FACTOR OF SAFETY VERSUS REDUNDANCY – THE CLIFF-HANGER QUESTION

Dr Weng Poh
Umow Lai Pty Ltd
10 Yarra Street, South Yarra,
Victoria 3141, Australia

ABSTRACT

Imagine you were hanging off a cliff. Is it safer to be attached to two ropes or a single rope that is twice as strong? This question was raised in response to a proposition advocated during a previous Fire Engineering Conference that redundancy can be quantified using factor of safety. Much debate followed but the question remains unanswered.

In order to answer the above question, this paper presents a detailed examination of the two key design aspects — factor of safety and redundancy. They were explored for various cliff-hanging arrangements and their associated probabilities of failure were analysed quantitatively. The exercise shows that not only factor of safety and redundancy are separate aspects that can be independently incorporated into a system; they also have different impact on the probability of failure of the system. It demonstrates that factor of safety and redundancy are not the same, and it will be erroneous for redundancy to be quantified using factor of safety. Different redundancy arrangements, including load-sharing and standby, were also explored. It is shown that, with the appropriate arrangements, it is safer to be attached to two ropes than a single rope that is twice as strong.

As a corollary to the outcome of cliff-hanging scenarios, factor of safety and redundancy are further discussed with respect to fire engineering designs. Direct analogies were drawn to two building designs, one with two exits and the other with a single exit twice as large. It is concluded that the former provides a safer solution than the latter due to increased redundancy in the design. This is despite the fact that both designs may have the same factor of safety based on *ASET-RSET* assessment.

This paper demonstrates that a high factor of safety does not guarantee a low probability of failure, or a high level of safety. To raise the bar for fire engineering designs and to ensure a high level of safety is achieved, one must look beyond using factor of safety as the sole design criteria. Failure of components and system must be carefully examined to ensure sufficient redundancy and robustness of the designs.

INTRODUCTION

In a previous Fire Safety Engineering conference, it was advocated during a presentation that redundancy in a fire engineering design equals its factor of safety; and that redundancy can be quantified using factor of safety [1]. I did not fully agree with the proposition and put forth the following analogy during the question time:

> *Imagine two scenarios where you were hanging off a cliff. In the first scenario, you were attached to two ropes that each could carry your weight. If one failed, you had another one to hang on. In this case, you could argue that you had redundancy in your system. In the second scenario, you were attached to a single rope that was twice as strong. In this case, you could argue that you have a factor of safety of two. Comparing these two scenarios, one had greater redundancy and the other greater factor of safety. Are they equivalent? Is it safer to be attached to two ropes or a single rope that is twice as strong?*

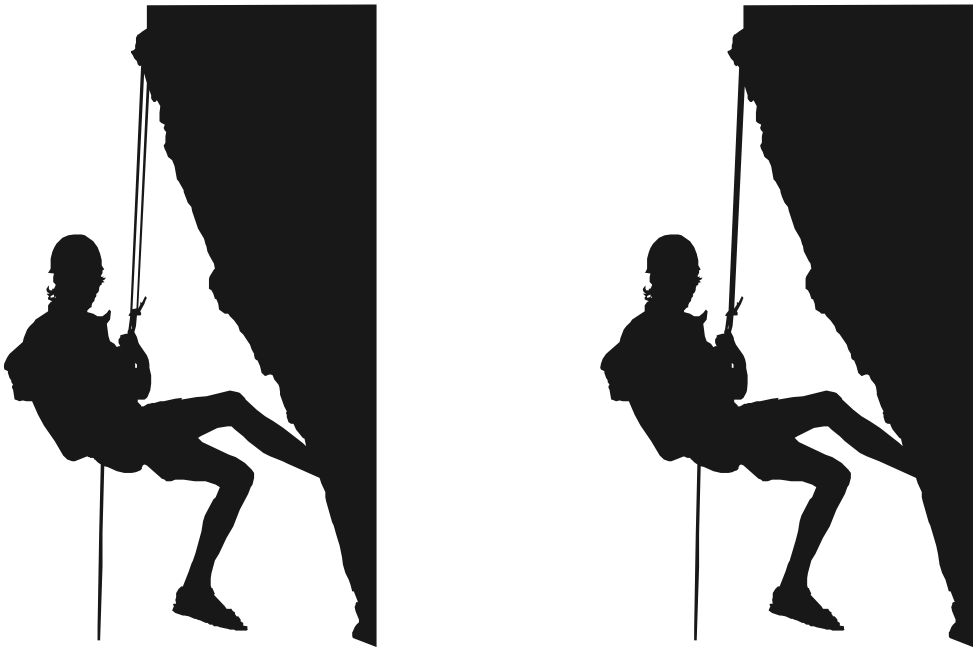


Fig 1. Two Ropes vs a Single Rope Twice as Strong

There were much comments and debates from the speakers and the floor during the question time, and later into the rest of the day. However, there were no definitive answers to these very fundamental and commonly asked questions in fire engineering designs. *What is the factor of safety of your design? What is the redundancy of your design?*

Before we answer these questions, we must first understand what are factor of safety and redundancy. These are discussed below with respected to their associated probabilities of failure.

