International Journal of Risk and Contingency Management
Volume 9 • Issue 2 • April-June 2020

Reducing the Risk of Failure by Deliberate Weaknesses

Michael Todorov Todinov, Oxford Brookes University, Oxford, UK

ABSTRACT

The deliberate weaknesses are points of weakness towards which a potential failure is channeled in order to limit the magnitude of the consequences from failure. The article 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 article 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.

KEYWORDS

Consequences of Failure, Deliberate Weaknesses, Domain-Independent Methods, Fail-Safe Design, Reliability Improvement, Risk Reduction, Sacrificial Link, Weak Link

DOI: 10.4018/IJRCM.2020040103

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 weak links 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