PB 289714

UCLA-ENG-7528
NOVEMBER 1975

Prepared for the
National Science Foundation
Under Grants GI-39416 and OEP75-20318

"A General Evaluation Approach to
Risk-Benefit for Large Technologcial Systems
and its Application to Nuclear Power"

David Okrent, Project Director

THE EFFECT OF A CERTAIN CLASS OF POTENTIAL COMMON MODE FAILURES ON THE RELIABILITY OF REDUNDANT SYSTEMS

G.E. APOSTOLAKIS

UCLA • SCHOOL OF ENGINEERING AND APPLIED SCIENCE

published by

REPORTS GROUP
SCHOOL OF ENGINEERING AND APPLIED SCIENCE
UNIVERSITY OF CALIFORNIA, LOS ANGELES 90024

BIBLIOGRAPHIC DATA SHEET	1. Report No. NSF/RA-X-75-035	2.	3. Recipient's Accession No. PB 247 914
4. Title and Subtitle: The Effect of a Certain Class of Potential Common Mode Failures on the Reliability of Redundant Systems			5. Report Date: November, 1975 6.
7. Author(s): Apostolakis, George E.			8. Performing Organization Rept. No. UCLA-ENG-7528
9. Performing Organization Name and Address: School of Engineering and Applied Science University of California, Los Angeles Los Angeles, California 90024			10. Project/Task/Work Unit No. 11. Contract/Grant No. OEP-75-20318
12. Sponsoring Organization Name and Address: Office of Energy R&D Policy National Science Foundation 1800 G Street, N. W. Washington, D. C. 20550			13. Type of Report & Period Covered 14.

15. Supplementary Notes: One in a series of reports in a study titled "A General Evaluation Approach to Risk Benefit for Large Technological Systems and its Application to Nuclear Power" (Final Report, NTIS No. PB-280110).

16. Abstracts

A theoretical investigation of the importance of common mode failures on the reliability of redundant systems. These failures are assumed to be the result of fatal shocks (e.g., from earthquakes, explosions, etc.) which occur at a constant rate. The method presented allows analytical prediction of results obtained in the past which showed that the probability of a common mode failure of the redundant channels of the protection system of a typical nuclear power plant was orders of magnitude larger than the probability of failure from chance failures alone. Furthermore, since most reliability analyses of redundant systems do not include potential common mode failures in the probabilistic calculations, criteria are established which can be used to decide either that the common-mode-failure effects are indeed insignificant or that such calculations are meaningless, and more sophisticated methods of analysis are required, because common mode failures cannot be ignored.

17. Key Words and Document Analysis. 17a. Descriptors

Reliability
Redundancy
Statistical Analysis
Nuclear Engineering
Safety Engineering
Nuclear Reactor Safety

17b. Identifiers/Open-Ended Terms

17c. COSATI Field/Group 13M, 14D, 18E, 18I

18. Availability Statement	19. Security Class (This Report)	21.
UNLIMITED	UNCLASSIFIED	
	20. Security Class (This Page) UNCLASSIFIED	22. Price PC A03 MF A01

UCLA-ENG-7528
NOVEMBER 1975

THE EFFECT OF A CERTAIN CLASS OF POTENTIAL COMMON MODE FAILURES ON THE RELIABILITY OF REDUNDANT SYSTEMS

George E. Apostolakis

Prepared for the National Science Foundation
under Grants GI-39416 and OEP75-20318

"A General Evaluation Approach to Risk-Benefit for Large Technological Systems and its Application to Nuclear Power"

Energy and Kinetics Department
School of Engineering and Applied Science
University of California
Los Angeles, California

Preparation of this material was supported, in part, by the National Science Foundation under Grant No. OEP-75-20318. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the National Science Foundation.

PREFACE

This report represents one aspect of a National Science Foundation funded study at UCLA entitled, "A General Evaluation Approach to Risk-Benefit for Large Technological Systems and Its Application to Nuclear Power," (NSF Grant GI-39416). The objectives of this project can be defined to include the following:

1) To make significant strides in the provision of improved bases or criteria for decision-making involving risk to the public health and safety (where a risk involves a combination of a hazard and the probability of that hazard).

2) To make significant strides in the structuring and development of improved, and possibly alternative, general methodologies for assessing risk and risk-benefit for technological systems.

3) To develop improvements in the techniques for the quantitative assessment of risk and benefit.

4) To apply methods of risk and risk-benefit assessment to specific applications in nuclear power (and possibly other technological systems) in order to test methodologies, to uncover needed improvements and gaps in technique and to provide a partial selective, independent assessment of the levels of risk arising from nuclear power.

Reports prepared previously under this grant include the following:

1. Mathematical Methods of Probabilistic Safety Analysis, G. E. Apostolakis, UCLA-ENG-7464 (September 1974).
2. Biostatistical Aspects of Risk-Benefit: The Use of Competing Risks Analysis, H. N. Sather, UCLA-ENG-7477 (September 1974).

3. Applying Cost-Benefit Concepts to Projects which Alter Human Mortality, J. Hirshleifer, T. Bergstrom, E. Rappaport, UCLA-ENG-7478 (November 1974)

4. Historical Perspectives on Risk for Large Scale Technological Systems, by W. Baldewicz, G. Haddock, Y. Lee, Prajoto, R. Whitley and V. Denny, UCLA-ENG-7485 (December 1974)

5. A Prediction of the Reliability of the Core Auxiliary Cooling System for a HTGR, K.A. Solomon, D. Okrent and W. W. Kastenberg, UCLA-ENG-7495 (January 1975)

6. Pressure Vessel Integrity and Weld Inspection Procedure, K. A. Solomon, D. Okrent and W. E. Kastenberg, UCLA-ENG-7496 (January 1975)

7. A Survey of Expert Opinion on Low Probability Earthquakes, D. Okrent, UCLA-ENG-7515 (February 1975)

8. On the Average Probability Distribution of Peak Ground Acceleration in the U.S. Continent due to Strong Earthquakes, T. Hsieh, D. Okrent and G. E. Apostolakis, UCLA-ENG-7516 (March 1975)

ACKNOWLEDGMENTS

The author wishes to thank Drs. G. Weber and L. Caldarola of the Kernforschungzentrum Karlsruhe for several useful comments on the original manuscript.

