Safety by Design

by Mohammad Rajabali Nejad
Enschede, The Netherlands

I have been teaching design engineers for many years, seeing them trying to achieve the best for their customers given the available resources. Despite the constraints, they often enjoy a freedom of choices in the early design. This is because problems often can be solved in a variety of ways, and early choices are more easily made. These choices often remain, perhaps for the full project lifecycle and sometimes with the next generation of the product. If these early decisions are not proper, there are extra costs subsequently imposed on the project. Figure 1 highlights the increasing costs for mitigations as the project advances. In other words, designers often enjoy exploring design choices in early design phases, and they have the most influence on the design of products or systems, as well as their safety.

Safety in Engineering Performance

Constraints on resources, however, push designers to focus on market-driven performance indicators. These indicators for engineering performance are primarily cost, quality and time-to-market — the so-called performance triangle [Ref. 2]. Safety is not explicitly present among these performance indicators, but this does not mean that safety is absent. In the performance triangle for engineers, safety strongly correlates with quality and costs. Quality products or quality systems are more likely to be safe. In fact, the uncertainty in performance of quality products or services is small, reducing the possibility of unexpected consequences. There is still a possibility of using a quality product in an unsafe situation, purposefully or not, yet people often equate quality with safety, e.g., a "high-quality" car is likely to be a "safe" car. Furthermore, paying attention to safety saves cost, especially in early designs. Products that have been pulled off the market because they have been assessed as "unsafe" are daily examples that proper implementation of safety saves

