Configuration Determination for k -out-of- n Partially Redundant Systems

Lixuan Lu¹

School of Energy Systems and Nuclear Science

and

Faculty of Engineering and Applied Science

Gregory Lewis

Faculty of Science, Mathematics

University of Ontario Institute of Technology

Oshawa, ON L1H 7K4 Canada

Abstract

The k -out-of- n configuration is a widely adopted structure for partially redundant safety systems. This configuration ensures a high level of reliability and safety with limited financial and space resources. It also facilitates on-line Test and Maintenance (T&M) without having to shut the system down. One question a decision maker needs to answer when adopting k -out-of- n systems is: what is the best configuration for the application, i.e., how many channels in total need to be utilized and among these channels, how many channels need to function simultaneously in order for the system to function. There are various factors to consider in order to make this decision. This paper looks at this problem from a reliability engineers point of view. A quantitative analysis is performed for both unavailability and probability of spurious operation due to independent failure. In particular, the relative gain

and/or loss of these quantities that occurs due to changing from one configuration to another are compared through rigorous mathematical analysis. The results provide important information that can be used when choosing system configurations to meet regulatory requirements and financial constraints. The two different configurations for shutdown systems in Nuclear Power Plants, the 2-out-of-3 system and the 2-out-of-4 system, are utilized as an example to illustrate the theoretical results.

Key words: Unavailability, Probability of Spurious Operation, k-out-of-n Redundant Systems, Shutdown Systems, Nuclear Power Plants

1 Introduction

Redundant channels are often employed in standby safety critical systems for safety critical applications [1]. The k -out-of- n logic is a widely adopted configuration for partially-redundant standby safety critical systems. For a k -out-of- n system, as long as at least k channels function, the system will function. Series and parallel systems are special cases of k -out-of- n systems, where $k = n$ for series systems and $k = 1$ for parallel systems.

A k -out-of- n system can fail in two different modes. One such mode of failure occurs when the system is unavailable when needed. In this case, more than $n - k$ channels fail, and thus less than k channels are available to monitor the system. This is a serious safety issue because if a safety system fails during emergency, the plant will not be secured and catastrophic consequences might occur. Therefore, when designing safety systems, one often strives to

¹ Corresponding author: Lixuan.Lu@uoit.ca, Tel: 1-905 721-3111 Ext. 3456, Fax: 1-905 721-3046.

achieve the lowest unavailability possible [2,3]. There are also general standards in place for these systems in order to ensure their availability [7,8]. The other failure mode is spurious operation. This occurs when at least k channels function spuriously when all the system parameters are within safe operating range. In this case the k -out-of- n system will shutdown the plant unnecessarily. The spurious operation could be very costly for a utility due to the interruption of plant operation and the expenses related to the restart of the plant. Even though there are no written rules for the target probability of spurious operation from the regulatory side, it should be considered from an economic point of view when designing a safety system [5,6].

Independent failure is one of the major causes for a k -out-of- n system to fail. Various techniques are often applied to minimize the occurrence of Common Cause Failures (CCF), which is a condition or an event that can cause multiple channels to fail simultaneously. For example, the philosophy of diversity and defense-in-depth is widely adopted in Nuclear Power Plant (NPP) design. There are two shutdown systems, Shutdown System Number One (SDS1) and Shutdown System Number Two (SDS2), in Canada Deuterium Uranium (CANDU) NPPs. These two shutdown systems use two completely different systems to avoid CCF. The SDS1 adopts electromechanical systems and shut-off rods to shut down the reactor, while the SDS2 adopts chemical systems and poison to shut down the reactor. Even within SDS1 and SDS2, different channels are separated physically and technically as well. Such strategies are effective in circumventing CCFs. Therefore, independent failures are the main focus of this paper.

In practice, two redundant configurations are commonly used in Nuclear Power Plants: the 2-out-of-3 system and the 2-out-of-4 system. A 2-out-of-3 system

has three channels and a 2-out-of-4 system has four channels. In both systems, as long as two channels function normally, the logic will ensure that the system works as intended. The SDS1 and SDS2 in CANDU NPPs adopt 2-out-of-3 systems [9]. In Pressurized Water Reactors (PWR) such as the European Pressurized Water Reactor (EPR) (<http://www.framatome-anp.com>) and the VVER type of reactors which is a Russian version of the PWR (<http://www.nucleartourist.com>), there is only one safety system which adopts the 2-out-of-4 configuration.

Preliminary results for the analysis of the unavailability and probability of spurious operation of 2-out-of-3 and 2-out-of-4 systems have been presented in our previous paper [10]. In the present paper, we extend the analysis and generalize the results to all k -out-of- n systems. The results of the analysis provide formulas, as well as insight, that can be used to determine the optimal configuration for a k -out-of- n system. In sections 2 and 3, we provide a mathematical definition of the unavailability and probability of spurious operation, respectively, due to independent failure, and we derive expressions that describe the changes in these quantities that occur when a single channel is added to the configuration. Formulas for the relative improvement or degradation of the unavailability and probability of spurious operation that are induced by various changes in the values of k and n are derived in section 4. In section 5, the range of acceptable k and n , given some regulatory specifications on unavailability and some maximum probability of spurious operation, are derived. The Emergency Shutdown Systems (ESDs) in different types of NPPs are used as example systems to illustrate the theoretical analyses. A conclusion follows.

2 Unavailability

The unavailability is defined as the probability that a system will fail during an emergency. In this section we analyze the unavailability of k -out-of- n systems under independent failures and investigate the effect on the unavailability due to the addition of a channel to the configuration.

