Rethinking engineering: risk and reliability analysis

Dennis Camilleri argues that while absolute safety is an illusion, engineers should make best use of the analytical tools available

The year 2001 will be remembered for the tragedy of the Concorde crash and the destruction of the Twin Towers in New York. Both were engineering feats and landmarks in their own field. Their destruction has meant the loss of human lives. The importance of risk and reliability analysis in engineering appears to be growing in importance by the day.

The risk, safety and reliability methodology has come out of its childhood, it is now in its youth and has yet to mature. However, as a result of the above recent developments there is greater urgency to reach maturity.

To an engineer the 'risks' associated with a hazard are a combination of a probability that that hazard will occur and the consequences of that hazard[1].

A log file of the project should be readily available as a common framework for risk and safety considerations

Consequences include: injury or loss of life; reconstruction costs; loss of economic activity; environmental losses. When explicitly addressed, a risk analysis is carried out and the result is compared with the maximum acceptable risks. These fundamental levels of safety have to be acceptable to society as a whole, for it is on their behalf that engineers make such decisions. The UK Health & Safety Executive (HSE) has defined a maximum level of risk, which is just tolerable, and a minimum level below which further action to reduce risks may not be required.

The target probability for one year should be 10^{-4} for 'normal cases', as this is what society nowadays seems to accept or is unavoidable anyway. For voluntary activities involving economic benefits or other profits, a higher value may be considered as acceptable. However, if somebody is involuntarily put to an unnatural risk from which he/she has no benefits at all, such as those living close to a plant or near a transport route of dangerous materials, the target must be lower, at 10^{-5} per year. Yet further risk reduction measures may be considered in relation to *de minimus* annual risk levels (i.e. the levels below which risks are of no legal concern), of 10^{-6} for a worker and 10^{-7} or 10^{-8} for a member of the public[2] (Table 2).

Table 1: Levels of risk

Workers all occupations (upper limit)	1/1 000 per year per person (10^{-3})
Public at risk from industrial operations	1/10 000 per year per person (10^{-4})
Public at risk from nuclear industry operations	1/100 000 per year per person (10^{-5})

Table 2: Maximum annual failure probabilities for structures depending on their safety class (consequence of failure) and the type of failure

Safety class	Ductile with reserves	Ductile	Brittle
Low	10^{-3}	10^{-4}	10^{-5}
Normal	10^{-4}	10^{-5}	10^{-6}
High	10^{-5}	10^{-6}	10^{-7}

A shortcoming of the present Ultimate Limit State method is that in the partial coefficients applied no indication is given on how safe the structure is, and no size of coefficient is given for a corresponding level of safety. The Nordic Codes indicate the partial coefficient to be adopted for a maximum failure probability depending on the safety class and type of failure.

High safety class represents situations when failure can result in large societal consequences and risks of injuries. In practice all road bridges belong to high safety class.

Eurocode 1 (EC1) differentiates structures in relation to risk to life, and risk of economic and social losses, as in Table 3. Such a classification may be used to select appropriate degrees of reliability according to such consequences. EC1 also refers to Design Working Life, as referred to in Table 4.

To overcome the problem of the partial coefficient not giving an indication of the probability of failure indicated above, the Nordic Code specifies the requirement in the ultimate limit state for the structural safety specified with reference to failure types and failure consequences, i.e. safety class with the requirements for the formal yearly probability of failure P_f. From Table 5, it is possible to calculate the formal yearly probability P_f or the corresponding reliability index β, it is possible to determine whether the requirements for the safety are fulfilled or not.

The centred value of Table 5 should be considered as the most common design situation. For example, in the Eurocode the value of $\beta = 3.8$ ($P_f = 0.7.10^{-5}$) is mentioned for a reference period of 50 years.

The NKB[3] also gives guidelines for above value:

- 0.97 is given for a 'low safety class', having a 'ductile failure with reserves', also a 'good accuracy for the calculation model', with a 'good representation of structural behaviour', and 'good quality control'.
- 3.51 is given for a 'high safety class', having a 'brittle failure', also a 'poor accuracy for the calculation model', with a 'poor representation of structural behaviour', and 'poor quality control'.

It is to be noted that the Very High Safety Class, as listed in Table 3, is not included in Table 5. The consequences are regarded as extreme and a full cost-benefit analysis involving estimates of the monetary value of potential costs and benefits is necessitated.

