Preface

The following book is the result of over 20 years of professional experience in the field of functional safety. When I started my career after graduating as an engineer in 1992, plant engineering and construction was highly influenced by catastrophic events such as 'Bhopal' and 'Seveso'. The first set of rules and regulation which led later to IEC 61508 and ISO 26262 that addressed the issue of functional safety was the VDI/VDE guideline 2180 "Sicherung von Anlagen der Verfahrenstechnik; Safeguarding of industrial process plants by means of process control engineering" from 1966. However, it only covered the mere process of how to establish a safe environment in such facilities. In 1984 the differentiation between operational safety and safety equipment as well as monitoring and safeguarding equipment were added to the guideline. Thereafter, DIN VDE 31000—"General guide for designing of technical equipment to satisfy safety requirements" got published, which elaborated on the correlation between risk, safety and danger and introduced tolerable risk. At this time machinery standards, which prohibited the use of micro-controller for safety applications, were still common. However, an established market for safety-related control systems already existed. Different rules and standards defined the base of requirements for examinations, certifications and design of such systems. Those requirements were scaled in requirement classes (AK 1-8) according to DIN V 19250, independently from application or technology and explained a qualitative risk assessment procedure with the help of a risk graph.

In 1990 DIN V VDE 0801 "Principles for computers in safety-related systems" was released and in its revision of 1994 terms such as 'well-proven design principles' and the usage of 'consideration item' were added. By then, 'redundancy' was the only known answer to the various risk and requirement classes. However, various measuring principles were already used in measurement and control system engineering in order to detect hazardous situations early.

The technical rules for steam or the regulations for pressure vessels already required the redundant measurement of steam and temperature due to safety issues. Even the German Water Ecology Act mentioned the filling quantity limit from tanks according to regulations as well as the independent overfill safety device as a

safety measure. A lot of those safety principals emerged from the safety standards of plant operators and even served as a foundation for official permits or releases. Even before in the early sixties DGAC (Direction General de L´Aviation Civil in France), CAA (Civil Aviation Authority) in Great Britain or FAA (Federal Aviation Administration) in USA and the military and space industry defined regulations about "Functional Safety", but those were not in the focus of the development of standards like IEC 61508 and ISO 26262. Due to today's discussion about 'autonomous' or 'automated' driving, those standards become more and more in the focus of the automotive industry. Especially topics such as safety-in-use, fail-operational, security, operational safety are becoming important for future revisions of ISO 26262.

In 1998, at the time I started my job as a sales manager of safety-related control systems, discussions over the early drafts of IEC 61508 took place, especially in countries such as England, the Netherlands and Norway. The scalable redundancy was a known concept so the discussion focused on the distinction between redundancy for safety and availability. Micro-controllers were coupled according to the lockstep principle and could change the program sequence or control logistics during runtime of a plant. Programming software was available, which allowed configuring the safety logic within a defined runtime environment.

The publication of IEC 61508 introduced a lifecycle approach for safety systems. Additionally, it formulated a process approach for product development and the relations to quality management systems were formulated.

During my graduate studies at the Faculty of Business and Economy at the University of Basel, I was able to hear a lecture of Prof. Dr. Walter Masing, who had a huge impact on quality management systems in Germany. The introduction of implemented diagnostics for the safety of functions and the electric carrier systems of these functions, respectively, broadened the view of safety architecture. In 1998, I introduced the first passive electronic system in Birmingham, which until SIL 4 was certified according to IEC 61508. I witnessed when the first certificate for a single-channel control system got signed after SafeTronic in 1999, which took place in the facilities of TÜV-Süd. This system was completely developed according to IEC 61508.

During VDMA-events (Verein Deutscher Machinen und Anlagenbauer; German machinery and plant engineering association) I reported on my experiences with IEC 61508 regarding plant engineering and its influence on the development of safety-related control systems. In these days, the machinery engineering industry was still heavily influenced by relay technology. Nobody wanted to believe that software-based safety technology would change the industry so drastically and in such a short time by providing new solutions and change existing systems. In 2001 I became the head of product management; the main task was to find new applications for new safety systems. Another main topic was 'safe network technology', which was so far based on serial link data busses. The challenge was to realize distributed and decentralized safety systems based on dynamic, or situation-, or condition-dependent safety algorithm. The only possible solution turned out to be 'Ethernet'. It was important to make the existing computer or data technology for

safety technology easily manageable. In Norway, in the context of diploma theses, safety control systems got distributed, which exchanged safety-relevant data within the data network of the Norwegian mineral oil association “Statoil”. The experiences with the data transfer over satellites between oil platforms and plants ashore or between Norway and Germany as well as various solutions to the pipeline monitoring via radio systems proved that the safety technical data systems were also able to be realized based on Ethernet.

Hans-Leo Ross

http://www.springer.com/978-3-319-33360-1

Functional Safety for Road Vehicles
New Challenges and Solutions for E-mobility and Automated Driving
Ross, H.-L.
2016, XV, 269 p. 128 illus., 101 illus. in color.,
Hardcover
ISBN: 978-3-319-33360-1