**PRELIMINARY RELIABILITY ANALYSIS
FOR FFTF SAFETY CIRCUITS**

OSCAR B. MONTEITH

MARCH, 1968

**AEC RESEARCH &
DEVELOPMENT REPORT**

BATTELLE

NORTHWEST

BATTELLE MEMORIAL INSTITUTE

PACIFIC NORTHWEST LABORATORY

3000 STEVENS DRIVE, P. O. BOX 999, RICHLAND, WASHINGTON 99352

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

PACIFIC NORTHWEST LABORATORY

RICHLAND, WASHINGTON

operated by

BATTTELLE MEMORIAL INSTITUTE

for the

UNITED STATES ATOMIC ENERGY COMMISSION UNDER CONTRACT AT(45-1)-1830

PRINTED BY/ FOR THE U. S. ATOMIC ENERGY COMMISSION

3 3679 00060 7541

BNWL-661
UC-80,
Reactor Technology

PRELIMINARY RELIABILITY ANALYSIS
FOR FFTF SAFETY CIRCUITS

By

Oscar B. Monteith
FFTF Project
Safety and Reliability
Analysis Section

March 1968

FIRST UNRESTRICTED
DISTRIBUTION MADE

APR 3 '68

PACIFIC NORTHWEST LABORATORY
RICHLAND, WASHINGTON

Printed in the United States of America
Available from
Clearinghouse for Federal Scientific and Technical Information
National Bureau of Standards, U.S. Department of Commerce
Springfield, Virginia 22151
Price: Printed Copy \$3.00; Microfiche \$0.65

PRELIMINARY RELIABILITY ANALYSIS
FOR FFTF SAFETY CIRCUITS

Oscar B. Monteith

ABSTRACT

A preliminary reliability prediction for the Fast Flux Test Facility Reactor Safety System is reported. The system is analyzed for two failure modes; failures that cause spurious responses (reactor scrams), and failures that result in the inability to respond to unsafe conditions. Results are preliminary because the system is a conceptual version and components have not been specified.

TABLE OF CONTENTS

ABSTRACT	iii
INTRODUCTION	1
SUMMARY AND CONCLUSIONS.	2
NOMENCLATURE	3
SYSTEM OPERATIONAL REQUIREMENTS.	3
System Functions and Boundaries.	3
Anticipated Operational Conditions	4
Mission Profiles, Operating Time, and Duty Cycles.	5
Effectiveness Goals.	6
RELIABILITY ANALYSIS	6
Fail-To-Unsafe Condition	6
Common Elements Unsafe Condition Probability	7
Logic Diagrams	7
System 13 Probability of Fail-to-Unsafe.	9
Instrumentation Input and Common Elements Combined Unsafe Condition Probability.	10
Overall System 13 Probability of Fail-to-Unsafe Condition.	11
Recommendations.	12
Failures Causing Spurious Operation.	13
Common Element Spurious Operation Probability.	14
dc Power Supply and Nickel-Cadmium Battery	16
Overall System 13 Probability of Failure to Cause a Spurious Response	17
Effect of Expected Spurious Response on Reactor Availability	18
Recommendations.	18
ASSUMPTIONS.	18
MATHEMATICAL MODELS FOR COMPUTER USE	19
REFERENCES	20
APPENDIX A - Mathematical Model for Fail-to-Unsafe	A-1
APPENDIX B - Mathematical Model for Failures to Cause Spurious Response	B-1

PRELIMINARY RELIABILITY ANALYSIS
FOR FFTF SAFETY CIRCUITS

Oscar B. Monteith

INTRODUCTION

This report is a preliminary reliability analysis of the FFTF Reactor Safety System, System 13. Results obtained in this analysis are an initial estimate because of the preliminary state of system design. In addition, the component part failure rates, which are the basis of any reliability analysis, are unknown for the application and environment of the anticipated use in FFTF. These failure rates were estimated from data found in literature and other sources. This analysis will be updated and refined as more information on design and reliability of components becomes available. The purpose of this preliminary analysis is to point out areas for improved reliability early in the design phase and to indicate the need for establishing component part reliability specifications.

Conventional techniques for predicting system reliability, previously developed and published, provide the basis of the study. Methods of analysis detailed in References 1 and 2 were applicable and useful. Failure rates for the system components were obtained from the listed references, and it is believed these failure rates are pessimistic. Failure rates are expressed in failures per million hours, or failures $\times 10^{-6}$ per hour. A time base of 1000 hours has been used in the reliability and availability calculations.

Two separate evaluations are presented in this analysis. The first determines the probability of a failure in System 13 that can cause an unsafe condition at the reactor, by not actuating the safety rods on a bona fide demand. The second

determines the probability of a failure in System 13 that will cause spurious operation of the safety rods (an unwanted scram). The first of these criteria relates to reactor safety, and the second affects the availability of the reactor.

SUMMARY AND CONCLUSIONS

This reliability analysis predicts numerical probabilities as measures of the effectiveness of the Reactor Safety System. The effectiveness is investigated for safe operation of the reactor, and for the unavailability of the reactor for radiation testing.

The effectiveness of System 13 for safe operation of the reactor, in terms of the probability of a failure to cause an unsafe condition during a reactor lifetime of 20 years, is predicted as $q_{FU}^* = 4.5 \times 10^{-3}$. If suggested changes in the instrumentation voting redundancy are incorporated, the probability of failure decreases to $q_{FU}^* = 2 \times 10^{-6}$.

