5313

RELIABILITY METHODS APPLIED TO REACTOR SAFETY:

TRENDS AND PROGRESS *

Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830

P. Rubel

September 7, 1971

A surge of interest in applying reliability engineering methods to enhance reactor safety appeared after 1965. The resulting accomplishments in one principal area, quality assurance, are now a familiar story. In the other major area, reliability analysis, the situation has become obscured by conflicting claims and criticisms, and the initial enthusiasm has tapered off somewhat. However, despite that some ambitious early goals still seem rather remote, there has been perhaps more progress in analysis development and application than is generally appreciated. Hence it is timely to review the current prospects for analysis as found during a recent study. ⁽ⁱ⁾

It is not immediately apparent as one first views reliability analysis that the practice divides roughly between studies to establish general figures-of-merit for defined systems and studies which determine probabilities of successful operation in specific situations. There is a wide range of problem sophistication within each of these classes. The ultimate questions of reactor safety, however, concern actual risks, whose evaluation involves the more difficult reliability problems of the latter class.

Table 1, columns 2 and 3, identifies the levels of analysis capability represented by current safety-related studies. They progress from the simplest subsystem availability calculations through overall plant risk evaluations, which introduce many factors beyond the usual scope of "reliability." Each succeeding stage places further demands on the analysis with regard to:

*Research sponsored by the U. S. Atomic Energy Commission under contract with the Union Carbide Corporation.

(1) problem formulation, (2) support information requirements, (3) ^{model} ~~problem~~ *evaluation techniques* ~~solution capability~~, and (4) resolution of uncertainties. The following sections deal with the progress in each of these areas toward more conclusive analyses.

Problem Formulation

The basic reliability or "hardware" model represents a system as an array of components which can either be "good" or "failed" at any moment of interest. If the parts work, the system works. ~~(basic)~~ ^{at best} Models of this kind are simplistic and it should be apparent that many effects are embedded in each component reliability expression.

Two types of problems are treated with the reliability model: those which determine serviceability of operating systems and those concerning availability of standby systems, e.g., most protection systems. The latter are the ^{focus} ~~forms~~ of safety interest, although operating systems also affect safety to the extent that their failures may induce needs for protective action.

Availability analyses alone may only partially or indirectly answer the pertinent safety question, ~~Will~~ ^{Will} a protection system respond adequately to meet a specific plant contingency condition? Special attention must then be given to formulating more elaborate problems to represent the conditions. For example, the problem may be expanded into two or more phases, e.g., availability up to moment of demand, probability of initial response, and reliability during operation over a critical interval. A set of hardware systems may be involved, with "success" parameter^s selected for each system consistent with the situation of interest.

With reactor plants and their protection systems growing ever more complex, it becomes increasingly difficult even to define the contingency

conditions of interest. Addressed to this need are the event and decision tree methods of diagramming fault and response sequences, and the Failure-Mode-and-Effect and Common-Mode Failure analysis techniques for ferreting out potential sources of system failures. Component failures are simply one class of events in the tree diagrams. These methods are essentially qualitative, however, the tree diagrams can be evaluated by probabilistic techniques where it is reasonable to estimate the elemental event probabilities.

The decision tree in particular offers the framework and capability for risk analysis and overall safety evaluation. To accomplish these ambitious aims, however, the analyses must be expanded to include initiating event or condition probabilities at the front end, and outcome consequences - perhaps various alternatives - at the conclusion. The practical limitations are all too clear. Nevertheless, some noteworthy attempts to evaluate overall plant risks have given valuable insights as to where the actual hazards lie and thus have had considerable influence on the protection system designs.

One appeal of the tree diagram - particularly the fault tree - is that it can be applied by the individual engineer with access only to paper and pencil. Any degree of detail can be accommodated, the method lending itself to problem partitioning via subsidiary trees. Numerical evaluation by hand methods is restricted to the simpler trees of gross events. Beyond that, the main limitations are imposed by the analyst's ability to envision all of the significant contributing events and to estimate their probabilities.

