REDUCING THE RISK OF FAILURE BY DELIBERATE WEAKNESSES

Michael Todinov

Oxford Brookes University

School of Engineering, Computing and Mathematics

Oxford, Wheatley, OX33 1HX, UK

mtodinov@brookes.ac.uk

ABSTRACT

The deliberate weaknesses are points of weakness towards which a potential failure is channelled in order to limit the magnitude of the consequences from failure. The paper shows that reducing risk by deliberate weaknesses is a powerful domain-independent method which transcends mechanical engineering and works in various unrelated areas of human activity. A classification has been proposed of categories and classes of deliberate weaknesses reducing risk as well as discussion related to the underlying mechanisms of risk reduction. It is shown that introducing and repositioning existing weaknesses is an effective risk-reduction strategy which transcends engineering and can be applied in many unrelated domains. The paper shows that in the case where the cost of failure of the separate components in a system varies significantly, an approach based on deliberate weaknesses has a significant advantage to the equal-reliability/equal-strength design approach.

1. INTRODUCTION

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, measures specific to the particular domain are selected and the risk reduction is conducted exclusively by experts in the domain. This contributed to the false perception that efficient risk reduction can only be delivered successfully by using methods offered by the specific domain, without resorting to general methods for risk reduction. This common approach resulted in ineffective reliability improvement and risk reduction in all areas of the human activity. Valuable opportunities for improving reliability and reducing risk have been overlooked which led to serious accidents resulting in big financial losses, fatalities and damage to the environment. The most effective results in risk reduction are obtained when domain-independent risk reduction methods are combined with domain-specific knowledge. The great advantage of the domain-independent thinking in improving reliability and reducing risk across many unrelated domains of human activity has been recently demonstrated in (Todinov, 2019).

Accordingly, the present paper focuses on an important domain-independent method for risk reduction based on introducing deliberate weaknesses or repositioning existing weaknesses. The deliberate weaknesses are deliberately created weak spots towards which a potential failure is channelled. By channelling failure into weak spots, designed to fail in a predictable way, the consequences from failure are reduced. Should the unfavourable conditions occur, the deliberate weakness is the one to fail and protect the expensive parts of the system. In this way, the losses are limited. Another advantage is that the deliberate weaknesses are maintenance-free and constantly ready to operate.

Risk reduction by introducing weak links and stress limiters has already been used in engineering for preventing the stresses from reaching dangerous levels (Eder and Hosnedl, 2008). Familiar examples of deliberate weaknesses are the electrical fuses and circuit breakers, the crumple zones in road cars, the crash cones in racing cars, the shear pins, the sacrificial anodes and the rupture disks in pressure vessels.

Although the weak links have been used widely in engineering, their discussion in the reliability and risk literature is very limited, restricted around the few very well-known applications mentioned earlier. Although standard reliability textbooks (e.g. Lewis,1996; Ebeling, 1997; O'Connor 2002; Dhillon 2017; Modarres et al, 2017) do allocate substantial space for discussing risk reduction methods such as introducing redundancy, derating, eliminating common cause and condition monitoring, there is a surprising lack of discussion related to reducing risk by introducing deliberate weaknesses.

A common reliability allocation strategy in engineering design is to make all parts with comparable reliability or strength and not to leave deliberate weak links. Such is, for example, the AGREE methods described in (Ebeling, 1997) and the maximum "distance" to the constraints strategy described in (Thomson, 1999). To the best of our knowledge, no existing reliability and risk publication deals with reducing risk by creating deliberate weaknesses or by repositioning existing weaknesses. This constitutes a substantial gap in the existing reliability and risk research.

Next, in the mechanical engineering design literature (Thompson 1999; French 1999; Collins 2003); Pahl et al. 2007; Norton 2006; Childs 2014; Budynas and Nisbett 2015; Mott et al, 2018; Gullo and Dixon, 2018), there is a clear lack of discussion on the use of deliberate weaknesses to reduce risk. Thus, in (Pahl et al, 2001), deliberate weak links have only been mentioned as protective devices in discussing indirect safety. The discussion of deliberate weak links in (Booker at al., 2001) has been reduced to a discussion of the design of shear pins in transmission shafts only.

Despite the existence of numerous applications of deliberate weaknesses in design, the different categories and classes of deliberate weaknesses and the mechanisms through which the deliberate weaknesses from each category reduce risk have not been discussed in the design literature. The engineering design literature is concerned mainly with reducing risk by removing weaknesses not by creating or repositioning weaknesses. This constitutes a significant gap in the existing research.

Nonetheless, the importance of reducing risk by implementing deliberate weaknesses is increasing. The modern tendency towards light-weight designs requires reducing to a minimum the cross sections and the factors of safety of components. As a result, components are fully loaded and utilised which results in working stresses that are close to the critical stresses triggering failure. Compared to the old and heavy designs with large safety factors, the modern lightweight designs have small or non-existent safety factors. As a result, the critical stresses in modern lightweight designs can be exceeded even by a moderate overload. Furthermore, while old design codes are based on static loading, modern design codes are trying to capture the effects of dynamic loading and the effects from sudden application of loads which are associated with a great deal of uncertainty. For example, it is a well-documented fact that the stresses from sudden application of the load are approximately twice the stresses from slow, static load application (Gere and Timoshenko, 1999).

Introducing deliberate weaknesses is an important barrier assuring the protection of valuable entities from damage due to excessive stresses.

Consequently, the presented paper introduces a new method for reducing the consequences of failure based on repositioning of existing weaknesses, proposes a detailed classification of the categories of deliberate weaknesses that can be used for risk reduction and reveals the mechanisms through which the deliberate weaknesses reduce risk. The paper also demonstrates that combining the domain-independent method of deliberate weaknesses with domain-specific knowledge results in effective risk reduction. Finally, the drawbacks of the equal-reliability concept are discussed.

