Hans-Leo Ross

Safety for Future Transport and Mobility

Springer

Safety for Future Transport and Mobility

Hans-Leo Ross

Safety for Future Transport and Mobility

Springer

Hans-Leo Ross
Lorsch, Hessen, Germany

ISBN 978-3-030-54882-7 ISBN 978-3-030-54883-4 (eBook)
https://doi.org/10.1007/978-3-030-54883-4

The work was first published in 2014 by Carl Hanser Verlag München Wien with the following title: *Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen*

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

During the last pages of this book, my father died after a long illness at the age of 89 years. Of course, he had a great influence on my thinking and my professional development. He was born in the years between the two world wars, and his childhood was marked by the aftermath of the First World War and people mourned the Imperial Era.

At that time, Göttingen was still considered the technical centre of science, and the language of science was still German.

At the very beginning, I would like to apologise to all readers for thinking like a German when writing this book. I live my daily life in German, with my children and my wife I only speak German. Most of the conversations about the topics in this book I have conducted in German. I continue to try regular contact with China, France, England and Scandinavia and with companions from the USA, but they all confirm that I think typically German. With many of these people, I speak English, but I still think the complex matters in German thoughts. It is an insight of this book that the language context is a major influence on the understanding of the content. Norbert Wiener and the scholars of these days also knew that the linguistic context has an essential influence on what and how you understand something. The mathematicians had an intensive exchange with the universities and professors in China, and by reflection and communication the common understanding was formed.

The parents of Norbert Wiener had decided to emigrate to America, as so many Jewish families had to do. He himself not only conducted an intensive exchange with the scholars in Germany, but also with France, England and Russia, forming networks such as the philosophical network of the Vienna Circle (Wiener Kreis). However, the new rising power in Asia was China, which already offered interesting aspects to many scholars. China offered a good ground for the scholars and the exchange with Japan soon proved to be just as difficult because the harbingers of the Second World War were in the offing. My father was able to attend a gymnasium for a few more years, but after the war, the focus was on feeding the family and educating the younger siblings. After the Second World War, Germany was divided, we in the West oriented ourselves more towards France and the USA;

the East oriented itself towards Russia and a few made trips to communist China. Aeronautics and space travel now developed in the English language, and in the development of cybernetics, the Russians were more likely to stand on their own feet. German was lost as a scientific language.

My father became first a truck driver, later a CNC miller and machinist in a chemical plant. Later on, he was very active in a large enterprise for the unions and the works council. All this influenced my own professional career. Even as a student, I worked in chemical plants. In one plant, hydrogen was also produced by electrolysis and used for hydrogen peroxide and other bleaching agents. Some chemicals from the plants were used for catalysts. During my professional education, I learned how to maintain and install telecommunication systems. At that time, telecommunication exchange and switching centres still existed in large buildings with relay technology. We were allowed to look into the future during our apprenticeship and practised the first programs on a Sinclair computer with a Z80 processor. During my basic studies, IT technology was still called “electronic data processing”, and we learned the basics of algorithms and embedded control on UNIX machines or with assembler on 8-bit controller. During my studies of communication engineering, the iron curtain opened and Germany was reunited. As part of my diploma thesis, I built and programmed a three-phase converter to test the performance of IGBTs and investigate their behaviour under massive EMC interference. A special challenge was a robust software that could control the inverter with very precise pulse widths in the audible frequency band using 8-bit controllers.

After my studies of electrical engineering, I first had enough and did not want to fill my head with more wisdom. But as a pensioner, I wanted to study philosophy again. My father followed my professional career, but now he mostly just listened to me or told me about his experiences and observations when the first cars were developed into a Volkswagen or sporty racing cars. The one or other story from his time as a truck driver was also always present. He did not know the scientific basics of all process engineering topics, but he always said, a manager can say what he wants, a physical law cannot be overridden. With the law of conservation of energy, nobody could contradict him, with everything else we developed the ambition to sound out the limits of physics.

My first job as an engineer was in plant construction at an engineering contractor with a focus on liquid–gas process engineering. My first own project was an automatic rail tank wagon loading system in a refinery. My boss said it is not a big project because it was only about the release for loading and automation of the transfer locomotive. About this mistake, I got to know the safety engineering. It was actually only a matter of a few signals within the nominal function, but the safety analyses and measures taken to ensure safety were enormous. Therefore, I quickly became a safety expert in the automation projects. The experienced engineers preferred to keep their distance from the safety technology. Another interesting project was the planning and implementation of the first safety concept for an LPG liquid–gas tanker according to the IMCO Gas Code. At that time, the current machinery directive still stated that software-based safety functions were not permitted. All shutdown systems consisted of relay technology. Here, of course, the connection between reliability and safety was quickly learned. The one or other redundancy naturally helped to design the safety technology in such a way that the gas system on the ship was not permanently in a safe state and was therefore not available for the intended function. At times, I also headed the service department for the gas tankers, so in addition to the product liability aspects, I also became familiar with the lifecycle issues and the business aspects. Here, the availability of transportability was the decisive factor, so investments in maintenance and service were made with foresight. Afterwards, I changed to the sales department of the still leading manufacturer of safety-related safety control systems. I was responsible for the UK, Northern and Eastern Europe. In particular, the offshore and pipeline business was an essential aspect of my sales area. Among other things, I was involved in the automation and safeguarding of Europipe 2 or in projects for the remote control of unmanned oil platforms or shuttle tankers. Here in Norway, satellite technology or the IT networks of the oil companies were also used to implement safety functions. During my time in sales, I studied business administration with a focus on marketing on a part-time basis at the University of Basel, because I wanted to better understand the basics of business relationships. Moreover, I was able to put legal topics, innovation and technology management, etc., into practice very quickly. In Norway and the UK, the new emerging IEC 61508 was discussed very intensively. I had active contact with the fathers of this standard. In my company, there were many people who also developed the German derivation of the standard, the VDE 803. The then current safety control system is still the basis for the architecture metrics in this standard today. Since I returned from my sales trips permanently with new safety requirements, I took over as head of product management. Here, new safety concepts were developed and the topic of safe Ethernet was systematically implemented in products. Thus, we developed the safety technology from the relay-based approach of that time into safe network technology.

