SAFETY BY DESIGN

Engineering Products and Systems

Dr. Mohammad Rajabali Nejad

SAFETYCUBE.COM

Safety Cube

Copyright © 2020 Mohammad Rajabali Nejad

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without prior written permission from the copyright holder.

ISBN 978-9-46418-182-1

Key words: safety, design, engineering, product, system, integration, safetycube

Cover: Integration Rainbow merged with the Safety Cubes, designed by the author.

Published and distributed under the imprint of SafetyCube.com

For further information:
visit www.safetycube.com,
email contact@safetycube.com

LEGAL NOTICE
The publisher is not responsible for the use which might be made of following information.

PRINTED IN THE NETHERLANDS

Preface

Spending many years of my career on observing the efforts of engineers, I have seen their struggles for achieving results at the highest possible level, all of this to satisfy their customers.

Their resources were limited. They had to achieve their tasks with what they had. It is a privilege to see how they use their creativity in favour of getting to the best results. That is the exact reason designers require freedom and flexibility for exploring the almost infinite possibilities.

Nevertheless, there is no room to try and error in the competitive environment where expectations are high. Even a single failure may lead to falling behind the other ones. Safety must be well-thought in the course of design. The need for a thorough approach for achieving safety and security in early phases is rather apparent, and this book aims to address the need.

The book intends to implement safety into design. It provides a reference for designers who want to achieve safety and security in their everyday practice, safety engineers who wish to seek a closer relationship with other engineers or developers, and managers who need to find a balance between safety and other performances of the system. The book describes the theory for safe integration and offers a methodology for the complete safety assessment across the full life cycle and different hierarchical levels.

Mohammad Rajabali Nejad
Hengelo, The Netherlands

Contents

Part II. WHO MAKES IT SAFE?

Key Definitions

Cubic engineering refers to engineering a system or product concerning the aspects related to the system or product under consideration, the related environment, the stakeholders, and the possible interactions among these aspects (see Figure 18.1)

Design failure refers to a failure for which the hazard is known to the designer, yet the user or operator is unaware of the hazard or associated risks (see Figure 17.5)

Functional aspect relates to specified action or activity which can be performed by technical means or human beings and has a defined output in response to a defined input (see Section 14.1)

Integral safety refers to both safety and business perspectives where safety is an integral part of the success

Integration engineering concerns the discovery, analysis, learning, planning, designing, developing, executing, managing and monitoring of integration matters across the full product or system life cycle

Integration Rainbow refers to the seven levels of integration which are subsystem, technical system, human-system, sociotechnical system, political, and global integration (see Figure 15.1)

Operational aspect relates to the operational phase of the system or product life cycle (see Section 14.3)

Safe integration is a state of integration where the system, human, and the environment of the system can safely function together and deliver the expected performances.

Safety by design is the process that identifies, assesses, evaluates, removes, controls or communicates possible hazards, hazardous situation or events, and the associated risks through the design process to overcome circumstances where the risks pose a serious threat to humans, the environment or property by design (see Figure 17.1)

Safety by integration targets safe integration by looking into the complete picture, technical and non-technical aspects, internal and external interfaces, past experiences, and foreseeable challenges in order to reduce the risks into a tolerable level

Safety Cube Method integrates the aspects of hierarchy, life cycle, past and fu-

ture together, examines needs, assesses safety-risks, and embeds risk reduction, control, and communication into system architecture and design (see Figure 20)

Safety Cube Theory stipulates six fundamental aspects of safety: the human, the technical system, the environment of the technical system, the interaction of human with the technical system, the interaction of the technical system with the environment, and the interaction of the human with the environment (see Chapter 12)

Safety spiral refers to safety as the foundation for growth through the seven stages of personal safety, social safety, self-esteem, performance, investment, income, and demand for more safety (see Figure 2.1)

Success framework provides an integrated view for the critical success factors through a shared understanding of objectives, cocreation, cointegration, and cooperation considering the four pillars for success which are namely: the user, operation, technology and supplier (see Figure 8.1)

System integration, or integration at the system level, refers to the integration of components, elements or subsystems, or human interactions to realise a system that accomplishes the system objectives

Technical aspect is an aspect related to a technical system which means a product or an assembly of products including the design, implementation, and support documentation (see Section 14.2)

Chapter 1

Introduction

Designers need to be able to innovate. The problems they get and have to solve have often different and sometimes nearly endless ways of solving. The first choices are made fast, but they usually do not change during the full project life cycles and sometimes even several generations after. If these decisions are suitable and beneficial for the project, then nothing is wrong. Still, if the choices are inappropriate for the project, there are going to be negative consequences imposed.

To put it in another way, designers often perceive exploring the broad design choices in early design phases enjoyable, and the designers have the most power to change something in the design of products or systems as well as the safety of those products or systems.

In other words, when the project is in the service, or production phase, the costs of the setback risks are higher than when the project is still a concept. There are many examples to show that the late fault assessment has tremendously increased the cost of lessening setbacks. For illustration, Section 3.7 reviews a few cases where some easy-to prevent failures contributed to national downfalls or caused the most tragic events in our history.

