CONF-760435--1

TIGER IN THE FAULT TREE JUNGLE*

(Submitted for presentation at the Seventh Annual Pittsburgh Conference on Modeling and Simulation, April 26-27, 1976, Pittsburgh, Pennsylvania.)

Paul Rubel

Send correspondence to:
Paul Rubel
Oak Ridge National Laboratory
P.O. Box Y
Building 9201-3, MS-7
Oak Ridge, Tennessee 37830
Telephone (615)483-8611, Ext. 3-7449

*Research sponsored by the U.S. Energy Research and Development Administration under contract with the Union Carbide Corporation.

DRAFT
PRubel
4/9/76

ABSTRACT

~~TIGER IN THE FAULT TREE JUNGLE~~

There is yet little evidence of serious efforts to apply formal reliability analysis methods to evaluate, or even to identify, potential common-mode failures (CMF) of reactor safeguard systems. The prospects for event logic modeling in this regard are examined by the primitive device of reviewing actual CMF experience in terms of what the analyst might have perceived a priori. Further insights of the probability and risks aspects of CMFs are sought through consideration of three key likelihood factors: (1) prior probability of cause ever existing, (2) opportunities for removing cause, and (3) probability that a CMF cause will be activated by conditions associated with a real system challenge. It was concluded that the principal needs for formal logical discipline in the endeavor to decrease CMF-related risks are to discover and to account for strong "energetic" dependency couplings that could arise in the major accidents usually classed as "hypothetical". This application would help focus research, design and quality assurance efforts to cope with major CMF causes. But without extraordinary challenges to the reactor safeguard systems, there must continue to be virtually no statistical evidence pertinent to that class of failure dependencies.

DRAFT
PRubel
4/8/76

INTRODUCTION

We tend to lose sight of the fact that the basic building block of our present sophisticated reliability analysis methods is the random independent failure of a component in a system. This is clearly a simplistic view of real-world failures. Nevertheless, it has proven enormously useful in the development of successful systems so complex that they could not have been attempted thirty years ago. Surely a major factor in that success is that the engineering of reliable systems has followed from the theory. A particular aspect of this is pertinent to the theme of this paper, ~~mainly~~ namely, that deliberate efforts are made to achieve physical independence of redundant system parts, not just from harmful conditions within systems but from external effects as well.

A measure of the achievement through traditional reliability methods, and also their limitations, is the emergence of dependency-coupled event sets as a relatively important source of system failures. These, too, have been reduced in number and potency through careful engineering and quality assurance. Yet, the occasional appearance of an unexpected strong dependency failure link in a vital system is cause for concern that other such couplings may exist, possibly capable of defeating protective systems at crucial times. Such defeats of redundant system functions are termed common-mode failures (CMFs). They are the lurking "tigers" to which the title alludes.

Common-mode failures in nuclear power plants have been receiving a great deal of attention in recent years. We may ask why, then, has so little emerged in the way of new analytical methods or adaptations of

old ones that specifically address the CMF problem? Some insights of the considerable problem difficulties are sought here through a selective review of reactor plant CMFs, experienced and postulated, from the standpoint of whether established analytical methods could conceivably (1) identify and evaluate the actual dependency couplings a priori so positively as to justify corrective action; (2) call out the importance of special classes of dependency coupling on which to concentrate design and QA attention; and/or (3) support evaluation or prediction of the general risk stemming from CMFs.

In most of the CMFs examined, it appeared that fault trees would not have contributed materially to discovery of the fairly obvious specific causes. This confirms the view, held by many engineers, that tree-logic analysis is not a substitute for engineering analysis. Moreover, the generally low frequency of actual CMFs suggests that formal tree analysis would be largely redundant where high standards of conventional engineering and quality assurance prevail. But further consideration of the hypothetical major accidents discloses real and compelling needs to apply formal logic in the search for dependency couples. These are with regard to the "complex energetic" couplings whereby, for example, a weather extreme or a major component failure can directly impact many components, whose responses—in some cases failures—could, in turn, affect other components. To explore and account for such effects methodically then becomes a prerequisite for focussing the engineering and QA efforts by which components will be developed to withstand unusual stresses, and suitable backup defences deployed. Another promising adaptation seen for logic methods is with regard to minimizing the potential for, and effects of, human errors under duress of plant upset conditions.

GENERAL CMF PROBABILITY AND RISK MODEL

The prime concern over CMFs is how much they contribute to plant accident risks. Some appreciation of the essential nature of CMF-related risks—and of their large uncertainties—can be gained by examining the elemental factors comprising the risk probability. Accordingly, a simple risk model is proposed which expresses CMF dependency couplings as conditional probabilities. The CMF counterparts of component test, repair, and reliability growth in the "random-independent" reliability model are embedded in the expression.

