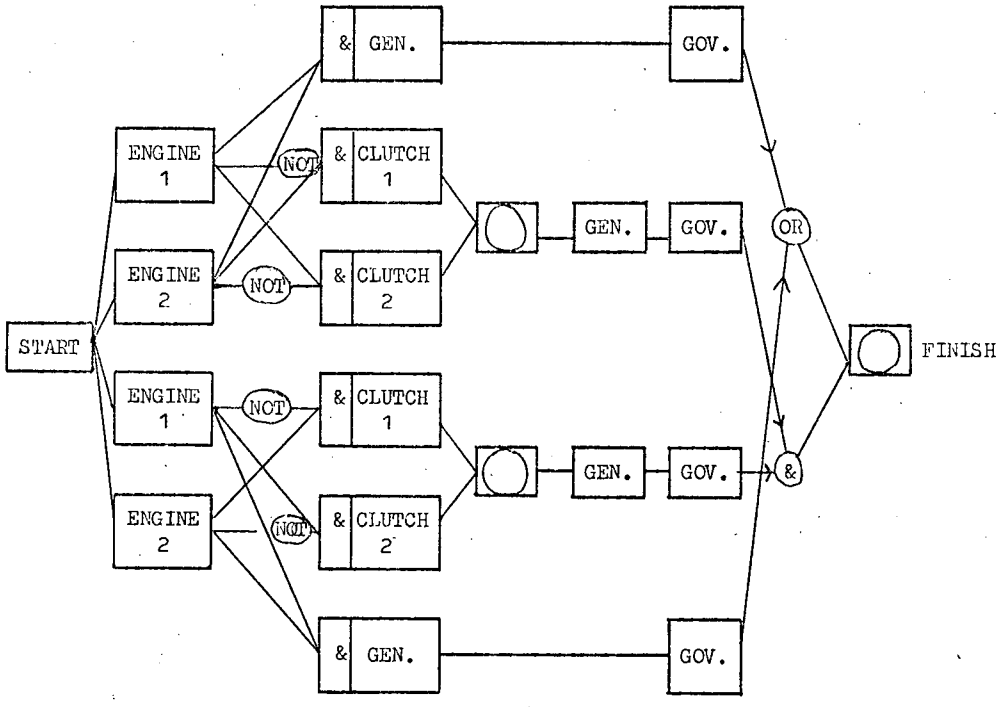
These two possibilities are mutually exclusive, and we can calculate system success from the following success flow diagram:



[redacted]

where again we have the 'EXCLUSIVE OR' box to indicate that the two possibilities are mutually exclusive.

Thus we can now construct the success flow diagram appropriate to a NOTED run by combining the diagrams in (d) and (e).



[redacted]

APPENDIX 5

Simple Comparison between the Fort St Vrain H.T.R. and Sequohah P.W.R. Emergency Electrical Supply Systems

1. In reference 2 it is stated that "the system represents a departure from the usual reactor emergency power supply safety requirement (U.S.) that a single/ engine generator unit be capable of handling the largest transient demand imposed by the vital loads." It is therefore pertinent to compare the Fort St Vrain System with a "standard" system.

2. The S.R.S. are not completely familiar with the detailed implementation of the "General Design Criteria for Nuclear Power Plants" but have to hand the P.S.A.R. for the Sequohah P.W.R. plant. In this report it is stated under 8.1-2 that "the plant has three emergency diesel generators, any two of which are capable of supplying sufficient power for the operation of necessary engineered safety features and protection systems required to avoid undue risk to public health and safety", i.e. there are three 50% generators each driven by a 50% diesel engine.

Thus the Sequohah system is a two from three system and the failure probability for less than two engines is approximately $3\,\bar{p}^2$ where $\bar{p}$ is the failure probability of the starting circuit + starting motors + governor + engine + generator. Thus by evaluating the above using the same values for the various items (where appropriate) as those used for Fort St Vrain a direct comparison can be made between the two systems for random failures.

