CONF-791103--71

GA-A15499

MASTER

TREATMENT OF OPERATOR ACTIONS IN THE HTGR RISK ASSESSMENT STUDY

by

K. N. FLEMING, F. A. SILADY, and G. W. HANNAMAN

DECEMBER 1979

GENERAL ATOMIC COMPANY

GA-A15499

TREATMENT OF OPERATOR ACTIONS IN THE HTGR RISK ASSESSMENT STUDY

by

K. N. FLEMING, F. A. SILADY, and G. W. HANNAMAN

This is a preprint of a paper presented at the ANS Winter Meeting, San Francisco, California, November 11-16, 1979, and published in the Transactions.

Work supported by
Department of Energy
Contract DE-AT03-76ET35300

GENERAL ATOMIC PROJECT 6400
DECEMBER 1979

GENERAL ATOMIC COMPANY

The purpose of this paper is to present methods for the treatment of operator actions, developed in the AIPA risk assessment study (Ref. 1), and to give some examples of how these methods were applied to the analysis of potential HTGR accidents. Realistic predictions of accident risks required a balanced treatment of both beneficial and detrimental actions and responses of human operators and maintenance crews.

The essential elements of the human factors methodology used in the AIPA study include event tree and fault tree analysis, time-dependent operator response and repair models, a method for quantifying common cause failure probabilities, and synthesis of relevant experience data for use in these models.

The predominantly beneficial operator actions such as those that can be taken to terminate or recover from an accident or mitigate its consequences are treated with the use of a simple time-dependent model of the form

$$P(t) = 1 - e^{-t/MTOR} \leq P_o < 1 \qquad (1)$$

where $P(t)$ is the probability of completing the specified action by time t, P_o is an upper limit on $P(t)$, MTOR is the mean time for operator response, and t is the time available to complete the action, often dictated by the timing of physical processes during the accident. Values for P_o and MTOR are estimated from experience data, simulator test data, and subjective judgments. A model similar to (1) is used for the repair of failed equipment.

Human errors in operating, testing, and maintaining equipment that cause component or system failures are treated explicitly in the system fault tree analyses and implicitly in the method used to model the reliability characteristics of common cause failures in redundant systems (Ref. 2) (Beta factor method). Implicit treatment arises from the use of failure rate and common cause failure experience data which include contributions from human errors (Ref. 3).

The application of AIPA human factor methods to an HTGR accident involving core heatup (Ref. 1) is summarized in Table 1. The slow evolution of the accident, an inherent characteristic of the HTGR because of its large core heat capacity and low power density, provides ample time for operator actions to influence the accident progression. In this regard, the time-dependent operator response model plays an important role in obtaining realistic estimates of operator action probabilities in 7 of the 9 events listed in Table 1.

An important variable in the operator response model is the time available for operator action, which is determined from computer models that simulate the physical processes of the accident and the transient response of key components. In this sequence, the times available for operator actions are determined by the transient thermal and structural response of the reactor core, PCRV internals and concrete, heat transport equipment inside the PCRV, and, finally, the containment structure (Refs. 4, 5).

Table 1 also includes specific operator actions identified by fault tree analysis and implicit treatment of operator, test, and maintenance errors with use of the Beta factor method of common cause failure analysis. Most of the former and all of the latter in Table 1 have an increasing effect on the risk estimated for the accident. In view of the positive influence of the actions treated using the time-dependent models, the overall consideration of operator actions in Table 1 is balanced.