In the period around the turn of the millennium, electronics were also used more and more intensively in automotive engineering and electronics were now also needed as a protection and safety mechanism. I changed to the automotive industry and was now responsible for setting up the organisational structures for the development of safety technology at Continental. In my first working week, I was already involved in customer discussions for an active front steering system, a by-wire steering system, attended my first FAKRA meeting and was involved in the escalations around EHB, a by-wire brake system. FAKRA was a department of the German Automobile Association (VDA) that developed the vehicle safety standards. Later, I took over the leadership of the German mirror committee, which developed the ISO 26262. After the merger with Siemens VDO, I also took over the management of the corporate engineering process, methods and tool department. In 2011, my twins were born and in 2013 my daughter saw the light of day. While the boys are gathering their first experiences as citizens of the earth, I wrote my first book about the experiences and insights into functional safety. In the context of electromobility, it quickly became apparent that the regulations for high voltage and touch protection showed that legal regulations were necessary in order to give electromobility the necessary safety. The SimTD field test showed the first challenges for automated driving. It soon became clear that a functional safety standard would not be sufficient for the targets of automated driving. As in the case of E-mobility, the homologation regulations had to be adapted. However, all traffic regulations and the basis of the homologation were based on the Vienna Convention. There, the driver or the guide of draught animals was named as the person responsible for behaviour in road traffic. Now the vehicle should be guided by a system in public road traffic. It was necessary to initiate worldwide working groups to obtain a possible revision of this worldwide basis. In 2016, a change of the Vienna Convention came into force, which allows system driving in public roads. However, that was just the starting point; the driver still plays a significant role. The approval regulation UN ECE R79 was considered the basis for the approval of vehicles, especially the appendix 6 allows an override by electronic systems, which was already used for the by-wire systems several times, had to be revised. Furthermore, the regulation did limit the allowed steering assist power and defined several speed limits for electronic steering functions. The driving was only allowed hands-on, and hands-free driving was forbidden in most national homologation standards. Working groups consisting of functional safety and homologation experts start with the proposals for modification, and under the umbrella of UN ECE the basics are still under development. National implementations and harmonisations with existing regulations start. The outcome of currently pending and future proceedings cannot be predicted with any certainty, so that reliable regulations are not mature enough for design of acceptable safety functions yet.

In my second book, I published in English language, and here I already contributed more about software security than what was described in ISO 26262. At that time, we did not think that we needed such complex safety standards as the aviation industry, but more than what was written in ISO 26262 was certainly necessary.

When the standard was published, I wanted to prove to myself that safety engineering is not just processes and methods. I switched to a Korean supplier who was about to set up his new development centre for Europe. Here I was primarily responsible for cross-functional development. This task included setting up the entire development infrastructure for chassis systems and setting up corresponding development teams. A team had to be set up that could develop base software for electronic braking systems in accordance with the safety regulations, standards and AUTOSAR compatible. Furthermore, projects were acquired for electronic parking brake systems that were integrated into Bosch or Continental Brake Systems. A basic development and a development for electronic series products naturally required a completely different process landscape. At the beginning, I also took over the management of ESP development until the main responsible person for ESP development in Europe could be taken on board. After the successful acquisition of several series projects and joint basic developments with the German vehicle manufacturers, the Koreans decided to transfer the basic development back to Korea. I found a new challenge at Bosch Engineering a safe German port also for my family. Service for safety was already an interesting aspect during my time in the plant construction business.

During my time in sales, I had already acquired the sport pilot licence (PPLA), so I was pleased to take over the coordination of the safety activities of Bosch General Aviation Technology. Applying a vehicle motor management system for an aviation propulsion system taught me what safe availability really means. In addition to the flight area, I also coordinated the security activities for the service area automotive engineering and for the connectivity activities. On this topic, the consulting activity and the development of security concepts for Automated Valet Parking was a very valuable experience. In these areas of application, the legal safety aspects again became the focus of my work. Not only the extremely legal-oriented processes in the aviation industry, but also the massive differences between the legal regulations in Europe and North America posed a challenge. In the field of electromobility, people suddenly looked at China to see with astonishment what high standards were being established there. Many aspects of standards were transformed into laws or legal recommendations in China. My third book was in German again, where the German road traffic act was at the beginning of all considerations. I already wrote a lot about control engineering and the challenge that the vehicle control systems had to change to make the dream of automated driving come true. I received a further boost from the fact that I was able to support a lecture series at the Heilbronn University on the subject of "functional safety". I really enjoyed my role as a lecturer. This gave me a closer connection to science, and I was able to write some good theses, especially on the topics of control engineering and software engineering, and I got to know great experts and promising students. This also reawakened my interest in cybernetics. During my studies, the term cybernetics came up again and again, but I always pushed it too far into the branch of philosophy, which I only wanted to deal with later. In a Christmas lecture, I discussed the benefits of E2E machine learning with the students, it was great what aspects the students brought to the topic.

While 10 years ago, it was thought that automation was an evaluative process resulting from driver assistance, it has now become clear that automation is more of a disruptive development.

