Domain-independent approach to risk reduction

Michael Todinov
School of Engineering, Computing and Mathematics
Oxford Brookes University, Oxford, OX33 1HX
e-mail mtodinov@brookes.ac.uk

Abstract. The popular domain-specific approach to risk reduction created the illusion that efficient risk reduction can be delivered successfully solely by using methods offered by the specific domain. As a result, many industries have been deprived from efficient risk reducing strategy and solutions.

This paper argues that risk reduction is underlined by domain-independent methods and principles which, combined with knowledge from the specific domain, help to generate effective risk reduction solutions. In this respect, the paper introduces a powerful method for reducing the likelihood of computational errors based on combining the domain-independent method of segmentation and local knowledge of the chain rule for differentiation.

The paper also demonstrates that lack of knowledge of domain-independent principles for risk reduction misses opportunities to reduce the risk of failure even in such mature field like stress analysis.

The domain-independent methods for risk reduction do not rely on reliability data or knowledge of physical mechanisms underlying possible failure modes and are particularly well suited for developing new designs, with unknown failure mechanisms and failure history. In many cases, the reliability improvement and risk reduction by using the domain-independent methods reduces risk at no extra cost or at a relatively small cost.

The presented domain-independent methods work across totally unrelated domains and this is demonstrated by the supplied examples which range from various areas of engineering and technology, computer science, project management, health risk management, business and even mathematics.

The domain-independent risk reduction methods presented in this paper promote building products and systems characterised by high-reliability and resilience.

Keywords: risk reduction; reliability improvement; domain-independent methods; domain-specific methods; TRIZ

1. Introduction

For many decades, the focus of the reliability and risk literature (Barlow and Proshan, 1965,1975; Bazovsky, 1961; Ang and Tang, 1975; Billinton and Alan, 1992; Ramakumar, 1993; Ebeling, 1997; Meeker and Escobar, 1998; Bedford & Cooke 2001; Booker et al, 2001; Vose 2002; Trivedi, 2002; Andrews and Moss, 2002; Aven 2003), has been covering exclusively identifying risks, reliability and risk assessment, reliability and risk modelling, decision making and reliability prediction. However, the strategic topic related to methods for improving reliability and reducing risk of failure has not been covered in sufficient depth. There is very little discussion related to general

principles for improving reliability and reducing technical risk even though these are key to a successful risk management. Despite that sophisticated tools for quantifying uncertainty are already available, they are relatively unused because risk managers rarely believe these will help their decision process (Goldstein, 2011).

While a great deal of agreement exists about the necessary common steps of risk assessment (Aven, 2016), there is 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 in the specific domain. To reduce the likelihood of failure or the consequences from failure, commonly, measures specific to a particular domain are selected and the risk reduction process is conducted exclusively by experts in the specific domain. This created the illusion that efficient risk reduction can be delivered successfully solely by using methods offered by the specific domain, without resorting to a unified methodology. As a result, the industry has been deprived of efficient risk reducing strategy and solutions. Without a unified methodological risk-reduction framework, the same mistakes in design are made again and again, resulting in inferior products, and processes associated with high risk of failure. At the same time, opportunities to improve reliability at no extra cost or at a small cost are constantly missed. A compilation and analysis of common mistakes in design of structures that led to catastrophic failures has been presented in (Petroski, 1994).

The domain-specific approach led to a situation that for many domains, even the existence of a reliability and risk science has been forgotten. In textbooks on mechanical engineering and design of machine components for example, there is hardly any mention of general methods for improving reliability and reducing the risk of failure of the engineering products.

For a long time, reliability improvement and risk reduction relied 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 be strengthened 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. In some cases, such as

environmental pollution with disposable plastic products, the delay associated with such approach can be catastrophic to the environment.

For a long time, the risk science failed to appreciate that risk reduction is underlined and governed by general (domain-independent) methods and principles which work in many unrelated domains.

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

Here it needs to be pointed out that 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 approach. Combined with knowledge from the specific domain, the domain-independent methods help to obtain superior solutions.

The ALARP approach to risk management (Cullen, 1990; HSE, 1992; Melchers 2001), for example, advocates that risks should be reduced as low as reasonably practicable. 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 the 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.

Thompson (1999) stressed the importance of effective integration of maintainability and reliability considerations in the design process and the importance of FMEA in design. The popular Failure Mode and Effects analysis (FMEA) widely used in industry is useful for tracking how the malfunctioning of a component will manifest into a failure mode of the system but it does not provide any guidance on the principles underlying the design for reliability. 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.

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, 2007). Most of the discussed principles, are not focused on improving the reliability and reducing risk 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.

The development of the physics-of-failure approach to reliability improvement (Pecht et al, 1990) has been prompted by some deficiencies of the data-driven approach: (i) models based on data collected for particular environment (temperature, humidity, pressure, vibrations, corrosive agents, etc.) give sometimes poor predictions for the time to failure of products working in different environment; (ii) the data-driven approach is critically dependent on the availability of past failure rates. According to the physics-of-failure approach, failures and decline in performance occur due to known underlying failure mechanisms. Failure mechanisms lead to accumulation of damage and failure is initiated when the amount of accumulated damage exceeds the endurance limit. As a result, the time to failure of products can be physically modeled.

The physics-of-failure approach was very successful in addressing the underlying causes of failure and eliminating failure modes and contributed to a widespread view among reliability practitioners that only physics-of-failure models can deliver a real reliability improvement.

However, it is necessary to point out that 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. Physics-of-failure modelling certainly helps, for example, in increasing the strength of a component by conducting research on the link between microstructure and mechanical properties of the material. However, this approach requires arduous and time consuming research, special equipment and human resource. 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.

