Klaus Hörmaier, Dipl.- Ing.

Excessive Electromagnetic Interferences as Fault - Methodology for Automotive Electromagnetic Compatibility with Respect to Functional Safety

DOCTORAL THESIS

to achieve the university degree of

Doktor der technischen Wissenschaften

submitted to

Graz University of Technology

Supervisor

Univ. Prof. Dipl.-Ing. Dr. (techn.) Hubert Zangl

Institut für Elektrische Meßtechnik und Meßsignalverarbeitung

Graz, October 2015

AFFIDAVIT

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present doctoral thesis.

Date

Signature

Acknowledgements

I am immensely grateful to my supervisor **Univ. Prof. Dipl.-Ing. Dr. (techn.) Hubert Zangl**, for his continuous support throughout my entire thesis. He supported me in numerous ways. He motivated me in difficult phases and helped me to refocus on the most promising parts of the research. He helped me with his detailed technical and economical understanding as well with his deep knowledge within science in general. He shared his knowledge with me in several discussions and always provided me with excellent feedback. Not least of all, he granted me more time than is typical by other supervisors.

Not only in the context of this thesis but for all the years of support in all kinds of situations, I want to thank my parents **Karin and Roland Hörmaier**. They always gave me the confidence that I am able to achieve all targets and set the framework within which to accomplish my goals.

I would like to show my gratitude to **Claudia Schett** and **Lisa-Marie Faller** for their untiring support in editing this manuscript. Without their highly professional help this work would not achieved the quality requirements. Not only for their support in editing, but also for their critical questions and role as contact persons in all kinds of problems I am very thankful.

I would like to thank the responsibilities at **Infineon Technologies Austria AG** who allowed and founded this thesis. Mainly the goodwill of **Franz Wachter**, **Alois Rainer** and **Robert Czetina** ensured the project's success.

I owe my deepest gratitude to **Herbert Zojer** who showed me another way of thinking and inspired me with new ideas and fruitful discussions, especially during the setup of this thesis.

The research leading to these results has received funding from the **ARTEMIS Joint Undertaking** under grant agreement Nr. 295311, and Nr. 269335, as well as from the Austrian Research Promotion Agency **FFG** under the program "Forschung, Innovation und Technologie für Informationstechnologien (FIT-IT). Thus I want to thank also the funding authorities for partially sponsoring my work.

Abstract

A multiplicity of electrical and electronic systems support humans in their daily work or protect them from hazards as for example active safety systems in a vehicle. However, these systems might harm or injure humans in case of malfunctions caused by random hardware faults. Unexpected malfunctions as for example an incorrect steering command caused by a fault in the steer-by-wire system might lead to accidents with physical injury. Thus, reliable system operation is mandatory. However, building zero-failure systems is impossible which is well accounted in functional safety standards as for example the IEC 61508 or ISO 26262 which permit a very small failure rate.
Electromagnetic interference, generated by artificial or natural sources, can be the root cause of system's malfunctions. In order to mitigate malfunctions caused by electromagnetic interference high robustness against interference is required. Thus, in order to achieve high robustness often additional safety-components have to be built in. However, additional components, which possibly introduce further failures into the system, might decrease the system's overall failure rate. On the other hand, intensive electromagnetic interference is often caused by component faults whereby the interference's probability of occurrence can be related to the components failure rate. Thus, this work shows how to calculate and further minimize the system's overall failure rate. The work moreover shows that electromagnetic interference shall not only be treated as environmental factor but as fault or faulty condition, which can be covered by the standard functional safety process. Thereby, the work provides evidence that the concepts of fault metrics, fault tree analysis and dependent failure analysis are fully applicable onto electromagnetic interference. Additionally required data to perform quantitative analysis is gathered by the analysis of neighbouring faulty systems within the vehicle. This includes the occurrence probability of electromagnetic interference, generated by faulty systems, with certain amplitude / time characteristics. The novel approach of this work links the failure rates of the assembled systems with the interference characteristics and allowing to further calculate the system under development's failure rate.
It is essential to characterise the generated interference in advance. Therefore faults are injected by purpose into the system and the thereby generated emission is measured. Efficient simulation of interference sources shall enable a broad acceptance and increase the applicability. Therefore, this work provides simulation methods which allow interference simulation as quality measure in the same way as interference simulation as safety analysis method. Finally, methods to reduce the simulation time and the detection of interference sources in time domain will be presented.
This work provides a comprehensive and easily applicable guideline on safety analysis considering electromagnetic interference, enabling a broad acceptance.

Kurzfassung

Eine Vielzahl elektrischer und elektronischer Systeme unterstützt Menschen in ihren Tätigkeiten oder schützt sie vor möglichen Gefahren. Ein Beispiel dafür sind aktive Sicherheitssysteme im Fahrzeug. Derartige Systeme können jedoch aufgrund zufälliger physikalischer Fehler auch zur Gefahr für Menschen werden. Durch unvorhergesehene Ausfälle - beispielsweise dass Lenkbefehle des Fahrers bei einer elektronisch kontrollierten Lenkung („Steer-by-wire“), aufgrund eines Defekts nicht mehr korrekt umgesetzt werden - kann es zu Unfällen mit Personenschaden kommen. Daher ist der zuverlässige Betrieb derartiger Systeme unverzichtbar, wenngleich eine absolute Sicherheit nicht erreichbar ist Aktuelle Standards der funktionalen Sicherheit, wie die IEC 61508 oder ISO 26262, berücksichtigen diesen Umstand und gestatten nur eine extrem kleine Fehlerrate.
Eine der möglichen Ursachen für das Fehlverhalten elektronischer Schaltungen sind elektromagnetische Störungen, welche von natürlichen oder künstlichen Quellen erzeugt und ausgesendet werden. Um Fehler, verursacht durch elektromagnetische Störungen, zu vermeiden, ist eine hohe Robustheit des Systems gegenüber diesen Störungen gefordert. Um das zu erreichen müssen oftmals zusätzliche Schutzkomponenten eingebaut werden. Allerdings können diese zusätzlichen Komponenten wiederum selbst ausfallen und damit unter Umständen die Zuverlässigkeit des Gesamtsystems reduzieren. Die Ursache von großen elektromagnetischen Störungen liegt oftmals wiederum in defekten Komponenten begründet, sodass die Wahrscheinlichkeit des Auftretens letztlich mit in einer Ausfallswahrscheinlichkeit von Komponenten in Zusammenhang steht. Daher wird in dieser Arbeit gezeigt, wie die Fehlerrate des Gesamtsystems, mit all seinen Aufgaben, berechnet und schlussendlich minimiert werden kann. Es wird gezeigt, dass elektromagnetische Störungen nicht nur als Umwelteinfluss, sondern auch als Fehler oder fehlerhafter Zustand gesehen und daher im gewöhnlichen funktionalen Sicherheitsprozess mit abgehandelt werden können. Dabei werden Konzepte wie Fehlermetriken, Fehlerbaumanalyse und Abhängigkeitsanalyse wirksam auf elektromagnetische Störungen angewendet. Die zusätzlichen benötigten Daten, die für eine quantitative Analyse benötigt werden, werden in dieser Arbeit anhand im Fahrzeug benachbarter fehlerhafter Systeme ermittelt. Dazu gehört auch die Wahrscheinlichkeit mit welcher eine elektromagnetische Störung, ausgesendet von fehlerhaften Systemen, bestimmter Amplitude und zeitlichem Verlauf auftritt. Als neuen Ansatz werden in dieser Arbeit die Fehlerraten der verbauten Systeme mit den Störamplituden gekoppelt, um letztendlich die Fehlerrate des untersuchten Systems berechnen zu können.
Um die im Fehlerfall generierte Störemission vorab charakterisieren zu können wird vorgeschlagen, künstlich Fehler in die Systeme zu injizieren und die dabei generierten elektromagnetischen Emissionen aufzunehmen. Durch effiziente Simulation der elektromagnetischen Störquellen, soll eine breite Akzeptanz und Anwendbarkeit erreicht werden. Es wird gezeigt wie Emissionssimulationen zur Qualitätssicherung auf die gleiche Art und Weise wie Emissionssimulationen zur Fehleranalyse durchgeführt werden kann. Schlussendlich werden Methoden zur Simulationszeitreduktion von Störquellenemissionsspektrum-Simulationen und zur Störquellendetektion im Zeitbereich vorgestellt. Die Arbeit stellt folglich einen umfassenden, leicht anwendbaren Leitfaden zur Sicherheitsanalyse unter Berücksichtigung elektromagnetischer Störungen mit hoher Akzeptanz dar.

Table of Contents

Chapter 1

Introduction

1.1 Motivation

Electrical and **E**lectronic (E/E) systems support humans in their daily work. Humans rely, or have to rely on systems to behave as expected, since in the event of a malfunction, harm or injuries might be caused. For example, if a big robotised automation machine changes its movement unexpectedly, staff working beside it might get injured. Thus, the developed systems have to operate safely, in the sense that they do not expose humans to unreasonable risk or cause economic losses.

Developing a safe product is the responsibility of all engineers involved and a challenging job that requires specific knowledge and a lot of experience. Companies bear a moral commitment, to build safe products but rivalry among competitors and high pressure on cost and time reduction hinder the safe development. To limit uncontrolled marked entries of hazardous, profit oriented products, national and international regulation authorities introduce laws and standards.

Unfortunately, it is mostly not possible to create a 100% safe product as it is impossible to consider all combinations of unlikely random events that may lead to failures[1]. Standardization committees are aware of this fact and accounted for it in standards such as the *Road Vehicle Functional Safety Standard ISO 26262* [1] or the *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems IEC 61508* [2]. Thus, these standards explicitly accept unreliability due to random hardware faults but only up to a (very low) defined limit. Nevertheless, the requirements are strict and often difficult to fulfil.

Engineers have to consider various influencing factors during the different development phases, heavily loading the engineers. High workload and high complexity increases the risk of human errors during product development, hindering placement of safe products on the market. Thus, engineers need guidance to ease their work when facing the continuous increase of product complexity and work packages. This is not only true for present-day products but also essential to be able to cope with upcoming challenges of more complex products. Some standards already provide certain guidance but they often cover the engineers' needs only superficially. The large number of standards with often overlapping / interlinked topics does not ease this fact.

Furthermore, late or insufficient safety considerations might also lead to economical costs. From time to time announcements of problems with leak of safety are published, often in combination with expensive recalls of the products. An example of such a problem is given in the following announcement. In January 2013 the car manufacturer Toyota had notified the

[1] The safety standard targets safety related functions which are for example identified by safety analysis like fault tree analysis or dependent failure analysis.

National Highway Traffic Safety Administration about a safety recall of about 880.000 cars. In their report Toyota explained the problem as follows [3]:

> *Through observations made during ASIC bench testing, nanosecond level noise created by operating certain electrical components in the vehicle could resonate and transform into microsecond level noise through damped oscillation. After investigating additional working air bag modules recovered from in-use Corolla and Matrix vehicles, it was found that the ASIC was susceptible to latch-up due to certain levels of microsecond electrical noise. Further investigation determined the electrical noise level in the subject vehicles was higher compared to other vehicles and confirmed the source of the higher noise level could be attributed to operation of certain vehicle electrical components. In addition, the ASICs in the subject vehicles, which had been produced by National Semiconductor for TRW, had a wide variation of insulation against electrical overstress, and there was no thermal protection circuit in the generation of the SRS ECU in the vehicles to help guard against potential overstress and heat-related damage. Toyota determined the noise can resonate and transform causing latch-up to occur, which could result in thermal damage to the ASIC and inadvertent air bag and/or seat belt pretensioner deployment.*

As this example illustrates, it is advisable to view **e**lectro**m**agnetic **c**ompatibility (EMC) or the product's robustness against **e**lectro**m**agnetic **i**nterference (EMI) not only as a pure quality requirement (e.g., radio reception in regions far off), but as a necessary property of safety related products which has to be fulfilled. For certain product segments, it is unacceptable to fail due to EMI, for example, Anti Blocking System (ABS), Electronic Stability Program (ESP).
Thus, safety standards already take EMC or more precisely EMI into account,for example, in IEC 61508 or ISO 26262.
An interesting aspect is that EMC and **F**unctional **S**afety (FS) are not often referenced in combinations, not to mention the different flows of handling these fields. In general both areas even follow different work processes. This might be because theoretically EMC implicitly addresses FS topics and vice versa. Nevertheless, the published standards advise considering the complementary field, but do not provide sufficient information on how to do this. Furthermore, it is not evident whether this can even be handled in the proposed processes. Adversely, this undermines the potential efficiency and smoothness of the work, due to non-consistent handling of EMI and FS. Sometimes, engineers only take EMC vaguely into account which hinder efficient safety analysis. Gathered information is often imprecise or even ambiguous, which forces, from FS point of view, to go as far as to take a worst-case scenario into account which in turn leads to unintentional increase in complexity. In case of doubt, additional design measures to increase robustness or to reduce emission have to be implemented which are not needed in the for the environment the system is supposed to operate in.
In addition, defined limits for emission and for immunity of components strongly differ. As example, the **L**ocal **I**nterconnect **N**etwork (LIN) standard specifies the maximum allowed emission of the LIN node, measured with the 150 Ω method at a frequency of 30 MHz, with 20 dBµV. However, the required immunity level measured with the **D**irect **P**ower **I**njection (DPI) method (see. Figure 1.2) at a frequency of 30 MHz, is given as 33 dB Watt at 50 Ω , which can be converted to dBµV resulting in around 170 dBµV. The difference between the allowed emitted emission to the minimal required immunity level is 150 dB, which is a factor of 31.585.000 ($\approx 3 \cdot 10^7$). Undeniably, a certain margin between the robustness of components and the emitted electromagnetic signals is needed to guarantee radio communication also over large distances.

