



Safety and Reliability of Reactor Instrumentation with Redundant Instrument Channels

Timmermann, P.; Rasmussen, Jens

Publication date:
1962

Document Version
Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

Citation (APA):
Timmermann, P., & Rasmussen, J. (1962). *Safety and Reliability of Reactor Instrumentation with Redundant Instrument Channels*. Forskningscenter Risø. Denmark. Forskningscenter Risø. Risø-R No. 34

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Safety and Reliability of Reactor Instrumentation
with Redundant Instrument Channels

by

Jens Rasmussen and P. Timmermann

Danish Atomic Energy Commission

Research Establishment Risö

Electronics Department

Abstract

The safety and reliability of reactor instruments and redundant systems are described by the rate of reactor shut downs from safe failures, and the fraction of time, in which unsafe failures exist. The effect of repair and test during operation is considered. The parameters are determined for redundant systems, so as "n out of m" systems.

Contents

	<u>Page</u>
Foreword	5
1. Introduction	7
2. Assumptions	8
2.1. Modes of failure	8
2.2. Instrument channels are independent	9
2.3. Failure rate is constant	9
2.4. Repair and maintenance policy	10
3. System analysis	11
3.1. Single channels	12
3.2. n out of m systems	13
3.3. Other redundant systems	27
4. Example	28
5. Conclusion	30
6. References	31
Appendix 1. Single channel	32
Appendix 2. Mean life of a redundant system	33
Appendix 3. Probability of failure	35
Appendix 4. Dead time	35
Appendix 5. Other redundant systems	37

Author's Foreword

During the installation of the three Danish research reactors at the Risö site, the electronics department encountered the problems connected with the reactor instrumentation and felt an urgent need for gaining more experience in the field of reliability and safety. A collection of failure data and a study of coincidence systems were initiated at an early stage of the work.

The problems have been amplified through the work of the safety committee and the design of large electronic instrumentations for experiments. The work is therefore extended to include studies in component reliability, prediction of instrument failure rates and system analysis.

This report, which is the first in a series, is based on an internal report from 1960. It is intended for use in design work, operational work at the reactors, and in the safety committee. A purely statistical approach has, therefore, been avoided, the weight being laid on the technical side of the problems.

Risö, January 1962.

1. Introduction

A nuclear reactor instrumentation should be capable of accomplishing a protective action when demanded by the physical conditions in the reactor without causing any unwanted shut downs due to environmental conditions or component failures in the instrumentation itself during normal operation.

In the reactor field, safety considerations have been given priority, which has led to the design of instruments with fail to safe features. This has resulted in a high degree of inherent safety, but, due to complexity, also in poor reliability which in itself is an unsafe condition, as an operator is inclined to defeat troublesome instruments.

An improvement of component reliability will increase the safety and decrease the unwanted shut down rate, but the method has a natural limitation. Therefore the principle of redundancy is employed in the instrumentation, and different redundant systems are widely used. The safety and the continuity of operation of these systems are greatly influenced by the number of channels involved, their coupling and of the maintenance and repair policy.

It is of great importance to obtain a measure of the safety build into different parts of the instrumentation in order to reach the same overall standard.

It is of equal importance to be able to predict the operational features to allow an economical evaluation related to unwanted stops, and to be able to make possible corrections in the design.

System reliability has during the last few years received chief attention, especially in the military field. Reactor systems have been treated by Siddall [1] and Jacobs [2] and most recently by Broccardo [3] and Cowper et al [4].

This report describes some of the characteristics of redundant systems by means of a simple probabilistic theory which provides an approximate picture adequate for many problems.

An analysis of redundant systems has to be based on known failure rate figures, but the uncertainty of such figures justifies a simple derivation which provides a comprehensive picture of the problems and assumptions.

Different repair policies may change the characteristics of a redundant system considerably, and the maintenance problems are of great importance in system analysis. The derivation from first principles in this report indicates the order of magnitude and may serve as a guide in preparing operational procedures for repair. A more advanced probabilistic treatment of systems with repair has been given by Barlow et al [5] .

Though the terminology is borrowed from the reactor field, some of the calculations may be useful in other fields, e.g. experimental instrumentation, especially if the automatic data handling is to be applied.

2. Assumptions

Let a parameter in a nuclear plant, i.g. a temperature or neutron flux, be monitored by a group of instrument channels forming a system. A channel may contain transducer, amplifiers, cables, trip-circuits and possibly a shut down mechanism. The following discussion is related to such a system about which some assumptions will be made.

The term trip is used to describe the output condition of a single channel and not necessarily the condition of the reactor. An actual reactor stop is designated a shut down.

2.1. Modes of failure

A component failure can be related to the property of the channel after failure. From a safety point of view, a channel will change in a safe manner, if the failure causes a trip from the channel. It will change to become unsafe, if

a trip signal, after occurrence of a failure, cannot be given when the controlled parameter reaches a dangerous level. In this case the reactor remains unprotected as long as the failure exists. The two modes of failure are called safe and unsafe failures, respectively.

It may happen that an unsafe failure is followed by a safe failure. This will sometimes change the system from an unsafe to a safe state, and will sometimes prevent a failure-trip which would otherwise occur. This situation is disregarded in the present report, and the effects of safe and unsafe failures are treated separately.

2.2. The instrument channels are independent

In the calculations the instrument channels in a system are assumed to be absolutely independent, it is to say a failure in one channel will have no influence on the functioning of other channels.

The coupling between channels may eliminate completely the advantage gained from the use of redundant systems. Therefore, the probability of simultaneous damage to or failure of several channels should be very low. To this end, no component should be common to more channels, and it may be necessary to go as far as to use different routing of the cables in the different channels.

In the case of dependency, the system can be treated as a combination of systems in the calculations.

2.3. The failure rate is constant

It is possible to use a simple mathematical model for system failures only if the failures are assumed to be random events with a failure rate, which is constant in time. This implies that the probability of failure in an arbitrary short time interval is independent of time, viz. not dependent on the age of the instrument.

The model of random events will provide a fairly accurate description of most electronic systems of a certain com-

plexity. Many components will fail in a random way, but even wear out failures will tend to be random when the number of components having this failure mechanism increases. The reason is that the deviation from the mean life time is normally considerable, so that replacement will soon be made at random times. Often replacement is made before a component reaches the wear out state, because wear out is followed by slight changes in the characteristics, which can be found during routine maintenance.

Randomness implies exponential life time distribution as illustrated in appendix 1.

2.4. Repair and maintenance policy

Safety and operational continuity of the system are both greatly influenced by the repair and maintenance policy adopted. Generally, an instrumentation system is checked at fixed time intervals, when instruments are calibrated and failures corrected. In a single channel system this has to be done during shut down periods. In redundant systems it is possible to check and repair the instruments during normal operation.

Safe failures will always give a trip signal, and can therefore be detected immediately by the operating personnel. Unsafe failures may be very difficult to detect during normal operation. Few continuous checking systems are in operation, but the usual way to cope with unsafe failures is by manual routine checking between or during scheduled shut down periods.

Instruments giving a warning for unsafe failures will greatly improve both safety and reliability, and the claim on fail to safe features may be reduced considerably.