The basic risk model for a particular kind of failure, common-mode or independent, occurring in conjunction with a particular initiating event is:

$$(\text{Risk Rate})_{ab} = \beta_a \left[P_b \middle| a\right] \left\{\sum_k P_{abk} D_{abk}\right\} ,$$

where,

β_a = rate of occurrence of initiating event or condition "a",

$\left[P_b \middle| a\right] \equiv \left[P_b(t) \middle| a\right]$ = probability of failure type "b", given "a"

= $P_b(t)$, if failure type "b" is independent of "a", i.e., the random failure probability,

$P_{abk} \equiv P_{abk}(t)$ = probability of an outcome "k" which could follow from "a" and "b",

D_{abk} = consequences of the outcome "k".

The term $\left(P_b|a\right)$, representing a CMF, can be expanded to represent various causes and opportunities for correction before "a" occurs:

$$\left(P_b|a\right) = \left[\begin{array}{l}\text{P:I - CMF Susceptibility is original or is introduced before "a" occurs}\end{array}\right] \times \left[\begin{array}{l}\text{P:II - CMF Susceptibility is } \underline{\text{not}} \text{ discovered and corrected before "a" occurs}\end{array}\right] \times$$

1. Design
2. Equipment selection
3. Manufacture
4. Installation
5. Miscalibration
6. Defeat by improper operation or maintenance

(Above apply to independent as well as dependent failures)

a. Tests, inspections*
b. Actual failure occurs under benign conditions; cause then corrected
c. Similar failure occurs remotely; common cause recognized, reported and corrected, e.g., by revised "task specs."

(*Similar to repair in reliability theory when no actual system improvement is made; if a "permanent fix" is made, it contributes to reliability "growth")

(CMF cause discovery more subject to chance than is ordinary component failure which is subject to regular test)

$$\left[\begin{array}{l}\text{P:III - CMF Susceptibility is "activated" by conditions associated with event(s) "a"}\end{array}\right]$$

i. For original or "constant" susceptibility, (P:III)<1 if it is not certain that "a" will induce CMF

ii. For progressive deterioration that increases CMF susceptibility with time, (P:III)<1 until CMF certainty threshold is reached; this corresponds to "wearout" in reliability model of independent failures.

It should be apparent that the ~~single~~ simple product above does not convey the actual branching of conditional probabilities of which $\left(P_b \middle| a\right)$ is comprised. For a particular CMF, "b", the more rigorous expression is:

$$\left(P_b \middle| a\right) = \sum_{\ell}(P:I)_{\ell}\left\{\sum_{m}(P:II)_{m}\left[\sum_{n}(P:III)_{n}\right]\right\} ,$$

where ℓ, m, and n represent susceptibility, prior correction and activation event probabilities pertinent to "b" and "a" together.

Not only are the sources of CMF-related risk evident in the above expressions, but also the opportunities to reduce such risks. Moreover, the latent nature of many CMF "susceptibilities" suggests that, even when given the proper initiating conditions, there may be a wide range of uncertainty regarding CMF occurrence probability. The total risk rate, independent and CMF-related, includes an almost limitless number and variety of condition-susceptibility couples, all summarized in the deceptively simple expression:

$$\text{Risk Rate} = \sum_{i}\beta_i\left[\sum_{j}\left(P_j \middle| i\right)\left(\sum_{k}P_{ijk}D_{ijk}\right)\right] ,$$

where i and j stand, respectively, for all the individual "a" and "b" in the preceding expressions.

CMF Experience

A recent study[1] at ORNL reviewed reactor CMF experience and classified CMFs according to type of dependency coupling mainly responsible. Most of the cases selected to represent dependency classifications in the report of that work are summarized here in Table 1. A few other examples from industrial experience are included in the table to illustrate particularly obscure couplings.

The potential risk probability elements are then rated subjectively for most of the cases in Table 1, according to the CMF probability expression described in the preceding section. Thus, a subjective estimate is made of (P:I), the prior probability of a dependency having existing; of (P:II), the probability such a dependency is not removed before challenge; and of (P:III), the probability that a safety-significant challenge of the required kind would "activate" the dependency to cause an actual CMF. Accident risks associated with each case are discussed.

