6-11
705 up Recd
Hester in C-92b

UC-80

172

AI-AEC-13074

22,186

OPERATIONAL HAZARDS EVALUATION
FOR
5-kwe REACTOR THERMOELECTRIC SYSTEM
GROUND TEST

AEC Research and Development Report

Atomics International Division
Rockwell International

P.O. Box 309
Canoga Park, California 91304

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Atomic Energy Commission, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

Printed in the United States of America
Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22151
Price: Printed Copy \$3.00; Microfiche \$0.95

OPERATIONAL HAZARDS EVALUATION
FOR
5-kwe REACTOR THERMOELECTRIC SYSTEM
GROUND TEST

R. J. TUTTLE

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Atomic Energy Commission, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

Atomics International Division
Rockwell International

P.O. Box 309
Canoga Park, California 91304

CONTRACT: AT(04-3)-701
ISSUED: JUNE 11, 1973

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISTRIBUTION

This report has been distributed according to the category "Systems for Nuclear Auxiliary Power (SNAP) Reactor – SNAP Program," as given in the Standard Distribution for Classified Scientific and Technical Reports, M-3679.

CONTENTS

	<u>Page</u>
Abstract	4
I. Introduction	5
II. Accident Evaluation	11
III. Control and Safety System Interaction	19
IV. Operational Limitations	27
V. Potential Errors and Failures	31
VI. Summary and Conclusions	33
Acknowledgments	33
References	34

FIGURES

1. Ground Test Facility	6
2. Ground Test System Installed in Vacuum Chamber	7
3. Ground Test Reactor, as Oriented in Vacuum Chamber	8
4. Simulation Model for 5-kwe Reactor Thermoelectric System	10
5. Maximum Power Resulting From Ramp Insertion at 0.524 ϕ /sec, as a Function of Power Trip Point	14
6. Maximum Power With Period Trip	15
7. Overshoot Following Power Scram as Function of Initiating Ramp Rate and Scram Rate (Startup accident)	18
8. Segment Motion Resulting From Scram During Insertion	20
9. Net Force as a Function of Insertion and Motion of Segment With Failed Phase	22
10. Variation of Work With Segment Insertion	24
11. Recommended Limitations on Segment Position, Beginning of Life	28
12. Change in Segment Position Boundaries Through Reactor Operating Life	30

ABSTRACT

Selected reactor accidents, analyzed by a digital computer simulation program, and the requirements for scram protection, are discussed. Prevention of undesirable interaction between the control and safety systems is described. Operational limitations on segment positions are presented that afford adequate shutdown protection throughout the reactor lifetime. Potential operator errors and equipment malfunctions and failures are discussed.

I. INTRODUCTION

The SNAP 5-kwe Reactor Thermoelectric System is intended to produce 5 kw of electrical power in space with thermoelectric modules heated by flowing NaK from a beryllium-reflected U-ZrH reactor.⁽¹⁾ A ground test of the complete system would have been conducted, to demonstrate the feasibility and reliability of the design, and to determine operating characteristics, if the program had continued. The ground test would have simulated operating conditions in space as closely as possible, including a vacuum environment with heat rejection from the power system by thermal radiation, automatic startup and control, and minimal differences from the space-flight configuration.

Operation of the ground test system would utilize an existing facility, previously used for the SNAP 8 Demonstration Reactor (S8DR) test. The arrangement of this facility is shown in Figure 1. The reactor is located in a well-shielded chamber, provided with high-capacity vacuum pumps and chilled walls. Radiation from the core is reduced to acceptable levels in operating areas by distance and the shielding provided by concrete and earth.

The ground test system is shown, installed in the vacuum chamber, in Figure 2. The reactor is located toward the bottom of the pit, with the conical-cylindrical radiator extending above it. A closeup view of the reactor is shown in Figure 3.

Control of the reactor is provided by motion of two segments in the radial beryllium reflector. For normal control, this motion is slow; for a scram, the segments are driven out rapidly. A backup shutdown mechanism is provided by forcing the two radial reflector halves to swing away, under the combined force of gravity acting on the offset center of mass and torsion springs mounted on the support pivots.