A transmitted radio signal shall be, at the location of the radio receiver, still large enough so that the electromagnetic field emitted by the for example, a LIN node next to the radio receiver does not influence the reception. On the other hand another LIN node near the radio transmitting station, where the electromagnetic field is much higher due to the closer location, shall also not be influenced in its function. Nevertheless, the dramatically high margin cannot be reasoned only by the undisturbed radio reception but by unnecessary overtesting to have higher subjective confidence in the developed product.

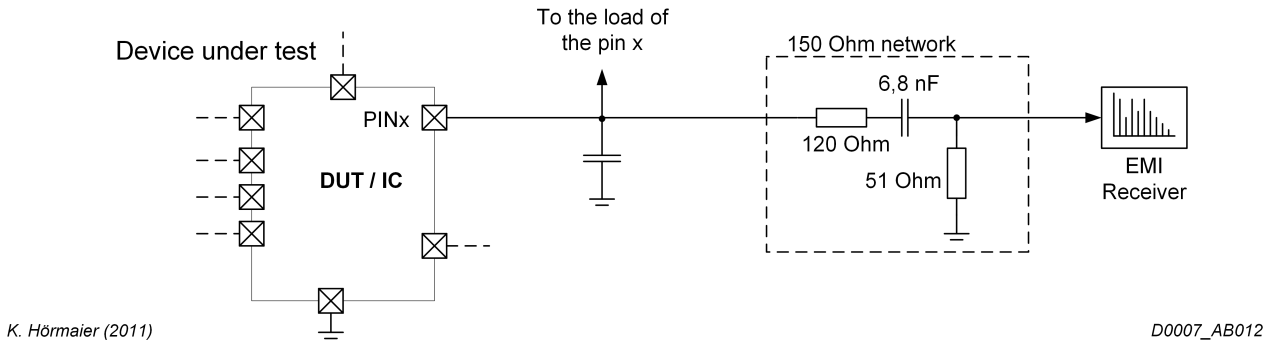


Figure 1.1: 150 Ω emission measurement method according IEC 61967 [4]. The emission of the DUT is measured with an EMI receiver together with the 150 Ω impedance coupling network.

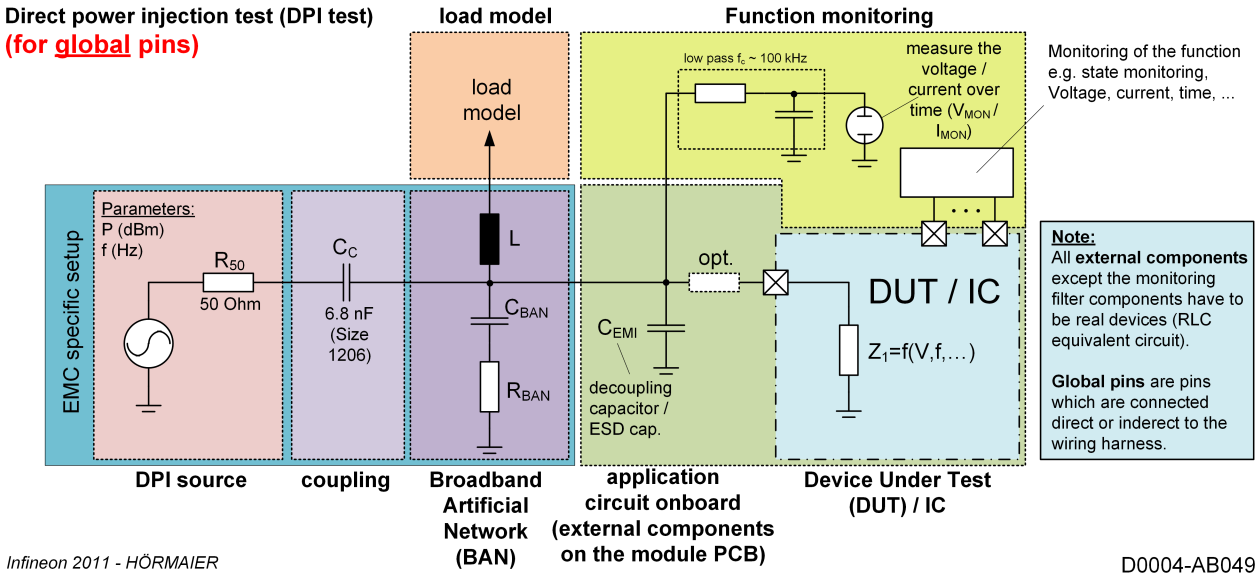


Figure 1.2: The direct power injection immunity test method (IEC 62132) to characterize the susceptibility of the device under test against electromagnetic interference is shown.

Furthermore, the limits are independent of the LIN module's function within the system. Thus, the robustness is specified independently from the realized system's safety level which, in the safety engineering domain is unusual.
The misconception that increasing the EMI robustness leads to safer applications is widely spread. Often additional components have to be assembled to increase the EMI robustness. But all additional components exhibit failure rates unequal to zero and might influence the system's function. Thus, the overall failure rate might even increase by an improvement of EMI robustness. Not only the risk of increasing the product's failure rate exists but also the

risk of introducing systematic faults due to increased complexity. A safety system shall always be as simple as possible to mitigate the risk of systematic failures. Unnecessary increase of robustness further indicates the insufficient understanding of the system itself and the environment in which the system operates. Thus, the project might be questioned and additional information has to be requested or gathered. In conclusion, increase of over-engineering and robustness shall be avoided, which is reasonable not only from an economical point of view, but also from a safety point of view.

The strongest impact for all considerations can be found in the decision whether EMI is treated as an environmental condition or as a fault. Thereby, a simple assignment of EMI to the environmental conditions or to faults is not constructive. Even standardization is in this context ambiguous, ISO 26262 continuously treats EMI as environmental condition however IEC 61508 treats EMI at least partially as random fault but also as environmental condition. Thus, a clear approach of distinction between fault and environment is required.
Inside the vehicle, several electrical and electronic systems are operating which contribute to, or generate the inner **e**lectro**m**agnetic (EM) environment. Disturbance generated by those systems is strongly limited and known. Emission is generally strongly regulated, and admitted emission levels are very low. An example is the emission of integrated circuits, measured with the 150 Ω measurement method [4] (see Figure 1.1), are in the range of several tens of dBµV. Only in case of faults, systems tend to produce high emission. The emission is therefore related to faults (leading to failure modes) and not to normal operation. Thus, failure rates can be assigned to the high power EMI events and therefore can be included in the failure analysis. With this approach, further steps in the typical safety analysis process can be followed with few changes leading to a tight integration of EMI in the context of FS.

1.2 Goals

This work aims to show the feasibility of fully integrating electromagnetic compatibility into the functional safety process. Methods which are already used for FS shall be analysed regarding their applicability on EMC topics. The applicability of these methods shall be proven and necessary extensions shall be proposed. Furthermore guidance on correct and efficient application of the methods shall be part of the work.
Since early safety assessment saves effort and costs, applicable simulation methods will be provided. Simulation optimization, with regard to effort reduction will complete the approach and will show the industrial useability.

1.3 Scope

Both, the field of electromagnetic compatibility and the field of functional safety are very broad, especially considering all domains and the environments. To limit the scope of the work, the automotive domain has been chosen as representative, since it deals with safety related mobile systems operated within diverse environmental conditions.
The types of applications are various in the modern vehicle. Electrical motors, light and displays, magnetic actuators, ignition plugs and **I**ntegrated **C**ircuits (ICs) can be assembled in the car. Due to the high number of ICs and their significance in the realisation of functions the ICs have been chosen as the main example. They are often the source of electromagnetic emission and are often susceptible to electromagnetic interference. Indeed, the methods described later

in this work are transferable to all other domains, nevertheless the referenced standards and models are picked from the automotive domain.
For several analysis methods which will be presented later in this work, data regarding electromagnetic interference is needed. For an early analysis, this information is gathered by simulation.

1.4 Organisation of the Document

Chapter 2 provides an state of the are review for EMC and FS, followed by an analysis of the publications which examine EMC and FS in a combined manner. Chapters 3 and 4 describe the basics of FS and EMC as well as summarize all information needed to follow the explanations provided in Chapter 5. Thereby, Chapter 3 targets only EMC topics and Chapter 4 provides detailed information about FS. Chapter 5 explains the approach of including EMC into the FS process and provides evidence, that the approach is valid. The described process requires extensions in simulation, which are presented in Chapter 6. Additionally, the chapter's content provides guidance for engineers on how to efficiently simulate EMC problems, and delivers proofs and optimization of simulation setting. A summary and conclusion including an outlook is given in Chapter 7.

Chapter 2

State of the art

In this chapter relevant work regarding EMC as well as functional safety will be presented. Up to now, only a few documents, discussing the combination EMC and FS, have been published. However, standards exist that already target the combination of EMC and FS. In this chapter the relevant publications targeting both topics in combination will be provided alongside the most relevant publications addressing EMC topics and FS topics separately will be presented.

Starting from the pure EMC point of view, several standards exist. These standards mainly describe the electromagnetic environment and measurement or testing techniques. The basic standard for EMC is the IEC 61000 [5]. The IEC 61000 includes guidelines how to describe EM phenomena and the EM environment. It describes measurement and testing techniques including the limits as well as guidelines on installation and mitigation. And finally it can be seen as a handbook on how to characterise the EM environment. A detailed description of the EM environment discussing the IEC 61000 is given in [6] focusing on problems of characterizing the EM environment and possible classification approaches. But also other publications describe the EM environment, as for example the following two.
In [7] the EM environmental conditions inside a coal mine have been measured and analysed using wavelet analysis. With the obtained permitted EMI the equipment has been optimized regarding the EM environment. In [8] the needed EMI profile, a vehicle is exposed to during a typical driving cycle, is discussed.

Beside the environment, EMC standards focus on measurement and testing. A detailed survey on automotive EMC test standards is given in [9] and a detailed overview of IC level immunity test is given by [10].
Beside the standards published by standardisation authorities, a couple of in-house standards of **O**riginal **E**quipment **M**anufacturers (OEMs) exist. Some examples are: Audi/VW: TL965, TL82066, TL82166, TL82366, TL82466, TL82566; BMW: GS95002; Daimler: MBN 10284-1, MBN 10284-2; Ford: CS2009; General Motors: GMW3097; MAN: M3285; Renault: 36-00-808; Volvo STD 515-0003.
The standard LV124, introduced by the German Association of the Automotive Industry (VDA) combines and consolidates the requirements of some of the previously mentioned EMC standard from German OEMs [11]. The standard, based on ISO 7637, includes test methods, test setups and test conditions for E/E components within the vehicle.
Beside the standards, articles are published describing how to model standardised measurement components for example, [12] which provide simulation models of the coupling clamp according to IEC 61000-4-4.

The uncertainty of emission measurements considering the different operation modes and load conditions of the equipment under test has been discussed in [13]. In this work problems with the indication of the worst-case conditions have been raised.

Several safety or functional safety standards exist. A detailed overview of the different safety standards, considering the domains: aeronautics, automation, rail, automotive and nuclear, are listed in [14]. From the functional safety point of view the following standards have the highest importance in their domain:

- IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- ISO 26262 - Road Vehicles - Functional Safety
- DO 178 - Software Considerations in Airborne Systems and Equipment Certification
- EN 50126[1] - Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

All the previously mentioned standards demand the consideration of robustness against electromagnetic interference, for example IEC 61508-2 7.2.3.2

> *The E/E/PES safety integrity requirements specification shall contain the* ***electromagnetic immunity*** *limits (see IEC 61000-1-1) which are required to achieve electromagnetic compatibility - the electromagnetic immunity limits should be derived taking into account both the electromagnetic environment (see IEC 61000-2-5) and the required safety integrity levels;*

Many research publications exist dealing with reliability, safety design and analysis methods. Like a model-based synthesis of fault trees from Matlab-Simulink models [15] or from timed automata models [16].
A new EMI-based fault injection technique, comparable with other commonly used fault injection approaches, such as heavy-ion radiation, power-supply disturbances (also known as pin-level fault injection), mutation analysis or saboteurs, was presented in [17]. Thus it shows, that the direct power injection (DPI) test can be used as a pin-level fault injection method.
A method for a hierarchical modeling of faults is given in [18]. A simulation with the mutated (fault injected / defect injected) circuit gives a new behavior which can be included in the next hierarchy.