3. From Section 4.2 of the main report the failure probability of a single engine to run and start is given a 6×10^{-3} for weekly testing. The corresponding figure for the generator is 7×10^{-4}

$\therefore\ \bar{p}$ for Sequohah $= 6.7 \times 10^{-3}$

[redacted]

hence the failure probability for Sequohah $= 3\,\bar{p}^2 = 3 \times (6.7 \times 10^{-3})^2$

$= 1.34 \times 10^{-4}$

For the Fort St Vrain System (Section 4.9) of the main report the total system failure probability for weekly testing is $\underline{2.5 \times 10^{-4}}$. This is for the same values for engine starting and the generator as above and a figure of 7×10^{-3} for the governor system.

If the upper fractional deadtime of 2×10^{-2} is used for the governor (Section 3.8 main report) then the total system failure probability for Fort St Vrain is $\underline{9.8 \times 10^{-4}}$.

The main point to be noted from the above is the important difference the governor makes between the reliability of the two systems. If a figure of 0.7 faults per year can be substantiated for the Woodward Governor then the Fort St Vrain System is of the same order of reliability as the "standard" system i.e. approximately 10^{-4} failure probability. On the other hand if the fault rate for the Woodward Governor System is 2 faults/year, then the Fort St Vrain System would be approximately a factor 10 worse than the "standard" system i.e. approximately 10^{-3} failure probability. This emphasises the point made in the main report of the importance of establishing a low failure probability for the Woodward Governor, both in an absolute sense and also in comparison with the "standard" system, e.g. Sequohah.

[redacted]

TABLE 1

Component Failure Rates

Components	Fault rate (Faults/yr)
Generator	0.07
Relay (simple type i.e. coil + contacts)	0.005
Time Delay Relay	0.1
Coil (Relay - open and short circuit)	0.003
Contact (per pair - open and short circuit)	0.002
Solenoid Valve	0.05
Air Motor (Prob. of failure per demand)	10^{-2} to 10^{-3}
Clutch (Prob. of failure per demand)	10^{-3}
Diesel Engine (Prob. of failure to start)	5×10^{-3}

Notes on Failure Rates

The values have been derived from information in the data bank and in some instances from that obtained from assessments on specific equipments. These are mean values and there are obviously upper and lower values. Furthermore, although they are not specific to the components in use, in this exercise they represent adequate information to enable the order of reliability associated with the various parts of the system to be determined.

[redacted]

TABLE 2

Engine Starting Circuit

Component	Fault	Fault Rate (Faults/year)
Aux. Lockout Relay	Normally energised and is de-energised to operate. Hence any O.C. & S.C. fault would be fail safe.	
86 RT Contact	Fails to close	0.001
SR1 to SR5 Contacts	Failure of these to be closed would be alarmed via the "IL ready to start circuit"	
Reset Switch	Failure to be at reset position would be alarmed via the "IL ready to start circuit"	
CS/CO Contact	Failure to close. It would seem this has to be energised closed. Hence allow relay fault rate plus contacts.	0.004
286 DGIB L.O. Relay	Failure of contacts to be in closed position	0.001
CS/C Switch	Failure to be at 'auto' position. This would be alarmed via the "IL ready to start circuit"	
STOP Button	Failure to make contact	0.001
Locked isolator button	Contact failure only	0.001
IR relay	Failure to energise and operate	0.005
IR contact	Failure to close	0.001
AR contacts	Failure to be in closed position	0.002
	Total unrevealed final danger faults in start circuit	0.016
Solenoid Valve for Air Motor Supply	Failure to energise and operate	0.05

[redacted]

TABLE 3

Clutch Opening Circuit

Component	Fault	Fault Rate (Faults/year)
OCT/TDE Timer	Failure of Timer to energise and operate	0.1
OCT/TDE Timer Contact	Failure of contact to close after 45 secs.	0.001
SR3 Overcrank Failure to start relay	Failure to energise, e.g. due to short circuit or open circuit	0.003
SR3 Contact	Failure to close	0.001
Clutch Solenoid C.S.	Failure to energise and operate	0.05
	Total fault rate for inhibiting clutch operation	0.155

