MANTECH Publications
Journal of Product Design, Quality Engineering & Technology
Volume 7, Issue 3, September-December 2022

Use of Safety Cube to Assimilate Safety Features in Design

Manisa Irshad Wani[1], Akanksha Mishra[2]
Professor[1], Student[2]
Department of Mechanical Engineering
Sharda University Greater Noida
Email ID: *akanshamishra4@rediffmail.com[2]*

Abstract

During the design process, safety is frequently viewed as a need or a performance indicator, which does not necessarily result in ideally safe products or systems. This article proposes incorporating best safety standards into the design process to enhance the exploration experience for designers and create value for customers. For this goal, frequently used safety standards and design methodologies were examined, and their common blocks were united to produce the Safety Cube. Through an integrated approach, Safety Cube incorporates common blocks for design, hazard detection, risk assessment, and risk reduction. An example application shows how to utilise Safety Cube to build machines.

Keywords*: - Safety, safety cube, design, product, system, machinery*

INTGRODUCTION

Safety in Engineering Design Practice

THIS study expands on the conference paper [1].Safety is frequently viewed as one of the performance metrics in the engineering design process, hopefully among the more significant ones. The major indices for engineering success, as discussed above, are cost, time to market, and quality. In addition to these, the engineering design practice is composed of various phases, beginning with issue analysis, determining requirements, developing ideas and concepts, embodying the chosen concept, detail design, and testing [3]. Similar patterns are followed by other generally recognized techniques, such as the V model in Systems Engineering [4]. In this approach, safety is frequently considered as a criterion that must be met or as one of the indications that must be handled. Furthermore, if

details are available, safety-related procedures are frequently used before and after idea formulation. Common safety procedures, such as Preliminary Hazard Analysis (PHA) is used to alert stakeholders to potential hazards or dangers. Failure Mode and Effect Analysis (FMEA) is a technique that is often used to investigate potential failure situations, assign failure probability, and analyses the repercussions or consequences.

Fault Tree Analysis (FTA) or Event Tree Analysis (ETA) are often used to describe the hierarchy of faults or subsequent events. The core of these methodologies is component failure; a system failure is represented as a logical chain of events or faults. Methods such as the Fishbone diagram, Cause and Effect diagram, and Root Cause Analysis concentrate on the link between danger and probable occurrences. Probabilistic Risk Assessment (PRA) techniques, Bayesian Belief Networks (BBN), or the Incident Tree Method (ITM) [5] can be used to evaluate the likelihood of these incidents. These techniques frequently presume that if a product performs as intended, there will be no failure and the product will be safe. In this context, reliability is equated with safety, and the tools used become incapable of capturing a situation that is unsafe but was not initiated by a failure. When systems become more complex, the flaws in this assumption become more apparent [5]. The following section outlines the issue.

Problem Statement

While designers are focused on creating something that must meet the demands of the client, they must also consider foreseeable abuse scenarios or malfunctions. Due to time or other resource constraints, they may create an erroneous opinion about the safety of their ideas. For example, a short glance at Fig. 1 may lead to the incorrect perception of three linked pipes. This is an illustration of how rapidly designers can think of correct product operations and usage rather than misuse or malfunction scenarios.

In his book "Thinking, Fast and Slow," Daniel Kahneman [6] addresses this quandary in a broader framework. In fact, best practices indicate that regularly used patterns for designers be created in such a way that they encourage designers to think quickly when thinking of functions or solutions and leave no room for designers to consider abuse or malfunction situations [3]. As a result, designers may think slowly while exploring unusual situations for their own creations. To overcome this

issue, safety must be given more consideration during the design process [7]. This research looks at the idea of creating "safety space" throughout the design process. To do this, the building blocks for design, risk, and safety must first be defined, as detailed below.