As mentioned before, a standard already targeting the combination of EMC and FS exists. With part IEC 61000-1-2 (Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena), EMC is brought into context with functional safety. It covers the actions to be taken from the beginning of the development until the phase out of the product. It "*establishes a methodology for the achievement of functional safety only with regard to electromagnetic phenomena of electrical and electronic systems and installations, as installed and used under operational conditions*" [19].
In [20] a survey of EMC standards adequate for ICs have been analysed regarding their usability for functional safety related developments. In addition performance criteria were discussed and

[1] Typically the EN 50128 and EN 50129 are referenced together with the EN 50126.

brought into functional safety context. It ends with the discussion of the insufficient data problem for describing the EM environment.
Ogunsola [21] highlights the problem that it is difficult to guarantee EMC since the definition of EMC includes the term electromagnetic environment. The environment at a certain location can vary and might be difficult to characterise. The paper also explains the controlled and uncontrolled electromagnetic environment. It furthermore raises concerns that standards cannot provide immunity levels for products to achieve functional safety.
The problem of different probabilities between safety standards and EMC test standards has been discussed in [22]. The authors proposed to reduce the overlap between the immunity level and the disturbance level to fit to safety levels.
The possible temperature dependency of aging effects in combination with EMI have been discussed in [23]. Product samples have been tested directly after production and after exceeding five years of operation. In both cases the product passed the immunity test. In addition the EMC related parts in the ISO 26262 have been listed.
Armstrong in [24] questioned "Why EMC immunity testing is inadequate for functional safety". He stated that EMC risk analysis is not done and that foreseeable faults are not addressed by immunity testing. In [25] Armstrong showed a supporting process for documenting EMC related tasks within the products life cycle. Beside the immunity testing to guarantee functional safety, in [26] the importance of emission testing has been mentioned in addition. In this context he stated: *"It is also important to have sufficient confidence that they will remain so over the system's anticipated lifetime in its physical environment."* This means a foreseeable change of the emission inside a system has to be considered. Vehicle manufacturers "overtest" the systems but cannot validate their choice of the test levels because real-life electromagnetic environments do not include such high levels [27].
The satellite's electromagnetic environment described by random variables has been analysed in [28]. The three dimensional relation between frequency, amplitude and probability of interference has been shown and the need to take this probability into account when developing a safety or mission critical system has been highlighted.
In [29], Helmers et all raised the concern of high EMI exposure caused by a system's failure mode. Within the fault-free system, EMI does not cause problems but in case of a system's failure an EMI source is activated. At the same time a highly susceptible receiving function is active, which leads to an interfered reception leading to hazardous malfunctions of the system. Thus, critical combinations of functional states regarding electromagnetic interference have to be analysed. Therefore [29] proposes a rule-based analysis of functional information and EMC information.
In [30], the definitions for classifying performance degradation have been questioned and concerns regarding over testing were raised. A new approach for immunity testing has been proposed which allows to identify the susceptibility threshold and the safety margin.
The systematic construction of the fault tree, taking other system components into account, has been presented in [31]. A workflow of how to include electromagnetic compatibility into functional safety analysis in a systematic way was presented by using methods of a model based design.
Alexandersson [32] described where in the FS process, EMC inputs are needed. Furthermore the idea to use the **F**ault **T**ree **A**nalysis (FTA) and the **F**ailure **M**ode and **E**ffects **A**nalysis (FMEA) to analyse the system's safety including EMI has been published.

Chapter 3

Electromagnetic Compatibility - Theory and Basics

A component is electromagnetic compatible if the emitted interference is low enough to not disturb other devices and if it is robust enough not to be disturbed by other sources of disturbance [33]. In the following sections, the source of disturbance (interference) is called aggressor and the component which might be influenced by this disturbance is called victim. Each active component can act as aggressor and as victim at the same time.
Each EMC problem is composed of a victim, a coupling path and an aggressor. Thereby, a coupling path connects an aggressor with a victim as shown in Figure 3.1.

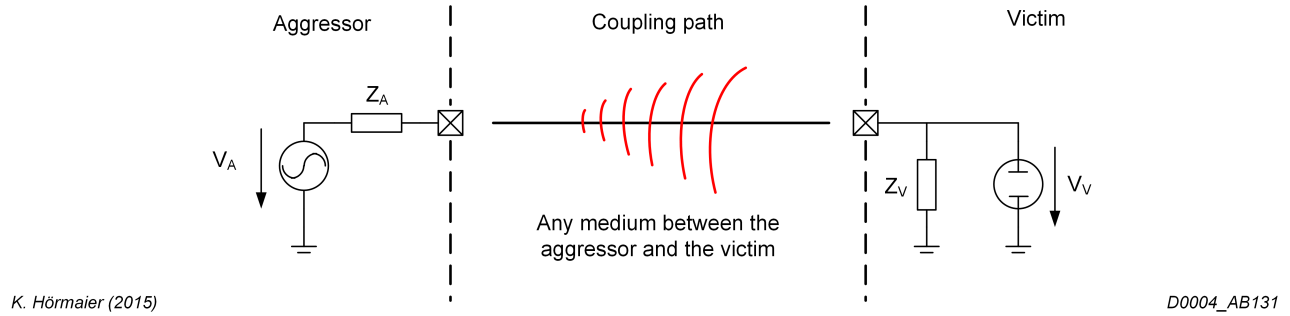


Figure 3.1: Sketched topology of an EMC problem consisting of the aggressor, the coupling path and the victim. In addition, the inner impedance of the aggressor and the victim are shown.

To mitigate or solve problems of missing EMC, countermeasures are needed. Due to the fact that each EMC problem consists of an aggressor, a coupling path and a victim, the following three different approaches can be used [34]:

- increasing the robustness of the victim,
- decreasing the emission generated by the aggressor or
- weaken the coupling between victim and aggressor.

Depending on the constrains one or a combination of approaches has to be used.

An EM wave, per definition, consists of an electrical and magnetic component. Nevertheless, in this work the term EM is used for all kinds of interference (including purely magnetic, purely electric and interference galvanically coupled to the victim).

In the literature several terms in context of EMC exist, which shall be shortly listed and roughly explained. **Electromagnetic emission** names the electromagnetic field which is generated and emitted by the aggressor. **Electromagnetic interference** names the electromagnetic field which might have the ability to disturb electrical / electronic systems. Sometimes, in older publications the term **Radio Frequency Interference (RFI)** is used instead of EMI. **Electromagnetic robustness** describe the ability to resist EMI its opposite formulation is the **electromagnetic susceptibility** which describes the weakness of the system regarding EMI.

3.1 Coupling

The victim is spatially separated from the aggressor. Thus, the interference generated by the aggressor needs a propagation mechanism to reach the victim, which is described by the coupling. Theoretically infinitely many coupling paths between a victim and an aggressor exist, but typically only some of them are effective. The effectiveness of the coupling describes the ability of the coupling path to transport the energy or power from the aggressor to the victim. Generally, the coupling can be subdivided into galvanic coupling, near-field coupling and far-field coupling. All these coupling mechanisms are sketched in Figure 3.2. Thereby, near-field coupling can be subdivided into either electric field coupling or magnetic field coupling. In comparison the far-field (radiated) coupling consists of an EM wave, whereby the EM wave always consists of an electrical and magnetic component. The following sections describe the coupling mechanisms in detail.

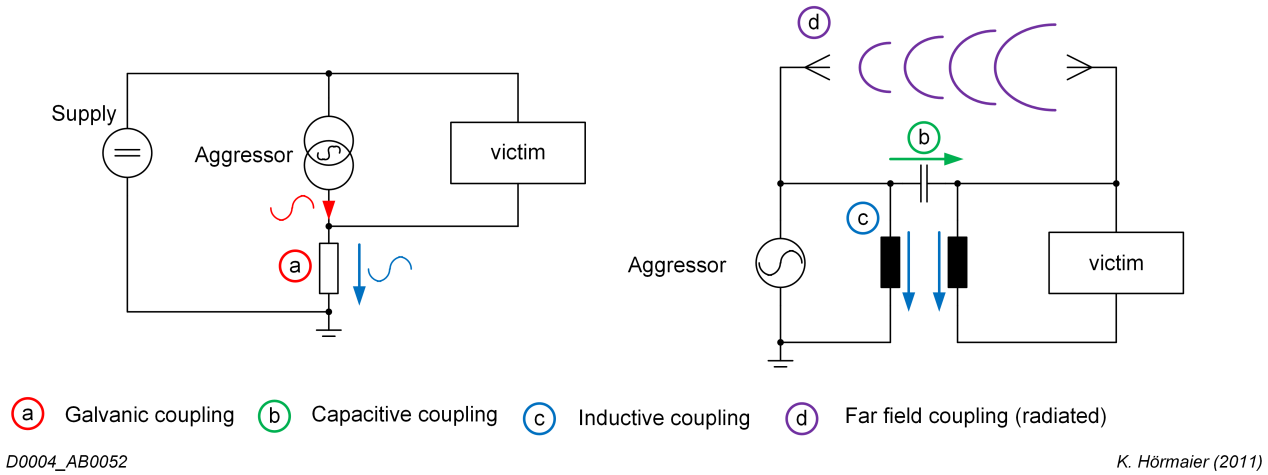


Figure 3.2: Different types of coupling between aggressor and victim.

All of the coupling mechanisms need certain structures at the victim and aggressor, to be relevant. Thus, the locations or structures through which interference can couple into a victim system are called injection points. The bulk of interference enters the system via these injection points, the remaining amount of EM power entering the system via other coupling paths is negligible.

3.1.1 Galvanic Coupling

Galvanic coupling is characterised by a common impedance between the aggressor and the victim. The aggressor current generates a voltage rise via a common impedance, possibly influencing the victim. The coupling can be calculated by Ohm's law:

$$v_{EMI}(t) = Z \cdot i_A(t) \tag{3.1}$$

with the interference voltage $v_{EMI}(t)$, the common impedance Z and the aggressor current $i_A(t)$. Thereby, the impedance typically depends on the frequency ($Z = f(f)$).

3.1.2 Capacitive Coupling

By capacitive coupling, the interference is transmitted via an electrical near-field from the aggressor to the victim. Thus a voltage difference is the source of emission. The coupling depends on the mutual capacitance between the aggressor and the victim. Depending on the geometry of the victim and the aggressor and other components in the surrounding the calculation of the mutual capacitance can get difficult. But not necessarily all geometries are complex. Many problems can already be covered by the equation for a parallel plate capacitor:

$$C = \varepsilon_0 \varepsilon_r \frac{A}{d} \tag{3.2}$$

C is the capacitance of two electric conductors of which, both have a parallel area A and a distance from each other of d with a medium in between with a constant permittivity $\varepsilon_0 = 8.8542 \frac{\mathrm{AS}}{\mathrm{Vm}}$ and a relative permittivity ε_r. For the calculation of a more complex layout the conductors can be divided into subelements equivalent to a plate capacitor and afterwards the subelements are summed up. Thus, the mutual capacitance C_m can be approximately calculated as

$$C_m = \sum_{1}^{N} C_n \tag{3.3}$$

where C_n is the capacity of the subelement on the position n and the number of subelements is N.
Since the geometrical structures might get very complex, the usage of sophisticated methods is advisable. Methods like the finite element method (FEM), finite difference method (FDM) or method of moments (MoM) which are used to calculate the EM problems are realized in a couple of commercially available software products. EMC Studio [35], for example, provides a useful framework to simulate EMI between cables and devices. The same is possible with FEKO [36]. Both tools allow defining a cable tree, attaching circuits and simulating the interference in terms of parasitic voltages, currents, and critical frequency ranges. Powerful hybrid tools such as COMSOL Multiphysics [37], also allow correct simulation of EMI providing a profound knowledge of electromagnetism. Tools supporting a straightforward extraction of parasitic elements (capacitances / inductances) of **P**rinted **C**ircuit **B**oards (PCBs) and ICs are ANSYS Redhawk [38] and CTS Studio Suite [39].
Beside the mutual capacitance, the impedance of the aggressor (Z_A) and the victim (Z_V) as well as the source frequency (f) are needed to calculate the coupling. According to Figure 3.1 the coupling factor ξ is:

$$\xi = \frac{Z_A + Z_V + \frac{1}{2i\pi fC}}{Z_V} \tag{3.4}$$

Finally the voltage at the victim side (V_V) can be calculated as:

$$V_V = \xi V_A \tag{3.5}$$

with the voltage at the aggressor (V_A).