Analysis Support Information

The popular criticism of reliability or other probabilistic analysis is lack of credible data. Mainly, the data sought have been characteristic

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.

component service ~~likes~~ and failure rates; risk evaluations, of course, depend also on additional information to ~~define~~^{describe} fission product release, dispersion, and consequences.

By tradition - that is, as treated in most military and aerospace reliability work - the component failure probabilities are determined from observed performance either in service or on test. But the scale factors of time and quantity have not been favorable to this approach for most reactor system equipment. In fact, technological progress itself has been a major obstacle to gathering conclusive statistics.

More penetrating evaluations of reactor protection systems (indicated higher up in Col. 3), consider the functioning of these systems under emergency conditions, at which times the equipment may be unusually stressed. Ordinary or "average" service statistics then may not provide good insight as to whether a component or subsystem will perform to the necessary standards. Moreover, the emergency conditions may be so rare that there is virtually no prospect for acquiring statistical information to account for them.

Attempts to upgrade the equipment reliability data base have taken several forms. Of these, the most publicized is the data bank approach, exemplified by the UKAEA Syrel and the IMEC information systems (the latter temporarily mothballed). Both of these systems are conceived as "active" in the sense that they promote data gathering to uniform high standards, provide engineering evaluation of the information received, and attempt to combine and interpret information according to users' problem requirements. Another notable effort along the same lines is the pilot program to gather component service data in the Connecticut Yankee reactor power plant, a project begun with USAEC support through Holmes & Narver, Inc., but now

carried on privately. Finally, considerable discussion has centered on the prospects for a similar program for the USA on an industry scale, to be supported jointly by the utilities and manufacturers and carried out by an organization, such as EEI, with current industry contacts.

While the data banks for reactor equipment still tend to emphasize statistical information, they are also showing a healthy awareness of qualitative information to supplement areas where massive direct experience is not available. Others more closely involved with equipment applications are likewise beginning to exploit component qualification test observations and basic engineering analyses to evaluate reliability of components. Typical of the qualification test approach was the demonstration of BWR main steamline isolation valves reported by Jacobs; ^③ one valve was tested over many cycles and under simulated conditions more severe than the anticipated emergency service conditions. Engineering analyses have been used by General Electric to synthesize component reliability estimates out of parts and materials considerations; such studies also give guidance in setting quality assurance goals and in designing qualification tests. The IEEE standards effort on electric motors for service inside containment enclosures similarly encourage qualification testing, again not on the scale that would be necessary to yield conclusive failure rate or life statistics.

Some of the additional information needed for risk evaluation is simply more reliability data, particularly for the operating equipment whose failure could induce need for protective action. Beyond this are such matters as natural event frequency and severity, fission product release and transport, meteorological conditions, population dispersion, and dose effects. A great deal of the information has been developed through the various safety programs,

which are beyond the scope of this paper.

Model Evaluation Problem Solution Techniques

The most satisfying progress in analysis has been with regard to problem solution capabilities. Digital computer applications have dominated the scene since about 1965, expanding the capability by orders of magnitude beyond what can reasonably be done via hand methods.

The early computer programs were clearly classifiable as analytical or simulation. A pioneer analytical program was the ARMM, greatly improved versions of which are still widely applied. It's salient feature is that the significant combinations of component failures in a system are identified by truth table, i.e., by testing the system logic model with every allowed combination of component failures. The probability of each identified failure combination is evaluated at a selected "age" of the system, the sum of the (exclusive) combination probabilities then being the probability of system failure at one point in time. The first noteworthy simulation program also employed a system logic model, which was tested repeatedly corresponding to increments in system real time up through the interval of interest. For each increment, every system component was given a random opportunity to fail according to its characteristic failure versus time probability; this was accomplished by a Monte Carlo technique in which a digital computer simulated the random effects and an analog computer determined the component time-dependent reliability factors. Many iterations over the main interval produced the "simulated" system failure statistics of interest.