The probability that failure in System 13 will cause unwanted reactor scrams, is predicted as $q_{FS}^* = 0.134$ for 1000 hr of operation, or a spurious tripping rate of one per 7000 hr. Since the assumed reactor downtime is 1 hr for each of these failures, the associated reactor unavailability is 0.134 hr for each 1000 hr. These values are to be compared with the effectiveness criteria of a spurious tripping rate of one per 10,000 hr and a reactor unavailability of 0.1 hr per 1000 hr of operation. It is recommended that reliability requirements be included in the design specification for the safety rod solenoids, to insure against a disproportionate increase in the spurious tripping rate caused by failures in these solenoids.

The Reactor Safety System effectiveness for safe operation of the reactor can be greatly improved if suggested changes in the voting redundancy circuits are implemented. Cost and/or space may become dominant criteria in a trade-off comparison for making any change in the voting circuitry, and these considerations are not included in this analysis.

NOMENCLATURE

q_i	Probability of failure of an element, component, or subsystem
q_{FU}	Probability of fail-to-unsafe condition
q_{FS}	Probability of fail-safe condition
q_{MC}	Probability of failure of mercury wetted contact relay (MWC) contact pair
q_{CBC}	Probability of failure of circuit breaker contact pair
q_{CBT}	Probability of failure of circuit breaker trip mechanism
q_{IN}	Probability of failure of System 13 input combinations
q_{CH}	Probability of failure of one input channel of System 13 elements
λ	Generic failure rate of an element (failures/ 10^6 hr)
q^*	Predicted value of q

SYSTEM OPERATIONAL REQUIREMENTS

SYSTEM FUNCTIONS AND BOUNDARIES

The Reactor Safety System provides the necessary components and electrical circuits to implement automatic shutdown of the reactor in the event of conditions which are hazardous to the reactor, building, occupants, or the surroundings. The components comprise relays, circuit breakers, solenoids, suppressor diodes, power supply, and interconnecting circuitry. They are connected through logic schemes to provide fail-safe and positive actuation of the safety rods. System 13 does not include the instrumentation sensors and signal conditioning components of Reactor Instrumentation, and it does not include the Safety Rods.

Trip inputs to the Reactor Safety System are limited to the following:

- 1) Subcritical neutron flux period
- 2) Intermediate range neutron flux period

- 3) Power range neutron flux period
- 4) Power range rate-of-change
- 5) Sodium bulk over-temperature on primary loop
- 6) Loss of sodium flow in primary loop
- 7) Earthquake
- 8) Sodium over-temperature on each of 90 individual subassembly tubes
- 9) A manual trip is also included.

The outputs of System 13 are the interrupts to actuate the safety rods, and other interrupts to alarms and indicators to signal a trip or scram.

ANTICIPATED OPERATIONAL CONDITIONS

The safety rod solenoids of System 13, which are located within the safety rod assembly, will be exposed to elevated temperatures and nuclear radiation. The solenoid design for FFTF shall consist of materials and provide performance to accommodate this environment.

The remaining components of System 13 will be contained in standard rack enclosures mounted in the controlled environment rooms for Electrical and Instrument equipment within the FFTF Reactor Building. At this time, no anticipated problems are expected from this mounting and installation. In addition, a maintenance plan will provide for complete testing at least once each year, of the System 13 components and circuits.

The Reactor Safety System will interface with the following FFTF systems:

- 1) Reactor Instrumentation System
- 2) Electrical Services, Plant Power
- 3) Reactor Control System.

There are no anticipated interferences or interactions between System 13 and these interfacing systems. It is expected that the operation of relays and the switching of inductive circuits will produce interfering noise on adjacent circuits; however, the relays and inductive circuits of System 13 will remain in a quiescent state during an operating cycle of the reactor, and the only switching of elements will occur when a scram is initiated.

The present concept for the design of System 13 employs fail-safe circuitry and logic. From this premise, failures of components which result in opening of circuits will produce spurious trips (or reactor scrams). The opposite condition, i.e., those failures of components which continuously energize a circuit, will result in an unsafe condition, because the safety rods will not be actuated on a bona fide demand.

MISSION PROFILES, OPERATING TIME, AND DUTY CYCLES

The Reactor Safety System will be energized and the safety circuit "made up" during the following reactor operations:

- 1) Refueling
- 2) Nuclear startup
- 3) Power level operation
- 4) Controlled shutdown
- 5) All conditions of core reactivity.

Present plans call for six weeks of reactor operation with two weeks shutdown period following each operational period. A typical shutdown period will provide five days for refueling, and startup. Thus, it appears that normally nine days every two months will be allowed for maintenance and downtime. These duty cycles will be repeated in a continuous series for the life of the reactor.

EFFECTIVENESS GOALS

There are two effectiveness goals for System 13. The first of these concerns the reactor safeguards, and the second concerns the spurious operation of the safety rods.

The first goal is of primary interest, from the safety standpoint, in order to estimate the chance of the equipment failing in an unsafe manner. This probability of failure to cause an unsafe condition is particularly important where safety reliance is being placed upon the equipment concerned. There are no quantitative requirements in industry relating to the safety reliability of Reactor Safety Systems. The fail-to-unsafe failure rate of components in general are a small part of the overall failure rate, and in some cases, only an estimate is available. The effectiveness criterion for the fail-to-unsafe condition is not easily established because there is no precedent, and the general subjective "feeling" is that the Reactor Safety System should be "100 percent fail-safe."

The second goal relates to the probability that a failure causes a spurious response and an unwanted scram of the reactor. This is more straightforward than the first discussed, because these failures represent the majority of cases and the condition is more easily analyzed from an objective viewpoint. From experience, a reasonable goal for spurious fail-safe events is initially established at one per 10,000 hr of operation (approximately one per year). Since a spurious event causes a reactor trip, the associated reactor downtime is assumed to be 1 hr⁽³⁾ per 10,000 hr of operation; thus, 0.1 hr downtime per 1000 hr is considered for the unavailability allocation of the Reactor Safety System.