3.1.3 Inductive Coupling

A inductive coupling occurs if the flux generated by a source (current conducting structure) flows trough the structure of the victim [40]. The coupling can be described by a mutual inductance (M). To illustrate the inductive coupling the following example shall be considered. Two wires, with a distance (d) between each other are routed parallel for the length (l). Considering the wires are only surrounded by air, the following equation can be used to calculate the mutual inductance (M) [40]:

$$M = 0.002 \cdot l \left(ln \left(1 + \frac{2l}{d} \right) + \frac{d}{l} - 1 \right) \tag{3.6}$$

By using the mutual inductance (M), the voltage (V) injected into the second wire by a dynamic current (di/dt) in the first wire can be calculated as:

$$V = M \frac{di}{dt} \tag{3.7}$$

For more complex structures tool support as described in Section 3.1.2 is advisable.

3.1.4 Far Field Coupling

The wave length of the EM wave can be calculated as follows:

$$\lambda = \frac{c}{f} \tag{3.8}$$

where, c is the speed of light and f is the frequency of the EM wave.
The material depending speed of light can be calculated by

$$c = \frac{1}{\sqrt{\epsilon_0 \epsilon_R \mu_0 \mu_R}} = \frac{1}{\sqrt{8.8542 \cdot \epsilon_R \cdot 10^{-12} \frac{\text{As}}{\text{Vm}} \cdot 4 \cdot \pi \cdot 10^{-7} \frac{\text{Vs}}{\text{Am}} \cdot \mu_R}} \tag{3.9}$$

with the permittivity of free space $\epsilon_0 = 8.8542 \cdot 10^{-12} \frac{\text{As}}{\text{Vm}}$ and the permeability of free space $\mu_0 = 4 \cdot \pi \cdot 10^{-7} \frac{\text{Vs}}{\text{Am}}$ as well as the, material depending relative permittivity ϵ_R and relative permeability μ_R.
EM radiated far-fields can only be emitted if an antenna with sufficient figure of merit is in place. The figure of merit depends on the wave length compared to the length of the antenna. A widely spread rule of thumb states that a steady wave can only be established, if the ratio of the wavelength (λ) compared to the length of the possible antenna is 1/20 [41].

3.2 Aggressor

The aggressor generates the EMI and therefore can be seen as the source of EMI. It is characterised by its **e**lectro**m**agnetic **e**mission (EME). The EME can have various generation principles. To act as aggressor, electrical power does not necessarily have to be generated like, for

example, in electrical machines. Rather the aggressors can also generate emission by acting as a load connected to an electrical power supply. The emission can either be generated due to the intended functionality or by unintended side effects. An example for intended emission are typically wireless communication interfaces using antennas to transport information from the transmitter to the receiver, or a wireless power transmitter device used to supply mobile consumer with electrical power. Examples for unintended generation of EME are voltage bouncing of a common ground net due to high switching currents or the fast change of lines voltage used as a communication interface.
All active electrical systems generate emission. The systems only differ by the emission they emit. To characterise the emitted emission, measurement standards have been published defining the setup and the measurement procedure in order to make products comparable. The following automotive related standards to evaluate the immunity regarding EMI are:

- CISPR 12 - Vehicles, boats and internal combustion engines – Radio disturbance characteristics – Limits and methods of measurement for the protection of off-board receivers
- CISPR 25 - Vehicles, boats and internal combustion engines – Radio disturbance characteristics – Limits and methods of measurement for the protection of on-board receivers

The CISPR 12 covers emission from the vehicle to the environment compared to the CISPR 25 which targets the emission of a subsystem inside the vehicle and remaining in the vehicle. Beside automotive the automotive standards the general standard IEC 61967 is used to measure the emissions generated by integrated circuits.

3.3 Victim

All electrical or electronic systems can be victims to EMI. Depending on their robustness, the systems can be more or less susceptible to EMI. Insufficient robustness leads to a loss of functionality or a deviation of the specified product characteristics, during the exposure to EMI. Figure 3.3 illustrates the failure characteristic of a device depending on the EMI amplitude. Depending on the failure characteristic a different selection of possible counter measures is available. The typical classification originated by the ISO and SAE standards [9] is slightly different. The standards divide the status into four classes:

- The function performs as designed during and after the test.
- The function does not perform as designed during the test but returns automatically to normal operation after the test.
- The function does not perform as designed during the test and does not return to normal operation without a simple driver/passenger intervention such as turning on and off the DUT or cycling the ignition switch after the disturbance is removed.
- The function does not perform as designed during and after the test and can only be returned to proper operation with more extensive intervention such as disconnecting and reconnecting the battery or power feed. However, the function shall not have sustained any permanent damage as a result of the testing.

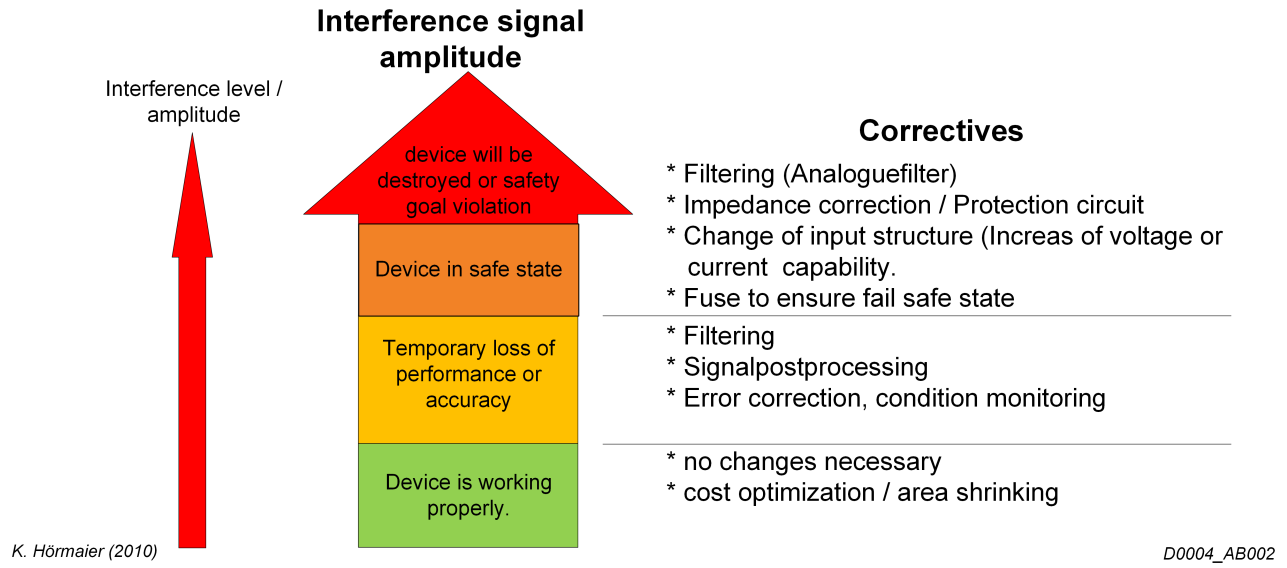


Figure 3.3: Depending on the robustness of the system and the EMI amplitude, the failure characteristic can change. Depending on the failure characteristic the selection of possible measures to mitigate the problem also changes.

Various root causes for problems on the victim side exist. The failures can mainly be caused by:

- voltage
- current
- energy

High voltage injected into the system can lead to a brake through of the electrical isolation. Often the path gets low-impedance and conducts high current, further leading to thermal destruction. Or the injected voltage changes the signal amplitude of a communication interface leading to loss of data or erroneous information.
Reference current sources or communication interfaces, encoding data by using current profiles, can be interfered by injected currents.
The injected energy can lead to overheating possibly causing a thermal destruction of the component. However, high temperature can also lead to untypically high parameter variation influencing the component's function.
For immunity testing of electrical components in the automotive domain the following standards are applicable:

- ISO 7637 - Road vehicles - Electrical disturbances from conduction and coupling
- ISO 11451 - Road vehicles - Vehicle test methods for electrical disturbances from narrow-band radiated electromagnetic energy
- ISO 11452 - Road vehicles - Component test methods for electrical disturbances from narrowband radiated electromagnetic energy
- IEC 62132 - Integrated circuits - Measurement of electromagnetic immunity, 150 kHz to 1 GHz

The ISO 7637 specifies test methods and procedures to ensure the compatibility to conducted electrical transients of equipment assembled in cars. It describes bench tests for both the injection and measurement of transients. The ISO 11452 and the IEC 62132 are very similar in their proposed methods. Both standards target radiated as well as conducted immunity tests. For radiated immunity tests the TEM cell method is used. For near-field coupling the bulk current method is proposed and as line coupled measurement method the direct radio frequency power injection method (DPI) is recommended.

Chapter 4

Functional Safety - Theory and Basics

This section will describe the mathematical basics needed for safety analysis and all common definitions and methods for safety analysis.

4.1 Terms and definitions

This section provides the important terms and definitions needed for a common understanding of the following chapters and sections. The majority of them match the definitions of the ISO 26262 Part 1. The first and most important definition term is the safety goal.
The **safety goal** describes what has to be realized to achieve functional safety. It formulates the avoidance of an unreasonable risk to humans and therefore can be seen as highest safety requirement. A violation of a safety goal would lead to an unreasonable risk. A safety goal example is given by the following: The airbag system assembled in a vehicle has to protect the driver in case of a accident. From the system's point of view, a accident can be detected if a high deceleration (= negative acceleration in driving direction) is observed. Thus the following requirement can be formulated: The driver front airbag shall deploy if the acceleration of the vehicle in negative drive direction exceeds the acceleration low level ($-XX_L\ m/s^2$).
Derived from the safety goal(s) are the **safety requirements**. The safety requirements formulate what the system shall do (behaviour, functionality). They are the basis for the design and for the verification. Thus they have to be precise in the sense that no misunderstandings, incompleteness or contradictions shall be included. Tools exist which support the requirements analysis such as [42].
The **Automotive Safety Integrity Level (ASIL)**, which is allocated to a safety goal and is comparable with Safety Integrity Level (SIL) ba,sed on IEC 61508 provides a measure for the importance of a safety goal. The importance depends on the severity of the hazardous event, the frequency of occurrence and the controllability. Details will be provided in Section 5.7.1.
Safety analysis is all about failures. A **failure** is the "*termination of the ability of an element to perform a function as required*" [1].
The most important characteristic of a failure is the failure rate. The **failure rate** is the frequency with which the system fails or as defined in [1] the "*probability density of failure divided by probability of survival for hardware elements*".

4.2 Mathematical Background

This section describes the mathematical background needed for failure rate, reliability, ... calculations. Basics can be found in [43].

Random Variables
A random variable is a property of a random experiment. Thus, a random variable maps a drawn sample to the real axis [44].
Random variables can be dependent or independent. If the two variables A and B are dependent random variables the probability that B is true is zero, if A is true and vice versa. Thus, if event A occurs, event B can not occur (see Figure 4.1). If A and B are independent variables and the event A occurred no information of B can be derived. Thus, if A occurred B might or might not occur as shown in Figure 4.1 on the right graph.

Figure 4.1: On the left side, the events A and B are dependent, however on the right side the events A and B are independent because a sample leads to the occurrence of the faults A and B or only one or none of them.

The resulting probability $Pr(A \cap B)$ of the intersection ($\cap$) of the two independent random events ($Pr(A) = 0.3$ $Pr(B) = 0.2$) can be calculated as:

$$Pr(A \cap B) = Pr(A) \cap Pr(B) = Pr(A) \cdot Pr(B) = 0.3 \cdot 0.2 = 0.06 \tag{4.1}$$

If the events are dependent, the probability of $Pr(A \cap B)$ is zero. For the calculation of the set union of the same two independent random variables ($\cup$) following equation can be used:

$$Pr(A \cup B) = Pr(A) \cup Pr(B) = Pr(A) + Pr(B) - Pr(A) \cdot Pr(B) = 0.3 + 0.2 - 0.3 \cdot 0.2 = 0.44 \tag{4.2}$$

For very small probabilities of $Pr(A)$ and $Pr(B)$ the cut-set terms $Pr(A) \cdot Pr(B)$ can be neglected which reduced the Equation 4.2 to:

$$Pr(A \cup B) = Pr(A) \cup Pr(B) = Pr(A) + Pr(B) \tag{4.3}$$

Cumulative Distribution Function (CDF)
The CDF $F(x)$ describes the probability that a random variable X is lower than the limit x.

$$F(x) = Pr(X < x) \tag{4.4}$$

For the CDF following equation applies.

$$\lim_{x \to \infty} F(x) = 1 \tag{4.5}$$

Probability Density Function (pdf)
The pdf $f(X)$ describes the distribution of the random variable's probability over the possible value range, with the area below the pdf equal to one. The pdf can be calculated by differentiating the CDF.

$$f(x) = \frac{dF(x)}{dx} \tag{4.6}$$

The other way around, the CDF can be calculated by integrating the pdf ($f(x)$) in the range from $-\infty$ to X.

$$F(x) = \int_{-\infty}^{X} f(x)dx \tag{4.7}$$

Complementary Cumulative Distribution function (CCDF)
The CCDF $\bar{F}(x)$ is given as:

$$\bar{F}(x) = 1 - F(x) \tag{4.8}$$

4.3 Reliability and Failure

4.3.1 Unreliability

The unreliability $F(t)$ describes the probability Pr that a component fails until the time t. The unreliability is mathematically described by the CDF shown in Equation 4.9.

$$F(t) = Pr(T \leq t) \tag{4.9}$$

where T is the random number describing failure time.