Suppose that the probability that a given channel will fail is independent of the other channels, i.e. we consider independent failure, and suppose that this probability, represented by q , is the same for each channel. In this case, the number of unavailable channels (X) of a k -out-of- n system follows a binomial distribution ($X \sim B(n, q)$). When there are greater than or equal to $n - k + 1$ channels that fail during an emergency, the k -out-of- n system is unavailable. Therefore, if we denote Q_i as the probability that *exactly* i channels fail, then the unavailability of a k -out-of- n system ($Q_{\text{ind}}^{k/n}$) under independent failures can be calculated as the sum of Q_i over all $n - k + 1 \leq i \leq n$, That is,

$$Q_{\text{ind}}^{k/n} = \sum_{i=n-k+1}^n Q_i = \sum_{i=n-k+1}^n \binom{n}{i} q^i (1-q)^{n-i}, \quad (1)$$

where

$$\binom{n}{i} = \frac{n!}{(n-i)!i!} \quad (2)$$

is referred to as “ n choose i ”, and $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot (n)$ is the factorial of n .

In order to aid in design choices, we are interested in gaining insight into how the unavailability is affected by variation of k and n . We begin with a comparison between the k -out-of- n and k -out-of- $(n-1)$ systems. In particular,

we investigate

$$\Delta Q = Q_{\text{ind}}^{k/(n-1)} - Q_{\text{ind}}^{k/n}. \quad (3)$$

If n is replaced with $n-1$ in (1), we have that for the k -out-of- $(n-1)$ system,

$$Q_{\text{ind}}^{k/(n-1)} = \sum_{i=n-k}^{n-1} \binom{n-1}{i} q^i (1-q)^{n-i-1}. \quad (4)$$

With a change of the index $i \rightarrow i+1$, the lower limit of the sum becomes $n-k+1$, the upper limit of the sum becomes n , and Eqn. (4) becomes

$$Q_{\text{ind}}^{k/(n-1)} = \sum_{i=n-k+1}^n \binom{n-1}{i-1} q^{i-1} (1-q)^{n-i}. \quad (5)$$

By substituting Eqns. (1) and (5) into Eqn. (3), we obtain

$$\Delta Q = Q_{\text{ind}}^{k/(n-1)} - Q_{\text{ind}}^{k/n} = \sum_{i=n-k+1}^n \left[\frac{1}{q} \binom{n-1}{i-1} - \binom{n}{i} \right] q^i (1-q)^{n-i}. \quad (6)$$

Using the definition (2) for “ n choose i ”, we can write the coefficient of (6) as

$$\frac{1}{q} \binom{n-1}{i-1} - \binom{n}{i} = \frac{1}{q} \frac{(n-1)!}{(n-1-i+1)!(i-1)!} - \frac{n!}{(n-i)!i!}, \quad (7)$$

which after some algebraic manipulation can be simplified to

$$\frac{1}{q} \binom{n-1}{i-1} - \binom{n}{i} = \left[\frac{i}{nq} - 1 \right] \binom{n}{i}. \quad (8)$$

Thus, we have that

$$\Delta Q = Q_{\text{ind}}^{k/(n-1)} - Q_{\text{ind}}^{k/n} = \sum_{i=n-k+1}^n \left[\frac{i}{nq} - 1 \right] \binom{n}{i} q^i (1-q)^{n-i} \quad (9)$$

Because n , q , k and $n-k$ are all positive, it is clear that ΔQ must be positive

when

$$\frac{i}{nq} > 1 \quad (10)$$

for all i , or equivalently, when

$$q < \frac{i}{n}. \quad (11)$$

The right-hand side of this inequality will be a minimum when i is a minimum, i.e. when $i = n - k + 1$. Thus we can replace the last inequality with

$$q < 1 - \frac{k-1}{n}. \quad (12)$$

In summary, we have proved that whenever

$$q < 1 - \frac{k-1}{n}, \quad (13)$$

we have $\Delta Q > 0$, or equivalently

$$Q_{\text{ind}}^{k/(n-1)} > Q_{\text{ind}}^{k/n}. \quad (14)$$

Note the condition (13) is sufficient, but not necessary.

In practical systems, it is expected that q is very small while n , k or $n - k$ will not be large. Thus the condition (13) is expected to always be satisfied. The inequality (14) indicates that, when subjected to independent failures, the k -out-of- n system has a lower unavailability compared with the k -out-of- $(n - 1)$ system, i.e., adding a channel always reduces unavailability.

3 Probability of Spurious Operation

Suppose the probability of spurious operation of a given channel in a k -out-of- n system is the same for each channel, namely q_s . When considering only independent failures, the number of unavailable channels (Y) will follow a binomial distribution ($Y \sim B(n, q_s)$). When there are greater than or equal to k channels that function spuriously, the k -out-of- n system functions spuriously. Therefore, the probability of spurious operation of a k -out-of- n system ($S_{\text{ind}}^{k/n}$) under independent failures can be calculated as the sum of S_i over all $k \leq i \leq n$, where S_i is the probability that *exactly* i channels function spuriously. That is,

$$S_{\text{ind}}^{k/n} = \sum_{i=k}^n \binom{n}{i} q_s^i (1 - q_s)^{n-i}. \quad (15)$$