This report discusses some of the potential hazards that have been reviewed for the ground test operation. Evaluation of these hazards lead to certain recommended design requirements and operational limits, that are also discussed.

In considering potential hazards, it is useful to classify them according to the severity of possible results. Three categories may be established:

- 1) Minor — causes temporary interruption in the test program. As an example, a period scram occurring at low power during startup

72-JU20-2-185

Figure 1. Ground Test Facility

72-JY3-2-507A

Figure 2. Ground Test System Installed in Vacuum Chamber

Figure 3. Ground Test Reactor, as Oriented in Vacuum Chamber

introduces a delay for review and restartup, but causes no damage and does not interfere with future operation.

- 2) Major — causes sufficient damage to terminate the test program or lead to later premature termination. This may result from an over-power excursion that ruptures fuel cladding or severely damages the diffusion barrier.
- 3) Catastrophic — potential injury to the operating staff and the public. This would require an accident of sufficient violence to release significant amounts of radioactive material. The safety analysis report (SAR) for operation of the S8DR⁽²⁾ showed that such an accident was not credible. The unique properties of hydride fuel provide a temperature-sensitive and temperature-limiting shutdown mechanism that, in connection with the facility design, prevents release and spread of radioactive material. Such an accident is not considered credible with the present reactor.

6531-5521

Figure 4. Simulation Model for 5-kwe Reactor Thermoelectric System

II. ACCIDENT EVALUATION

This report discusses the hazards studied to date. The study has not been a complete one; however, a variety of safety questions have been answered. The response of the protection system has been studied by means of a dynamic simulation computer program. The other problems studied were: (1) scram motion with a failed actuator phase coil or during normal actuation, (2) falling in of a segment, and (3) operating limitations on segment positions.

The computer simulation program was written by F. J. Halfen, using the IBM modeling language, CSMP. A schematic diagram of the system, as modeled in the program, is shown in Figure 4. Each block represents a temperature node.

The reactor kinetic behavior was calculated as the prompt subcritical multiplication of the delayed neutron source. This approximation is accurate for reactivity up to a few cents less than prompt critical. The maximum reactivity encountered in these simulations was 60¢, so no error was introduced by this approximation. Reactivity was computed from insertion and withdrawal rates, and the temperature coefficients.

The NaK flows in the primary and secondary systems are calculated, based upon the pump thermoelectric module performance as a function of temperature. Similarly, the current generated by the thermoelectric power converter is calculated, based on the primary and secondary side temperatures. Heat rejection is by thermal radiation from the radiator to the environment at an ambient temperature of 100° F, corresponding to the effective temperature of the vacuum vessel walls.

While reactivity additions are actually in discrete steps of $\pm 0.524\text{¢}$, for simplicity, the startup and control phases were converted to equivalent rates. The fuel temperature coefficient was divided among the various fuel nodes in proportion to the square of the relative power.

This simulation model was used to investigate various accident conditions. Startup accidents, in which reactivity is added without regard for the condition of the reactor, have been simulated. Occurrence of such an accident requires that the operating crew be unaware of the true condition of the reactor or unable

to act, as a result of a control system malfunction. In all of the accidents considered, no operator action has been used to halt or modify the development of the accident.

The manual control system is to provide a maximum segment drive rate of 1 step/sec; the automatic controller is limited to one-half of that. A drive rate of 1 step/sec corresponds to a reactivity rate of 0.524 β /sec. A family of accidents, based on this rate, was studied. These include: (1) an unprotected startup accident, in which no protective action is provided, (2) similar startup accidents protected by scrams triggered by high power or short period signals, and (3) an overpower excursion, started at full power.

