1

Domain-Independent Methods for Reliability Improvement and Risk Reduction

1.1 The Domain-Specific Methods for Risk Reduction

A systematic classification of generic methods for reducing technical risk is crucial to risk management, safe operation, engineering designs, and software. However, this very important topic has not been covered with sufficient depth in the reliability and risk literature. For many decades, the focus of the reliability research has been primarily on identifying risks, risk assessment, and reliability prediction rather than methods for reliability improvement and risk reduction. The as low as reasonably practicable (ALARP) approach to risk management (Cullen 1990; HSE 1992; Melchers 2001), for example, advocates that risks should be reduced ALARP. This is commonly interpreted in the sense that risks have to be reduced to a level at which the cost associated with further risk reduction outweighs the benefits arising from further reduction (HSE 1992; Melchers 2001). While a decision about implementation of risk-reducing measures can be taken by implementing cost–benefit analysis, the focus of the ALARP approach is whether risk-reducing measures should be implemented or not. There is little clarity on the risk-reducing methods that can be used to achieve the risk reduction.

Reliability improvement and risk reduction also relied for a long time on the feedback provided from reliability testing or on feedback from customers. Once the feedback about a particular failure mode is available, the component is redesigned to strengthen it against that failure mode. The problem with this approach is that the feedback always comes late, after the product has been manufactured. Therefore, all changes consisting of redesign to avoid the discovered failure modes will be costly or impossible. In addition, conducting a reliability testing programme to precipitate failure modes is expensive and adds significant extra cost to the product.

General guidelines on risk management do exist. Risk management, according to a recent review (Aven 2016) can be summarised to (i) establish the purpose of the risk management activity, (ii) identify adverse events, (iii) conduct cause and consequence analysis, (iv) make judgement about the likelihood of the adverse events and their impact and establish risk description and characterisation, and (v) risk treatment.

While a great deal of agreement exists about the necessary common steps of risk assessment, there is profound lack of understanding and insight about the general methods for reducing risk that can be used. The common approach to risk reduction is the domain-specific approach which relies heavily on *root cause analysis* and detailed knowledge from the specific domain. Measures specific to a particular domain are selected for reducing the likelihood of failure or the consequences from failure and the risk

Methods for Reliability Improvement and Risk Reduction, First Edition. Michael Todinov.

reduction is conducted exclusively by experts in the specific domain. The risk reduction is effectively fragmented into risk reduction in numerous specific domains: nuclear industry, aviation, construction industry, food storage and food processing, banking, oil and gas industry, road transportation, railway transportation, marine transportation, financial industry, cyber security, environmental sciences, etc.

As a result, the domain-specific approach to risk reduction created an illusion: *that efficient risk reduction can be delivered successfully solely by using methods offered by the specific domain without resorting to general methods for risk reduction*.

The direct consequence of this illusion is that many industries have been deprived from effective risk-reducing strategy and reliability improvement solutions. The same mistakes are made again and again, resulting in numerous accidents and inferior products and processes, associated with high risk of failure. Examples of such repeating mistakes are:

- insufficient reliability built in products with very high cost of failure;
- designing components with homogeneous properties where the stresses are clearly not uniform;
- creating systems with vulnerabilities where a single failure causes the collapse of the system;
- redundancy compromised by a common cause.

At the same time, excellent opportunities to improve reliability and reduce risk are constantly missed. Examples of such missed opportunities are:

- failure to increase reliability of systems and components at no extra cost (e.g. by a simple permutation of the same type of components in the system);
- failure to increase the reliability of components and systems by a separation of properties and functions;
- failure to reduce by orders of magnitude the probability of erroneous conclusion from imperfect tests;
- failure to increase by orders of magnitude the fault tolerance of components;
- failure to reduce risk by including deliberate weaknesses.

The weaknesses of the risk management in many specific domains were exposed by a string of costly failures and disasters (e.g. catastrophic oil spills, financial crises, serious industrial accidents, transport accidents, power blackouts, etc.).

In some cases, correct solutions were indeed found by 'reinventing the wheel', after a series of costly and time-consuming trials and errors.

An important contributing reason for this highly undesirable situation is *the absence of a framework of domain-independent methods for reliability improvement and risk reduction that could provide vital methodological knowledge to many unrelated domains*.

