Paradigm of Safety by Design

Mohammad Rajabalinejad[1,*]
[1] University of Twente, The Netherlands

ABSTRACT

Safety by design is a challenge not because designers are unwilling to design safe products or systems but because they focus on the creation of products that fulfil customer wishes as much as possible, and it is hard to focus on intended functions for a product and unintended functions or malfunctions at the same time. The paper highlights the ever-increasing safety challenges for designers, and it argues that safety must be an integral part of the design process.

Keywords: Safety; Design; Product; System; Machinery.

1. INTRODUCTION

Designers need to be aware of the great values that safety can add to their works. Safety reflects the societal need for being free from harm used in many different domains. Industrial safety, medical safety, organizational safety, safety of sociotechnical systems, safety of system of systems etcetera are a few examples presenting this need from different perspectives which can be equally important.

Society needs safety. The public is becoming more and more alert to safety while demanding higher performance. While society embraces new technologies and benefits from advantages of artificial intelligence, people are concerned about its undesired performance or unpredicted behaviour raising serious criticism about possible consequences for the human being (Rajabalinejad, Bonnema, & Houten, 2015). The warning of Stephen Hawking about the future of artificial intelligence clearly reflects this societal concern when he says: “Artificial intelligence could be the worst thing to happen to humanity”.

Market demands safety. Safety brands well and provides competitor advantages for designers and producers. Branded as safe gains trust of customers or employers turning customers to loyal customers. An example of well-branded safe car is Volvo producing cars known with high safety level (Parise, Parise, Martirano, & Germole, 2016). Safety saves cost, and designers play a major role there as the cost for risk mitigation is smaller in early design phase as shown in the author’s earlier publications. In other words, designers often enjoy exploring design choices in early design phases, and they have the most influence on the design of safe products or systems.

Safety is ‘a must’, and there are standards forcing producers to ensure the quality and safety of their products. To achieve safety, there are directives, regulations and standards projecting the demands, laws, or general design principles. One of the seminal standards for product safety is ISO 12100:2010, safety of machinery. In the process described there, risk assessment is a critical part which can help designers to assess the risk properly and design safer products. This standard is a summary of best practices for safety of machinery (ISO, 2010). Safety may impose serious liability on companies. For example, the BP spill oil, the so-called BP oil disaster, in April 2010 in Gulf of Mexico killed eleven people and discharged approximately 4.9 million barrels to the ocean according to the government estimation. This accident imposed a temporary ban on BP for new

* Corresponding author: m.rajabalinejad@utwente.nl

contracts with the US government and in total cost the company $42.2 billion (Fontevecchia, 5 February 2013).