It should be noted, in considering the results of these simulations, that two values of fuel temperature coefficient have been calculated. One value, -0.07 β /°F, is applicable for static calculations or dynamic simulations in which the time scale is long, compared with transfer of heat into the coolant. The other, -0.10 β /°F, is applicable for transients in which the time scale is short (i. e., the SNAPTRAN transients). In these initial calculations, the less negative value was used, providing a significantly conservative bias. More realistic simulations, using the transient coefficient (which were planned, but not run), would show milder accidents than those discussed in this report.

For the unprotected startup accident, reactivity insertion at 0.524 β /sec was started with the reactor 50 β subcritical, at a power of 0.3 w and a temperature of 100°F. Reactivity insertion continues uninterrupted throughout the accident. The maximum reactivity is 60 β , at which point sufficient energy has been released to overcome the insertion rate and start reducing reactivity. The power continues to increase, however, until a peak of ~ 2 Mw is achieved. As the reactivity continues to decrease, the power decreases. The excursion was terminated in this simulation by a postulated partial disintegration of fuel, occurring when the maximum fuel temperature reaches 1900°F. [This was chosen to be slightly lower than the 1930°F observed for energy probes in the SNAPTRAN-3 experiments,⁽³⁾ because of the slower time scale in the simulated transient.] The energy release to this point was ~ 48 Mw-sec. In comparing this result with SNAPTRAN-3, which disintegrated with 32.5 Mw-sec, it should be noted that the present core mass is more than double that of SNAPTRAN-3, thus requiring more energy to reach the same temperature.

Taking, as an approximation, that the peak power varies inversely with the value of the negative temperature coefficient, use of the more negative fuel coefficient, as discussed earlier, would lead to a calculated energy release of ~ 40 Mw-sec, with the excursion terminated by the temperature defect. Fuel disintegration would probably not occur, in this case. For slower insertion rates, the power rise would occur at lesser reactivities, and the energy release would be reduced.

For such an accident to take place, total inattention by the operating crew, and failure of the instrumented safety systems, are required. The instrumented safety systems consist of period and power-level scrams, both of which are redundant. The operating crew must ignore the power and period indicators and alarms, and the operator must continue to insert the segments. Since this is a startup accident, and startups will be rare, such inattention is extremely unlikely.

More realistic accident results are obtained by including the action of the safety system. The scram signals that are effective for a startup accident are short period and high power. In the simulation model, a delay of 0.5 sec was introduced between exceeding the scram level and the start of protective action. This is a conservative representation of the effects of filtering and instrument time response, which would be considerably shorter than this.

The protective action resulting from a normal scram consists of driving out the reflector control segments at 5 steps/sec, which removes reactivity at a combined rate of $-5.24 \text{ } \beta/\text{sec}$.

The startup accident simulation was calculated with a power scram set at 125% of full power, and with a period scram set at 5 sec and at 10 sec. The peak power achieved when protective action is started by the power level scram was 200 kw; the maximum fuel temperature was 273°F .

The period scrams are more effective in shutting off the excursion. A 5-sec scram level limits the power to 2 kw, while a 10-sec scram level limits the power to 30 w. In both cases, the fuel temperature rise is negligible.

The maximum power occurring for power and period scrams is shown in Figures 5 and 6, respectively. As the power trip point is increased beyond ~ 300 kw, the maximum power does not increase proportionately, because of the

6531-4502

Figure 5. Maximum Power Resulting From Ramp Insertion at 0.524 ϕ /sec, as a Function of Power Trip Point

AI-AEC-13074

Figure 6. Maximum Power With Period Trip

effect of the temperature coefficient for the greater energy releases. For slower insertion rates ($< +0.524 \text{ } \phi/\text{sec}$), the maximum power would be less.

The plot of maximum power against period trip point shows that the power increases rapidly as the trip point moves to shorter periods. The shortest period achieved with a ramp rate of $0.524 \text{ } \phi/\text{sec}$ is 3.35 sec; the temperature coefficient starts reducing reactivity before shorter periods can be attained. Slower ramp rates would result in greater maximum powers.

The choice of period trip point is a compromise between limiting the maximum power and avoiding spurious scram signals. The probability of a spurious scram increases as the trip point is set at longer periods. Thus, it is undesirable to use an unnecessarily conservative trip point.