BUILDING BLOCKS FOR DESIGN AND SAFETY

A. Common Building Blocks

The design process and the safety management process both employ comparable building pieces. References of best practices for systems safety [8, systems engineering [4, machinery safety [9], and requirements engineering [10] were investigated to uncover these common building blocks for design and safety. Systems engineering provides tried-and-true methodologies for integrating key building pieces and controlling hazards. The system safety standard is the most established common technique for investigating system safety principles. The system safety standard outlines the DoD (Department of Defense of the United States of America) strategy to limiting risks and eliminating hazards when practicable [8]. This Standard practice addresses dangers in the design, development, testing, manufacture, use, and disposal of systems, products, equipment, and infrastructure. Furthermore, the worldwide standard ISO12100, a foundational reference for equipment safety, defines important categories for machinery safety evaluation.

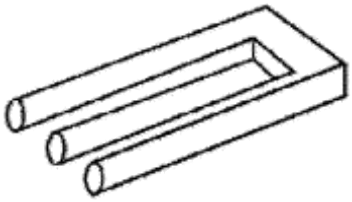

Fig. 1: Blivit illusion drawn by M.C. Escher (Escher Print)

When comparing the approaches outlined above, three common blocks (components) must be included in every design or safety analysis process. As seen in Fig. 2, they are the system, the environment, and the people. Systems engineering and risk management collaborate on these three blocks to enable proper hazard detection and management during system design, implementation, and operation.

As a result, it is clear that the system of interest (SoI) is the key emphasis for designers. The system is made up of subsystems or components and has interfaces with (connections to) the environment or other systems (the so-called super-systems). In addition, the system communicates with individuals (e.g. operation or use). This is expanded upon in the next section.

B. System and Operation

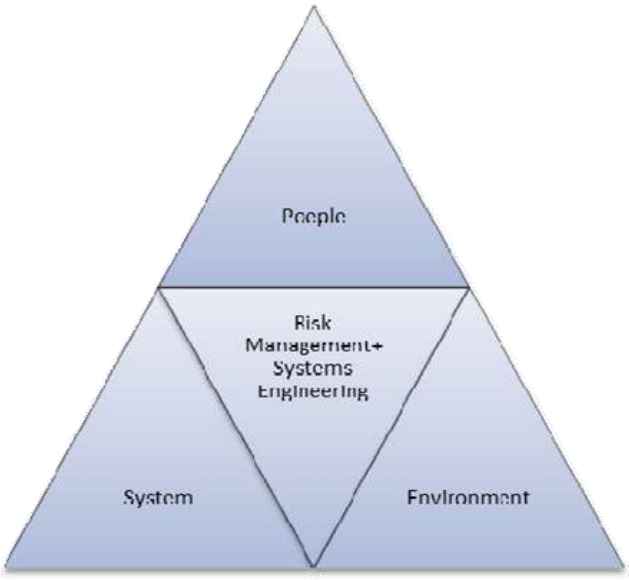

Fig. 2: System, environment and people are the three common elements for system design and system safety.

ISO12100 specifies three primary criteria for assessing the safety of machinery: operation, physical structure, and functions. Structure is required for optimal functioning and usage. While this ISO standard focuses on existing systems, it is impossible not to include past experiences and future predictions. This has been implicitly (and occasionally explicitly) mentioned in standards but has an explicit function in design.

C. Experience and Future Trend

Experience and foresight into the future enable design for the present. Designers must address the effects of time not just over the whole lifespan, but also in previous and future generations. This not only stimulates designers, provides them with rich information, and provides them with further insight, but it is also required by safety requirements. Furthermore, looking into previous design or operating experience, documenting previous accidents or incidents, and considering potential future usage, or future abuse, are all part of normal safety standards.

Meanwhile, researching potential environmental changes and the history of product evolution allows for the development of goods or systems that are more adaptable to environmental changes. Recognizing future trends is commonly acknowledged to play a role in success [11].

As a result, designers must have access to previous systems and think about future advancements. Learning from failures is only feasible if previous failures can be accessed and recommendations for future adjustments can be made. Time is an important consideration for designers. To put greater emphasis on this, these aspects should be highlighted before, throughout, and after the lifetime (or in service). This implies that previous knowledge regarding the three main factors for design and safety, namely system, environment, and people, should be widely available and accessible to designers.