FACTOR OF SAFETY

In engineering designs, factor of safety (λ) is used for describing the ratio of the capacity (C) to the applied load (L) of a system.

$$\lambda = C/L$$

Let us ignore redundancy for a moment and return to the cliff-hanging scenario where you were securely attached to only one rope. If your total weight, including the items you carried, were 1.0 kN, and the rope had a load carrying capacity of 1.5 kN; this gives λ =1.5/1.0 = 1.5. If you used a stronger rope with twice the capacity (i.e. C= 3.0 kN), λ is simply doubled to 3.0.

If we adopt a deterministic approach and establish L and C as two distinct point values, no failure occurs so long as λ is greater than unity, and safety is assured (see figure below). This is the case regardless of whether λ is 1.5 or 3.0.

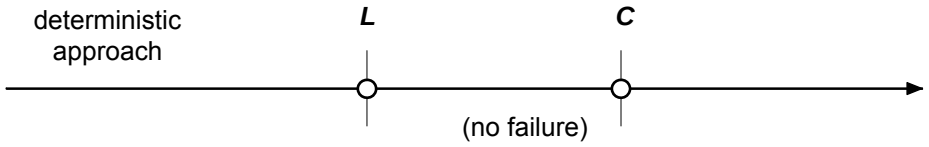


Fig. 2 Deterministic Approach and Failure Criterion

It is noted that *safety margin* is sometimes used. This is simply the difference, C - L.

Probability of Failure

From a probabilistic viewpoint, failure may still occur even when λ is greater than unity. This is due to the fact that L and C cannot be determined with absolute certainty owing to our lack of knowledge of all the factors that may influence their values. In the cliff-hanging scenario, your total weight might vary depending on the gears you carried, and the rope might vary depending on its variability in its material properties. In order to account for this uncertainty or variability, L and C are more appropriately represented by probability density functions (*pdf's*), rather than single points as discussed earlier (see following figure).

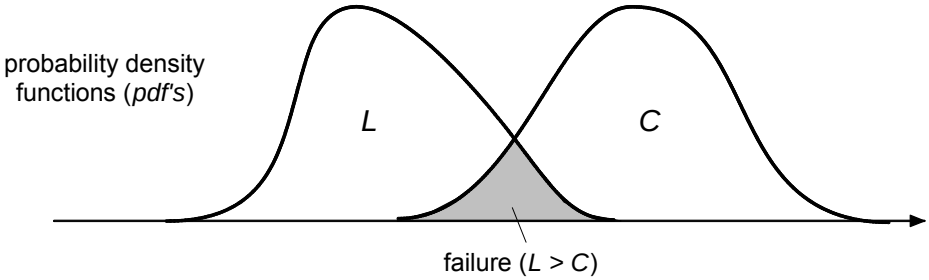


Fig. 3 Probability Density Functions and Probability of Failure

Within the spectrum of the variability or uncertainty, there is a chance that L is higher than C, and if such combination occurs, the system fails as indicated by the shaded area in the figure above.

If L and C were normally distributed with a mean μ_L and μ_C; and a standard deviation σ_L , σ_C, respectively, then the probability of failure can be calculated as follows [2]:

$$P_F = \Phi(-\beta) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\beta} e^{-\frac{u^2}{2}} du \; ; \text{ where } \beta = \frac{\mu_C - \mu_L}{\sqrt{\sigma_L^2 + \sigma_C^2}} \text{ (reliability index)}$$

a) ***Case 1* - single rope**

If we go back to the previous example and assume that $\sigma = 0.2\mu$, i.e:

- *Load:* μ_L=1.0kN, σ_L =0.2 kN
- *Capacity:* μ_C=1.5kN, σ_C =0.3 kN

The factor of safety remains at λ = 1.5. The probability of failure of the rope can be calculated as $P(A) = \Phi(-1.387) = 8.28\text{x}10^{-2}$ (see following figure).

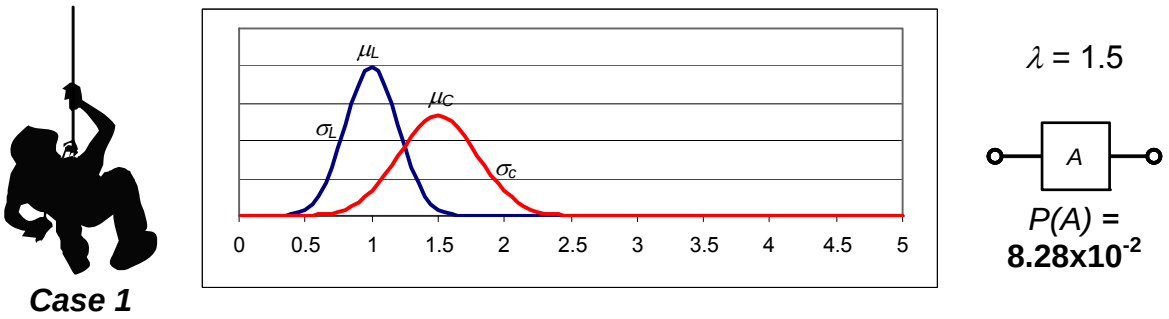


Fig. 4 *Case 1* – Single Rope

b) ***Case 2* - single rope twice as strong**

If you were to use another rope of the same material but twice as thick, then μ_C and σ_C are doubled. Hence

- *Load:* μ_L=1.0 kN, σ_L = 0.2 kN
- *Capacity:* μ_C=3.0 kN, σ_C = 0.6 kN

The factor of safety is also doubled. This gives $P(A) = \Phi(-3.162) = 7.83\text{x}10^{-4}$.