The probability of a spurious scram is greater at low power, because of the relatively greater random fluctuations in the power. However, it is not necessary to utilize a period trip in the lowest power range, since adequate protection is still provided by a scram occurring at higher power.

At the upper extreme, near normal operating power, the protective advantage afforded by a period scram compared to a power scram becomes minimal. For example, a ramp insertion of $0.5 \text{ } \phi/\text{sec}$, started at full power, causes a power scram at 125%, before the period has become shorter than 200 sec. It is estimated that, for an unlimited insertion of $0.524 \text{ } \phi/\text{sec}$, starting at a moderate power (as would occur in a power adjustment, for example), the protection afforded by a 10-sec period trip and a 125% power trip are equivalent for an initial power of 62 kw. Below this power, the period trip provides more protection; while, above this, the power trip is more protective. For slower insertion rates, the crossover power would be higher.

On the basis of the preceding discussion, it is recommended that the period trip have the following characteristics: (1) bypassed below 10 w, to provide immunity to spurious scrams due to low-level noise, (2) trip at period shorter than 10 sec, to provide significantly better protection than the power scram for a wide range of insertion rates, and (3) bypassed above 10 kw, where the relative advantage over the power scram is reduced, to eliminate a potential source of spurious scrams.

The effect of one segment not being withdrawn on scram was simulated for several insertion rates during startup. The maximum power reached during the excursion, which was terminated by a power scram at 125%, is shown in Figure 7. It can be seen that withdrawal of both segments limits the power more effectively than the single-segment scram, but in none of the cases did any temperatures exceed acceptable values.

In some cases, as would be expected, the rise to peak power was excessively severe, in terms of temperature differences and rates of change.

Scram signals are also provided, if the outlet plenum temperature exceeds 1250° F, or if the primary pump power fails. These were found to be required only in the case of loss of flow. The high outlet temperature is a result of loss of flow, while power failure is a cause. Assuming loss of pump power at full reactor power, the temperature scram limits the outlet temperature to 1350° F, and the peak fuel temperature to 1470° F. The loss-of-pump-power scram limits these temperatures to 1266 and 1340° F, respectively, by acting sooner.

In the unlikely event that the normal scram system should fail to act, the fallaway action of the reflector halves is available as a backup shutdown mechanism. The possibility of thermal shock, resulting from the more rapid shutdown of the reactor caused by use of this mechanism, was investigated by simulating a power scram at 125% following a rise from long-term operation at full power. Falling away of the reflector halves is calculated to be worth -\$18.18. It is estimated that this reactivity removal requires <0.2 sec; for the purpose of this simulation, it was assumed to occur instantaneously. Shutdown by the normal scram (-5.24 ¢/sec) was also simulated for the same conditions, and the results compared.

All temperature differences and rates of change were equally acceptable for both cases. While the backup shutdown (dropping the reflector halves) causes the reactor power to drop to 10% instantly, compared to 46 sec for a similar decrease with the normal scram, the most significant difference between the two cases was only a small difference in the temperature rate in the outlet plenum. With the backup shutdown, this was -86° F/min; with the normal scram, -75° F/min. This difference is unimportant.

Figure 7. Overshoot Following Power Scram as Function of Initiating Ramp Rate and Scram Rate (Startup accident)

III. CONTROL AND SAFETY SYSTEM INTERACTION

The reflector control segments and actuators perform two functions, serving as the operating control system and as the protective system. Interaction between these two functions must be reviewed to insure that the control function does not interfere with the safety function.

Electrical isolation of the control and protection circuits is provided by diodes in the supply lines to the actuators, where the two systems join. These diodes stop pulses from the protection circuit from passing into the control circuit; and, in particular, they avoid the hazard of a short circuit in the control system preventing scram current pulses from operating the actuator.