The likelihood estimates represent no more than my own cursory evaluation of conditions pertinent to events which did or could have occurred. I attributed rather high likelihoods to the (P:I)s in order to allow for other possible errors which could have created the same kind of dependency couple that was observed. However, most of the (P:I) × (P:II) products reflect the opinion that there is little likelihood that significant couples will remain until an "activating" challenge occurs, a situation which seems consistent with operating experience. The risk discussions point out

Table 1. Common-mode failure experience: Risk Aspects

CMF event description* (see Ref. 1 unless otherwise noted)	Dependency couplings	(P:I) Estimate of prior probability of dependency ever existing	(P:II) Estimate of probability that dependency is not removed before serious challenge	(P:III) Estimate of probability that safety-significant challenge will "activate" dependency to cause actual CMF	Accident risk Implications
1. Two series-redundant valves are intended to prevent flow of nitrogen to reactivity control activator. Leakage caused improper motion of activator, which might have resulted in a reactivity transient if incident had not occurred during shutdown tests.	--Component application --System design (Each valve requires appreciable ΔP to seat; correct leak-tight closure of either valve, or its small leak, precludes adequate seating ΔP for the other valve.)	0 to 0.25 for any similar application (to avoid error positively requires that designer fully understands the ΔP requirement.)	0.2 to 0.5	1.0 (CMF is source of challenge and removes protection)	(Risk was economic)
2. Several electrical relays in one installation stuck closed during plant preoperational testing.	--Component common manufacturing defect (primer applied to pole pieces was not properly cured).	0.01	0.01	0.01	Negligible risk: either failures are distributed widely in time or condition is discovered and corrected.
3. Several control rods jammed in their shroud tubes in a test reactor.	--Inadequate mechanical design of core assembly.	0.001 to 0.25 for designs of various difficulty or complexity	0.01 to 1.0, dependency or reason for jamming.	0.01 to 1.0, dependency or reason for jamming.	Experience suggests that probability of multiple failure in conjunction with actual challenge is small; if consequences serious, back-up shutdown facilities would be provided.

Table 1. (Cont'd.)

CMF event description* (see Ref. 1 unless otherwise noted)	Dependency couplings	(P:I) Estimate of prior probability of dependency existing	(P:II) Estimate of probability that dependency is not removed before serious challenge	(P:III) Estimate of probability that safety-significant challenge will "activate" dependency to cause actual CMF	Accident risk implications
4. Gross miscalibration of safety system flow elements due to incorrect dimensions of common flow venturi.	--Design error	0.001	0	1.0 (Signifies merely that CMF cause is continuous until deliberately removed.)	Essentially 0 probability that this condition could carry over into reactor operation.
5. Resistance temperatures broke off in coolant flow stream during first few weeks of preoperational testing.	--Design deficiency	0.01 to 0.1 for any similar application	0.0001 to 0.2 (higher limit is for slower weakening)	0.001 to 0.2 (higher limit is for transient stress, associated with challenge, causing failure)	Essentially 0 risk because of very low probability of multiple failure in conjunction with challenge; also some RTD elements "fail safe", and diverse backup protection is provided.
6. ~~Rebearing~~ Reactivity control plate guide bearings wore excessively; several failed in service (no actual operating difficulty was experienced) (Ref. 9)	--Design deficiency (Obscure flow induced vibrations were not anticipated.)	0.01 to 0.1 for any similar application	0.01 to 0.1	0.001 to 0.01	No evidence of potential scram failure; if there had been, there would still be only a small probability of multiple failure in conjunction with challenge; also diverse backup shutdown facilities provided.
7. Emergency engine-generator overheated and tripped out of service.	--~~Contamination~~ Contamination (pieces of fish clogged engine cooling passages)	0.001 to 0.1 for similar systems, all contaminants	0.001 to 0.5, dependency on load test frequency and degree of clogging.	0.1 to 1.0 (high limit signifies independence from challenge conditions)	Minor risk increment corresponding to overall reduction of emergency power supply reliability by perhaps a factor of 2.

CMF event description* (see Ref. 1 unless otherwise noted)	Dependency couplings	(P:I) Estimate of prior probability of dependency even existing	(P:II) Estimate of probability that dependency is not removed before serious challenge	(P:III) Estimate of probability that safety-significant challenge will "activate" dependency to cause actual CMF	Accident risk Implications
8. Emergency engine-generator failed to crank on test start attempt	--Contamination, "injected" --Human error, maintenance (wrong lubricant used on ring gear; starter pinion did not engage)	0.001 to 0.1, dependent on "quality" of maintenance effort.	0.001 to 0.01	1.0 (signifies merely that CMF cause is independent of challenge)	With customary regular weekly startup tests, there is only very small probability of multiple failure in conjunction with challenge.
9. Two control rods failed to drop in simulated scram test.	--Contamination, "built-in" (Excess epoxy material was applied during maintenance of clutch device)	0.01 to 0.1	0.001 to 0.01	1.0 (signifies merely that CMF cause is independent of challenge)	Negligible risk increment (similar to case 2); also actual failure burdens back-up shutdown system.
10. Hydraulic controllers of steam valves malfunctioned.	--Chemical reaction (moisture in hydraulic fluid reacted with fluid to produce acid which caused corrosion whose products damaged servo metering surfaces.)	0.001 to 0.1	0.001 to 0.01	0.001 to 0.1	Essentially 0 risk.
11. Excessive heat due to fuel concentration burned through barrier between core and blanket region of the aqueous homogeneous reactor (no reference provided).	--Phase change (uranyl nitrate solution in water sustained localized phase change)	0.1	(No safety	jeopardy involved)	(Economic loss sustained)