TABLE 1
OPERATOR ACTIONS ALONG AN HTGR CORE HEATUP ACCIDENT SEQUENCE

Time (hr)	Event Along Accident Sequence	Operator Actions Affecting Event Probability	Impact on Event Probability[a]	Impact on Risk of Accident[a]	Methods Used to Estimate Impact on Event Probability[b] F	B	T	Components Whose Response Determines Time Available for Operator Action
0	Loss of condenser function	Operator, test, and maintenance errors	+	+	X	X		
0	Reactor trip	Trip control rods, reserve shutdown system	+	-	X		X	Control rod drives, control rod, and reserve shutdown system guide tubes
		Operator, test, and maintenance errors	-	+	X	X		
0-5	Core cooldown on main loops	Start auxiliary boiler, valve in condensate tanks	+	-	X		X	Main steam system
		Operator and maintenance errors	-	+	X	X		
5	CACS[c] fails to start	Operator, test, and maintenance errors	+	+	X	X	X	Lower cross ducts, heat exchangers, circulators
5-20	Unsuccessful attempts to restore core cooling	Repair and restart of main loops and CACS	-	-	X		X	Lower cross ducts, heat exchangers, circulators
35	PCRV[d] depressurizes, containment isolation valves close	Operation and maintenance errors	-	+	X	X		
		Repair and manual isolation valve closure	+	-	X		X	Primary coolant system, PCRV relief valve
110	PCRV liner cooling system fails	Operator and maintenance errors	+	+	X	X	X	Upper thermal barrier, PCRV liner, top head and sidewall concrete
210-310	Containment water-gas burning prevented	Inject helium and nitrogen	+	-	X		X	PCRV top head and side-wall concrete, containment atmosphere
		Deenergize spark-producing circuits	+	-	X		X	PCRV top head and side-wall concrete, containment atmosphere
310	Containment over-pressurizes							

(a) + indicates increase; - indicates decrease.

(b) F = fault tree analysis.
B = beta factor method of common cause failure analysis.
T = time-dependent operator response/repair model.

(c) CACS = core auxiliary cooling system.

(d) PCRV = prestressed concrete reactor vessel.

Although the consideration of human factors in the AIPA study was balanced between beneficial and detrimental actions in line with the objective to make realistic risk estimates, certain elements of the treatment may be viewed as conservative and still others as optimistic. Among the former are the use of maintenance data to quantify the timing of operator actions during accident situations, and the omission of consideration of (1) human ingenuity to terminate the accident and (2) mobilizing experts and technicians to supervise long-term, external actions to mitigate the accident consequences such as those at Three Mile Island. The most important class of actions whose omission can lead to underestimates of accident risk appear to be errors of commission that either initiate accidents or compound their consequences and those that cause failure of multiple, otherwise independent, systems.

REFERENCES

1. "HTGR AIPA Status Report, Phase II Risk Assessment," DOE Report GA-A15000, General Atomic Company, April 1978.
2. Fleming, K. N., and P. H. Raabe, "A Comparison of Three Methods for the Quantitative Analysis of Common Cause Failures," Proceedings of the ANS Topical Meeting on Probabilistic Safety, Los Angeles, California, May 8-10, 1978.
3. Hannaman, G. W., and A. P. Kelley, Jr., "Synthesis of Experience Data for Risk Assessment and Design Improvement of Gas-Cooled Reactors," Proceedings of the ANS Topical Meeting on Probabilistic Safety, Los Angeles, California, May 8-10, 1978.
4. Wakefield, D. J., T. D. Dunn, and F. A. Silady, "PCRV Integrity During HTGR Core Heatup," Trans. Am. Nucl. Soc. 28, 405 (1978).
5. Deremer, R. K., et al., "Primary Coolant System Response to an HTGR Core Heatup," Proceedings of the ANS Topical Meeting on Thermal Reactor Safety, Sun Valley, Idaho, August 1977, p. 1-457.

SLIDES PRESENTED AT THE MEETING

TREATMENT OF OPERATOR ACTIONS IN THE HTGR RISK ASSESSMENT STUDY

BY

K. N. FLEMING
F. A. SILADY
G. W. HANNAMAN

WHAT IS THE IMPACT OF OPERATOR ERROR ON NUCLEAR PLANT SAFETY?

1978 LEWIS REPORT NUREG/CR–400:

"... THE RSS RISK ASSESSMENT DEPENDS SIGNIFICANTLY UPON THE NUMERICAL VALUES OF CERTAIN HUMAN ERROR RATES. ALSO, THE ROLE OF OPERATORS IN MITIGATING THE CONSEQUENCES OF EQUIPMENT FAILURES SHOULD BE IMPORTANT."