4.3.2 Reliability

The reliability $R(t)$ can be expressed by the relationship with the unreliability as:

$$R(t) = 1 - F(t) \tag{4.10}$$

Another way to express the reliability is via the probability as:

$$R(t) = Pr(T > t) \tag{4.11}$$

The equation states the probability Pr of the component surviving until the time t. The reliability is from the statistical point of view a CCDF ($= 1 - CDF$). The probability of survival starting at time $t = 0$ equals one. In other words, initially all systems work as expected but fail over time. After infinite time all systems failed, resulting in a reliability for $t = \infty$ of 0.

4.3.3 Failure Density

The probability $f(t)$ of a failure is described by the pdf,

$$f(t) = \frac{dF(t)}{dt} \tag{4.12}$$

It is the derivative of the unreliability $F(t)$. It gives the probability of a failure at a certain time.

4.3.4 Failure Rate Function

The failure rate function $h(t)$ (see Equation 4.13) is given as the division of the probability of failure $f(t)$ by the reliability $R(t)$. The unit of the failure rate function $h(t)$ is defined as failure per time.

$$h(t) = \frac{f(t)}{R(t)} \tag{4.13}$$

The above described characteristics are plotted in Figure 4.2 for the exponential failure distribution. The exponential failure distribution $F(t) = 1 - e^{-\lambda t}$ is typically used for electronic components to model the useful life period.

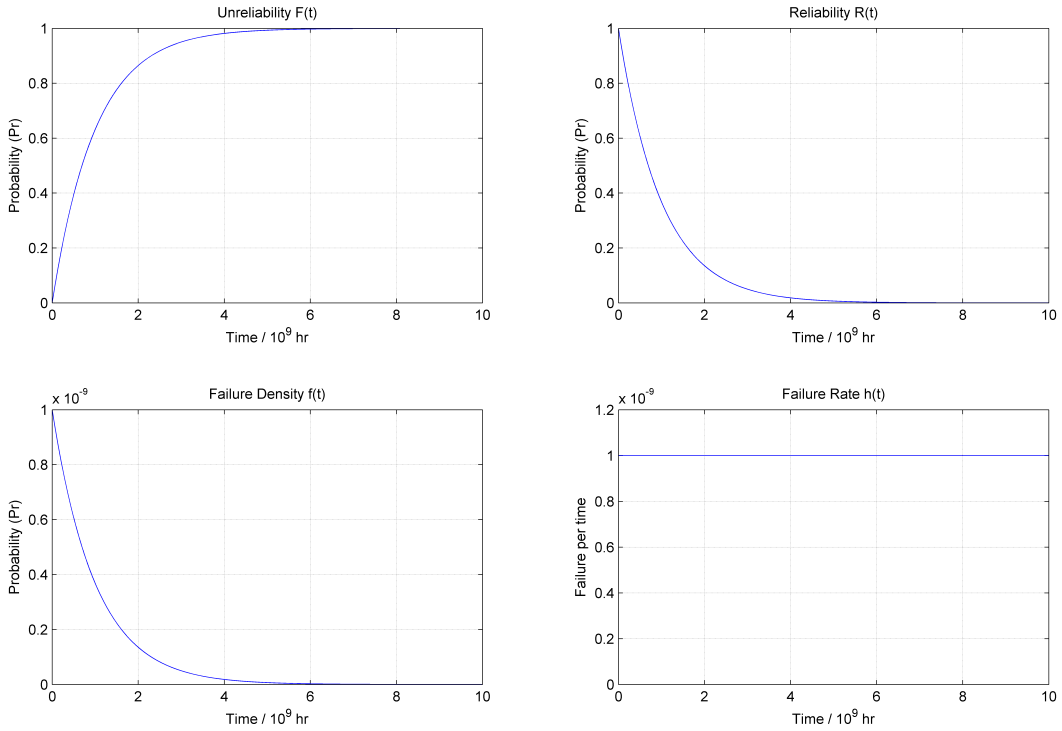


Figure 4.2: The subplots show the different characteristics for the exponential failure distribution. Plotted is $F(t) = 1 - e^{-\lambda t}$ *with* $\lambda = 10^{-9} \frac{\text{Failures}}{\text{Hour}}$.

4.3.5 Failure Rate

Safety standards such as the ISO 26262 limit the failure rate λ to certain values. For example, to achieve ratings of ASIL D, the standard permits a maximum failure rate for the item of $< 10^{-8}$ hours. When talking about the failure rate λ a constant failure rate function is assumed. This holds if the probability of failure is an exponential distribution $f(t) = \lambda e^{-\lambda t}$. In this case the failure rate function is

$$h(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \tag{4.14}$$

Values for components failure rates can be found in for example, [45] or [46].

4.3.6 Failure in Time

The failure rate is often expressed in **F**ailure **I**n **T**ime (FIT). Hereby the failure rate is normalized to 10^9 hours as shown in Equation 4.15.

$$\lambda_{FIT} = \lambda \cdot 10^9 \tag{4.15}$$

Thereby the unit of λ has to be one divided by hours $(1/h)$.

4.3.7 Failure Mode Distribution

Typically, the failure rate is assigned to a component, however the component can have several failure modes. Since different failure modes can lead to different effects on the components functionality, the safety analysis has to consider the failure modes and their characteristics separately. Thus, the failure rate has to be distributed accordingly over the individual failure modes. Therefore, the **F**ailure **M**ode **D**istribution (FMD) is used. The failure mode distribution (FMD) is a discrete distribution with N discrete values, where N is the number of failure modes. The failure rate of an individual failure mode $h_{COMP\_FM\_n}$ at the position n, for $n \in [1...N]$, is the component failure rate $h_{COMP}(t)$ multiplied by its FMD_n.

$$h_{COMP\_FM\_n}(t) = h_{COMP}(t) \cdot FMD_n \tag{4.16}$$

The sum of the values of the failure mode distribution has to be 1. An example is given for a resistor with four possible failure modes (short circuit, open circuit, reduced value to 0.5× nominal value and increased value up to 2× nominal value). Table 4.1 presents a possible failure mode distribution.

Table 4.1: Failure mode distribution of a resistor with four failure modes.

Failure Mode	Symbol	Contribution to Failure Mode
Short circuit	FMD_1	0.1
Open circuit	FMD_2	0.6
reduced value to 0.5× nominal value	FMD_3	0.15
increased value up to 2× nominal value	FMD_4	0.15

Assuming, the failure rate of the resistor $h_{COMP}(t)$ is given as 0.7 FIT. Applying Equation 4.16 the failure rate for the failure mode short circuit $h_{COMP\_FM\_1}(t)$ is 0.07 FIT.

4.4 Environmental Conditions

Each system operates in an environment which surrounds it. The environment, which interfaces with the system at the system boundaries, is characterised by several properties like:

- Temperature
- Vibration
- Pressure
- Mechanical stress

- Chemical substances
- Water / humidity
- Ionizing radiation
- **Electromagnetic interference**
- User inputs or other inputs (e.g., supply voltages)
- ...

The environment has a strong influence on the development. Each system has to be designed in such a way, that it operates within the environment as expected. The environment and its properties depend on the system's location. Investigating the environment for each new system would cost a lot of effort. Thus, the environment can roughly be classified as: military, space or aero space, industrial, automotive, medical, consumer where each domain has its specific characteristics from which the system requirements (e.g., temperature) can be derived. The environmental properties for these domains can also be found in standards like IEC 60721 [47] or AEC Q200 [48].

4.5 Fault-Error-Failure

One of the most important fundamentals in safety analysis is the distinction between [49]

- fault,
- error, and
- failure.

The fault is the initiating event (root cause) leading to an error. The error caused by a fault is a deviation of the function or behaviour from the fault free state. An example is a solder pad crack causing an increase of the resistance by 50%. In this example the increase of resistance is the error and the crack is the fault. The error might propagate possibly leading to a failure. Depending on the robustness of the design, not necessarily all errors lead to a failure. The strength of a system to prevent errors become failures is therefore called robustness. A failure itself again manifests in a specification violation. A failure is an unwanted behaviour of the designed element. An example is, that the car's brakes do not work (failure) because the braking peddle signal is too low (error).
As shown in Figure 4.3, fault-error-failure can be brought into the context of abstraction levels or hierarchy. A failure on the lower abstraction level represents a fault on the upper abstraction level [50].

4.6 Failure Modes

A component can fail with different failure modes. The failure mode is an abstract way to describe the behaviour of how the component fails. The failure mode becomes active with the fault, and remains activated as long as defined by the fault classification (this terminology will be further explained in Section 4.8). A component can have several failure modes depending

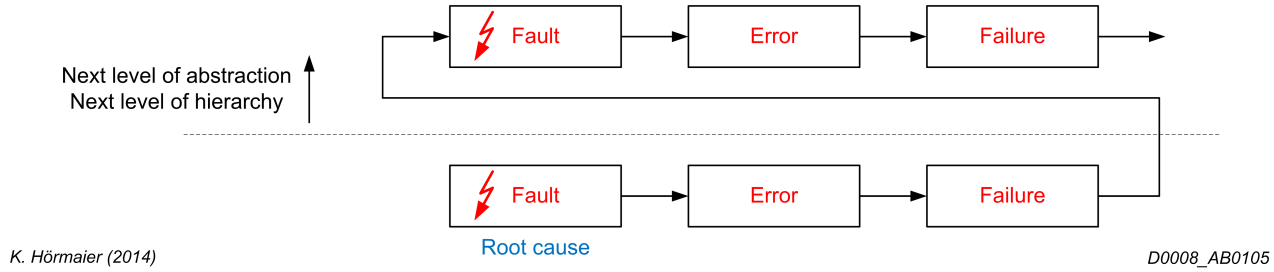


Figure 4.3: The hierarchical propagation of a fault is shown. A fault causes an error which further causes a failure. And a failure of the lower abstraction level gets a fault in the higher abstraction level [50].

on its functionality. The knowledge of the failure modes is the basis for safety analysis. An example is a metal film capacitor could have three different failure modes: short circuit, open circuit and change of value ($C < 0.5C_N || C > 2C_N$) [51].
In a tailored development process, it's the supplier's responsibility to deliver the failure modes to the system integrator. However, only the failure modes on the highest abstraction are of interest.

4.7 Fault Model

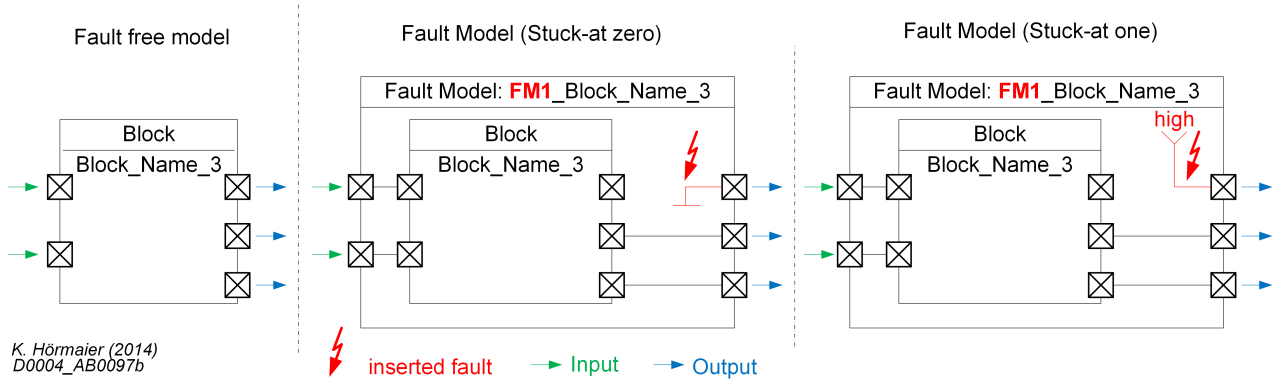


Figure 4.4: The Normal (fault free) model of a component can, for safety analysis, be replaced by its fault models. The fault models consist of the same interfaces as the normal model but have a changed behaviour due to the included faults. For example the faults stuck-at zero and stuck-at one are shown in the two fault models.