With the exception of a few simple and well-known domain independent methods such as *implementing redundancy, strengthening weak links*, *upgrading with more reliable components, simplification of components, systems and operations*, and *condition monitoring*, the framework of domain-independent methods for reliability improvement and risk reduction is missing.

Thompson (1999) stressed the importance of effective integration of maintainability and reliability considerations in the design process and the importance of failure mode analysis in design. Thompson (1999) correctly identified that knowledge of the principles of risk are

important aids to achieving good reliability, however, no domain-independent principles for improving reliability and reducing risk have been formulated.

Samuel and Weir (1999) covered problem solving strategies in engineering design and stressed the importance of satisfying design inequalities in defining the domain of acceptable designs. However, no domain-independent methods for improving reliability have been discussed.

French (1999) formulated a number of general principles to be followed in conceptual design, but they were not oriented towards improving reliability and reducing technical risk. General principles to be followed in engineering design have also been discussed in Pahl et al. (2007). Most of the discussed principles, however, are either not related to reducing the risk of failure or are too specific (e.g. the principle of thermal design), with no general validity. Collins (2003) discussed engineering design with failure prevention perspective. However, no risk-reducing methods and principles with general validity were formulated.

Taguchi's experimental method for robust design through testing (Phadke 1989) achieves designs where the performance characteristics are insensitive to variations of control (design) variables. This method can be considered to be a step towards formulating the domain-independent risk reduction principle of robust design for which the performance characteristics are insensitive to variations of design parameters.

1.2 The Statistical, Data-Driven Approach

A common approach to reliability improvement is to select a statistical-based, data-driven approach. This approach relies on critical pieces of data: *failure frequencies, load distribution, strength distribution*, etc., in order to make predictions about the reliability of components and systems.

To describe the reliability on demand, which is essentially the probability that strength will exceed load, data covering the variation range of the load and the variation range of the strength are needed. These data are necessary to fit an appropriate model for the strength, an appropriate model for the load, and to estimate the parameters of the models fitting the load distribution and strength distribution. Next, a direct integration of the load–strength interference integral or a Monte Carlo simulation can be used to estimate the probability that, on demand, strength will be greater than the load (Todinov 2016a).

To calculate the time to failure of a system, the time-to-failure models of the components are needed. For each component, from the past times to failure, an appropriate time-to-failure model must be fitted and subsequently used to evaluate the reliability of the system built with the components (Todinov 2016a). However, the time-to-failure models of the components depend strongly on the environmental stresses. For example, increasing temperature accelerates material degradation and shortens the time to failure. Because of this, the time to failure of a seal working at elevated temperatures is significantly shorter than the time to failure of a seal working at room temperature. Reducing temperature also gives rise to dangerous failure modes (e.g. brittle fracture) which reduce the time to failure. The time to failure in the presence of a corrosive environment, high humidity and vibrations is shorter than the time to failure in the absence of such environmental stresses.

It is a well-established fact that time-to-failure models built on past reliability data collected for a particular environment yield poor predictions if applied automatically to another environment. To fit a reliable and robust model, the past failure data need to cover

all possible duty cycles and different environmental conditions (temperature, humidity, vibrations, pressure, corrosion stresses, etc.) the product could encounter. This is a near to impossible task. As a result, the time-to-failure models built on past failure data, not covering all possible operating conditions and environmental stresses, lead to increased levels of uncertainty in the model parameters and poor predictive power.

Finally, the data-driven approach provides feedback about the product performance after it has been released in the field. The time delay in receiving this feedback, long after the design stage, makes it expensive to improve reliability.

Calculating the reliability built in a product by using past data is often a difficult task because reliability-critical data (failure frequencies, strength distribution of the flaws, failure mechanisms, and repair times) may not be available, particularly for new designs, with no failure history. This does not permit meaningful analysis and correct prediction of the reliability of components and systems, for different environments or uses.

The pure statistical approach does not normally address the physical principles controlling the operation and failure of engineering systems and components.

