1978

Optimal design of a quasi-redundant protective system for nuclear reactors

J. M. Kontoleon
University of Wollongong

Optimal design of a quasi-redundant protective system for nuclear reactors

Abstract

In many instances protective systems used in nuclear reactors are quasi-redundant systems; each of a number of safety channels feeds a number of independent protective units. A reactor shutdown is initiated if more than a specified number of units are in favour of shut down. The objective is to achieve a very high reliability at a reasonable cost. An analysis is presented to obtain the reliability, failsafe and fail-danger probabilities of a quasi-redundant system. Three algorithms are given for: (a) the design of a quasi-redundant system having the maximum reliability subject to a cost constraint, (b) the optimal design satisfying a given reliability level at the minimum cost and (c) the optimal design satisfying a combined safety requirement at the minimum cost. The algorithms are illustrated by way of examples.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as Kontoleon, JM, Optimal design of a quasi-redundant protective system for nuclear reactors, IEEE Transactions on Nuclear Science, 25(6), 1645-1648, 1978. Copyright Institute of Electrical and Electronics Engineers 1978. Original article available here

IEEE Transactions on Nuclear Science, Vol.NS-25, No.6, December 1978

OPTIMAL DESIGN OF A QUASI-REDUNDANT PROTECTIVE SYSTEM FOR NUCLEAR REACTORS

J.M. Kontoleon*

ABSTRACT

In many instances protective systems used in nuclear reactors are quasi-redundant systems; each of a number of safety channels feeds a number of independent protective units. A reactor shutdown is initiated if more than a specified number of units are in favour of shut down. The objective is to achieve a very high reliability at a reasonable cost. An analysis is presented to obtain the reliability, fail-safe and fail-danger probabilities of a quasi-redundant system. Three algorithms are given for:
(a) the design of a quasi-redundant system having the maximum reliability subject to a cost constraint,
(b) the optimal design satisfying a given reliability level at the minimum cost and
(c) the optimal design satisfying a combined safety requirement at the minimum cost. The algorithms are illustrated by way of examples.

1. Introduction

The major objectives of every design of a reactor protective system is to achieve a low probability of failure to initiate the protective action and a low probability of the occurrence of any spurious protecton action. In most instances, the methods used to achieve the first objective, cause a deviation from the second one and vice versa[1]. As a consequence, the design must be "optimal", in the sense that it should involve a compromise between the desired objectives, and satisfy the imposed techno-economical constraints.

To achieve the desired objectives, redundancy is commonly used. The usual type of redundancy is to connect n units so that to obtain a m-out-of-n:G system; the protection action is initiated when a coincidence of m or more unit trips occurs. If m=1, then the probability of a reactor spurious trip is maximum; if m=n, then the probability that the protective system will initiate the protection action is minimum. Thus, the proper selection of m, n will give a compromise between the desired design objectives of the m-out-of-n:G system. In the case of a dynamic redundant system[2], this compromise can be achieved by adjusting the frequency of scanning of the redundant units.

This paper presents an analysis of a quasi-redundant reactor protective system and develops three algorithms which result in the optimal design of such systems. The quasi-redundant system[3], is neither without redundancy nor with parallel redundancy and is shown in Figure 1. It can be seen that each of the safety channels (a channel involves the sensor and the safety line) is connected to a number of protective units (e.g., reactor temperature rate trip-amplifier units); if there are J channels and M units per channel, then the protective action is initiated when K-out-of-J·M units vote in favour of the protective action. Reference 3 analyses the reliability of such a system when each channel and unit are either good or bad. In this work, three states are considered for each channel and unit (good, fail-safe and fail-danger) and the objectives are:

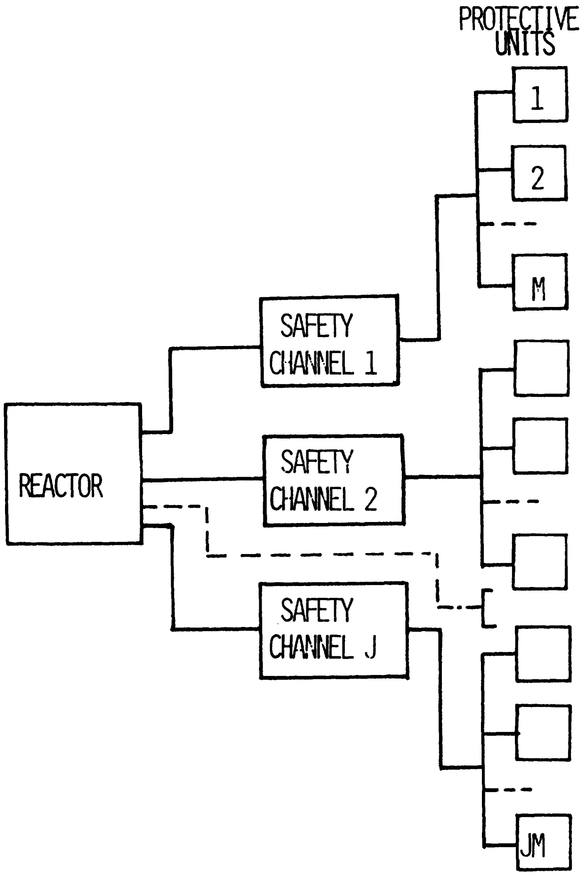

Figure 1. J-M-K Quasi-Redundant System

(a) to obtain the optimum J, M, K which result in the maximum reliability subject to a cost constraint;

(b) to obtain the optimum J, M, K in order to achieve a specified level of reliability at minimum cost; and

(c) to obtain the optimum J, M, K resulting to a reliability level above a specified one and to a fail-danger probability below a specified level, at the minimum cost.

Following the notation given in the next section, the reliability, fail-to-safe and fail-to-danger probabilities of a quasi-redundant system are obtained. These are further used in the formulation of three

Manuscript received on July 11, 1978.

* Department of Electrical Engineering, University of Wollongong, Wollongong, N.S.W. 2500, Australia.

0018-9499/78/1200-1645$00.75 © 1978 IEEE

computer algorithms to solve the above described problems.

2. Notation and Assumptions

J	number of safety channels
M	number of protective units per channel
K	minimum number of votes to initiate the protective action
N	total number of units; $N \equiv J \cdot M$
q_{us}	unit fail-to-safe probability of failure
q_{ud}	unit fail-to-danger probability of failure
q_{cs}	channel fail-to-safe probability of failure
q_{cd}	channel fail-to-danger probability of failure
$R(J,M,K)$	reliability of the protective system
$Q_s(J,M,K)$	fail-to-safe probability of the protective system
$Q_d(J,M,K)$	fail-to-danger probability of the protective system
c_c	capital cost involved in a channel
c_u	unit capital cost
$C(J,M)$	protective system cost; $C(J,M) \equiv J \cdot c_c + N \cdot c_u$
C	cost constraint
FS, FD	denotes fail-safe and fail-danger channel or unit failure, as stated in the text
$[x]^*$	integer part of x

The following assumptions are made throughout the paper:

1. Safety channel and unit states are s-independent

2. Safety channels and units can be in one of the following three states: good, fail-to-safe and fail-to-danger.

3. A failed channel or unit cannot become good or change mode of failure.

3. Fail-Safe and Fail-Danger Analysis

(a) Fail-safe probability

The quasi-redundant system will cause a spurious reactor trip in the following cases:

(i) All safey channels are good or FD, and at least K-out-of-N units are FS; or

(ii) j safety channels are FS, and at least m-out-of-jM units are good or FS, and at least (K-m)-out-of-(J-j)M units are FS; m=0,1,...,jM, j=1,2,...,J.