Two fundamental improvements in the computer programs were largely due to the work of Holmes & Narver, Inc. Initially, the original simulation method was revised for all digital execution. The revision at the same time

did away with the procedure of considering the system by time increments within the interval of interest. Instead, a complete master schedule of all of component failures and restorations during the interval is developed as the first step; the system is then tested only for those points in time where a component event occurs. The other basic advance amounted to combining desirable features of analytical and simulation methods in order to promote calculation efficiency. Thus, later programs of the SAFTE series use biased Monte Carlo techniques to identify the significant combinations of failed components, then determine the probabilities analytically.

Most of the current reliability computations are done using programs based on the methods just described. However, there has also been some application of the GEM program in reactor work. The GEM program, developed by the U. S. Navy for logistics problems, exploits the Markov chain method by setting up and solving sets of differential equations which describe probabilities of system transitions among possible states (e.g., combinations of failed and unfailed components on other reversible events).

Once a basic program has been established, it seems the trend to devise a number of variations which will either expand its capability or improve efficiency; efficiency is often achieved at sacrifice of capabilities that may be unused in particular problems. Such evolution has resulted in a wide range of programs now available to the analyst. Some notable capability advances concern (1) sizes of systems analyzed, (2) analysis partitioning by problem sequence, (3) accommodation of different component failure versus time characteristics, (4) modelling of repairable components, (5) accounting for dependent probabilities, e.g., with system standby elements, and (6) providing system failure versus time characteristics rather than single points

for preset intervals.

Another significant area of computer program development deserves special emphasis, and that is event analysis. Essentially the same techniques used to determine probabilities of system failure or success ^{with regard to component random failures,} can also be applied more generally to evaluate combined event probabilities. The program organization may be somewhat different, however, corresponding now to the event tree or decision tree. The decision tree in particular requires the program to accommodate multiple outcomes, where other model forms concern only the single probability of the defined ultimate event. Several accounts appear of decision tree applications by the UKAEA ⁽¹⁾⁽²⁾ in reactor risk analyses, and at least one reactor manufacturer in the U.S. has developed similar analysis capabilities.

Analysis Uncertainties

Beyond questions of model relevance or completeness is the matter of system reliability and risk forecast[†] uncertainties with regard to input information. Such forecasts are usually point estimates, based on rather limited and inconclusive observations of components.

One approach in assessing accuracy of the point estimate is simply to find also the extreme or boundary problem solutions, i.e., using all-optimistic and all-pessimistic reliability values for the components. The obvious fallacy there is like that in summing dimension tolerances to determine maximum deviation: the individual deviations rarely if ever accumulate all in one direction. Moreover, the approach may yield absurdly broad limits for systems of many components or in cases where a reliability problem is carried out to ⁶ fine detail. Such broad limits, in turn, would detract from

studies which were attempting to compare system designs or effects of added features.

Vesely of Idaho Nuclear Corporation is attempting to account for data uncertainties by applying dimension analysis techniques, ^① whereby the magnitude and direction of each component failure rate (λ) deviation from "best estimate" is treated as a distributed continuous variable. He assumes the density function to be log-normal in form, ~~then determines~~ ^{actual} the distribution for each component ~~so as to reflect~~ ^{reflecting} a confidence interval consistent with the component data resolution. Substituting the probability distributions for the usual single-valued estimates in a system analysis, then, is done so as to weight the effects of the individual deviations on the system reliability outcome. The overall effect is essentially that of synthesizing a system confidence interval.

Analysis Applications and Trends

Having dealt with state-of-the-art, we turn to ~~current~~ ^{recent} analysis applications and trends. Most of the current reactor analysis work in the U.S. is being performed by the reactor manufacturers, hence the studies are proprietary and little publicized. What literature appears nowadays gives the impression that reliability analysis is more talked about than practiced. Regardless of the amount of analysis being done, however, the continued attention has been beneficial to protection system design and quality assurance.