2. Domain-independent methods for improving reliability and reducing risk.

There is plenty of evidence demonstrating the advantages of the domain-independent thinking in improving reliability and reducing risk across unrelated domains of human activity. Thus, implementing the domain-independent method of *active and passive redundancy* improved tremendously the safety of operations in chemical plants, air travel, nuclear plant operations, the reliability of electrical distribution networks and the reliability of computers.

The domain-independent concept of *condition monitoring* has been successful in improving the safety and reliability in mechanical engineering, civil engineering, transportation, electrical distribution, chemical plants, nuclear plants and many other areas. Introducing deliberate weak links (such as electrical fuses, mechanical fuses or sacrificial anodes) prevents failure of expensive equipment in all areas of human activity.

The need for increasing efficiency and the need for 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 (translated from Russian as Theory of Inventive Problem Solving) 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. The TRIZ methodology can certainly be considered as evidence of the power of the domain-independent thinking in reducing harm.

Despite the power of the domain-independent thinking for creative problem solving demonstrated by TRIZ, a major weakness preventing the effective use of TRIZ for reliability improvement and risk reduction is that the TRIZ methodology is not backed by mathematical models or algorithms which, in a number of cases, are absolutely necessary to determine the level of risk and see clearly the reliability improvement resources.

By providing a succinct description of the system, a mathematical model or algorithm could deliver significant risk-reduction 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.

- A mathematical model or an algorithm provides a way of tracking the impact of the risk-critical factors on the level of risk and to determine the optimal balance between level of risk and cost of the risk reduction resources.

In what follows, the basic underlying ideas are formulated for the following little-known and very efficient domain-independent methods: i) *method of segmentation*; ii) *method of separation*; iii) *method of inversion*; iv) *method of self-reinforcement* v) *method of permutations* and vi) *method of substitution*.

These methods have been distilled from a large number of engineering solutions, each of which was analyzed to assess its effect on reliability and risk. The available solutions have also been analyzed for recurring reliability improvement patterns and invariants which were captured into categories and classes. Often, reliability improvement and risk reduction by these methods is achieved at no extra cost or at a very small extra cost.

3. Improving reliability and reducing risk by segmentation and separation

3.1 Method of segmentation

Underlying idea: *to prevent failure modes and reduce the vulnerability to a single failure, by dividing an entity into a number of distinct parts*.

Implementation

To implement the method of segmentation, critical elements (e.g. forces, volumes, masses, areas, lengths, etc.) are identified and segmented and the effect of the segmentation on reliability and risk is investigated. The mechanisms through which this is achieved is (i) by limiting the spread of damage caused by the segmentation, (ii) by reducing the vulnerability to a single failure, (iii) by reducing the hazard potential of substances because of reducing the quantities handled, (iv) by reducing the likelihood of an error because of simplifying the problem due to the segmentation.

Segmentation of a macro-level entity into a number of micro-level entities working in parallel also makes the entity resistant to a single failure at a micro-level. Segmentation

effectively replaces *a single failure* occurring at a macro level with non-critical failures occurring at a micro level.

Application examples:

An example related to *limiting the spread of damage* can be given with a monolithic glass panel which is shattered totally if hit by an object because the initial crack from the projectile spreads through the entire panel. Dividing the glass panel into small glass segments limits the spread of damage thereby reducing the consequences of failure.

Reducing the hazard potential is achieved by the segmentation of hazardous substances which limits the amount of energy locked in the substance and its potential to cause harm. Processing very small (segmented) volumes of toxic substances at a time, for example, significantly reduces the hazard potential of the handled substance and improves safety by eliminating the risk of poisoning in case of accidental spillage.

Reducing the variation of returns by segmenting and diversifying an investment portfolio into any non-correlated stocks is a well-documented technique for reducing financial risk by segmentation. With increasing the segmentation, the variance (volatility) of the portfolio is reduced (Teall and Hasan, 2002). Segmentation works also very well in reducing the risk from opportunity risk-reward bets: bets whose expected profit is a positive value. Segmenting an opportunity bet into several bets with the same probability of success and failure but with a smaller amount of risked quantity, significantly reduces the probability of a net loss (Todinov, 2013).

Segmentation is a universal domain-independent concept for risk reduction and applied with domain-specific knowledge can, for example, used to reduce the risk of computational errors.

Consider the domain-specific chain rule for differentiation of a function of a function, which is a well-known concept from calculus (Ellis and Gulick, 1991).

Suppose that a process is a complex continuous function $y = y(x)$ of the input parameter x. Finding the derivative $\frac{dy}{dx}$ which describes the process rate is often very difficult because of the complex function $y = y(x)$. The direct differentiation, if at all practicable, often leads to enormous, very complex expressions, during whose derivation the likelihood of errors is very high. These difficulties disappear if the method of segmentation through the chain rule is applied. The complex continuous function $y = y(x)$ is segmented into several simpler functions. Suppose that y is

expressed as a continuous and differentiable function $y(u_1)$ of the parameter u_1; the parameter u_1 is expressed as a continuous and differentiable function $u_1(u_2)$ of the parameter u_2 and so on, until a parameter u_n is reached, which is expressed as a continuous and differentiable function $u_n(x)$ of *x*. As a result, $y = y(x)$ is effectively segmented into a nested composition of *n* continuous and differentiable functions:

$$y = y(u_1(u_2(u_3(...u_n(x))))) \tag{1}$$

Applying the chain rule for the derivative dy/dx, of the expression (1):

$$\frac{dy}{dx} = \frac{dy}{du_1} \times \frac{du_1}{du_2} \times \frac{du_2}{du_3} \times ... \times \frac{du_n}{dx} \tag{2}$$

is obtained. Expression (2) is effectively a segmentation of the complex derivative dy/dx into derivatives dy/du_1, du_1/du_2, du_n/dx whose evaluation is relatively easy. Reducing the risk of errors comes from the circumstance that the evaluation of each of the separate derivatives $\frac{du_i}{du_{i+1}}$ is associated with a significantly smaller likelihood of errors than the evaluation of the original derivative $\frac{dy}{dx}$. The complex task related to determining the rate $\frac{dy}{dx}$ has effectively been reduced to a number of sub-tasks with easy solutions. The solution of the original problem is assembled simply by multiplying the solutions of the partial problems, which is a straightforward operation, not normally associated with high possibility of error.