This work was also partially supported by the Electric Power Research Institute under Contract RP297-1, "Methodology and Application of Probabilistic Evaluation to Thermal-Reactor Safety."

ABSTRACT

This is a theoretical investigation of the importance of common mode failures on the reliability of redundant systems. These failures are assumed to be the result of fatal shocks (e.g., from earthquakes, explosions, etc.) which occur at a constant rate. This formulation makes it possible to predict analytically results obtained in the past which showed that the probability of a common mode failure of the redundant channels of the protection system of a typical nuclear power plant was orders of magnitude larger than the probability of failure from chance failures alone. Furthermore, since most reliability analyses of redundant systems do not include potential common mode failures in the probabilistic calculations, criteria are established which can be used to decide either that the common-mode-failure effects are indeed insignificant or that such calculations are meaningless, and more sophisticated methods of analysis are required, because common mode failures cannot be ignored.

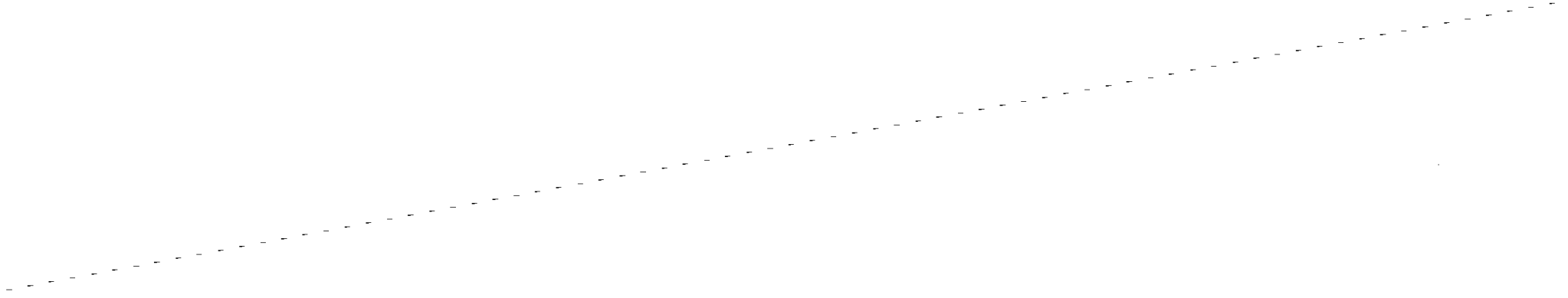

TABLE OF CONTENTS

LIST OF FIGURES

I. Introduction

The subject of common mode failures (cmf) has attracted considerable attention in the study of the safety of complex systems. The recognition of the fact that the appearance of a cmf can eliminate any degree of redundancy employed in the system creates uneasy feelings among safety analysts and undermines the confidence in the results of usual reliability analyses.

Failure of many components due to a single cause is classified as a common mode failure. It is evident from this definition that there is a vast number of potential cmfs even in a simple system and it can be safely assumed that the identification of all of them is simply impossible. Any common property of the components introduces dependencies among them and can result in a cmf. The most obvious common property is the simultaneous presence of the components in the system which makes them vulnerable to events occurring in their common environment, e.g., fires, earthquakes, etc.

The recommended measures against cmfs are naturally based on different forms of diversity. Several broad categories of potential common mode failures are defined and from these various preventative measures are recommended.[1,2,3] A cmf may be attributed to design deficiency, functional deficiency, maintenance error or the external environment. By using different types of equipment, more than one logical way to monitor the state of the system, physically separating redundant components, having more than one operator to review personnel actions, and employing other forms of diversity, it is reasonable to expect that the probability of a common mode failure is reduced. It is evident that in such an approach, the term "probability" is interpreted subjectively, i.e., as a measure of our belief that a common mode failure will not occur in the time interval of interest.

In this work the influence of potential common mode failures on the reliability of redundant systems is examined. First the mathematical model for the common mode failures of concern to us is developed. Then the probability of a common mode failure is compared to the probability of failure of a redundant system when its components are assumed to be subject to chance failures alone. An example of the usefulness of these comparisons is presented, which involves the failure probabilities of the redundant channels of a protection system of a typical nuclear power plant. Finally, more general models are considered, in which the components of a system can be repaired at a constant rate, and the significance of potential common mode failures is examined. The derived simple inequalities can be proven useful in applications, where a decision must be made as to whether common mode failures do not represent a serious threat to the system or the opposite is true and the results of conventional reliability analyses, which consider chance failures only, must be modified to include the possibility of a cmf.

II. The Mathematical Model

The failure of a system to accomplish its intended function is the result of many processes which occur during its lifetime. The time-to-failure T is, of course, a random variable and the objective of a safety analysis is to predict how failures will materialize and, ultimately, to make the mean time to failure as large as possible.

The possible causes of failure of the components of the system will be called risks. A failure mode of the system is a set of risks that have materialized and, as a result, the system has failed.

A risk may affect a single component or groups of components. The materialization of a risk that simultaneously destroys a group of components is what is commonly identified as a common mode failure of these components. A special case of this model, known as the competing-risk model, has been used extensively in biostatistics to analyze the mortality data of populations.[4,5,6] In this case, each risk represents the possibility of death of an individual from a specific disease.

In this work we will assume that failures occur when the components receive a fatal "shock" where a shock is an event which imposes abnormal stresses on the components leading to their failure. A further assumption is that the occurrence of the shocks is governed by independent Poisson processes, i.e.,

$$p(n;\lambda_j) = e^{-\lambda_j t} \frac{(\lambda_j t)^n}{n!} \tag{1}$$

is the probability that exactly n shocks of the j^{th} type (j^{th} risk) occur in the interval $(0,t)$. Equation (1) leads to the exponential failure distribution for the components which are subject to the j^{th} risk, i.e.,

$$F_j(t) = 1 - e^{-\lambda_j t} \qquad (2)$$

A simple application of the above concepts involves a parallel system of two resistors: each has its own failure rate λ_1 and λ_2 and, in addition, both are subject to failure from current surges which occur at a rate λ_{cm}. As a further example, consider the engines of an aircraft. If the explosion of engine 1 can cause failure of engine 2 and the rate of occurrence of this event is $\lambda_{1\to2}$ then this is the failure rate of both engines from this particular risk. Furthermore, explosion of engine 2 may cause failure of engine 1 and this introduces an additional failure rate $\lambda_{2\to1}$. The total failure rate of our theory, λ_{cm} is then $\lambda_{cm} = \lambda_{1\to2} + \lambda_{2\to1}$, that is, the rate λ_{cm} is the sum of the rates of the risks which affect simultaneously both the components. This summation is the result of the assumed independence of the Poisson processes. For more than two components the parameters of the Poisson processes that govern the occurrence of shocks to single components and groups of two, three, etc., must be identified. Shock models were utilized by Marshall and Olkin[7] in their derivation of the multivariate exponential distribution. Further details are discussed in the Appendix.