The fault model is generic representation of a failure (see ISO 26262 Part 1 1.43). The failure mechanism, which *is the physical, chemical, or other process which results in failure* [52, p. 101] is similar to the fault model. The fault model is a mathematical / physical model which replaces the functional model used for simulating the normal (fault free) behaviour. A well-known and easily understandable fault model is for example the stuck-at fault. The stuck-at fault model represents the loss of ability to change from on-state to the off-state or vice versa. In this case, in the fault model, the output is disconnected from the normal (fault free) functional block and instead connected to zero or one as shown in 4.4. Fault models can be constructed for all levels of abstraction. Often, measurements are used to get the behaviour of a component in a failure

mode. An example is found in [53] where the characterisation of electronic switches without destruction has been shown.

4.8 Fault Classification

Faults are classified into two main categories, **systematic faults** and **random faults** [54]. Systematic faults are caused by designers during development. A systematic fault is permanently present but might not affect the system's functionality permanently. Whether the fault has an impact on the functionality may additionally depend on external conditions or system inputs.
Random faults are due to physical causes such as corrosion, thermal stressing and wear-out. Random faults could be represented by random variables and therefore statistical methods shall be applied. Further distinction on the occurrence of random faults is also possible. Random hardware faults can be sub-divided into the following fault occurrence classes [50]:

- transient fault,
- intermittent fault and
- permanent fault.

Transient faults occur once for a certain short time span and will not be present afterwards. The most famous example is a fault caused by α-particles. On the basis of a flip-flop the transient fault will be exemplified. The flip-flop consists of several transistors, building a 1 bit information storage. An α-particle, hitting a transistor gate, may charge this gate possibly leading the transistor to change its state, subsequently leading to a bit flip of the flip-flop. As soon as new information is latched in the flip-flop, its functionality is again available and correct.
Intermittent faults randomly appear (occur / get active) and disappear. An example for an intermittent fault is a loose connection.
The **permanent fault** stays active once it appears. The permanent fault can only be dissolved by repair or replacement. Consider a transistor which has been thermally over-stressed leading to a melting of the connections (open circuit). Thus, the transistor loses its ability to switch current. The behaviour or function is permanently changed. There is no self-healing of melted connections.
Developing a safe product means responsibility for all engineers involved and is a challenging task requiring profound experience. Unfortunately, it is often impossible to create a safe product that is 100% safe, since it is impossible to consider all combinations of unlikely random events that may lead to failures[1]. Standardization committees are aware of this fact and have taken this into account when creating the ISO 26262. Not only can hardware fail, but also the functions that it should carry out. Thus, safety standards require the developed product to be free of systematic faults, but not necessarily free of random hardware faults. To be on the safe side, the accepted probability of failing is limited depending on the assigned ASIL level[2]. This is reflected in the random hardware failure rates (see. ISO 26262 Part 5 Clause 9.4.2.1). To be on the safe side engineers have to take care to achieve these limits or rates. An example for ASIL D, which is the highest safety level, ISO 26262 claims a failure rate of $< 10^{-8}\mathrm{h}^{-1}$.

[1]The safety standard targets only safety related functions which can be identified by safety analysis like fault tree analysis or dependent failure analysis.

[2]The ASIL level depends on the controllability, the exposure rate and the severity of hazardous event on system level.

4.8.1 Dependent Failure

For dependent failures, the occurrence of two failures at the same time increases due to a dependency on a certain event. As shown in Venn diagram (Figure 4.5) the occurrence of the event (CCI) changes the probability of the simultaneous occurrence of the events A and B. Thus, a random sample which is in the overlapping area of A and B will trigger the events A and B simultaneously. The overlapping O of the areas A and B can be within the boundary $O = (0...1]$.

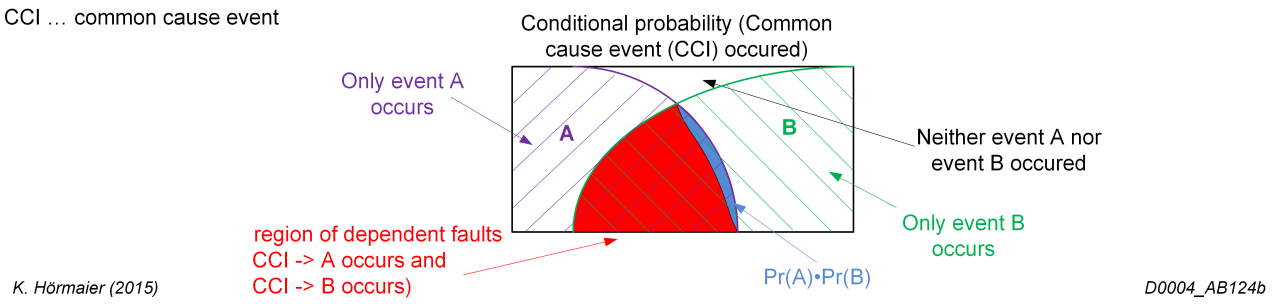


Figure 4.5: The Venn diagram shows the probability that the events A and B occur assuming that a common event (CCI) happened. The probability which is over the whole are one, can be separated into the following probabilities: the probability that not A and not B occurred, the probability that only A occurred, the probability that only B occurred, the probability that A and B occurred randomly simultaneously and the probability that A and B occurred because of the same event (their dependency).

4.8.2 Common-Cause Failure

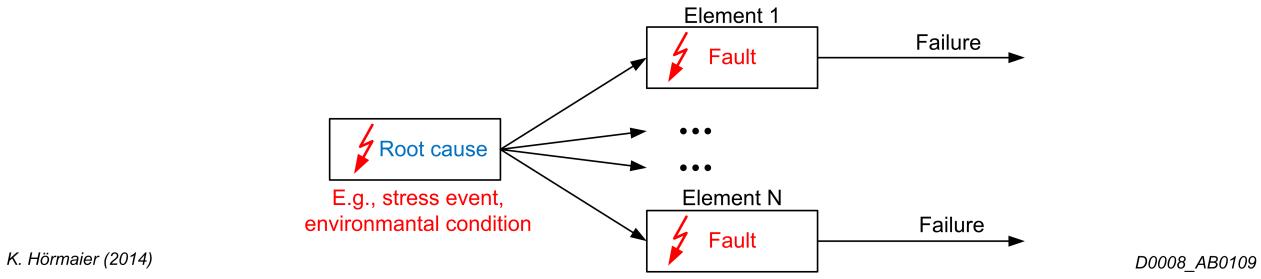


Figure 4.6: A single root cause leads to parallel faults further leading to multiple failures. Thus several components might fail due to the same (common) cause. Such a failure is therefore called common cause failure.

The common-cause failure is defined as the failure of more than one component due to the same cause (root cause) as shown in Figure 4.6. Common-cause failures are a subset of the dependent failures [55], as discussed in Section 4.8.1. Possible common-cause failure sources are for example, high temperature or fire, shared or common resources, seismic events, floods, **EMI**. The main problem of common-cause failures is that they can eliminate the advantages of a redundant system [56]. In a redundant system one function has to be realized / implemented more than one time, so that in case of a fault one implementation takes over the workload of the failing function. It shall be noted, that for the functionality of a fault free system no redundant

functions are needed. To overcome the problem caused by common-cause failures, redundancy shall be extended by diversity. In diverse designs, the same function is implemented in different ways or technologies so that faults cannot effect both implementations at the same time.
In ISO 26262-Part 1 [1] the definition of the common-cause is represented as shown in Figure 4.7 (a). It clearly shows the failing of several components due to one root cause. In comparison, in [57] the definition of common-cause failures has been extended by coupling factors. As shown in Figure 4.7 (b) unfortunately the representation proposed by [57] misses representing the failing of several components. Thus, both representations are not optimal. Nevertheless, the combined view with focus on EMI will be provided in Section 5.4.6.

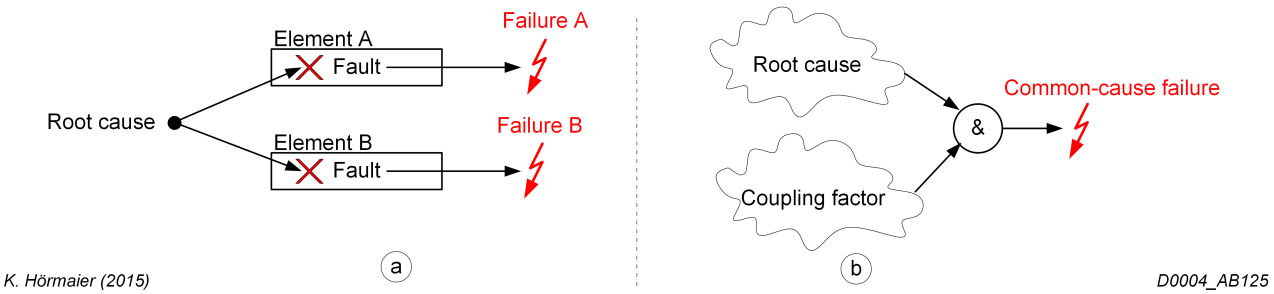


Figure 4.7: Graphical representation of the two different definitions of the common-cause failure. Both representations are somehow not optimal. The left (a) definition [1] misses the explicit labeling of the coupling pathes and the right (b) definition [57] misses the resulting failures caused by the common-cause failure.

4.9 Failure Characteristics

To describe failures and especially their time dependent behaviour several characteristics used in reliability engineering are summarized. This section is based on [56, 58, 59], in which detailed description can be found. The characteristics describe random hardware faults and their probability to occur. Randomness of hardware faults implicates the need for statistical methods. Random hardware faults can mathematically be described by a random number.

4.9.1 Failure Rate over Operating Time

The failure rate of electronic components is typically not constant over the operating time[3]. At the beginning as well as at the end of the operation time an increased failure rate typically leads to a failure distribution resembling a bathtub. As shown in Figure 4.8 the lifetime of an E/E component can be separated into three major phases:

- Period of early failure
- Useful life period
- Wear out period

[3]The operating time is defined according to ISO 262626-1:2011 1.82 [1] as "*cumulative time an item or element is functioning*".

A component's life starts with a period of early failure, where the failure rate decreases until it continues with the useful life period. Here the component exhibits a constant failure rate. Finally the component's life goes for the wear out period characterised by an increasing failure rate.

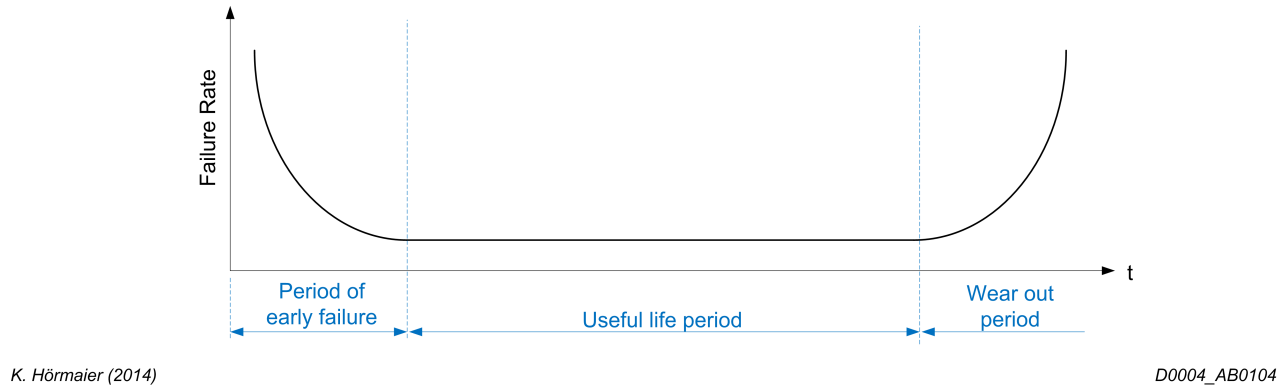


Figure 4.8: The bathtub curve models the time dependency of the failure rate of electronic components.