The method of chain-rule segmentation remains the same if any of the parameters depends not on a single parameter but on two or more parameters. In this case, partial derivatives are used.

As a result, the domain-specific knowledge of the chain rule in calculus and the domain-independent method of segmentation through the chain rule are combined to achieve a substantial decrease in the risk of computational errors.

Consider now an application from structural engineering. It is not at all obvious that segmenting loading forces could achieve a significant reduction of the internal stresses in a loaded structure. One of the mechanisms by which segmentation achieves such a reduction is that segmenting loading forces reduces the magnitudes of the bending moments and reducing the magnitudes of bending moments reduces the magnitudes of the internal stresses.

Consider the simply supported beam with length *l* and uniform cross section in Figure 1, loaded with a concentrated force *P*.

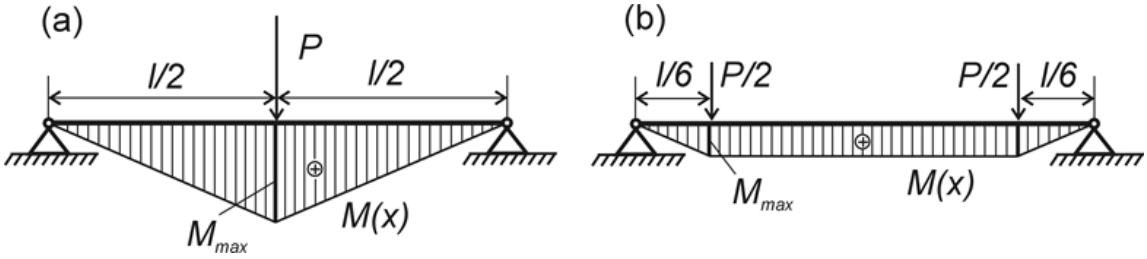

Figure 1. Reducing the risk of overstress failure of a beam by segmenting the external concentrated load *P*.

Segmenting the concentrated load *P* into two concentrated loads with magnitudes *P/2*, applied at distances *l*/6 from the supports, reduces the maximum bending moment which, in turn, reduces the internal tensile stresses from bending. Reducing the magnitudes of the internal tensile stresses increases the resistance to overstress failure and therefore reduces the risk of overstress failure. A similar reliability improvement effect is also present if external concentrated moments, instead of concentrated forces are segmented.

As a result, the domain-specific knowledge in strength of materials combined with the domain-independent method of segmentation delivered a substantial decrease in the risk of overstress failure.

Strength of components is a mature and well-developed field (Hearn 1985; Budynas, 1999; Gere and Timoshenko, 1999; Shigley and Mischke, 1989; Thompson 1999; French 1999; Collins 2003; Hibbeler, 2004; Norton, 2006). Despite this, to the best of our knowledge, the ideas of segmenting external loads in order to reduce the risk of overstress failure have not been used. This rather surprising omission in mature domains shows that effective risk reduction cannot be achieved solely by knowledge from a specific domain without enhancing it with knowledge of domain-independent methods.

3.2 Method of separation

Underlying idea: *eliminating failure modes by separating functions, properties and risk-critical factors*.

Implementation: To apply the method of separation, different functions are assigned to different parts, instead of having a single part carrying all the functions. This permits the

separate parts to be optimised for carrying their function in the most efficient way, avoids overloading of the parts and improves their resistance to overstress failure. Different properties can also be assigned to different components or different parts of the same component, in proportion of the loads experienced during service. Separation of the properties is necessary in cases where the average property characterising a homogeneous state cannot provide the necessary resistance against the risk factors. Design engineers often select materials with uniform properties despite that the loading and the stresses in the components are clearly non-uniform. Homogeneous materials, with average value of the strength (resistance), are not optimised according to the local type of loading and cannot provide sufficient resistance in all zones where high resistance is needed.

Separation of risk-critical factors is implemented to prevent a dangerous simultaneous occurrence of risk-critical actions at a given point in time or at a given space location. Logical separation of risk-critical factors is implemented to make it logically impossible for two or more objects/events to be in a dangerous proximity or two or more incompatible actions to occur simultaneously.

Logical separation avoiding dangerous simultaneous occurrence of actions can be implemented relatively easily by using the mechanism of the shared unique key. The same unique key is required for activating each action in accomplishing a particular task. As a result, dangerous overlapping of actions cannot occur because the unique key cannot be simultaneously available to activate more than one action.

Risk is sometimes the result of the simultaneous presence of risk-critical factors. Such are for example the random demands for a particular life-saving equipment from patients in a critical condition.

Risk then depends on the time separation of risk-critical random demands. The underlying idea of stochastic separation is *to reduce risk by making overlapping of risk-critical demands less likely*. This must be achieved by making a careful balance between health risk and cost of life-saving equipment and other resources. The method of stochastic separation requires determining the expected time fraction of overlapping of a particular order, for risk-critical random events on a time interval. This can be done by using the analytical methods presented in (Todinov, 2017).