Unlike alternative neutral viewpoints of risk (Giddens, 1999) where risk could also be associated with potential benefits, the risk in the present treatment is understood to be always associated with potential loss. In the treatment presented next, risk is understood as a unity of an adverse event with the potential to cause damage/loss, the likelihood of its occurrence and the magnitude of the consequences given that the event materialises. Failures of equipment, systems, operations and processes are such adverse events. They are inevitably associated with financial losses, damage to health, fatalities and damage to the environment.

2. DELIBERATE REPOSITIONING OF AN EXISTING WEAKNESS TO REDUCE THE CONSEQUENCES OF FAILURE

The essence of this method consists of a deliberate re-positioning of an existing weakness which minimises the consequences of failure. To some extent, this method is related to a method described later which consists of introducing a deliberate weakness which deflects the failure location to a place where the cost of intervention is minimal. The difference is in the circumstance that for the method described in this section no deliberate weakness is created but an existing weakness is repositioned in time or space with the purpose of reducing the consequences from failure. To the best of our knowledge, no such method has been reported or exploited before.

The processes considered in this section consist of a number of operations that can be executed in any order. A process is considered to be successfully completed if all operations composing the process have been completed successfully. Failure of a single operation causes the process to stop. Many processes in unrelated domains are conducted in this manner.

Consider a manufacturing line that has stopped. There is a possibility that the reason for the interruption is a fault but there is also possibility that the interruption has other cause. Suppose that the line consist of several sections characterised by different probabilities that the fault, if it exists, will be present there. The inspection then must start with the section characterised by the largest likelihood of a fault, not with the section which is the easiest to inspect. They may not necessarily be the same section.

This approach can sometimes be rather counter-intuitive. If a long chain of calculations fails to deliver an answer in the expected range of values, the checking for errors invariably starts at the very beginning, with the easiest block of calculations. To reduce the time spent on checking for errors, the checks must start with the section where the likelihood of error is largest. The input data from the previous section can be assumed to have been obtained correctly. If an error is discovered in the section and corrected, this often avoids checking the sections preceding the corrected section.

Suppose that the process is composed of n operations that can be executed in any order. The cost of conducting the ith operation is C_i (which is measured in monetary units or time). Failure of a single operation causes the process to stop. Each operation, except the nth of operation, is characterised by a probability of failure q and the nth operation is characterised by a probability of failure $p >> q$. Consider executing the operations in such an order that the operation associated with highest probability of failure p is the last operation. Loss can then be generated in n mutually exclusive ways: if failure occurs at the first operation, if failure occurs at the second operation and so on.

The expected loss generated by a failure at the ith operation ($1 \leq i \leq n-1$) is given by $(1-q)^{i-1} q \times i \times C_0$. It is a product of the probability $(1-q)^{i-1}$ that failure will not occur at any of the first i-1 operations, the probability q that the ith operation will fail and the loss iC_0 associated with the first i operations (because they all must be repeated). The expected loss generated by a failure at the nth operation is given by $(1-q)^{n-1} p \times n \times C_0$. It is a product of the probability $(1-q)^{n-1}$ that failure will not occur at any of the first n-1 operations, the probability p that the nth operation will fail and the loss nC_0 associated with the n operations (because they all must be repeated).

As a result, the expected loss L_0 associated with executing the process in the described order is

$$L_0 = qC_0 + q(1-q) \times (2C_0) + ... + q(1-q)^{n-2}((n-1)C_0) + p(1-q)^{n-1} nC_0 \tag{1}$$

Now, by a deliberate repositioning in time of the last weak operation, characterised by the highest probability of failure p (p>>q), an early failure of the weak operation will makes it unnecessary to execute the rest of the operations and will reduce significantly the waste of resources on repeating already executed operations.

Consequently, the weakness (the operation characterised by the highest probability of failure) must be repositioned by placing it first in the order of executing the operations. By using reasoning similar to the reasoning used to derive equation (1), the expected loss associated with executing the process starting with the weakest operation is:

$$\begin{aligned} L_1 &= pC_0 + q(1-p)(2C_0) + q(1-p)(1-q)(3C_0) + ... \\ &+ q(1-p)(1-q)^{n-2}((n-1)C_0) + q(1-p)(1-q)^{n-1} nC_0 \end{aligned} \tag{2}$$

To illustrate the effect of the repositioning of the weakness, an illustrative numerical example is considered. Suppose that a component consists of three sections which are made of particular fast setting material. Because of size limitations, the sections are made sequentially and to ensure that the bonding interfaces are of sufficient strength the work on the next section is initiated before the material fully sets in the current section. If any of the sections fails (for example because of a defect) the process must be stopped because once a section sets, it is no longer possible to produce a sound bonding interface with the neighbouring section.

Suppose that the three sections are characterised by a probability of being defective 0.02 and 0.02 and 0.25, correspondingly. For the sake of simplicity suppose that the cost of manufacturing of each section is £200.

In the case of manufacturing the sections without repositioning the weak operation (characterised by a probability of failure 0.25), the expected losses, according to equation (1), are:

$$L_0 = 0.02 \times 200 + 0.02 \times (1 - 0.02) \times (200 + 200) + 0.25 \times (1 - 0.02)^2 \times (200 + 200 + 200) = 156$$

If the weakest operation is repositioned to be first, the expected loss, according to equation (2) is:

$$\begin{aligned} L_1 = 0.25 \times 200 + 0.02 \times (1 - 0.25) \times (200 + 200) + \\ 0.02 \times (1 - 0.25)(1 - 0.02) \times (200 + 200 + 200) = 64.8 \end{aligned}$$

These results have been confirmed by Monte-Carlo simulations involving ten million trials. The simulation algorithm is straightforward and details regarding its implementation have been omitted. The Monte Carlo simulation results are identical to the calculated values from the theoretical dependencies (1) and (2).

