UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

TELEPHONE: (510) 643-8678
TELEFAX: (510) 643-8919
E-MAIL: bea@ce.berkeley.edu
HTTP://www.ce.berkeley.edu/

CENTER FOR CATASTROPHIC RISK MANAGEMENT
DEPARTMENT OF CIVIL & ENVIRONMENTAL ENGINEERING
212 McLAUGHLIN HALL
BERKELEY, CALIFORNIA 94720-1710

Target Reliabilities for Engineering: A Primer

Professor Robert Bea
Center for Catastrophic Risk Management (CCRM)

Introduction

Target reliabilities are those that will be used to engineer and manage the systems during their life. There are a variety of complimentary ways to help arrive at decisions concerning these target reliabilities. Such decisions must be made by those that bear the primary responsibilities for the activities associated with the systems and for the consequences associated with those activities. The system engineers can provide information and insights concerning the tradeoffs between reliability and 'costs'. The system managers (corporate and public regulatory) must provide the decisions regarding what target reliabilities will be used to engineer the facilities.

The approaches include economics and utility based approaches, approaches based on historic or actuarial data for similar systems, and approaches based on present-day standards of practice. Each of these approaches has its advantages and disadvantages (limitations).

Economics – Utility Approaches

A risk based approach could be based on a the total life cycle risks (Rt) associated with a system:

$$Rt = Rti + Rtf$$

Rti are the initial risks associated with design, construction, and commissioning the system. Rtf are the future risks (present valued) associated with the operation of the system. These risks could be evaluated as developed below. The objective would be to define the system that could develop the minimum total risk during the life of the system.

An example application for the quality attribute of 'safety' could be developed as follows. Let the expected probability of failure to achieve adequate safety be $\overline{Pfj} = \overline{Pf2}$. This probability will be expressed on an annual basis (probability of failure per year of exposure).

Let the expected operating costs associated with the inadequate safety be $\overline{Cf2}$. Then $\overline{Rf2} = \overline{Pf2} \bullet \overline{CF2}$. Let the expected initial risks associated with varying Pf2 be a linear function of the logarithm of Pf2 that has a slope ΔCi (the cost required to change Pf2 by a factor of 10). The equation for the total risk (initial plus operating) could be differentiated and equated to zero to determine the minimum total risk and thus define the Pf2 that would develop the minimum total risk:

$$Pf2o = 0.4348 / Rc\ (pvf)$$

Rc is a ratio of the costs associated with the safety failure (CF2) to the cost required to reduce the Pf2 by a factor of 10 (ΔCi). This a non-dimensional measure of the initial and operating costs.

The pvf is a Present Value Function that is used to bring to present value terms the future costs associated with the compromises in safety. In this example, the pvf will be based on replacement of the system in the case of the compromises in safety and a continuous discounting function:

$$pvf = [1-(1+r)^{-L}]/r$$

where r is the net discount rate (investment rate minus inflation rate) and L is the life or exposure of the system in years. For long life systems ($L \geq 20$ years), pvf $\approx r^{-1}$. For short life systems ($L \leq 5$ years), pvf = L. The product of Rc times pvf is an expression of the 'effective life' of the system.

Another 'boundary' on the safety risk could be defined by equating the slope of the total cost expression to unity. It is at this point that there is a rapid rise in the total expected cost with the change in Pf2. In this case the expression becomes Pf2m = 2 Pf2o, or the 'marginal' Pf is twice the 'optimum' Pf. The results are graphed in Figure 1.