RELIABILITY ANALYSIS

FAIL-TO-UNSAFE CONDITION

This part of the reliability analysis predicts the probability of a failure in System 13 which will cause an unsafe condition in the FFTF. By definition, q_{FU} is the fail-to-unsafe probability of an element, component, or subsystem.

The Reactor Safety System is required to provide reactor shutdown if various control parameters are exceeded. Therefore, a combination of failures which will result in System 13 not initiating shutdown when required, is a fail-to-unsafe condition. The following analysis determines these combinations of failures and establishes their probabilities of occurrence.

Common Elements Unsafe Condition Probability

The common elements comprise mercury-wetted-contact relays, the AK-2-15 type circuit breakers, and the safety rod solenoids. All contacts of relays and circuit breakers are normally open. Therefore, to "make up" the safety circuit, all relay coils, safety rod solenoids, and circuit breaker trip mechanisms must be energized; and the corollary logical condition requires all contacts to be closed.

For these logic states, the fail-to-unsafe condition failure rates of the elements are estimated to be:^(1,2,4)

MWC relay coil and suppressor diode = 0

Safety rod solenoid and suppressor diode = 0

Circuit breaker trip mechanism = $0.2 \times 10^{-6}/\text{hr}$

MWC relay contacts = $0.1 \times 10^{-6}/\text{hr}$

Circuit breaker contacts = $0.2 \times 10^{-6}/\text{hr}$

Logic Diagrams

The common elements reliability logic diagram is shown in Figure 1, and the logic diagrams for the instrumentation inputs are shown in Appendix A. These diagrams are drawn in the manner of "success" logic diagrams for reliability analysis purposes. Since this report is a study of failure identification, the reader is cautioned to exercise care when using the success diagrams to examine the probability of failure of the various combinations.

MWC = MERCURY WETTED CONTACT
CONT = RELAY CONTACT PAIR

MWC
COIL = MWC RELAY COIL

CB = CIRCUIT BREAKER
TRIP = TRIP MECHANISM

CB = CIRCUIT BREAKER
CONT = CONTACT PAIR

ROD
SOL. = SAFETY ROD SOLENOID

FIGURE 1. Common Elements Reliability Block Diagram Fail-To-Unsafe

System 13 Probability of Fail-to-Unsafe

The development of the mathematical model for the probability of fail-to-unsafe of System 13 is contained in the Appendices. The resulting probability expressions for the various logic subgroups, and the numerical value for 1000 hr operation, are listed below.

Common elements:

$$q_6 = q_{MC}^4 (1 + 2q_{CBC}^2 + 2q_{CBT} + q_{CBC}^4 + 2q_{CBC}^2 q_{CBT} + q_{CBT}^2) = 1 \times 10^{-16}$$

Battery and power supply:

$$q_8 = 0$$

Seismoscope input:

$$\begin{aligned} q_{IN} &= 27q_{MC}^2 \\ &= 27 \times 10^{-8} \end{aligned}$$

High range flux input:

$$\begin{aligned} q_{IN} &= 108q_{MC}^3 \\ &= 0.011 \times 10^{-8} \end{aligned}$$

Intermediate range flux input:

$$\begin{aligned} q_{IN} &= 27q_{MC}^2 \\ &= 27 \times 10^{-8} \end{aligned}$$

Subcritical range flux input:

$$\begin{aligned} q_{IN} &= 4q_{MC}^2 \\ &= 4 \times 10^{-8} \end{aligned}$$

Primary loop flow input:

$$\begin{aligned} q_{IN} &= 108q_{MC}^3 \\ &= 0.011 \times 10^{-8} \end{aligned}$$

Primary loop temperature input:

$$\begin{aligned} q_{IN} &= 108q_{MC}^3 \\ &= 0.011 \times 10^{-8} \end{aligned}$$

Subassembly outlet temperature input:

$$\begin{aligned} q_{IN} &= 28q_{MC}^2 \text{ for each tube} \\ &= 28 \times 10^{-8} \text{ for each tube} \\ &= 2520 \times 10^{-8} \text{ for 90 tubes} \end{aligned}$$

Instrumentation Input and Common Elements Combined Unsafe Condition Probability

The probability of fail-to-unsafe condition for each of the Instrumentation Inputs and the common elements of System 13 is developed as follows:

The probability of failure of the combined major blocks above is given by:

$$q_{FU} = q \text{ fail-to-unsafe} = q_{IN} + q_6 - q_{IN}q_6 \approx q_{IN} + q_6$$

Table 1 lists the resulting probabilities of failure to an unsafe condition for each of the instrumentation inputs. These probabilities of failure are determined for an operating time of 1000 hours.

TABLE 1. Overall System 13 q_{FU}

	Instrumentation Input	Common Elements	$q_{FU} = q_{IN} + q_6$
Input	q_{IN}	q_6	q_{FU}
Seismoscope	27×10^{-8}	1×10^{-16}	27×10^{-8}
Neutron Flux Hi Range	0.011×10^{-8}	1×10^{-16}	0.011×10^{-8}
Neutron Flux Intermediate Range	27×10^{-8}	1×10^{-16}	27×10^{-8}
Neutron Flux Subcritical Range	4×10^{-8}	1×10^{-16}	4×10^{-8}
Primary Loop Flow	0.011×10^{-8}	1×10^{-16}	0.011×10^{-8}
Primary Loop Temperature	0.011×10^{-8}	1×10^{-16}	0.011×10^{-8}
Each Subassembly Outlet Temperature	28×10^{-8}	1×10^{-16}	28×10^{-8}
90 Subassembly Temperature	2520×10^{-8}	1×10^{-16}	2520×10^{-8}

It is obvious that the major contributor to the probability of fail-to-unsafe condition is the instrumentation voting input; the common element's contribution is negligible.