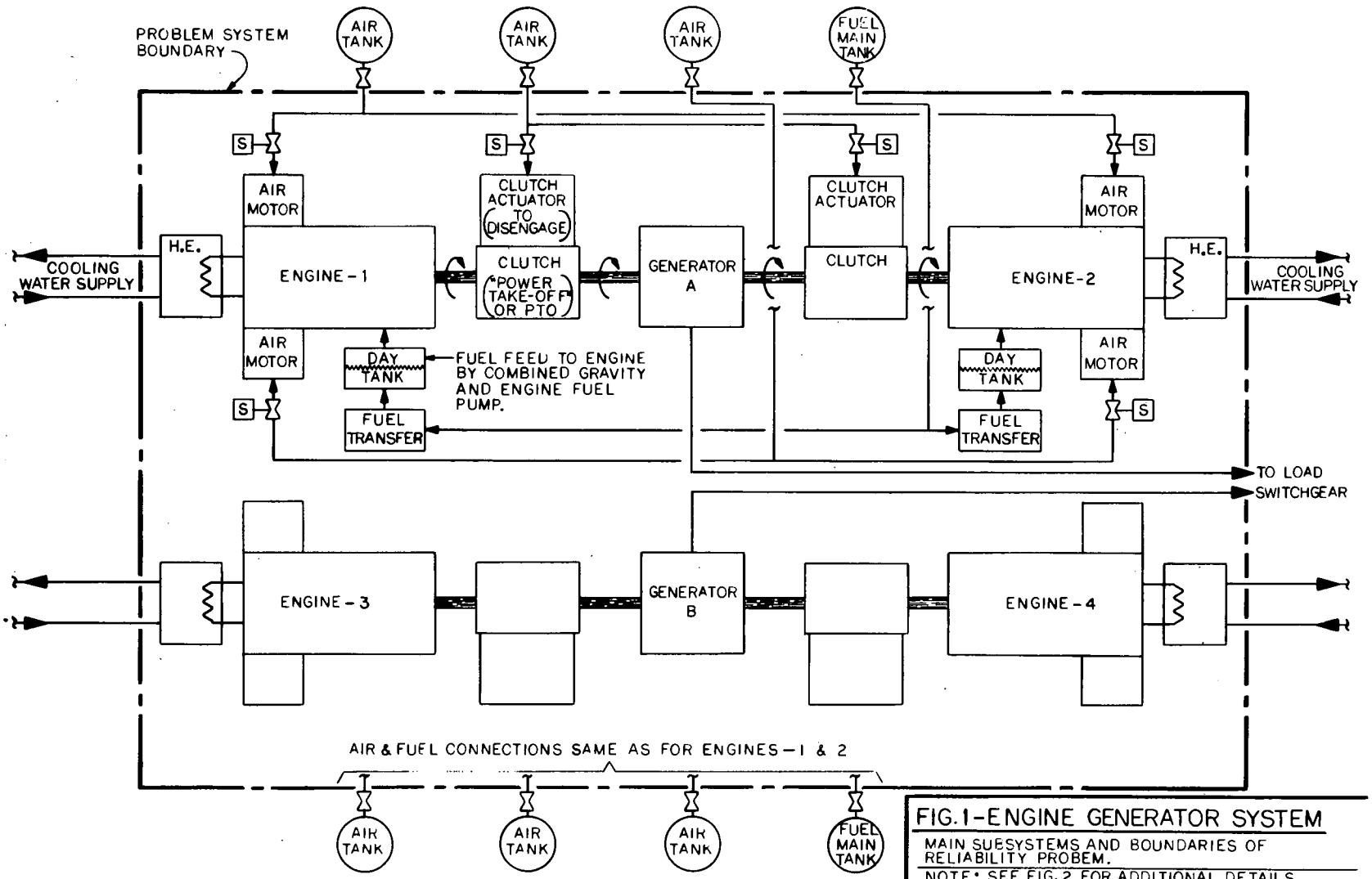