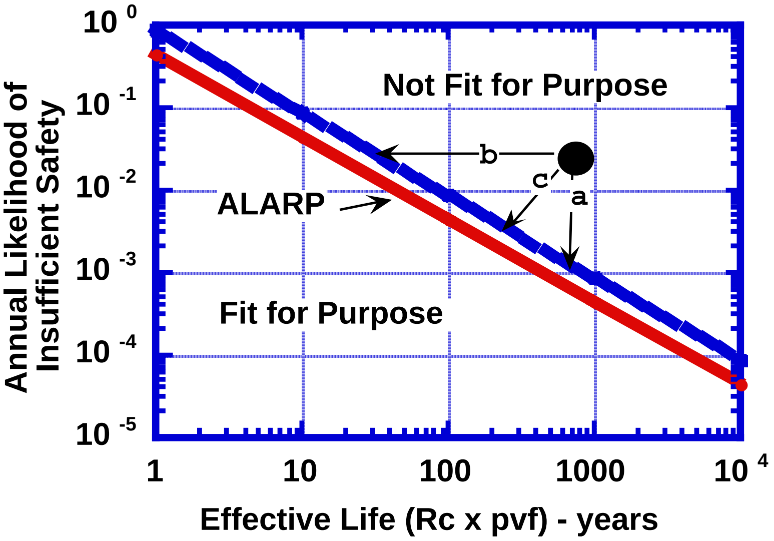

Figure1– Fitness for purpose reliability evaluation guideline

The line indicated as ALARP is the same as determined based on Pf2o. ALARP is taken to be 'As Low As Reasonably Practicable'. The dashed line indicates the marginal Pf. The combination of Pf and the measure of the initial and operating costs that lies above the dashed line is indicated as 'not fit for purpose'. The combination of Pf and the measure of initial and operating costs that lies below the solid line is indicated as 'fit for purpose'. The area between the two lines can be interpreted as the area that is subject to economic cost-benefit analyses to define an acceptable combination of likelihoods of failure and the consequences associated with the failure.

In the economics or utility based approach considerations of the broad category of potential 'consequences' associated with a failure is important. It is at this point that the very sensitive and difficult issues associated with potential environmental impacts must be addressed – including potential human impacts (injuries, fatalities). There are two basic approaches to address such impacts. The first is to address the potential impacts as a separate issue, not integrating the potential environmental injury (including human life) impacts with the other potential impacts (e.g. property losses, production and productivity losses). The second is to address the potential environmental impacts by integrating them with the same metrics to evaluate the other potential consequences.

It is at this point that the question is often raised: what is the value of a human life that should be included in the economics based approach? The reasonable way to pose the question is how much should be invested to save a human life in association with the proposed system operations? Terms like ICAF (Incremental Cost of Averting a Fatality) have been developed to help answer such questions. Analyses of the ICAF implicitly integrated into current design guidelines for natural hazards (e.g. storms, earthquakes, North American, European) indicates ICAFs in the range of U.S.$1 to $25 millions (2000). Recent studies of societal ICAFs indicate values in the range of U.S. $1 millions for developed countries like the U.S. and Norway. For developing countries like Mexico, Brazil, China, and India the ICAFs are in the range of U.S. $0.1 to 0.3 millions.

It must be remembered that the objective of the entire Target Reliability process is an attempt to identify the 'best' alternative for design and operation of a system. 'Best' means to identify that alternative (or alternatives) that can provide the best chance to realize a system that has desirable and acceptable quality and reliability during its life cycle. Once such a system has been identified (together with the associated risk assessment and management processes), then the objective shifts to implementing the risk assessment and management process during the system life cycle that can result in a system with 'zero failures' – the objective is desirable and acceptable quality in the context of resources that should be expended to achieve such goals.

Historic 'Actuarial Data' Based Approaches

A second approach is based on experience with engineered systems in which actuarial or historic data is used to identify historic precedents associated with other engineered systems. The premise of this approach is that societies and the organizations that are parts of these societies through time and experience arrive at judgments concerning what is acceptable and what is not acceptable in terms of risks.

An expression of the historic approach is given in Figure 2. This expression is based on historic annual probabilities of failure (high consequence events) and the consequences associated with the failures. The probabilities of failure are actuarial in the sense that they are based on the statistics associated with the failures of systems in the past. They are not notional in the sense that they are analytically derived or computed. The consequences are expressed in terms of U.S. dollars (1984) and deaths. Note that the expression indicates that a statistical death equates to about U.S. $1 millions.

Are there problems with the historic approach? Certainly there are! Risks associated with systems change with time. Statistically based risks involve 'mixed populations' of systems that are different in their details. The historic failures involve a wide variety of 'causes' that range from natural (caused by 'acts of God') to unnatural (caused by acts of 'man'). Many failures are never reported.

In Figure 2, note that fixed drilling rigs have a Pf ≈ 1 E-3 per year. This is due to all causes. Further examination of the causes indicates that about 20% can be attributed to 'natural' causes; the rest are due to 'accidents' (e.g. blowouts, collisions, fires, explosions). Thus, Pf for natural hazards would be about 2E-4 per year. If there were a balance between natural and accidental hazards, then the Pf for natural hazards would be about 5E-4 per year.