Overall System 13 Probability of Fail-to-Unsafe Condition

It is not possible to obtain an elegant expression for the probability of fail-to-unsafe condition for the overall System 13. The principal reason for this is the inherent redundancy found in the instrument subsystems. For example: the neutron flux hi-range subsystem is backed up by the primary loop temperature and

process tube temperature subsystems; the primary loop flow subsystem is backed up by the primary loop temperature subsystem. However, these are not true system redundancies, and each condition that would place a demand on System 13 requires an individual analysis.

A possible figure of merit, for the overall System 13 reliability, may be obtained by summation of the fail-to-unsafe probabilities for those subsystem components required for operating the FFTF at full power. These subsystems are: seismoscope, neutron flux hi-range, primary loop flow, primary loop temperature, and subassembly outlet temperatures of 90 tubes. This arbitrary grouping of components results in the following probability of fail-to-unsafe condition for System 13:

$$q^*_{FU} = 26 \times 10^{-6}.$$

Expressed in terms of probability of success (Reliability), we can say that System 13 has a Reliability of 0.999974 for an operating time of 1000 hours.

Assuming the lifetime of the FFTF reactor is 20 years, the probability of failure during this period is 4.5×10^{-3} .

Recommendations

It is noted that the voting redundancy combination of 2-out-of-4 provides superior reliability to the combination of 2-out-of-3, (and 1-out-of-2), instrument channels. The ratio of the two probabilities of failures are:

$$\frac{q_{2/4}}{q_{2/3}} = \frac{4q_{CH}^3 - 3q_{CH}^4}{3q_{CH}^2 - 2q_{CH}^3}$$

If $q_{CH} \ll 1$ (as is true in this case) then,

$$\frac{q_{2/4}}{q_{2/3}} \approx \frac{4}{3} q_{CH}.$$

As an example, assume the probability of failure of one channel is $q_{CH} = 1 \times 10^{-4}$;

$$\text{then } q_{2/4} \approx 4 \times 10^{-12}$$

$$q_{2/3} \approx 3 \times 10^{-8}$$

and the improvement in reliability is $3/4 \times 10^4$.

If all of the voting redundancy inputs to System 13 were of the 2-out-of-4 type, then the overall probability of fail-to-unsafe condition for the system would be

$$q^*_{FU} = 0.96 \times 10^{-8} .$$

The following comparisons indicate the improvement to be gained through use of 2-out-of-4 voting redundancy in all inputs to System 13:

	<u>2/3 Redundancy</u>	<u>2/4 Redundancy</u>
Probability of failure in 1000 hours	26×10^{-6}	0.96×10^{-8}
Reliability for 1000 hours	0.999974	0.99999999
Probability of failure in 20 years	4.5×10^{-3}	2×10^{-6}

FAILURES CAUSING SPURIOUS OPERATION

This part of the reliability analysis predicts the probability of failures in System 13 which cause spurious operation, or unwanted trips, of the safety rods. By definition, q_{FS} is the probability of failure of an element, component, or subsystem to cause spurious operation of System 13 (fail-safe condition).

In this analysis it is presumed that because of various interlocks, the inadvertent operation of one safety rod causes all other rods to scram. In addition, since System 13 is fail-safe in design, it follows that most single component failures

in the common elements cause a spurious operation. Thus, except for the DC power supply and instrumentation inputs, the reliability logic diagram for the failure analysis of q_{FS} is a series combination of the components. The following analysis determines these failures and establishes their probability of occurrence.

Common Element Spurious Operation Probability (q_{FS})

The common elements of System 13 have been described previously, and their logical states noted. As the safety circuit is "made-up", these logic states are: all relay coils and solenoids energized, and all contacts closed. The failure rates of the failure modes which cause spurious responses are estimated to be: (2,3,4)

MWC relay coil = 0.3×10^{-6} per hour

MWC relay contact pair = 0.1×10^{-6}

Circuit breaker trip mechanism = 0.3×10^{-6}

Circuit breaker contact pair = 0.1×10^{-6}

Rod solenoid = 0.3×10^{-6}

Suppressor diode = 0.2×10^{-6}

As shown in the reliability logic diagram of Figure 2, all of the logic blocks that comprise System 13 are in a series combination with the parallel redundant power supply and battery. Note that only one of the three flux range instrumentation inputs is included in the logic diagram; the other two flux range instrumentation inputs are used during startup operations and would be considered only for failure analysis involving that period.

The development of the mathematical model for the probability of failure causing a spurious operation is contained in Appendix B.

To effect the mathematical modeling of System 13 according to Figure 2, it is necessary to represent the redundant power supply and battery with a single logic block. Since the battery and power supply combination are a unique problem for reliability analysis, an approximate solution is discussed in the next paragraph.

15

BNWL-661

FIGURE 2. Reliability Block Diagram Failure to Cause Spurious Event

dc Power Supply and Nickel-Cadmium Battery

The Reactor Safety System will be energized with dc power of nominally 128 V. This dc power is obtained from a dc power supply with a floating nickel-cadmium battery on the line, and the battery will be maintained at full charge by the power supply. The power supply source is the ac plant power of Electrical Services.

An analysis for failures which cause spurious operation of this combination is relatively complicated because: (1) the battery is in standby redundancy with periodic maintenance and replacement, (2) partial loss of the rated output of the battery will still provide some standby energy, (3) the battery is not a subsystem or combination of components, but rather a chemical source of energy, and (4) there are no accepted failure rates in the conventional sense, for nickel-cadmium batteries.