Especially, the relation to the requirements of the operational safety concept showed essential insights into automated driving. In the context of vehicle safety, several customer projects were tackled where start-ups could be helped to enter the field of E-mobility. Series concepts for the E-powertrain with range extender were also developed for established customers. A special experience was the activities in the field of fuel cell technology. Safety concepts for the propulsion, charging and storage of hydrogen in trucks were developed for an American company. On my many trips to the West Coast of the USA, I met many old friends of safety technology and also new people who are dealing with completely new ideas of vehicle technology and its automation. Whether it was technology that originated in graphics cards for PCs or car manufacturers who wanted to create entire cars from the 3D printer on customer demand, all this broadened my horizon immensely. With the 2018 revision of ISO 26262, not only commercial vehicles came in the focus of the standard, also ASICs and FPGAs, etc. Here I was able to adapt to support the new software and safety processes to the new technology and integrating new microcontroller concepts such as CPUs according to the ARM specification. This was applied to the development of lidar technology as well as to the use of new hardware concepts such as many cores or hardware accelerators for artificial intelligence. At the beginning of 2019, I moved to the central engineering department and, in addition to vehicle safety, was involved in new areas of application for safety technology. In the course of this activity, one can deal very intensively with the state of science and technology, not only for reasons of product liability. The idea that this book brought the subject of cybernetics beyond the legal limits, and thus the limits of social acceptance, arose from my disposition to search for the ultimate answer or origin. In my search for possible Ph.D. fathers for a topic on how to relate the behaviour of the vehicle to the people acting in road traffic, I was repeatedly reminded of the fundamentals of cybernetics. But communication technology, control engineering and the state of the art in safety engineering did not provide an adequate answer. Nevertheless, the discussions with the professors and the thesis on risk analysis provided me with a good framework to consolidate my image of automation in mobility.

Besides the law of conservation of energy, we also know the law of conservation of momentum from physics. Today, many people fear the conservation of information theorem. We have to deal with all these conservation laws and learn to control the risks; otherwise, we will not be able to get a hold of the technology. All these conservation laws can be put into a different context again and again, how one then adds the necessary energy to a system can happen in many different ways, where one can let off steam as an engineer. Nevertheless, such fundamentals of laws, like the Vienna Convention, cannot be completely abolished or overridden. It is a way of preserving information, which has been in people's minds for generations, and on which people's sense of justice is based. However, the better we understand such principles, the more likely we are to find solutions that we can introduce for the benefit of humankind and whose risks we can assess appropriately.

My father saw his task in providing a good home for the family, and we did not have to experience a lack of essential things. If he recognised a lack, he often only showed us a way how we ourselves could acquire the necessary means or the necessary knowledge. My mother has always been the organising hand, who also took care of my father until the very last day. She kept the household budget together and taught us how to use the available resources sensibly.

My father died in the midst of the turmoil of the corona pandemic. In the end, it was hard for me to make him understand all these connections. In his last days, he continued to ask me when we would finally bring electric Volkswagens on the road and how long it would take with the fuel cell. Unfortunately, I was no more able to answer him these questions.

Words of Thanks

Unfortunately, I could not thank to particular persons, because I would not be able to give them a weighting and I would have forgotten an essential person anyway. Beside my parents, my children and wife, I had so many exciting experiences with friends, colleges, professors, students who gave me a lot of reflexion to build up my mind for this book. Especially, the digital media are impressive, so that you could get in contact with people all over the world and what kind of feedback you got from the social media. However, the personal contact is during many rounds, in workshops, at conferences, or when we met just for discussions in a restaurant. For example, I met people from all over the world in a beautiful restaurant in my hometown Lorsch, and we discussed in this beautiful small town about our future ideas in regards to mobility and communication. During the corona lockdown, we established even a digital exchange with experts from aviation and automotive industry. Some of the experts did enjoy their beer during that fruitful exchange, since they did not need to return by car afterwards.

My memories are with my father and my younger brother, who are now reunited in heaven. In my thoughts, they are also united with the many great experts from whom I have learned so much. The feedback from the deceased I must now collect in my imagination. What might they have thought about this book?

Lorsch, Germany Hans-Leo Ross

Introduction

My first book did focus more on the standards for safety and addresses methods how to develop safety mechanisms for automotive electronics. The historical and philosophical background has often been reflected upon in previous books. In this book, special emphasis is placed on cybernetics, which is considered the mother of control engineering, communications engineering and automation technology. The derivations of cybernetics into sociology give us many indications of how we can evaluate human behaviour. The origin of many methods from today's system engineering comes from people who have made a name for themselves in the further development of cybernetics. The methods and principles have established themselves in other industries and fields of application. Such methods and principles cannot be transferred directly into a new context, but they certainly offer different perspectives and approaches to thinking about a problem in a completely different way. Cybernetics has also given us ideas for predicting the future or even for travelling into the future or past. Although fortune telling is not a proven means of safety, there have always been warlords in history who listened to oracles, fortune-tellers and shamans more than to their strategists. Systematic use of predictive methods, however, must be applied to the intended functionality as well as to the possible behaviour in case of failure; otherwise, we are not able to build a safety argumentation. Today, strategists have learned to include such evaluations and uncertainties in their strategic planning. Unfortunately, populism is still heard despite today's clarification. Based on systematic methods, the populism could be exposed as charlatanism.