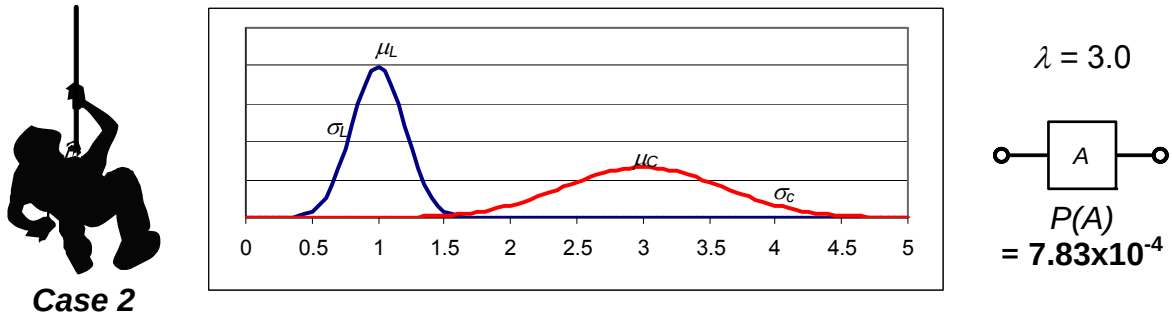


Fig. 5 *Case 2* – Single Rope Twice as Thick

The decrease in probability of failure is to be expected, since a thicker rope was used. In the case, λ is doubled and $P(A)$ is lowered by a factor of 106.

Cases 1 and *2* show that the probability of failure *P(A)* decreases increasing λ. However, it is important to note that *P(A)* is highly dependent on σ. The following figure shows the *P(A)* of the above two cases against σ_L. For the sake of simplicity, it is assumed that μ_L = 1.0kN.

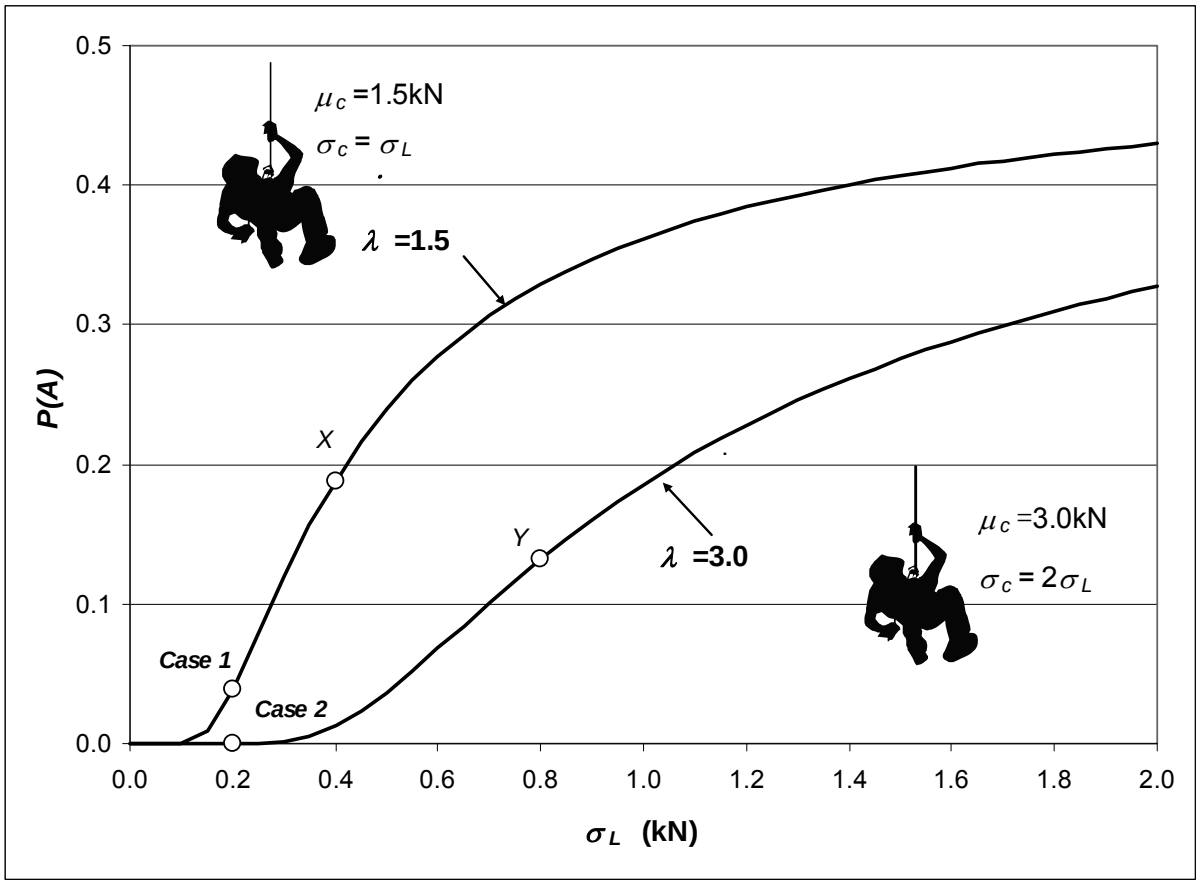


Fig. 6 Probability of Failure vs Standard Deviation

Two key points can be made regarding λ from the above analysis:

