Incorporation of Safety into Design Process: A Systems Engineering Perspective

M. Rajabalinejad

***Abstract*—**This paper suggests integrating the best safety practices with the design process. This integration enriches the exploration experience for designers and adds extra values and competitor advantages for customers. The paper introduces the safety cube for combining common blocks for design, hazard identification, risk assessment and risk reduction through an integral approach.

***Keywords*—**Safety, safety cube, design, product, system, machinery.

I. Safety in engineering design practice

In engineering design process, safety is often considered as one of the performance indicators, hopefully among the important ones. As explained elsewhere in [1], the primary indicators for engineering performances are: cost, time to market, and quality. Next to these, the 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 [2]. Other widely accepted approaches, e.g. the V model in Systems Engineering, follow similar pattern [3]. In this process, safety is often treated as a requirement must be addressed through the process or as one of the indicators need to be addressed. Furthermore, safety-related techniques are often applied during and after the concept formation where details are preferably known. 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 the possible failure scenarios, assigning failure probabilities and analyzing its effects or consequences. To represent hierarchy of faults or subsequent events, Fault Tree Analysis (FTA) or Event Tree Analysis (ETA) are commonly used. The essence of these methods is based on the component failure; a system failure is presented as a logical chain of events or faults. Methods like Fishbone, Cause & Effect diagram, or Root Cause Analysis focus on the relationship between hazard and possible events. To estimate the likelihood of these events, Probabilistic Risk Assessment (PRA) methods, Bayesian Belief Networks (BBN) or Incident Tree Method (ITM) [4] may be used.

Those methods, mentioned above, often assume that if a product does as intend 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. The shortcomings of this assumption are becoming more obvious when systems become more complex [5]. Next section summarizes the problem.

Dr. Ir. M. Rajabali Nejad is an Assistant Professor in the Department of Design, Production and Management in the Faculty of Engineering Technology, University of Twente P.O. Box 217, 7500 AE Enschede, The Netherlands (corresponding author, phone: 315-3489-3278; e-mail: M.Rajabalinejad@utwente.nl).

II. Problem statement

It seems to be a dilemma for designers to incorporate safety into the design process. While designers focus to create something that must fulfill the customer needs, they also must think about foreseeable misuse scenarios or possible malfunctions. To further clarify this, the famous drawing of “my wife or my mother in law” can be used as a metaphor that designers often intend to think about the functions and proper use of the product rather than its misuse scenarios or malfunctions. The book of “thinking, fast and slow” [5] highlight this dilemma in general context. In other words, the commonly practiced patterns for designers, recommended by best practices, are built such that they encourage designers to think fast when they are thinking of functions or solutions and they do not make vacant space for designers to think about misuse or malfunction scenarios [2]. Designers might think slow while explore unexpected scenarios for their designs. To address this problem, safety needs more space through the design process [6]. This study explores the possibility of building the “safety space” in the design process. For this purpose, first the building blocks for design, risk and safety needs to be identified as discussed next.

III. Building blocks for design and safety

By looking into best practices for safety or design e.g. [3, 7, 8], there are similar building blocks used for the design process and safety management process. To find the common building-blocks for design and safety from the systems engineering perspective, references of best practices have been studied for systems safety [8], systems engineering [3], safety of machinery [7] and requirements engineering [9]. Systems engineering offers proven techniques for integrating the main building-blocks and managing possible risks. The system safety standard is the oldest common-practice looking into system safety principles. The system safety standard presents the DoD (Department of Defense of the USA) approach for eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated [8]. This Standard practice covers hazards as they apply to systems, products, equipment, and infrastructure throughout design, development, test, production, use, and disposal. Also, the international standard ISO12100, a seminal reference for safety of machinery, identifies major categories for safety assessment of machinery.

Comparing the above-mentioned practices for design and safety, there are three common blocks (elements) must be considered in every design or safety analysis process. These common blocks are system, environment and people as shown in Figure 1. Focusing on these three blocks, systems engineering and risk management work together to ensure proper hazard recognition and management during system design, implementation or operation.