The above give,

$$Q_s(J,M,K) = (1-q_{cs})^J \sum_{m=K}^{N} \binom{N}{m} q_{us}^{m} (1-q_{us})^{N-m}$$

$$+ \sum_{j=1}^{J} \binom{J}{j} q_{cs}^{j} (1-q_{cs})^{J-j} \left[\sum_{m=0}^{jM} \left[\binom{jM}{m} (1-q_{ud})^{m} q_{ud}^{jM-m} \right.\right.$$

$$\left.\left. \left(\sum_{r=K-m}^{(J-j)M} \binom{(J-j)M}{r} q_{us}^{r} (1-q_{us})^{(J-j)M-r} \right) \right] \right] \qquad (1)$$

(a) Fail-danger probability

The system will be in the fail-to-danger state if:

(i) All safety channels are good or FS, and (N-K+1)-out-of-N units are FD: or

(ii) j safety channels are FD, and at least m-out-of-jM units are good or FD, and at least (N-K+1-m)-out-of-(J-j)M units are FD. Then,

$$Q_d(J,M,K) = (1-q_{cd})^J \sum_{m=N-K+1}^{N} \binom{N}{m} q_{ud}^{m} (1-q_{ud})^{N-m}$$

$$+ \sum_{j=1}^{J} \binom{J}{j} q_{cd}^{j} (1-q_{cd})^{J-j} \left[\sum_{m=0}^{jM} \left[\binom{jM}{m} (1-q_{us})^{m} q_{us}^{jM-m} \right.\right.$$

$$\left.\left. \left(\sum_{r=N-K+1-m}^{(J-j)M} \binom{(J-j)M}{r} q_{ud}^{r} (1-q_{ud})^{(J-j)M-r} \right) \right] \right] \qquad (2)$$

(c) Reliability

It is,

$$R = 1 - Q_s(J,M,K) - Q_d(J,M,K) \qquad (3)$$

4. Optimal Design Subject to a Cost Constraint

Consider the problem of maximising the reliability of a quasi-redundant system, subject to a given cost constraint, C. It is required to find the optimum values of J, M and K (J_{opt}, M_{opt} and K_{opt}), such that

$$R(J_{opt}, M_{opt}, K_{opt}) = \max R(J,M,K), \text{ for } C(J_{opt}, M_{opt}) \le C \qquad (4)$$

There are two extreme cases in the design of a quasi-redundant system, under the condition imposed by (4):

(i) J=1; then, M takes its maximum value, M_{max}

$$M_{max} = [(C-c_c)/c_u]^* \qquad (5)$$

(ii) M=1; then, J takes its maximum value, J_{max}

$$J_{max} = [C/(c_c + c_u)]^* \qquad (6)$$

Considering the above two extreme cases, it is reasonable to start with the one which gives the higher reliability and then modify the design until the maximum reliability is obtained. The algorithm is as follows:

Algorithm A

Steps:

```
0.  Read $q_{cs}$, $q_{cd}$, $q_{us}$, $q_{ud}$, $c_c$, $c_u$ and C.
1.  Obtain $J_{max}$ and $M_{max}$.  If $J_{max} = M_{max} = 1$,
      then set $K_{opt} = 1$, $R_{max} = R(1,1,1)$ and go to
      step 25;  otherwise continue.
2a. Set $R_{max} = 0$, $k = 0$.
 b. Set $k \leftarrow k+1$
3.  Evaluate $R(1, M_{max}, k)$;  if $R(1, M_{max}, k) \le R_{max}$,
      then go to step 5a, otherwise go to step 4.
4.  Set $R_{max} = R(1, M_{max}, k)$, $K_1 = k$;  go to step 2b.
5a. Set $R(1, M_{max}, K_1) = R_{max}$, $R_{max} = 0$, $k = 0$.
 b. Set $k \leftarrow k+1$
```

6. Evaluate $R(J_{max}, 1, k)$; if $R(J_{max}, 1, k) \le R_{max}$, then go to step 8a, otherwise go to step 7.

7. Set $R_{max} = R(J_{max}, 1, k)$, $K_2 = k$; go to step 5b.

8a. Set $R(J_{max}, 1, K_2) = R_{max}$, $k = 0$.

b. If $R(1, M_{max}, K_1) \ge R_{max}$, then go to step 9a; otherwise go to step 17a.