Even if all critical pieces of information were available, in some cases, a meaningful reliability prediction would still be a problem. Consider, for example, a simple assembly including a large number of identical components from the same batch. Suppose that the assembly fails whenever any of the identical components fail. The reliability of the assembly is then estimated by raising the estimated reliability R of a single component to a power equal to the number of the components in the assembly. Increasing the number of tests will reduce the uncertainty associated with the estimated reliability R of a single component but will never eliminate it.

A small error in estimating the reliability R of the identical components would result in an unacceptably large error (uncertainty) in the estimated reliability of the assembly, which renders the reliability prediction meaningless.

This can be illustrated by a simple analytical argument. Consider a simple assembly built on n identical components from the same batch, each characterised by reliability R. The reliability of the system then becomes $R_{sys} = R^n$. An error ΔR in the reliability of a single component leads to a relative error $\Delta R_{sys}/R_{sys} = n\,(\Delta R/R)$ in the predicted reliability for the system. For a system composed of 50 capacitors, logically arranged in series, from the same production batch, a mere 1% relative error in the estimated reliability of a single capacitor will result in $\Delta R_{sys}/R_{sys} = 50 \times 0.01 = 0.5$ (50%) error in the estimated system reliability, which makes the reliability prediction meaningless.

Furthermore, while the time to failure due to a particular wearout failure mode can, in some cases, be predicted with a great deal of confidence, no reliable prediction of the time to failure of software components is possible. It depends on a particular combination of input data, user choice, and other conditions, which cannot normally be predicted with confidence.

Some of these difficulties led some authors to question the appropriateness of reliability prediction based on past failure rates.

1.3 The Physics-of-Failure Approach

The development of the physics-of-failure approach to reliability improvement (Pecht et al. 1990; Pecht 1996) has been prompted by the major deficiency of the data-driven approach

discussed earlier – the critical dependency on the availability of past failure rates. The physics-of-failure approach created a widespread view among many reliability practitioners that only developing physics-of-failure models can deliver reliability improvement and developing physics-of-failure models is the only proper method to assess the reliability of a product. This view has also been fuelled by the failure of some statistical models to predict correctly the life of engineering components.

According to the physics-of-failure approach, failures and decline in performance of components and systems occur due to known underlying failure mechanisms. Unlike the data-driven approach, the physics-of-failure approach addresses the underlying causes of failure. Many failure mechanisms lead to accumulation of damage. Failure is initiated when the amount of accumulated damage exceeds the endurance limit and the time to failure of components can be physically modelled.

Despite these advantages, building accurate physics-of-failure models of the time to failure is not always possible because of the complexity of the physical mechanisms underlying the failure modes, the complex nature of the environment and the operational stresses. There is usually a great deal of uncertainty associated with the parameters of the physics-of-failure models. If the goal, for example, is to increase strength, the physics-of-failure modelling can help increase strength by conducting research on the link between microstructure and mechanical properties. This approach requires arduous and time-consuming research, special equipment and human resources while a positive outcome from the research is not guaranteed.

Furthermore, in many failure events, several failure mechanisms are often involved, interacting in a very complex fashion. Such is, for example, the corrosion fatigue where two very complex, interdependent, and synergistic failure mechanisms (‘corrosion’ and ‘fatigue’) contribute to failure. Corrosion increases the rate of fatigue damage accumulation and the progression of the fatigue crack increases the extent of corrosion. This complex interaction and synergistic behaviour cannot be captured and modelled successfully if limited research is done on corrosion, fatigue and their interaction.

Often, limited experimental evidence is available because of cost limitations. The experimental evidence necessary to build a correct model can be limited not only in terms of quantity but also in terms of quality. There is a difference between observed phenomena and driving force. The experimental evidence usually captures the visual component of damage (the observed phenomena), which may not necessarily reflect the driving force behind the damage accumulation and the total existing damage precipitating failure. As a result, only the visual manifestation of the damage is captured and quantified as opposed to the driving force behind the damage accumulation and the total damage reaching the damage endurance limit. Acquiring the necessary knowledge and data related to the failure mechanisms, capturing and quantifying all types of uncertainty, necessary for a reliable prediction of the time to failure, is a formidable task.

Despite their success and popularity, physics-of-failure models cannot transcend the initial narrow domain they serve and cannot normally be used to improve reliability and reduce risk in unrelated domains.