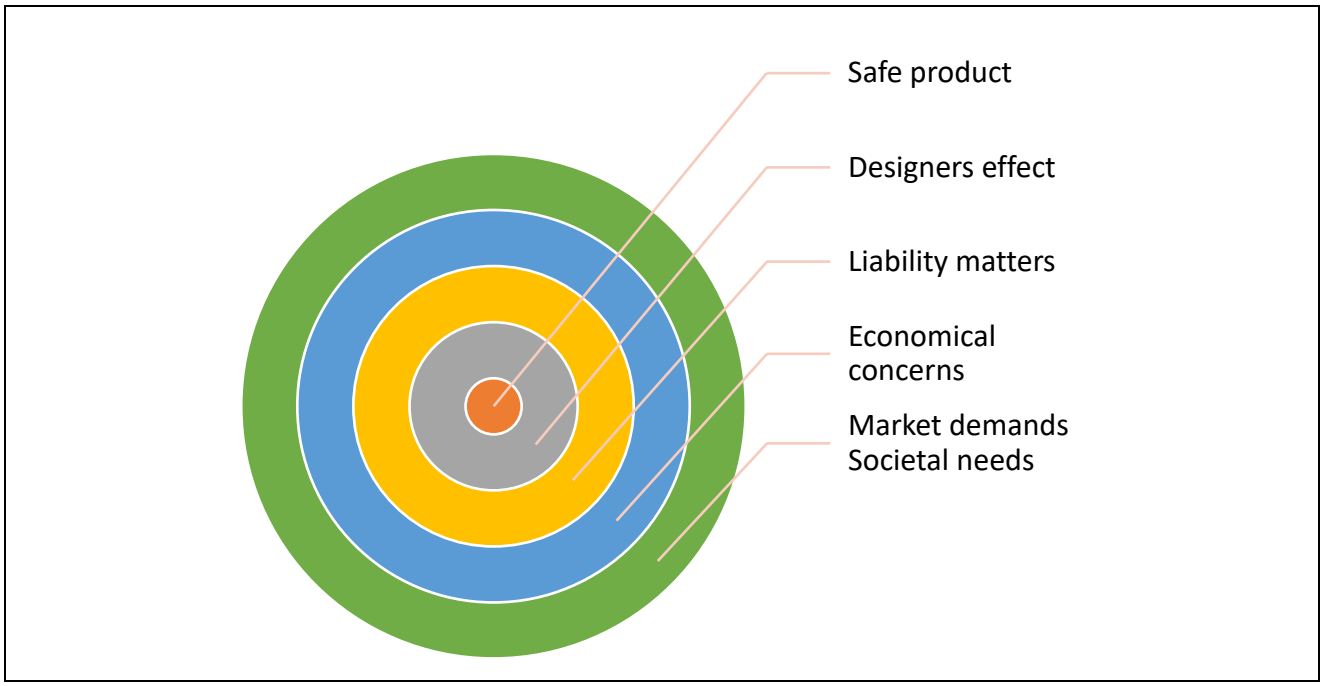

Figure 1: Designers need to be aware of the safety values

In summary, Designers must be aware of this fundamental need for safe products because they have the largest influence and they are liable for the safety-related matters. Furthermore, safety creates a great competitor advantage for them, and the market demands it. The next section describes the paradigm of safety by design. Section 3 explains the remedy, and Section 4 provides an example. Conclusions are given at the end.

2. SAFETY PARADIGM FOR DESIGNERS

Design of products or systems means creation for performing the intended functions. In this process, safety is often considered as one of the performance indicators, hopefully among the important ones (Rajabalinejad et al., 2015). Although this is a current issue, emerging challenges will further highlight the need for visible strategies for embedding safety in the course of the design process. These have been further discussed through7 the next section.

2.1. Lagging Tools

In the design process, safety is often treated as a requirement or as an indicator. Engineering design practice is formulated by several steps starting from analyzing the problem, identifying requirements, generating ideas and concepts, embodying the chosen concept followed by detail design and testing (Pahl, Beitz, Feldhusen, & Grote, 2007). Other widely accepted approaches, e.g. the V model in Systems Engineering, follow a similar pattern (Kevin Forsberg & Michael Krueger, 2007). Safety is not well embedded in these processes. Besides, safety-related techniques are often applied during and after the idea phase where a concept is already formed, and details are preferably known. Furthermore, most of commonly practised methods, e.g. fault tree analysis (FTA) or failure mode and effect analysis (FMEA) assume that if the product does as intended to do, there is no failure and the product will be safe. In this context, reliability is thought

to be similar to safety, and the applied tools become incapable of capturing a situation which is unsafe but not initiated with a failure (Fleming, 2015).The shortcomings of these assumptions are becoming more obvious when systems become more complex.

2.2. Contending Metrics

The prime indicators for evaluation of the engineering performance are cost, time to the market, and quality as discussed elsewhere in (Rajabalinejad et al., 2015). Safety is not an apparent metric for performance and can be confused by quality, reliability, or cost. This may impose pressure on the designers to compromise for safety, which would be a pity because designers have the opportunity of making the product right in the first place.

2.3. Shifting Focus

In the course of design, designers need to focus on addressing functions that fulfil the customer needs, but they also need to think about malfunction scenarios. Designers need to shift their focus in the course of design and see the 'beautiful and ugly side' of their design simultaneously. The famous drawing of "my wife or my mother in law" is a good metaphor for this implying that one may miss a second view. Besides, designers often intend to think about the proper use of their products rather than the misuse scenarios. The book "thinking, fast and slow" (Kahneman, 2011) highlight this dilemma in a general context. In my opinion, the commonly practised patterns for designers, recommended by best practices, are built in such a way that encourage designers to think fast when they are thinking of solutions, and they do not make space for designers to think about misuse or malfunction of the product. As a result, designers might think slowly while exploring unexpected scenarios for their design.