For sections characterised by different likelihood of being defective, to reduce the consequences of failure, the process must start with the manufacturing the section which is characterised by the highest likelihood of being defective. Next follows the section which is characterised by the second highest likelihood of being defective and so on. In this way, the weaknesses are deliberately repositioned in time so that a likely early failure makes it unnecessary to waste resources on manufacturing the rest of the sections.

The lack of knowledge of this method for example, causes inspection for a fault to start with the section where the inspection is easiest which leads unnecessary loss of time.

The proposed method based on repositioning an existing weakness is domain-independent. It can be applied in any domain where the process is characterised by (i) a possibility to change the order of executing the operations and (ii) if any of the operations fails the process must stop.

3. CLASSIFICATION OF TECHNIQUES FOR REDUCING RISK BY CREATING DELIBERATE WEAKNESSES

The techniques for reducing risk by creating deliberate weaknesses can be classified broadly into the following seven categories (Figure 1):

Deliberate weaknesses:

- *protecting from excessive stress*
- *preventing excessive damage*
- *deflecting damage from places where the cost of failure is high*
- *providing a warning*
- *providing a quick access*
- *providing a quick escape*
- *triggering protection systems*

In some of the categories different classes have been identified (Fig.1).

The categories and classes outlined in the classification have been distilled from a large number of engineering solutions, each of which was analyzed to assess for recurring risk reduction patterns. The classification presented in Figure 1 summarizes the current research done by the author on methods for reducing risk by deliberate weaknesses. In what follows, a description of the mechanisms through which the weaknesses from each category reduce risk is provided.

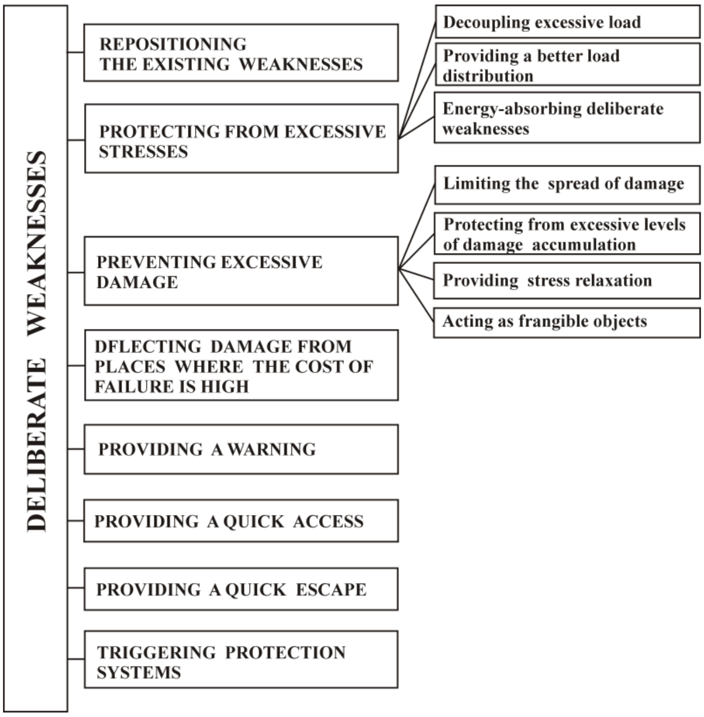
DELIBERATE WEAKNESSES
REPOSITIONING THE EXISTING WEAKNESSES
PROTECTING FROM EXCESSIVE STRESSES
Decoupling excessive load
Providing a better load distribution
Energy-absorbing deliberate weaknesses
PREVENTING EXCESSIVE DAMAGE
Limiting the spread of damage
Protecting from excessive levels of damage accumulation
Providing stress relaxation
Acting as frangible objects
DFLECTING DAMAGE FROM PLACES WHERE THE COST OF FAILURE IS HIGH
PROVIDING A WARNING
PROVIDING A QUICK ACCESS
PROVIDING A QUICK ESCAPE
TRIGGERING PROTECTION SYSTEMS

Figure 1. Classification of deliberate weaknesses used for reducing risk

3.1 Deliberate weaknesses protecting from excessive stresses

3.1.1 Deliberate weaknesses decoupling excessive load

The mechanism behind this class of deliberate weaknesses is preventing excessive load/stress causing damage by decoupling the load from the structure/component.

Thermal fuses, for example, decouple excessive levels of temperature. Electrical fuses and circuit breakers are familiar examples of deliberate weaknesses decoupling excessive currents while surge protection devices decouple excessive voltage. Shear pins and torque wrenches decouple excessive forces and torques while pressure relief valves and rupture disks decouple excessive pressure.

Many stress-limiting devices compete with the decoupling deliberate weaknesses in mitigating the consequences from failure. It needs to be pointed out that a large part of the stress-limiting devices are, in fact, active protection systems. They may include a sensor, a control unit and a device which disconnects the protected part of the system or limits the stress to which it is subjected. This introduces complexity and potential failure modes which decreases the reliability of the active protection system. In some critical cases (associated with high consequences of failure) a deliberate weakness is still needed as a back-up of the active protection system. Such is the case with the active protection system monitoring the pressure increase in a pressure vessel and activating a pressure-release valve if the pressure exceeds a certain critical limit. Despite the active protection system in place, a deliberate weakness such as a rupture disk is still needed as a back-up. Rupture disks have actually become a necessary part of the design codes of pressure vessels.