1.1. What is missing?

Even though there is plenty of freedom for exploration and choices, there are constraints in early design phases present as well. Restrictions that happen to be on the resources, however, tend to push the designers to focus on the market-driven performance indicators. These indicators for engineering performances are primarily cost, quality and time-to-market. We know them as the performance triangle.

Safety is not directly present among these performance indicators, but this does not mean that it is absent. Not at all. Safety is perhaps not there explicitly, but it is in their minds, processes, and reports. In the performance triangle for the engineers, safety is a lot influenced by the quality and the costs. Quality products or quality systems are more likely to be safe and reliable. The uncertainty in the performance

of quality products or services is small comparing it to another low(er) quality that is similar, making the possibility of risks or unexpected consequences much less.

There is still a possibility to use a quality product in an unsafe situation, yet people often associate a quality product with a safe one. For example, to make the statement clearer is that a quality car is more likely to be a reliable car than a low-quality vehicle. Alternatively, it is a prevailing thought to think a bulletproof glass is safer than regular glass. Furthermore, paying attention to safety reduces cost, especially in the early stages of design. There are plenty of products that are being taken off the market daily because they are unsafe. For example, every day, the European Commission receives alerts from the member states concerning dangerous products found on the European market. These alerts are sent through the rapid alert system for dangerous non-food products[1].

Next to products, unsafe situations occur daily, and they cause extra and sometimes enormous costs, cost much higher than paying attention to the design or development phases. Looking at it another way, products that are not safe enough according to standards impose liability costs and take the fame of the companies mercilessly. Ikea Malm dresser is an example of enormous consequences of unsafety for customers as well as the producer. This product took the life of six children in the US alone, injured more than 30 children, cost up to six billions of dollars for the company, raised public concerns, defamed the company, and led to angry customers.

In the competitive environment where expectations are high, there is no room to try and error. Even a single failure may lead to falling behind the other ones. Safety must be well-thought and implemented in the course of design. There have been problems started from a cup of coffee for a leading company in public services that got media attention. The company gave coffee to its customers as a side-service to create an enjoyable customer experience. Nevertheless, there was a mistake: the cleaner chose a wrong tablet to clean the coffee machine and accidentally added chemicals to the water reservoir. That injured a customer, then became the news, and influenced the whole company performance. It may be true that serving coffee was not the primary service of this company; however, that changed the entire performance, perception, and reputation.

While these facts explain themselves and are very legitimate, safety is often considered as one of the performance factors with hope among the most important ones in the engineering design process. Producers or service providers that still think that safety-related issues happen only to the others because it has not yet happened to them exist. By underestimating, they will have to learn it the hard way by failing and learning. Besides, safety continues to remain a beneficial source in the engineering performance triangle or engineering design models for practising.

Another way to put this: the commonly practised patterns for designers, recommended by the best practices, are generally made in such a particular way that they encourage designers to think and make decisions quickly when they are thinking

[1]see RAPEX on *https* : *//ec.europa.eu*

of functions or solutions, and they do not create a suitable and vacant space for designers to think about the scenarios where the product is (maliciously) misused or has malfunctioned. As a direct result, this causes the designers to think slow while they explore the various expected scenarios for their designs. Such a design situation is comparable to driving a car through a very narrow way; it is hazardous. It implies that safety needs even more space through the design process.

1.2. Why this book?

This book has a goal to truly shed light and enlighten people about the real importance of safety for the ones who design and in the actual real-life design practice. It describes the phenomenon of safety challenges for designers, includes and reviews the successful design practices for safety, marks the role of designers and policy-makers for having the power to influence safety. And for topping it all, this book offers an advanced method of producing safety assessment and a safe integration a the highest possible levels for products and systems. It provides a short but to the target description of the critical aspects needed for the proper understanding of safety-related matters for design and engineering of systems and products.

1.3. Threes and sevens

The key messages from across this book are in the form of threes and sevens. The main factors in the form of threes are:

3

Metrics for measuring the engineering performance are cost, time to the market and quality.
Ingredients for safety are human, technical system and environment.
Aspects that contribute to safety throughout the entire product or system life cycle are functional, technical and operational.

The main factors in the form of sevens are:

7

Steps of safety spiral are personal safety, social safety, self-esteem, performance, investment, income, and demand for safety.
Levels of hierarchy for safe integration are subsystems, technical systems, human-systems, the system of systems, sociotechnical systems, political systems, and the global system.
Aspects covered by the Safety Cube method, which are three fundamental elements (the human, the technical system, the environment), and four interactions among them.

1.4. Organisation of the book

This book has five different parts. The first part motivates the concept of 'safety by design'. It provides answers to the questions like 'why safety?', 'why design?', or 'why safety by design?'. The second part of the book covers the matter of responsibilities for dealing with safety. It describes the most competent people for making the society a safer place to live in and explains their challenges or strategies. Part three takes a rather deep and fundamental approach towards safety and explains the Safety Cube Theory. That is for tackling safety matters through an integrated social, technical, and environmental approach. The next part reviews the paradigm, process, and requirements for safety by design. The last part of this book explains how-to for safety by design and explains the Safety Cube Method, along with the other relevant and commonly practised processes and techniques.

Part I

WHY SAFETY BY DESIGN?