As in the case of unavailability, we investigate the changes in the probability of spurious operation that occur as a channel is removed. In particular, we define

$$\Delta S = S_{\text{ind}}^{k/n} - S_{\text{ind}}^{k/(n-1)}, \quad (16)$$

and use Eqn. (15) to obtain

$$\begin{aligned} \Delta S &= \sum_{i=k}^n \binom{n}{i} q_s^i (1 - q_s)^{n-i} - \sum_{i=k}^{n-1} \binom{n-1}{i} q_s^i (1 - q_s)^{n-i-1} \\ &= q_s^n + \sum_{i=k}^{n-1} \left[\binom{n}{i} - \frac{1}{1 - q_s} \binom{n-1}{i} \right] q_s^i (1 - q_s)^{n-i} \\ &= q_s^n + \sum_{i=k}^{n-1} \left[1 - \frac{1}{1 - q_s} \frac{n-i}{n} \right] \binom{n}{i} q_s^i (1 - q_s)^{n-i}. \end{aligned} \quad (17)$$

Using an argument similar to that presented in the previous section, we obtain that

$$S_{\text{ind}}^{k/(n-1)} < S_{\text{ind}}^{k/n} \quad (18)$$

whenever

$$q_s < \frac{k}{n}. \quad (19)$$

The condition (19) is expected to be met in all practical systems. Therefore, under independent failures, the k -out-of- n system has a higher probability of spurious operation compared with the k -out-of- $(n-1)$ system, i.e., for a given k , adding a channel increases the probability of spurious operation.

4 Quantitative Analyses

In this section, we extend the analysis of the previous section to determine, not only the sign, but the relative magnitude of the changes in the unavailability and probability of spurious operation induced by removing a channel. We also investigate the effects of varying k .

4.1 The Effect of Changing n

Define the relative increase $\eta_n = \eta_n(n, k, q)$ for the unavailability by changing from a k -out-of- n system to a k -out-of- $(n-1)$ system as:

$$\eta_n = \frac{Q_{\text{ind}}^{k/(n-1)} - Q_{\text{ind}}^{k/n}}{Q_{\text{ind}}^{k/(n-1)}}. \quad (20)$$

Using Eqns. (1) and (9), we obtain

$$\eta_n = \frac{\sum_{i=n-k+1}^n \left[\frac{i}{nq} - 1 \right] \binom{n}{i} q^i (1-q)^{n-i}}{\sum_{i=n-k+1}^n \binom{n-1}{i-1} q^{i-1} (1-q)^{n-i}}. \quad (21)$$

If the probability q that a given channel fails is sufficiently small, then we can assume that terms of $O(q^2)$ are negligible, i.e. an approximation that is linear in q will be sufficiently accurate. In this case, we need consider only the ratio of the first term of the sum in the numerator of (21) and the first term of the sum in the denominator.

Thus, we obtain that the relative increase

$$\eta_n \approx \frac{\left[\frac{n-k+1}{nq} - 1 \right] \binom{n}{n-k+1} q^{n-k+1} (1-q)^{k-1}}{\binom{n-1}{n-k} q^{n-k} (1-q)^{k-1}}, \quad (22)$$

which, with some algebraic manipulation, becomes

$$\eta_n \approx 1 - \frac{n}{n-k+1} q. \quad (23)$$

It can be seen from Fig. 1 that in the case when $n = 6$, $k = 4$, this approximation is sufficient for a wide range of q .

Eqn. (23) shows that the relative increase η_n varies approximately linearly with q with slope $-n/(n-k+1)$. That is, η_n decreases as q increases, which indicates that the benefit of adding an extra channel decreases as the unavailability of a given channel increases. The expression for the slope indicates that η_n is relatively insensitive to n . Also, as k decreases, the benefit of adding an extra channel decreases.

In the case of the probability of spurious operation, we define the relative increase $\xi_n = \xi_n(n, k, q_s)$ by changing from a k -out-of- $(n - 1)$ system to a k -out-of- n system as:

$$\xi_n = \frac{S_{\text{ind}}^{k/n} - S_{\text{ind}}^{k/(n-1)}}{S_{\text{ind}}^{k/n}}, \quad (24)$$

which can be expanded using Eqns. (15) and (17) to obtain

$$\xi_n = \frac{q_s^n + \sum_{i=k}^{n-1} \left[1 - \frac{1}{1-q_s} \frac{n-i}{n} \right] \binom{n}{i} q_s^i (1-q_s)^{n-i}}{\sum_{i=k}^n \binom{n}{i} q_s^i (1-q_s)^{n-i}}. \quad (25)$$

Again, we use the fact that q_s will be small and consider only the first term in each of the sums. The q_s^n term in the numerator is neglected because it is a higher power of q_s . This leads us directly to

$$\xi_n \approx 1 - \frac{n-k}{n} \frac{1}{1-q_s}. \quad (26)$$

We can further simplify this last expression by using the binomial expansion for $1/(1-q_s)$:

$$\frac{1}{1-q_s} = 1 + q_s + O(q_s^2), \quad (27)$$

and neglecting all terms of $O(q_s^2)$. Finally, we obtain that the relative increase

$$\xi_n \approx \frac{k}{n} - \frac{n-k}{n} q_s. \quad (28)$$

The leading term in this expression is k/n , while the leading term in η_n , given by Eqn. (23), is 1. This indicates that, for q comparable to q_s , ξ_n is small compared to η_n , i.e., for a given value of k , the addition of an extra channel

leads to a relatively large improvement in the unavailability compared to the degradation that occurs in the probability of spurious operation. Eqn. (28) also indicates that ξ_n is relatively insensitive to q_s when k is close to n .