Unlike the active protection systems, solutions based on deliberate weaknesses are very simple, maintenance-free and characterised by a very high reliability. As a result, the deliberate weaknesses provide additional, more secure layer of protection against failure modes.

It needs to be pointed out that there is a difference between deliberate weaknesses and stress limiters. While many deliberate weaknesses act as stress limiters, not all deliberate weaknesses are stress limiters and not all stress limiters are deliberate weaknesses (Figure 2).

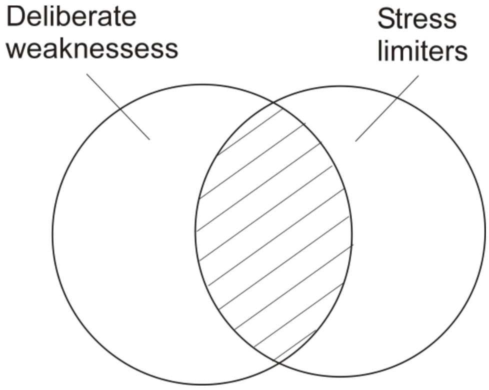

Figure 2. Logic diagram of deliberate weaknesses and stress limiters.

Deliberate weaknesses providing only warning about stress exceeding a dangerous limit, for example, are not necessarily stress limiters. Conversely, the screw with a shoulder (Erhard 2006) designed to prevent over-tightening of plastic materials is a stress limiter without being a deliberate weakness.

3.1.2 Deliberate weaknesses providing better load distribution

The mechanism behind of this class of deliberate weaknesses is the deliberate addition of an extra degree of freedom to ensure that a better balance of forces is obtained. Adding extra degrees of freedom to supports help to redistribute the load so that each support receives an equal portion of the load and overloading of supports is avoided. Introducing an extra degree of freedom helps the alignments of parts and reduces stresses. Common examples are the self-aligning bearings (Figure 3) where the reduction of the contact stresses at the edges (Figure 3a) is achieved by introducing an interface providing extra degrees of freedom (Figure 3b).

This example demonstrates reliability improvement resulting from combining domain-independent knowledge of deliberate weaknesses providing better load distribution and domain-specific knowledge from machine elements.

Statically indeterminate structures also benefit from this type of deliberate weaknesses which help to reduce the internal stresses. Introducing an elastic mounting of parts as opposed to a rigid mounting is also an example of a deliberate weakness which helps the part's alignment, the load redistribution and stress reduction.

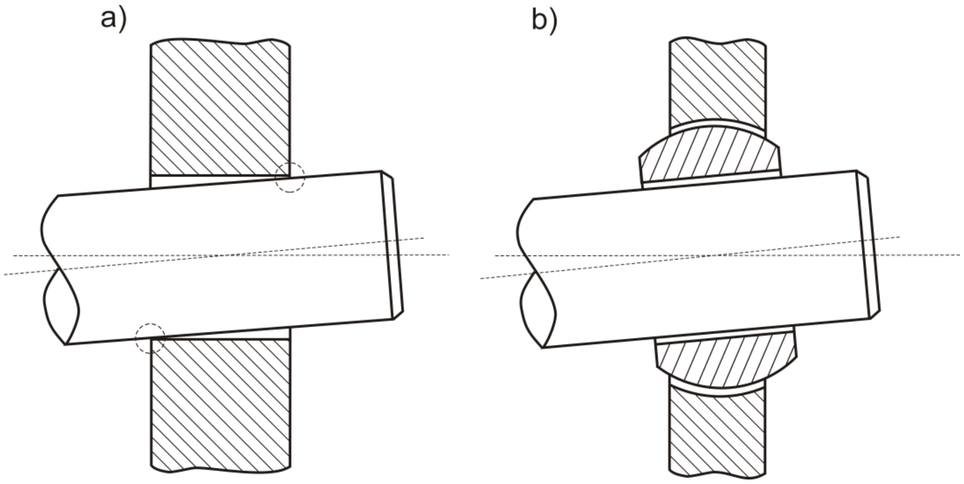

Figure 3. Deliberate weakness adding extra degrees of freedom.

3.1.3 Energy-absorbing deliberate weaknesses

The mechanism behind this this class of deliberate weaknesses is that their failure is associated with a large amount of consumed energy. As a result, the maximum load on the structure is reduced. Crumple zones in road cars and crash cones in racing cars are common examples. In the case of impact, the deliberate weaknesses deform and reduce the impact load on driver and passengers.

Deliberately weakened beams widely used in earthquake engineering have a similar purpose. In the case of earthquake, the weakened beams undergo plastic deformation which consumes a large amount of seismic energy. As a result, the seismic forces on the structure are significantly diminished and the consequences are reduced.

Elements with reduced elastic constants are examples of energy-absorbing deliberate weaknesses. In the case of impact, part of the kinetic energy of the impacting object is converted into elastic strain energy *U*. The elastic strain energy *U* is equal to the work done by the maximum force *P* during the impact:

$$U = \frac{1}{2} P\delta \tag{3}$$

where δ is the maximum displacement (in the elastic region) due to the impact. Reducing the elastic constant is equivalent to increasing the displacement δ which, according to equation (3), leads to a reduced impact force *P*.

The technique of reducing the maximum stress by introducing additional elastic element as a deliberate weakness is a technique that has been used to reduce the maximum stress in a cable subjected to large inertia forces due to sudden stopping.