The distinction was drawn earlier between generalized analyses of defined systems and the more specific "situation" studies. Certainly the bulk of the current quantitative analyses are of the former type, mainly for purposes of internal design review and optimization. Numerical evaluations are also sometimes offered to reactor purchasers to ~~substantiate~~ ^{substantiate} ~~substitute~~ claims of operating

system reliability. In reactor licensing, however, the quantitative methods have not yet been well accepted as a means for demonstrating reliability of protection systems.

Regarding the situation studies, it appears that the manufacturers are doing more qualitative analyses along this line than quantitative. Much of the work is in response to the USAEC regulatory groups' present emphasis on defense-in-depth against potential accidents. Thus, examples of, or references to, fault tree and failure mode and effect analyses are found in four recent reports, one by each of the major manufacturers of water-cooled power reactors, regarding protection from common-mode failures. At least one manufacturer has developed the capability for advanced decision analysis of complex systems, whereby risk evaluations could be made.

The UKAEA place considerably greater emphasis on formal risk analysis than is done in the U.S. Their literature indicates a general acceptance of Farmer's risk criterion and describes evaluation methods accordingly.

Conclusions

The extent to which the various kinds of reliability analysis are being accepted or deferred suggests what critical improvements are needed. But more important, it also marks a maturing attitude toward analysis. Thus, the benefits are coming to be viewed in terms of the system improvements which result from intensive study and from the placing of many factors in an understandable perspective; while numerical forecasts are gaining in credibility, there is also developing an understanding that even the most thorough analysis may not anticipate all significant factors.

^{about}
~~Regarding~~ system general reliability figures-of-merit, there seems to be agreement that such evaluations are useful as internal design aids. It is

also coming to be recognized that while simple availability or reliability figures alone are perhaps adequate to assess some systems, such figures may be only tenuously related to probabilities of system response under unusual emergency conditions. Wider application of reliability and availability quantitative analysis, then, appears to depend on the advent of better data and further appreciation for where such methods are suitable.

That situation probability and risk analyses are regarded as desirable is implied by the expanding use and regulatory acceptance of qualitative versions in the U.S., and by the emphasis placed upon these methods overall by the UKAEA. Further progress in applying the advanced methods seems to await not only better data but, in the U.S., more uniform problem approaches in which questions of technique will not distract attention from the solid issues.

1. P. Rubel, Reliability Engineering Methods in Reactor Safety Technology, USAEC Report ORNL-NSIC-83, Oak Ridge National Laboratory (to be published).
2. B. J. Garrick et al., Collection of Reliability Data at Nuclear Power Plants, USAEC Report HN-199, Holmes & Narver, Inc., December 1968.
3. I. M. Jacobs, Demonstration of the Performance and Reliability of the General Electric Company Boiling Water Reactor Main Steamline Isolation-Valves, presented at the CREST meeting on Reliability of Mechanical Systems and Components, Risø, Denmark, Sept. 1969.
4. B. J. Garrick et al., Reliability Analysis of Nuclear Power Plant Protective Systems, USAEC Report HN-190, Holmes and Narver, Inc., May 1967.
5. O. C. Baldonado, On Some Computer Methods for System Reliability Evaluation, presented at the International Conference on Quality Control, Tokyo, Japan, October 21-24, 1969.
6. S. Orbach, The Generalized Effectiveness Methodology (GEM) Analysis Program, Lab. Project 920-72-1, Progress Report 1, U. S. Naval Applied Science Laboratory, Brooklyn, New York, May 8, 1968.
7. E. R. Woodcock, The Calculation of Reliability of Systems: The Program Noted, UKAEA Report AHSB (S) R 153, 1968.
8. M. C. Pugh, Probability Approach to Safety Analysis, UKAEA Report TRG 1949 (R), 1969.
9. W. E. Vesely, Reliability and Fault Free Applications at the NRTS, IEEE Transactions on Nuclear Science, v NS-18 n 1, Feb. 1971, p 472-480 - also pers. comm. with P. Rubel.
10. T. W. T. Burnett, et al, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, WCAP-7306, Westinghouse Electric Corp., April 1969.
11. L. G. Frederick, et al, An Analysis of Functional Common-Mode Failures in GE BWR Protection and Control Instrumentation, NEDO-10189, General Electric Co., July 1970.
12. W. C. Coppersmith, C. L. Kling, A. T. Shesler, B. M. Tashjian, Reactor Protection System Diversity, CENPD-11, Combustion Engineering, Inc., Feb. 1971.
13. Systematic Failure Study of Reactor Protection Systems, BAW-10019, Babcock & Wilcox, Sept. 1970.
.. ..
14. J. R. Beattie, G. D. Bell, and J. E. Edwards, Methods for the Evaluation of Risk, UKAEA Report AHSB (S) R 159, 1969.