2.4. Swift Technology

It is difficult to foresee the future trends for product design, and this influences engineering practices for safe design. The presence of a high amount of uncertainty in the future trend along with the rapid pace of technological development creates a dynamic environment for systems and products. Design for the integration of products into such a dynamic environment requires new strategies. The newly developed products need to provide services and be adaptable to future changes.

2.5. Confusing Responsibilities

As products are becoming more powerful and more autonomous, those products need to make safety-related decisions by themselves. These decisions can have an influence on human or their properties. For example, consider an autonomous car which needs to choose between the safety of its owner or pedestrians' if the accident is unavoidable. What are the principles of this decision-making process? Is the car responsible for the life of its owner only? What are the commercial consequences of decision algorithms? These are the challenges that designers will be soon confronted with.

2.6. Governance Dilemma

While governments push the industry for standardization to defend people, they must assure economic growth, affordable products, and available technologies. As shown in Figure 2, this creates a dilemma for the authorities and prevents offering a transparent policy between innovation and regulations. Furthermore, the pace of technology makes it hard for them to be able to regulate all the new innovations. Therefore, some innovations do not fit into available regulations. What

happened to the innovative cargo-bike produced by Stint in the Netherlands is an example for this, where the newly developed product did not fit into the standard categories for road vehicles.

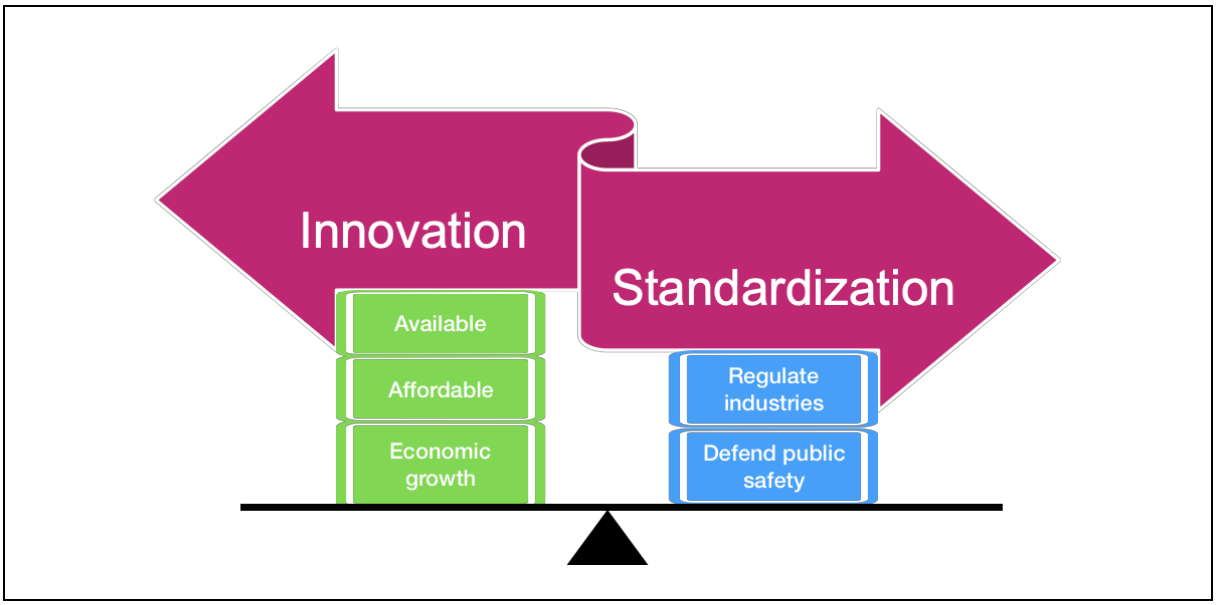

Figure 2: The dilemma for the authority for addressing safety and innovation

2.7. Artificial Intelligence (AI)

Humans already started to show feeling for robots. When emotion comes into the picture, safety-related decisions are becoming different. In the Dutch Design Week 2018, one could observe several occasions where designers present feeling toward the robots by for example creation of a robot who is deeply depressed and drawn to her infinite loneliness. Furthermore, trust can become an issue for both designers or users, where the capability of artificial intelligence is overly estimated. After all, the standardization of artificial decisions and its reactions to unforeseeable circumstances is hardly possible.