As a result, it is obvious that the system under design is of primary focus for designers. The system has connections to environment or other systems (the so-called super-systems) and is made of subsystems or components. The role of people in operation or use of the system is discussed next in further details.

A. System, its Past and Future

To perform the intended functions, a system or product requires a structure. This is a prerequisite for proper operation and use. ISO12100 identifies three major categories for safety assessment of machinery which are functions, physical structure and operation (or use). While this standard focuses on the current systems, it is inevitable to think about the experience and future expectations. This has been implicitly (and sometimes explicitly) indicated in standards but has an explicit role in design.

Experience and future insight are needed for design for present. Designers need to consider influences of time not only during the full lifecycle but the past and future generations. This not only inspires designers, offers them rich information and give them further insight, but also is requested by safety standards. Furthermore, looking into the design or operational experience from the past, documenting the past accidents or incidents, and thinking about possible future use, or future misuse, are parts of the standard safety practices. Meanwhile, looking into future changes in the environment and the history of product development enables developing products or system that better adapts to their environmental changes. It is widely accepted that recognition of future trend plays a role in success [10].

Therefore, designers must have access to past systems and consider future developments. Learning from failures is only possible if there is access to previous failures and a way for recommendation to future changes. For designers, the time element is to be considered as well. To give more focus to this, these elements need to be discussed in time spans before, during and after the lifecycle (or in service).

This suggests that the past information about the basic three elements for design and safety, which are system, environment and people, should be easily available and accessible for designers.

IV. Safe Design

A. Dilemma

Design of product, machinery or systems can be defined as creation for doing intended functions and operations (use). This is summarized in three pillars of structure, function and use in e.g. [7]. In the design process, however, there is often no explicit analysis of malfunction or misuse as discussed earlier in this paper (see e.g. [11]). From the safety perspective, risk assessment and risk reduction must be a part of the design process [12]. As a matter of fact, if the risk is unknown, it is less likely to be managed 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 m*anage the risk by safeguarding or other complementary* measures. Therefore, proper implementation of risk analysis in the design process alters is likely to improve safety.

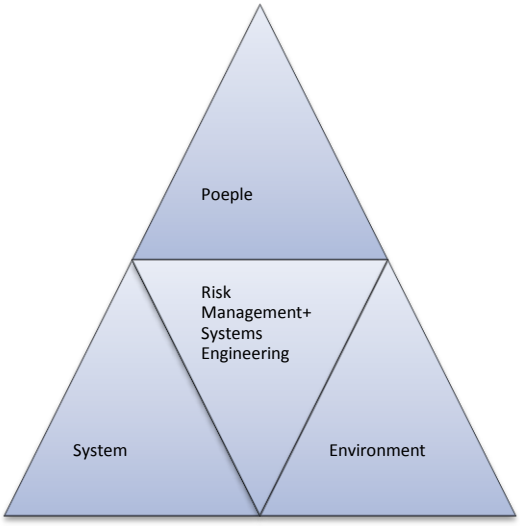

Figure 1. System, environment and people are the three common elements for system design and system safety

B. Safe by design

Safe by design identifies the risky situations and overcome circumstances where (failure in) structure, (mal)function or (mis)use cause harm to human, environment or property. Therefore, the safe by design process emphasizes on both the working structure and failed structure, the proper functions and malfunctions, and finally the proper use and misuse through the design course. The outcome creates specific space for identification of hazard leading to risk assessment and risk reduction plan altering the design for more safety.

V. Safety Cube

Safety Cube summarizes the principle elements for design and design discussed earlier in previous sections. It creates three views for system, operation and time. Further explanations on these views follow next.