- λ does not provide a measure of the probability of failure. Two systems can have the same λ and different probability of failure (e.g Point *X* in Fig. 6 represents a case having the same λ but higher probability of failure than *Case 1*).
- A larger λ generally results in a lower probability of failure. However, a larger λ does not guarantee a lower probability of failure (e.g. Point *Y* in Fig. 6 represents another case having a higher λ and higher probability of failure than *Case 1)*.

They are the uncertainties (i.e. σ_L and σ_C) that affect the probability of failure and make it impossible to guarantee the system is absolutely safe. It is interesting to note that the current standard of risk management [3] has redefined risk as the effect of uncertainty on objectives.

REDUNDANCY

Let us now turn our attention to redundancy.

In design, redundancy can be defined as the duplication of critical component(s) of a system with the intention of increasing reliability of the system. In system engineering, redundancy is often expressed as *N+K* where *N* is the minimum number of units required for system success and *K* is the number of backup units [4].

In the cliff-hanging scenario, if you attached a second rope, you could hang off it if the first one broke. This is referred to as an *N* + 1 system, and incidentally *N* also equals 1 in this case.

How does the introduction of redundancy affect the probability of failure? To answer this question, we must examine how the redundancy is arranged – *standby* or *load-sharing*. These are discussed below.

Probability of Failure

a) *Case 3* - Standby redundancy

Imagine you were hanging off a rope, which we now call it *Rope A*, as before; but now, you had a second identical rope (*Rope B*) attached in "standby" to support your weight in case *Rope A* broke. Total system failure occurs if *Rope B* also broke.

If we assume a seamless load transfer to *Rope B* when *Rope A* breaks, and they are independent, then $P(B|A)=P(B)=P(A)$. The probability of failure of both ropes breaking is simply $P(A \cap B) = P(A)P(B \mid A) = P(A)P(B)$.

Hence in the case where μ_L=1.0kN and μ_C=1.5kN, σ_C=0.3kN, $P(A)$=8.28x10^{-2}. This gives $P(A \cap B)$= 6.85x10^{-3} which is lower than the individual probabilities *P(A) and P(B)*.

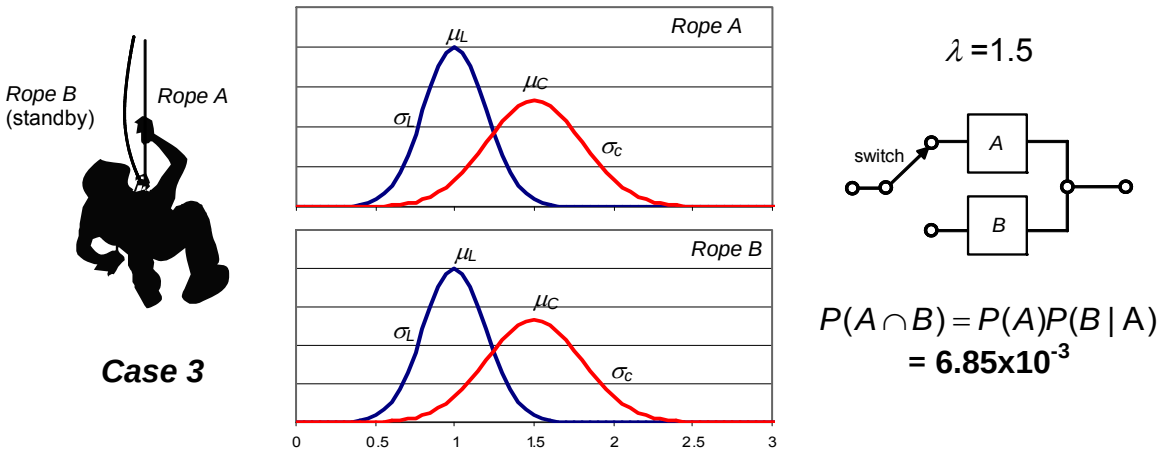


Fig. 7 *Case 3* – Two Ropes in Standby Redundancy Arrangement

Given that only one rope is carrying the load at any time, the introduction of *Rope B* does not alter λ for the system, and hence λ remains at 1.5.

b) ***Case 4*** **- Load-sharing redundancy**

Now, instead of letting *Rope B* hang loosely as "standby", you attached the two ropes such that they were both taut and shared the load equally. The capacity of each rope remains unchanged, but the load carried is halved.

Again, for a total failure, both ropes must fail, and the probability can be calculated as $P(A \cap B) = P(A)P(B)$.