Due to corona and the diesel gate, the society seems to change their mobility preferences. At the beginning of the new millennium, the idea of driver assistance systems was to be developed into autonomous vehicles. These were intended to make the driver's essential tasks of driving easier at first and to reduce them later on. This was to be achieved through evolutionary growth based on existing technology. In recent years, we became more and more aware that the idea of a sustainable technology had to become more and more a technological revolution in order to actually make the new functions suitable for humans. Even more, the society and consequently the authorities did not accept that autonomous vehicles provide safer road traffic just by automation of driver functions. The engineers realised that a human driver does much more things during driving, as the current systems based on today’s technology could ever realise. At the beginning, it was thought that it would be sufficient to realise the human brain and its functions by increasing the computing power for technical systems. The microcontrollers were enhanced by microprocessors from server technology, and the technology of graphics cards was used to provide additional functionality. Automotive microcontrollers and microprocessors usually still work with program memory, as John von Neumann had suggested a hundred years ago. On such controllers with von Neumann architectures, there are many new ideas about artificial intelligence or there are many offers for machine learning software solutions. Most of the vehicles are using current control units with traditional software on their actuators especially for brake and steering systems. The EE architecture for electrical energy and for the communication base is still on the platforms for motor vehicles with combustion engines. Whenever various parties implement new safety or security features, the communication gets less reliable due to timing latencies and logical inconstancies. Network technology has not really found its way into cars yet, most communication nodes are still very similar to CAN bus architectures. Especially, the existing ESP systems or steering assistance systems have not yet become remote controlled or by-wire braking or steering systems. Even the “active front steering systems” developed 20 years ago are only used to a small extent in the vehicle, mostly there are still three-phase power steering assist systems where the driver has to be held responsible for certain errors as a fallback level. Unfortunately, it must be said that today’s system approaches by far do not meet the requirements to actually automate such human capabilities. The ability to orientate oneself in road traffic, to make the right decisions in situations, or even to avoid a child who suddenly runs onto the road in front of a school like a reflection, cannot be provided by today’s vehicle systems. There is a lot of talk about uncertainty, imponderability and high complexity, but the sensors, the algorithms for object or environment perception as well as the actuators, cannot fulfil the required functions by far. Human perception, the human nervous system and intuitive reaction do not need 18 years of training for nothing before a human driver is ready to drive a car in traffic. Although national traffic and safety authorities motivate industry to find appropriate solutions, they require at least the same level of safety as for traffic with human drivers. Accident statistics are repeatedly shown to indicate that systems can control a vehicle far more reliably than the average motorist. However, research into the causes of these accidents does not necessarily show cognitive misconduct as the cause of the many traffic accidents, but speeding, risky overtaking, stress, alcohol, fatigue and so on are often cited as the primary causes. This is often countered by the fact that systems always behave deterministically, as the developers intended, and therefore, all these factors are no longer considered as causes of accidents in a system-controlled vehicle. In other words, one tries to argue that the automation system should be allowed to have the same accident statistics as the human driver. Even if one or the other state order is inclined to such arguments, society is questioning whether such positive risk balance is acceptable. For years, the automotive industry has been telling us that speed, more power, more interior space, higher seating position and increased comfort were the non-plus-ultra of the automotive industry. The fast and powerful SUVs had to be safe and the driver allowed himself riskier driving manoeuvres. Trucks with a speed limit of 80km/h were not accepted as well as a sports car that was locked below the 250km/h limit. Now such limits are being massively questioned by consumer protectionists, environmental associations and also traffic experts. Is 30km/h sufficient in city centres? Will such measures reduce particulate matter? Some manufacturers hope to increase their position in the market with environmentally conscious vehicles, others have already buried the economic viability of individual mobility. Can we only save our cities from collapse by reducing traffic or will this turn our inner cities into ghost towns and we have to get used to images like Detroit in Europe? Perhaps the renaturation of American cities will also become a positive example for Europe. Where is society's idea of safety heading? In Asia, more and more programs are being set up to bring together large numbers of people in a socially acceptable way in a small area to create a feel-good community. Entire residential areas are methodically planned and implemented on the basis of human-centric design. Disabled, elderly people, children should remain safe and mobile without impairment or adverse effects to the mobility and freedom of others. Express roads are planned to provide an optimal traffic flow, partly underground, so that pedestrians and cyclists have their own traffic space on the surface. This means that such expressways can be adapted more easily for automated driving functions. The car traffic moves in completely different lanes and levels, thus the risk of accidents between road users of different strengths is clearly reduced. In the Arabic countries, entire underground cities are planned; football stadiums will also be accessible from the underground and get air-conditioned. Each type of transport gets its own route. Will this also be a solution for Europe? Will our society accept such huge construction projects? Probably not in Europe. Is Europe therefore falling increasingly behind in terms of future mobility concepts? But why only think about tunnels, why not build upwards? We know bridges over bridges, motorway junctions over several levels from the USA. Does one feel comfortable in such cities? Not really. But there are new solutions to this problem, why build bridges over bridges, why not fly directly? The fuel cell can also be built-in aeroplanes, already more than a hundred years ago zeppelins flew with hydrogen. There is enough sun, then let us use the sun's energy to electrolyse hydrogen. Then air taxis will fly from one skyscraper to another. What a great show, the whole sky full of silent air taxis powered by electric motors. The noise of the rotor blades will be reduced to a minimum with artificial intelligence, noise will not be a problem. There will be no accidents, air traffic is already safer than individual road traffic. Maybe hydrogen will also be used in silent rocket propulsion systems to bridge larger distances between continents. Such rocket engines only need to be used to shoot the transport capsule into the atmosphere, after which it can glide to earth at the desired point without external energy. Will we love cities like this, where the big aeroplanes fly in swarms around our ears? Well, in the Arab cities, it will be too hot to feel comfortable on the surface anyway, so the swarms of aircraft would not seriously disturb anyone and in principle would not endanger anyone. In the deserts, solar energy is enough and people will never really feel comfortable in such areas. So why not use such areas to advance the basics for new technologies? These aspects would have been considered cynical in 2019, but many misjudgements and over-motivated forecasts, especially for the automotive industry, will become more transparent due to the corona crisis. Of course, the individual citizen lacks an orientation, the scientists and scholars are behaving cautiously, and the politicians try to save what can be saved. Some very populist and some with slogans of hope. Oren Harari made us already a bridge from the last industrial revolution transparent: "The electric light did not come from the continuous improvement of candles". At the moment, people like to hear sentences like: "Every crisis is also an opportunity!".