4.9.2 Environmental Stress

This section will describe the influence of the environment seen as stress [52]. Characterising the failure rate of a part included in a component is economically not possible. Thus, the failure rate from the same type as the part, will be used. Thereby, typically the load conditions or environmental conditions of the included part and the characterised part (reference part) are not identical. However, the load conditions or environmental conditions can have a significant influence on the resulting failure rate. The external conditions like temperature, voltage, current, etc. can be seen as stress applied to the part leading to pre-aging and a change of the failure rate. Thus, the external conditions at which the failure rate is valid have to be known. With the relationship between the failure rate and the stress, the failure rate of the included part can be calculated. A summary of relationships between failure rate and stress can be found in IEC 61709. The most common relationship between temperature as a stress factor and the failure rate is given by the Arrhenius Equation:

$$AF = e^{\frac{\Delta E}{k}\left(\frac{1}{T_{Ref}} - \frac{1}{T_{Stress}}\right)} \tag{4.17}$$

with the acceleration factor (AF), the Bolzmann constant ($k = 1.38 \cdot 10^{-23} \frac{\mathrm{VAs}}{\mathrm{K}}$), the activation energy (ΔE), the temperature of the reference part T_{Ref} and the temperature of the included part T_{Stress}. With the acceleration factor the resulting failure rate $h(t)$ with the increased stress can be calculated as

$$h(t) = AF \cdot h_{Ref}(t) \tag{4.18}$$

with h_{Ref} the failure rate of the reference part.

4.10 Hardware architectural metrics

To ensure certain levels of safety, additional characteristics have been introduced by the ISO 26262. Firstly, faults are classified to one of the below listed groups, followed by the calculation of fault metrics. Thus, faults are classified as:

- single-point,
- residual,
- multiple-point or
- safe faults.

In ISO 26262 the fault metric refers to constant failure rates λ. The following explanations summarize the definitions provided in ISO 26262 [1].
A **single-point fault** is a fault which directly leads to a safety goal violation. No additional fault is needed for a single-point fault to lead to a safety goal violation. A single-point fault cannot be detected or controlled by a safety mechanism. The failure rate for single-point failures, which results from single-point faults is λ_{SPF}.

A **residual fault** is the portion of a fault, which is not covered by a safety mechanism and thus leads to safety goal violation. The portion covered by the safety mechanism is assigned to the multiple-point faults. The residual fault failure rate is given as λ_{RF}.

A **multiple-point fault** is the combination of more than one independent fault. A multiple-point fault with the failure rate λ_{MPF}, can lead to a multiple-point failure implying a safety goal violation. Since not necessarily all multiple-point faults lead to a safety goal violation, an additional distinction is made as: Multiple-point faults can be subdivided into multiple-point faults latent $\lambda_{MPF,L}$ and multiple-point faults detected or perceived $\lambda_{MPF,DP}$ as given by:

$$\lambda_{MPF} = \lambda_{MPF,L} + \lambda_{MPF,DP} \tag{4.19}$$

Multiple-point faults detected or perceived are the portion of multiple-point faults which a safety mechanism covers or the driver perceives. Perceived faults are very specific for vehicles' functional safety, since a driver is available.
As example: A fault can be perceived as strange noise of the car or changed behaviour during braking which the driver can recognise. A multiple-point fault latent cannot be detected or perceived. The fault remains undetected within the system. An additional fault together with the latent fault might lead to a safety goal violation.
On the other hand, multiple-point faults latent are more dangerous because they remain undetected in the system. The repair rate for undetected (latent) faults is zero. The order of a multiple-point fault specifies the number of faults which can occur.

A **safe fault** is a fault in a safety related element which does not directly or indirectly violate a safety goal. The failure rate of a safe fault is represented by λ_{SF}. Important is to notice, that according ISO 26262 multi-point faults with a higher order than two can be considered as safe faults, except if the relevance of more than two independent faults is shown in the safety concept they must not be considered as safe fault. This assumption reduces the effort to be spent on safety analysis, dramatically.

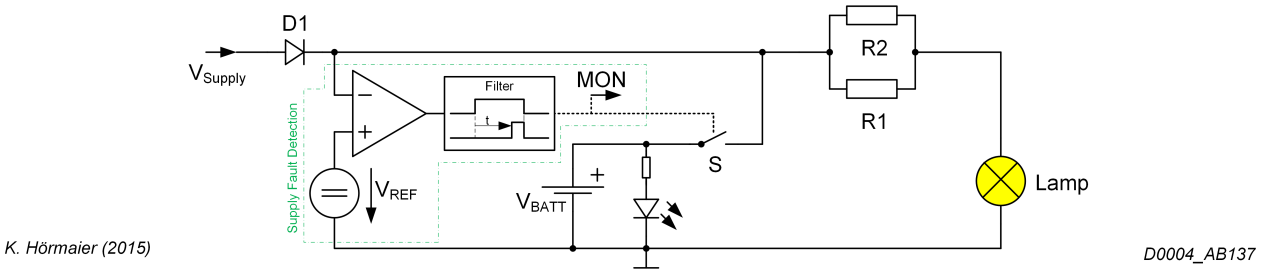


Figure 4.9: Schematic of the safety relevant circuit. The safety goal, which the circuit shall fulfill is to provide light permanently.

The previously listed fault types will be explained taking the circuit shown in Figure 4.9 into account. The system's function which equals its safety goal is to provided light permanently (e.g. light of an emergency exit). First, the system's functionality will be explained followed by the fault examination.
The system is supplied by the external supply voltage and in case of an external supply fault, a battery takes over the supply of the system within the fault tolerant time interval (see Section 4.12). The failing of the external supply can be detected by the supply fault detection circuit which closes the switch S to connect the battery with the lamp circuit. Thereby the diode $D1$ is required to prevent revers current into the external source which would shorten the battery voltage. The detection circuit includes a filtering function which activates the switch S only a certain time after the external supply decreased below the under-voltage detection level V_{REF}. In addition the battery voltage level function is monitored and battery faults are indicated by the light loss of the light emitting diode LED. The last function of the system, realized by the two resistors $R1$ and $R2$, is the adjustment of the lamp brightness.

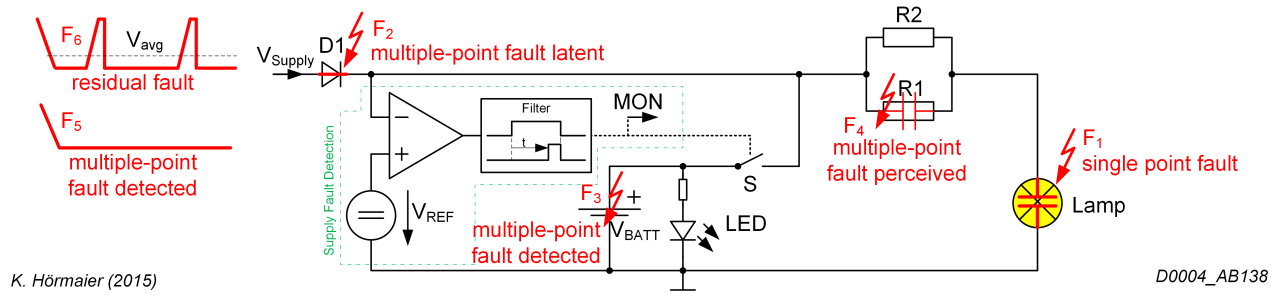


Figure 4.10: The schematic shown in Figure 4.10 has been modified by including faults. The injected faults are shown in red color and shall highlight the different possible fault classes.

Different faults are inserted into the system as shown in Figure 4.10 and explained in the following: The lamp fault ($F1$) directly leads to the loss of light, which equals the violation of the safety goal. Thus, this fault has to be classified as single-point fault. It is the only single-point fault in the circuit because for all other faults, a safety mechanism is in place.
The fault ($F4$) of the resistor $R1$ will not lead directly to a loss of light. The light will be off only if the second resistor fails additionally. Thus, this fault is classified as multiple-point fault. Since the fault also leads to a reduced brightness, which is assumed to be recognized by the operator, it can be classified as multiple-point fault perceived when going into detail.
A "short" of the diode (F2) will not have an effect on the lamp. However, with an external supply short circuit in addition, it would lead to a break down of the lamps voltage supply

Table 4.2: Recommended Values for the Single-Point Fault Metric and Latent-Point Fault Metric

	ASIL B	ASIL C	ASIL D
SPFM	$\geq 80\%$	$\geq 97\%$	$\geq 99\%$
LFM	$\geq 60\%$	$\geq 80\%$	$\geq 90\%$

leading to the safety goal violation. Since no detection mechanism is in place which is able to detect the diode's failure mode "short", this fault will remain in the system undetected. Thus this fault (failure mode) is classified as multiple-point fault latent.
A battery fault violates the safety goal only in combination with the external supply fault and the fault is detected due to the LED. Thus, this fault can be classified as multiple-point fault detected.
The fault caused by the external power supply has two different failure modes ($F5$ and $F6$) as sketched in Figure 4.10. If no safety mechanism is in place, both faults would lead to a safety goal violation. For the failure mode $F5$ the supply fault detection activates the safety mechanism realised by the battery supply, as expected. Thus, this fault is considered as multiple-point fault detected. On the other hand, due to the supply fault detection circuit's filter characteristic the $F6$ is not detected and therefore the switch S is not closed. The voltage of the external supply is insufficiently high to generate light and the battery is not activated. Therefore, the fault will lead to a safety goal violation. There is a safety mechanism (supply fault detection), but it does not cover this particular failure and is therefore classified as residual fault.

Diagnostic Coverage
To get quantitative failure rates for these fault classes, additionally the diagnostic coverage has to be determined. The diagnostic coverage gives the portion of an element's failure rate which can be detected or controlled by a safety mechanism (ISO 26262 Part 1 1.25 [1]).

Single-Point Fault Metric and Latent-Fault Metric
The single-point fault metric *SPFM* and the latent-point fault metric *LFM* are characteristic values for safety. The single-point fault metric can be calculated as given by the ISO 26262 Part 5 Annex C:

$$SPFM = 1 - \frac{\sum\limits_{SR,HW} (\lambda_{SPF} + \lambda_{RF})}{\sum\limits_{SR,HW} (\lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{SF})} \tag{4.20}$$

Thus, the Single-Point Fault Metric provides a relative robustness rate of an element.
The latent-fault metric can be calculated using the following equation:

$$LFM = 1 - \frac{\sum\limits_{SR,HW} \lambda_{MPF,L}}{\sum\limits_{SR,HW} (\lambda_{MPF} + \lambda_{SF})} \tag{4.21}$$

Note that for the single-point fault metric as well as for the latent-fault metric, only faults in a safety-related hardware element (*SR,HW*) have to be considered. Depending on the ASIL level different minimal ratings shall be achieved. In Table 4.2 the recommended values by ISO 26262 for the single-point fault metric and latent-fault metric are shown.

4.11 Analysis Methods

Many different methods for safety analysis have been proposed in literature and have been state of practice for several decades. Depending on the purpose or goals of the analysis a certain method or a combination of methods fits best. The following list provides a summary of the most famous or commonly used methods for safety analysis. The list is not exhaustive but shall include the methods which are applicable for EMC.

- hazard analysis and risk assessment (HARA)
- fault tree analysis (FTA)
- common cause analysis (CCA)
- dependent failure analysis (DFA)
- dependency fault tree analysis (DFTA)
- Failure Mode and Effects Analysis (FMEA)
- Failure Mode, Effect and Diagnostic Analysis (FMEDA)

In the following a comprehensive description of the listed methods is given.

4.11.1 Hazard Analysis and Risk Assessment (HARA)

Safety analysis typically starts with the **H**azard **A**nalysis and **R**isk **A**ssessment (HARA), which results in defined safety goals as well as in the safety goals' ASIL ratings. On the basis of the functionality, all operation situations shall be composed first. Afterwards possible hazards are collected using different methods like brain storming techniques, analysis of past accidents, FMEA etc. These hazards are further used to formulate safety goals.
The collection process is followed by the risk assessment. As described in [60] page 1606, risk assessment consists of three parts:

- event scenario
- probability of occurrence
- consequence

The event scenarios are the different system's operation modes. For each of the operation modes, the probability of occurrence is determined using a predefined template. In ISO 26262 Part 3 this is done by classifying the probability of exposure (E), which is the probability of occurrence, into five categories between incredible and high probability. In the next step, the consequence of a hazard is described by the severity (S) of harm to humans in case the hazard occurs. The classification is again given in ISO 26262 Part 3 with four classes starting from no injuries ending with life threatening injuries or fatal injuries. Specifically, ISO 26262 additionally requests the assessment of the controllability (C) of the hazardous situation, which is untypical for this type of assessment. This allows to take the driver, and his ability to control hazardous situations into account. Thus, the ISO 26262 explicitly includes the driver in the risk assessment. And finally, by combining the information of severity (S), exposure (E) and controllability (C), the safety goal's ASIL rating is obtained.