9a. Set $R_{max} = R(1, M_{max}, K_1)$, $J = 1$, $K_{opt} = K_1$, $M = M_{max}$ and $i = 0$.

b. Evaluate $x = C - C(J,M)$

c. Set $i \leftarrow i+1$; if $i > M-1$, then go to step 25 otherwise continue.

10a. Evaluate $y = (J \cdot c_u \cdot i + x)/(c_c + (M-i)c_u)$

b. If $y \ge 1$, then set $J \leftarrow J+[y]^*$ and go to step 11a; otherwise go to step 9c.

11a. Set $R_{max} = 0$.

b. Set $k \leftarrow k+1$

12. Evaluate $R(J, M-i, k)$; if $R(J, M-i, k) \le R_{max}$, then go to step 14 otherwise go to step 13.

13. Set $R'_{max} = R(J, M-i, k)$, $K_1 = k$ and go to step 11b.

14. If $R'_{max} > R_{max}$, then go to step 15; otherwise go to step 16a.

15. Set $M \leftarrow M-i$, $i=0$, $R_{max} = R'_{max}$, $K_{opt} = K_1$, and go to step 9b.

16a. Set $J_{opt} = J-[y]^*$, $M_{opt} = M$.

b. Evaluate $C(J_{opt}, M_{opt})$ and go to step 26.

17a. Set $J = J_{max}$, $M = 1$, $K_{opt} = K_2$ and $i=0$.

b. Evaluate $x = C - C(J,M)$.

c. Set $i \leftarrow i+1$; if $i > J-1$, then go to step 25 otherwise continue.

18a. Evaluate $y = (M \cdot c_u \cdot i + c_c \cdot i + x)/(J-i)c_u$

b. If $y \ge 1$, then set $M \leftarrow M+[y]^*$ and go to step 19a; otherwise go to step 17c.

19a. Set $R'_{max} = 0$

b. Set $k \leftarrow k+1$

20. Evaluate $R(J-i, M, k)$; if $R(J-i, M, k) \le R'_{max}$, then go to step 22, otherwise go to step 21.

21. Set $R'_{max} = R(J-i, M, k)$, $K_2 = k$ and go to step 19b.

22. If $R'_{max} > R_{max}$, then go to step 23; otherwise go to step 24.

23. Set $J \leftarrow J-i$, $i=0$, $R_{max} = R'_{max}$, $K_{opt} = K_2$ and go to step 17b.

24. Set $M_{opt} = M-[y]^*$, $J_{opt} = J$ and go to step 16b.

25. Set $J_{opt} = J$, $M_{opt} = M$ and obtain $C(J_{opt}, M_{opt})$.

26. Print J_{opt}, M_{opt}, K_{opt}, R_{max} and $C(J_{opt}, M_{opt})$; terminate the programme.

Example 1

Let $q_{cs} = 0.05$, $q_{cd} = 0.02$, $q_{us} = 0.1$, $q_{ud} = 0.07$; $c_c = 3$, $c_u = 1$ and $C = 15$ capital units. Following algorithm A it is:

Step:

0 - 1 : $J_{max} = 3$, $M_{max} = 12$

2 - 5a: $K_1 = 7$, $R(1, 12, 7) = 0.9299$

5b- 8a: $K_2 = 2$, $R(3, 1, 2) = 0.9244$

9a- 9b: $R_{max} = 0.9299$, $x = 0$

9c-10 : $i=1$, $y = 1/14 < 1$
$i=2$, $y = 2/13 < 1$
....
$i=7$, $y = 7/8 < 1$
$i=8$, $y = 8/7 > 1$, $[y]^* = 1$