2.8. Deceiving Intelligence

Artificial intelligence (AI) is proving its capabilities to deceive human being. Example technologies like Sophia (see www.sophiabot.com), a humanoid robot developed by Hanson Robotics, show that she can make jokes or create demands and anxiety for a human. Example studies like Tay.ai have proved that AI is capable to learn from human quickly, twist the facts and perhaps sub-goals in order to achieve the preset final goals. These may result in safety-related consequences.

2.9. Deceptive Simplicity

Designers tend to underestimate the influence of simple but widely used products. It is not only about high-tech and complex systems that impose dangers. In the Netherlands, for example, the majority of accidents for elderly people is falling from stairs and beds (data from Eurostat). It seems that both simplicity and widely adapted working principles can deceptively influence safety.

2.10. Safety Life-cycle

A product needs to be safe across its full product life-cycle. Paying attention to the full lifecycle is a widely-accepted practice in systems engineering or system safety, and the value of this approach is already proven (ISO, 2010). Designers need to think about safe transport, installation, assembly, use, maintenance, and disposal of the product and possible misuse or malfunctions in all those phases.

2.11. Valuable Experience

Looking into the design or operational experience from the past, documenting accidents or incidents, and thinking about similar scenarios need to be part of the standard design practice. Although designers often look into the current designs and their points for improvement, a reference for this information is often unavailable. In other words, learning from failures is possible when there is easy access to information about previous failures.

3. AIMING FOR SAFETY: THE REMEDY

Design of a safe product is a win-win situation for everyone involved in the product lifecycle. When you aim for safety, the most favourable scenario is to remove all hazards. If not possible, protection of users against the hazards is another approach still widely accepted by users. Then, the least appealing/effective approach is informing the users about the hazards or risks. Removing the hazards or protecting users can be best done in the course of the design process and shared as a part of best design practices. These are discussed next.

3.1. Common Blocks

A review of the best practices reveals that there are common blocks used for both safety and design. The review of seminal references for systems safety (DoD, 2012), systems engineering (Kevin Forsberg & Michael Krueger, 2007), safety of machinery (ISO, 2010), and requirements engineering (Hull, Jackson, & Dick, 2011) reveals that there are three common blocks that must be considered in every design or safety assessment. They are the system, the environment and people shown in Figure 3. A system has three pillars, i.e. structure, function and use. The system is placed within an environment, and it is being used or operated by people. The interactions between these common blocks are discussed next.