Maintenance and repair during normal operation mean that one channel of the system is not in operation, and two conditions are possible: During test and repair the channel may give a trip signal. In this case the safety of the system is not impaired by the repair, but the probability of a spurious shut down is increased. The trip signal may

be defeated during repair; in this case the safety would be lower, but the number of spurious shut downs would not be increased. Normally such a defeat during repair is not used due to the fail to safe philosophy.

3. System Analysis

Different figures of merit have been suggested as characteristics for systems. We have avoided the term reliability, because it may be related to safe as well as unsafe failures.

The ability to maintain operation after safe failures will be characterized either by the rate of unwanted reactor shut downs or by the probability of having no shut downs in a given period.

The fraction of time in which the instrumentation is unable to protect the plant due to unsafe failures will be used to characterize the safety. The term relative dead time is used for this quality.

The following symbols will be used in the system description.

t	time
τ	dead time
D	relative dead time. The proportion of time where the system provides no protection.
T	operation period
T_r	mean repair time
T_t	mean test time
m	number of independent channels in a system
n	number of channel trips necessary for a shut down
s	rate of safe failures
u	rate of unsafe failures
P_f	probability of failure during a certain period
$P_f\{T\}$	probability of failure during period T

3.1. Single channel

The single channel is regarded as the unit of the instrumentation. The rate of safe failures is named s and that of unsafe failures u .

In Appendix I are calculated the probability of survival in a operation period T , the complementary probability of failure P_f in T and the fractional dead time D for a system including only one single channel.

$$P_f = 1 - e^{-sT}$$

$$D = 1 - \frac{1}{uT} (1 - e^{-uT})$$

These are independent of the repair time, since repair on a single channel system can be done only during shut down periods.

When only plant operation time is considered, the spurious shut down rate F will also be the rate of safe failures.

$$F = s$$

In most cases we can assume $uT \ll 1$ and therefore

$$D \approx \frac{1}{2}uT$$

For most instruments s and u are so high that P_f and D reach values which are unacceptable in an instrumentation from which low shut down rate and high safety are required.

Simple series or parallel connections will improve one of the features, but will make the other worse, and only more complicated redundant systems may improve both.

3.2. n out of m systems

We will now discuss a redundant system containing m identical channels measuring the same reactor parameter. By means of a logic circuit, a system shut down is caused when at least n arbitrary channels are in a trip state.

With redundant systems it is possible, and in most cases necessary, to do repairs and tests on the system during operation, and therefore the influence of the maintenance policy on the safety and the number of unwanted shut downs has to be examined.

To illustrate the necessity of a careful choice of the repair policy, the shut down rate for a redundant system is calculated in appendix 2, where repair due to a safe failure of the instrumentation system is carried out only after a plant shut down. It is seen that a 2 out of 3 system gives $F = 6/5 \cdot s$, which is 20 % higher than a single channel.

Shut down from safe failures

The probability of failure in a given time interval and the shut down rate for systems with different repair policies can be found from the probability P_f of shut down for a system without repair during operation.

In appendix 3 is calculated this probability

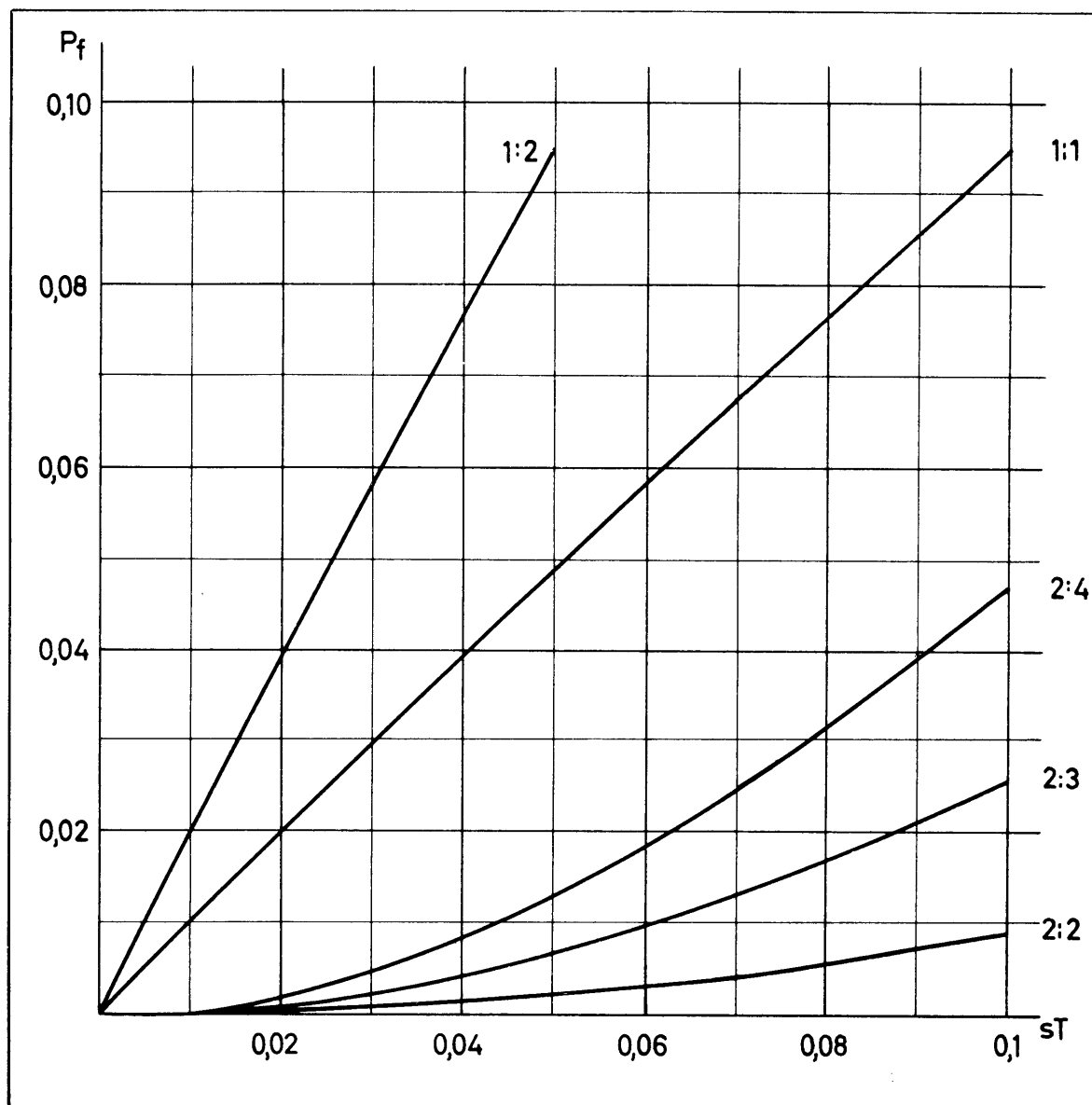
$$P_f \{t, n:m\} = \sum_{x=n}^m \binom{m}{x} (1 - e^{-st})^x (e^{-st})^{m-x}$$

In most cases $(m-n)st \ll 1$, and the following approximations are allowable.

$$P_f \{t, n:m\} \approx \binom{m}{n} (st)^n$$

Figure 1 and 2 show the exact and approximated curves for P_f .