Safe Design

Product design (machines or systems) may be described as the production of anything that will perform the required functions and operations (use). For example, [9] summarizes this in three pillars: structure, function, and usage. However, as described previously in this study, there is frequently no explicit examination of malfunction or misuse throughout the design process. As a solution, risk assessment and risk reduction must be incorporated into the design process [12]. Indeed, if a risk is unknown, it is less likely to be handled properly. If the danger is identified, a designer can devise a method to eliminate the hazard. If removing the danger is not practicable, the designer can control and manage the risk through safeguarding or other supplementary methods. As a result, adequate risk analysis implementation in the design process is likely to increase safety.

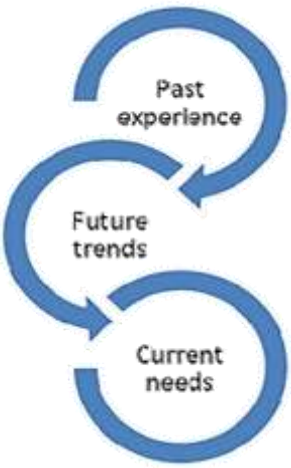

Fig. 3: The experience and future trends guide designers to design for present

Safe by design identifies and overcomes dangerous situations in which (failure in) structure, (mal)function, or (mis)use cause harm to humans, the environment, or property. As a result, the safe by design method focuses both the working and failing structure, correct functions and malfunctions, and lastly, suitable usage and abuse via design. The conclusion establishes a particular place for identifying risks that lead to risk and safety management strategies that adjust the design for greater safety.

Safety Cube

The Safety Cube integrates the main design and safety aspects. This cube may produce many perspectives. A description of different perspectives of the safety cube is shown in Fig. 4.

- The system view displays the system of interest (SoI), its surroundings (or super-system), and its components (or sub-systems). This encompasses the system, its subsystems, (user) interfaces, and competing or cooperating systems in general. This image depicts the interfaces between these components and their surroundings, failures in components or interfaces, and the chain of physical events.

- The operation view depicts how system structure or functions are used in practice. In terms of operation or use, the interaction of the system with humans (or other systems) is a crucial feature for the system described here. This interaction is frequently present at all levels of the system, including super-systems and subsystems. In addition to use, a cautious eye on potential abuse is essential. For example, scenarios for shipping, installation, operation, and recovery processes may occur differently than expected by the user.

- Identifying a correct set of requirements and functions is one of the important performances for system and safety engineers. Examples include system states and defect detection modes. Furthermore, future design expectations, recommendations, or criteria provide a useful set for future designs. These are displayed in the functional view.

- The time view displays changes along the time axis. While the SoI is the major focus for designers at the moment, it is unavoidable to investigate the system's development history (lessons learned) and contemplate future changes. While knowledge about the past (ex-generation) is typically accessible, implicit or explicit information regarding the future trend is required. An application example provides more explanations for various points of view.

Example Application

This paper presents a typical design for equipment to demonstrate the safety and design related perspectives made by a

safety cube. Table I highlights several perspectives on equipment design. The data in this table are examples of considerations for implementing ISO 12100 and obtaining safety-related certifications.

Table I's first three rows describe the system's structural parts, their interactions with one another and the environment, and potential failures. The third column depicts the current state of the system of interest, while the other columns highlight the experience and future aspirations.The system's operation, or its use and misuse, is the subject of the table's second three rows. Experience in areas like as transportation, installation, or system operation, as well as future trends such as low maintenance operation, all contribute to a more resilient design.

Table I's third-three rows highlight system operations, malfunctions, or needs such as startup or failure statuses. This can be housekeeping functions or a disruption in power supply at the super system or subsystem level. Functional defects that were tolerated (or were not tolerated), unscheduled maintenance or disruption, or the recovery process are examples of functional lessons that can be learned. Future developments may include, for example, integration with the internet (IoT), remote operation, and automated fault identification, self-repair and/or self-recovery.As a consequence, the information required for design and safety evaluation is collected and presented comprehensively via Safety Cube.