1979 KEMENY REPORT:

"... THE EQUIPMENT WAS SUFFICIENTLY GOOD; EXCEPT FOR HUMAN FAILURES, THE MAJOR ACCIDENT AT TMI WOULD HAVE BEEN A MINOR INCIDENT."

1979 GERMAN RISK STUDY:

"HUMAN ERROR IS RESPONSIBLE FOR MOST HYPOTHESIZED ACCIDENTS LEADING TO CORE MELT."

CONCLUSION: THE HUMAN IMPACT ON PLANT SAFETY IS SIGNIFICANT AND MUST BE CONSIDERED IN A BALANCED VIEW WITH BOTH FAVORABLE AND UNFAVORABLE INFLUENCE.

- OBJECTIVE OF AIPA STUDY WAS TO PROVIDE A REALISTIC ASSESSMENT OF THE PUBLIC RISK THAT STEMS FROM OPERATION OF THE HTGR.
- TO ACHIEVE THAT OBJECTIVE, OPERATOR ACTIONS WERE CONSIDERED.
- EXPLAIN HOW THIS WAS DONE.

CONSIDERATIONS OF HUMAN IMPACTS ON ACCIDENT SEQUENCES

- FAVORABLE AND UNFAVORABLE HUMAN ACTIONS
- ERRORS BEFORE ACCIDENT
- OPERATOR AND MAINTENANCE MITIGATION ROLES DURING ACCIDENTS
    - INFORMATION AVAILABLE FOR DIAGNOSING
    - EASE OF FINDING INFORMATION
- ERRORS DURING ACCIDENT SEQUENCE

COMPARISON OF SOME HUMAN TRAITS WITH THOSE OF SYSTEM AND COMPONENTS

	FAVORABLE	UNFAVORABLE
HUMAN BEING		
	• IMPROVISE	• NOT FULLY RELIABLE
	• IMAGINATION	• EMOTIONAL
	• SELF-CORRECTING	• INCONSISTENT
	• ADAPTABLE/FLEXIBLE	• STRESS/MONOTONY
	• ACT ON NONQUANTIFIED PHENOMENON	• SLEEP
MECHANICAL/ELECTRICAL COMPONENT		
	• HIGHLY RELIABLE	• MAINTENANCE
	• CONSTANT PERFORMANCE	• COSTLY
	• MULTI-FUNCTIONAL	• PREPARATORY WORK
	• REPETITIVE	• FUNCTIONALLY RESTRICTED
	• AVAILABLE 24 HOURS/DAY	• NOT SELF-CORRECTING

CONSIDER BLEND OF THE MAN–MACHINE INTERFACE IN DEVELOPING THE MOST FAVORABLE DESIGN

ELEMENTS OF HUMAN FACTORS METHODOLOGY IN AIPA STUDY

- EVENT TREE/FAULT TREE ANALYSIS WITH OPERATOR AND MAINTENANCE ERRORS OF COMMISSION AND OMISSION CONSIDERED
- TIME–DEPENDENT OPERATOR RESPONSE MODEL
- TIME–DEPENDENT REPAIR MODEL
- QUANTIFICATION OF COMMON CAUSE FAILURES (30–50% HUMAN ERROR)
- SYNTHESIS OF EXPERIENCE DATA FOR USE IN MODELS