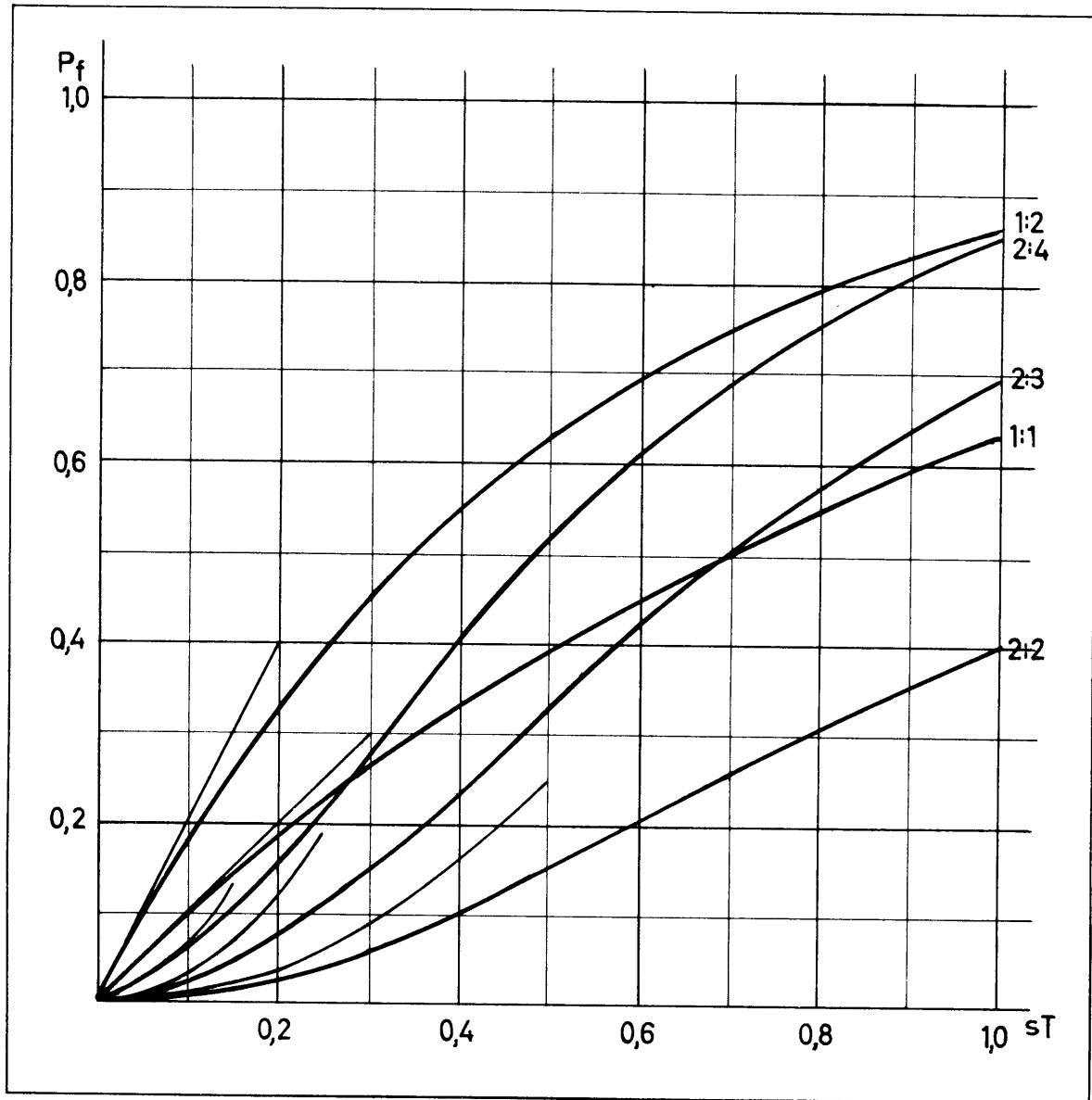
Figure 1



Probability of failure

$$P_f = \sum_{x=n}^m \binom{m}{x} (1-e^{-sT})^x (e^{-sT})^{m-x}$$

Figure 2



Probability of failure

$$— P_f = \sum_{x=n}^m \binom{m}{x} (1 - e^{-sT})^x (e^{-sT})^{m-x}$$

$$— P_f \approx \binom{m}{n} (sT)^n$$

If we assume that repair is carried out either during the scheduled shut down periods or after a system shut down in the operation period, and that the system is quickly re-established to the initial condition, then 2, 3 or more shut downs may occur during an operation period.

This will not affect P_f , which is strictly the probability of "first failures", but F depends on the probability of succeeding failures. If P_f is small, the probability of more than one shut down is negligible and F is simply,

$$F \approx \frac{1}{t} P_f \approx \binom{m}{n} s^n t^{n-1}$$

If P_f is not small, one will have to find the distribution of the number of shut downs in an operation period, and from this the mean number per period. The probability of no shut down is $1-P_f$. The probability of one shut down can be calculated from the distribution of life times for two systems coupled in sequence (in time). The following probabilities of 2, 3, 4 shut downs are found in a similar way, but are normally converging very fast to zero. The approximate expressions for F are given in table 1 for the lowest order systems.

Table 1

The probability of failure P_f and failure rate F

No repair during operation

Approximations applying to $(m-n)st \ll 1$

System	1:1	1:2	2:2	1:3	2:3	3:3	1:4	2:4	3:4	4:4
P_f	st	$2st$	$(st)^2$	$3st$	$3(st)^2$	$(st)^3$	$4st$	$6(st)^2$	$4(st)^3$	$(st)^4$
F	s	$2s$	$s^2 t$	$3s$	$3s^2 t$	$s^3 t^2$	$4s$	$6s^2 t$	$4s^3 t^2$	$s^4 t^3$

Repair and test. Influence on P_f

If the system is designed to give a warning on safe channel failures, repair of the failure could be done during plant operation, and the repair time would have to be introduced in the formulas and detailed knowledge concerning the repair time be necessary. To avoid complications an average repair time T_r is used, which is justified by the fact that s and u will be known only with a certain (low) degree of accuracy.

Furthermore, it is necessary to clarify the state of the instrumentation system in the time interval between the occurrence of a safe failure and the channel recovery when the failure has been corrected; i.e. the functioning of the system operating during this period has to be defined. A n out of m system with a safe failure in one channel is acting as a " $n-1$ out of $m-1$ " system, if the channel remains in the trip state, but if the channel is defeated during repair, the system would be reduced to a " n out of $m-1$ ".

It is also easy to account for any test procedure during operation. As most instruments are not designed to give a warning for unsafe failures, it may be necessary to carry out test on the system during plant operation to increase the safety; during such tests the system would again be functioning as a " $n-1$ out of $m-1$ " or a " n out of $m-1$ " system according to the test procedure.

If safe failures in an n out of m system are repaired within the time T_r following a warning, and the repair time is short in comparison with the mean time between failures, the rate of "first failures" in the system would with good approximation be $m \cdot s$.

A channel failure will lead to a system failure only if the system formed by the remaining $m-1$ channels fails to safe during the repair period. Normally, the repair is done with the failed channel in a safe state, and the remaining system would thus be a $n-1$ out of $m-1$ system. The probability that this system will fail safe during T_r , is $P_f \{T_r, n-1:m-1\}$ which is given in appendix 3, and the result-

ing shut down rate for the total system will be,

$$F = m \cdot s \cdot P_f \left\{ T_r, n-1:m-1 \right\}$$

The approximated figures for different systems are given in table 2.