In Fig. 2, the example of the relative increase ξ_n in probability of spurious operation obtained by taking away a channel for $n = 6$, $k = 4$ is plotted as a function of the probability q_s . Because the range of the graph is quite small, the figure indicates that the linear approximation is reasonably accurate.

4.2 The Effect of Changing k

The expressions (23) and (28) and the above discussion would be useful in helping an operator determine if it is worthwhile to add an extra channel. Also of interest would be the changes that would be induced by decreasing k by 1. Using a similar procedure as described in section 2, one can obtain

$$Q_{\text{ind}}^{k/n} - Q_{\text{ind}}^{(k-1)/n} = \binom{n}{n-k+1} q^{n-k+1} (1-q)^{k-1}. \quad (29)$$

It is clear that this expression is always positive, and thus

$$Q_{\text{ind}}^{k/n} > Q_{\text{ind}}^{(k-1)/n} \quad (30)$$

for all k , n , and q , i.e., unavailability always increases by increasing k . As above, we define the relative increase in unavailability that occurs by increasing the value of k by 1 as

$$\eta_k = \frac{Q_{\text{ind}}^{k/n} - Q_{\text{ind}}^{(k-1)/n}}{Q_{\text{ind}}^{k/n}}, \quad (31)$$

and use a similar analysis as described in section 4.1 to obtain

$$\begin{aligned}
\eta_k &= \frac{\binom{n}{n-k+1} q^{n-k+1} (1-q)^{k-1}}{\sum_{i=n-k+1}^n \binom{n}{i} q^i (1-q)^{n-i}} \\
&\approx 1 - \frac{k-1}{n-k+2} \frac{q}{1-q} \\
&\approx 1 - \frac{k-1}{n-k+2} q
\end{aligned} \tag{32}$$

In this case, in order to obtain all terms of $O(q)$ we need to consider two terms of the sum in the denominator. From this expression it can be seen that η_k is relatively insensitive to k , and insensitive to q when $n-k$ is large.

Likewise, we obtain that the relative increase in the probability for spurious operation induced by reducing the value of k by 1, defined by

$$\xi_k = \frac{S_{\text{ind}}^{(k-1)/n} - S_{\text{ind}}^{k/n}}{S_{\text{ind}}^{(k-1)/n}}, \tag{33}$$

can be approximated as

$$\xi_k \approx 1 - \frac{n-k+1}{k} q_s. \tag{34}$$

As for the case of the relative increase η_k , ξ_k is relatively insensitive to k . However, unlike η_k , ξ_k rapidly decreases with q_s when $n-k$ is large. The expression for η_k (32) and that for ξ_k (34) both contain a leading 1. Thus, unlike the case when an extra channel is added, it is expected that, depending on the relative values of q and q_s , an increase in k will cause an increase in unavailability that is of a similar magnitude as the decrease that it will cause in the probability of spurious operation. Although they will be of similar magnitude, Eqns. (32) and (34) indicate that if k is close to n , then ξ_k will be larger than η_k , and if k is small, then the opposite will be true.

In Figs. 3 and 4, examples for the relative increase of unavailability η_k and of spurious operation ξ_k , respectively, are plotted.

4.3 The Effect of Changing Both n and k

The results of the previous sections have indicated that the unavailability will decrease when a channel is added, and increase when the value of k is increased. On the other hand, the probability of spurious operation will increase when a channel is added, and decrease when the value of k is increased. It is useful to know the relative increases when both a channel is added and the value of k is increased. To zeroth order these can be derived directly from the relative increases η_n , ξ_n , η_k and ξ_k , given by the expressions (23), (28), (32) and (34), respectively. Alternatively, a similar analysis as was used in the previous sections can be used to obtain first order approximations.

If we define the relative increase η_{kn} in unavailability induced by both adding a channel and increasing the value of k as

$$\eta_{kn} = \frac{Q_{\text{ind}}^{k/n} - Q_{\text{ind}}^{(k-1)/(n-1)}}{Q_{\text{ind}}^{k/n}}, \quad (35)$$

then it can be shown that

$$\eta_{kn} \approx 1 - \frac{k-1}{n} - \frac{k-1}{n}q. \quad (36)$$

That is, if q is small, then unavailability will increase if both n and k are increased by 1. However, from the leading term in Eqn. 36, it can be seen that this increase may not be very large depending on the relative value of n and k . Qualitatively, this can be seen from the relative values of η_n and η_k shown

in Figures 1 and 3. For the range of q shown in the figures, it can be seen that the decrease in unavailability incurred from adding a channel is not as large as the increase in unavailability due to adding one to the value of k .

Similarly, if we define the relative increase ξ_{kn} in probability of spurious operation induced by both adding a channel and increasing the value of k as

$$\xi_{kn} = \frac{S_{\text{ind}}^{(k-1)/(n-1)} - S_{\text{ind}}^{k/n}}{S_{\text{ind}}^{(k-1)/(n-1)}}, \quad (37)$$

then it can be shown that

$$\xi_{kn} \approx 1 - \frac{n}{k} q_s. \quad (38)$$

Thus, if q_s is small, there will be a very large decrease in the probability of spurious operation when n and k are increased by 1. This is not surprising given that adding a channel had relatively little effect on the probability of spurious operation, while it shows a relatively large decrease when the value of k was increased by 1.