TABLE 1
OPERATOR ACTIONS ALONG AN HTGR CORE HEATUP ACCIDENT SEQUENCE

Time (hr)	Event Along Accident Sequence	Operator Actions Affecting Event Probability	Impact on Event Probability[a]	Impact on Risk of Accident[a]	Methods Used to Estimate Impact on Event Probability[b] F	B	T	Components Whose Response Determines Time Available for Operator Action
0	Loss of condenser function	Operator, test, and maintenance errors	+	+	X	X		
0	Reactor trip	Trip control rods, reserve shutdown system	+	-	X		X	Control rod drives, control rod, and reserve shutdown system guide tubes
		Operator, test, and maintenance errors	-	+	X	X		
0-5	Core cooldown on main loops	Start auxiliary boiler, valve in condensate tanks	+	-	X		X	Main steam system
		Operator and maintenance errors	-	+	X	X		
5	CACS[c] fails to start	Operator, test, and maintenance errors	+	+	X	X	X	Lower cross ducts, heat exchangers, circulators
5-20	Unsuccessful attempts to restore core cooling	Repair and restart of main loops and CACS	-	-	X		X	Lower cross ducts, heat exchangers, circulators
35	PCRV[d] depressurizes, containment isolation valves close	Operation and maintenance errors	-	+	X	X		
		Repair and manual isolation valve closure	+	-	X		X	Primary coolant system, PCRV relief valve
110	PCRV liner cooling system fails	Operator and maintenance errors	+	+	X	X	X	Upper thermal barrier, PCRV liner, top head and sidewall concrete
210-310	Containment water-gas burning prevented	Inject helium and nitrogen	+	-	X		X	PCRV top head and sidewall concrete, containment atmosphere
		Deenergize spark-producing circuits	+	-	X		X	PCRV top head and sidewall concrete, containment atmosphere
310	Containment overpressurizes							

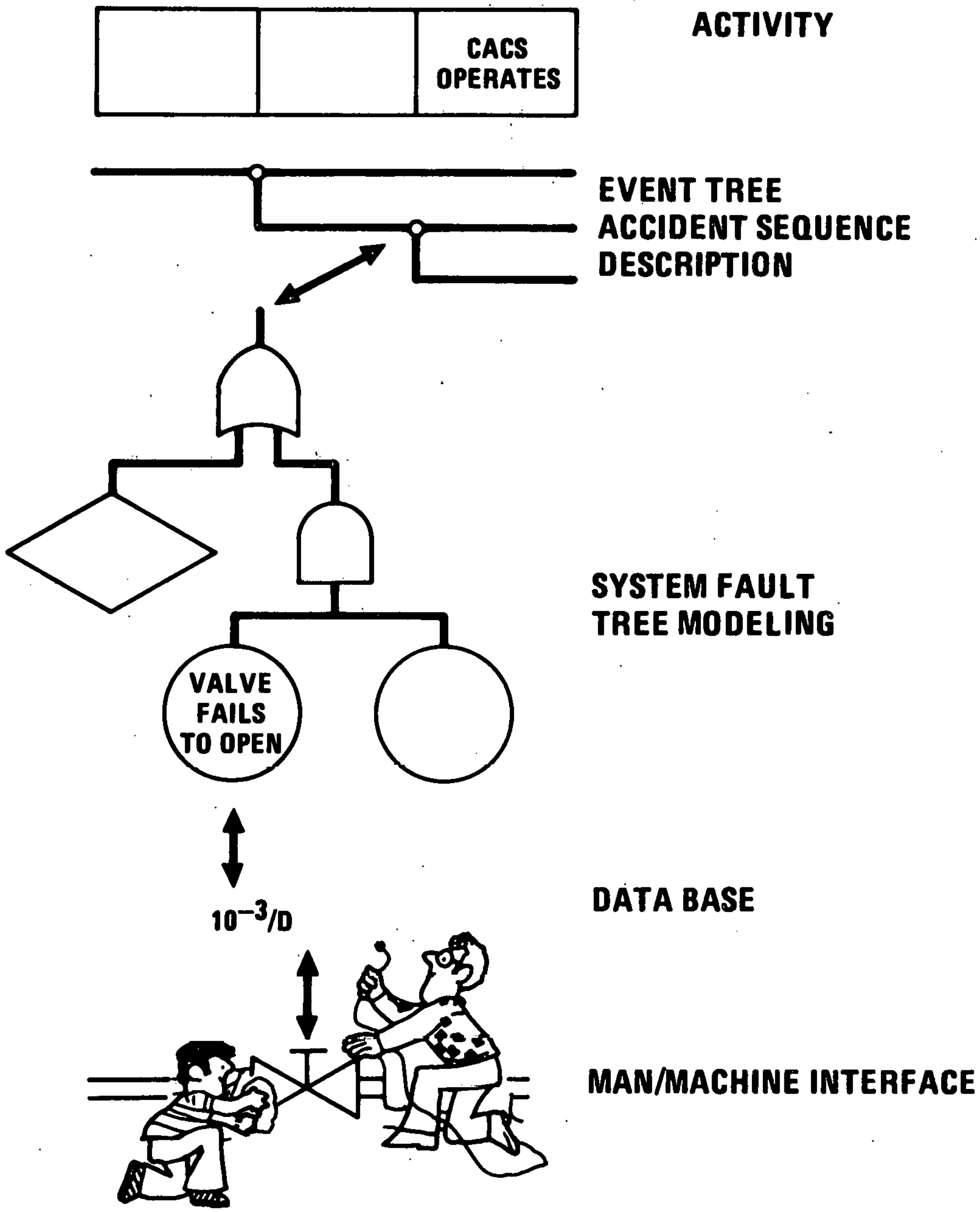
(a) + indicates increase; - indicates decrease.