The above picture of the risks is too general to be useful in applications such as the study of the reliability of the safety systems of nuclear power plants. The difficulty lies in the fact that the parameters of the Poisson processes cannot be estimated. The reason is that even systems which are built to perform the same function under the same, in principle, conditions are not identical. Therefore, failure data collected in the past, if it exists at all, cannot be used in the estimation of the failure rates.

A common assumption regarding the risks to single components is that the corresponding failure rates can be estimated from the failure data of

similar components which were used under similar conditions. This is standard reliability practice for the rate of "chance" failures of components (risks of single components).

Unfortunately, this assumption loses its validity when the risks can affect more than one component, that is, in the case of common mode failures. While it is true that experience from similar systems can be used as a guide to take preventative measures against common mode failures, there is always the possibility that a completely new multiple failure will occur, which will be unique to the system.

In view of these uncertainties, it is evident that a mathematical treatment of common mode failures cannot be as rigorous as the conventional reliability models which involve chance failures only. It can be very useful, however, in determining, under reasonable assumptions, what are the parameters of importance and how they affect the various measures of successful performance of the system, such as, its mean time to failure.

III. Redundancy and Common Mode Failures

In conventional reliability studies each component of a system is assigned a failure rate representing the possibility of chance failures. Then the reliability of various redundant configurations can be calculated.[8,9] A common feature of these results is that the reliability can be made very close to unity if sufficient redundancy is added to the system. In real applications, of course, this is not true since other factors enter the picture which forbid the reliability from being very close to unity. Simple calculations by Epler[10] which included common mode failures led him to the conclusion that there are "serious doubts as to the usefulness of a reliability calculation that considers random events only, when the common mode failure may be dominant by as much as a factor of 10^5". It is the relative importance of chance failures and common mode failures that concerns us here.

Consider a redundant system of n identical units. The failure distribution of each unit from "random causes" is

$$F_r(t) = 1 - e^{-\lambda t}. \tag{3}$$

Let the failure distribution of the system be $\Phi_r(t)$. (When failures are caused by this type of events). Then, it is well known, that if the units are in parallel and k are needed for the system to work, $\Phi_r(t)$ is given by[8]

$$\Phi_r(t) = \sum_{i=0}^{k-1} \binom{n}{i} [1 - F_r(t)]^i \, [F_r(t)]^{n-i} \tag{4}$$

For small λt (less than 0.1) we can use the approximation

$$F_r(t) \simeq \lambda t \tag{5}$$

and write Equation (4) as

$$\Phi_r(t) = \sum_{i=0}^{k-1} \binom{n}{i} (1 - \lambda t)^i (\lambda t)^{n-i}$$

$$\simeq \sum_{i=0}^{k-1} \binom{n}{i} (\lambda t)^{n-i} \quad , \quad \text{for not very large n,} \qquad (6)$$

In the case of standby redundancy (one unit on-line and n-1 units on standby) the failure distribution of the system is

$$\Phi_r(t) = 1 - e^{-\lambda t} \sum_{i=0}^{n-1} \frac{(\lambda t)^i}{i!} \qquad (7)$$

The hazard function of the system is determined by

$$h_r(t) = \frac{1}{1 - \Phi_r(t)} \frac{d\Phi_r(t)}{dt} \qquad (8)$$

Although the expressions of $h_r(t)$ are different for the various types of redundancy, the behavior of the hazard function for small and large times is qualitatively the same. This behavior is in the heart of the concept of redundancy itself. For a system with exponential components $h_r(t)$ is zero at $t = 0$ and it tends to a limit h_ℓ for large times. The limit h_ℓ is the hazard function of the system when it is in its last "good" state, i.e., immediately before failure. Thus, for a k-out-of-n system of identical components $h_\ell = k\lambda$. The type and degree of redundancy determines how rapidly $h_r(t)$ tends to h_ℓ. The higher the redundancy the longer it takes for $h_r(t)$ to start to rise. The behavior for small t can be shown if the expressions for $h_r(t)$ are expanded in Taylor series. Thus for the k-out-of-n system we have[11]

$$h_r(t) = \frac{n!}{(k-1)!\ (n-k)!} \lambda^{n-k+1} t^{n-k} \qquad (9)$$

and for the standby system

$$h_r(t) = \frac{\lambda^{n_t} n-1}{(n-1)!} \cdot \tag{10}$$

Define the quantity

$$H_r(t) = \int_0^t h_r(x)\, dx \tag{11}$$

that is, $H_r(t)$ is the area under the curve $h_r(t)$ from 0 to t; then the probability that the system will survive chance failures is

$$1 - \Phi_r(t) \equiv R_r(t) = e^{-H_r(t)} \tag{12}$$

According to our previous model, a complete analysis of all the risks would have to include risks that affect groups of two, three,...components. It is doubtful, however, that such detailed information will ever be available and, in addition, the computations become unnecessarily complex, which is not justified given the gross uncertainties in the data. The effect of potential common mode failures can be effectively studied, at least qualitatively, by assuming that all the components can be simultaneously destroyed by shocks which occur at a rate λ_{cm}. This rate will have to be estimated using available data, if any, and mainly engineering judgment.

The reliability of the system against common mode failures is then

$$R_{cm}(t) = e^{-\lambda_{cm} t} \tag{13}$$

Since we have assumed independence of the risks, the reliability of the system is

$$R(t) = R_r(t) R_{cm}(t) = e^{-[H_r(t)+\lambda_{cm} t]} \tag{14}$$

and the hazard function of the system is

$$h(t) = h_r(t) + \lambda_{cm} \tag{15}$$

and a typical plot is shown in Figure 1.

From Equation (14) it is evident that no matter the degree of redundancy of the system, its reliability can never be greater than $R_{cm}(t)$.