Thus, the relative increases η_n , ξ_n , η_k , ξ_k , η_{kn} , and ξ_{kn} given by the expressions (23), (28), (32), (34), (36), (37), respectively, can be used to determine whether an extra channel should be added, or whether the value of k should be changed, or both. For example, if it is found that a k -out-of- n system is not sufficiently reliable, while it is still necessary to avoid a large increase in the probability of spurious operation, then the above arguments suggest that an extra channel should be added. Alternatively, if it is found that the probability of spurious operation is unacceptable while the unavailability is well below requirements, then the value of k should be increased. Furthermore, the expressions for the relative increases can be used to give the magnitude of the changes. The values

of the relative increases supply important information that a system designer can use, along with other information (e.g. system costs) to determine the final system configuration.

It is natural to ask if there is a combination of changing values of k and n that would always lead to a decrease in both unavailability and the probability of spurious operation. From above, we know that changing the value of n has relatively small effect on the probability of spurious operation, while it has a large effect on unavailability. From this we might predict that if two channels are added and the value of k is increased by only 1, then both Q and S will decrease. To show this we can again perform the similar type of analysis as above. Define the relative increases in the unavailability induced by going from a $(k-1)$ -out-of- $(n-2)$ system to a k -out-of- n system as

$$\eta_{kn2} = \frac{Q_{\text{ind}}^{(k-1)/(n-2)} - Q_{\text{ind}}^{k/n}}{Q_{\text{ind}}^{(k-1)/(n-2)}}, \quad (39)$$

and the relative increase in the probability of spurious operation for the same change as

$$\xi_{kn2} = \frac{S_{\text{ind}}^{(k-1)/(n-2)} - S_{\text{ind}}^{k/n}}{S_{\text{ind}}^{(k-1)/(n-2)}}. \quad (40)$$

We can then show that bounds that assure that the relative increases η_{kn2} and ξ_{kn2} are positive are given by

$$q < \frac{1}{n} \quad \text{and} \quad q_s < \frac{1}{n}, \quad (41)$$

respectively. These bounds assure that all terms in the difference in the numerators of (39) and (40) are positive, where in this case the terms with large powers of q become negative first as q is increased.

We can also write down the linear approximations

$$\eta_{kn2} \approx 1 - \frac{n(n-1)}{(n-k+1)(k-1)}q, \quad (42)$$

and

$$\xi_{kn2} \approx 1 - \frac{n(n-1)}{k(n-k)}q_s. \quad (43)$$

In Figs. 5 and 6, examples for the relative increase of unavailability η_{kn2} and of spurious operation ξ_{kn2} , respectively, are plotted.

When plotted as a function of q or q_s , the approximations of the relative increases η_{kn2} and ξ_{kn2} both decrease with a relatively steep slope. However, even for large values of q , both the unavailability and the probability of spurious operation for the k -out-of- n system is a factor of two smaller than that of the $(k-1)$ -out-of- $(n-2)$ system. For smaller values of q , this factor rises significantly.

5 Configuration Determination

Often guidelines are set in place by regulatory bodies that specify a maximum value of the unavailability Q_{max} . For example, the Canadian Nuclear Safety Commission (CNSC) requires the target unavailability for the safety systems in CANDU NPPs [4] to be 10^{-3} . If the probability q for failure of a single channel is known or can be estimated, then for a given number of channels n , it is possible to determine a range of k that will assure that the unavailability of the k -out-of- n system is less than the required value Q_{max} . That is, for a

given number of channels n , we are interested in finding all k such that

$$Q_{\max} \geq Q_{\text{ind}}^{k/n} = \sum_{i=n-k+1}^n \binom{n}{i} q^i (1-q)^{n-i}. \quad (44)$$

If we assume that the probability q is small, the first term of the sum in (44) can be used to approximate the entire sum. This can be seen by observing that each subsequent term in the sum will decrease by a factor of q . Thus, we obtain

$$Q_{\max} \geq \binom{n}{n-k+1} q^{n-k+1} (1-q)^{k-1}. \quad (45)$$

We can determine the border of the range of acceptable values of k by replacing the inequality in Eqn. (45) with an equality. This leads us to the following equation

$$\binom{n}{n-k+1} q^{n-k+1} (1-q)^{k-1} - Q_{\max} = 0, \quad (46)$$

which, for fixed q , defines a curve on the (n, k) plane. For a given value of n , the value of the curve gives the maximum value of k for which the unavailability is within the required limit.

We can find points on the curve given by Eqn. (46) by specifying values of n and solving the resulting nonlinear equation in k . In practice, the curve will not pass through integer values of k , thus it is convenient to write this equation in terms gamma functions instead of factorials. The gamma function $\Gamma(x)$ is given by

$$\Gamma(x) = \int_0^{\infty} t^{x-1} e^{-t} dt, \quad (47)$$

and has the property that for integer values $x = n$

$$\Gamma(n+1) = n!. \quad (48)$$

Thus, we obtain that if an (n, k) pair lies below the curve defined by

$$\frac{\Gamma(n+1)}{\Gamma(n-k+2)\Gamma(k)} q^{n-k+1} (1-q)^{k-1} - Q_{\max} = 0, \quad (49)$$

then the corresponding unavailability $Q_{\text{ind}}^{k/n}$ is less than the required $Q_{\max}$. If the pair (n, k) lies above the curve then $Q_{\text{ind}}^{k/n}$ is above the required limit.

An example for $Q_{\max} = 10^{-3}$ and $q = 0.01$ is plotted in Fig. 7. It is also possible to include the full sum of (44) in the definition of the curve. Although this slightly increases the complexity of the coding, the solution method is fundamentally the same. Results from solving the full equation are also plotted in the figure. It can be seen that the approximation is very accurate for this value of q .