The evaluation of economic costs and benefits is relatively straightforward, but the evaluation of monetary costs associated with risks of death is controversial, as it involves assigning a monetary value to life. Furthermore, any procedure for determining a monetary value of life may be challenged from a philosophical point of view. The conclusion of this analysis might be that the structure should not be

Table 3: Examples of reliability differentiation according to life and economic and social loss risks

Degree of reliability	Potential risk to life, risk of economic and social losses	Examples of buildings and civil engineering works
Extremely high	Very high	Nuclear power reactors, major dams and barriers, strategic defence structures
> Normal	High	Significant bridges, grandstands, public buildings where consequences of failure are high
Normal	Medium	Residential and office buildings, public buildings where consequences of failure are medium
< Normal	Low	Agricultural buildings where people do not normally enter, greenhouses, lightning poles

built at all!

The Twin Towers, besides being a functional office building were also defined as a Monument. This placed them in the Very High Safety Class of Table 3, thus besides requiring higher partial coefficients for their design also necessitated a full cost-benefit analysis prior to proceeding with the project.

Whilst codified design is suitable for 'normal structures', it is apparent that for novel structures regard has to be taken of methods of probabilistic risk analysis. Together with refined statistical models of loading and material resistance a direct determination of failure probability may be the basis for decisions on the design.

For important projects it may be feasible to reduce the uncertainty by updating the assumed physical models by test programmes. The updated figures are used to estimate the structural reliability and the risk to the users. Structures, for which it is not practicable to reduce risks to negligible limits, include structures that are exposed to significant risks of extreme loading (e.g., due to severe earthquakes, hurricanes, cyclones or landslips). Appropriate risk-acceptance criteria related to societal expectations of life protection need to be identified.

During the lifetime of a project it goes through a number of distinct phases. During the different phases it may have varying characteristics, with the risk varying from phase to phase. A number of decisions will have to be made during its lifetime and different decision-makers will determine these.

A 'log file' containing all relevant data on the history and decisions taken on the project should be readily available, as a common framework for risk and safety considerations to be taken during different project phases. The wrong decisions taken during the Twin Towers evacuation, whilst still standing after the terrorists' strike, cost dearly in terms of human lives lost.

Safety is an ever-increasing requirement from society. Whereas absolute safety is an illusion, tools exist for achieving a trade-off, which is an optimum with respect to the aims of the decision maker. The techniques for risk and reliability can be applied with benefit in all phases of a project[4]. se

Table 4: Design working life examples

Design working life	Examples
1-5 years	Temporary structures
25 years	Replacement structural parts e.g. handrails, small canopies, protective features (slats, caps, etc)
50 years	Buildings, footbridges and other common structures
100 years	Monumental buildings and other special or important structures
120 years	Highway and rail bridges

Table 5: Safety requirements in the ultimate limit sate specified as the formal yearly probability of failure P_f and the corresponding reliability index β by the Nordic Committee (NKB)[2]

Failure consequences (safety class)	Failure type I, ductile failure with remaining capacity	Failure type II, ductile failure without remaining capacity	Failure type III, brittle failure
Less serious (low)	$P_f \leq 10^{-3}$; $\beta \geq 3.09$	$P_f \leq 10^{-4}$; $\beta \geq 3.71$	$P_f \leq 10^{-5}$; $\beta \geq 4.26$
Serious (normal)	$P_f \leq 10^{-4}$; $\beta \geq 3.71$	$P_f \leq 10^{-5}$; $\beta \geq 4.26$	$P_f \leq 10^{-6}$; $\beta \geq 4.75$
Very serious (high)	$P_f \leq 10^{-5}$; $\beta \geq 4.26$	$P_f \leq 10^{-6}$; $\beta \geq 4.75$	$P_f \leq 10^{-7}$; $\beta \geq 5.20$

REFERENCES

1. 'Risk assessment and risk communication in civil engineering', *CIB Report*, *Publication 259*, 2001.
2. 'Acceptable Risk Criteria', Reid, *Progress in Structural Engineering & Materials*, Wiley, 2000.
3. Nordic Committee for Building Regulation, (NBK): *Guidelines for load and safety determination of structures*, 1978.
4. 'Risk and safety considerations at different project phases', Hoej, *Safety, risk and reliability – trends in engineering*, International Conference, Malta, 2001.