Another challenge associated with this approach regards the uncertainties and variabilities that are incorporated into this actuarial data based approach; there are no Type II uncertainties. Modeling variabilities are not present in actual tests (the median or central tendency values are!). Thus, when this approach is used, the information must first be carefully evaluated to eliminate Type III uncertainties (those due to human and organizational factors), and then it must be realized that the remainder represents fundamentally Type I uncertainties (due to natural variabilities). It is important there is a consistent treatment of the reliability targets with the analytical processes that are used to help demonstrate that these targets can be achieved. It is for this reason, that some reliability analysists favor not including the additional Type 2 uncertainties – but, they do favor including the necessary corrections to the predictive analytical models to assure that they develop realistic results; this means that the Bias central tendency corrections must be included.

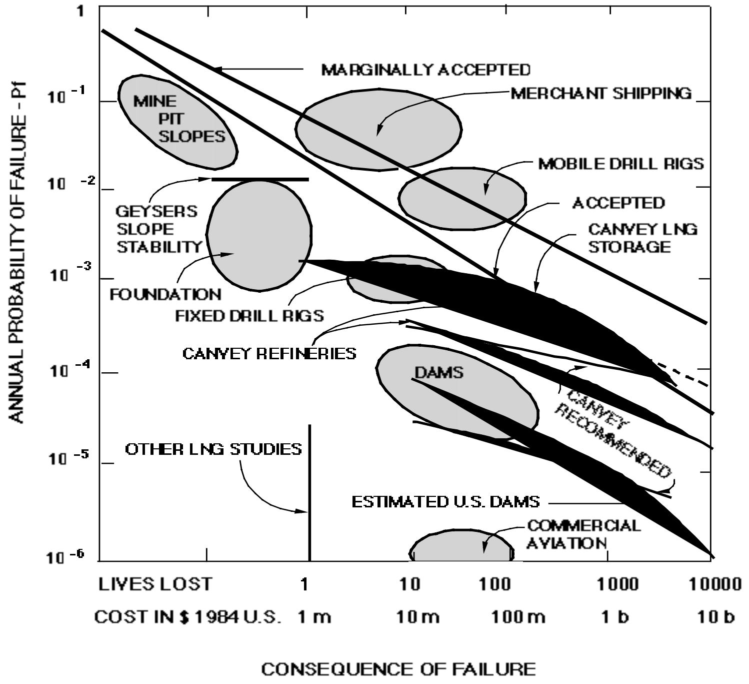

Figure 2- Historic Risk Tradeoffs

Typical collapse failure rates for engineered public structures like domestic housing, commercial office buildings, and bridges in the U.S., Canada, western Europe have been estimated to be in the range of 2E-5 per year.

Another expression of historic risk tradeoffs is that of the FAR (Fatal Accident Rate). The FAR is the number of fatalities per 10E8 hours of exposure to given activities. Figure 3 summarizes some current FARs for activities in the U.K. Commercial industrial activity FARs range from 4 (chemical processing) to as high as 250 (commercial aviation). The commercial aviation FAR increases by factors of up to 10 at different locations around the world (Africa and China have the highest FARs).

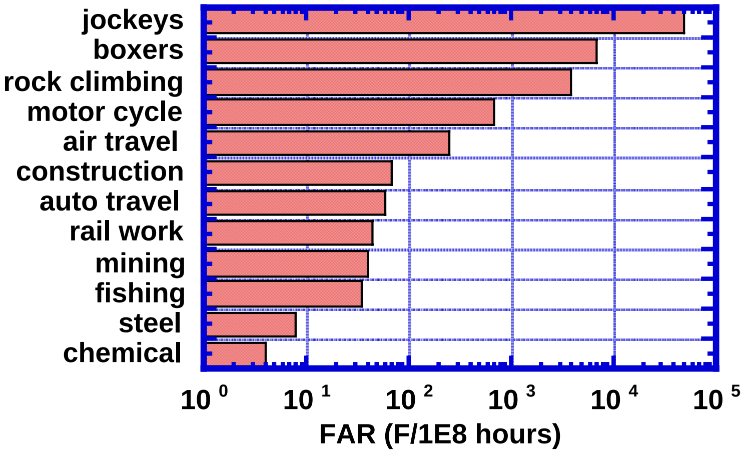

Figure 3 - General activity fatal accident rates

Figure 4 summarizes the FAR for onshore and offshore exploration and production (E&P) workers worldwide during the period 1988 – 1992 (about 75% of the hours were onshore). The E&P FAR range from a low of about 3 to a high of about 40. Operations in the North Sea area and U.S. have the lowest FAR (average of 5 to 6). Operations in South America and Africa have the highest FAR (average of 20 to 25).