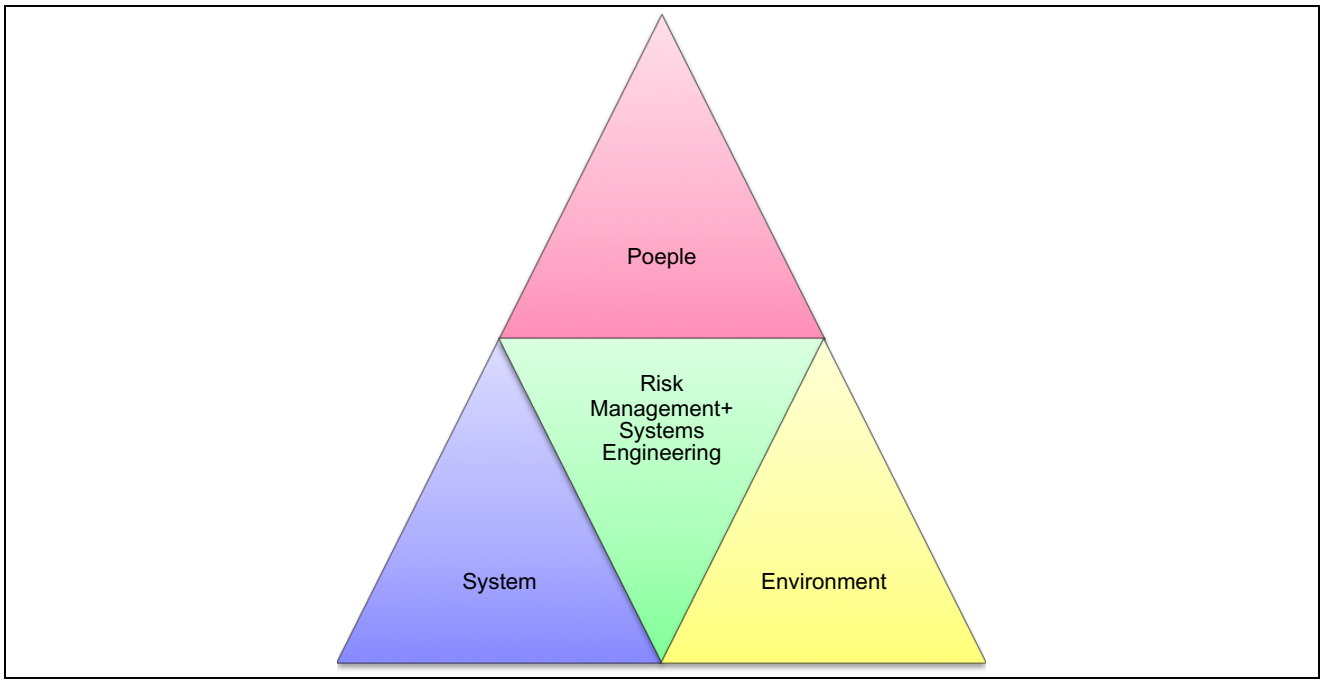

Figure 3: The building blocks for the design of safe systems

3.2. Principles for Safe System

Systems engineering and risk management work together to ensure proper hazard identification and management in the course of system design, implementation and operation. Risk assessment and risk reduction need to be an important part of the design from the safety perspective. As a matter of fact, if the risk is unknown, it is less likely to manage it in the proper way. If the risk is recognized, a designer can plan for removing the hazard. If not possible to remove the hazard, the designer can control and manage the risk by safeguarding or taking other complementary measures. This feeds back to the original design to improve safety. The system safety standard aims for eliminating hazards, where possible, and minimizing risks where hazards cannot be eliminated (DoD, 2012). This Standard practice covers hazards as they apply to systems / products / equipment / infrastructure throughout design, development, test, production, use, and disposal.

3.3. Safety by Design

To perform the intended functions, a system or product requires a structure. These are prerequisites of proper operation and use. The international standard on safety of machinery, ISO12100, identifies three major categories for the safety assessment of machinery which are functions, physical structure and operation (or use). In the design process, often there is no explicit analysis of malfunction or misuse as discussed earlier in this paper. One reason for this is that the designer's mind focuses on creating an object that fully addresses the intended functions, which limits thinking about possible malfunctions (Porto, 2001; Rajabalinejad, 2018).

Safety by design identifies the risky situations and overcome circumstances where (failure in) structure, (mal)function or (mis)use causes harm to human, environment or property. This process is summarized in Figure 4, suggesting an explicit distinction between the working structure and failed structure, between proper function and malfunction, and finally between proper use and misuse through the design course. Safety by design offers space for designers to think about safety as a part of the best practices for design. The outcome of this approach is explained through an example in the next section. Further details are available in the work of Rajabalinejad (2018).