The stepping sequence of the control circuit requires ~ 1 sec. During startup by manual control, the stepping rate may be as rapid as 1 step/sec, so that an actuator would always be in motion. Therefore, an actuator may be stepping, as required by the control circuit, when a scram occurs.

A scram signal halts the brake release current from the control circuit, and stops the generation of phase coil pulses. At the same time, the scram controller sequencer is started. This consists of the pulse sequence ADCBADCB ..., with the brake being released during the first A pulse. It is likely that the actuator would not be aligned with the A phase when the scram sequence begins, and the scram controller and actuator would be initially out of phase. This causes a loss of torque, which, under certain nonhazardous conditions, may result in the segment falling. This problem will be discussed more fully later. In general, however, this nonsynchronization simply results in a slight variation of the withdrawal rate, compared to the normal condition. This is shown in Figure 8, where the motion of a segment being inserted when the scram occurs is compared for different stages in the stepping sequence. In two of the cases, a partial insertion occurs after the scram signal. Each phase movement requires 50 msec, and is worth one-fourth of a step, or 0.13°. Such a small addition of reactivity for so short a time would have no significant effect on the protection afforded by the scram. In addition, since the control system is restricted to driving only one segment at a time, the other segment is ready for normal scram action.

6531-4505

Figure 8. Segment Motion Resulting From Scram During Insertion

During insertion or withdrawal of a segment, both the stepping torque and the holding torque are provided by the magnetic field linking the rotor and the stator. This field is established by current flowing through a redundant pair of phase coils. If no current flows during the required time interval, no torque is developed, and the actuator is free to turn, in response to external forces.

Loss of current can occur, in principle, for a variety of failures. Some of these are: (1) loss of continuity in both phase coils or the input or output lead, (2) short circuit to ground along the input lead, (3) open circuit failure of the isolation diode, (4) open circuit failure of both power switches in the controller, or (5) failure of the phase sequencer in the controller to turn on the power switches. These failures can be guarded against by careful engineering and fabrication, and by provision of redundant circuit paths, where necessary. In the present design, the occurrence of any of these failures is regarded as unlikely.

The imbalance of the segment weight and the anti-backlash spring force at various stages of compression develops an external force on the segment. This force favors insertion at the fully withdrawn position. As the segment is inserted, the spring force, which inhibits insertion, increases, due to compression of the springs. As the spring force increases significantly beyond the segment weight, a net force favoring withdrawal is developed.

While the behavior of a segment actuator with a failed phase has not been analyzed in detail, qualitative conclusions can be drawn by considering the net force and motion of the segment during the failed phase time interval. The net force, as a function of insertion, is shown in Figure 9. Comparing this net force with torque curves calculated for the drive system suggests the existence of four regions, each having a different segment motion during the failed phase. In the first region, corresponding to the furthest withdrawn position of the segment, the segment will fall in a distance equivalent to about one phase rotation, during the time the phase fails to act during the scram. In the next region, the weight and spring force are nearly balanced, and the segment will not move appreciably. In the third region, the spring force overcomes the weight, and the segment will move out the equivalent of one phase. The furthest inserted region exhibits a motion equivalent to two phases.

STEP	SCRAM WITHDRAWAL	REGION			
		1	2	3	4
1	A ₁	A ₁	A ₁	A ₁	A ₁
	D ₁	D ₁	D ₁	D ₁	D ₁
	(C ₁)	A ₁	D ₁	C ₁	B ₁
	B ₁	B ₀	D ₁	B ₁	B ₁
2	A ₂	A ₁	A ₁	A ₂	A ₂
	D ₂	D ₁	D ₁	D ₂	D ₂
	(C ₂)	A ₁	D ₁	C ₂	B ₂
	B ₂	B ₀	D ₁	B ₂	B ₂
3	A ₃	A ₁	A ₁	A ₃	A ₃
	D ₃	D ₁	D ₁	D ₃	D ₃
	(C ₃)	A ₁	D ₁	C ₃	B ₃
	B ₃	B ₀	D ₁	B ₃	B ₃
4	A ₄	A ₁	A ₁	A ₄	A ₄
	D ₄	D ₁	D ₁	D ₄	D ₄
	(C ₄)	A ₁	D ₁	C ₄	B ₄
	B ₄	B ₀	D ₁	B ₄	B ₄