Table 2

Failure rate with repair of safe failures within T_r

Approximate expressions

System	1:1	1:2	2:2	1:3	2:3	3:3	1:4	2:4	3:4	4:4
F	-	-	$2s^2T_r$	-	$6s^2T_r$	$3s^3T_r^2$	-	$12s^2T_r$	$12s^3T_r^2$	$4s^4T_r^3$

If the system is tested for unsafe failures during plant operation with a test rate f_t per channel in such a way that the channel is tripped in the test period T_t , then the total shut down rate would be

$$F = m \cdot s \cdot P_f \left\{ T_r, n-1:m-1 \right\} + f_t \cdot m \cdot P_f \left\{ T_t, n-1:m-1 \right\}$$

Generally we have

$$F = \sum f_i \cdot m \cdot P_i$$

where f_i is the frequency of the periods in which a channel is in an abnormal state, and P_i is the probability of a shut down from the remaining system in these periods.

It may be of interest to calculate the probability of a plant shut down in a given operation time T .

The channel failures occur at random at the rate $m \cdot s$. If the repair time T_r is short in comparison with the time between scheduled down periods, the probability of a plant shut down would be the same for all repair periods, and in this case the shut downs would also be random. Thus the probability of a system failure in the time T is,

$$P_f = 1 - e^{-T \cdot m s P_f \{T_r, n-1:m-1\}}$$

This should be combined with the probability of failure during testing periods which, however, is easily calculated, since the number of testing periods during T will be known.

Example

As an example is chosen a n out of m system. Repair of a safe channel failure is done within T_r with trip, and testing for unsafe failures is done with a frequency f_t with channel in the safe state, during time interval T_t . Then the above formula gives,

$$F = m \cdot s \cdot \binom{m-1}{n-1} \cdot (s T_r)^{n-1} + f_t \cdot m \binom{m-1}{n-1} (s \cdot T_t)^{n-1}$$

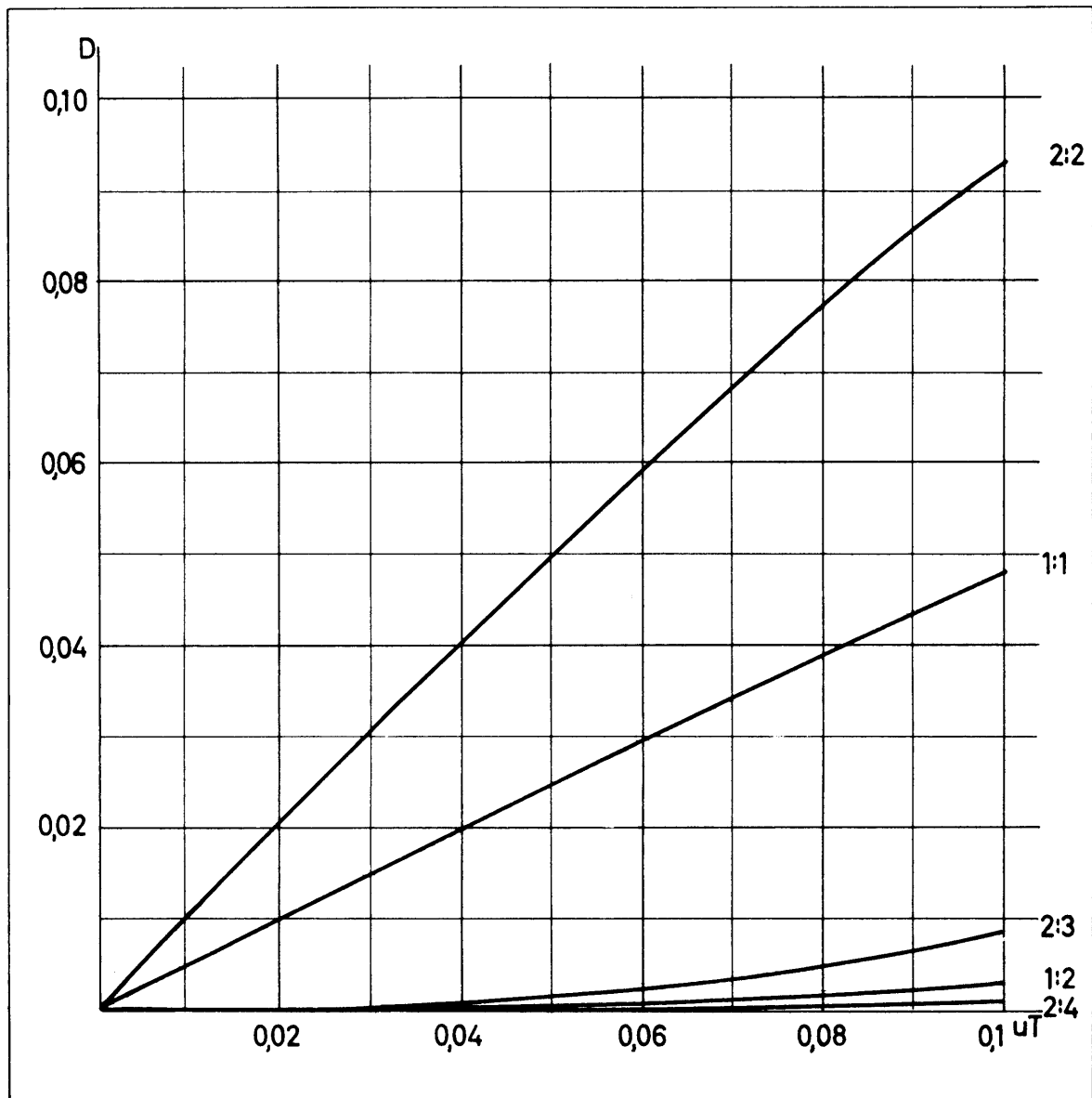
$n=2$ and $m=3$ gives,

$$F = 6s^2 T_r + 6s f_t T_t$$

Dead time from unsafe failures

The system is unable to protect the plant if there is an unsafe failure in more than $m-n$ channels, and the fraction of the operating time during which the system is unsafe has to be calculated.