In Figure 2 the hazard functions $h_r(t)$ and λ_{cm} are plotted again and it is assumed that

$$\lambda_{cm} > h_\ell \tag{16}$$

Then it is obvious that for any t

$$\lambda_{cm} t > H_r(t) \tag{17}$$

and, as a result,

$$R_r(t) > R_{cm}(t) \tag{18}$$

or

$$\Phi_{cm}(t) > \Phi_r(t) \tag{19}$$

that is, the probability of system failure due to common mode failures is always greater than that from random causes.

In Figure 3 it is assumed that

$$\lambda_{cm} < h_\ell \tag{20}$$

Then it is clear that there exists a time T for which the common mode failures again dominate, since

$$\lambda_{cm} t > H_r(t), \quad t < T \tag{21}$$

At time T the areas under the two curves are equal and for $t > T$ the risk of failure from random causes becomes dominant, since

$$\lambda_{cm} t < H_r(t), \quad t > T \tag{22}$$

Clearly, the higher the degree of redundancy the larger T becomes.

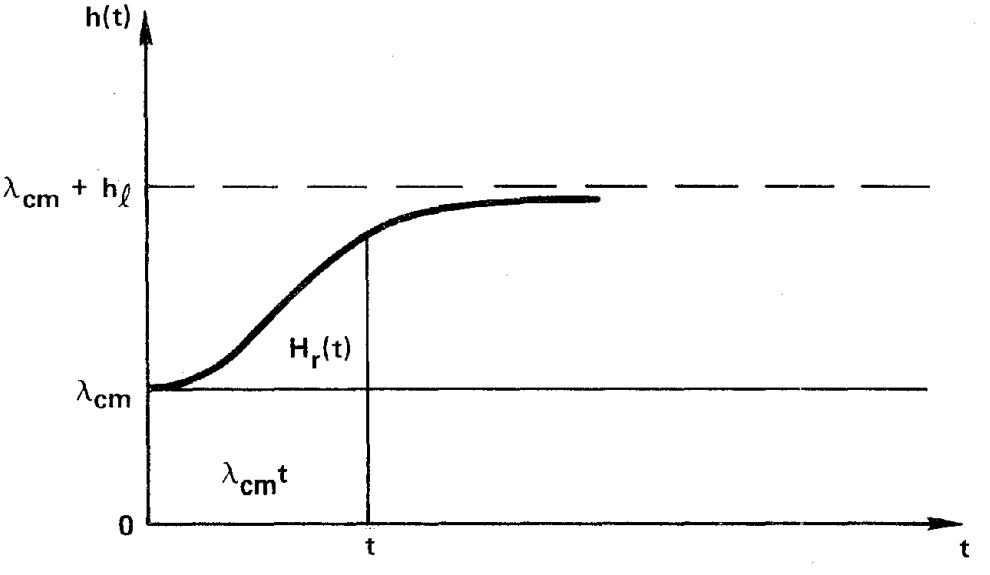

Figure 1. Hazard Function of a System Subject to Random and Common Mode Failures.

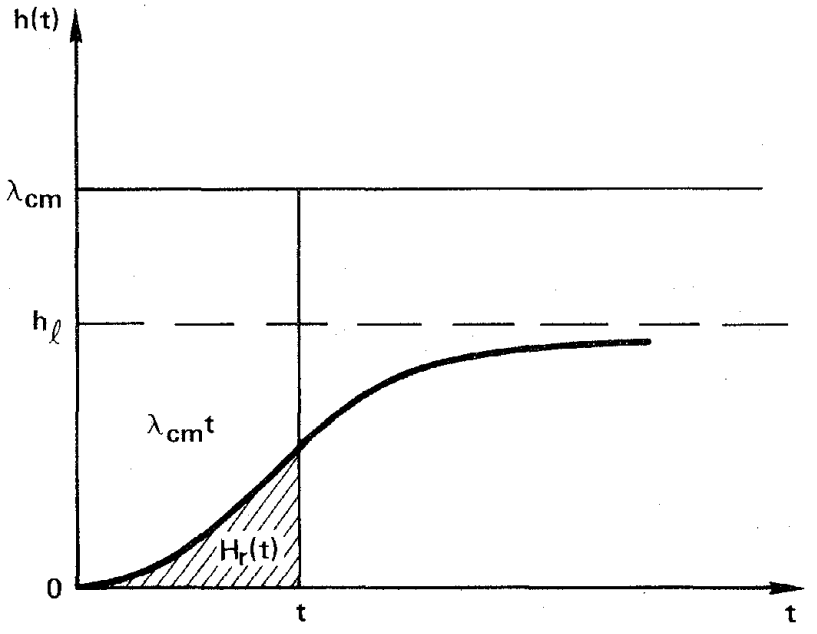

Figure 2. Comparison of the Hazard Functions Due to Random Causes and Common Mode Failures. ($\lambda_{cm} > h_\ell$).

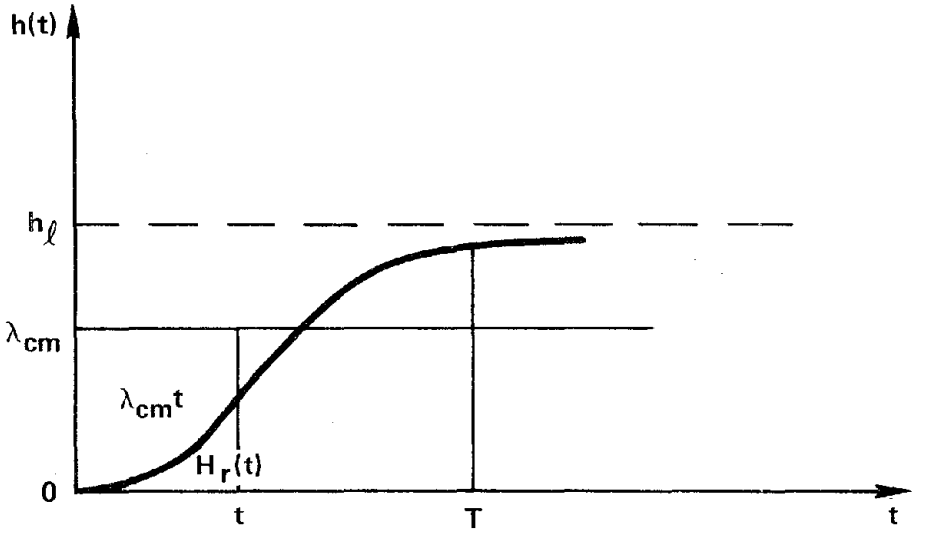

Figure 3. Comparison of the Hazard Functions Due to Random Causes and Common Mode Failures. ($\lambda_{cm} < h_\ell$).