Suppose that a deliberate weak link has been introduced in the form of an additional component (effectively acting as a spring connected in series, Fig.4b, component 2), whose elastic modulus k_2 is significantly smaller than the elastic modulus k_1 of the cable (1). The equivalent stiffness of the cable and the deliberate weakness (Figure 4b) is given by the well-known relationship (Samuel and Weir, 2004):

$$k_e = \frac{1}{\frac{1}{k_1} + \frac{1}{k_2}} = \frac{k_1 k_2}{k_1 + k_2} = \frac{k_2}{1 + k_2 / k_1} \tag{4}$$

For $k_2 / k_1 << 1$, $k_e \approx k_2$.

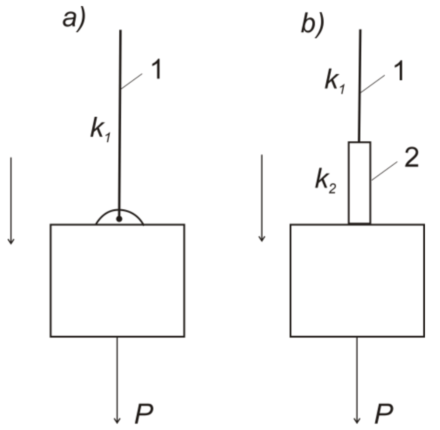

Figure 4. Deliberate weak link reducing stress by increasing the energy-absorbing capacity

The strain energy *U* accumulated by elastic elements with effective constant k_e is given by $U = \frac{P^2}{2k_e}$ (Gere and Timoshenko, 1999) where *P* is the maximum force acting on the component. For prismatic components with length *l*, cross-sectional area *A* and material with Young's modulus *E*, loaded in tension/compression, this equation takes the form: $U = \frac{P^2 l}{2EA}$. Consider a body with mass *m* and velocity v impacting a structure. Suppose that, upon the impact, the fraction γ of the kinetic energy $E_k = \frac{mv^2}{2}$ of the body at the point of impact is transformed entirely into strain energy of the impacted structure. The dynamic force resulting from the impact can then be evaluated by equating *U* and γE_k: $\frac{P^2}{2k_e} = \gamma E_k$, from which the dynamic force *P* can be obtained:

$$P = \sqrt{2k_e \gamma E_k} \tag{5}$$

From the last equation, it is clear that reducing the equivalent elastic constant from k_1 to k_e by introducing an elastic element in series results in a significant decrease of the magnitude of the dynamic force.

This is an example demonstrating how combining domain-independent knowledge of energy-absorbing deliberate weaknesses and domain-specific knowledge from stress analysis yield a significant reduction of the risk of overstress.

Deliberate weaknesses can also be found naturally. Thus, the energy-dissipating properties of the deliberate weaknesses known as "sacrificial bonds" account for the formidable fracture toughness of natural materials. The high toughness of natural materials is due to the reversible, molecular-scale energy-dissipation mechanism provided by sacrificial bonds in the structural molecules (Fantner et al., 2006). These tough natural materials have been mimicked in the fabrication of synthetic polymeric materials where part of the synthesis is the introduction of energy-dissipating sacrificial bonds (Zhou et al, 2017).

3.2 Deliberate weaknesses preventing excessive damage

3.2.1 Deliberate weaknesses limiting the spread of damage

The central ideas behind this class of deliberate weaknesses is (i) to restrict the spread of damage and (ii) to prevent excessive damage accumulation by decoupling the damaged parts of the system from the rest of the system.

An example of this type of deliberate weakness is the sectioning of a pipeline with weak interfaces between the individual sections. As a result, the propagation of a crack appearing in one of the sections is arrested at the weak interface and the crack is confined within a single section only. Consequently, the cost of repair includes the replacement of a single section only. Without restricting the spread of the on a pipeline, a crack appearing in one section could travel along a very large distance of the pipeline (particularly cleavage cracks in steel pipelines at sub-zero temperatures).

Deliberate weaknesses of this type can even increase the load-carrying capacity and fault tolerance of monolithic columns by segmenting them and creating weak interfaces between the individual segments. As a result, damage is confined in small area and its propagation is severely inhibited.

Suppose that a column (loaded in compression) has been segmented into bricks. Suppose that the interfaces between the bricks have been deliberately made weak so that failures of the individual bricks are not linked. Because of the weak interfaces, a crack starting from a critical flaw in any of the bricks cannot spread through the neighbouring bricks thereby causing the collapse of the entire column. A crack appearing in a particular brick causes only failure of that brick.

Connecting modules with deliberately weak links is an important protection technique. In the case of overstress, the weak links fail and the stress is not transmitted to the expensive modules. An example of this type of deliberate weaknesses is a network with hubs connected with deliberate weak links. Suppose that the links are sufficiently strong to provide the necessary connections and sufficiently weak to fail in the case of overstress and protect the rest of the network from damage escalation. Then, the result is damage contained in a small region while the rest of the network is not affected.

Compared to some traditional protection methods which require significant investment such as condition monitoring or strengthening the links in the network, a technique based on deliberate weak links is a low-cost solution constantly ready to operate.

In the current climate of globalised trade and a network of interdependent financial centres, the existence of such protection is essential to limiting the spread of defaults and triggering a financial crisis.

This class of deliberate weaknesses is particularly important for interdependent networks (e.g. communication network and power distribution network) with positive feedback loops, where failure in one of the networks triggers failures in the other network which in turn triggers more failures in the first network. This process commonly results in cascading failures which could bring down the entire interconnected system.

3.2.2 Deliberate weaknesses protecting from excessive levels of damage accumulation

The underlying mechanism for this class of deliberate weaknesses is protection against excessive damage accumulation by making damage accumulate in inexpensive weak links instead of accumulating in the valuable parts of the system.

Familiar examples of deliberate weaknesses from this class are the sacrificial anodes attached to underground pipes, ship hulls, storage tanks etc. By corroding preferentially, they save the metal surface to which they are attached. Sacrificial coatings such like zinc coatings are similar in function and are commonly used for corrosion protection of outdoor structures.