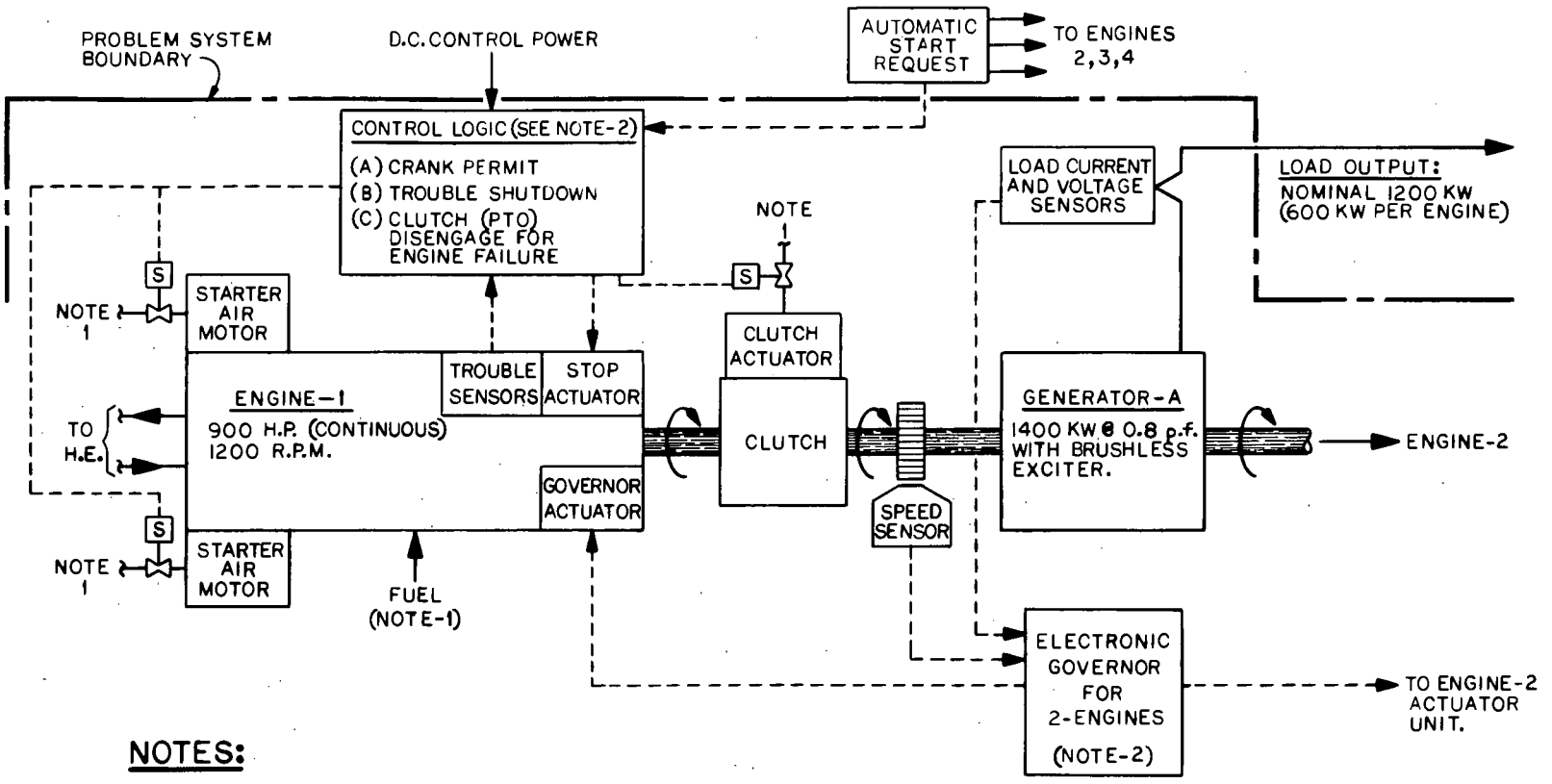