ABSTRACT

The present main roles of reliability engineering methods in reactor safety are to improve the design of protection systems and enhance quality assurance. This paper reviews the continuing efforts to strengthen the credibility of probabilistic safety evaluations and to expand the analysis role in guiding safety support activities. A trend toward situation-oriented analysis is noted, along with innovations in exploiting the limited information available for analysis input.

Table 1 - Reliability and Risk Analysis

(Approx. Time Progression)	Analytical Capabilities	Problem Formulation
(Some attempts after ~1965)	{ Probability/reliability analysis programs coupled to other programs: interleaved or sequential programs.	(Combine initiating conditions, response, and consequence evaluation as required).
1970	Combined all-digital simulation and analytical evaluation.	Account for multiple outcome probabilities: "decision tree"
	All-digital "Markov chain".	Trees of dependent events/determine probability of defined ultimate event as determined by component failure probabilities and other external events.
	All-digital "simulation".	
1965	Reliability "analytical" calculation by digital computer.	Account for changing operating mode or conditions: availability and reliability sequence probabilities
	Reliability "simulation" by combined analog and digital computer (hybrid).	
1960	"Markov Chain" by analog computer.	Increasingly complex arrays of components (larger systems or structure); each subject to random failure; account for component repair, standby service.
	System Success-Failure Logic by Switch Matrix Analogy.	
1950	Hand calculations.	Model array of system main components each subject to random failure "average" conditions/Determine Reliability or Availability: or $R(t)$, A -avg or $A(t)$.
1945	(Identify component life and failure characteristics by statistical methods).	

Analysis Applications:
Conclusions Sought

Required Kinds of
Input Information

dition, system
ce evaluations

(Assess overall plant
safety).

(Assurance that all significant
contributing factors are accounted
for)

come
a tree"

Assess specific risks.

Individual initiating event
probabilities/consequence
effects.

is/determine
ultimate
component
and other

Assess probabilities of alternative
responses by complex system or array
of systems, to defined initiating
condition.

Assess probability of complex
system response in terms of random
component failure and other events.

Probabilities of external events
which affect system response

erating
liability
problems.

Components failure rates, by
operating modes and conditions
time-to-repair.

ays of system
ns or finer
random
ponent test,

Assess probability of complex system
response in terms of random component
failures only.

Parts life and failure rate,
average and severe conditions

in components,
ailure under
etermine simple
ity: R-avg

Average Reliability or Availability
Figure-of-Merit for System.
Compare Alternative Systems or
Features with respect to R or A.
Economic optimization of R or A.

Components "average" life or
failure rate.

Analysis Applications:
Conclusions Sought

Required Kinds of
Input Information

is overall plant

(Assurance that all significant contributing factors are accounted for)

specific risks.

Individual initiating event probabilities/consequence effects.

probabilities of alternative uses by complex system or array systems, to defined initiating event.

probability of complex response in terms of random component failure and other events.

Probabilities of external events which affect system response.

Components failure rates, by operating modes and conditions; time-to-repair.

probability of complex system response in terms of random component failures only.

Parts life and failure rate, average and severe conditions.

Age Reliability or Availability
of Merit for System.
are Alternative Systems or
res with respect to R or A.
mic optimization of R or A.

Components "average" life or failure rate.