CMF event description* (see Ref. 1 unless otherwise noted)	Dependency couplings	(P:I) Estimate of prior probability of dependency even existing	(P:II) Estimate of probability that dependency is not removed before serious challenge	(P:III) Estimate of probability that safety-significant challenge will "activate" dependency to cause actual CMF	Accident risk Implications
12. Main steam header pipe ~~of~~ [illegible] rupture in fossil-fueled power plant, vintage 1943 (Ref. 9).	--Phase change (Graphite migration in alloy steel led to nodule formation that weakened material)	0.001 to 0.1	0.01 to 0.2	0.001 to 0.2	Reactor counterpart is Loss of Coolant Accident (LOCA), for which risk is evaluated in the Reactor Safety Study, reference 3.
		--(Elaborate precautions taken to prevent similar problems with reactor vessel and primary piping)			
13. Three emergency engine-generators failed to assume load due to slow action of speed governors.	--Design deficiency --Environment (Insufficient heating provided in engine room for extreme outside cold; governors sluggish due to low temperature)	0.01 to 0.1 for similar installation; allows for possible inadequate maintenance of heaters.	0.01 to 0.5	0.001 to 1.0 (High limit is for cold weather causing loss of offsite power)	Appreciable risk increment; probability of offsite power loss is relatively high during extreme cold weather.
14. (Not a specific instance). Moisture condenses in idle electric motor or generator and reduces dielectric strength of aged electrical insulation; machine fails when energized, usually, startup. (undocumented)	--Environment (moisture) --Design deficiency (neglect to apply enclosed machines or heaters in housings of open machines) --Maintenance deficiency (neglect to maintain heaters or conduct dielectric tests)	0.01 to 0.1	0.01 to 0.5 --(high limits are for gross misapplications of equipment)--	0.01 to 0.1	(Condition widely recognized in design practice and pertinent criteria).

CMF event description* (see Ref. 1 unless otherwise noted)	Dependency couplings	(P:I) Estimate of prior probability of dependency ever existing	(P:II) Estimate of probability that dependency is not removed before serious challenge	(P:III) Estimate of probability that safety-significant challenge will "activate" dependency to cause actual CMF	Accident risk Implications
15. Engine-generator failed to break in startup test; two redundant starter systems failed, each for different reason.	--Inadequate testing (human factors)	0.01	0.001 to 0.01	0.001 to 0.01	Small increase in overall probability of one engine failing to start on demand.
16. Engine-generator rejected load and surged repeatedly. (undocumented)	--(Discovered during correct test on one unit, i.e., no actual CMF occurred)	0.001 for general load rejection on two independent units.	0.01	0.01 to 1.0	If this condition occurred where two engine-generator units were parallel. there would very probably be a delay in the availability of the unfailed unit
17. Contact-making meters would not "make" at setpoint unless signal approached this value rapidly.	--Component application --Inadequate testing (condition allowed to remain for long interval)	0.001 to 0.1	0.01 to 0.5	0.1 to 1.0	Appreciable risk increment.
18. All rods failed to scram on demand.	--Design deficiency (Sneak circuit permitted via failure of single component)	0.01	0.01	1.0	Appreciable risk increment, corresponding to difference in reliability between combined primary and secondar shutdown systems, an secondary alone; in this case secondary system did function adequately.

CMF event description* (see Ref. 1 unless otherwise noted)	Dependency couplings	(P:I) Estimate of prior probability of dependency ever existing	(P:II) Estimate of probability that dependency is not removed before serious challenge	(P:III) Estimate of probability that safety-significant challenge will "activate" dependency to cause actual CMF	Accident risk Implications
19. Control rod withdrew on "Insert" signal.	--Design deficiency (unrecognized capability of 2-phase rod drive motor to operate single phase, i.e., with second phase excited from other load elements, when one lead was disconnected)	0.01	0.01 to 0.1	(Not Applicable)	Negligible risk increment; [illegible] potential is challenge to the protection system.
20. Erroneous indications of level in pressurizer vessle; 2 of 3 channels.	--Design deficiency (allowed partial loss of pressure in common reference leg to affect signals in redundant level instruments)	0.01	0.0001	1.0	Negligible risk increment; diverse protection provided.
21. High flux protection defeated; failure to scram of HTRE-3.	--Design error (noise filters in output of flux amplifiers limited output signal)	0.01	0.01 to 0.5	1.0	(Core melt occurred, with economic consequences).
22. Protected power distribution bus normal supply interrupted and engine-generators did not start or assume load.	--Design deficiency (bus trip caused by overvoltage, which did not initiate engine start since undervoltage was required; UV relay on transformer secondary instead of on bus)	0.01 to 1	0.5	0.001 to 0.1	Negligible risk increment; probable effect is short delay in power availability at bus.