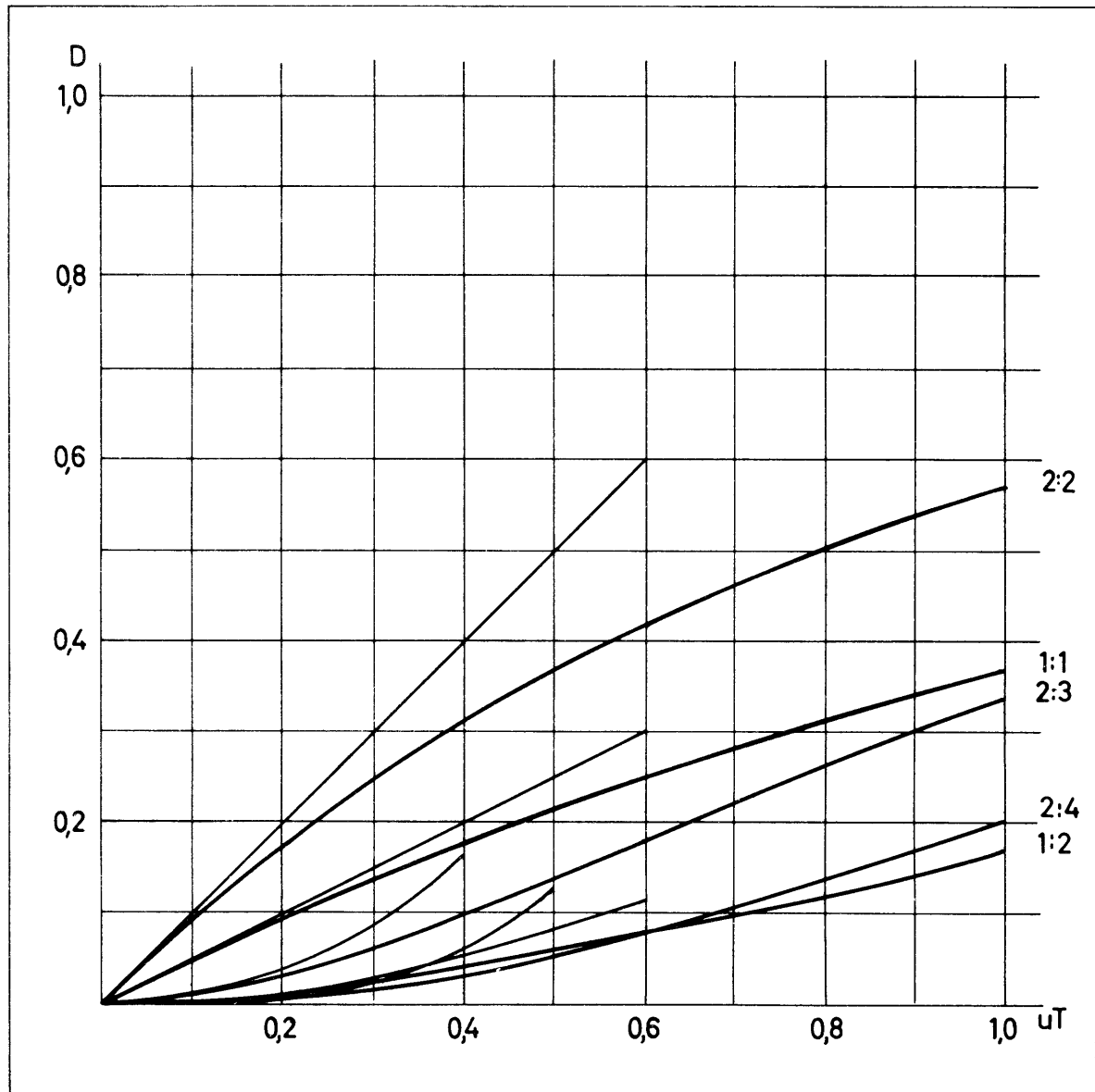
Figure 3



Relative dead time

$$D = \frac{1}{T} \int_0^T \binom{m}{m-n} (1-e^{-ut})^{m-n} (e^{-ut})^m (T-t) n u dt$$

Figure 4



Relative dead time

$$— D = \frac{1}{T} \int_0^T \binom{m}{m-n} (1-e^{-ut})^{m-n} (e^{-ut})^m (T-t)^n u dt$$

$$— D \approx \frac{m!}{(m-n+2)!(n-1)!} (uT)^{m-n+1}$$

If the system is known to be operating properly at the beginning of a period T and no test or repair is carried out, the mean dead time to be expected would be,

$$\tau \{ T, n:m \} = \int_0^T \binom{m}{m-n} (1-e^{-ut})^{m-n} (e^{-ut})^n (T-t)^n \cdot u dt$$

as found from appendix 4.

In most cases the approximation $nuT \ll 1$ holds, and one gets,

$$D = \frac{1}{T} \cdot \tau \{ T, n:m \} \approx \frac{m!}{(m-n+2)!(n-1)!} (uT)^{m-n+1}$$

The relative dead time is given for different systems in table 3 and the range in which the approximation holds is shown in figs. 3 and 4.

Table 3

Relative dead time caused by unsafe failures
No repair of unsafe failures during operation

Approximations applying to $nuT \ll 1$

1:1	1:2	2:2	1:3	2:3	3:3	1:4	2:4	3:4	4:4
$\frac{1}{2}(uT)$	$\frac{1}{3}(uT)^2$	(uT)	$\frac{1}{4}(uT)^3$	$(uT)^2$	$\frac{3}{2}(uT)$	$\frac{1}{5}(uT)^4$	$(uT)^3$	$2(uT)^2$	$2(uT)$

Repair and test. Influence on dead time

In redundant systems test can be carried out during plant operation. Table 3 can still be used, if T means time between tests and not operation time.

The influence on dead time from repair and maintenance periods will now be discussed. The calculation is more intricate than was the case of the shut down rate, since unsafe failures may be present in the system when a test period for unsafe failures or a repair for safe failures begins.

In these periods the system in operation is changed to a more simple system as mentioned earlier, and the contribution to the dead time from these periods has to be estimated.

If a channel is in a tripped state during test or repair, the number of faults necessary to make the system unsafe will remain unchanged. As the number of channels is one less during maintenance, the chance to get unsafe failures is reduced. But as the maintenance time is only a small fraction of the operation time, the dead time is only slightly decreased.

If a channel is defeated during test or repair, the situation is greatly changed. Defeat of a channel means that an unsafe failure is introduced at the beginning of the maintenance period. If $n-1$ unsafe failures already exist and an unsafe channel is not removed by chance, the system would be dead during the whole maintenance period, and consequently, the total dead time will be considerably increased. Especially for simple systems there is a considerable chance of $n-1$ failures at the start of a repair.

Example

By way of illustration, a 2 out of 3 system is discussed. First we will consider a test period T_t per channel. The three channels are tested in sequence so that the total test time is $3 T_t$, placed at the end of T .

If no unsafe failure exists when the test starts, the system is reduced to a 2 out of 2 and the contribution to the total dead time is still insignificant.

In the case of an unsafe failure in one channel (with probability $3uT$) and this channel is not taken out for test in the first test period (with probability $2/3$), then the system would be unsafe during the whole test period. This means that the average contribution to the dead time from the test interval would be $\tau_1 = 3 uT \cdot \frac{2}{3} \cdot T_t$.

The second time interval would be unsafe if the unsafe failure still remains in the system (probability $\frac{2}{3} \cdot \frac{1}{2}$), so that this interval gives a contribution of $\tau_2 = 3 uT \cdot \frac{1}{3} \cdot T_t$.

The third interval will never be unsafe because of an earlier failure, so we get the total $\tau = \tau_1 + \tau_2 = 3 uT T_t$.

The mean relative dead time including the period of operation is then

$$D = (uT)^2 + 3 uT T_t$$

disregarding the insignificant contributions from the reduced system itself.

The contribution from T_t can be greater than the basic dead time not only when T_t is increased, but also when T is decreased even with $\frac{T_r}{T}$ being constant.