However since each rope now carries only half the load, *P(A)* and *P(B)* decrease to 7.83×10^{-4}. This gives $P(A \cap B) = 6.13 \times 10^{-7}$.

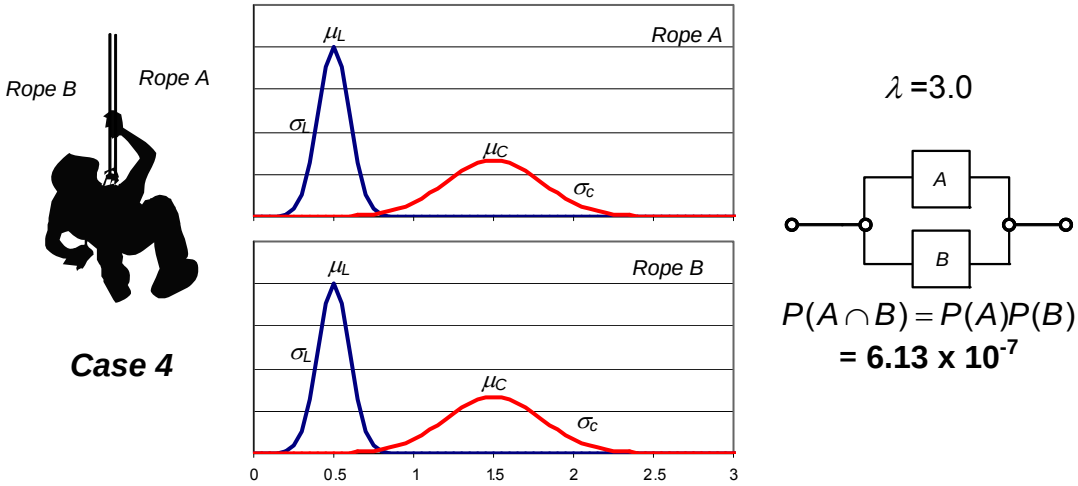


Fig. 8 *Case 4* – Two Ropes in Load-sharing Redundancy Arrangement

Given the capacity of each rope remains unchanged and the load is halved, λ for the system is doubled to 3.0.

FACTOR OF SAFETY VS REDUNDANCY

The results of analysis are summarised in the table below, taking *Case 1* as the base case for comparison.

Case	λ	Redundancy	P(failure)	Comment
1	1.5	*N*+0	8.28×10^{-2}	Base case
2	3.0	*N*+0	7.83×10^{-4}	Increase λ only
3	1.5	*N*+1	6.85×10^{-3}	Increase redundancy only
4	3.0	*N*+1	6.13×10^{-7}	Increase λ and redundancy

The table above shows that factor of safety and redundancy are separate aspects of a design and can be independently incorporated into a design. Increase in either will lower the probability of failure, and increase in both will lower it further.

It is noted that greater redundancy can be achieved by increasing the number of ropes. Combination of load-sharing and standby can also be used.

COMPONENT VS SYSTEM FAILURE

The foregoing discussion focuses on only one component (or sub-system) of a total system – i.e. the ropes. In a system with multiple components, other components may also have a significant impact the overall success of the system. For example, in the cliff-hanging scenarios, the attachments of the ropes to the cliff face are also critical components. If the attachments give way, the system also fails. This failure, which may be caused by breakage of the attachment or a local dislodge of the attachment point, has been ignored in all the cases examined earlier.

If we include the probability of failure of the attachments, which we now denote as *P(C)*, we can further calculate the system failure of the previous four cases.

a) ***Cases 1 & 2*** **– Single rope**

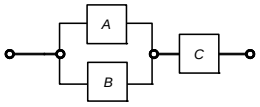
For *Cases 1* and *2*, system fail occurs when either the rope or the attachment fails. Hence the probability of failure is:

$$P(A \cup C) = P(A) + P(C) - P(A \cap C)$$

b) ***Cases 3 & 4*** **– Two ropes**

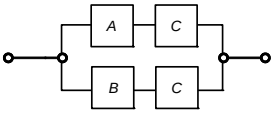
For *Cases 3* and *4*, if the two ropes were attached to a single point, then the probability of failure is similar to that expressed above, i.e.

$$P((A \cap B) \cup C) = P(A \cap B) + P(C) - P((A \cap B) \cap C)$$



However, if the ropes were attached to two separate points, each having a probability of failure of *P(C),* then the probability of failure becomes:

$$P((A \cup C) \cap (B \cup C)) = (P(A) + P(C) - P(A \cap C))(P(B) + P(C) - P(B \cap C))$$



If we assume the each rope was separately attached, the cases discussed above are summarised in the figure below.