Application examples

Separation of functions, found in software development (also known as 'separation of concerns') is a well-known concept in the design of computer programs (Reade 1989). To avoid costly bugs, the function related to developing the code is separated from the function related to testing the software. The method of division of tasks featured in Pahl et al. (2007) is effectively an application of the method of separation in mechanical design.

Separation of functions in handling financial transactions (e.g. authorising the transaction, receiving the funds, depositing the funds, recording the transaction, reconciling the bank statement) reduces the possibility of fraud. By separating the functions, no single individual has the ability to both perpetrate and conceal fraud because this would require collusion between several people.

Separation of properties is often applied to reduce the risk of failure. Stronger alloys are used in places where the stresses are high. Simultaneously, weight is reduced by using plastics in the parts where the stresses are low.

Logical separation of risk-critical factors is present, for example, in the case where both hands of an operator are required to activate the blade of a metal cutting guillotine. This prevents the dangerous failure mode "operator's hand residing in the cutting area while the cutting blade is being activated".

Separation distancing triggers from hazards and hazards from targets reduces the likelihood and the consequences of an accident and is the essence of the concept 'barrier' (Svenson 1991; Eder and Hosnedl 2008; Hollangel 2016).)

Separation of methods reduces the risk of incorrect computational results. Thus, a computer programme based on Monte Carlo simulation and hand calculations based on probability theory can both be used to obtain a particular result. Obtaining the same result from the two distinct methods provides a very strong confirmation of the validity of both, the theoretical model and the simulation programme.

An example of stochastic separation is given next. Consider, for example, n patients placing with probability γ a demand of duration d for a particular life-saving equipment. The demand is randomly located over a time interval of length L. It has been shown (Todinov, 2017) that the expected time fraction of overlapping of random demands (simultaneous random demands) of order k = 0, 1, 2,...,n is given by the binomial expansion of the expression $[(1-\gamma\psi)+\gamma\psi]^n$, where $\psi = d/L$. The quantities $a = 1-\gamma\psi$ and

$b = \gamma\psi$ are treated as separate variables. Thus, the expected time fraction of no random demands is given by $f(0) = (1-\gamma\psi)^n$; the expected time fraction of exactly one random demand is given by $f(1) = n(1-\gamma\psi)^{n-1}(\gamma\psi)^1$; the expected time fraction of two simultaneous random demands is given by $f(2) = [n(n-1)/2] \times (1-\gamma\psi)^{n-2}(\gamma\psi)^2$ and so on. Clearly, $f(0) + f(1) + ... + f(n) = [(1-\gamma\psi) + \gamma\psi]^n = 1$.

Suppose that there are *m* pieces of life-saving equipment servicing the random demands and each piece of equipment can service no more than a single random demand. If an overlapping of random demands of order $k > m$ occurs, there will be unsatisfied random demand (with grave consequences).

The expected time fraction of overlapping of random demands of order greater than k = 0, 1, 2,...,*n*-1 is obtained from the equation:

$$1 - [(1-\gamma\psi) + \gamma\psi]^n = 0 \tag{7}$$

which is equivalent to 0 = 0.

This is a "mathematically structured zero" that packs a significant amount of information. It measures the expected fraction of unsatisfied demand for any number *m* $0 \le m \le n-1$ of sources servicing the random demands. Stochastic separation can be done by reducing the probability γ with which the random demands are initiated, by reducing the number of random demands *n* and by increasing the number of units *m* servicing the random demands (Todinov, 2017). The optimal number of units *m* servicing the random demands can be determined, which provides the optimal balance between acceptable risk level and cost.

4. Improving reliability and reducing risk by inversion and self-reinforcement

4.1 Method of inversion

Underlying idea: *to avoid failure modes by inverting relative position, orientation, functions, motion, features, properties, thinking or by introducing inverse states*.

Implementation

Inverting the relative location of features, state, motion and properties usually preserves the required function but often, the inverted state is characterised by fewer failure modes compared to the original state.

Thus, introducing inverse stress states (compressive stresses) creates a counterbalance against tensile loading stresses and increases the resistance against overloading. Inverse thinking, by changing the focus from how to improve the reliability of an entity to how to make the entity fail, provides a different perspective and helps identify difficult to discover failure modes.

Application examples:

An example related to *improving reliability by inverting the relative position* can be given with the cover on a container under pressure. Inverting the position of the cover from outside the container to inside, improves significantly the reliability of the seal and reduces the loading stresses on the screws fixing the cover. In addition, the reliability improvement is done at no extra cost.

Often, inverting the direction of motion eliminates failure modes and results in improved reliability. This idea underlies the Cosworth® sand casting process (Campbel 2015) where the molten metal is not poured down the sand mold as is the case in the classical sand casting process. In the Cosworth® sand casting process, the molten metal flows uphill into the mold, which avoids turbulence and trapping sand particles into the metal. This type of inversion of motion increases significantly the fatigue strength of the cast component.

An example related to eliminating failure modes by *inverting a function* can be given with the fail-safe air breaks of trucks. Instead of air pressure energizing the breaks when these are needed, the function is inverted. The air pressure keeps the brakes released which permits the truck to move. In case of a low pressure in the air line due to a puncture or failure of the compressor, the brakes are applied securing the truck. In this way, a dangerous failure mode is avoided: loss of air pressure and inability to apply breaks when these are needed. Inverse states in the form of compressive residual stresses introduced to increase the fatigue life of aircraft structures have been recently reviewed in Fu et al (2015).