- The system view presents the system of interest (SoI), its environment (or super-system), and its components (or sub-systems). In principle, this covers the system, its subsystems, (user)interfaces and competing or cooperating systems.
- The operation view presents the system structure or functions in use. The Interaction of system with people or other systems is an important aspect for the system described here in terms of operation or use. This interaction is often present at all different levels of system, super-system and subsystem.
- The time view presents changes across the time axis. While focusing on a system of interest for the present time is the primary purpose for designers, it is inevitable to explore the history of the system

development (lessons learnt) and consider future developments. While normally the information about the past (ex-generation) is available, the information about the future is mainly in the form of expectations, recommendations, or requirements. For designers, the experience and future insight help designing the system.

VI. EXAMPLE APPLICATION

A typical design for machinery is presented here in this paper to show the safety and design related views.

TABLE 1 summarizes these views for design of machinery. The information presented in this table are example requirements for implementation of ISO 12100 and achieving safety-related certificates. As a result, the information needed for design and safety assessment is presented in one single view through an integral approach.

VII. CONCLUSIONS

Although it has been recommended by seminal references, safety is not an explicit part of the design process commonly used by practitioners. The paper recommends implementation of safety into the design process by using the safety cube. This approach demands for creating a formal space for safety, risk assessment and control plans to alter the original design if necessary. The paper, therefore, attempts to make the safety an explicit and integral part of the design practice.

TABLE 1.
PHYSICAL SYSTEM, ITS USE AND FUNCTIONS IN PAST, PRESENT AND FUTURE

	Past	Present (In use/life time)	Future
Structure/ failure in structure			
Environment or super-systems for SoI	Environment of ex-machine in service	Environment of machine in service	Environment of future machine in service
System of interest (SoI)	Drawing of previous machines	Machinery specification	Expectations for next generation
Subsystems or components of SoI	Component failures of ex-machine in service	Components of machine in service, wear out	Strategic changes in future components
Use/ misuse			
Environment or super-systems for SoI	Transportation, installation or assembly	User specification, information for use	Digitally supported services
System of interest (SoI)	Accident, incident or similar machinery	Different machine operating modes	Keep the machine running all the time
Subsystems or components of SoI	History of damage, noise, vibration, etc.	Different intervention procedures	Low maintenance operations
Functions/ malfunctions			
Environment or super-systems for SoI	Power supply distribution	Housekeeping, environmental requirements	Functions demanded by IoT or smart environment
System of interest (SoI)	Functional faults: (not)tolerated	Start-up, possible states, fault-finding	Remotely controlled operation
Subsystems or components of SoI	Unscheduled stops and recovery	Disturbance in power supply	Self-repaired, self-maintained

REFERENCES

[1] M. Rajabalinejad, G. M. Bonnema, and F. J. A. M. v. 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, 7-10 September, 2015.
[2] G. Pahl, W. Beitz, J. Feldhusen, and K.-H. Grote, *Engineering Design A Systemmatic Approach*. Springer, 2007.
[3] C. Kevin Forsberg and C. Michael Krueger, "Systems Engineering Handbook A Guide For System Life Cycle Processes and Activities." 2007, p.^pp. Pages.
[4] C. A. Ericson, *Hazard Analysis Techniques for System Safety*. John Wiley & Sons, 2005.
[5] D. Kahneman, *Thinking, fast and slow*. Macmillan, 2011.
[6] N. J. Bahr, *System Safety Engineering and risk assessment*. CRC Press, 2014.
[7] *EN-ISO 12100:2010 Safety of machinery - General principles for design - Risk assessment and risk reduction*, 2010.
[8] *MIL-STD-882E: 2012 Department of Defense Standard Practice System Safety*, 2012.
[9] E. Hull, K. Jackson, and J. Dick, *Requirements Engineering*. Springer, 2011.
[10] J. Hesket, "Past, Present, and Future in Design for Industry," *Massachusetts Institute of Technology Design Issues*, vol. 17, no. 1, 2001.
[11] G. G. Porto, "Safety By Design: Ten Lessons From Human Factors Research," *Journal of Healthcare Risk Management*, no. 3, 2001.
[12] M. Rajabalinejad, "Modelling and Prioritization of System Risks in Early Project Phases," *International Journal on Advances in Telecommunications*, vol. 9, no. 3-4, 2016.