In most practical applications condition (20) is true and the situation just described applies. Furthermore, it is reasonable to expect that, before time T elapses, inspection and corrective action will be taken, because in most cases T is large enough as to make the total reliability unacceptably small for $t > T$.

These results explain readily the calculations of Epler.[10] He assumed that the protection channels of nuclear reactors have a typical common mode failure rate $\lambda_{cm} = 0.01\ yr^{-1}$ and that the failure rate from random causes is $\lambda = 0.1\ yr^{-1}$. The channels are tested every $T_i = 0.1$ yr and the reliability of the channels during this period is of interest.

For one-out-of-n parallel systems the limit h_ℓ equals λ, therefore $h_\ell = 0.1\ yr^{-1}$. Since $\lambda_{cm} T_i$ and $h_\ell T_i$ are both less than 0.1 the approximation (5) can be used for the evaluation of the failure probabilities. Here $\lambda_{cm} < h_\ell$ and the probability of common mode failures is $\lambda_{cm} T_i = 10^{-3}$. The probabilities of random failures are 10^{-4} $(n = 2)$, 10^{-6} $(n = 3)$, 10^{-8} $(n = 4)$. Clearly common-mode-failure probabilities dominate by orders of magnitude. This means that $T_i < T$ according to our model.

These results can be predicted as follows. For the given failure rates and inspection interval we can estimate the range of n (degree of redundancy) for which the probability of common mode failures is less than that of random failures (that is, we estimate the range of n for which $T_i \geq T$). Using Equation (6) for $k = 1$ we find n from

$$(\lambda T_i)^n \geq \lambda_{cm} T_i \qquad (23)$$

which leads to

$$n \leq \frac{\log(\lambda_{cm}\, T_i)}{\log(\lambda\, T_i)} \qquad (24)$$

For the given values of λ_{cm}, λ and T_i we find that n must be less than 1.5, which means that, in this particular case, the common mode failure risk is dominant for any degree of redundancy (i.e., T_i is less than T for $n \geq 2$).

The conclusion is that for redundant systems which are inspected at regular intervals there is an upper bound to the degree of redundancy which can be employed and higher redundancy than the bound is meaningless, since the common mode failure risk becomes dominant. For one-out-of n systems Equation (24) can be used and similar relations can be developed for other types of redundant systems by using Equations (6) or (7).

IV. An Upper Bound on λ_{cm}.

IV.1 The General Case

As indicated previously the rate of occurrence of common mode failures λ_{cm} will have to be estimated based largely on engineering judgment, since no significant data exist. The problem that concerns us here is the derivation of criteria which will help us decide whether λ_{cm} is so small that this type of cmf can be completely ignored in the calculations as being insignificant.

The case we consider here is more general than the situation described in Section III in that the approximation of Equation (5) is not made and more general logical configurations are considered. In addition, repair of the components is possible. As a measure of how good the system is we will use its mean time to failure (MTTF).

Suppose that a redundant system consists of n units each having its own failure rate and that failed components can be repaired. The type of the repair distributions and the number of repairmen is, for the moment, arbitrary. Under these conditions the failure distribution of the system is $\Phi_r(t)$. The calculation of $\Phi_r(t)$ in the general case is not easy; results for two-unit redundant systems under various repair policies are given in Ref. 12. Clearly $\Phi_r(t)$ represents a risk to the system which is the outcome of the competition of the "chance" failures of the components and the repair processes. An independent risk is that of common catastrophic shocks which occur at a rate λ_{cm}. Equation (14) applies again and the failure distribution of the system is

$$\Phi(t) = 1 - [1-\Phi_r(t)]e^{-\lambda_{cm}t} \tag{25}$$

The failure density of the system is then

$$\phi(t) = \phi_r(t)e^{-\lambda_{cm}t} + [1 - \Phi_r(t)]\,\lambda_{cm}\,e^{-\lambda_{cm}t} \tag{26}$$

and its Laplace Transform is

$$\tilde{\phi}(s) = \tilde{\phi}_r(s+\lambda_{cm}) + \frac{\lambda_{cm}}{s+\lambda_{cm}} - \frac{\lambda_{cm}\phi_r(s+\lambda_{cm})}{s+\lambda_{cm}}$$

$$= \frac{\lambda_{cm} + s\tilde{\phi}_r(s+\lambda_{cm})}{s+\lambda_{cm}} \tag{27}$$

Therefore, it suffices to calculate $\Phi_r(t)$ using the usual reliability techniques and then Equation (27) can be used to include common mode failures in the analysis. As it is well known, the mean time to failure is related to the failure density by

$$M = -\frac{d\tilde{\phi}(s)}{ds}\bigg|_{s=0} \tag{28}$$

thus, in the present case,

$$M = \frac{1 - \tilde{\phi}_r(\lambda_{cm})}{\lambda_{cm}} \tag{29}$$

This approach was used by Harris (Ref. 13) to derive the MTTF for one-out-of-two systems. Thus for identical parallel components with failure rate λ and repair rate μ we have that (two repairmen)

$$\tilde{\phi}_r(s) = \frac{2\lambda^2}{s^2+(3\lambda+\mu)s + 2\lambda^2} \tag{30}$$

and from Equation (29) we get

$$M = \frac{3\lambda+\mu+\lambda_{cm}}{2\lambda^2+(3\lambda+\mu)\lambda_{cm}+\lambda_{cm}^2} \tag{31}$$

Since $\tilde{\phi}_r(s)$ is very difficult to obtain we use Equation (29) to derive an upper bound for λ_{cm} in the sense that when λ_{cm} is smaller than the bound, the MTTF of the system M will be very close to the MTTF of the system

ignoring common mode failure effects, say M_r. This M_r is, of course, the mean of the time to failure T_r from chance failures alone.

For small λ_{cm} we can approximate $\tilde{\phi}_r(\lambda_{cm})$ by the first three terms of its Taylor expansion, i.e.,

$$\tilde{\phi}_r(\lambda_{cm}) \simeq 1 - E[T_r]\ \lambda_{cm} + \frac{1}{2} E\left[T_r^2\right] \lambda_{cm}^2 \tag{32}$$

where $E[\cdot]$ denotes expected value, and $E[T_r] \equiv M_r$.