Inserts into spray nozzles is another example. By undergoing wear preferentially, the inserts act as deliberate weaknesses where damage accumulates thereby protecting the expensive spray nozzle from excessive wear. Inserts into journal bearings have a similar purpose. The wear accumulates in the insert and instead of replacing an expensive journal bearing, only the inexpensive insert is replaced.

The wear piece behind the impeller of a sludge pump carries out the function of a sacrificial wear element. The wear piece takes the brunt of heavy wear and protects the expensive pump.

Rubber coatings covering the segments of conveyors perform a similar function. Damage accumulates in the inexpensive rubber which, after certain level of damage, is replaced and the expensive segments of the conveyor are protected.

3.2.3 Deliberate weaknesses providing stress relaxation

Common examples of deliberate weaknesses of this class are the expansion offsets accommodating dilatations from thermal expansion/contraction of pipes, railways, bridges, girders, etc., which could otherwise destroy the structures.

The deliberate gaps introduced at regular intervals on a pavement have a similar purpose.

Designing joints free to rotate in trusses (instead of welding) eliminates bending and reduces the magnitude of the internal stresses.

Segmenting structures by providing surfaces free of shear stresses also reduces the magnitude of the internal stresses.

3.2.4 Deliberate weaknesses acting as frangible objects

Frangible objects/structures are deliberately designed to break easily upon overstress. The purpose is to protect the more valuable object and minimise damage. The lighting towers in airports are a typical example. Upon collision with an aircraft, they easily break and protect the aircraft from excessive damage. Frangible light poles are another example. They fail easily upon collision with a car thereby reducing the consequences to drivers and passengers.

Weakly fixed objects are designed with a similar purpose. For example, the detachment of an aircraft engine upon emergency landing protects the aircraft from fire.

3.3 Deliberate weaknesses deflecting damage from places where the cost of failure is high

The mechanism underlying this class of deliberate weaknesses consists of deflecting the location of damage accumulation and failure away from parts where the cost of failure or cost of intervention is high.

The example given in Fig.5 depicts a pipe (1) carrying fluid with debris. The debris have a tendency to clog the pipe and if this happens in the zone with difficult access, a costly and lengthy intervention will be required.

To avoid this, a deliberate weakness deflecting the clogging has been installed in an easily accessible place in the form of a deliberately narrowed section with ribs (2) which make clogging easier compared to the rest of the pipe. This arrangement permits the deliberate weakness to be removed, cleaned and installed back in place. Without the deliberate weakness, clogging could occur in the zone (3) which requires costly intervention associated with delays.

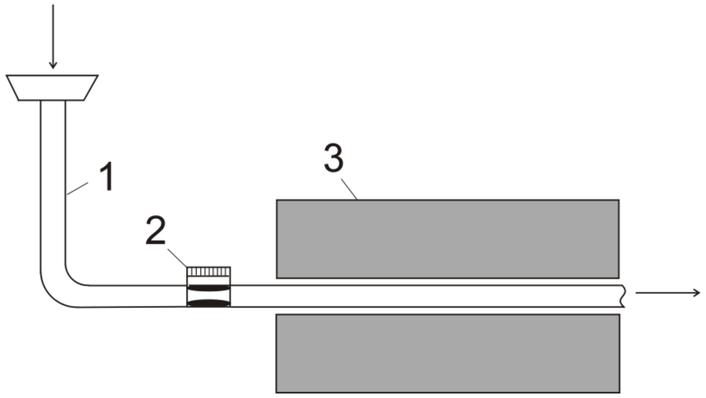

Figure 5. Reducing the risk of increased delay due to blockage by deflecting the potential failure in a place where the intervention for repair is easier.

This example also demonstrates that combining domain-independent knowledge of deliberate weaknesses deflecting damage and domain-specific knowledge related to transporting fluids with debris results in significant risk reduction.

The deliberately weak interfaces in layered structures are also deliberate weaknesses deflecting damage. Propagating cracks are deflected along weak interfaces and their penetration into the components is stopped or delayed significantly.

Narrow, deliberately made pre-cracks along underground cables are extended if the temperature drops significantly below zero and causes the ground to freeze. As a result, the formation of cracks across the cables and severing of the cables is prevented.

The application of this class of deliberate weaknesses transcends engineering. Thus, in computer security, "sacrificial hosts" built outside the internet firewall of an organisation are intended to lure and bait potential attackers, delay them, issue warning and even obtain information about the identity of the attackers.

Pilot projects in project management have a similar function. A relatively small investment is allocated for the pilot project and if failure does occur, the loss is relatively small because it is confined in the pilot project not in the expensive main project. In addition, if failure does occur in the pilot project, valuable lessons are still learned about the technical feasibility of the product, the market place and customers. As a result, the risk of a significant loss of investment is mitigated.

Leaving a deliberate weakness to be attacked in order to regroup forces and concentrate on striking elsewhere has always been an important element of the military tactics. The well-known "pincer manoeuvre" leaves a weakened centre to be attacked by advancing enemy forces followed by ambushing the flanks of the enemy formation by the concealed sides.

3.4 Deliberate weaknesses providing warning

This class of deliberate weaknesses provide a warning about increasing levels of stress/strain which could damage components and structures. Mechanical fuses on cables are a good example of this type of deliberate weaknesses (Tunno and Larsen, 2011). In normal operating conditions, the load is carried by the deliberately weakened fuse. Should load exceed a dangerous limit, the fuse deforms and the load is transferred to the cable.

Sand probes in pipelines are another example. They provide warning about excessive erosion due to excessive sand particles in pipelines transporting crude oil.