6531-4506

Figure 9. Net Force as a Function of Insertion and Motion of Segment With Failed Phase

The region boundaries are estimated from torque calculations for an effective coefficient of friction of 0.1. For a higher coefficient of friction, the second region, in which no motion occurs, would be larger. For sufficiently high friction, no movement would occur during the time of the failed phase. This results in a stuck segment. The extreme case occurs for the minimum frictional forces in the drive system. This allows the net force to have the greatest effect.

The resultant motion is listed in Figure 9, assuming, for this case, that Phase C develops no torque. In the list, each phase is identified by its letter, and a subscript indicating the step that it is associated with. (A subscript 0 indicates one step in the opposite direction.) For withdrawal, correct motion results while in the two furthest inserted regions. In the first and second regions, the segment is effectively stuck.

During a normal control step, the duration of each phase is four times as long as during a scram step. Thus, the motion in Regions 1, 3, and 4 will be greater during a normal control step than during a scram step. It is probable that a normal control insertion step in Regions 3 and 4 will be accompanied by outward motion of the segment, if a phase has failed. This contrary motion would be noticeable during operation, and would certainly be detected during periodic testing.

If the fault were determined to be in an accessible component, a repair would be made.

It should be noted that Regions 3 and 4 essentially cover the range of segment positions from initial power operation on. Because of this, partial protection is provided, even if a phase has failed. The faulty segment will move out partway, until the spring force is no longer sufficient to move the segment during the failed phase. The amount of protection afforded under these conditions is reduced for higher values of friction.

The actual behavior of a segment drive system with a failed phase should be determined during pre-operational checkout, to quantify the estimates discussed here.

As previously mentioned, since the anti-backlash springs in the present design do not entirely balance the control segment weight in the fully withdrawn

6531-4507

Figure 10. Variation of Work With Segment Insertion

position, the possibility exists of a reactivity insertion due to a falling segment. The significance of this problem has been evaluated by studying two extreme cases of drive system failure.

In one case, the drive system remains connected mechanically, but an assumed electrical failure causes the actuator to lose its holding torque. Faults leading to such a failure are: (1) energizing the brake release coil without correctly energizing the phase coils, which may be caused by a controller malfunction or by breakage of leads to or from the phase coils, and (2) a mechanical failure of the brake, which would have a similar result.

This type of failure was analyzed by comparing the work components due to gravity, spring compression, and friction as the segment falls in. A modification of the computer program used to calculate the electromagnetic torque requirements for the actuator was used to calculate these work components for 1/4-in. increments of segment travel. These calculations were done, assuming a friction coefficient of 0.1, a ball screw efficiency of 0.9, and a spring temperature of 800° F.

The net work expended for each 1/4-in. increment is shown in Figure 10 for the first inch of travel. Where the net work is negative, the segment is being moved in by gravity. The net work done in falling in to ~0.28 in. (as determined from the intersection of a straight line through the midpoints of the calculated values) results in kinetic energy which is then expended against the springs and friction. The kinetic energy drives the segment in to 0.56 in. Since work must be expended to move the segment past 0.28 in., no free movement will result, if the failure occurs when the segment is inserted beyond this position.

In the other case, the segment is assumed to break loose from the supporting ball nut, and fall freely. Neglecting friction provides an upper limit of 2.32 in. travel from the fully withdrawn position. Reduced movement would occur for partial insertions up to 1.16 in., beyond which no inward movement would occur.

This case was considered in order to provide an absolute upper limit to the possible hazard posed by a falling segment. Since friction is neglected, the segment falls freely past the equilibrium point (where segment weight and spring force are balanced), by a distance equal to the distance the segment was initially

above the equilibrium point. This distance is 1.16 in. when the segment is fully withdrawn. Therefore, the total distance fallen is 2.32 in. Approximating the differential worth of a segment as \$1/in., the maximum reactivity insertion would be \$2.32. If this occurred in the cold shutdown condition, the reactor would still be $\sim 70\%$ subcritical.