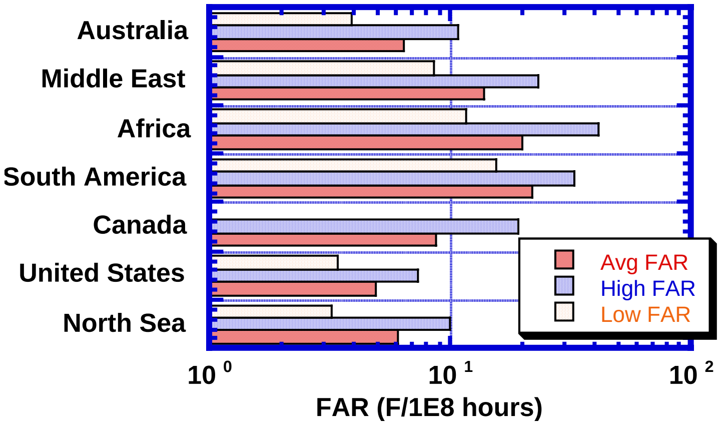

Figure 1 - Worldwide exploration and production fatal accident rates 1988 - 1992

Standards of Practice Approach

A third approach is that of the ‘standards-of-practice.’ Standards-of-practice are represented in the design codes and guidelines that are utilized by organizations and industries. Standards-of-practice are also included in the decisions that are made by system owners / operators and the associated regulators to design, requalify, and operate such systems.
Codes and guidelines can be analyzed using reliability based models to determine the reliabilities inherent in the codes and guidelines. The American Society of Civil Engineers (ASCE) Standard “Minimum Design Loads for Buildings and Other Structures” defines four categories of buildings and other structures that represent increasing hazards to human life in the event of failure (Table 1).

Table 1 – Classification of buildings and other structures for definition of design loadings (pa = per annum)

Occupancy	Category
Low hazard to human life (agriculture facilities, temporary and storage facilities)	I (10^{-2} pa)
Structures except Categories I, III, and IV	II (10^{-3} pa)
Substantial hazard to human life (more than 300 occupancy buildings, more than 250 occupancy schools, more than 500 occupancy adult education facilities, more than 50 occupancy health care facilities)	III (10^{-4} pa)
Essential structures (hospitals, emergency facilities, power facilities)	IV (10^{-5} pa)

For example, for wind loadings, Category II facilities have an importance factor, I, of 1.0. The design wind loading are associated with an annual probability of 0.02 or an average return period of 50 years (98 %tile, 2.05 standard deviations from the median). Given an uncertainty in the annual maximum wind loadings of: σ_{lnV}. = 0.72 ln ($V_{10,000\ yr}$ / $V_{100\ yr}$) = 0.72 ln (250 mph / 125 mph) = 0.50. The wind force varies as a function of the square of the wind speed, thus the uncertainty in the wind force could be estimated as: σ_{lnD}. = 2 (0.5) = 1.0. The ratio of the design wind force to the median annual maximum wind force would be: B_{D50} = exp (2.05 x 1.0) = 7.8. Given a design factor of safety of FS = 2.0, a capacity median bias of B_{C50} = 1.5, a design force median bias of B_{D50} = 0.67, and an uncertainty in the structure capacity of σ_{lnC}. = 0.25, the annual Safety Index could be determined from: β = ln (7.8 x 2.0 x 1.5 x 1.5) / 1.03 = 3.5, or an annual probability of failure of Pf ≈ 2.3 E-4. The average return period of the wind force that would bring the structure to its ultimate limit state would be approximately 5,000 years. Category III and IV structures would be designed to have greater capacities and reliabilities.