Item (4) above is further explained in the technical paper by L. Gomberg and H. Thierfelder,⁽⁵⁾ where it is indicated that failure rates of nickel-cadmium batteries are unavailable for several reasons: insufficient test data, lack of knowledge regarding the detailed chemical operation of the cell, and existing test data which indicates that reliability is a function of the depth of discharge, overcharge rate, cell temperature, and cycle histories.

A simplified approach to this analysis difficulty is possible by considering the dc power supply redundant with the battery, and assuming a reasonable failure rate for the battery. Thus,

$$\lambda_{\text{COMB}} \approx (\lambda_{\text{POWER SUPPLY}}) (\lambda_{\text{BATTERY}}) \quad .$$

Representative failure rates for these components which cause a spurious operation of System 13 are:

$$\begin{aligned} \lambda_{\text{POWER SUPPLY}} &= 20 \times 10^{-6}/\text{hr} \\ \lambda_{\text{BATTERY}} &= 100 \times 10^{-6}/\text{hr} \quad . \end{aligned}$$

Substituting these values yields

$$\lambda_{\text{COMB}} = 0.002 \times 10^{-6}/\text{hr} .$$

For 1000 hours of operation the probability of failure is

$$q_{\text{COMB}} \approx 2 \times 10^{-6} .$$

Overall System 13 Probability of Failure to Cause a Spurious Response

Table 2 lists the resulting probabilities of failures (q_i) for each of the blocks in Figure 2. For the overall System 13, the probability of failure q_{FS} for 1000 hr is:

$$\begin{aligned} q_{\text{FS}}^*(1000) &= 1 - e^{-\sum q_i} \\ &= 1 - e^{-0.144} = 0.134 . \end{aligned}$$

Thus, there is a probability of 0.134 that a spurious operation of the Reactor Safety System will occur per 1000 hours of reactor operation. The expected tripping rate will be about one per 7000 hr of operation.

TABLE 2. Overall System 13 q_{FS}

1 Seismoscope Input	0.0192	$\times 10^{-4}$
1 Neutron Flux Hi-Range Input	0.0384	$\times 10^{-4}$
1 Primary Loop Flow Input	0.0384	$\times 10^{-4}$
1 Primary Loop Temperature Input	0.0384	$\times 10^{-4}$
90 Subassembly Tube Temperature Input	0.173	$\times 10^{-4}$
412 Mercury Wetted Contact Pair	412	$\times 10^{-4}$
196 Mercury Relay Coil	588	$\times 10^{-4}$
4 Circuit Breaker Contact Pair	4	$\times 10^{-4}$
2 Circuit Breaker Trip Mechanism	6	$\times 10^{-4}$
204 Suppressor Diodes	408	$\times 10^{-4}$
6 Safety Rod Solenoids	18	$\times 10^{-4}$
1 dc Power Supply (W/Battery Backup)	0.02	$\times 10^{-4}$
	<u>1436.3274</u>	$\times 10^{-4}$

$$\sum q_i = 0.144$$

Effect of Expected Spurious Response on Reactor Availability

A spurious response of the Reactor Safety System causes an unwanted trip of the reactor. The associated reactor downtime (D) is approximately one hour.⁽¹⁾ The reactor unavailability for the expected spurious tripping rate is:

$$q_{FS} \times D = 0.134 \text{ hr per } 1000 \text{ hr} \quad .$$

This reactor unavailability does not include the downtime necessary to diagnose the cause of failure, nor to implement corrective action to the Reactor Safety System. It has been assumed that suitable failure indicators are included in the Reactor Safety System design, which provide quick and efficient diagnosis of a spurious trip.

Recommendations

It is noted that the only components in System 13 which are exposed to an adverse environment are the safety rod solenoids. These solenoids, located within the safety rod assembly, will be exposed to elevated temperatures and nuclear radiation. In this present analysis, a failure rate for these solenoids has been used which is based on conventional designs operating in conventional environments. The contribution of the rod solenoids to the overall q_{FS}^* for System 13 is small by employing this failure rate. However, if the failure rate for the solenoid design to be used in FFTF turns out to be very much greater, this small contribution will not be valid. No severe difficulty is expected in producing the required design, but we recommend that the specification contain reliability requirements.

ASSUMPTIONS

Simplifying assumptions have been made in the preparation of this analysis; some are stated, others implied. A list of the more important assumptions follow:

- 1) Components are operating in their useful life phase where the failure rate is constant and the distributions of time between failures can be expressed by exponential distributions.

- 2) Many component failure rates have been estimated based on published data of similar equipment.
- 3) Component failures are independent. Dependent or secondary failures have not been considered.
- 4) The system and components are performing exactly as designed at the beginning of each time period of study, and there are no design deficiencies.
- 5) Testing and/or repairs have neither altered the original design, nor added new faults.
- 6) Only permanent failures have been considered; transient and intermittent failures are not analyzed.

MATHEMATICAL MODELS FOR COMPUTER USE

Mathematical models of the probabilities of failures are desired for use with a computer program. The following models are a first pass approximation based on available design data of the Reactor Safety System.

- 1) Probability of failure to cause an unsafe condition:

$$q_{FU} = 2547q_{MC}^2 + 320q_{MC}^3 + q_{MC}^4 (1 + 2q_{CBC}^2 + 2q_{CBT}^2 + q_{CBC}^4 + 2q_{CBC}^2 q_{CBT} + q_{CBT}^2)$$

where q_{MC} = the probability of fail-to-unsafe mode of the mercury wetted contact pair.