No credible failure has been identified that can lead to this free fall case. The maximum torque of the actuator is insufficient to pull the ball nut from the segment. Stalling of the actuator would result, causing loss of synchronization and torque. This could occur, for example, if the limit switch circuit were to fail to signal to the scram controller that the segment was fully withdrawn. While this may allow the segment to fall in, as described in the first case, it would limit the torque applied to the drive system and prevent any damage. The reactor would still be subcritical.

IV. OPERATIONAL LIMITATIONS

Limitations on the independent movement of the two segments are recommended, based on consideration of several safety criteria. (These limitations also exclude combinations of segment positions that could lead to a safety hazard in either of the falling segment failures discussed previously.) These limitations arise because of the dual use of the control segments for control and protection. Control operations that could interfere with performance of the protection function must be avoided.

The recommended limitations, for the beginning of life, are shown in Figure 11. Acceptable segment positions are those within the region bounded by the solid lines. This region is formed by the intersections of boundaries determined by various criteria with the following assumptions:

- 1) Segment differential worth is \$1/in.
- 2) Shutdown reactivity is -\$3, relative to cold critical.
- 3) Reactivity loss from cold critical to full power is \$2.50.
- 4) Prompt reactivity temperature coefficient is $-0.1 \text{ } \$/^{\circ}\text{F}$.

These boundaries, as indicated by numbers in the figure, are:

Boundary 1. Insures that, if one segment becomes stuck, the other has sufficient worth to shut the reactor down to cold critical. This is a somewhat arbitrary choice, but, with the added shutdown capability provided by keeping the temperature above the cold condition, it affords a sufficient shutdown margin.

Boundary 2. Limits reactivity to $5\text{ } \%$ above normal full power operation, thus limiting the prompt temperature increase from full power to 50°F . This is chosen to limit the maximum outlet temperature to 1250°F , assuming a full-power temperature of 1200°F .

Boundary 3. Provides significant protection, if one segment is stuck, by requiring that the inserted reactivity be shared between the two segments. The shape of the boundary is rather arbitrary, but was chosen to provide \$1 shutdown at cold critical, and larger amounts of prompt, temporary relief at higher temperatures.

6531-4508

Figure 11. Recommended Limitations on Segment Position, Beginning of Life

Boundary 4. Reflects that limits are not necessary, so long as the reactor is sufficiently subcritical. In this case, -1.50 has been chosen as an acceptable subcriticality.

Boundary 5. Represents an operational compromise to aid transition from Boundary 4 to Boundary 3, and to share the reactivity control more evenly between the two segments. This boundary avoids the possibility that partial withdrawal of a segment would be required as the other is inserted to go from Boundary 4 to Boundary 3.

It is expected that these limits would not unduly inhibit normal operations. The tightest limit imposed is that the two segments must be balanced within 0.5 in. at full-power operation. A much wider span, 1.75 in., is available with the reactor at a temperature near 600°F , if it is desired to check segment calibrations over such a range.

During the course of operation, it is expected that a steady loss of reactivity will occur. As a result, the segment positions required to maintain criticality will move inward. The boundaries limiting permissible segment positions must be revised periodically, to account for this. This revision should be done annually or semiannually, using the known critical conditions and the criteria discussed for the boundaries. The estimated progression of the boundaries, as determined at the beginning of each year of operation and at the end of life, is shown in Figure 12. So long as the long-term reactivity change is negative, boundaries established at any time will be conservative at any subsequent time. A positive long-term drift would require more frequent revision of the boundaries.

6531-4509

Figure 12. Change in Segment Position Boundaries Through Reactor Operating Life

AI-AEC-13074

V. POTENTIAL ERRORS AND FAILURES

A very limited review of errors and failures potentially leading to hazardous conditions was conducted. This review considered both physical failures and operator errors, but only in the limited domain of the reactor control system.