The ASCE Standard specifies a two-level design for important facilities. The strength level earthquake is specified to have an average return period of 475 years. The maximum capable earthquake is specified to have an average return period of 1000 years. The later specification would imply a probability of failure of the order of 1E-4 per year. These results are consistent with the guidelines issued by the U.S. Department of Energy for natural phenomena hazards and the onset of significant damage. For facilities in which there are concerns for occupant safety and continued operation, the annual probabilities of 'failure' (onset of significant damage) are in the range of 1E-4 to 5E-4 per year.

A standard-of-practice approach to avoid some of the problems associated with the economics and historic data based approaches. An expression of the standard-of-practice approach is given in Figure 5. The probabilities of failure are computed or notional and include only Type I or 'natural' (inherent randomness). The probabilities of failure are the total Pf and include both intrinsic (environmental, natural) and extrinsic (human, organizational) caused failures. The consequences of failure include the best estimates of economic costs associated with loss of property, injuries, restoration, productivity, and resources. The data points shown are for new and existing platforms that have been evaluated to determine their risks. The two lines labeled acceptable and marginal are those placed by the author based on the decision making processes that have accepted or rejected the assessed risks.

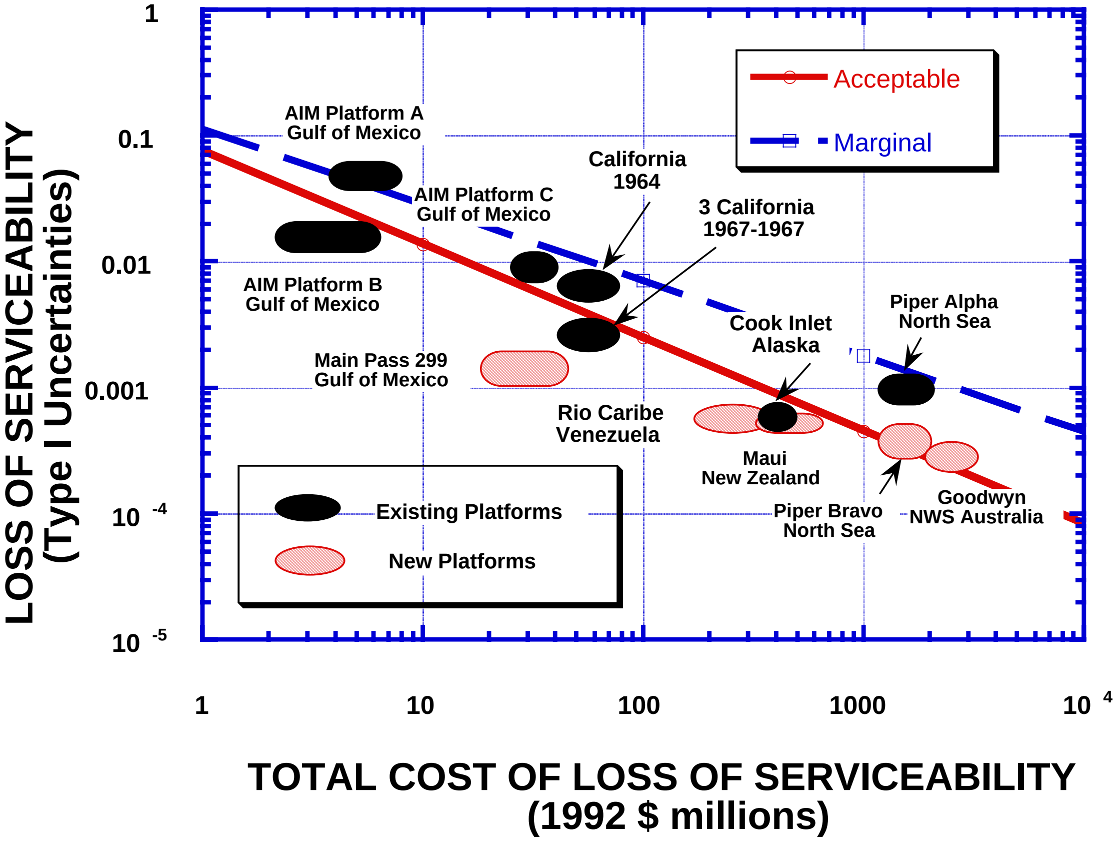

Figure 5 - Standard-of-Practice Approach

The U.K. Health and Safety Executive (HSE) have stipulated an individual risk of 1E-3 per year as a maximum tolerable criterion for workers (FAR = 30). An individual risk of 1E-4 per year is used by the HSE as a maximum tolerable criterion for members of the public from any large-scale industrial hazard (FAR = 3). These criteria have been proposed for application to average individual risk on offshore installations as 1E-3 per year for the maximum tolerable for installations in general and 1E-4 per year for new installations.