Then Equation (29) gives

$$M \simeq M_r - \frac{1}{2} E\left[T_r^2\right] \lambda_{cm} \tag{33}$$

and the common mode failure effect is negligible if

$$M_r >> \frac{1}{2} E\left[T_r^2\right] \lambda_{cm} \tag{34}$$

As noted by Barlow and Proschan,[14] $E\left[T_r^2\right]$ is often large compared to M_r^2 (and, hence, to M_r), therefore, λ_{cm} must be quite small for Equation (34) to hold.

In applications, redundant systems usually consist of identical components each having a failure rate λ and each can be repaired at a constant rate μ, i.e., the repair distribution is the exponential

$$G(t) = 1-e^{-\mu t} \tag{35}$$

Under these conditions we can calculate M_r and $E\left[T_r^2\right]$ using the theory of birth and death processes and then utilize Equation (34) to express the bound in terms of the failure and repair rates.

IV.2 Birth and Death Processes

A redundant system of n identical units possesses the following mutually exclusive states:

0: all the components are "up"

1: one component is down, (n-1) are up

2: two components are down, (n-2) are up

. .

. .

. .

n: all the components are down,

(the number of each state indicates how many components are down).

Let $P_i(t)$ be the probability that the system is in state i at time t. Then the row vector

$$\underline{P}(t) = (P_0(t), P_1(t),..., P_n(t)) \tag{36}$$

of state probabilities is the solution of the initial value problem

$$\frac{d\underline{P}(t)}{dt} = \underline{P}(t)A \tag{37}$$

$$\underline{P}(0) = \underline{C}$$

where $\underline{C}$ is the initial probability vector. We will assume that all the components are initially good, that is,

$$\underline{C} = (1,0,0,---) \ . \tag{38}$$

A is a (n+1) x (n+1) constant square matrix whose elements are defined as

$i \neq j$, $a_{ij}\Delta t \equiv$ conditional probability that the system will be in state j at time $t+\Delta t$, given that it is in state i at time t,

$$i = j, \quad a_{ii} = -\sum_{\substack{j=0 \\ j\neq i}}^{n} a_{ij}$$

The matrix is determined when the transition rates among states are known.

In the case of exponential failure and repair distributions, the only transitions that can occur are from a state to its immediate neighbors (birth and death process, Reference 14). Then the matrix A is a Jacobi matrix, i.e.,

$$a_{ij} = 0 \text{ for } |i-j| \geq 2 \tag{39}$$

Following the notation of Barlow and Proschan[14] we write A as

$$A = \begin{pmatrix} -\lambda_0 & \lambda_0 & 0 & \cdots & 0 & 0 \\ \mu_1 & -(\mu_1+\lambda_1) & \lambda_1 & & 0 & 0 \\ 0 & \mu_2 & -(\mu_2+\lambda_2) & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & -(\lambda_{n-1}+\mu_{n-1}) & \lambda_{n-1} \\ 0 & 0 & 0 & \cdots & \mu_n & -\mu_n \end{pmatrix} \tag{40}$$

The quantities λ_j and μ_j can be expressed in terms of the failure and repair rates of the components once the logical configuration is known.

Karlin and McGregor (References 14, 15) have developed simple expressions for the mean and the variance of the first-passage time to go from state 0 to state j. They are determined from A without having to solve the system (37).

If we define the quantities

$$\rho_j = \frac{\lambda_0\lambda_1 \cdots \lambda_{j-1}}{\mu_1\mu_2 \cdots \mu_j} \tag{41}$$

$$\rho_0 = 1$$

then, the mean time to reach state j starting from state 0 is given by

$$M_{0j} = \sum_{k=0}^{j-1} \frac{1}{\lambda_k\rho_k} \sum_{r=0}^{k} \rho_r \tag{42}$$

$$M_{00} = 0$$

and the mean of the square of the above time is

$$\gamma_{0j}^2 = 2M_{0j}^2 - 2 \sum_{t=0}^{j-1} \frac{1}{\lambda_t\rho_t} \sum_{r=0}^{t} \rho_r M_{0r} \tag{43}$$

Therefore, having the failure and repair rates of the components and their logical interconnection, we can formulate the matrix of Equation (40) and calculate ρ_j (Equation (41)). If j is the first "bad" state of the system (i.e., the system is down if at least j components are down), Equations (42) and (43) will give M_r and $E\left[T_r^2\right]$ and then Equation (34) can be used to estimate the bound on λ_{cm}. The following examples show such calculations for common systems.

Examples:

m-out-of-n systems with n repairmen.

In this case the elements of matrix A are:

$$\lambda_k = (n-k)\lambda \tag{44}$$

and

$$\mu_k = k\mu \tag{45}$$

Then

$$\rho_k = \binom{n}{k} \frac{1}{x^k} \tag{46}$$

where

$$x = \frac{\mu}{\lambda} \tag{47}$$

If all the units are needed (series system) the only good state is 0 and the first bad state is 1. Then the MTTF is

$$M_r \equiv M_{01} = \frac{1}{n\lambda} \tag{48}$$

and

$$E\left[T_r^2\right] \equiv \gamma_{01}^2 = 2\left(\frac{1}{n\lambda}\right)^2 \tag{49}$$

(as expected, repair does not affect the reliability of the series system). From Equation (34) we get

$$\lambda_{cm} << n\lambda \tag{50}$$

for the common-mode-failure effect to be negligible. This condition could have been derived directly, since the failure rate of the series system is $n\lambda$ and the above inequality simply states that the rate of occurrence of common mode failures must be much smaller than the failure rate of the system.