FIG. 1 - ENGINE GENERATOR SYSTEM

MAIN SUBSYSTEMS AND BOUNDARIES OF RELIABILITY PROBEM.

NOTE: SEE FIG. 2 FOR ADDITIONAL DETAILS.



NOTES:

1. SEE FIG. 1 FOR OVERALL SYSTEM AND PROBLEM BOUDARIES.
2. SEE DWG. 1208 (SARGENT & LUNDY) FOR CONTROL SCHEMATICS.
3. ADDITIONAL LAYOUTS AND DETAILS GIVEN AS FOLLOWS:
   (A)- CLUTCH CONTROL PNEUMATIC SYSTEM: DWG. M169-5 (HAWTHORNE).
   (B)- ENGINE PLAN AND SECTIONAL VIEWS: DWGS. M169-14 & 15 (HAWTHORNE).
   (C)- PROCESS FLOW SHEET: DWG. PI-92 (SARGENT & LUNDY).
   (D)- ENGINE GENERATOR ELEVATION: DWG. 683982 (HAWTHORNE).
   (E)- CLUTCH INSTRUCTIONS: TWIN DISC CO. LITERATURE.
   (F)- GOVERNOR INSTRUCTIONS: WOODWARD GOVERNOR CO. LITERATURE.

FIG. 2-ENGINE GENERATOR SUBSYSTEMS

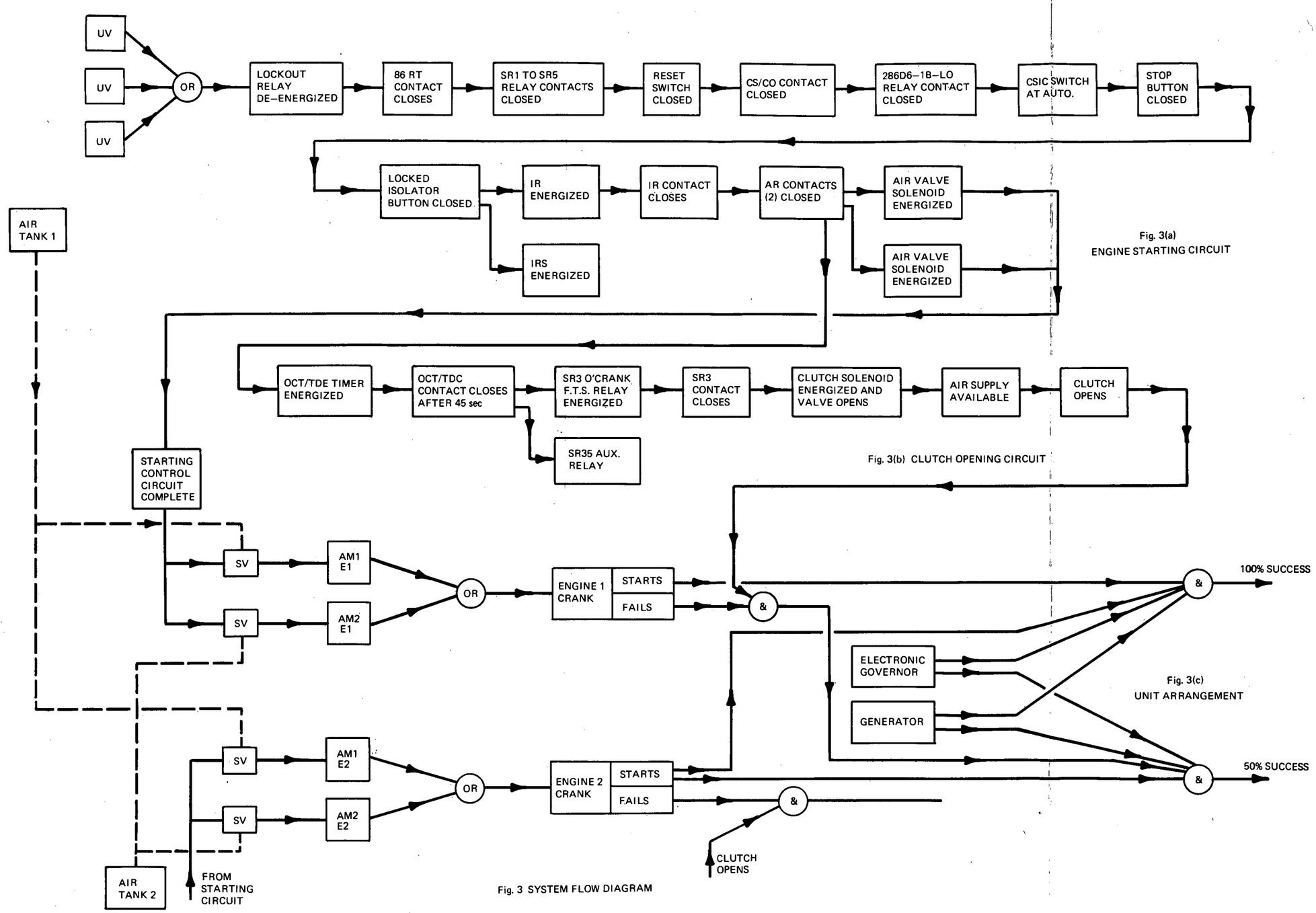


Fig. 3(a) ENGINE STARTING CIRCUIT

Fig. 3(b) CLUTCH OPENING CIRCUIT

Fig. 3(c) UNIT ARRANGEMENT

Fig. 3 SYSTEM FLOW DIAGRAM

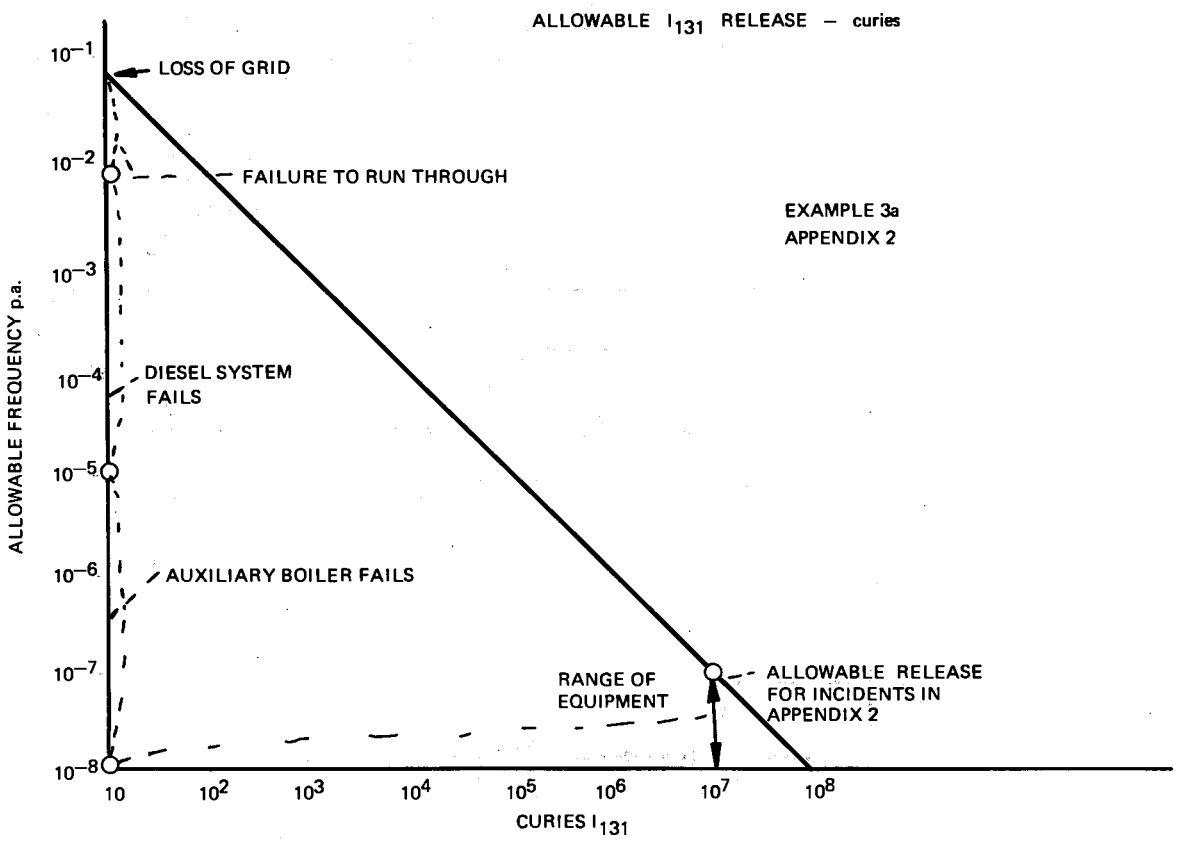

ALLOWABLE I_{131} RELEASE – curies
LOSS OF GRID
FAILURE TO RUN THROUGH
EXAMPLE 3a
APPENDIX 2
DIESEL SYSTEM FAILS
AUXILIARY BOILER FAILS
RANGE OF EQUIPMENT
ALLOWABLE RELEASE FOR INCIDENTS IN APPENDIX 2
ALLOWABLE FREQUENCY p.a.
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10