CMF event description* (see Ref. 1 unless otherwise noted)	Dependency couplings	(P:I) Estimate of prior probability of dependency ever existing	(P:II) Estimate of probability that dependency is not removed before serious challenge	(P:III) Estimate of probability that safety-significant challenge will "activate" dependency to cause actual CMF	Accident risk Implications
23. (Not a specific instance). Groups of motors on common ungrounded multiphase power supply fail "simultaneously" (Ref. 30).	--Design deficiency (lack of understanding of complex resonant condition prior to about 1947)	(0.5*)	(1.0*)	(0.0001*) (*For ungrounded networks, which were prevalent up to 1950; present probabilities are virtually 0.)	(Condition recognized in design practice and industrial codes).
24. Cable tray fire and subsequent reactor shutdown; manually controlled core cooldown (Brown's Ferry Plant, 1975) (Ref. 4).	--Inadequate design (lack of adequate fire-fighting facilities; cable separation problems, etc.) --Maintenance error (flame test for barrier leak)	0.001 to 0.1	0.1 to 0.5	0.0001 to 0.5 (extreme variability represents spectrum of safeguard malfunctions which could result from cable fire)	Appreciable risk increment; burden of shutdown cooling placed on backup facilities.

where the consequences associated with even the remote chance of a CMF have been sufficient reason to provide diverse backup facilities, e.g., for emergency shutdown of the reactor (e.g., items 3, 9, 18).

CMFs POSTULATED IN REACTOR SAFETY ANALYSES

Much of the controversy over reactor safety falls within the broad purview of common-mode failure. Table 2 summarizes the principal kinds of dependency couplings which could conceivably dominate the outcomes of several postulated accidents of LWRs. Notable is that all except perhaps the ATWS involve "energetic" events which may affect many components in different ways and to different degrees. The other potential major common risk factor is design ignorance: to remove uncertainties in matters of ECCS performance and design to withstand seismic forces is the objective of extensive analytical and test programs.

ANALYSES TO IDENTIFY POTENTIAL CMFs AND EVALUATE ASSOCIATED RISKS

There is no question that any given common-mode failure or failure dependency can be described by any of the familiar reliability logic models. Likewise, the use of conditional probabilities to represent known dependencies is convenient and straightforward. Of interest here, however, is how useful these formal analytical tools might be in finding potential CMFs, a priori, and in deciding which are sufficiently important risk contributors to warrant special efforts to reduce their effects.

Table 2. Dependency couples in hypothetical accidents

Initiating Event Type	Dependency couples that affect risk rate	Problem treatment in safety analyses
1. "Anticipated Transients Without Scram" (ATWS)	a) Condition ".... Without Scram" is given, i.e., (P:No Scram) = 1.0. Although this includes all likelihood that stress or other aspect of plant transient is a factor in protection system failure, no strong CMF coupling is evident from the engineering analyses. b) Conditions developing from ATWS present more rigorous challenges to safeguard systems than if scram was accomplished. If any safeguard system design bases limit is violated by transient conditions, this would imply a strong CMF coupling.	Purpose of analyses with arbitrary "no scram" are to evaluate safeguardsystems capabilities to prevent or mitigate accidents. This is a determinatic exercise. However, the results are to aid in deciding whether reliabilities reasonably achievable with the present LWR shutdown systems are adequate, or if diverse-redundant systems are desirable. (e.g., Ref. 11)
2. Earthquake	a) "Energetic" coupling to seismic motions involves all plant components; degree varies greatly due to different seismic characteristics; ability of structure to absorb, transmit, or amplify motions; etc. b) Structure and components designs largely determine strength of CMF couplings.	Principle concerns are (a) earthquake intensity vs plant location as basis for seismic design and component qualification and (b) validation of seismic analysis and design methods; these are focus of safety efforts. (Ref. 12) ~~NSIC-28~~
3. Missile from steam turbine failure-disassembly	a) "Energetic" coupling via missile path. b) Design of plant with regard to turbine location and orientation, and missile barriers. c) Design of turbine with respect to structural safety margins. d) Operation and maintenance of turbine, e.g., to assure balance, clearances, etc.	Target strike probabilities are calculated on basis of ejection velocities, angles, etc., given turbine failure occurs. Penetration and damage are derived from ballistic formulae. (Refs. 13 and 14) ~~NSIC-22~~ NSIC-4 of 433

Table 2. (Cont'd.)