For a two-out-of-three system we have n = 3 and j = 2. Then

$$M_r \equiv M_{02} = \frac{5\lambda+\mu}{6\lambda^2} \tag{51}$$

and

$$E\left[T_r^2\right] = \gamma_{02}^2 = \frac{(5\lambda+\mu)^2}{18\lambda^4} - \frac{1}{3\lambda^2} \tag{52}$$

and from Equation (34) we get

$$\lambda_{cm} << \frac{6\lambda^2\,(5\lambda+\mu)}{19\lambda^2+10\lambda\mu+\mu^2} \tag{53}$$

If there is no repair we set $\mu \equiv 0$ and we get

$$\lambda_{cm} << \frac{30}{19}\,\lambda \tag{54}$$

When repair is possible, in most applications we have that $\mu >> \lambda$, then (53) reduces to

$$\lambda_{cm} << 6\,\frac{\lambda^2}{\mu} \tag{55}$$

Thus, if we assume that $\lambda = 10^{-6}$ hr^{-1} and $\mu = 10^{-2}$ hr^{-1}, Equation (55) gives

$$\lambda_{cm} << 3\times10^{-10}\ \text{hr}^{-1} \tag{56}$$

and the common mode failures can be ignored in the calculations if they occur at a rate which is at least four orders of magnitude smaller than λ.

Table I summarizes these results for common logical structures. Notice that since λ_{cm} is required to be orders of magnitude smaller than the values of the table, the numerical factors can be ignored in a quick estimation. For nonmaintained systems ($\mu\equiv0$), it suffices to compare λ_{cm} to λ.

For repairable systems we observe that as the redundancy gets higher the bound decreases by powers of $\frac{\lambda}{\mu}$, hence the common-mode-failure rate must be unacceptably small, for the effect to be negligible. As a result, in such systems the results of conventional reliability analyses which consider chance failures alone are meaningless.

Standby Systems

If the system consists of one on-line unit and n-1 units on standby (n repairmen), the elements of the matrix A are:

$$\lambda_k = \lambda \tag{57}$$

and

$$\mu_k = k\mu \tag{58}$$

Therefore,

$$\rho_k = \frac{1}{k!}\frac{1}{x^k} \tag{59}$$

Suppose n = 2 and j = 2 (two-unit standby system). Then we find that

$$M_r \equiv M_{02} = \frac{2\lambda+\mu}{\lambda^2} \tag{60}$$

and

$$E\left[T_r^2\right] \equiv \gamma_{02}^2 = 2\,\frac{(2\lambda+\mu)^2}{\lambda^4} - \frac{2}{\lambda^2} \tag{61}$$

therefore the condition on λ_{cm} is

$$\lambda_{cm} << \frac{(2\lambda+\mu)\lambda^2}{(\lambda+\mu)(3\lambda+\mu)} \tag{62}$$

For $\mu \equiv 0$ Equation (62) gives

$$\lambda_{cm} << \frac{2}{3}\lambda \tag{63}$$

and for $\mu >> \lambda$

$$\lambda_{cm} << \frac{\lambda^2}{\mu} \tag{64}$$

Situations where the number of repairmen is less than the number of units can be handled similarly by finding the appropriate values of μ_k.

Note added in proof

It was pointed out to the author by Dr. Caldarola that for a m-out-of-n system with n repairmen and under the assumption $\mu > > \lambda$ the distribution of T_r tends to become exponential, in which case we have that

$$E[T_r^2] \rightarrow 2M_r^2$$

Then Eq. (34) reduces to

$$\lambda_{cm} << \frac{1}{M_r}$$

Under these assumptions it can be readily shown that

$$\frac{1}{M_r} = \frac{n!}{(m-1)!(n-m)!} \frac{\lambda^{n-m+1}}{\mu^{n-m}}$$

This expression makes possible a rapid calculation of the upper bounds in the last column of Table I.

Table I. Upper bound to λ_{cm} for m-out-of-n systems (n repairmen)

LOGIC m/n	$\mu \equiv 0$	$\mu >> \lambda$
1/2	$\frac{6}{7}\lambda$	$2\frac{\lambda^2}{\mu}$
1/3	$\frac{66}{85}\lambda$	$3\frac{\lambda^3}{\mu^2}$
2/3	$\frac{30}{19}\lambda$	$6\frac{\lambda^2}{\mu}$
1/4	$\frac{60}{83}\lambda$	$4\frac{\lambda^4}{\mu^3}$
2/4	$\frac{156}{115}\lambda$	$12\frac{\lambda^3}{\mu^2}$
3/4	$\frac{84}{37}\lambda$	$12\frac{\lambda^2}{\mu}$

V. Summary

The effect of common mode failures on the reliability of redundant systems has been examined. These failures were assumed to be the result of shocks catastrophic to all the components which occur at a constant rate λ_{cm}.

For non-repairable components it was shown that in practical applications there is always an initial time period (0,T) during which the probability of a common mode failure dominates that of chance failures. As a consequence of this result, if the redundant components are to be inspected every T_i and $T_i < T$, the effort should be directed towards decreasing the potential of a common mode failure, since it is the dominant cause of failure. Conversely, for a given inspection interval T_i there is a maximum degree of redundancy which is effective in reducing the probability of chance failures and further addition of redundant elements is unnecessary, because chance failures are not as important any more.

Finally, the significance of these potential common mode failures was examined in the case of repairable components and useful bounds to λ_{cm} were derived which give a quick estimate of their importance. Because of the uncertainties involved in the determination of λ_{cm} these bounds become even more important in applications.

References

1. I. M. Jacobs, "The Common Mode Failure Study Discipline," IEEE Trans. on Nucl. Sci., Vol. NS-17, pp. 594-598, 1970.

2. W. C. Gangloff and T. Franke, "An Engineering Approach to Common-Mode Failure Analysis," CSNI Specialist Meeting on the Development and Application of Reliability Techniques to Nuclear Plants, Liverpool, April 8-10, 1974.

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

4. C. L. Chiang, Introduction to Stochastic Processes in Biostatistics, Wiley, N. Y., 1968.

5. M. L. Moeschberger and H. A. David, "Life Tests Under Competing Causes of Failure and the Theory of Competing Risks," Biometrics, Vol. 27, pp. 909-933, 1971.

6. D. G. Hoel, "A Representation of Mortality Data by Competing Risks," Biometrics, Vol. 28, pp. 475-488, 1972.

7. A. W. Marshall and I. Olkin, "A Multivariate Exponential Distribution," J. Am. Stat. Assoc., Vol. 62, pp. 30-44, 1967.

8. G. H. Sandler, System Reliability Engineering, Prentice-Hall, Englewood Cliffs, N. J., 1963.

9. M.L. Shooman, Probabilistic Reliability: An Engineering Approach, McGraw-Hill, N.Y., 1968.

10. E.P. Epler, "Common Mode Failure Considerations in the Design of Systems for Protection and Control," Nuclear Safety, Vol. 10, pp. 38-45, 1969.