An example related to *risk reduction achieved by inverse thinking* can be given with improving the defense against unauthorized access to a valuable service provided by a computer program (e.g. computer program controlling the access to a bank account). An important path to improving the defense against unauthorised access is to invert the problem from "how to improve the security of the computer programme" to „how to compromise the computer program controlling the access and make it fail“. Invariably,

the inversion of thinking reveals software vulnerabilities which could be exploited to gain unauthorized access.

The subversion analysis technique and the anticipatory failure determination approach described in Kaplan et al. (1999) are largely an application of the method of inverse thinking. The focus of these approaches is on how to invent failures by using the available resources and these techniques are useful for identifying rare and unexpected failure modes.

4.2 Reliability improvement and risk reduction through self-reinforcement

Underlying idea: *to improve reliability by creating a design where increasing the external/internal forces intensifies the system's response against these forces. As a result, the driving net force towards precipitating failure is reduced.*

Implementation

There are several ways of implementing self-reinforcement: *self-reinforcement by capturing a proportional compensating factor*, *self-reinforcement by self-balancing* and *self-reinforcement by feedback loops*.

Self-reinforcement can be implemented by identifying and capturing the effect from a particular factor to diminish the negative effect created by an external force or the deviation of the system's response from a specified value. Thus, the negative effect from increased weight can be captured to provide extra stability and increased resistance to overturning. The negative effect from increased wind pressure on a panel can be captured to induce rotation of the panel and self-alignment, which reduces the negative effect of the excessive wind pressure. An important feature of self-reinforcement that distinguishes it from mere „reinforcement" is that increasing the magnitude of the external/internal forces always increases the resistance against these forces.

Self-reinforcement by self-balancing can be implemented by identifying and capturing effects that compensate particular negative effects. Increasing the magnitude of the negative effect increases the self-balancing response.

Self-reinforcement by negative feedback loops is based on stabilising the system or process. Self-reinforcement by positive feedback loops is based on discovering and eliminating positive feedback loops with negative impact or creating positive feedback loops with positive impact. Positive feedback loops with positive impact, for example, can be used for self-locking, self-energising or for a quick departure from unwanted equilibrium states.

Application examples

Self-locking devices, such as self-locking screws, grips, hooks and self-energizing breaks are effectively applications of the method of self-reinforcement. Costache at al (2016) for example, recently introduced self-locking grips for anchoring fiber-reinforced tendons.

An example of *self-reinforcement by capturing a proportional factor* can be given with the crowd fence in Figure 2a. The crowd fence without a self-reinforcement in Figure 2a can be overturned relatively easily by the forces created by people pushing the fence. If the lower end of the fence on the crowd side is made wider, people will have to stand on the fence while they push against it (Figure 2b). The more people push on the fence, the more weight forces will be available for counteracting the overturning moment. Reliability has been improved at a relatively small extra cost.

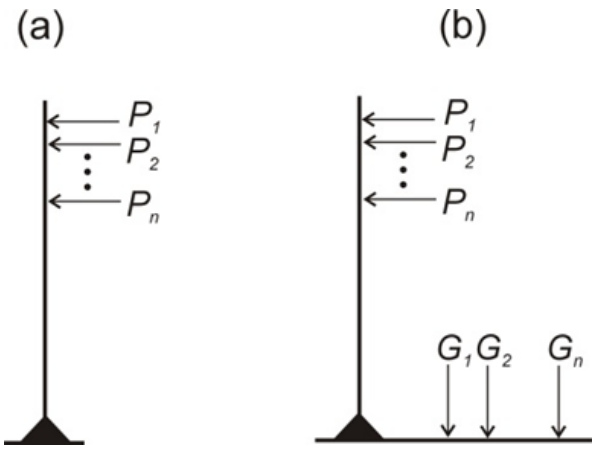

Figure 2. Reducing the risk of overturning of a crowd fence by self-reinforcement.

An example of *self-reinforcement by self-balancing* can be given with twisting wires to cancel their magnetic interference. The flow of current through the wire results in an electromagnetic field around the wire which could generate noise in the neighbouring wires. Twisted wires carry equal and opposite currents whose electromagnetic fields cancel. Increasing the current, increases proportionally the self-balancing response.

Self-reinforcement by self-balancing can be seen in the symmetrical design used to minimise the axial forces in turbine shafts (Matthews 1998).

Positive feedback loop with a negative impact can for example be triggered by the withdrawal of investment from a country, triggered by a political crisis. This leads to poverty which in turn leads to a further withdrawal of investment.

Positive feedback loop with negative impact can also be seen in human behaviour, created by the factors belief and choice. For example, belief in an incorrect model (Todinov, 2010) determines its choice to the extent of ignoring experimental evidence clearly contradicting the model. The belief leads to choosing the incorrect model by more researchers, which leads to strengthening the belief in the wrong model. This leads to a firmly entrenched false modelling paradigm. The positive feedback loop can only be broken by a strong experimental evidence, theoretical argument or simulations exposing the wrong model. The theory of ether in physics in the late 1800s is such a notable example. This theory that ether is the medium which light propagates through was widely believed and universally accepted until the famous Michelson-Morley experiment (Michelson and Morley, 1887) disproved the theory.

5. Improving reliability by permutations and by substitution

5.1 The method of permutations

Underlying idea: *to improve reliability of a system by interchanging components with the same type but with different reliability.*

Implementation and justification

The method of permutations will be demonstrated on parallel-series arrangements which are very common (for example, the system in Figure 3). Indeed, almost any safety-critical system based on detectors working in parallel (detecting increased pressure, increased temperature, toxic gas release, etc.), is a parallel-series system. The system detects the critical event if at least one of the detectors working in parallel detects the critical event. The parts composing each detector are normally logically arranged in series (a detector fails if any of its parts fails).