We now examine the case of spurious operation. An occurrence of a spurious operation of the system has potentially serious financial consequences. Thus, based on the cost per shutdown, a decision maker may wish to set a maximum $S_{\max}$ for the probability of spurious operation. As in the case for unavailability, if the probability q_s for spurious operation of a given channel is known or can be estimated, then for each n , a minimum value of k can be found for which all k above this value will ensure that $S_{\text{ind}}^{k/n} \leq S_{\max}$. From (15) we obtain

$$S_{\max} \geq S_{\text{ind}}^{k/n} = \sum_{i=k}^n \binom{n}{i} q_s^i (1-q_s)^{n-i}. \quad (50)$$

If q_s is small, we can approximate the sum with a single term. Thus, to ensure sufficiently low probability of spurious operation we require

$$S_{\max} \geq \binom{n}{k} q_s^k (1 - q_s)^{n-k}. \quad (51)$$

As in the case for unavailability, we can write the equation

$$\frac{\Gamma(n+1)}{\Gamma(n-k+1)\Gamma(k+1)} q_s^k (1 - q_s)^{n-k} - S_{\max} = 0 \quad (52)$$

that describes a curve in the (n, k) plane. When an (n, k) pair lies above this curve, we have $S_{\text{ind}}^{k/n} \leq S_{\max}$, and the opposite when the pair lies below the curve. If values for $S_{\max}$ and q_s are given, then for each n we can solve the nonlinear equation (52) in k to plot out this curve. An example with $S_{\max} = 10^{-3}$ and $q_s = 0.01$ is plotted in Fig. 8. Also plotted in the figure is the curve obtained by using the full expression for $S_{\text{ind}}^{k/n}$ instead of the one-term approximation. It can be seen that for these values of $S_{\max}$ and q_s , there is little gained by considering the full expression.

Finally, we can put both of these results together to obtain an ‘acceptable’ region in the (n, k) plane, i.e. the n -out-of- k systems for which the (n, k) pairs lie within this region satisfy both criteria

$$Q_{\text{ind}}^{k/n} \leq Q_{\max} \quad \text{and} \quad S_{\text{ind}}^{k/n} \leq S_{\max}. \quad (53)$$

This region is defined as the area that lies below the unavailability curve given by (49) and that lies above the spurious operation curve given by (52). An example is plotted in Fig. 9.

As an additional visual aid, contours of Q and S could be plotted on the same graph to determine the magnitude of changes in Q and S as system

configuration is changed. This could be done by replacing $Q_{\max}$ and $S_{\max}$ with various values of Q and S and solving the resulting equations (49) and (52), respectively. If, in addition, we would like not only to be within a given bound, but also to choose a configuration that shows improvement in both unavailability and probability of spurious operation, we may make a slight modification to the above analysis. That is, in addition to plotting curves with the value of k for a given n that will result in an unavailability of $Q_{\max}$ and a probability of spurious operation $S_{\max}$, we can also plot the value of k for a given n that will result in no change in the unavailability, and likewise for the probability of spurious operation. For example, if we have a 2-out-of-3 configuration, we can plot a curve k versus n for which all configurations corresponding to points on the curve have an unavailability of $Q^{2/3}$. See Fig. 10 for an example. In the figure, the region that lies between the $Q^{2/3}$ and $S^{2/3}$ curves will correspond to configurations with both lower unavailability and lower probability of spurious operation compared to the 2-out-of-3 system.

6 Application in NPP

There are two main configurations adopted in the Emergency Shutdown Systems (ESDs) in different designs of NPPs: 2-out-of-3 and 2-out-of-4 systems.

6.1 2-out-of-3 System

In CANDU NPPs, there are ten reactor operational parameters that are under surveillance. If any one of them goes beyond the safety range, the shutdown systems should function in sequence to shutdown the reactor. Both shutdown

systems (SDS1 and SDS2) in CANDU NPPs adopt the 2-out-of-3 configuration. The logic relationship of the Trip Logic 1 is shown in Fig. 11. When all reactor parameters are within the safe operating range, the contacts in the relays (RL-20D, RL-21D, RL-20E, RL-21E, RL-20F and RL-21F) are closed and the shutoff rods are held in place above the reactor. Whenever a reactor parameter moves outside the safe operating range, the contacts of at least two relays are open upon receiving the trip signal and the shutoff rods are dropped into the reactor to shut it down [9].

6.2 2-out-of-4 System

The reactor trip system in VVER adopts a 2-out-of-4 logic. Similar to the SDS1 in CANDU NPPs, whenever a reactor parameter goes out of the safe operating range, the reactor trip signal is issued to shutdown the reactor. The main difference is that there are four channels in this system, and the decision logic is 2-out-of-4 [11].

The detailed logic relationship of the 2-out-of-4 system is shown in Fig. 12. When all the reactor parameters are within the safe operating range, the contacts in the relays RL-Channel A, RL-Channel B, RL-Channel C and RL-Channel D are closed. Whenever a reactor parameter goes outside the safe operating range, the contacts on at least two relays are open and the corresponding clutches are de-energized so that the reactor is shutdown.

The above two systems illustrate different configurations for the same purpose in real applications. If we set $n = 4$ and $k = 2$, then from Eqns. (23) and (28),

and assume that $q = 0.02$, we have that

$$\eta_n \approx 0.973 \quad \text{and} \quad \xi_n \approx 0.490 \quad (54)$$

That is, the 2-out-of-4 system has a substantially lower unavailability than that of the 2-out-of-3 system. However, it has a probability of spurious operation approximately twice that of the other system. See [10] for further discussion.