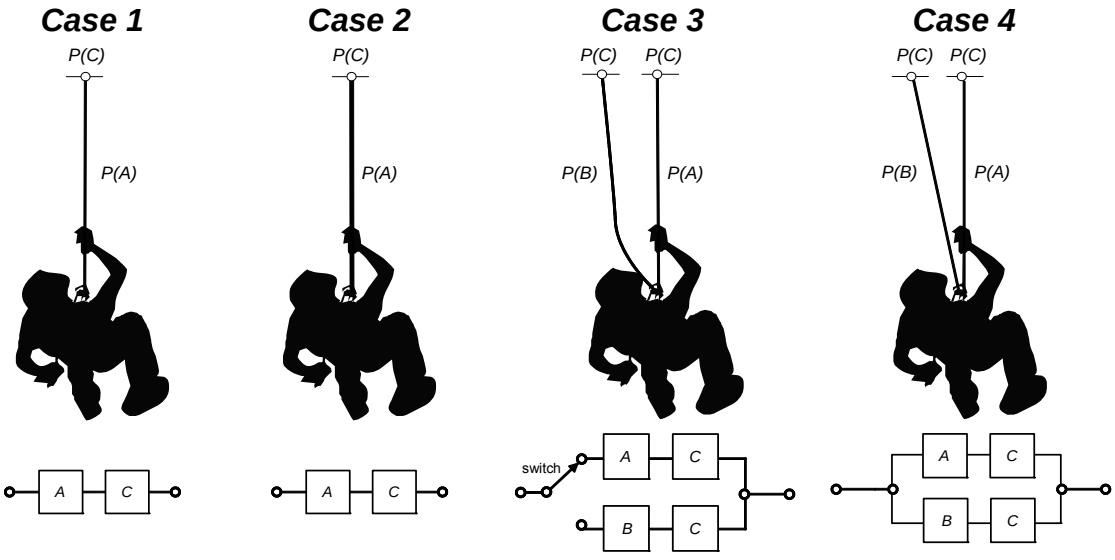


Fig. 9 Component vs System Failure

The probabilities of failure of the system for the 4 cases for the entire spectrum of *P(C)* from 0 to 1 are shown in the following figure.

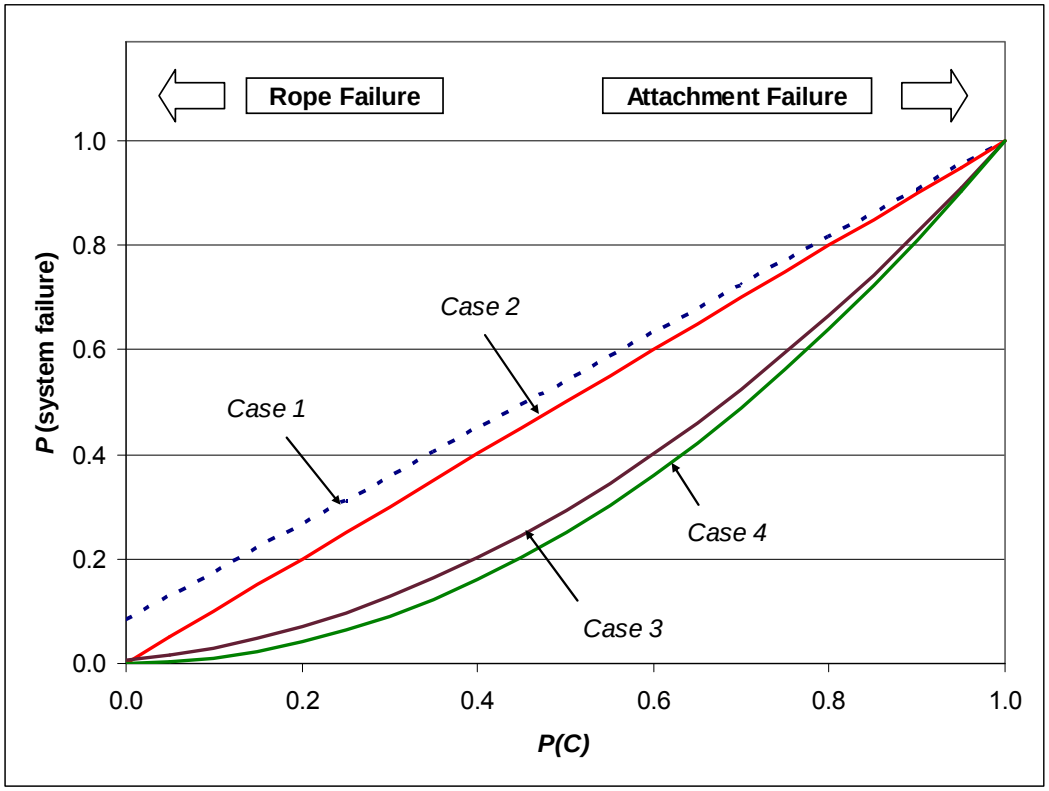


Fig. 10 System Failure vs Component Failure

The results show that, the probability failure of the system is governed by that of the ropes and that of the attachments, for high and low *P(C)* values, respectively.

The following generally comments can also be made:

- *Case 4* (two ropes in load-sharing arrangement) is the safest. It gives the lowest probability failure for the entire spectrum of *P(C).*
- *Case 3* (two ropes in standby arrangement) is the next safest. However, the probability of failure is higher than that of *Case 2* when the *P(C)* value is very low.
- *Case 2* is not as safe as *Case 4* or *Case 3.* This is despite *Case 2* has the same factor of safety as *Case 4* and a higher factor of safety than *Case 3.*

Answers to the Cliff-hanger Questions

Let us return to the questions posed earlier in the Introduction.