With regard only to this system, two types of operator error can cause problems. One type is the continued insertion of the segments beyond a safe position. This may result from operator inattention or distraction, or a bad estimate of the critical position, and would be possible only during a startup or an increase in power from low-power operation. Few startups are expected, and the time required is short, so that the chance of the operator not paying proper attention is very unlikely. Changes in power require operator attention for a very short time, and have a specific goal or target power, so that operator inattention is even less likely.

The other potentially hazardous operator error is the incorrect actuation of the segment drive switch, to insert a segment when withdrawal is desired. The consequences of this error depend upon the circumstances under which it occurs. Because of the slow maximum insertion rate allowed by the actuator drive circuit, the information available to the operator regarding segment position and reactor power and period, and the involvement of other persons in the operation, a large reactivity insertion is unlikely to result from such an error. In addition, a careful operator qualification, training, and testing program, the use of two-tone audible signals to indicate segment stepping, and "push-in, pull-out" actuator switches to facilitate the operator in relating his actions to the motion of the segments, will all help guard against the occurrence of such an error.

Considering component or system failures in the control system as a whole leads to a similar identification of only two types of potentially hazardous malfunction: (1) continued insertion, and (2) insertion instead of withdrawal. Each segment step is accompanied by an audible tone, to signal the action to the operating crew. Thus, segment motion is not likely to occur without the operator being aware of it. Since there are three independent control systems (manual, automatic, and computer), the operator can switch from a faulty system to an alternate system, to avoid excessive reactivity insertion. Provision of two different tones, one to indicate insertion, the other to indicate withdrawal, would

help to alert the operator to a malfunction resulting in insertion rather than withdrawal. Careful design, with redundant components combined so that likely failures produce nonhazardous results, must be exercised to reduce the chance of hazardous malfunctions.

VI. SUMMARY AND CONCLUSIONS

While this hazards evaluation has necessarily been incomplete, a variety of potential hazards have been investigated. These included: (1) hypothetical start-up accidents, with and without safety system protection, (2) the dependence of the safety system performance on trip levels, (3) possible causes of reactivity accidents, and (4) failure of a segment actuator system. Other subjects are: (1) the interaction of the safety and control systems, and the need for isolation, (2) required limitations on segment positions, and (3) the action of the backup shutdown mechanism.

The simulation case run for the hypothetical startup accident showed that, without safety system protection, some fuel disintegration would occur; it is probable that use of a more realistic temperature coefficient in the simulation would show this not to occur. Use of a period trip at 10 sec in the intermediate channel range, and a power trip at 125%, were shown to provide adequate protection for all accidents that were considered. The possible accident causes that were identified were shown qualitatively to have low probability. Only one of the various forms of failure of a segment actuator system, an incredible mechanical failure, was found to pose any serious hazard.

Possible interaction of the control and safety systems was shown to not impede the scram action. Electrical isolation of the actuator power circuits was recommended. Limitations on the positions of the two segments were specified that insure adequate shutdown margins, and also eliminate any hazard from failure of an actuator. The action of the backup shutdown mechanism was shown to not result in any unacceptable thermal transients, so that it would be a usable scram mechanism, if required.

No problems were identified which would indicate a potential hazard that is not protected against by careful design and operation.

ACKNOWLEDGMENTS

Many of the particular problems discussed in this report benefitted from contributions by E. J. Donovan, F. J. Halfen, L. M. Maki, T. S. Nakae, and R. J. Thexton.

REFERENCES

1. J. H. Van Osdol, "5-kwe Reactor Thermoelectric System Summary," AI-AEC-13096 (to be published)
2. W. C. Miller, "Safety Analysis Report, SNAP 8 Development Reactor," NAA-SR-Memo-11373 (1967)
3. J. F. Jackson, W. F. Rhoades, and L. I. Moss, "Analysis of SNAPTRAN-1 and -2 Reactor Kinetics Experiments," NAA-SR-11850 (1967)