Implementing measures aimed at eliminating hydrogen embrittlement in welds, for example, is a very important step towards improving the reliability of welds and reducing the risk of failure. These measures, however, cannot transcend the narrow domain of the welding technology. They cannot, for example, be applied to reduce risk in computer networks, finance, economics, etc.

For this reason, physics-of-failure methods cannot normally be generalised as domain-independent reliability improvement methods.

1.4 Reliability Improvement and TRIZ

The need for increasing efficiency and reducing the weight of components and systems while maintaining high reliability is a constant source of technical and physical contradictions. Hence, it is no surprise that several principles for resolving technical contradictions formulated by Altshuller in the development of TRIZ methodology for inventive problem solving (Altshuller 1984, 1996, 1999) can also be used for reducing technical risk. Eliminating harmful factors and influences is the purpose of many inventions and Altshuller's TRIZ system captured a number of useful general principles which could be used to eliminate harm.

Here, it needs to be pointed out that many of the principles for technical risk reduction with general validity are rooted in the reliability and risk theory and cannot possibly be deduced from the general inventive principles formulated in TRIZ, which serve as a general guide in developing inventive solutions, as an alternative to the trial-and-error approach. For example, the domain-independent principle which states that the reliability built-in a system should be proportional to its cost of failure is rooted in the risk theory and cannot be deduced from general inventive principles.

Another limitation of TRIZ is the lack of coverage of the mechanisms through which the inventive methods could achieve reliability improvement and risk reduction.

Another weakness preventing the effective use of TRIZ for reliability improvement is that the TRIZ methods are not backed with mathematical models or algorithms which, in a number of cases, are absolutely necessary to unlock the reliability improvement resource. Indeed, by providing a succinct description of the system, a mathematical model or algorithm could deliver significant benefits:

- The system can be described by taking into consideration a very complex interaction of risk-critical factors which could not be intuitively contemplated by design engineers. In many cases, the only way to extract risk-reduction benefit is to build and analyse a mathematical model or algorithm. Such is the case, for example, of reducing the risk of overlap of risk-critical events which requires a relevant mathematical model to be built.
- A mathematical model or an algorithm provides a way of tracking the impact of the risk-critical factors on the level of risk. In this respect, the mathematical model/algorithm provides an insight into which control variables are essential and which seemingly important variables have actually no practical impact on the reliability and risk level.
- A mathematical model or algorithm provides insight into which factor needs to be altered and by how much in order to extract the maximum risk-reduction benefit.

1.5 The Domain-Independent Methods for Reliability Improvement and Risk Reduction

The reliability and risk literature (Bazovsky 1961; Barlow and Proschan 1965, 1975; Ang and Tang 1975; Billinton and Allan 1992; Ramakumar 1993; Ebeling 1997; Meeker and

Escobar 1998; Vose 2000; Booker et al. 2001; Bedford and Cooke 2001; Kuo et al. 2001; Trivedi 2002; Andrews and Moss 2002; Aven 2003) is oriented towards risk modelling, risk assessment, risk management and decision making and there is very little discussion related to domain-independent principles for reducing technical risk.

Well-known methods for improving reliability and reducing risk such as *simplification of components and systems, introducing redundancy, strengthening weak links* or *condition monitoring* have the potential to reduce risk in many unrelated domains (e.g. computer networks, finance, economics, etc.). They are domain-independent and do not rely on reliability data or knowledge of physical mechanisms underlying possible failure modes. As a result, they are very well suited for developing new designs, with no failure history and unknown failure mechanisms.

The domain-independent risk reducing methods are not a substitute for domain-specific methods. Rather, they are a powerful enhancement of the domain-specific risk reduction methods and help to obtain superior solutions. Consequently, the domain-independent methods form an important part of risk science.

The systematic distilling, formulating and classifying of domain-independent methods and principles for improving reliability and reducing technical risk started in a 2007 book (Todinov 2007), continued in a subsequent book (Todinov 2016a) and was recently accelerated in a series of papers introducing a number of new domain-independent methods for reliability improvement and risk reduction (Todinov 2017a,b,c). In the 2007 book (Todinov 2007), the domain-independent principles for risk reduction have been broadly divided into: 'preventive' – reducing mainly the likelihood of failure; 'protective' – reducing mainly the consequences from failure; and 'dual' – oriented towards reducing both the likelihood of failure and the consequences from failure.