- *Are factor of safety and redundancy equivalent?*
  The answer is “no”. Based on the cases examined, factor of safety and redundancy are clearly two different and independent design aspects, and they have different impacts on the safety level of a system.

- *It is safer to be attached to two ropes or a single rope that is twice as strong?*
  The answer is “two ropes”. This is particularly so if the two ropes actively sharing the load and are attached to two separate points, as in *Case 4*.

FACTOR OF SAFETY AND REDUNDANCY IN FIRE ENGINEERING DESIGNS

Fire engineering evaluations are often based on deterministic approaches to establish point values to gauge the performance of a design. Arguably, the most common evaluation is the calculations of Available Safe Egress Time (*ASET)* and Required Safe Egress Time (*RSET)*. Factor of safety is calculated as the ratio of *ASET* to *RSET* [5].

$$\lambda = ASET/RSET$$

The design is considered to be safe when λ is greater then unity.

However, due to the various uncertainties in establishing the *ASET* and *RSET* values, they are more appropriately represented as *pdf*'s, as shown in the figure below.

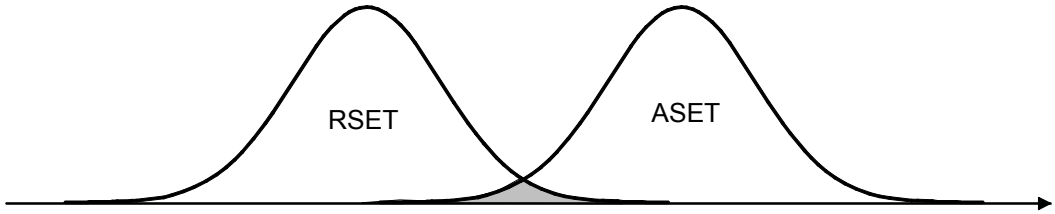


Fig. 11 ASET and RSET as *pfd*'s

This means that failure could still occur, as indicated in the shaded area in the figure able. Also, as shown earlier in this paper, increasing the factor of safety does not guarantee a lower probability of failure. Redundancy of the design must also be examined to ensure a high level of fire safety is achieved.

In order to explore this further, let us now look at two building designs where all the building characteristics, travel distances, occupant numbers are the same except one contains two exits and the other one exit that is twice as large (see figure below).

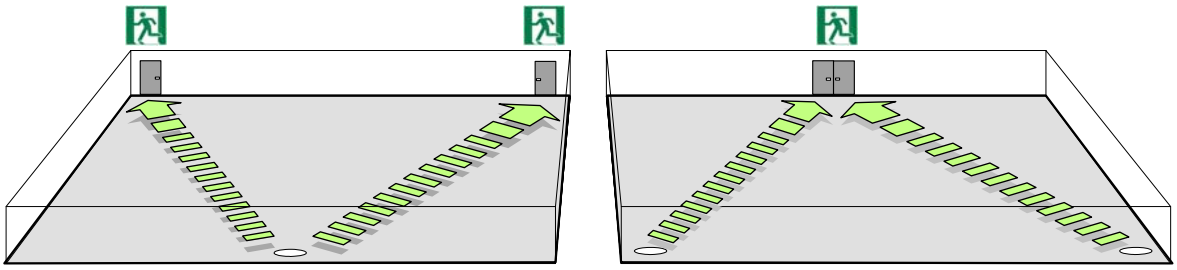


Fig. 12 Two Exits vs One Large Exit

Given the building characteristics, travel distances, occupant numbers are the same, the *ASET* and *RSET* will be the same for both designs, and so will be the factor of safety based on the *ASET-RSET* assessment.

However, do the two designs offer the same safety level? This comes back to the cliff-hanger question: *Is using two ropes equals to using one rope twice as strong?*

Since we have already evaluated cliff-hanging scenarios, we can simply use the results and equate the cliff-hanging scenarios to the building designs as follows:

- *Load on the ropes* ⇒ *ASET*
- *Capacity of the ropes* ⇒ *RSET*
- *P(attachment failure)* ⇒ *P(exit affected by fire, given a fire occurs)*

For example, if ASET = 100 ± 20 s; RSET = 300 ± 60 s; and *P*(exit affected by fire, given a fire occurs) = 0.05, then the probability of failure (see *Cases 4* and *2*):

- With two exits = $6.13\text{x}10^{-7}+0.05-6.13\text{x}10^{-7}\text{x}\ 0.05$ = **$2.57\text{x}10^{-3}$**
- With one exit twice as large = $7.83\text{x}10^{-4}+0.05-7.83\text{x}10^{-4}\ \text{x}\ 0.05$= **$5.07\text{x}10^{-2}$**

Hence, the building design with two exits, which is in load-sharing arrangement, the probability of failure is significantly lower that that with a single large exit. This is due to the fact that the former has a redundancy while the latter does not (see figure below).