In the area of security, tapes which easily delaminate and fracture are used to provide warning against tampering or unauthorised access.

3.5 Deliberate weaknesses providing quick access

In a number of cases, the quick access to emergency resources is of critical importance. Such is the case of medical resources, alarm push-buttons, ammunition etc. In this case, deliberate weakening of the casing (housing) provides quick access in case of emergency. The alarm push-button behind a weakened glass cover is an example of a deliberate weakness from this category.

3.6 Deliberate weaknesses providing quick escape

The mechanism is to provide quick escape in critical circumstances by deliberately weakening particular components in the system. Such are the various quick-release pins, break-away escape links, break-away buckles for pet-animal collars and break-away links attaching life boats. The break-away tagline used in air rescue operations includes such a deliberate weaknesses. In the event of entanglement of the tagline, the break-away weak link allows the tagline to be easily broken by the personnel thereby allowing the helicopter to escape.

This category of deliberate weakness is also found in nature. Some animals lose a particular body part as a defence mechanism (*autotomy*). The Gecko lizard is a well-known example. Gecko's tail contains a deliberately weak connective tissue that can easily break when the animal is in danger.

3.7 Deliberate weaknesses triggering protection systems

The purpose of this category of deliberate weaknesses is to provide indirect protection by triggering a specially-designed protection system in case of overload.

Common examples are the deliberately weakened plugs in fire protection systems consisting of an alloy with low melting point or a weakened glass bulb. In the case of fire, the deliberately weakened plug fails and the sprinkler fire protection system is activated.

The hydraulic damper secured by weakened pins is another example. In case of strong earthquake forces, the pins shear and release the hydraulic damper which mitigates the damage to the building.

4. THE EQUAL-RELIABILITY/EQUAL-STRENGTH CONCEPT AND THE DELIBERATE WEAKNESS CONCEPT

A discussion on deliberate weaknesses in design will be incomplete if the relationship between the deliberate weakness concept and the equal-reliability concept is not clarified.

A common reliability allocation strategy in engineering design is to make all parts with comparable reliability or strength and not to leave weak links. Such is, for example, the AGREE methods described in (Ebeling, 1997). The essence of this strategy is to allocate to each module in a system an equal share of the reliability of the system.

In (Thomson, 1999), for example, it has been advocated that the safety margins of all components are selected in such a way that a maximum "distance" to the constraints preventing the separate failure modes from occurring is maintained. The underlying idea is that this strategy will maximise system reliability and offer maximum protection against uncertain variations caused by loads and environmental conditions.

Another reliability allocation strategy (Ebeling, 1997) is to optimize the reliability allocation, so that the cost of achieving the required reliability is minimised.

Neither of the described reliability allocation strategies takes into account the cost of component failure. Following any of these reliability allocation strategies could be justified only if the cost of system failure due to failure of any component/part is approximately the same. In reality, the cost of system failure due to failure of the individual components is different. Neither designing the parts in the system with equal (comparable) reliability nor achieving the system reliability in the least-cost manner minimises the expected loss given that failure occurs.

The expected loss given failure $\bar{C}_f$ of a system with *M* components logically arranged in series is given by (Todinov, 2004)

$$\bar{C}_f = \sum_{k=1}^{M} \frac{\lambda_k}{\lambda_1 + \ldots + \lambda_M} \bar{C}_{k|f} \tag{6}$$

where λ_i, $i = 1,...,n$ are the hazard rates characterising the separate components, and $\bar{C}_{k|f}$ is the expected loss given failure, characterising the ith component.

Consider a simple system consisting of two blocks only (*A* and *B*). The cost of repair C_A of block *A* is much higher than the cost of repair C_B of block *B* ($C_A \gg C_B$). Suppose that λ_1 is the failure rate of block *A* while λ_2 is the failure rate of block *B*. For the sake of simplicity, let $\lambda_1 \approx \lambda_2$. According to equation (6), the expected loss given failure $\bar{C}_f$ is given by

$$\bar{C}_f = \frac{\lambda_1}{\lambda_1 + \lambda_2} C_A + \frac{\lambda_2}{\lambda_1 + \lambda_2} C_B \approx (1/2)C_A + (1/2)C_B \tag{7}$$

Introducing a deliberate weakness in block *B* will make its hazard rate $\lambda_2^{'}$ much greater than the hazard rate of block *A*: $\lambda_1 / \lambda_2^{'} \approx 0$. The expected loss given failure now becomes:

$$\bar{C}'_f = \frac{\lambda_1}{\lambda_1 + \lambda_2^{'}} C_A + \frac{\lambda_2^{'}}{\lambda_1 + \lambda_2^{'}} C_B = \frac{1}{1 + \lambda_2^{'} / \lambda_1} C_A + \frac{1}{\lambda_1 / \lambda_2^{'} + 1} C_B \approx C_B \tag{8}$$

As a result, the consequences from failure will be reduced because it is much more likely that block *B* will fail in the case of overload. The expected cost of replacement if a deliberate weakness is present will be significantly lower compared to the expected cost of replacement if no deliberate weakness is present.

Creating components with comparable reliability or strength, for example, will make the failure occurrence to be equally likely in any component, irrespective of its cost of failure, which, in many cases is highly undesirable. In a number of cases, to reduce the cost of failure, it is of critical importance that failure occurs in a controlled manner and at a predictable location.

Consider, for example, sections of subsea oil and gas production equipment. Some of them are located on a floating platform and the other are located on the sea bed. The design should be made in such a way that if failure occurs, the likely failure location is in the sections on the floating platform. On the floating platform the cost of intervention for repair is much lower compared to the cost of intervention for repair in the subsea sections. The intervention for repair of these sections is a complex process which typically requires remotely operated underwater vehicles or oil rigs.