One can of course follow such slogans as: "Every business is a software business now", but Dean Leffingwell did not mean you can solve any problem with software. Thomas Watson forecasted 50 years ago: "I think there is a market for maybe five computers worldwide". He never expected that people use the opportunity to develop their own market and that they saw in the computer the chance for progress and new business. In Chap. 3 of the book, I try to bring some first experience with a networked nation from Russia, the idea of a digital nation—Cybertonia. As early as the 1950s, ideas began to be developed to network the whole country. What was an advantage for central control was also an opportunity for productive local economic cells. This means that these local cells could have developed their own intelligence. From an economic point of view, Peter Bartels coined the phrase: "Anyone who believes that they can master digitization in isolation will find it difficult in a networked world. Networking includes competition".

Also, in China, they see digitization as a great opportunity for developing the nation. They never even tried to attack the Western autoindustry with their own combustion engine concept. Instead, the future was seen in the electric motor, which initially relied solely on battery electric vehicles and now also on hydrogen, and the fuel cell technology makes significant progress. In addition to this, China has also secured access to raw materials such as rare earths, lithium and cobalt. worldwide. The Chinese communication companies are world leaders, and the whole world is thinking about how to implement a communication strategy in the nations that is independent of Chinese technology. Chinese wisdom goes well with this: "When the wind of change blows, some people build walls, others build windmills". Of course, everyone thought that with the industrialisation of course China primarily thinks of building the Great Wall of China higher and higher, but here we were wrong. In the digital age, you will not be able to make progress through walls, this is only being attempted at the border with Mexico. In the digital age, you will have to learn that progress can only be achieved with maximum freedom, but limited by the ability to control it through the organisation. This goes with the quote from Melvin E. Conway: "Organizations which design systems are constrained to produce designs which are copies of the communication structures of these organizations", which we can still attribute to the EE architectures of our cars today. But that also means that with today's organisational structures, we can only try to stick to the old principles and cannot make any real progress. But what will our mobility look like in the future? How do you reconcile digitization and mobility? To make money with the new technology one day, a market has to be created again. The organisational structures have to be adapted to the needs of the market. The need for internal combustion engines will no longer excite anyone. Nevertheless, today's car will have to meet our mobility needs for at least another 10 years. But innovations are no longer expected in this area, so the fuel-powered car will only be able to prolong its lifecycle somewhat through hybridization. But there is a discrepancy between digitization and mobility. The radio technology enables us to overcome distances very well and communicate virtually, but we will not be able to exchange affection and feelings. Apparently, there is an essential aspect behind all future products and values, which could be formulated as follows: "In a digital world, what will be most valuable one day that cannot be digitized".

What are the chances of finding the new markets? One of the often-demanded needs is "safety". In German as well as in Chinese language, there is only one word for safety and security. How the two terms are distinguished from each other is not elucidated in any legislation, in the different social classes, professions and in the different languages. On the one hand, we speak of social security, on the other hand we speak of safety in the sense of accident prevention. Here in the book, the term safety is used as a generic term under the aspect that cybersecurity is an essential prerequisite for safety. In the technical sense, the term "dependability" is also often used as an umbrella term, but this term has not yet found a clear definition in the automotive world. Safety and security are demanded, requested and propagated by many parties, beneficiaries or so-called stakeholders in the mobility society. The need for safety behind these demands is quite heterogenic. Especially through populism and lobbying, primary needs often take a back seat, and the press also has a strong influence on opinion making. The safety need of the individual is in a different relationship than the safety need of society. Investment security, contract security, location security and trade security are terms used to describe hygienic factors to safeguard business. But also, terms like trust, reliability, loyalty, etc., are demands for good business partners. Threats, dangers and hazards are used to articulate the opposite, to say what one does not want. Here we experience again and again that the feeling of safety and security often contains a contradiction in itself. A sheltered environment is often a preferred safety feature. The sheep are protected from the wolf. A person who feels permanently observed becomes more and more insecure in his behaviour. An environment that is too closely monitored restricts the freedom of the individual, and when organised on a large scale, it restricts the freedom of an entire society. Here one finds another term, which is defined very differently, the term protection. How does protection relate to safety? Is protection a safety mechanism? What is the generic term, how do the terms differ? In addition to the fuzziness of the term safety, the relation to risk is correspondingly fuzzy. The perceived risk of the individual and the socially accepted risk are very different parameters, which are often understood very differently in the development of technical systems and are applied very differently in the argumentations. When developing a new product, one must be guided by the socially accepted risk.

Many of these questions and definitions have not been clarified for society and industry, and many initiatives are needed to find our way into the new mobility. In this book, aspects of how to grasp the challenges and make them transparent will be highlighted. The book does not describe solutions but only gives hints on the right way to go in order to find solutions. Often a solution is simply offered for discussion. These are many questions about the automobile market or the mobility market of the future as such. The question arises immediately: What does this have to do with safety? Many safety guidelines have their origins in trade legislation. Essential aspects, which particularly address the domain of norms and standards, consider state of the art or state of science and technology in the context of product liability. There are quite a number of initiatives to reduce such trade barriers, which will of course be rekindled by the discussions in the post-corona period. But essentially due to the risks of the corona pandemic, society has developed a more intense sense of safety and security. Why are the individual nations discussing IT security laws? What is the object to be protected? Are state-mandated Trojans an effective means against terrorism and sabotage? How much transparency is necessary and which transparency is dangerous because too much information about security, safety and protection mechanisms is disclosed.