A *well-ordered* parallel–series arrangement, is obtained if the available components are used first to build the branch with the highest possible reliability; next, the remaining components are used to build the branch with the second-highest reliability, and so on, until the entire parallel–series arrangement is built. The well-ordered arrangement is

characterised by the largest possible system reliability the proof of which can be found in (Todinov, 2014).

Application

Suppose that there are three types of components with different age (new, medium-age, and old), and the reliability of a new component is greater than the reliability of a medium-age components while the reliability of a medium-age components is greater than the reliability of an old component.

According to the statement proved earlier, the minimum risk of failure is achieved if all new components are arranged in a single branch, the medium-age components in another branch, and all old components are grouped in a separate branch (Figure 3). Components of similar level of deterioration (reliability levels) should be placed in the same parallel branch.

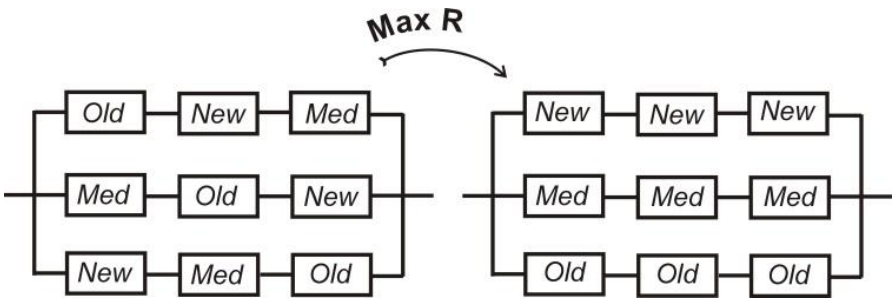

Figure 3. Minimising the risk of failure of a parallel–series system by permutation of interchangeable components.

Unlike traditional approaches, a risk reduction by permutation of components with equivalent functions can be achieved at no extra cost.

The principle of the well-ordered systems provides an opportunity to remove the maximum amount of system risk by concentrating the available budget on monitoring or renewing single parallel branches as opposed to randomly monitoring or replacing aged components in the system.

This result also provides the valuable opportunity to improve the reliability of common systems with parallel-series logical arrangement of their components *without the knowledge of their reliabilities and without extra investment*. Unlike all traditional approaches, which invariably require resources to achieve reliability improvement and risk reduction, a system risk reduction can also be achieved by appropriate permutation of the available interchangeable components in the parallel branches.

The risk reduction principle based on permutation of interchangeable components has wide applications reaching far beyond its initial engineering context. The principle of well-ordered systems also works in project management. Consider an example of three groups of people (teams 1,2, and 3), each of which includes three independently working team members (Fig.4).

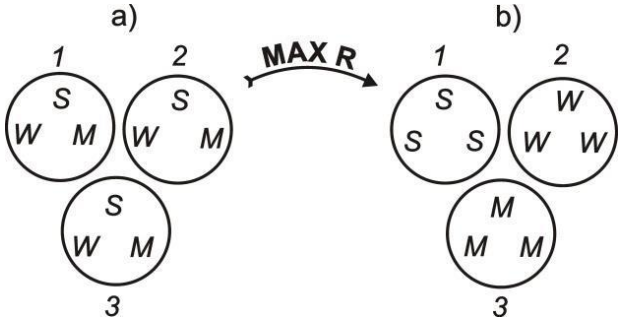

Figure 4. Three groups of people working towards achieving the same goal.

The teams work in parallel towards achieving the same goal. The goal is achieved if at least one of the teams succeeds in achieving the goal. Within each team, the task of achieving the goal is divided into sub-tasks among the team members. Each person in a team must accomplish their sub-task successfully in order for the team to achieve the goal. Suppose that the level of training of each team member is from one of the following categories: S (strong), W (weak), and M (medium). A person with a strong level of training has a better chance of accomplishing a sub-task successfully compared with a person with medium training and a person with medium training has a better chance of accomplishing the sub-task successfully compared with a person with weak training. Separating the people in groups with a similar level of training ([S,S,S]; [M,M,M] and [W,W,W]), similar to the different age components in (Figure 3) yields the highest chance of achieving the goal.

The risk reduction by permutation of components with equivalent functions is achieved at no extra cost.

5.2 Improving reliability and reducing risk by substitution

Underlying idea: *to eliminate dangerous failure modes by a substitution with assemblies/systems delivering the same required functions but working on a different physical principle.*

Implementation

A central point in the implementation is to identify whether the substitution of one type of assembly (e.g. mechanical assembly) with an assembly performing the same function but working on a different physical principle (e.g. electrical, optical, magnetic assembly, software) will eliminate particular failure modes or reduce the rate of damage accumulation. Thus, substituting a mechanical assembly with magnetic assembly often results in reliability improvement because, unlike the mechanical assembly, the magnetic assembly practically does not undergo wear. Eliminating the need for lubrication for the magnetic assembly, simplifies the system and eliminates the failure modes of the lubrication system. Substitution of a mechanical (electro-mechanical) assembly with an optical assemblies avoids the need for a direct contact, which decreases wear, increases precision, increases and makes the operation possible in hazardous surface conditions (high voltage, high temperature, etc.).

Substituting a mechanical (electro-mechanical) assembly with an optical assembly avoids the need for a direct contact, which decreases wear, increases precision, increases and makes the operation possible in hazardous surface conditions (high voltage, high temperature, etc.).

Substituting mechanical (electro-mechanical) systems with software systems eliminate deterioration and variability which are major contributing factors to unreliability. The substitution with software components also introduces sensing capabilities which make the system capable to adapt to changing environment.