If repair time from safe failures is considered and channels are defeated, T_t would have to be changed to T_r . The safe failures occur with probability $3sT$, but the repair intervals will be distributed over the whole period T . The mean arrival will be in the middle of the period and the probability of a preceeding unsafe failure is $3u\frac{T}{2}$. Then the contribution to the dead time is $\tau_3 = 3sT \cdot 3u\frac{T}{2} \cdot \frac{2}{3} T_r = 3suT^2 T_r$.

Here it must be borne in mind that a channel will normally be in a safe state during repair, whereas it will often be unsafe (defeated) during test or at least some part of the test period due to improper test procedure i.e. dismantling of the channel for connecting simulated inputs.

Warning from unsafe failures

The claim on "fail to safety" characteristics of the instruments in safety systems is due to the fact that normally unsafe failures are only detectable by test procedures. Tests are normally carried out manually at rather long time intervals, and therefore fail safe instruments are necessary to obtain a high degree of safety.

Fail safe instruments are often highly complex instruments, and their additional components may cause a considerable number of safe failures, and in some cases it may be doubtful whether the absolute number of unsafe failures is really lower than with instruments of a more simple design.

The claim on fail to safety features may be less strong if the intervals between testings are short, as may be the case with an automatic testing system. Such a system should, however, be used with great care. It is difficult to design a system that will not merely pass the fail to safety problems from the safety system on to the test system. Furthermore, it should be possible by the system to detect all unsafe failures, and no coupling should be introduced between the different channels of the system.

Another approach is to try and design the single measuring channels so as to become continuously self-checking in such a way that an unsafe fault will give a warning signal just as the safe faults do. In a radiation monitoring system for example, a great number of unsafe failures may be detected simply by raising the "no radiation" reading by means of a small radioactive source placed on the detector, and to let the system give a warning when reading is zero. If this principle could be extended to detect all unsafe failures, the dead time would be reduced very significantly, and periodic tests would be unnecessary. In that case dead time could appear only in the periods of repair of safe or unsafe failures. If we include as above, the time from the warning is given until the actual repair

is started, in T_r , and this delay is considered a main part of T_r , then a safe failure would result in a $n-1$ out of $m-1$ system, and an unsafe failure in a n out of $m-1$ system. In this case the relative dead time is determined by,

$$D = m \cdot s \cdot \mathcal{T}\{T_r, n-1:m-1\} + m \cdot u \cdot \mathcal{T}\{T_r, n:m-1\}$$

where \mathcal{T} can be calculated from the expressions in table 3 after multiplication by T_r .

$$D = 3 \cdot s \cdot \frac{1}{3} u^2 T_r^2 \cdot T_r + 3u^2 T_r^2 = u^2 T_r^2 (sT_r + 3) \quad 3u^2 T_r^2$$

which normally is considerably lower than the no warning case where $u^2 T_r^2$ is the most significant part.

It must be borne in mind that this low figure is only realistic if no coupling is introduced between the channels, and if no unsafe faults arise without actuating the warning signal.

Safety and reliability of combined systems

In most cases a plant is monitored by several independent systems. In reactor safety instrumentation for instance, there will be independent systems for neutron flux, coolant temperature and flow etc. These systems will all be capable of ensuring unwanted shut downs, and if one mechanism fails the plant will most likely be properly protected by the remaining systems. In this way the reliability of the combined system will be lower and the safety higher than the figures obtained for a single coincidence system.

Generally, the shut down rate for the combined system is simply the sum of the shut down rate for the different sub systems, but the safety cannot be adequately described by a single figure for the entire installation, and the question whether the remaining systems will protect the plant when one system is unsafe, and consequently one plant parameter is not monitored, cannot be answered without detailed knowledge of the reactor and the accident considered.

3.3. Other redundant systems

A "n out of m" system is sometimes so arranged that only certain combinations of n channels can cause a shut down. In the two systems most commonly used, the channels are so grouped that either all channels in one group or one channel in each group must trip to operate a shut down.

The former system, which will be named system A, consists of k groups each containing n channels. All channels in one group must trip before a stop occurs. The latter system, system B, consists of n groups each containing k channels. One channel in each group must trip before a stop occurs. References to series or parallel connections are avoided, because they are not clearly defined.

Appendix 5 calculates the probability of failure P_f and dead time D.

In case repair is not carried out during operation the results are:

The system A (all channels in one group) gives,

$$P_f = 1 - \left\{ 1 - (1 - e^{-st})^n \right\}^k$$

and system B (one channel in each group) gives,

$$P_f = (1 - e^{-kst})^n$$

The approximated expressions are,

$$\text{For system A: } P_f \approx k(st)^n \quad D \approx \frac{n^k}{k+1} (uT)^k$$

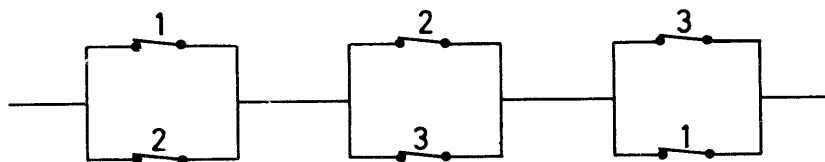
$$\text{For system B: } P_f \approx k^n (st)^n \quad D \approx \frac{n}{k+1} (uT)^k$$

In the approximate expressions, P_f depends on st in the same way as a real "n out of m" system, where $P_f \approx \binom{m}{n} (st)^n$.

If repair is done on channels during operation, the system will not be reduced to a system of the same type but of a lower order, as was the case in earlier calculations. If we consider a system A with k groups each containing n channels, the remaining system during repair will consist of $k-1$ groups each containing n channels and in addition one group containing $n-1$ channels. The repair case is discussed in appendix 5.

4. Example

The following example will show the advantage gained by using a "1 out of 2" or "2 out of 3" system instead of a single channel.



The figure symbolizes a "2 out of 3" system. The contacts are supposed to open when a channel is tripped.

As realistic average figures for instruments in reactor instrumentation are chosen

$$s = 5 \text{ failures per year}$$

$$u = 0.5 \quad " \quad " \quad "$$

Channel tests for unsafe failures are assumed to be 5 min. = 10^{-5} yr. per channel and the repair time for both safe and unsafe failures is set to be 0.5 h = $6 \cdot 10^{-5}$ yr.

A normal program for a research reactor is a 3 weeks operation ($= 6 \cdot 10^{-2}$ yr) followed by a shorter or longer shut down period. Therefore, the time unit used in the example means an operation year and not a calendar year.

The probability of failure during an operation period (3 weeks) P_f , the mean number of failures per year F , and

the dead time D are calculated to be, with no repair during plant operation

	1:1	1:2	2:3
P_f	0.26	0.45	0.15
F	5	10	3.0*
D	1.5%	0.03%	0.09%

If repair is carried out immediately after failure, the probability of shut down would be considerably reduced. This, of course can be done only in a "2 out of 3" system. If test for unsafe failures is carried out, the dead time is decreased, and the shut down rate increased. It is assumed that the channel is tripped during repair and test.

2:3 system				
	no test	1 week test	8 hour test	
P_f	$6 \cdot 10^{-4}$	10^{-3}	$2 \cdot 10^{-2}$	
F	$9 \cdot 10^{-3}$	$2 \cdot 10^{-2}$	0.3	shut downs pr. year
D	0.09%	0.01%	$2.5 \cdot 10^{-5}\%$	

P_f is still the probability of failure in a 3 week operation period.