11 -14 : $R'_{max} = R(2, 12-8, 6) = 0.9416$
$M = 4$
$R_{max} = 0.9416$

9b : $x=1$

9c-10 : $i=1$, $y = 3/6 < 1$
$i=2$, $y = 1$, $[y]^* = 1$

11 -14 : $R'_{max} = R(3, 4-2, 4) = 0.9683$
$M = 2$
$R_{max} = 0.9683$

9b : $x=0$

9c-10 : $i=1$, $y = 3/4 < 1$
$i=2 > M-1=1$

25 : $J_{opt} = 3$, $M_{opt} = 2$, $K_{opt} = 4$
$R_{max} = 0.9683$, $C(3,2) = 15$.

5. Specified Reliability at Minimum Cost

The problem posed in this section is to achieve a given reliability R_g, at minimum cost; i.e., it is required to obtain J_{opt}, M_{opt} and K_{opt} such that

$$C(J_{opt}, M_{opt}) = \min, \text{ for} \tag{7}$$

$$R(J_{opt}, M_{opt}, K_{opt}) \ge R_g \tag{8}$$

Consider the case of the simplest possible design, i.e., J=1, M=1; if (8) is satisfied, then this is the optimal design since (7) is satisfied. In general (8) will not be satisfied for the case of the simplest design, and therefore the design should be adjusted sytematically until both (7) and (8) are satisfied. Algorithm B is used to obtain the optimal design for the present problem (it includes algorithm A).

Algorithm B

Steps:

0. Read q_{cs}, q_{cd}, q_{us}, q_{ud}, R_g, c_c, c_u.

1. Set $J=1$, $M=1$ and $K=1$. If $R(J, M, K) \ge R_g$, then go to step 6; otherwise continue to step 2.

2a. If $c_c < c_u$, then set $w = c_c$; otherwise set $w = c_u$.

b. Set $C = c_u + c_c$

3. Set $C \leftarrow C + w$

4. Use algorithm A to obtain J_{opt}, M_{opt}, K_{opt} and R_{max}.

5. If $R_{max} \ge R_g$, then go to step 7; otherwise go to step 3.

6. Set $J_{opt} = J$, $M_{opt} = M$, $K_{opt} = K$.

7. Print J_{opt}, M_{opt}, K_{opt} and $C(J_{opt}, M_{opt})$; terminate the programme.

Example 2

Let $q_{cs} = 0.06$, $q_{cd} = 0.04$, $q_{us} = 0.12$, $q_{ud} = 0.08$, $c_c = 2$, $c_u = 1$ and $R_g = 0.89$; following algorithm B it is:

Step:

0 - 1 : $R(1, 1, 1) = 0.7200$

2a- 2b: $w=1$
$C=3$

3 : $C=4$

4 - 5 : $J_{opt} = 1$, $M_{opt} = 2$, $K_{opt} = 2$
$R_{max} = 0.7488$

3 : $C=5$

4 - 5 : $J_{opt} = 1$, $M_{opt} = 3$, $K_{opt} = 2$
$R_{max} = 0.8479$

3 : $C=6$

4 - 5 : $J_{opt} = 1$, $M_{opt} = 4$, $K_{opt} = 3$
$R_{max} = 0.8634$

3 : $C=7$

4 - 5 : $J_{opt} = 1$, $M_{opt} = 5$, $K_{opt} = 4$
$R_{max} = 0.8830$

3 : $C=8$

4 - 5 : $J_{opt} = 1$, $M_{opt} = 6$, $K_{opt} = 4$
$R_{max} = 0.8901$

7 : $J_{opt} = 1$, $M_{opt} = 6$, $K_{opt} = 4$
$C(1,6) = 8$.

Algorithm B can be easily improved by adding an acceleration parameter in step 3; this will cause C to increase quickly until $R_{max} > R_g$; when $R_{max} > R_g$, the value of C is reset to that of the previous step, and the acceleration parameter is reset to 1. The process terminates when the reliability level is achieved for a cost $C(J_{opt}, M_{opt})$ and it is not achieved for $C(J_{opt} - M_{opt}) - w$.