Application examples:

An example of a substitution of a mechanical assembly with an electrical assembly with the same function is the mechanical push button switch. The mechanical contact promotes (i) mechanical deterioration caused by fatigue and wear; (ii) contact erosion caused by arcing and (iii) collection of dirt and corrosion products which prevent a good contact. Substituting the mechanical push button switch with a switch whose operation is based on the Hall effect (Ramsden, 2006), reduces dramatically the rate of damage accumulation and increases the durability of the switch from tens of thousands to tens of millions of actuations.

Replacing a mechanical measuring system with magnetic or optical measuring system often eliminates the need for calibration which is necessary for conducting an accurate measurement.

An example of replacing a mechanical assembly with a magnetic assembly is provided by the magnetic worm drive (featured in the US patent US3814962; Baermann 1971) whose worm gear is made of permanent magnet material. The teeth of the worm gear and the worm wheel are also magnetised so that the like poles on the wheel and on the worm gear face one another. Magnetic repulsion transmits force from the rotating worm gear to the worm wheel which causes the rotation of the worm wheel.

The advantage of the magnetic worm drive compared with the conventional mechanical worm drive is the frictionless transfer of torque which eliminates contact stresses and wear. The need for lubrication is also eliminated, together with its failure modes. Furthermore, the clearance between the teeth of the worm gear and the worm wheel eliminates failure modes caused by misalignment which enhances the life of the bearings. The clearance also eliminates the spread of vibrations through the worm wheel which reduces wear and further enhances the reliability of the assembly.

An example of improving reliability by eliminating mechanical contact could be given with the replacement of the contact measurement of the temperature of metal surfaces with optical (contactless) measurement by using infrared thermometers (pyrometers) (Childs, 2001).

The presented domain-independent methods work across totally unrelated domains and this is demonstrated by the supplied examples which range from various areas of engineering and technology, computer science, project management, health risk management, business and even mathematics.

Conclusions

• Risk reduction is underlined by domain-independent methods and principles which combined with knowledge from the specific domain help to generate effective risk reduction solutions.

• The domain-specific approach to risk reduction created the illusion that efficient risk reduction can be delivered successfully solely by using methods offered by the specific domain. As a consequence, many industries have been deprived from efficient risk reducing strategy and solutions which resulted in inferior products and processes, associated with high risk of failure.

• The paper introduces a powerful method for reducing the likelihood of computational errors based on combining the domain-independent method of segmentation and local knowledge of the chain rule for differentiation. The method can

be used for reducing the likelihood of computational errors in determining the rate of change of output parameters part of complex processes.

• The paper demonstrated that lack of domain-independent knowledge even in such mature field like stress analysis, misses opportunities to reduce the risk of failure.

• The domain-independent methods for risk reduction 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.

• Unlike some traditional reliability improvement methods like: 'introducing redundancy', 'selecting high-quality materials', 'strengthening weak links' and 'condition monitoring', the discussed domain-independent methods improve reliability at no extra cost or at a relatively small cost.

• 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 because of cost limitations. 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.

• The presented domain-independent methods work across totally unrelated domains and this is demonstrated by the supplied examples which range from various areas of engineering and technology, computer science, project management, health risk management, business and even mathematics.

Acknowledgement

The author thanks the anonymous reviewers whose suggestions helped to improve the quality of the manuscript

REFERENCES

Altshuller G.S., 1984. *Creativity as an exact science: The theory of the solution of inventive problems*, Gordon and Breach Science Publishing, New York.

Altshuller G.S., 1996. *And suddenly the inventor appeared, TRIZ, the theory of inventive problem solving*, Translation from Russian by Lev Shulyak, Technical Innovation Center, Worcester, MA.

Altshuller G.S., 1999. *The innovation algorithm, TRIZ, systematic innovation and technical creativity*, Technical Innovation Center, Inc., Worcester.

Ang A.H.S. and W.H. Tang, 1975. *Probability concepts in engineering planning and design, vol. 1, Basic principles*, John Wiley & Sons, Inc., New York.

Andrews J.D. and T.R. Moss, 2002. *Reliability and risk assessment*, Professional Engineering Publishing, London.

AvenT., 2003. *Foundations of RiskAnalysis:A Knowledge and Decision-Oriented Perspective*, John Wiley & Sons.

Aven T.,2016. "Risk assessment and risk management: review of recent advances on their foundation", *European Journal of Operational Research*, 253: 1-13.

Baermann, M., 1971. Magnetic worm drive. US Patent 3,814,962.

Barlow R.E. and F., Proschan, 1965. *Mathematical theory of reliability*, John Wiley & Sons, Inc., New York.

Barlow R.E. and F. Proschan, 1975. *Statistical theory of reliability and life testing*, Rinehart and Winston, Inc., New York.

Bazovsky I., 1961. *Reliability theory and practice*, Prentice-Hall, Inc., Englewood Cliffs.

Beasley M., 1991. *Reliability for engineers: An introduction*, Macmillan Education Ltd, London.

Bedford T. and R. Cooke, 2001. *Probabilistic risk analysis, foundations and methods*, Cambridge University Press, Cambridge.

Billinton R. and R.N. Allan, 1992. *Reliability evaluation of engineering systems*, 2nd ed., Plenum Press, New York.

Booker J.D., M. Raines and K.G. Swift, 2001. *Designing capable and reliable products*, Butterworth-Heinemann, Oxford.

Budynas R.G., 1999. Advanced strength and applied stress analysis, 2nd ed., McGraw-Hill, New York.

Campbel, J. 2015. *Complete Casting Handbook, Metal Casting Processes, Metallurgy, Techniques and Design*, 2e. Amsterdam: Butterwoth-Heinemann.