* This figure is calculated from the distribution of number of shut downs as indicated on page 16. Regarding only the possibility of zero or one failure per operation period would give $F = 2.5$.

If defeat takes place, the dead time is calculated according to

$$D = (uT)^2 + 3 uT_t$$

which gives,

with no test	$D = 0.09\%$
" 1 week test	$D = 0.01\% + 0.0015\% = 0.01\%$
" 8 hour test	$D = 2.5 \cdot 10^{-5}\% + 0.0015\% = 1.5 \cdot 10^{-3}\%$

It is possible to introduce a warning for unsafe failures, and to assume that an unsafe failure is repaired in half an hour. Following a warning the channel may be immediately switched to a safe condition or it may remain unsafe until repair is finished.

For a "2 out of 3" system,

$$D = 3 \cdot 10^{-7}\% \text{ with defeat of channel (unsafe)}$$

$$D = 3 \cdot 10^{-11}\% \text{ " no " " " (safe)}$$

It will be clear that the characteristics of the system in practice is not determined by these last figures, but rather by a more unreliable functioning of checking circuits and logic systems, but this is not considered here.

5. Conclusion

In the preceeding discussion an attempt has been made to show an approach to an instrumentation which could at the same time have safe features and a good operational record.

The calculations serve as a comparison of different systems working under equal conditions. It is realized that

the figures obtained are only approximate figures. Low figures, especially, must be used with great care, because the reliability in this case may be governed by factors not dealt with in this report.

The conclusion is that the characteristics of a system can be greatly changed by using different repair and test policies. Therefore, reliability is not fed into the instrumentation at the design state alone, but has to be combined with suitable operational directions. Redundant systems of low order can be given so good records that fail to safety features of the channels can be reduced, without impairing the safety.

When the magnitude of safe and unsafe failure rates is known, this report can serve as a guide to the choice of a proper system that will increase the reliability and safety of a single group of instruments to some level common to the whole reactor including the mechanical equipment.

6. References

- [1] E. Siddall, A Study of Serviceability and Safety in the Control System of the NRU Reactor. AECL 399(CRNE 582), Nov. 1954.
- [2] I.N. Jacobs, Safety Systems for Nuclear Power Reactors, AIEE-Pacific general meeting, paper 57-906, Nov. 1957.
- [3] U. Broccards, Safety and Serviceability in Reactor Instrumentation Safety Circuits. Nuclear Power, June, July, October 1961.
- [4] M.J. Cowper and D. Wray, Reliability of Protective Systems for Zero Energy Reactors. AHSB(S)R-23 Harwell 1961.
- [5] R.E. Barlow and L.C. Hunter, Mathematical Models for System Reliability, Sylvania Technologist, Jan. and April 1960.

Appendix 1

Shut down failures and dead time for a single channel system

In this appendix safe and unsafe failures are treated separately. An examination of the actual circuit may show that a safe failure will not always be followed by a trip because of an existing unsafe failure. This depends on the mutual effects of the failures.

The rate of safe failures is named s and that of unsafe failures u .

The basic assumption of randomness implies that the probability of safe failure occurring in a short time interval Δt , is $s\Delta t$, independent of the location of Δt on the time axis. The complementary probability of no failure during Δt is $1-s\Delta t$.

If a time interval t is formed by n intervals of length Δt , then the probability of survival of t is

$$(1-s\Delta t)^n$$

which expresses the combined probability of survival in each time element Δt . If $\Delta t \rightarrow 0$ with $n \cdot \Delta t$ being constant then

$$(1-s\Delta t)^n \rightarrow e^{-st}$$

which gives the well-known exponential distribution.

Unsafe failures can be treated similarly.

Shut down failures

If an instrument is operating at $t=0$, the probability, dP , of obtaining a life time between t and $t+dt$ is the combination of survival between 0 and t and failure between t and $t+dt$, which is $dP = e^{-st} \cdot sdt$.

The mean life time is then

$$\int_0^{\infty} t \cdot e^{-st} \cdot sdt = \frac{1}{s}$$

The probability of failure in a time interval T is the complement to probability of survival and thus:

$$P_f = 1 - e^{-sT}$$

Dead time

The probability, dP , of obtaining an unsafe failure between t and $t+dt$ is $dP = e^{-ut} u dt$. An unsafe failure is detected by testing during scheduled shut down periods and consequently repair takes place at $t = T$. The system is thus in an unsafe state in the time interval $T-t$.

The mean unprotected time per period T is,

$$= \int_0^T (T-t) e^{-ut} \cdot u dt = T - \frac{1}{u} (1 - e^{-uT})$$

and the fractional dead time,

$$D = 1 - \frac{1}{uT} (1 - e^{-uT})$$

If $uT \ll 1$, then $e^{-uT} \approx 1 - uT + \frac{1}{2}(uT)^2$ and

$$D \approx \frac{1}{2} uT.$$

This may be seen directly, since u is the frequency of unsafe periods and $\frac{1}{2}T$ their mean length.

Appendix 2

Mean life of a redundant system

A "n out of m" system would give a shut down between t and $t+dt$ if $n-1$ failures have occurred between 0 and t ,

and one failure occurs between t and $t+dt$.

The probability of failure in the $n-1$ first channels is $(1-e^{-st})^{n-1}$, and of no failure in the rest of the channels $(e^{-st})^{m-n+1}$. $n-1$ numbers can be drawn from m in

$$\binom{m}{n-1} = \frac{m!}{(m-n+1)!(n-1)!}$$

different ways, so that $n-1$ failures during the time, t , has a probability,

$$P_f \left\{ t, n-1 : m \right\} = \binom{m}{n-1} (1 - e^{-st})^{n-1} (e^{-st})^{m-n+1}$$

The probability of one or more channel failures in the remaining $m-n+1$ channels between t and $t+dt$ is

$$1 - (1 - sdt)^{m-n+1} \approx (m-n+1) sdt.$$

A life time between t and $t+dt$ for the system has thus a probability

$$dP = \binom{m}{n-1} (1 - e^{-st})^{n-1} (e^{-st})^{m-n+1} \cdot (m-n+1) sdt$$

Then the mean life is,

$$\frac{1}{F} = \int_0^{\infty} t \cdot dP$$

and the shut down rate

$$F = \frac{1}{\int_0^{\infty} t \cdot dP}$$

For a "2 out of 3" system the formula gives $F = \frac{6}{5} s$, from which is seen that with repair only after a system failure, this system would not be preferable.

To get the full benefit of redundant systems, it is necessary to repair within a reasonable short time after a channel failure.

Appendix 3

Probability of failure

Appendix 2 calculates the probability of obtaining exactly $n-1$ failures

$$P_f \{t, n-1:m\} = \binom{m}{n-1} (1 - e^{-st})^{n-1} (e^{-st})^{m-n+1}$$

in m identical channels during time t .

If n failing channels produce a shut down, then the probability of no shut down is equal to the probability of failure in less than n channels:

$$P = \sum_{x=0}^{n-1} \binom{m}{x} (1 - e^{-st})^x (e^{-st})^{m-x}$$

and the complementary probability of shut down,

$$P_f \{t, n:m\} = \sum_n^m \binom{m}{x} (1 - e^{-st})^x (e^{-st})^{m-x}$$

Appendix 4

Dead time

If more than $m-n$ channels have failed to unsafe, the system will not protect the plant.