Initiating Event Type	Dependency couples that affect risk rate	Problem treatment in safety analyses
4. Loss of Cooling Accident (LOCA) in PWR due to pipe failure located so that primary coolant pump overspeeds and its flywheel fractures.	a) "Energetic" coupling via missile path such that low pressure injection system pipe is ruptured. b) Design of plant with regard to pump location and orientation, and missile barriers.	Overall event sequence (LOCA - LPI failure) probability estimated at 1.3×10^{-6} per reactor-year. (Ref. 3) RSS Draft Append. IV p. 68
5. Airplane crash on reactor plant structure.	a) "Energetic" coupling via aircraft impact point, speed, weight, angle, etc. b) Design of plant with respect to ability to withstand impact c) "Energetic" coupling via fire following impact.	Probability of impact on containment vessel formally estimated for "representative" site as 3×10^{-6} per reactor-year. (Ref. 3) RSS Append. III, p. 101 Extensive probabilistic risk analysis. (Ref. 15)
6. Loss of Cooling Accident (LOCA) - Major.	Physical factors which could defeat function of Emergency Core Cooling System (ECCCS), assuming system operates.	Deterministic analyses of core and extensive test programs to establish or validate calculation parameter.

Event Logic Modeling

A brief review of the logical procedures generally used to identify system failure causes will indicate how each method might perceive CMF dependencies. The simplest of the methods is the popular Failure Mode and Effects Analysis (FMEA), to which is sometimes added consideration of failure cause (FMCEA). This is no more than a format for listing component or system failure and malfunction modes, and how each affects other system parts or functions. As such, it is more-or-less limited by the analyst's understanding of systems and equipment, and his perception of the more direct functional relationships among them; it is unusual in FMEA practice to trace branching effects more than one or two steps, or to probe extensively for obscure failure causes. One interesting variant of FMEA is "Sneak Circuit Analysis,"[2] a computerized technique for accomplishing what the name implies; its application is not restricted to electrical circuits.

In concept, event (or "decision") tree logical structuring of events resembles FMEA. That is, event trees help the analyst explore event paths devolving from defined initiating events or conditions. In applications such as the Reactor Safety Study,[3] use of the method has been restricted to sequences of major events, detailed expansions being done by subsidiary fault trees. The logic structure of this method is apparently well suited to exploring in depth the effects of any component failure or other condition. However, it is correspondingly capable of encouraging the analyst to introduce trivial branches which distract from, rather than focus on, potentially important failure dependencies.

By contrast, the fault tree represents a deductive logical process whereby an undesirable outcome of significance in postulated first, and then a search is undertaken to identify event combinations which will produce that outcome. The acceptance that this method has achieved is due largely to its facility for showing just which combinations of components are essential to successful system or mission performance. One evident way that this capability has been used to attack the CMF problem is to screen and reduce the number of component combinations among which it is worthwhile to search for failure dependencies. Some argue, however, that finding such combinations is a minor problem compared to that of discovering—or recognizing—obscure coupling mechanisms.

Logic Models vs Actual CMFs

The examples summarized in Table 1 represent a sampling of "practical" CMF experience. These are reviewed below in terms of whether, or to what approximation, they could have been anticipated by the event-logic analyses just described. The cases are grouped for discussion purposes according to causal factors which are disposed toward discovery through particular kinds of prior knowledge or reasoning:

A. Readily Apparent Errors or Omissions in System Design

From an engineering standpoint, it seems that the design deficiencies underlying cases 1, 7, 13, 14, 17, 19, 20, 21, 22, 23, and 24 could—perhaps should—have been discovered by careful reviewers with a good ~~graph~~ grasp of the equipment involved. If it was lack of organization of design reviews that occasioned some rather obvious failure causes to be overlooked, then FMCEA discipline might have benefitted such efforts. Regarding case 7, analysis

would not be expected to single out the agent that clogged the engine cooling system; instead, the general need for coolant water quality control would have been ~~called out~~ emphasized. Similarly for case 13, engine governor performance probably would not have been identified within the general requirement for engine environment control. Cases 1, 14, 17, 19, 22, and 23 exemplify needs for the specialist's knowledge of obscure problems peculiar to various systems and equipment; I venture that not one in ten recent graduates in electrical engineering have even heard of the "restriking ground fault" (No. 23), which is one reason why ungrounded distribution systems are now considered bad practice. Case 18 was included in this group despite the very small likelihood that its "sneak circuit" cause would have been found in any ordinary review; the sneak circuit was discovered, however, in an exercise to demonstrate the "Sneak Circuit Analysis" method, conducted after the incident. Regarding case 24, the Brown's Ferry fire, subsequent reviews brought out the obvious need for improved fire prevention and control facilities. Overall, a striking aspect of the above cases is that the "computer approach" to systems reliability analysis, i.e., simply to assume various combinations of components failed, would not have yielded the slightest clue to the existence of these CMF causes. In several cases, there was no actual component malfunction while in others the failure or malfunction of a critical component was due to an obscurely (but strongly) coupled condition.