Since $q_{MC} \ll 1$, and neglecting higher terms

$$q_{FU} \approx 2547q_{MC}^2$$

- 2) Probability of failure to cause a spurious response:

$$\begin{aligned} \sum q_i = & 6q_{ROD \text{ SOL}} + 4q_{CB \text{ CONT}} + 2q_{CB \text{ TRIP}} \\ & + 412q_{MW \text{ CONT}} + 196q_{MW \text{ COIL}} + 204q_{SUPPRESSOR} \\ & + q_{POWER \text{ SUPPLY}} + 97q_{INPUT} \end{aligned}$$

The major contributors to the summation are:

$$\sum q_i \approx 6q_{\text{ROD SOL}} + 412q_{\text{MC CONT}} + 196q_{\text{MW COIL}} \\ + 204q_{\text{SUPPRESSOR}} .$$

The model for the probability of failure to cause a response is:

$$q_{\text{FS}} = 1 - e^{-\sum q_i} .$$

REFERENCES

1. MIL-Handbook-217A. Department of Defense, Washington, December 1, 1965.
2. A. E. Green and A. J. Bourne. "Safety Assessment With Reference to Automatic Protective Systems for Nuclear Reactors," AHSB(S) R117. United Kingdom Atomic Energy Authority, 1966.
3. D. C. Boyd to G. H. Strong. Pacific Northwest Laboratory, Richland, Washington, August 1967. "Preliminary Reliability Analysis of Primary Electrical Systems," August 17, 1967. Personal Communication.
4. R. A. Owens and T. J. Dolcimascolo. "Quantitative Reliability Prediction," Institute of Electrical and Electronic Engineers, Proceedings on Reliability, 1966.
5. L. Gomberg and H. Thierfelder. "Assuring Reliability in Aerospace Batteries," Institute of Electrical and Electronic Engineers, 11th National Symposium on Reliability and Quality Control, 1965.

APPENDIX A

MATHEMATICAL MODEL FOR FAIL-TO-UNSAFE

APPENDIX A

MATHEMATICAL MODEL FOR FAIL-TO-UNSAFE

The logical expression for the probability of fail-to-unsafe condition of the System 13 common elements is developed as follows:

(all q_i are probability of failure of an element or component)

Refer to Figure 1

$$q_1 = 0$$

$$q_2 = (q_{MC})^2$$

$$q_3 = q_4(q_5 + q_{CBT}) = q_{MC}^2 q_{CBC}^2 + q_{MC}^2 q_{CBT}$$

$$q_4 = (q_{MC})^2$$

$$q_5 = (q_{CBC})^2$$

$$q_6 = (q_2 + q_3)^2 = q_2^2 + 2q_2q_3 + q_3^2$$

$$q_7 = q_{IN} + q_6 - q_{IN}q_6 \cong q_{IN} + q_6 \text{ since } q_{IN}q_6 \approx 0$$

q_{IN} is the instrumentation voting redundancy input.

On substituting in the expression for q_6 , the following is obtained:

$$q_6 = q_{MC}^4 (1 + 2q_{CBC}^2 + 2q_{CBT} + q_{CBC}^4 + 2q_{CBC}^2 q_{CBT} + q_{CBT}^2)$$

The probabilities of fail-to-unsafe condition for an operating time of 1000 hr for these common elements are:

$$q_{MC} = \text{MWC Relay Contacts} = 0.1 \times 10^{-3}$$

$$q_{CBC} = \text{Circuit Breaker Contacts} = 0.2 \times 10^{-3}$$

$$q_{CBT} = \text{Circuit Breaker Trip} = 0.2 \times 10^{-3}$$

$$q_2 = (q_{MC})^2 = 1 \times 10^{-8}$$

$$q_4 = (q_{MC})^2 = 1 \times 10^{-8}$$

$$q_5 = (q_{CBC})^2 = 4 \times 10^{-8}$$

$$q_3 = q_{MC}^2 q_{CBC}^2 + q_{MC}^2 q_{CBT} \approx 2 \times 10^{-12} \text{ neglecting higher order terms.}$$

$$q_6 = q_2^2 + 2q_2q_3 + q_3^2 = 1.00040004 \times 10^{-16}$$

It is noted that an adequate approximation is obtained for q_6 by dropping the higher order terms:

$$q_6 \approx (q_{MC})^4 = 1.0 \times 10^{-16}$$

The elements which make up the power source for System 13 are a dc power supply with a redundant nickel-cadmium storage battery as backup supply. The fail-to-unsafe condition of this combination is assumed to be zero. Therefore, the fail-to-unsafe probability of the power supply is:

$$q_8 = 0$$

SYSTEM 13 INSTRUMENTATION VOTING INPUTS UNSAFE CONDITIONS PROBABILITY

Each of the instrumentation channels that supply an input to the System 13, Reactor Safety System, employs mercury-wetted-contact relays in a logic scheme called "voting redundancy."

Seismoscope Input

The seismoscope input comprises three instrumentation channels that are combined in a voting redundancy of 2-out-of-3.

$$q_{CH} = q_{\text{CHANNEL}} = 3q_{MC} - 3q_{MC}^2 + q_{MC}^3 \approx 3q_{MC}$$

$$q_{IN} = 3q_{CH}^2 - 2q_{CH}^3 \approx 27q_{MC}^2$$

$$q_{IN} = 27 \times 10^{-8} \text{ for seismoscope input}$$

Neutron Flux, High Range Input

The neutron flux high range input comprises 4 instrumentation channels that are combined in a voting redundancy of 2-out-of-4.

$$q_{CH} = 3q_{MC} - 3q_{MC}^2 + q_{MC}^3 \approx 3q_{MC}$$

$$q_{IN} = 4q_{CH}^3 - 3q_{CH}^4 \approx 108q_{MC}^3$$

$$q_{IN} = 108 \times 10^{-12} = 0.011 \times 10^{-8} \text{ for high range flux input}$$