6. Combined Safety Requirements

Consider the design of a quasi-redundant protective system satisfying two requirements; for example, let one requirement be to achieve a reliability above a specified level R_g, and the other to achieve a fail-to-danger probability below a specified level Q_g. Both the above requirements should be achieved at the minimum possible cost. The previous algorithms can be used to solve the present problem. Algorithm B (includes algorithm A) can be easily modified as follows:

Algorithm C

Steps:

```
0.   : As step 0 of algorithm B; read $R_g$, $Q_g$.
1-4  : As steps 1-4 of algorithm B.
5a.  : If $R_{max} \geq R_g$, then go to step 5b; otherwise
       go to´ step 3.
b.   : Set $k=0$, $R' = 0$ and $Q' = 1$.
c.   : Set $k \leftarrow k+1$
d.   : Evaluate $A = R(J_{opt}, M_{opt}, k)$ and
       $B = Q_d(J_{opt}, M_{opt}, k)$; if $A \geq R_g$ and $B < Q_g$,
       then go to step 7; otherwise go to step 5e.
e.   : If $A < R(J_{opt}, M_{opt}, k-1)$ or $B < Q_d(J_{opt}, M_{opt}, k-1)$, then go to step 3; otherwise go
       to step 5c.
6-7  : As steps 6-7 of algorithm B.
```

Example 3

Let $R_g = 0.945$, $Q_g = 0.003$ and assume the parameters used in Example 2. Following the steps of algorithm C it is:

Step:		$R(J_{opt}, M_{opt}, k)$	$Q_d(J_{opt}, M_{opt}, k)$
0 -5b :	$J_{opt}=3$, $M_{opt}=3$, $K_{opt}=5$ $R_{max}=0.9579$		
5c-5e :	$k=1$	0.2629	$\simeq 0.$
	$k=2$	0.5868	0.0001
	$k=3$	0.7783	0.0006
	$k=4$	0.9018	0.0033
3 -5b :	$J_{opt}=3$, $M_{opt}=4$, $K_{opt}=7$ $R_{max}=0.9691$		
5c-5e :	$k=1$	0.1791	$\simeq 0.$
	$k=2$	0.4723	$\simeq 0.$
	$k=3$	0.6941	0.0001
	$k=4$	0.8099	0.0006
	$k=5$	0.8962	0.0024
	$k=6$	0.9526	0.0053
3 -5b :	$J_{opt}=4$, $M_{opt}=2$, $K_{opt}=5$ $R_{max}=0.9711$		
5c-5e :	$k=1$	0.2814	$\simeq 0.$
	$k=2$	0.6018	$\simeq 0.$
	$k=3$	0.8377	0.0004
	$k=4$	0.9460	0.0029
7 :	$J_{opt}=4$, $M_{opt}=2$, $K_{opt}=4$ $R(4,2,4) = 0.9460 > R_g$ $Q_d(4,2,4) = 0.0029 < Q_g$		

7. Conclusions

The use of the developed algorithms allows the design of quasi-redundant systems to satisfy the desired safety characteristics. The algorithms presented have been implemented in FORTRAN IV and a number of design problems have been solved. By letting either $q_{cs} = q_{cd} = 0$, the results are applicable to conventional K-out-of-N:G systems.

References

1. H.G. O'Brien and C.S. Walker, "Protection Instrumentation Systems in Light-Water-Cooled Power Reactor Plants", ORNL-NSIC-29, UC-80, October 1969.

2. J.M. Kontoleon, "Analysis of a Dynamic Redundant System", IEEE Trans. Reliability, R-27, No.2, June 1978.

3. L.T. Htun, "Reliability of a System Having Quasi-Redundancy", IEEE Trans. Reliability, R-15, No.1, May 1966.