B. Prior Common Deficiency in Components

Cases 2, 4, 5, 9, and 12 are characterized by component problems of unusual kinds. Concerning case 2, reliability analyses would routinely consider stuck relays, but for several to stick concurrently would be dismissed as "too improbable". Similarly, for several EFW elements to

break off within a short time span as in c e 5, or for several rods to fail simultaneously to scram as in case 9, would also seem highly unlikely from independent causes. No failure occurred in case 4, improper dimensions of a common flow element. Case 5, steam ~~bender~~ header failure, was due to an unsuspected metallurgical condition which developed in service. While none of the usual analyses seem suited to predicting these CMFs, a special kind of event tree has been used to find whether adequate protection is provided, given that all redundant elements of one kind are failed. This technique, used by Jacobs,[5] is pertinent to case 5 and perhaps also to case 4.

C. Obscure Problems in System Design

Complex, novel systems may incorporate failure mechanisms despite the best efforts to design conservatively and to anticipate all environmental or operating conditions. In case 3, mechanical design of a reactor core neglected conditions which caused several rods to jam in their guide tubes. Cases 5* and 6 involved flow turbulence forces that fatigued components (*Case 5 also considered in Group B). Case 10 was the culmination of a chemical reaction, corrosion, erosion sequence which began with water contamination of the organic fluid in a hydraulic system; either the possibility or the consequences of water ingress were overlooked. Neither the experience gained from a prototype reactor nor the impressive talent focussed on the design of the HRT anticipated the ~~corrosion~~ hot-spot effects in case 11.

D. CMFs Due to Human Error in Operation or Maintenance

Several prime examples of human error were left out of Table 1 only because they could not be described adequately in a limited space. Of

those ~~related~~ selected, cases 15, 16 and 17 exemplify inadequate test procedures. Case 8 is clearly a maintenance error, but again weak procedures or administration could have been causes. In case 24, that the fire damage at Brown's Ferry was so extensive was due partly to procedures and partly to design factors. With respect to this group of CMFs, it is noted that human factors in reactor plant design, operation, and maintenance are receiving increased attention.[3] The analytical methods used to assess and reduce human error potential include event tree adaptations which map the performance of task elements.

E. Large-Scale "Energetic" CMFs

Aspects of case 24, other than those discussed in Groups A and D, qualify it as an "energetic" CMF. In particular, the cable fire involved many control and power cables. To evaluate the enormous number of possible combinations of individual open- and short-circuit faults, as functions of time, is a futile exercise. However, logical procedures are very useful in the endeavor to achieve functional independence through cable groupings and separation.

LOGIC MODELS OF HYPOTHETICAL ACCIDENTS

Table 2 considers "hypothetical" situations which are an important part of the design bases of reactor plants. Excepting perhaps the ATWS, these situations involve strongly energetic, primary dependencies. Implied is that latent and secondary dependencies of the kinds described in Table 1 also may be "activated" by stresses or operating conditions that occur during or after the initial transient events. The possible combinations are virtually limitless.

A realistic, future role of event or fault tree analyses in developing protection against rare design basis conditions has been shown tentatively in the Reactor Safety Study[5] to be that of exploring and comparing potential risks. This could help create the perspective needed to allocate finite resources among competing costly defense measures. In the past, however, the most important decisions have been made without formal cost-benefit analyses, for example, to design structures and qualify equipment for withstanding seismic effects, to undertake extensive analysis and test programs that will validate ECCS design bases, to validate design bases for heavy-section steel vessels, etc.

PROBABILITY MODELS OF CMFs

The incentives for quantifying common-mode failure probabilities are clear. Not only would this establish the importance of individual CMFs, hence what corrective measures are worthwhile, but it would also remove some major uncertainties from risk analysis. The predictive models which have been proposed[6,7] seem to recognize the various CMF origins and dependency aspects. However, the prospects for evaluating the model parameters from plant experience statistics are extremely limited. Some additional data pertinent to particular kinds of CMF dependency could possibly be obtained from control room simulation tests and from special tests of equipment such as used for seismic qualification, but this has been done only to a very limited extent.