10^2
10^3
10^4
10^5
10^6
10^7
10^8
CURIES I_{131}

Fig. 4

INTERNAL DISTRIBUTION

1. H. G. Arnold
2. S. E. Beall
3. M. Bender
4. C. J. Borkowski
5. R. H. Bryan
6. J. R. Buchanan
7. D. W. Cardwell
8–12. W. B. Cottrell
13–17. H. J. de Nordwall
18. S. J. Ditto
19. A. P. Fraas
20. D. A. Gradiner
21. W. R. Grimes
22. E. W. Hagen
23. F. L. Hebble
24. F. A. Heddleson
25. H. W. Hoffman
26. F. L. Hudson
27. W. H. Jordan
28. S. I. Kaplan
29–67. P. R. Kasten
68. M. I. Lundin
69. R. N. Lyon
70. R. E. MacPherson
71. H. C. McCurdy
72. A. J. Miller
73. F. H. Neill
74. L. C. Oakes
75. A. M. Perry
76. H. B. Piper
77. M. W. Rosenthal
78–88. P. Rubel
89. M. R. Sheldon
90. M. J. Skinner
91. I. Spiewak
92. D. A. Sundberg
93. J. R. Tallackson
94. D. B. Trauger
95. G. D. Whitman
96–97. Central Research Library
98. Document Reference Section
99–101. Laboratory Records Department
102. Laboratory Records (RC)

EXTERNAL DISTRIBUTION

103. G. Caprioglio, Gulf General Atomic Co., P.O. Box 608, San Diego, Calif. 92112
104. R. A. Clark, U.S. Atomic Energy Commission, Division of Reactor Licensing, Washington, D.C. 20545
105. J. E. McEwen, U.S. Atomic Energy Commission, Division of Reactor Development and Technology, Washington, D.C. 20545