Shell has published guidelines for assessing individual worker risks (1993): if above 1E-3 per year, fundamental improvements are needed and only to be considered if there are no alternatives and people are well informed; if 1E-4 to 1E-3 per year significant effort required to improve; if 1E-5 to 1E-4 per year investigate alternatives; if 1E-6 to 1E-5 per year consider cost-effective alternatives. British Petroleum (1995) uses an ALARP approach with a maximum of 1E-3 per year for the most exposed workers.

In development of design guidelines for systems to be located offshore Canada, the Canadian Standards Association (CSA) based the guidelines on two Safety Classes: Safety Class 1 involved great risk to life or high potential for environmental pollution or damage in the event of failure; Safety Class 2 involved small risk to life and low potential for environmental pollution or damage. Annual probabilities of failure of 1E-5 and 1E-3 were stipulated for these two Safety Classes. The CSA specified the average return periods for three classes of loadings that could act on the offshore structures: 1) frequent environmental processes 100 years (with a load factor of 1.35), 2) rare environmental events 1,000 to 10,000 years (with a load factor of 1.0), 3) accidental loading events 1,000 to 10,000 years (with a load factor of 1.0).

Insights

Inferring reliabilities of structures from analyses of design codes and guidelines also leaves much to be desired. The analyses frequently omit the critical and difficult to define ‘biases’ (hidden conservatism). Because design codes and guidelines only address elements in the structures, the ‘system’ effects are generally omitted. Static and elastic focused methods replace the true nonlinear dynamics of the platform environment and ‘reality’ is lost.

There is no perfect approach to solve the difficult problem of determining what is an acceptable and desirable risk of associated with an engineered system. One of the most important elements of the question of "how safe is safe enough?" is the process of answering that question. The process of looking in a fundamental and deliberate manner at what constitutes an acceptable and desirable risk is perhaps the most valuable part of developing an answer to this question. The process must include effective communications of the risks that are to be taken so that understanding and agreement are developed.

A fundamental objective should be to optimize the use of economic resources while preserving 'reasonable' protection for life, property, and the environment. Consider three alternative systems. One is designed, constructed, operated, and decommissioned in a 'perfect' manner. This system results in the highest possible net life-cycle income for the venture. The second system is designed, constructed, operated, and decommissioned in a 'minimum compliance' manner. While this system has a lower initial cost, its future costs bring its life-cycle benefits to a very low value. The search is for the combination of design, construction, operation and decommissioning strategies and activities that will bring the system to have the highest possible benefits. Perfection is not possible. Something close to it is possible and this is the challenge faced by engineers and managers in today's business environment.

Systems that are indicated as not fit for purpose (e.g. Figure 1) can be modified to be fit for purpose by using three basic strategies:

1. Reduce Pf – reduce the likelihoods of failures,
2. Reduce the consequences of failures - decrease CF, decrease pvf,
3. Combinations of a) and b).

Additional strategies for risk management include:

4. Avoiding the hazards
5. Transferring all or a portion of the risks (e.g. insurance, project partners).

A risk management system should be practical, realistic, and be cost and benefit effective. Risk management systems need not be complicated. Excellent risk management results from a combination of uncommon common sense, qualified experience and judgment, knowledge, intuition, wisdom, and integrity. Mostly an excellent risk management system is a willingness to operate in a caring and disciplined manner in approaching the critical features of any activity in which risk can be generated. Risk management is largely a problem of doing what we know we should do and not doing what we know we should not do.

The purpose of a risk management system should be to enable and empower those that have direct and daily responsibilities for the quality and reliability of a system during its life cycle. The engineers can play vital roles in this empowerment. If technology is not used wisely, scarce resources and attention can be diverted from the true factors that determine quality and reliability. The purpose of a risk management system should be to assist the 'front line operators' to take the right (sensible, appropriate) risks and to achieve acceptable quality and reliability. To try to completely eliminate risk is futile. To help identify and manage risks and make appropriate use of technology to accomplish these objectives should be one of the key objectives of a risk management system.

Professor Robert Bea