The reactor plant statistics that have been used[3,7] to evaluate CMF model parameters are drawn from the same body of experience as the examples in Table 1. Thus, they reflect the "practical"—almost "random"—classes

of CMF that are encountered in ordinary plant operation. Regarding their associated accident risks, most of these examples were one-time-only occurrences, and their causes were removed before a serious challenge arose. The statistics tell virtually nothing about the strong "energetic" couplings of concern in accidents, because the "activating" conditions almost never arise; that is, in terms of the model proposed earlier, the conditions associated with a conditionally high (P:III) have not been met. This is not to say that any such couplings actually exist, but merely that pertinent statistical evidence is not obtainable. We must, therefore, continue to put our faith in conservative design, aided by mainly deterministic modeling, to protect against the energetic CMFs. Similarly for CMFs due to human operator error, the statistics of current reactor operating experience do not reflect the known deterioration of human reliability under great stress. And while this can be estimated very well for specific task elements, it is very difficult to predict just how the operators may have to intervene in a plant upset, and much more difficult to assess all the attendant opportunities for error.

CONCLUSIONS

To the extent that the experience cited is representative of common-mode failures, it appears that formal logic models are only marginally effective for identifying the specific causes. The experience further suggests that most of the "ordinary" CMF dependencies will be discovered and removed before the functions involved receive a safety-significant challenge. Three kinds of "unusual" CMF dependency require special

attention, which can be focussed effectively by logical-probabilistic analysis: (1) energetic couplings, (2) human error under duress, and (3) insufficient understanding of conditions pertinent to design of complex equipment.

Regarding energetic couplings, the emerging role of formal logic procedures is to explore and account methodically for branching dependent events and conditions. This has been demonstrated by the Reactor Safety Study as a highly effective way to organize, first, the design bases for systems and equipment which must withstand unusual accident-induced stresses and, second, the deployment of backup safeguards.

The case for event trees in optimizing human factors is similar. There, it is principally the mapping of possible operator interventions during plant upset conditions that can provide the basis for decisions to automate or to minimize the potential for error in executing crucial tasks.

Logic alone will not overcome inadequate understanding of obscure conditions that affect equipment. However, to recognize that there are major unknown factors in a design is to acknowledge the need either to obtain sufficient information or to provide adequate defenses against failure. The role of tree analyses, then, is clearly to explore the spectrum of conditions to be defended against.

Statistical evidence suggests that good engineering and quality assurance have held the "ordinary" CMF rates to acceptably low levels. There is virtually no evidence pertinent to the energetic CMFs or human errors under duress that could occur during hypothetical major plant upsets; we may reasonably hope that no such evidence will ever be provided by real experience.

REFERENCES

1. K. C. Hayden, Common-Mode Failure Mechanisms in Nuclear Plant Protection Systems, ORNL/TM-4984, December 1975.

2. J. P. Rankin, "Sneak Circuit Analysis", Nuclear Safety 14(5), pp. 461-468, Sept. - Oct. 1973.

3. USAEC, Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, Draft (August 1974).

4. USNRC, Recommendations Related to the Brown's Ferry Fire, NUREG-0050, February 1976.

5. I. M. Jacobs, "The Common-Mode Failure Study Discipline", IEEE Transactions on Nuclear Science, NS-17(1), pp. 594-598 (February 1970).

6. K. N. Fleming, A Reliability Model for Common-Mode Failure in Redundant Safety Systems, GA-A13284, General Atomic Co. {(Date and location)

7. K. N. Fleming, et al., HTGR Accident Initiation and Progression Analysis Status Report, GA-A13617, General Atomic Co., October 1975.

8. A. P. Fraas and A. A. Abbatello, Problems with the HFIR Control Rod Drives and Their Solutions, ORNL/TM-2505, November 1969.

9. C. H. Mahoney and W. S. Dritt, Graphitization in the Power Station at the Oak Ridge Gaseous Diffusion Plant, K-1404, November 1958.

10. Electrical Transmission and Distribution Handbook, Third Ed., 1944, Westinghouse Electric & Manufacturing Company.

11. L. G. Frederick, et al., An Analysis of Functional Common-Mode Failures in General Electric Boiling Water Reactor Protection and Control Instrumentation, NEDO-10189, General Electric Co., July 1970.

12. T. F. Lomenick, et al., Earthquakes and Nuclear Power Plant Design, ORNL-NSIC-28, July 1970.

13. R. C. Gwaltney, Missile Generation and Protection in Light-Water-Cooled Power Reactor Plants, ORNL-NSIC-22, September 1968.

14. S. W. Swan and Mr. Maleis, "A Method of Calculating Turbine Missile Strike and Damage Probabilities", Nuclear Safety 16(4), pp. 443-451, July-August 1975.

15. I. B. Wall, "Probabilistic Assessment of Aircraft Risk for Nuclear Power Plants", Nuclear Safety 15(3), pp. 276-284, May-June 1974.