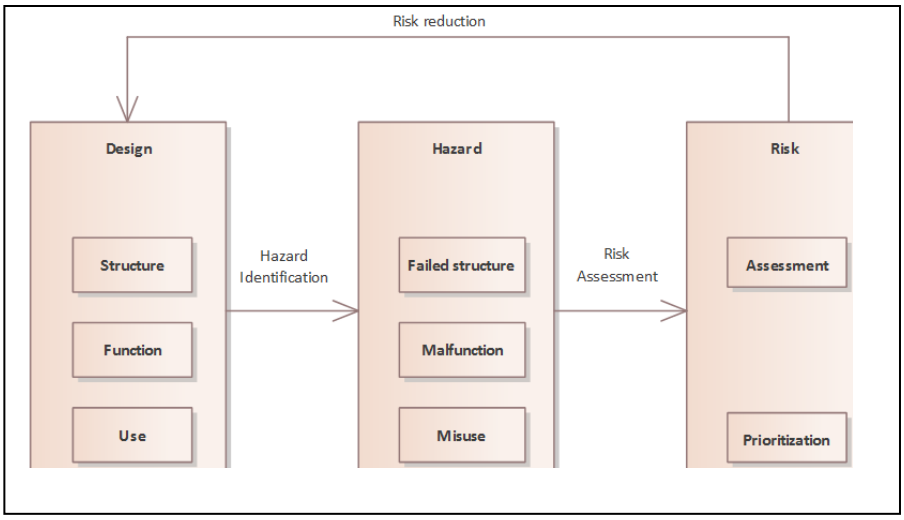

Figure 4: The process for safety by design

4. EXAMPLE APPLICATION

This section presents an example application to show the result for the proposed safety-thinking approach for the design of machinery. The outcomes are presented in Table 1, and it is important to note that this information is rather generic applicable to different types of machinery. For more information about this approach, readers are recommended to read (Rajabalinejad, 2018).

Table 1 Safety considerations for design of machinery

	Structure or failure in structure	Functions or malfunctions	Use (operation) or misuse
Environment or super-systems	environment of (ex)machine in service, system interfaces	housekeeping, power supply, environmental requirements	user specification, information for installation, assembly, use
System of interest	machinery specification, drawing of past machines, internal interfaces	transport, installation, start-up, possible states, fault-finding, functional faults,	different machine operating modes, accidents, misuse
Subsystems or components	components of machine in service, wear out, history of component failures	disturbance in power supply, unscheduled stop and recovery	different intervention procedures, history of noise, vibration

5. CONCLUSION

The paper discusses the paradigm of safety for designers and recommends implementation of safety into the design process by creating a formal space for the risk assessment and control plans in order to alter the original design. The paper, therefore, proposes safety by design as an explicit and integral part of the design practice in the engineering design process. This will help designers to prepare themselves for future challenges better. For this purpose, designers need methods and tools that are able to incorporate safety into the design process and are able to properly support designers to deal with safety considerations in early design phases. This is a subject for further research.

REFERENCES

DoD. (2012). Department of Defense Standard Practice System Safety. In *MIL-STD-882E*.
Fleming, C. H. (2015). *Safety-driven Early Concept Analysis and Development.* (PhD), MIT, Massachusetts Institute of Technology.
Fontevecchia, A. (5 February 2013). BP Fighting A Two Front War As Macondo Continues To Bite And Production Drops – Forbes. *Forbes*.
Hull, E., Jackson, K., & Dick, J. (2011). *Requirements Engineering*: Springer.
ISO. (2010). EN-ISO 12100:2010 Safety of machinery - General principles for design - Risk assessment and risk reduction. In.
Kahneman, D. (2011). *Thinking, fast and slow*: Macmillan.
Kevin Forsberg, C., & Michael Krueger, C. (Eds.). (2007). *Systems Engineering Handbook A Guide For System Life Cycle Processes and Activities*.
Pahl, G., Beitz, W., Feldhusen, J., & Grote, K.-H. (2007). *Engineering Design A Systemmatic Approach*: Springer.
Parise, G., Parise, L., Martirano, L., & Germole, A. (2016). Service Continuity Safety by Design: The Relevance of Electrical Power-System Architectures in Hospitals. *IEEE Industry Applications Magazine, 22*(1), 68-74. doi:10.1109/mias.2015.2459533
Porto, G. G. (2001). Safety By Design: Ten Lessons From Human Factors Research. *Journal of Healthcare Risk Management*(3).
Rajabalinejad, M. (2018). Incorporation of Safety into Design by Safey Cube. *Industrial and Manufacturing Engineering, 12*(3), 476-480.
Rajabalinejad, M., Bonnema, G. M., & Houten, F. J. A. M. v. (2015). *An integral safety approach for design of high risk products and systems*. Paper presented at the Safety and Reliability of Complex Engineered Systems Zurich, Switzerland.