Chapter 1 tries to approach the topic from the legal side. It is based on the hypothesis that safety is seen as the absence of intolerable risks, whereby the state authority prescribes the minimum level of safety requirements within the framework of its laws. I would like to warn in advance that the interpretations attempted here will indeed lead to the desired justice in court “safely”. Each case must be considered in its specific context. The state, legislators and regulatory authorities must be seen as key stakeholders in future mobility. It ensures safe roads, it prescribes the traffic rules, it monitors traffic, it ensures justice in court, and the public prosecutor brings charges in the case of capital crimes. But also, insurance companies, various lobbying organisations and consumer protection groups introduce quite a lot of safety requirements, which often also relate to the state of the art in case of damage. This legal context is a major driver for the architecture and design of means of transport and systems that control such means of transport.

Chapter 2 is about making the risk of mobility comprehensible. What is the relationship between risk and safety in relation to the laws and the various standards? What are the main differences in the various risk management systems? Which risks are relevant, how can the risks be assessed? What is the risk for which party in the development of a complex networked transport system or its means of transport? What is the relationship between intended use and unintended use? What is misuse, foreseeable misuse? How are the risks of cybersecurity related to the risks of accidents? Do the same standards apply here for the extent of damage and probability of occurrence of the risk? How can the infrastructure share the risk with the means of transport? How do other road users share the risk with the vehicle for individual mobility? All these aspects and questions are examined, and the chapter tries to show different points of view and outline possible aspects for solutions.

Chapter 3 makes a digression into cybernetics. Cybernetics is considered the basis of control engineering and communications engineering. But many aspects of behavioural physiology have also been derived from cybernetics. How can we describe safe and correct behaviour in public road traffic? What help does cybernetics provide? In this chapter, I also try to give an argumentation why one should not speak of autonomous vehicles. From some aspects of cybernetics, I try to derive the essential basics for the automation of individual mobility. What does a driver do when he drives a car? What does he observe, what does he have to pay attention to? To what and which aspects must he react, to which aspects he must not react? What does all this have to do with his reflexes?

Another important aspect will be shown in Chap. 3: What are the functions that a person has to perform in the mobility context and what skills do they need? The term ability is an analogy or contradiction to what are functional requirements and what is necessary, what skills the corresponding system must have in order to fulfil such requirements. What motivated the fathers of cybernetics to do all this research and postulated all the many principles that are used in technology today? What would a technical system look like that reflects the abilities of humans? Does the human being function at all like a single control unit or is the human being a networked system that forms its consciousness through many feedback loops and learns continuously? How does the idea of bionics differ from our current idea of networked automation? Does "automation" really only mean transferring human functions into technical systems? Is it not an essential task of the automation engineer to find better and more appropriate implementations for technical systems? Isn't it the benefit of the user of the system that is at the centre of the automation task? What benefit does the automation task bring? The chapter does not deal with the commercial benefit, but rather methodically to find the bridge to necessity and the relation to applicability. What else can we learn from the functions and the "human" system? What is the task of the individual functional elements and what distinguishes them when they work together? Which means does the human being use for perception, why is it important to recognise oneself in one's own context? Which control loops are used for perception? How are the control cascades hierarchised? Which closed control loops does the driver use when driving a car? There have already been many approaches to robots, what connects the tasks of robotics with automation technology? Many of these topics have to do with the human being at the centre of technology. What chances do we have of finding a new and significant customer benefit in the digital millennium from these more than 100-year-old findings?

In Chap. 4, systems engineering is presented as a central solution approach. How to put a system into the right context, how important is the context for a correctly functioning system? What do the different views and perspectives mean for the system? Why is it necessary to describe a system hierarchically structured in different levels of abstraction? Chapter 4 creates an activity matrix, which also includes the planning of the basic operational functions. It is shown that in principle the activities are similar, but they change due to their new context. Based on a V-model approach, the classical safety lifecycle could be extended to close the gap for safe operation concepts. In the operational domain, all the necessary intended functions derive from the intended behaviour and necessary protection mechanisms could be identified. The operational domain found the basis for all active safety function, not only for system protection also for occupancy, cyclist and pedestrian protection systems. All the performance and timing constraints derive from the operational domain. Another traffic situation, different weather or road condition leads to other needed system responses and consequently to other behaviour demands of the road vehicles. During sunny days and on perfect roads with low traffic, the risk is significantly lower than in a continuously changing context. Why does the same system behave differently in different environments or contexts? Why does a human being react differently in different situations, even though human–machine interfaces would allow for uniform handling? What is the difference between function and system development? How does software development relate to this? Is a software development process always the same? What is the purpose of software in a system network? Are we talking about a software safety or security mechanism, is it necessary to implement a protection mechanism or is it about the realisation of an initial intended functionality? What has to be considered in this context? Why is a basic software and the development or integration of an operating system, a completely different task, requires a different process than to realise an application software? How could we realise safe communication systems for future mobilisation demands? How can we control the necessary performance? System engineering needs to balance technical requirements like performance, timing, availability, safety and security. Not even the safest system from one point of view means a safer solution from another viewpoint, is the more secure system safer than the high available system? All those questions and how to balance depend on the context of the intended use of the system. This Chap. 4 tries to provide several viewpoints and perspective in order to assess the necessary measures to develop safe systems.

Chapter 5 provides perspectives on systems and their context from a organisational viewpoint. Many causes of risk derive from organisational inadequacies. Several methods identify causes of organisational risk. Are the cooperation models still the same for the future mobility? The role of owner, driver, manufacturer and supplier will change. What will be the role of an operator for transportation services? Do we find structure like in the railway or in the aviation business? How do TIERs reach the end-user, just via the aftermarket or could they sell new services and safe functions during the operation of the vehicle?