(b) F = fault tree analysis.
B = beta factor method of common cause failure analysis.
T = time-dependent operator response/repair model.

(c) CACS = core auxiliary cooling system.

(d) PCRV = prestressed concrete reactor vessel.

PROBABILISTIC METHODOLOGY FOR ACCIDENT INITIATION AND PROGRESSION ANALYSIS (AIPA)



EXAMPLES OF UNFAVORABLE OPERATOR ACTIONS THAT COMPOUND ACCIDENT CONSEQUENCES

1. DURING AN ATTEMPT TO VENT THE CONTAINMENT DURING A CORE HEATUP, A VALVE IS OPENED TOO QUICKLY, RESULTING IN A BLOW-OUT OF THE VENT FILTER AND AN INCREASE IN RADIOACTIVITY RELEASED.

2. GAGS ARE INADVERTENTLY LEFT IN PCRV RELIEF VALVES DURING TEST. LATER DURING CORE HEATUP, RELIEF VALVES FAIL TO OPEN, CAUSING PCRV OVERPRESSURE.

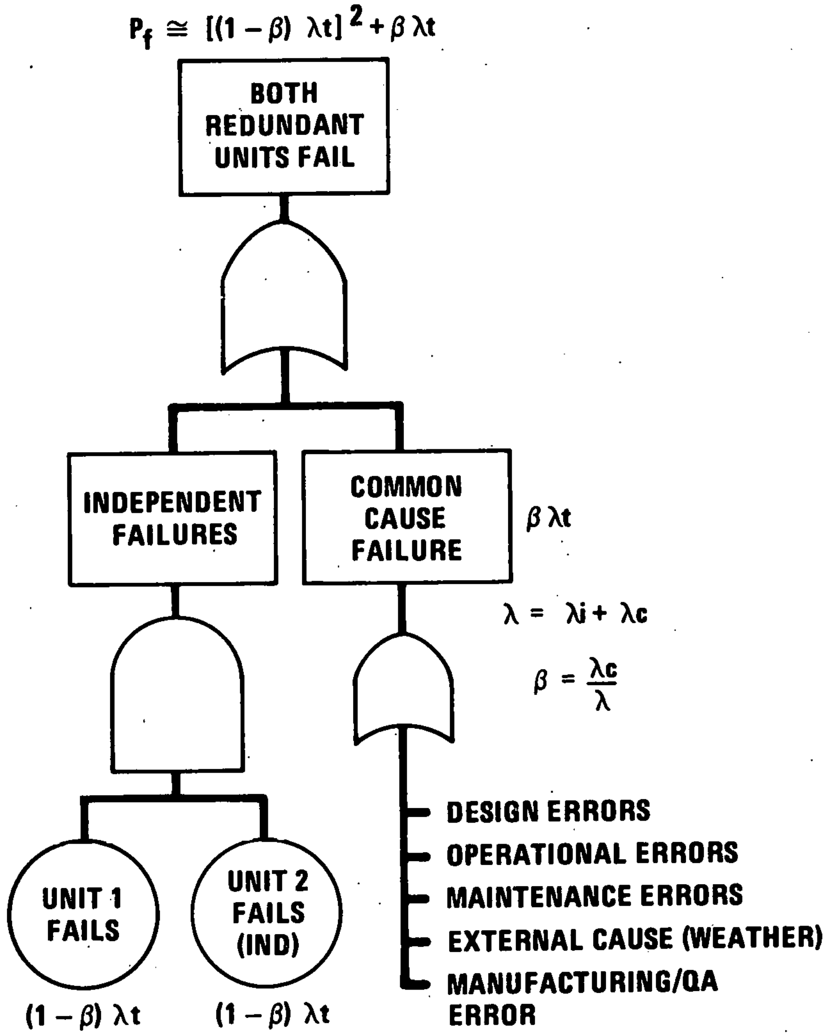
3. AFTER A REHEATER TUBE LEAK AND SUCCESSFUL ISOLATION, OPERATOR INADVERTENTLY OPENS A DRAIN VALVE, ALLOWING ESCAPE OF RADIOACTIVITY OUTSIDE CONTAINMENT.