11. M. Messinger and M. Shooman, "Exponential and Weibull Approximations for Chain Structures," IEEE Proc. Ann. Reliab. Symp., New York, 1968.

12. S. Osaki, "Renewal Theoretic Aspects of Two-Unit Redundant Systems," IEEE Trans. on Rel., Vol. R-19, pp. 105-110, 1970.

13. R. Harris, "Reliability Applications of a Bivariate Exponential Distribution," Operations Research, Vol. 16, pp. 18-27, 1968.

14. R. E. Barlow and F. Proschan, Mathematical Theory of Reliability, Wiley, N. Y., 1965.

15. S. Karlin and J. McGregor, "Coincidence Properties of Birth and Death Processes," Pacific J. Math., Vol. 9, pp. 1109-1140, 1959.

16. S. H. Bush, "Probability of Damage to Nuclear Components due to Turbine Failure," CONF-730304, USAEC, Topical Meeting on Water Reactor Safety, Salt Lake City, March 26-28, 1973.

Appendix

Further details on the shock models that were used in the paper are presented here. We assume for simplicity and without loss of generality that the redundant system consists of two components in one-out-of-two arrangement.

Suppose that certain events which impose high stresses on the components occur according to the Poisson process with rate δ_{cm}. If such an event occurs, then the probability that both components will fail is q_{cm}. We can derive the probability that both components will survive this type of failure in the interval $(0,t)$ by writing

$$R_{cm}(t) \equiv P[\text{both components survive past } t] =$$

$$= \sum_{n=0}^{\infty} P[n \text{ events occur in } (0,t)]\, P[\text{the components survive given the occurrence of } n \text{ events}] =$$

$$= \sum_{n=0}^{\infty} e^{-\delta_{cm} t} \frac{(\delta_{cm} t)^n}{n!} (1-q_{cm})^n \qquad (A.1)$$

Summing the series of Eq. (A.1) we find

$$R_{cm}(t) = \exp(-\lambda_{cm} t) \qquad (A.2)$$

where

$$\lambda_{cm} \equiv \delta_{cm} q_{cm} \qquad (A.3)$$

This is the rate of occurrence of common mode failures as used in the main text. Notice that it is the product of the rate of occurrence of the hazardous events (shocks) and the probability that the event is strong enough to destroy both components simultaneously.

For each component we argue as follows: a shock of the above type may occur that is not strong enough to destroy both components but it may cause failure of the i^{th}, $i = 1, 2$, component with probability $q_{cm,i}$. In addition, shocks that occur at a rate δ_i may destroy this component with probability q_i.

These shocks are assumed to occur independently and they affect only the i^{th} component. The probability that the i^{th} component will not fail in (0,t) is then

$$R_i(t) = \left[\sum_{n=0}^{\infty} e^{-\delta_i t} \frac{(\delta_i t)^n}{n!} (1-q_i)^n\right]\left[\sum_{k=0}^{\infty} e^{-\delta_{cm} t} \frac{(\delta_{cm} t)^k}{k!} (1-q_{cm,i})^k\right] \qquad i = 1, 2 \quad \text{(A.4)}$$

Notice that this is the probability that the i^{th} component will not fail due to a shock that destroys that component only, i.e., the possibility of a common mode failure is not included in Eq. (A.4).

Summing the series in Eq. (A.4) we get

$$R_i(t) = \exp(-\lambda_i t) \qquad , \; i = 1, 2, \qquad \text{(A.5)}$$

where

$$\lambda_i \equiv \delta_i q_i + \delta_{cm} q_{cm,i} \; , \quad i = 1, 2, \qquad \text{(A.6)}$$

This λ_i is the "chance" failure rate of the i^{th} component as used in the text.

It is interesting to compare the derived expressions for the failure rates with the actual practice.

The rate δ_{cm} appearing in Eq. (A.3) represents the rate of occurrence of external events and it may or may not be possible to decrease it. If, for example, the risk under consideration is the possibility of damage due to missiles from the turbo-generator of a plant, δ_{cm} will be the rate of turbine failure, which is about 10^{-4} yr^{-1} (Ref. 16). This is the assessed current value but it is expected to decrease in the future. This is not the case, however, when natural phenomena are considered. There the rate δ_{cm} is constant.

The probability of simultaneous component failure given that the external event has occurred, i.e., q_{cm}, is the one that can be decreased significantly by the various preventative measures that are usually taken, like physical separation of the redundant components. An important difference between δ_{cm} and q_{cm} is that the former can be calculated from statistical data (e.g., from past turbine failures, from the earthquake history of a certain region etc.), whereas the evaluation of the latter is more difficult to do and will possibly require the use of other probabilistic models and engineering judgment (see Ref. 16 for some calculations regarding the probability that an energetic missile from a turbine will strike critical components and that it will cause damage to them).

The above considerations hold true for the individual failure rates also as given by Eq. (A.6). An additional complication arises however due to the term $\delta_{cm} q_{cm,i}$ which implies that, strictly speaking, even the chance failure rate should be adjusted to include the influence of the external events. Such an analysis of the fine details is not usually done, but a failure rate which was derived from the failure record of similar components in similar environments is used. This value contains the corresponding terms of the right side of Eq. (A.6) which pertain to those environments. Since our components are working under similar conditions, the required correction to λ_i is not significant and it can be neglected in a first approximation.

In order to generalize the above concepts to systems with more than two components we have to introduce additional failure rates. Thus for a system with three redundant components we need seven rates, i.e., λ_i, $i = 1, 2, 3$ (the failure rates of the individual components), λ_{ij}, $i \neq j$, $i,j = 1, 2, 3$ (the rate at which components i and j fail simultaneously) and λ_{cm} (the rate of common mode failures). In this case the calculations become considerably

more complicated (e.g., the matrix A of Eq. (40) would not be a Jacobi matrix anymore, since condition (39) would not hold). In addition, such detailed information is not available. We have used only the λ_i and λ_{cm}, because this simplifies the model and makes it possible to derive simple criteria and in addition it is λ_{cm} that is the most crucial, since it represents the possibility of complete simultaneous failure of the components. If it is felt that the simultaneous failure of all but one of the components is also intolerable, our results can be used with an appropriately increased λ_{cm}, i.e., we can make the conservative assumption that the whole system fails when an event actually destroys all but one of the redundant components.