Chapter 6 provides solutions for automated driving. Solutions are considered which are derived from the human system or solutions which demonstrate safe applications by means of machine learning. The limits of artificial intelligence are also shown. In order to drive automatically, the tasks that were previously assigned to the driver must now all be completely assigned to one or more systems. This of course is in addition to the functions that the vehicle had to fulfil so far. But how the distribution looks like, what the driver or the system has to perceive while driving and what he has to bring along to be able to drive safely, will probably change. We will probably have to advance our systems, because the systems today are far from mature in terms of perception and their translation into adequate and timely responses.

Some examples derive from other industry or technology areas and are mapped onto new mobility solutions. Especially, the aerospace industry has many solutions ready which can also make road transport safer. Even though aviation is still far away from air taxis, drones for the transport of passengers, aerospace technology offers very ideas, interesting approaches and safe solutions. Some predict that autonomous flying drones are faster in the sky than autonomous vehicles on the road. The risks are different in every context, so the measures are not transferable. However, comparisons and experiences in different industries can help us to better assess the possible solutions and their risks.

I conclude the book with a personal outlook on what questions can lead to safe mobility and what safety means for the benefit of humankind. The book does not contain any recipes that can be simply worked through; it is primarily intended to help people think more intensively about safety issues.

Will it be safer to fly with flying robots from one meeting to the next or simply to use digital communication? the reader himself should judge this.

Contents

Chapter 1
Safety the Basis for Future Mobility

Mobility often means a compromise between people having advantages of being mobile and people see a personal afflict of mobility. Today's traffic situation shows that noise, smell, exhaust gases and the spatial of roads, air corridors, but also railway routes, is doubtless accepted by society. Today's discussions about air taxies and press releases already about autonomous drones show the demand for finding a new contract between society and mobile service providers. How fast how many people are supposed to be moved from one place to another location is since Jules Verne part of every science fiction novel. Science fiction has always provided an imagination of future technology.

The nature of human being makes people sceptic if it comes to new technology or any creature that behave differently than the known before. Could you trust the news? Does not anybody try to misuse the new technology?

Biology, chemistry and nucleonic brought a lot of benefits for human beings, but all technology provided also new cruelty in the way how we fight against people or how we could make war. Many accidents have made us aware that we need to control the new technology in order to prevent accidents.

People need to experience and get trust in that new technology. The need for global principals of use with biological and chemical technology had been leading to the foundation of organisations like the United Nations and many others. Some of the organisations focus on.

- how to use the technology during wars,
- what are the ethical limits to impact humans (like cloning people),
- common agreements on the range of technical usage (what is generally acceptable for people, animals, etc.),
- how we manage, monitor and control the limits,
- how we deal and prevent accidents, and many more aspects.

Basic understandings and agreements had been defined that safeguards the society to beware of extensive usage of the new technology.

H.-L. Ross, *Safety for Future Transport and Mobility*,
https://doi.org/10.1007/978-3-030-54883-4_1

It seems to be the challenge for the new millennium to do that with the “Digital Technology”.

What are our moral principles, concepts, the rules and limits how do we develop the society with the new “Digital Millennium”? Can we control that development? On the other hand, do we need to make the same experiences as we did in the last millennium with ABC? We approaching A (Atomic), B (Biological), C (Chemical), D (Digital), we need to find a harmonised approach how to make use and coexistence of the technology with freedom of the society, piece and benevolent of humans and their environment.

In a military context people discussing the impact of remote-controlled drones or missiles and that, the soldiers do not feel any more the cruelty of their weapons. People feel concerned that the threshold of accepted collateral damage increases if they got aware that such weapons kill civilians or even hit schools and hospitals. People fear new weapon systems. These have one aspect that they offer special protection for the users. Another aspect appeals to the fears which are poked if the weapons are not applied or how many human lives are saved by the use of such weapon systems. From it there originates fast the question, need we to diminish the new technology also around the risks in the traffic?

In civil life, people feel more and more impacted by cybersecurity or any other kind of data criminality. The misuse of vehicles to attack people becomes more and more credible scenarios. Today it will be no special risk for the road users if a hacker cracks data from traffic offenders, vehicle data bank or driving licence holder. Nevertheless, there are many publications how by hacker’s attacks also traffic systems can become dangerous weapons of terrorists.

The new millennium provides us with a further challenge on how to deal with ABCD because the A seems to fail as an energy source. The Diesel-gate provides an enormous acceleration for the electro-mobility. How to generate on a green-basis sufficient electrical energy and how to store that energy on the moving vehicle are still with many question marks.

Would be hydrogen the answer? Only water coming out of our exhaust is a perfect image.

Do people need any more a driving licence, if the car makes the decisions in the road traffic? What is the reason even to own a car? Is it just the availability in case of demand?

We pay money to park a car, to drive on roads.

Vehicles occupy mayor parts of our land. Millions of vehicles are on the motorways every day in a traffic jam with just one person inside.

1.1 Safety is Much More Than Safety Engineering

The German words “Sicherheit” and “Fehler” are widely used terms. “Sicherheit” in the German understanding means also a protected environment, no fear, welfare, social security and feeling comfortable.

"Fehler" means an error, bugs, mistakes, deviation from expectations, but in many cases not a failure. In German language, failure is often translated as.

"Ausfall"—termination of fulfilling a function (e.g. athlete could not attend due to illness) or.

"Versagen"—fail in performance (e.g. athlete does not win as expected).

The new ideas of mobility require obviously a new understanding of all those terms and at least new or further interpretations of the current understanding of current society rules.

Due to the digitalisation of our life, the border between people who are afraid of the new technology and those who are enthusiastic about it must be redefined.

When in 2011 the ISO 26262 was published as an international standard, certain electronic systems were already very far further developed in the vehicle. The homologation laws even already demanded some of such systems like the airbag or the antilock braking systems. At the beginning of the twenty-first century as the first German working group in the VDA (association of the automotive industry) started with Functional Safety of EE systems, a slender standard for electronic products or systems was the target.