A natural question to ask is which system is better. Of course there is no clear answer to this question, because it depends on the regulations, cost of system shutdowns, and other factors.

Another possible question to ask is whether there is another configuration that is in some sense better than both of these. The results of Section 4.3 indicated that if we add two channels while adding 1 to the value of k , then we can decrease both the unavailability and the probability of spurious operation due to independent failures. However, this is only an indication relative to a given configuration.

We might gain some insight by applying the technique described in Section 5. That is, we can plot the value of k for a given n that will result in no change in the unavailability, and likewise for the probability of spurious operation, for both the 2-out-of-3 system and the 2-out-of-4 system. In Fig. 13, we plot an example with $q = 0.01$ and $q_s = 0.01$. The region that lies below both the $Q^{2/3}$ and $Q^{2/4}$ curves and above both the $S^{2/3}$ and $S^{2/4}$ curves correspond to system configurations that have both a lower unavailability and lower probability of spurious operation than both the 2-out-of-3 system and the 2-out-of-4 system. In particular, the curves in Fig. 13 predict that a 3-out-of-6 system will have a lower unavailability and probability of spurious operation than both the

2-out-of-3 and the 2-out-of-4 system.

7 Conclusion

In this paper, we develop some simple tools and insight that could help a designer choose the optimal system configuration of a k -out-of- n redundant safety system.

We show that when the probability that a single channel fails is sufficiently small, which is generally satisfied in practical systems, a k -out-of- n system always has a lower unavailability and a higher probability of spurious operation than a k -out-of- $(n - 1)$ system. Furthermore, the magnitude of decrease in probability of spurious operation is lower than the increase in unavailability. However, a k -out-of- n system always has a higher unavailability and a lower probability of spurious operation than a $(k - 1)$ -out-of- n system.

Formulas are derived that give the relative increase in the unavailability and probability of spurious operation that occur upon various changes in the values of k and n . These formulas provide a quantitative assessment of the benefit or negative effect of making these changes, and would be of interest to a system designer in determining whether it is appropriate to add a channel or to increase the value of k . Of particular interest is that it is shown that it is possible to decrease both unavailability and probability of spurious operation due to independent failures by introducing two channels and increasing the value of k by 1.

We also present a procedure whereby an acceptable region in the (k, n) plane can be determined from predefined unavailability and probability of spurious

operation. With this graphical procedure, it is possible to visualize all the configurations that satisfy various constraints, e.g. maximum unavailability imposed by a regulatory body, and/or a maximum probability of spurious operation imposed by financial considerations.

These results alone can not determine an optimal configuration, because we have not taken into account various important financial and practical factors, such as cost of the system, cost of maintenance, or ease of implementation. However, the results will provide useful information that will aid a system designer in the decision making process.

Vitae

Lixuan Lu received her BEsc. and MEsc. in 1998 and 2001 respectively, from Beijing Institute of Technology in China, Ph.D in 2005 from the University of Western Ontario, Canada. Upon graduation she became an assistant professor at the School of Energy Systems and Nuclear Science and Faculty of Engineering and Applied Science, the University of Ontario Institute of Technology, Canada. Her research interests include Reliability and Safety Assessment, Wireless Networked Control Systems, Sensor Networks, Resource Allocation, Operations Research and Instrumentation and Control Systems in Nuclear Power Plants.

Gregory Lewis received his BSc and MSc in 1991 and 1994, respectively, from McGill University in Montreal, Canada, and his PhD of Mathematics in 2000 from the University of British Columbia in Vancouver, Canada. Following, he took up a postdoctoral fellowship at the Fields Institute for Research in Mathematical Science, and subsequently was hired as an assistant professor of Mathematics, in the Faculty of Science at the University of Ontario Institute of Technology in Canada. His research interests include Applied and Industrial Mathematics.

Fig. 1. Relative increase η_n in system unavailability obtained by changing from a 4-out-of-6 system to a 4-out-of-5 system.

Fig. 2. Relative increase ξ_n in probability of spurious operation obtained by changing from a 4-out-of-5 system to a 4-out-of-6 system.

Fig. 3. Relative increase η_k in system unavailability obtained by changing from a 3-out-of-6 system to a 4-out-of-6 system.

Fig. 4. Relative increase ξ_k in probability of spurious operation obtained by changing from a 4-out-of-6 system to a 3-out-of-6 system.

Fig. 5. Relative increase η_{kn2} in system unavailability obtained by changing from a 4-out-of-6 system to a 3-out-of-4 system.

Fig. 6. Relative increase ξ_{kn2} in probability of spurious operation obtained by changing from a 4-out-of-6 system to a 3-out-of-4 system.

Fig. 7. The unavailability of the k -out-of- n system will be below $Q_{\max}$ if the (n, k) pair lies below this curve. Both the single term approximation and the full equation are plotted. Example uses $Q_{\max} = 10^{-3}$, and $q = 0.01$.

Fig. 8. The probability of spurious operation of the k -out-of- n system will be below $S_{\max}$ if the (n, k) pair lies above this curve. Both the single term approximation and the full equation are plotted. Example uses $S_{\max} = 10^{-3}$, and $q_s = 0.01$.

Fig. 9. The ‘acceptable’ region is the area that lies below the unavailability curve ($Q_{\max}$ curve) and above the spurious operation curve ($S_{\max}$ curve). Example uses $Q_{\max} = 10^{-3}$, $q = 0.01$, $S_{\max} = 10^{-3}$, and $q_s = 0.01$.