106. T. W. McIntosh, U.S. Atomic Energy Commission, Division of Reactor Development and Technology, Washington, D.C. 20545
107. T. R. Moffette, Gulf General Atomic Co., P.O. Box 608, San Diego, Calif. 92112
108. H. G. O'Brien, Tennessee Valley Authority, 211 Union Building, Knoxville, Tennessee 37901
109. A. J. Pressesky, U.S. Atomic Energy Commission, Division of Reactor Development and Technology, Washington, D.C. 20545
110. G. L. Stiehl, Gulf General Atomic Co., P.O. Box 608, San Diego, Calif. 92112
111. T. V. Tung, Gulf General Atomic Co., P.O. Box 608, San Diego, Calif. 92112

112. J. M. Waage, Gulf General Atomic Co., P.O. Box 608, San Diego, Calif. 92112
113. C. S. Walker, Tennessee Valley Authority, 211 Union Building, Knoxville, Tenn. 37901
114. R. F. Walker, Public Service Company of Colorado, Box 840, Denver, Col. 08202
115–117. Directorate of Licensing, USAEC, Washington, D.C. 20545
118–119. Direcorate of Regulatory Standards, USAEC, Washington, D.C. 20545
120–136. Manager, Technical Information Center, AEC, Oak Ridge
137. Research and Technical Support Division, AEC, ORO
138–139. Technical Information Center, AEC