A deliberate weakness can be created easily by rating the deliberate weakness at the level of stress at which its failure must be triggered and by eliminating safety margins. Leaving safety margins will make the behaviour of the deliberate weakness unpredictable. Due to the safety margin, the deliberate weakness may not fail and protect the valuable part of the system. Almost any physical property can potentially be used for creating a deliberate weakness: shear strength, yield strength, electrical resistance, electrochemical potential, magnetic properties, melting point, stiffness, fracture toughness, etc.

The shear pin is an example where the shear strength of the material is used to create a deliberate weakness. The thermal fuse is an example where the melting point of an alloy is used for this purpose and the sacrificial anode is an example where the electrochemical potential of a metal/alloy is used.

It is important to emphasise that the design of a deliberate weakness requires examining its failure modes and their causes. A fault tree is a suitable structure for this purpose. The basic function of the deliberate weakness is to fail at the pre-determined level of stress. Negating this function gives two fundamental types of failure: (i) failure significantly below the pre-determined level of stress and (ii) failure significantly above the predetermined level of stress.

Consider failure of a shear pin significantly above the predetermined level of stress. Possible contributing reasons for this type of failure are: (i) large variation of the shear strength of the material (ii) inhomogeneous material, causing a local fluctuation of the shear strength in the shear zone; (iii) bending of the pin instead of shearing; (iv) incorrect shape and dimensions of the shear pin; (v) incorrect material of the shear pin (vi) ageing of the material of the shear pin associated with second-phase precipitations increasing strength.

5. CONCLUSIONS

A classification has been proposed of various categories and classes of deliberate weaknesses reducing risk as well as discussion related to the underlying mechanisms of risk reduction. It is shown that introducing and repositioning weaknesses is an effective risk-reduction strategy which transcends engineering and can be applied in many unrelated domains. The fundamental difference between a deliberate weakness and a stress limiter has been discussed, together with the advantages of the deliberate weaknesses compared to active protection systems.

A new domain-independent method for reducing risk has been proposed based on repositioning an existing weakness in time or space. The reduction of the consequences from failure of many processes comes from the circumstance that if failure occurs early, the rest of the operations composing the process do not need to be executed.

Introducing a deliberate weakness reduces significantly the expected cost given failure and has significant advantage to the equal-reliability allocation strategy in the case where the cost of failure of the separate components varies significantly.

Promising future research directions related to the application of the method based on deliberate weaknesses are (i) expanding the proposed classification of deliberate weaknesses with new categories and classes and (ii) detailed comparative study on the advantages and disadvantages of deliberate weaknesses versus active protection systems.

Acknowledgement

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

REFERENCES

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

Childs P.R.N. (2014). *Mechanical design engineering handbook*, Amsterdam: Elsevier.

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

Dhillon B.S. (2017). *Engineering systems reliability, safety, and maintenance*, Boca Raton, New York: CRC Press.

Ebeling, C.E. (1997). *An Introduction to Reliability and Maintainability Engineering*, New York: McGraw-Hill.

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

Erhard, G. (2006). *Designing with Plastics*. Munich: Hanser.

Fantner G.E., E.Oroudjev, G. Schitter, L.S. Golde, et al. (2006). Sacrificial Bonds and Hidden Length: Unraveling Molecular Mesostructures in Tough Materials, *Biophysical Journal*, 90, 1411–1418.

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

Gere J. and Timoshenko S.P. (1999). *Mechanics of Materials*, 4th edn, Stanley Thornes Ltd.

Giddens, A. (1999). Risk and Responsibility, *The Modern Law Review*, 62(1), 1-10.

Gere, J.M. and Timoshenko, S.P. (1999). *Mechanics of Materials*. Cheltenham: Stanley Thornes (Publishers) Ltd.

Gullo L.G., J.Dixon (2018). *Design for safety*, Chichester: Wiley.

Hedlund, F.H., Selig, R.S., and Kragh, E.K. (2016). Large steel tank fails and rockets to height of 30 meters rupture disc installed incorrectly. *Safety and Health at Work* 7, 130–137.

Lewis, E.E. (1996). *Introduction to Reliability Engineering*. New York: Wiley.

Modarres M., M.P.Kaminskiy, V.Krivtsov (2017). *Reliability engineering and risk analysis, a practical guide*, 3rd ed., CRC Press.

Mott R.L, E.M.Vavrek, J.Wang (2018). *Machine Elements in Mechanical Design*, 6th ed., Pearson Education Inc.

Norton R.L. (2006). *Machine design, an integrated approach*, 3rd ed., Upper Saddle River: Pearson Education Inc.

O'Connor, P.D.T. (2002). *Practical Reliability Engineering*, 4e. New York: Wiley.

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

Budynas R.G., J.K.Nisbett (2015). *Shigley's Mechanical engineering design*, 10th ed., McGraw-Hill Education.

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

Todinov M.T. (2004). Reliability analysis and setting reliability requirements based on the cost of failure, *International Journal of Reliability, Quality and Safety Engineering*, 11 (3), 273–299.

Todinov M.T. (2019). Domain-independent approach to risk reduction, *Journal of Risk research*, https://doi.org/10.1080/13669877.2019.1628093.

Samuel, A. and Weir, J. (1999). *Introduction to Engineering Design: Modelling, Synthesis and Problem Solving Strategies*, London: Elsevier.

Tunno, D. and Larsen, S. (2011). Retrofittable cable mechanical fuse. US Patent 20,110,027,007 A1.

Zhou X., B.Guo, L.Zhang and Guo-Hua Hu (2017). Progress in bio-inspired sacrificial bonds in artificial polymeric materials, *Chemical Society reviews*, 46(20), 6301-6329.