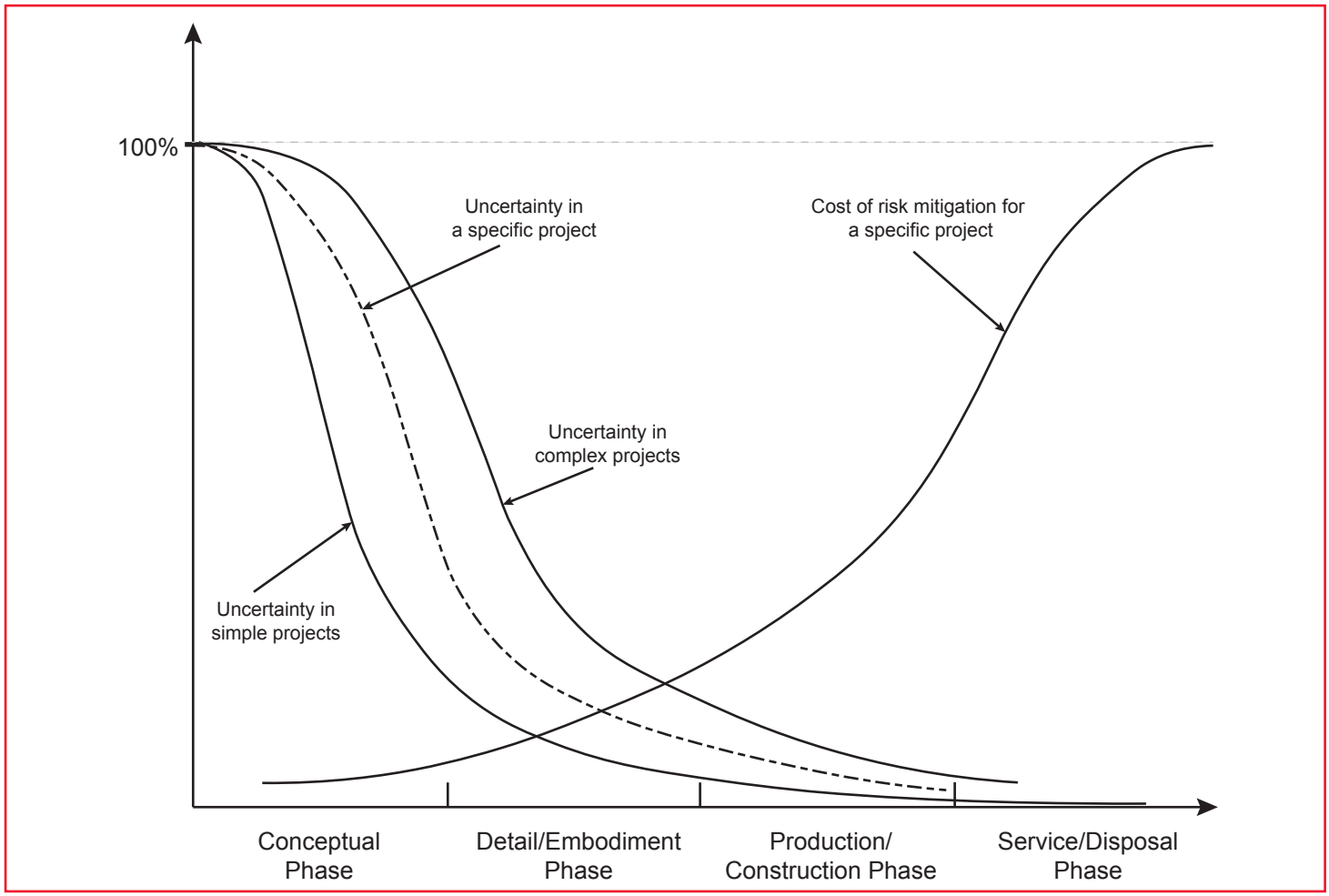

Figure 1 — Presence of Uncertainty and Risk in Full Project Lifecycle [Ref. 1].

what can sometimes be enormous costs. On the other hand, products that are not sufficiently safe impose liability costs and defame companies. The IKEA MALM dresser tip-over problem is an example of enormous consequences for customers, as well as companies; this product took the lives of six children in the U.S. with a cost of millions of dollars for the company. In today's highly competitive environment, there is no room for trial and error. Safety must be well thought-out and implemented in the course of design.

Safety is often considered a performance indicator; hopefully, among the most important in the engineering design process. There are many product or service providers who still think large safety issues happen only to others because "it has not yet happened to us." Safety continues to remain implicit in the engineering performance triangle or engineering design models for practice.

Safety in Engineering Design Models

The commonly practiced design models for engineers include several steps, starting with analyzing the problem and then identifying requirements, generating ideas and concepts and embodying the chosen concept followed by detailed design and testing [Ref. 3]. Other widely accepted approaches, e.g., the V model in systems engineering, follow a similar pattern [Ref. 4]. In these models, safety is often treated as a requirement that must be addressed through the process.

Common safety-related practices, e.g., Preliminary Hazard Analysis (PHA), are performed to inform stakeholders about possible hazards or risks. Failure Mode and Effect Analysis (FMEA) is commonly used for exploring possible failure scenarios, assigning failure probabilities and analyzing consequences. To represent the hierarchy of faults or subsequent

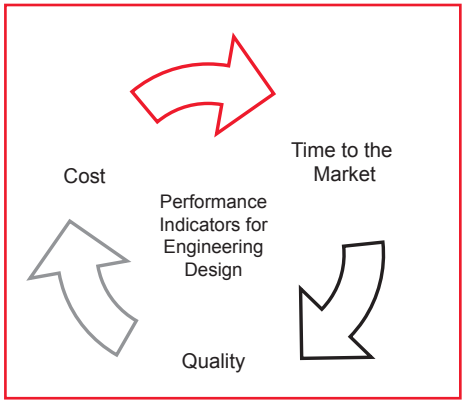

Figure 2 — Cost, Quality and Time to the Market are the Main Performance Indicators for Engineers.

Figure 3 — William Ely Hill's My Wife and My Mother-in-Law. *They are Both in the Picture —Find Them.*

events, Fault Tree Analysis (FTA) or Event Tree Analysis (ETA) are commonly used. The essence of these methods is based on component failure; a system failure is presented as a logical chain of events or faults. Methods like Fishbone, Cause and Effect diagram, or Root Cause Analysis focus on the relationship between hazards and possible events. To estimate the likelihood of these events, Probabilistic Risk Assessment (PRA) methods, Bayesian Belief Networks (BBN) or Incident Tree Method (ITM) [Ref. 5] may be used.

These tools often assume that if a product functions as it is intended, there is no failure and the product will be safe. In this context, quality or reliability is thought to be similar to safety, and the applied tools become incapable of capturing a situation that is unsafe, but not associated with a failure [Ref. 6]. The shortcomings of this assumption become more obvious when systems become more complex.

Designers' Dilemma

A question worth exploring is, "Why is safety not explicitly present among engineering performance indicators or in engineering design models?" I think there is no single answer to this question. In my experience, designers often rely primarily on their experience and intuition because there is a need for so much implicit information, but it is hard to formulate everything in early design. This results in a dilemma for designers. One of my students, who followed the course for "safety by design," wrote to me that "safety is just not the most inspiring part of design," and I think he is right. While designers focus on creating something that must fulfill the customer's needs, they also must think about possible malfunctions or misuse scenarios. To further clarify this, the famous drawing titled *My Wife and My Mother-in-Law* can be used as a metaphor for designers who often intend to think about the functions and proper use of the product rather than its misuse scenarios or malfunctions.