Childs, P.R.N. (2001). *Practical temperature measurement*. Oxford: Butterworth-Heinemann.

Costache, A., Glejbol, K., Sivebak, I.M., and Berggreen, C., 2016. Improved friction joint with self-locking grips. *Journal of Offshore Mechanics and Arctic Engineering* 138 (5): 051401.

Cullen The Hon Lord., 1990. The public enquiry into the Piper Alpha disaster. London: HMSO.

Collins J.A., 2003. *Mechanical design of machine elements and machines*, John Wiley & Sons, Inc., New York.

Dhillon B.S. and C. Singh, 1981. *Engineering reliability: New techniques and applications*, John Wiley & Sons, Inc., New York.

Ebeling C.E., 1997. *An introduction to reliability and maintainability engineering*, McGraw-Hill, New York.

Eder, W.E. and Hosnedl, S. 2008. *Design Engineering*. Boca Raton, FL: CRC Press.

French M., 1999. *Conceptual design for engineers*, 3rd ed., Springer-Verlag London Ltd, London.

Fu, Y., Ge, E., Su, H. et al. 2015. "Cold expansion technology of connection holes in aircraft structures: a review and prospect". *Chinese Journal of Aeronautics* 28 (4): 961–973.

Gadd K, 2011. *Triz for engineers: Enabling inventive problem solving*, Wiley.

Goldstein B.D., 2011. "Risk Assessment of Environmental Chemicals: If It Ain‟t Broke...", *Risk Analysis*, 3(9): 1356-1362.

Hearn E.J., 1985. *Mechanics of materials*, Volume 1 and 2, 2nd edition, Butterworth.

Hibbeler R.C. 2004., *Statics and mechanics of materials*, SI edition, Prentice Hall.

HSE., 1992. The tolerability of risk from nuclear power stations. London: Health and Safety Executive.

Hollangel, E. 2016. *Barriers and Accident Prevention*. Abingdon: Routlege.

Kaplan, S., Visnepolschi, S., Zlotin, B., and Zusman, A. 1999. *New Tools for Failure and Risk Analysis: Anticipatory Failure Determination*. Detroit: Ideation International Inc.

Matthews, C., 1998. *Case Studies in Engineering Design*. Arnold.

Meeker W.Q. and L.A. Escobar, 1998. *Statistical methods for reliability data*, John Wiley & Sons, Inc., New York.

Melchers R.E., 2001. "On the ALARP approach to risk management", *Reliability Engineering and system safety*, 71(2): 201-208.

Michelson, A.A. Morley E.W., 1887. On the Relative Motion of the Earth and the Luminiferous Ether. *American Journal of Science*. **34** (203): 333–345.

Norton R.L., Machine design, An integrated approach, 3rd ed., Pearson International edition, 2006.

Orloff, M., 2006. *Inventive thinking through TRIZ* (2nd ed.). Springer.

Orloff M.A., 2012. *Modern TRIZ A Practical Course with EASyTRIZ Technology, A practical guide*, 2nd ed., Springer.

Pahl G., W. Beitz, J. Feldhusen and K.H. Grote, *Engineering design*, Springer, Berlin (2007).

Phadke, M.S. 1989. *Quality Engineering Using Robust Design*, Englewood Cliffs, NJ: Prentice-Hall.

Pecht M., A.Dasgupta, D.Barker, C.T.Leonard. 1990. The reliability physics approach to failure prediction modelling, *Quality and Reliability Engineering International*, September/October (4): 267-273.

Pecht M. 1996. "Why The Traditional Reliability Prediction Models Do Not Work - Is There An Alternative" *Electronic Cooling* **2**(1): 10-12.

Petroski H., 1994. *Design Paradigms: Case Histories of Error and Judgment in Engineering*, Cambridge University Press, Cambridge.

Rantanen K., Domb E., 2008 *Simplified TRIZ, 2nd edition*, Auerbach Publications.

Ramakumar R., 1993. *Engineering reliability, fundamentals and applications*, Prentice Hall, Englewood Cliffs.

Ramsden E. 2006. *Hall-effect sensors: theory and applications* 2nd ed. Elsevier.

Savransky S.D., 2000. *Introduction to TRIZ methodology of inventive problem solving*, CRC press LLC.

Shigley J.E., C.R.Mischke, 1989. *Mechanical engineering design*, 5th ed., McGraw-Hill International editions.

Svenson, O., 1991. "The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries" *Risk Analysis* 11 (3): 499–507.

Teall, J.L. and Hasan, I., 2002. *Quantitative Methods for Finance and Investment*. Blackwell
Publishing.

Terninko J., A.Zusman, B.Zlotin 1998. *Systematic Innovation: An introduction to TRIZ*, CRC Press LLC.

Thompson G., 1999. *Improving maintainability and reliability through design*, Professional Engineering Publishing Ltd, London.

Todinov M.T., 2013. "New models for optimal reduction of technical risks", *Engineering Optimization*, 45 (6): 719–743.

Todinov M.T., 2017. "Reliability and risk controlled by the simultaneous presence of random events on a time interval" *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, 021003, Mechanical Engineering*, published online, *Part B: 4(2):* doi: 10.1115/1.4037519.

Todinov, M.T., 2014. "Optimal allocation of limited resources among discrete risk-reduction options", *Artificial Intelligence Research*, 3 (4): 15-27.

Trivedi K.S., 2002. *Probability and statistics with reliability, queuing and computer science applications*, 2nd ed., John Wiley & Sons, Ltd, Chichester.

Vose D., 2000. *Risk analysis, a quantitative guide*, 2nd ed., John Wiley & Sons Ltd., New York.