4. FOLLOWING A LOSS OF MAIN LOOPS AND FAILURE TO TRIP REACTOR, OPERATOR ATTEMPTS TO START CACS BEFORE RESERVE SHUTDOWN SYSTEM ACTIVATED. CACS HEAT LOADS EXCEED REMOVAL CAPABILITY, RESULTING IN CORE HEATUP.

TIME–DEPENDENT OPERATOR RESPONSE

EVENT	OPERATOR ACTION	TIME ALLOWED IN HTGR	LIMITING PROBABILITY	MEAN RESPONSE TIME
REACTOR TRIP	TRIP REACTOR IF AUTOMATIC SYSTEM FAILS	3 MINUTES	0.97	30 SECONDS
	$Ps(T) = 0.97\ (1 - e^{-180/30}) = 0.97$			
CACS START	MANUAL START OF DIESEL GENERATOR IF AUTOSTART CIRCUIT FAILS	20 MINUTES	0.98	15 MINUTES
	$Ps(T) = 0.98\ (1 - e^{-20/15}) = 0.72$			

COMMON CAUSE FAULT TREE MODEL



EXAMPLES OF HUMAN OPERATOR ERRORS IN DATA BASE
FACTORED INTO ESTIMATES OF β AND λ

- REDUNDANT SET OF PUMPS LEFT VALVED OUT AFTER TEST.
- REDUNDANT SET OF PRESSURE SWITCHES MISCALIBRATED.
- ATTEMPT TO MODIFY PROTECTION SYSTEM AT POWER CREATES MULTIPLE TRIPS.
- TEST JUMPERS ON SEVERAL INSTRUMENT CHANNELS PREVENTING TRIP.
- REDUNDANT INSTRUMENT CHANNELS TESTED AT SAME TIME.

HUMAN IMPACT FINDINGS IN THE HTGR STUDY

- PRE–ACCIDENT HUMAN ERRORS ARE SIGNIFICANT CONTRIBUTORS TO THE HTGR RISK PROFILE (COMMON CAUSE FAILURE DOMINANCE).
- REPAIR DURING AN ACCIDENT SEQUENCE WAS ENHANCED BY LONG TIMES ALLOWED BEFORE DAMAGE (UNIQUE FEATURES OF PLANT).
- THE HTGR IS FORGIVING TO HUMAN ERRORS OF COMMISSION BECAUSE OF SLOW THERMAL RESPONSE OF CORE AND HENCE LONG TIME WINDOWS ARE AVAILABLE FOR STABILIZING THE CONDITION.

RECOMMENDATIONS FOR FURTHER WORK

- OBTAIN OPERATOR RESPONSE TIMES FROM SIMULATORS OR OPERATING EXPERIENCE.
- DELINEATE SPECIFIC AND GENERAL OPERATOR ACTIONS UNDER ACCIDENT CONDITIONS FOR OPERATOR TRAINING.
- ESTABLISH SAFETY INSTRUMENTATION PRIORITIES FOR OPERATORS TO BE CONSIDERED IN CONTROL ROOM DESIGN.
- EVALUATE SENSITIVITY OF HUMAN IMPACTS ON PLANT SAFETY.
- DEVELOP IMPROVED MODELS FOR TREATING ERRORS OF COMMISSION.

GENERAL ATOMIC

GENERAL ATOMIC COMPANY
P. O. BOX 81608
SAN DIEGO, CALIFORNIA 92138