Neutron Flux, Intermediate Range Input

The intermediate range neutron flux input is a 2-out-of-3 voting redundancy (previously determined), and the probability of failure is:

$$q_{IN} = 27q_{MC}^2$$

$$q_{IN} = 27 \times 10^{-8} \text{ for intermediate range flux input.}$$

Neutron Flux, Subcritical Range Input

The subcritical range neutron flux input comprises 2 instrumentation channels that are combined in a voting redundancy of 1-out-of-2.

$$q_{IN} = 4 \times 10^{-8} \text{ for subcritical range flux input.}$$

Primary Loop Flow Input

The primary loop flow rate is a 2-out-of-4 voting redundancy (previously determined), and the probability of failure is:

$$q_{IN} = 108q_{MC}^3$$

$$q_{IN} = 0.011 \times 10^{-8} \text{ for primary loop flow input.}$$

Primary Loop Temperature Input

The primary loop temperature input is a 2-out-of-4 voting redundancy (previously determined), and the probability of failure is:

$$q_{IN} = 108q_{MC}^3$$

$$q_{IN} = 0.011 \times 10^{-8} \text{ for primary loop temperature input.}$$

Subassembly outlet

The subassembly outlet temperature input is a 2-out-of-3 voting redundancy (previously determined), and each of the 90 tubes will provide one temperature channel input to the System 13 common elements.

$$q_{CH} = 3q_{MC} - 3q_{MC}^2 + q_{MC}^3 \approx 3q_{MC}$$

$$q_V = 3q_{CH}^2 - 2q_{CH}^3 \approx 27q_{MC}^2$$

$$q_W = q_{MC}^2$$

$$q_{IN} = q_V + q_W = 28q_{MC}^2$$

$$q_{IN} = 28 \times 10^{-8} \text{ for each of 90 tubes, subassembly outlet temperature input.}$$

APPENDIX B

MATHEMATICAL MODEL FOR FAILURES
TO CAUSE SPURIOUS RESPONSE

APPENDIX B
MATHEMATICAL MODEL FOR FAILURES
TO CAUSE SPURIOUS RESPONSE

The probability of failure to cause a spurious response (q_{FS}) of System 13 is developed as follows:

For a series combination of elements

the probability of success is $p = p_A \times p_B \times p_C \dots\dots\dots$

and $p_A = e^{-\lambda_A t}$ where $\lambda_A = \sum \lambda_i$, and λ_i = the failure rate of the component failure mode causing a spurious operation.

$$p_A = (1 - q_A) \text{ and } q_A = 1 - e^{-\lambda_A t}.$$

If $\lambda_A t \ll 1$, then $e^{-\lambda_A t} \approx 1 - \lambda_A t$ and $q_A \approx \lambda_A t$.

$$p = e^{-\lambda_A t} \times e^{-\lambda_B t} \times e^{-\lambda_C t} \dots\dots\dots$$

$$= e^{-(\lambda_A + \lambda_B + \lambda_C \dots\dots\dots)t}$$

$$\approx e^{-(q_A + q_B + q_C \dots\dots\dots)}$$

$$q = 1 - p \approx 1 - e^{-(q_A + q_B + q_C \dots\dots\dots)}$$

$$\text{Therefore: } q_{FS} = 1 - e^{-(q_A + q_B + q_C \dots\dots)}$$

The exact expression for q is

$$q = 1 - (1 - q_A)(1 - q_B)(1 - q_C) \dots\dots$$

$$= 1 - [1 - q_A - q_B - q_C \dots\dots + q_A q_C + q_B q_C + q_A q_B \dots\dots]$$

$$\approx q_A + q_B + q_C \dots\dots \text{neglecting higher order terms,}$$

$$\text{and if } q_A, q_B, q_C \ll 1.$$

INSTRUMENTATION CHANNEL INPUTS

Each of the instrumentation channel inputs to the Reactor Safety System common elements employs a "voting redundancy" combination of channels. The combinations of failures, and their probabilities of occurrence, to cause spurious operation of System 13, will be determined.

Voting Redundancy 2-out-of-3

The voting redundancy combination of 2-out-of-3 is employed for the following instrumentation channel inputs:

- 1) Seismoscope Input
- 2) Neutron Flux Intermediate Level Input
- 3) Process Tube Temperature Input

The components that make up one input channel are: 3 mercury wetted contact pairs, and one mercury wetted contact relay coil shunted by a suppressor diode. The failure rate of the mode to cause spurious operation of System 13, for these components, is determined for 1000 hr operating time.

$$\begin{aligned}
 q_{MWC} &= \text{MWC Relay Contact Pair} = 1 \times 10^{-4} \\
 q_{MWC} &= \text{MWC Coil} = 3 \times 10^{-4} \\
 q_{SUPPRESSOR} &= \text{Suppressor Diode} = 2 \times 10^{-4}
 \end{aligned}$$

and $q_{\text{CHANNEL}} = 8 \times 10^{-4}$

For 2-out-of-3 voting redundancy:

$$q_{\text{IN}} = 3q_{\text{CH}}^2 - 2q_{\text{CH}}^3 \approx 3 \times 64 \times 10^{-8}$$

$$q_{\text{IN}} \approx 192 \times 10^{-8}$$

$$q_{\text{IN}} \approx 0.0192 \times 10^{-4}$$

Voting Redundancy 2-out-of-4

The voting redundancy combination of 2-out-of-4 is employed for the following instrumentation channel inputs:

- 1) Neutron Flux Power Level Input
- 2) Primary Loop Flow Input
- 3) Primary Loop Temperature Input

$$q_{\text{CH}} = 8 \times 10^{-4} \text{ (previously determined)}$$

$$q_{\text{IN}} = 6q_{\text{CH}}^2 - 8q_{\text{CH}}^3 + 3q_{\text{CH}}^4 \approx 6 \times 64 \times 10^{-8}$$

$$q_{\text{IN}} \approx 384 \times 10^{-8}$$

$$\approx 0.0384 \times 10^{-4}$$

Voting Redundancy of 1-out-of-2

The voting redundancy combination of 1-out-of-2 is employed for only one input channel:

- 1) Neutron Flux Subcritical Level Input:

$$q_{CH} = 7 \times 10^{-4}$$

$$q_{IN} = 2q_{CH} - q_{CH}^2 \approx 2 \times 7 \times 10^{-4}$$

$$q_{IN} \approx 14 \times 10^{-4}$$

DISTRIBUTIONNo. of
Copies

30	<u>AEC Library, Washington</u> M. Shaw, Director, RDT Asst Dir for Nuclear Safety Analysis and Evaluation Br, RDT:NS Environmental and Sanitary Engrg Br, RDT:NS Research and Development Br, RDT:NS Asst Dir for Plant Engrg, RDT Applications and Facilities Br, RDT:PE Components Br, RDT:PE Instrumentation and Control Br, RDT:PE Systems Engineering Br, RDT:PE Asst Dir for Program Analysis, RDT Asst Dir for Project Management, RDT Liquid Metals Projects Br, RDT:PM FFTF Project Manager, RDT:PM (3) Asst Dir for Reactor Engrg Control Mechanisms Br, RDT:RE Core Design Br, RDT:RE (2) Fuel Fabrication Br, RDT:RE Fuel Handling Br, RDT:RE Reactor Vessels Br, RDT:RE Asst Dir for Reactor Tech Chemistry and Chemical Separations Br, RDT:RT (2) Fuels and Materials Br, RDT:RT Reactor Physics Br, RDT:RT Special Technology Br, RDT:RT Asst Dir for Eng Std's
2	<u>AEC Chicago Patent Group</u> G. H. Lee, Chief R. K. Sharp, Richland
265	<u>AEC Division of Technical Information Extension</u>
1	<u>AEC Idaho Operations Office</u> C. W. Bills, Director
5	<u>AEC Richland Operations Office</u> FFTF Project Office (2) Engineering and Construction Div, J. M. Schivley C. L. Robinson Technical Information Library

No. of
Copies

1	<u>AEC San Francisco Operations Office</u> Director, Reactor Division
4	<u>AEC Site Representatives - PNL</u> P. G. Holsted (2) L. R. Lucas A. D. Toth
4	<u>AEC Site Representatives</u> Argonne National Laboratory Atomics International Atomic Power Development Assoc. General Electric Co.
2	<u>Argonne National Laboratory</u> R. A. Jaross LMFBR Program Office
2	<u>Atomics International</u> L. E. Glasgow R. W. Dickinson
1	<u>Atomic Power Development Assoc.</u> B. V. D. Farris
2	<u>Babcock and Wilcox Co.</u> S. H. Esleeck T. P. Farrell
3	<u>Battelle Memorial Institute</u>
1	<u>Combustion Engineering</u> W. P. Staker, Project Manager
1	<u>Douglas United Nuclear, Inc.</u> DUN File
1	<u>General Dynamics Corp.</u> D. Coburn
4	<u>General Electric Co.</u> Karl Cohen (3) Bertram Wolfe

Distr-3

No. of
Copies

1	<u>Idaho Nuclear Corporation</u> D. R. deBoisblanc
1	<u>PNL Representative</u> N. A. Hill (ZPR III)
1	<u>Stanford University</u> R. Sher
5	<u>Westinghouse Electric Corp.</u> J. C. R. Kelly
109	<u>Battelle-Northwest</u> G. E. Akre W. G. Albert S. O. Arneson F. J. Arrotta E. R. Astley J. M. Batch T. Bauman R. A. Bennett J. R. Boldt C. L. Boyd D. C. Boyd C. L. Brown W. L. Bunch C. P. Cabell A. C. Callen C. M. Cantrell J. R. Carrell W. E. Cawley W. L. Chase T. T. Claudson P. D. Cohn D. L. Condotta R. R. Cone J. H. Cox J. M. Davidson V. A. DeLiso D. R. Doman G. E. Driver R. V. Dulin J. F. Erben L. M. Finch R. C. Free

Battelle-Northwest (contd)

E. E. Garrett
S. M. Gill
V. W. Gustafson
J. P. Hale
R. A. Harvey (5)
B. R. Hayward
J. W. Helm
R. J. Hennig
G. M. Hesson
P. L. Hofmann
B. M. Johnson
H. G. Johnson
E. M. Johnston
J. H. Kinginger
D. D. Lanning
H. D. Lenkersdorfer
C. W. Lindenmeier
H. E. Little
W. W. Little
W. B. McDonald
M. H. Meuser
R. A. Moen
O. B. Monteith (10)
C. A. Munro
C. R. Nash
D. M. Nero
M. G. Patrick
J. A. Perry
R. E. Peterson
W. E. Roake
J. D. Schaffer
F. H. Shadel
D. W. Shannon (2)
D. E. Simpson
M. O. Slater
C. R. F. Smith
R. J. Squires
D. D. Stepnewski
G. H. Strong
C. D. Swanson
J. C. Tobin
K. G. Toyoda
M. A. Vogel
A. L. Vosmer
D. M. Walley
J. H. Westsik
L. A. Whinery
R. D. Widrig

Battelle-Northwest (contd)

T. W. Withers
N. G. Wittenbrock
M. R. Wood
F. W. Woodfield
M. Wiitala
FFTF File (2)
Technical Publications (2)
Technical Information (5)