During the following 10 years before the final publication of the ISO 26262 in 2011, these working groups 10 of volumes with roughly 1000 requirements compiled. Even if a lot of appropriate knowledge, methods and attempts were discussed in the course of the years, one found only one fraction of it in the ISO 26262. Some information was taken up as footnotes; some disappeared completely, to the final publication of the first standard.

Worldwide different standardisation projects were initiated to translate the standard into the respective national language; into German, the standard was never translated.

The ISO 26262 should never serve as a guide but formulate requirements for activities and methods with the help of a lifecycle model.

Then in 2018, the first reworking of the standard was published. Consciously the extent of the standard became in the essentials only around commercial vehicles like commercial trucks and buses as well as two-wheeled vehicles (or tricycles) complements (part 12). Besides some editorial changes and informative changes were tried to maintain the structure. Part 11 was complemented which deals with the functional safety of semiconductor, and in Part 10, some examples about safe availability are given.

In parallel with the reworking of ISO 26262, there was a massive recovery of the electro-mobility and the terms of the "automated driving" or even "autonomous driving" stamped the public discussion to the future mobility.

The aspects to the safety-in-use, high-voltage or touch-protection and active safety for electro-mobility became a separate standard ISO 6469 "Electrically propelled road vehicles—Safety specifications". It seems to be the basis or with similar contents also to legal requirements in the various countries.

All around the subject "automated driving" developed an intensive discussion, it in a standardisation project flowed under the name: "Road vehicles—Safety of the intended functionality" which as ISO/PRF PAS 21,448 (Publicly Available Specification) was published. The demand derived from the exception in the first ISO 26262, that safety of the nominal performance was exempted and functional or technical inadequacy not even addressed in the first edition of ISO 26262.

Furthermore, safety-in-use, safety impact due to non-EE-systems or any impact from the environment of the system under consideration, all aspects of misuse or security, privacy, etc., had been not addressed and legal requirements, protection measures are still not systematically addressed in current automotive safety standards.

Key characteristics of occupancy safety systems derives from legal standards; they specify their functionality and protection targets as well their safety-related special characteristics. During the last years, those requirements increased significantly due to consumer protection initiatives from New Car Assessment Program (NCAP) or insurance companies, etc. Beside occupancies also pedestrian and cyclists getting more and more a target for road traffic safety. Especially cyclists and pedestrians are increasing identified as weaker road users that need to be protected.

This second book considers road traffic safety under a new wider perspective and put the known sources of risk in the focus and does not focus on particular standards. We need to accept that risk and safety provide different requirements only in case the context changed.

Regulations, requirements, directives, etc., are always controversial without understanding with which context or from which perspective one considers this.

1.2 Safety as a Social Right

In each country, people have a degree of protection guaranteed by the constitution of their country. Law regulates the access to the countries, and the inhabitants and citizens of the respective countries have the right with their taxes to finance this protection. Law regulates even trade of goods.

The basis for all constitutions of most countries in the world is the human right laws from the United Nations (UN).

They provide the following information in the Internet:

What Are Human Rights?

Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more. Everyone is entitled to these rights, without discrimination.

International Human Rights Law

International human rights law lays down the obligations of Governments to act in certain ways or to refrain from certain acts, in order to promote and protect human rights and fundamental freedoms of individuals or groups.

One of the great achievements of the United Nations is the creation of a comprehensive body of human rights law—a universal and internationally protected code *to which all nations can subscribe and all people aspire. The United Nations has defined a broad range of internationally accepted rights, including civil, cultural, economic, political and social rights. It has also established mechanisms to promote and protect these rights and to assist states in carrying out their responsibilities.*

United Nations, https://www.un.org/en/sections/issues-depth/human-rights/.

The foundations of this body of law are the Charter of the United Nations and the Universal Declaration of Human Rights, adopted by the General Assembly in 1945 and 1948, respectively. Since then, the United Nations has gradually expanded human rights law to encompass specific standards for women, children, persons with disabilities, minorities and other vulnerable groups, who now possess rights that protect them from discrimination that had long been common in many societies.

In Europe, many of the aspects derive to regulations and guidelines from the European Union and their member have to implement those in country-specific legislations.

In Germany is the understanding that fundamental rights indicate the following common characteristics:

- They oblige primarily the state, namely no matter whether it concerns executive, legislative powers or judicative, alliance, country or local authority district. Obliged means that the fundamental rights must be followed.
- They It is not distinguished whether the state operates in the way of the immediate or indirect state management or whether it becomes under private law or public law or becomes active by means of legal entities of the private law.
- The fundamental right authorisation is a characteristic of the fundamental rights property. Comparably with the civil law "legal capacity", the fundamental right bearer must be able to hold the fundamental right.

One also speaks of "each fundamental rights" whose bearer is every person, hence, also the terms "human rights"; at least the German way of understanding.

Human dignity is in general view, on the one hand, the value that is ascribed to all people equally and regardless of her differentiation characteristics like origin, gender, age or status; and on the other hand, the value with which the person positions himself as a kind about all the other living beings and things.

In the antiquity, one has derived the fundamental rights from the reason (for example, Aristoteles) of the stronger in each case; these principles have in particular also flowed in onto the traffic right.

Thus also applies to the road traffic that every person who moves on public roads and a certain protection of the place stands.

In all life situations and also therefore in all branches where companies provide products or offer services, it is a matter of providing the safety or social security of the people to a certain degree. With it linked commitment protection is for the people of him in each case parties acted of implementing, so those dangers are excluded and impediments only to such an extent must be accepted which is valid as in the respective context as reasonable.

Therefore, these fundamental rights derive in all areas where products and services are offered. This has of course from that point of view massive effects on the laws