CONCLUSIONS

Safety is frequently absent from the design approach employed by practitioners or engineers. As a result, people may quickly create assumptions about the safety of their untested designs, which may differ from reality.To provide more room for safety throughout the design process, common blocks between safety and design were found and integrated to form the Safety Cube.

Through the design process, Safety Cube creates room for safety (and hence for risk assessment and control strategies to amend the original design if necessary). It also produces several perspectives for designers, systems engineers, and safety engineers. These perspectives enhance the exploration experience for designers, practitioners, and engineers while also adding value to the final design.

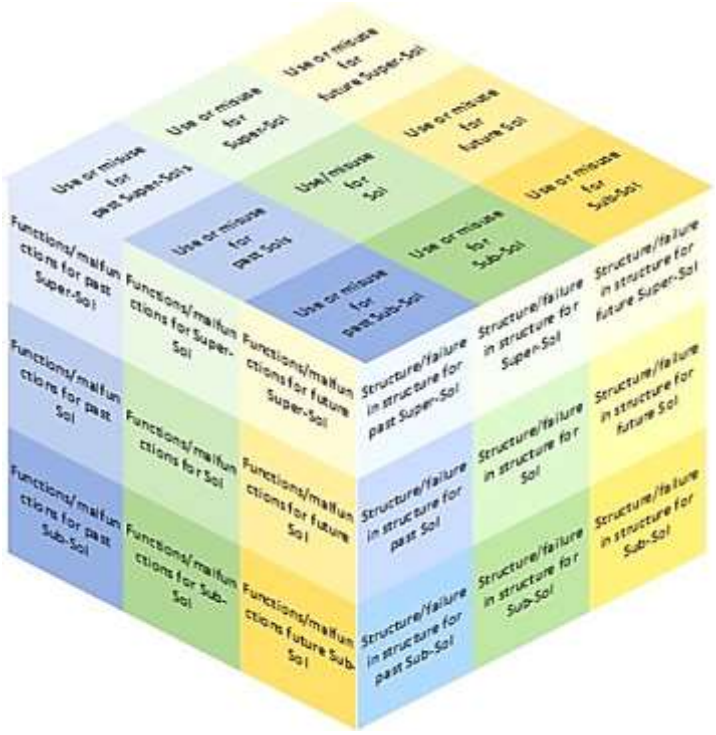

Fig. 4: Visual presentation of the Safety Cube

An example application for equipment design and ISO12100 implementation is successfully given, and future use of this approach is advised.

REFERENCES

1. M. Rajabalinejad, "Incorporation of Safety into Design Process: A Systems Engineering Perspective," in ICSSE 2018: 20th International Conference on Safety and Systems Engineering, Paris, France, 2018, vol. VIII, pp. 1366-1368: WASET.

2. 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.

3. G. Pahl, W. Beitz, J. Feldhusen, and K.-H. Grote, Engineering Design A Systemmatic Approach. Springer, 2007.

4. C. Kevin Forsberg and C. Michael Krueger, "Systems Engineering Handbook A Guide For System Life Cycle Processes and Activities." 2007, p.^pp. Pages.

5. C. A. Ericson, Hazard Analysis Techniques for System Safety. John Wiley & Sons, 2005.

6. D. Kahneman, Thinking, fast and slow. Macmillan, 2011.

7. N. J. Bahr, System Safety Engineering and risk assessment. CRC Press, 2014.

8. MIL-STD-882E: 2012 Department of Defense Standard Practice System Safety, 2012.

9. EN-ISO 12100:2010 Safety of machinery - General principles for designRisk assessment and risk reduction, 2010.

10. E. Hull, K. Jackson, and J. Dick, Requirements Engineering. Springer, 2011.

11. J. Hesket, "Past, Present, and Future in Design for Industry," Massachusetts Institute of Technology Design Issues, vol. 17, no. 1, 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.