Fig. 10. The region that lies between the $Q^{2/3}$ and $S^{2/3}$ curves will correspond to configurations with both lower unavailability and lower probability of spurious operation compared to the 2-out-of-3 system. As before, the ‘acceptable’ region is the area that lies below the $Q_{\max}$ curve and above the $S_{\max}$ curve. Example uses $Q_{\max} = 10^{-3}$, $q = 0.01$, $S_{\max} = 10^{-3}$, and $q_s = 0.01$.

Fig. 11. The 2-out-of-3 Logic Relationships of Trip Logic 1

Fig. 12. The 2-out-of-4 Logic Relationships

Fig. 13. The region that lies between both the $Q^{2/3}$ and $S^{2/3}$ curves and the $Q^{2/4}$ and $S^{2/4}$ curves will correspond to configurations with lower unavailability and probability of spurious operation compared to both the 2-out-of-3 and 2-out-of-4 systems. Example uses $q = 0.01$, and $q_s = 0.01$.

References

- [1] IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*, International Electrotechnical Commission (IEC), (1998).
- [2] G. Dragffy, “Hardware programmable VLSI emergency shutdown system,” *Reliab Engng Sys Safety*, **60**[4], 235 (1998).
- [3] H.G. Kang, T. Sung, “An analysis of safety-critical digital systems for risk-informed design,” *Reliab Engng Sys Safety*, **78**, 307 (2002).
- [4] Canadian Nuclear Safety Commission, *Requirements for Shutdown Systems for CANDU Nuclear Power Plants*, CNSC Regulatory Document R-8, (1991).
- [5] M. M. Cowing, M.E. Pate-Cornell, P.W. Glynn, “Dynamic modeling of the tradeoff between productivity and Ssafety in critical Eengineering systems,” *Reliab Engng Sys Safety*, **86**, 269 (2004).
- [6] G. Dragffy, “The design of a highly reliable safety critical emergency shutdown system,” *Reliab Engng Sys Safety*, **61**, 215 (1998).
- [7] IEC 61513, *Nuclear Power Plants - Instrumentation and Control for Systems Important to Safety - General Requirements for Systems*, International Electrotechnical Commission (IEC), (2001).
- [8] IEC 62138, *Nuclear Power Plants - Instrumentation and Control Important to Safety - Software Aspects for Computer-based Systems Performing Category B or C Functions*, International Electrotechnical Commission (IEC), (2004).
- [9] Bruce Power, *Introduction to CANDU Processes*, IMS 41001. Ontario: Nuclear Training, (1999).

- [10] L. Lu and G. Lewis, “Reliability Evaluation of Standby Safety Systems Due to Independent and Common Cause Failures” *IEEE Conference on Automation Science and Engineering*, (2006).
- [11] J. Zhang, J. Zhu, *Digitalized Instrumentation and Control Systems in Tian Wan Nuclear Power Plants*, Nuclear Power Ltd, Jiangsu, (2003).

List of Figures

- 1 Relative increase η_n in system unavailability obtained by
changing from a 4-out-of-6 system to a 4-out-of-5 system. 27
- 2 Relative increase ξ_n in probability of spurious operation
obtained by changing from a 4-out-of-5 system to a 4-out-of-6
system. 28
- 3 Relative increase η_k in system unavailability obtained by
changing from a 3-out-of-6 system to a 4-out-of-6 system. 29
- 4 Relative increase ξ_k in probability of spurious operation
obtained by changing from a 4-out-of-6 system to a 3-out-of-6
system. 30
- 5 Relative increase η_{kn2} in system unavailability obtained by
changing from a 4-out-of-6 system to a 3-out-of-4 system. 31
- 6 Relative increase ξ_{kn2} in probability of spurious operation
obtained by changing from a 4-out-of-6 system to a 3-out-of-4
system. 32
- 7 The unavailability of the k -out-of- n system will be below $Q_{\max}$
if the (n, k) pair lies below this curve. Both the single term
approximation and the full equation are plotted. Example uses
 $Q_{\max} = 10^{-3}$, and $q = 0.01$. 33

- 8 The probability of spurious operation of the k -out-of- n system will be below $S_{\max}$ if the (n, k) pair lies above this curve. Both the single term approximation and the full equation are plotted. Example uses $S_{\max} = 10^{-3}$, and $q_s = 0.01$. 34
- 9 The ‘acceptable’ region is the area that lies below the unavailability curve ($Q_{\max}$ curve) and above the spurious operation curve ($S_{\max}$ curve). Example uses $Q_{\max} = 10^{-3}$, $q = 0.01$, $S_{\max} = 10^{-3}$, and $q_s = 0.01$. 35
- 10 The region that lies between the $Q^{2/3}$ and $S^{2/3}$ curves will correspond to configurations with both lower unavailability and lower probability of spurious operation compared to the 2-out-of-3 system. As before, the ‘acceptable’ region is the area that lies below the $Q_{\max}$ curve and above the $S_{\max}$ curve. Example uses $Q_{\max} = 10^{-3}$, $q = 0.01$, $S_{\max} = 10^{-3}$, and $q_s = 0.01$. 36
- 11 The 2-out-of-3 Logic Relationships of Trip Logic 1 37
- 12 The 2-out-of-4 Logic Relationships 38
- 13 The region that lies between both the $Q^{2/3}$ and $S^{2/3}$ curves and the $Q^{2/4}$ and $S^{2/4}$ curves will correspond to configurations with lower unavailability and probability of spurious operation compared to both the 2-out-of-3 and 2-out-of-4 systems. Example uses $q = 0.01$, and $q_s = 0.01$. 39