The recently proposed new domain-independent reliability improvement and risk reduction principles and methods transcend the area of mechanical engineering where they originated and can be applied in diverse areas of human activity. For example, the new risk reduction methods (*separation, stochastic separation, segmentation, self-reinforcement, inversion, reducing the rate of accumulation of damage, introducing deliberate weaknesses, permutation and limiting the space and time exposure*) can be applied in various unrelated domains.

Without sound methodological knowledge of domain-independent methods, opportunities for decreasing risk by separating functions and properties, by segmentation, inversion or by introducing deliberate weaknesses cannot be seen and are often missed. Many of the domain-independent methods for risk reduction presented in this book reduce risk at no extra cost. This is a big advantage over many traditional methods for reducing risk (redundancy, upgrading components, condition monitoring) which are associated with substantial investment.

Consider the problem of increasing the reliability of a cylindrical pressure vessel with a specified volume. Typical domain-specific solutions are to increase the strength of the material of the pressure vessel or to increase the thickness of the shell. The first solution is costly because it requires, research, human resource, time, special equipment, and expensive alloys. The second solution is associated with increasing the weight and the cost of the pressure vessel. These undesirable consequences associated with both solutions can be avoided if the domain-independent method of *inversion by maintaining an invariant* (Todinov 2017b) is used. This method alters the shape of the pressure vessel by reducing its diameter, increasing the length, and decreasing the thickness of the shell while preserving

the volume. This reduces the maximum stress in the shell and improves reliability with a simultaneous reduction in weight and cost (see Chapter 8).

Improving the reliability of a seal on a pressure vessel by inverting the relative location of the cover or improving the reliability of drilling by inverting the orientation of the component are also improving reliability at no extra cost. By using separation in geometry, the reliability of a cantilever beam can be improved at no extra cost (Todinov 2017a). The logical separation, for example, leads to low-cost yet very efficient designs eliminating safety risks (Todinov 2017a). By using permutation of components of the same type and different age, the reliability of common parallel series systems can be improved at no extra cost (Todinov 2015). Using the domain-independent principle of introducing deliberate weaknesses towards which failure is channelled in the case of overloading, also leads to low-cost risk reduction solutions. The alternative is expensive upgrading of the reliability of components.

For an expert in a specific domain it is not obvious that the risk of an erroneous conclusion from an imperfect test can be decreased by orders of magnitudes by segmenting the test. The domain-independent method of segmentation leads to a low-cost risk reduction solution because no investment is made into more precise test equipment, associated with a smaller measurement error (Todinov 2017c).

In a number of cases, the reliability improvement by capturing a self-reinforcing response, by self-anchoring, and self-alignment is also achieved at no extra cost (Todinov 2017b).

Without understanding the reliability improvement mechanisms of the segmentation, it is counter-intuitive and difficult to see why a monolithic column loaded in compression is less fault-tolerant compared with a column built with bricks of the same material that are not linked.

For many domain experts, for example, it is not obvious that the reliability of a piece of wire loaded in tension can be increased significantly simply by decreasing the loaded length without altering the material of the wire or its cross-sectional area. The reliability improvement is achieved at a reduced cost because the amount of material used is reduced.

Without the prompt from the domain-independent method of separation, designers often select material with uniform properties even though the loading and the stresses are not uniform. This leads to premature failures and unreliable products. Applying the method of separation also leads to reliability improvement at no extra cost. Instead of selecting expensive material with the ability to resist all environmental stresses, a combination of cheap materials can be used, optimised to resist individual environmental stresses.

The application examples and case studies featured in this book cover *mechanical engineering, civil engineering* and *construction, electronics, software engineering, chemical engineering, financial control, management, project management, environmental sciences, logistics supply, economics*, etc.

By providing the theoretical foundation for solving risk management problems in diverse areas of human activity, the domain-independent methods change radically the existing risk reduction paradigm based exclusively on domain-specific methods.

The domain-independent methods for reducing risk are so powerful that some of them (e.g. *the method of segmentation, the method of separation*, and *the method of inversion*) can effectively be used as self-contained tools for solving problems unrelated to risk reduction.