In other words, the commonly practiced patterns for designers, recommended by best practices, encourage designers to think fast when they are thinking of functions or solutions, but do not make vacant space for designers to think about misuse or malfunction scenarios [Ref. 3]. To ad-

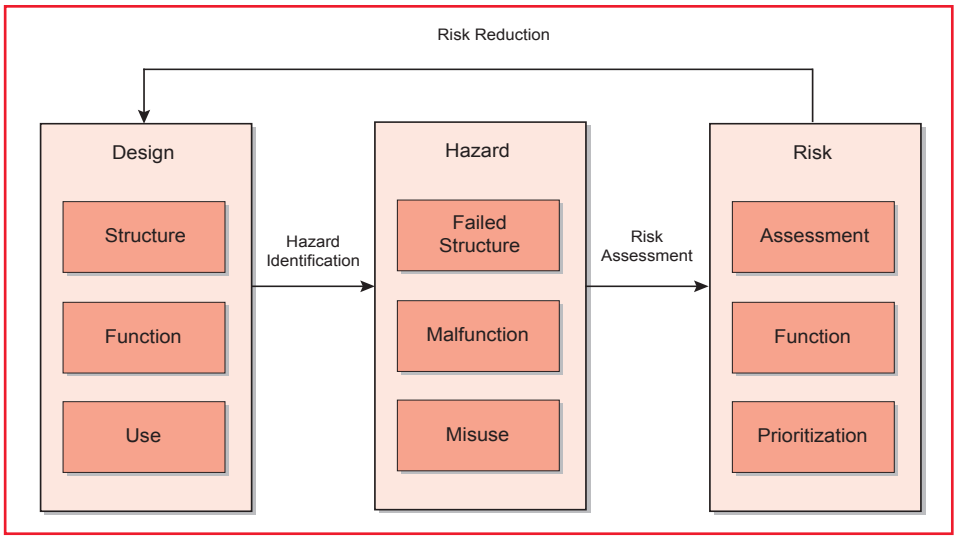

Figure 4 — The Process for Safety by Design.

dress this problem, safety needs more "space" throughout the design process [Ref. 7].

Safety by Design

Design of products or systems can be defined as "creations for doing intended functions and operations (use)." This is summarized in the three pillars of structure, function and use [Ref. 8]. Safety by design ensures that the risks have been properly addressed during the design phase — by either designing hazards out or by controlling hazards that cannot be removed. However, in general design processes, there is often no explicit analysis of malfunction or misuse as discussed earlier. From a safety perspective, risk assessment and risk reduction must be part of the design process [Ref. 1], and the proper implementation of risk analysis in the design process is likely to improve safety.

Safety can be achieved through design in different ways. Applying safety factors, making emergency stops, using redundant systems and fail-safe systems are all examples of implementing safety through the design process. In fact, safety by design is not new. Safety by design identifies risky situations and circumstances where (failure in) structure, (mal) function or (mis)use causes harm to humans, the environment or property. This process is summarized in Figure 4. This figure suggests a separation between the working structure and the failed structure, between proper function and malfunction, and — finally — between proper use and misuse through the course of design. This creates specific space for the identification of hazards leading to risk assessment and risk reduction, altering the design for more safety, if necessary.

Conclusions

Achieving safety through design is a widely accepted practice, in different engineering disciplines in different ways. Currently, the fast pace of technology and large effects of safety-related failures encourage engineers to further investigate ways for implementing safety in the early design process. Safety by design can help engineers deliver higher performance, yet it cannot promise to solve all safety-related issues for designers. Safety by design can help designers focus their minds to achieve safety against known issues or possible issues, but it cannot guarantee complete safety.

References

1. Nejad, M. Rajabali. "Modelling and Prioritization of System Risks in Early Project Phases," *International Journal on Advances in Telecommunications*, Vol. 9, No. 3-4, 2016.
2. Nejad, M. Rajabali, G. M. Bonnema and Frederikus J. A. M. van Houten. "An Integral Safety Approach for Design of High Risk Products and Systems," presented at the Safety and Reliability of Complex Engineered Systems, Zurich, Switzerland, September 7-10, 2015.
3. Pahl, G., W. Beitz, J. Feldhusen and K. H. Grote. *Engineering Design: A Systematic Approach*, Springer, New York, New York, 2007.
4. Forsberg, C. Kevin and C. Michael Krueger. "INCOSE Systems Engineering Handbook: A Guide For System Life Cycle Processes and Activities," 2007.
5. Ericson, C.A. *Hazard Analysis Techniques for System Safety*, John Wiley & Sons, Hoboken, New Jersey, 2005.
6. Fleming, C.H. "Safety-driven Early Concept Analysis and Development," Ph.D. dissertation, Massachusetts Institute of Technology, 2015.
7. Bahr, N.J. *System Safety Engineering and Risk Assessment*, CRC Press, Boca Raton, Florida, 2014.
8. "EN-ISO 12100:2010 Safety of Machinery — General Principles for Design — Risk Assessment and Risk Reduction," International Organization for Standardization, 2010.