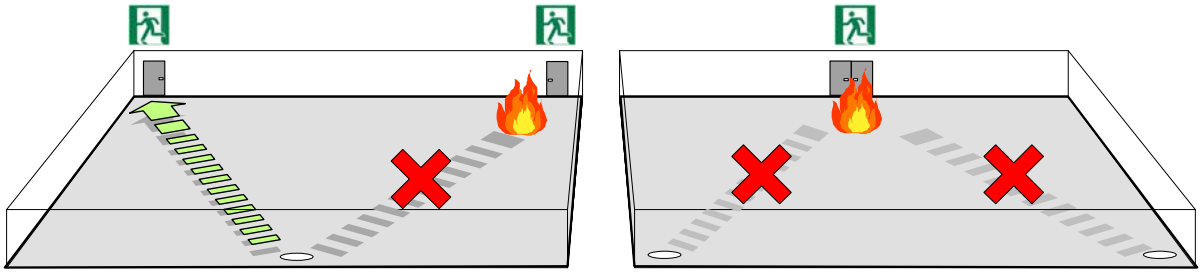


Fig.13 Effects of Redundancy

What about providing the redundancy in a stand-by rather than load-sharing arrangement?

With respect to egress, it is unusual for a stand-by arrangement unless the occupants have a preference to using one exit over another. The case in point may be a design where a non-designated exit, such as an escalator vehicle ramp, or a specially designed lift serving as a secondary means of egress when the primary exit is unusable (see figure below).

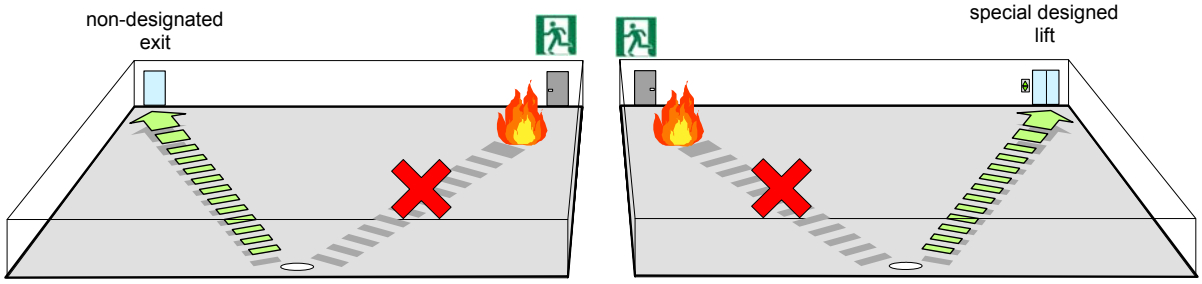


Fig. 14 Possible Stand-by Redundancy Arrangement

Nevertheless, the probability of failure in arrangement (see cliff-hanging scenarios *Case 3*):

- With two exits (one standby) = $(6.85\text{x}10^{-3}+0.05-6.85\text{x}10^{-3}\text{x}\ 0.05)^2$ = **$3.19\text{x}10^{-3}$**

This is not as safe as load-sharing arrangement. However, its probability of failure is still lower than that with a single large exit, although it has a lower factor of safety in the *ASET-RSET* assessment.

Hence, similarly in fire engineering designs, factor of safety alone does not give a true measure of the fire safety level of the building. The robustness of a design must be tested by examining the failure of the components in the system. These tests will demonstrate the redundancy and hence the robustness of the design.

CONCLUSIONS

The concepts of factor of safety, redundancy and probability of failure have been examined using the cliff-hanging scenarios. It has been demonstrated quantitatively that factor of safety and redundancy are separate aspects of design that result in deferent probabilities of failure of a system. Factor of safety and redundancy are not the same, and redundancy cannot be quantified using factor of safety.

It has also been demonstrated that, with the appropriate arrangement of redundancy, a safer system can be provided compared with one that the factor of safety is increased. This leads to the answer to the cliff-hanging question — using two ropes is generally safer than using one rope that is twice as strong.

Analogous to the cliff-hanging scenarios, factor of safety and redundancy with respect to fire engineering designs has also been discussed. Building designs with two exits and a single exit twice as large has been examined. It is similarly concluded that the former provides a safer solution than the latter. This is despite the fact that both designs have the same factor of safety based on *ASET-RSET* assessment.

It is demonstrated that a high factor of safety does not guarantee a low probability of failure, or a high level of safety. To raise the bar for fire engineering designs and to ensure a high level of safety is achieved, one must look beyond factor of safety as the sole design criteria. Failure of components and system must be carefully examined to ensure sufficient redundancy and robustness of the designs.

REFERENCES

1. Verghese, D. et al, “Designing for Failure: Redundancies in Fire Safety Engineering”, Fire Safety Engineering International Conference – The Future of Fire Engineering, Gold Coast, May 2006.
2. Hasofer, A.M., Beck, V.R., Bennetts, I.D., “Risk Analysis in Building Fire Safety Engineering”, Butterworth-Heinemann, 2007
3. “AS/NZS ISO 31000, Risk management— Principles and Guidelines”, Standards Australia, 2009.
4. Liotine, M., “Mission-critical Network Planning”, Artech House, 2003.
5. “International Fire Engineering Guidelines”, Australian Building Codes Board, 2005.
6. Walpole, R.E., Myer, R.H., Myer, S.L., Ye. K, “Probability & Statistics for Engineers & Scientists”, Eight Edition, Pearson Education International, 2007.