The probability that the system becomes inoperative at the time t is the combined probability that $m-n$ channels have failed unsafe in the period t and that one more chan-

nel fails to unsafe between t and $t+dt$:

$$dP_u = \binom{m}{m-n} (1 - e^{-ut})^{m-n} (e^{-ut})^n \cdot n u dt$$

The mean unprotected time during operation period T is therefore,

$$\tau = \int_0^T (T-t) dP_u$$

This integral can be solved using,

$$\int_0^T (T-t) k \cdot e^{-kt} dt = T - \frac{1}{k} (1 - e^{-kt})$$

If $uT \ll 1$

$$\tau \approx \binom{m}{m-n} n u \int_0^T (u t)^{m-n} (T-t) dt$$

$$= \frac{m!}{(m-n+2)!(n-1)!} (T)^{m-n+2} u^{m-n+1}$$

and the relative dead time

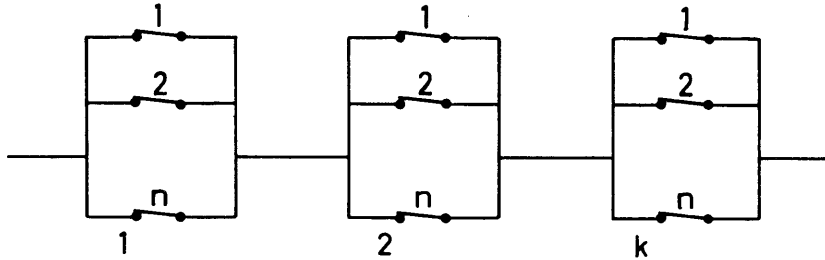
$$D \approx \frac{m!}{(m-n+2)!(n-1)!} (uT)^{m-n+1}$$

Appendix 5Other redundant systems

The probability of failure and dead time is calculated for the two systems, A and B, assuming first no channel repair during operation and secondly channel repair within the time T_r after failure

System A m channels are divided into k groups, each containing n channels. All channels in one group must trip before a stop occurs.

The system can be symbolized in the following way, assuming that a trip opens a relay contact.



The probability of failure in a group is $(1 - e^{-sT})^n$. The probability of no shut down for the whole system is then $[1 - (1 - e^{-sT})^n]^k$ and the complementary probability of failure,

$$P_f = 1 - [1 - (1 - e^{-sT})^n]^k$$

Approximations give,

$$P_f \approx k(sT)^n$$

$$F \approx k s^n T^{n-1}$$

The relative dead time is given by

$$D = \frac{1}{T} \int_0^T (T-t) dP_u$$

where dP_u is the probability of an unsafe system failure between t and $t+dt$ if the system is functioning at t . This would happen if at least one channel in $k-1$ groups has failed at t , and then the first failure in the last group occurs between t and $t+dt$.

The probability of no failure in a group is $(e^{-ut})^n$, and the probability of failure in $k-1$ groups is then $[1 - (e^{-ut})^n]^{k-1}$. The $k-1$ groups can be chosen in k ways. The probability of a first failure in the last group is $e^{-nut} \cdot n u dt$, so that

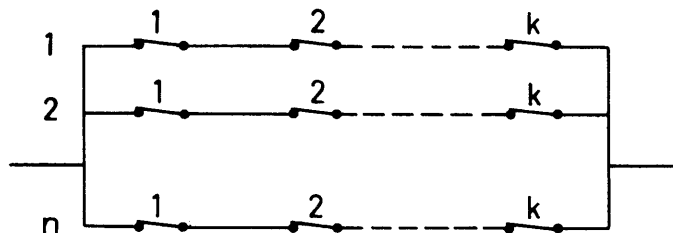
$$dP_u = [k (1 - e^{-nut})^{k-1}] \cdot [e^{-nut} n u dt]$$

Approximations give,

$$D \approx \frac{n^k}{k+1} (uT)^k$$

System B m channels are divided into n groups each containing k channels. One channel in each group must trip before a stop occurs.

The system can be symbolized in the following way, assuming that a trip equals a contact opening.



The probability of shut down is

$$P_f = (1 - e^{-ksT})^n$$

Approximations give

$$P_f = k^n (sT)^n$$

$$F \approx k^n s^n T^{n-1}$$

The dead time is

$$D = \frac{1}{T} \int_0^T (T-t) dP_u$$

where,

$$dP_u = [n \cdot k(1-e^{-ut})^{k-1} e^{-ut}] [u \cdot dt] [(1-(1-e^{-kut}))^{n-1}]$$

dP_u is the combined probability of $k-1$ failures in one group at t , the probability of the last channel in this group failing between t and $t+dt$, and the probability of less than k failures in any other group at t . (The system has not failed at t).

Approximations give,

$$D \approx \frac{n}{k+1} (uT)^k$$

Repair and Maintenance

When a channel repair takes place, we will assume that the channel remains tripped during repair. This will be the usual case.

System A

The probability of shut down in the operation period T caused by safe failures is named P_f .

The probability of no shut down during repair of one channel is the combined probability of no system failure in $k-1$ groups, and less than $n-1$ failures in the group under repair. Therefore

$$1 - P_f \{T_r\} = \left[1 - (1 - e^{-sT_r})^n\right]^{k-1} \cdot \left[1 - (1 - e^{-sT_r})^{n-1}\right]$$

If $(k-1)sT_r \ll 1$ this reduces to

$$\begin{aligned} 1 - P_f \{T_r\} &\approx \left[1 - (sT_r)^n\right]^{k-1} \cdot \left[1 - (sT_r)^{n-1}\right] \\ &\approx 1 - \left[(k-1)(sT_r)^n + (sT_r)^{n-1}\right] \\ &= 1 - (sT_r)^{n-1} \left[(k-1)sT_r + 1\right] \end{aligned}$$

and

$$P_f \{T_r\} \approx (sT_r)^{n-1}$$

The rate of "first failures" is $m \cdot s = n \cdot k \cdot s$, and then

$$F \approx k \cdot n \cdot s^n T_r^{n-1} \text{ and } P_f \approx 1 - e^{-kns^n T_r^{n-1} \cdot T}$$

System B

During repair this system is reduced to $n-1$ groups containing k channels.

$$P_f \{T_r\} = (1 - e^{-sT_r k})^{n-1}$$

and with usual approximations

$$F \approx nk^n \cdot s^n \cdot T_r^{n-1}$$

$$P_f \approx 1 - e^{-nk^n s^n T_r^{n-1} \cdot T}$$

When repair is carried out during operation, the repair periods will change the dead time. The discussion on repair and test of "2 out of 3" systems given on page 22 applies here, but in addition one has to treat a remaining system of a type different from the original. The remaining system in case A would be inoperable between t and $t+dt$ if either $n-2$ unsafe failures have occurred in the group under repair, or $n-1$ failures in at least one of the $k-1$ groups at t , and one failure occurs between t and $t+dt$ in the group in question. We will not go into details because it is easy to discuss the case along the given lines when the actual circuit is given.