4.11.2 Fault Tree Analysis (FTA)

One of the recommended safety analysis methods in [1] and [61] is the FTA. A detailed description of the FTA can be found in the "Fault Tree Handbook" [62].
The FTA is a deductive analysis method (top-down), used as a systematic method to show critical paths in order to define safety measures and safety mechanism. Thereby, the FTA can be conducted qualitatively or quantitatively. In Addition, with the FTA both systematic failures as well as random hardware failures can be examined. Thereby, the FTA is a two-step process consisting of the fault tree construction and the analysis of the constructed fault tree regarding a violation of the safety requirements. These two steps will be described in detail in the next sections.

Fault Tree Construction

As for all deductive methods, also the FTA construction starts from the top with a top event. The top event is the violation of at least one safety requirement as shown in Figure 4.11, or a hazardous event. Thus, the top event is the event to prohibit.
In the first step all functional failure modes, leading to the occurrence of the top event are identified. The different failure modes are connected together via logic operators depending on the system's architecture or system's functionality. Failure modes of a lower detail level are connected via logic operators to the failure modes of a higher detail level. The stepwise construction of the fault tree ends with events which build the bottom line of the fault tree. Basically, the bottom of the fault tree can be of the following types:

- Basic Event
- Conditioning Event
- Undeveloped Event
- External Event [62] or Trigger Event [56]

The **Basic Event** represents all faults which will remain permanently in the system, whereas intermittent faults can also be accounted to this event due to the intermittent faults' repetitive occurrence.
The **Conditioning Event** is used to connect two events at which the second event has only an influence if the first event occurred.
For all existing events which are negligible, because their probability is obviously very low, the **Undeveloped Event** is used. It shall indicate that the safety engineer has not forgotten the event but judged as expert that the event is not important for the analysis. Thus, it is for dissertational purpose only.
Finally, the **Trigger Event** represents all transient faults.
All those described types (initiators) are condensed in the term primary event.
Those faults can even be abstract, thus it is not necessary to go to the physical level during fault tree construction. No formal requirement exists stating when to stop the construction of the fault tree. Thus, the safety engineer judges by himself when to stop, which needs experience.
Depending on the type of FTA, qualitative or quantitative, additional information has to be assigned to the faults. For the qualitative FTA no further information is needed, but for the quantitative analysis, the failure rate of each fault has to be added to the primary event.

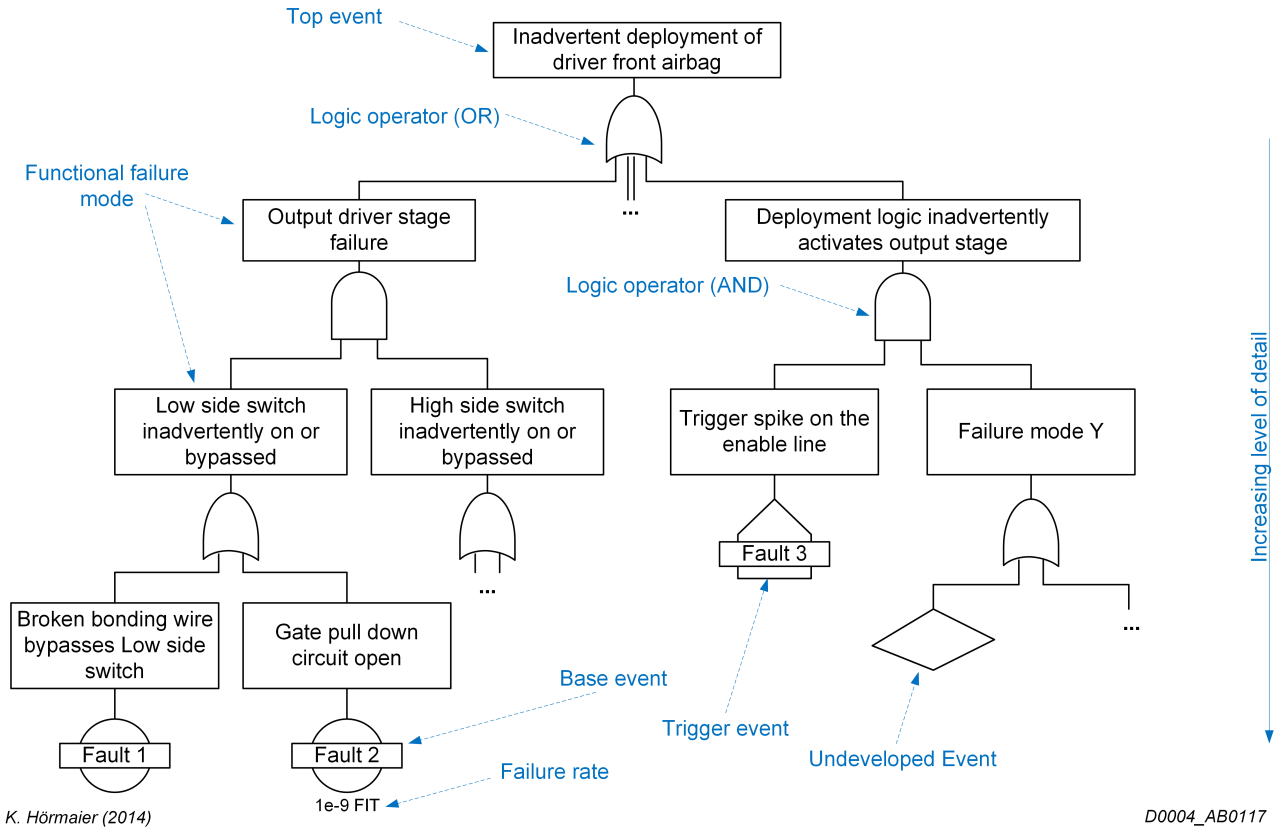


Figure 4.11: Extract of an airbag's fault tree.

Fault Tree Analysis

After the construction of the fault tree two ways of further analysis are possible:

- qualitative analysis or
- quantitative analysis.

The qualitative analysis is a cut-set analysis (or minimal cut-set analysis). A cut-set is a combination of primary events which have to occur in order to lead to the top event. The minimal cut-set indicates the minimal number of primary events to occur in order to trigger the top event. An example is, if the minimal cut-set is one, the primary event is a single point failure (one failure will directly lead to a safety goal violation). A design shall have at least a minimal cut-set of two otherwise, safety measures or safety mechanisms have to be put in place. Since no quantitative information (failure rate) is available, the qualitative analysis targets only the structure of the fault tree. It mainly helps to take appropriate architectural decisions to ensure a safe design.
On the other hand, the quantitative analysis provides more information because the failure rates are assigned to all primary events. Depending on the logic operators, failure rates for the hierarchically higher failure modes can be calculated, leading to the probability of occurrence of the top event. By using the laws of combining probabilities, provided in Section 4.2 the top event's failure rate can be obtained. The task of fault propagation calculation might not be executed manually but automatically by software tools. Several tools exist, which are also commercially available, supporting the engineer not only with the calculation but also with the construction of the fault tree. Furthermore, those tools provide a visualization of the results as

well as useful extras such as sorting and displaying the cut-set in the order of importance. A famous selection of these tools is:

- ISOGraph - Reliability Workbench (Faulttree+) [63]
- ikv++ - medini analyzer [64]
- APIS Informationstechnologien GmbH - APIS IQ-FMEA [65]

4.11.3 Dependent Failure Analysis (DFA)

The **D**ependent **F**ailure **A**nalysis (DFA) is an analysis which targets finding all dependent failures in the developed system. Thus, it considers common cause failures as well as cascading failures. A system consists of a huge number of elements which leads to an even higher number of faults and combination of faults. Consider a system with N elements and each of the elements can have at least one fault, the number of fault combinations to be analysed is $\binom{N}{2}$. An example is, for 10.000 components the number of combinations is larger than $50 \cdot 10^6$ combinations. This amount is not only unfeasible but also unnecessary. By filtering the number of carried out analysis tasks can be reduced. Thus, only these failures are considered which in combination lead to a safety goal violation. Thus, the DFA targets the analysis of redundant functions and safety mechanism, which might be shot down by the dependent failures.
Applying the concept on the fault tree (**D**ependency **F**ault **T**ree **A**nalysis (DFTA)), only the combination of faults which are connected via logical "AND" gates have to be analysed. Thus, faults which are connected via logical "OR" gates should not be analysed because the failing of two components simultaneously has the same impact on the safety goal as failing of one component (One component is sufficient for fault propagation). In Figure 4.12 the fault tree detail showing two dependent faults and their common portion is illustrated. The two faults (*Fault1* and *Fault2*), which are on divers branches of a logical "AND" gate, are assumed to be dependent. Thus, a new initiator, representing the common cause portion of the failure rate, depicted in red is added to the fault tree above the "AND" gate. By adding the new initiator both faults can be further treated as independent, but their failure rates have to be updated by subtraction of the common portion. A common method to consider dependencies is the use of the β-factor. The β-factor gives the portion of a fault which is common with another fault. Thereby the portion β is a number between zero and one. The resulting failure rates for all three initiators can be calculated using the equation provided in [56] as:

$$\lambda_C = \beta \cdot \lambda \tag{4.22}$$

with the failure rate of the common initiator (λ_C), the β-factor (β) and the origin failure rate (λ) of the component with the lower failure rate. The adapted failure rate of the components (λ_I) can be calculated as:

$$\lambda_I = (1 - \beta)\lambda \tag{4.23}$$

where, λ_I can be seen as the independent failure rate of the component [66]. The β-factor, designed for identical components with the same failure rate, can be used also for components with different failure rates. If the failure rate of the components differ, the basis for the calculation is the failure rate of the component with the lowest failure rate. Thus, the Equations 4.22 and 4.23 have to be adapted leading to

$$\lambda_{CC} = \beta \cdot \min(\lambda_1 \dots \lambda_N) \tag{4.24}$$

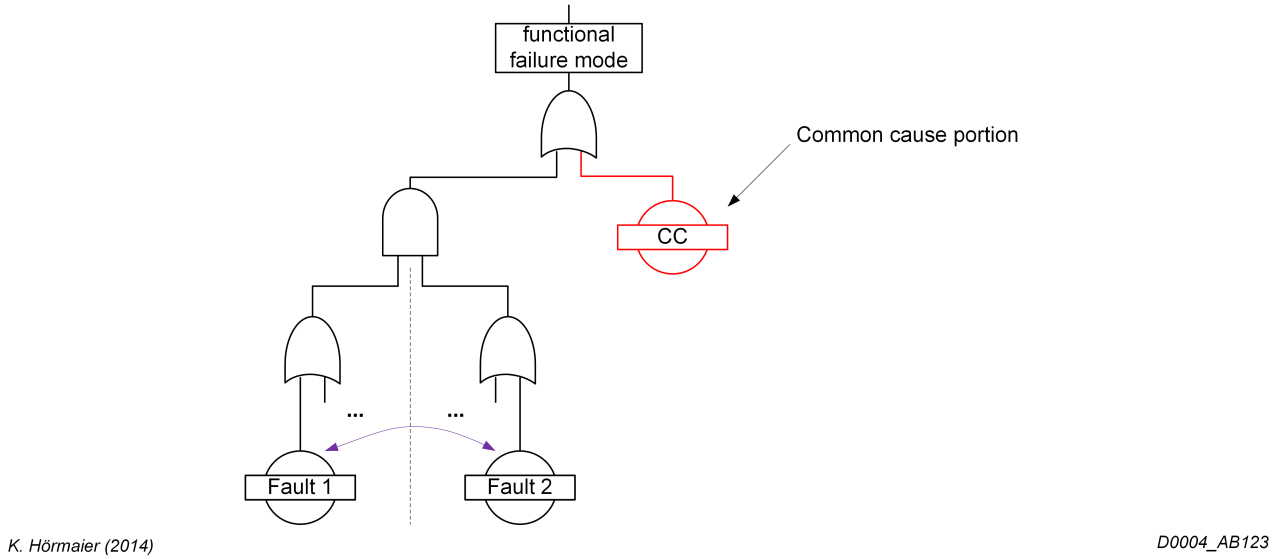


Figure 4.12: Dependent faults within a fault tree. The common portion of the faults (Fault1) and (Fault2) is given by the fault initiator labled as CC. [57]

$$\lambda_{In} = (1 - \beta \cdot \min(\lambda_1 \dots \lambda_N)) \cdot \lambda_n \tag{4.25}$$

where N is the number of faults and λ_n is the failure rate of the n-th element. The next example will show the usage by considering two faults (*Fault*1) and (*Fault*2) with the original failure rates of $\lambda_1 = 10$ FIT and $\lambda_2 = 3$ FIT. The failure rates, considering the dependencies with a β-factor of 0.01, can be calculated as follows:

$$\lambda_{CC} = \beta\lambda_2 = 0.01 \cdot 3 \text{ FIT} = 0.03 \text{ FIT} \tag{4.26}$$

$$\lambda_{I1} = \lambda_1 - \lambda_{CC} = 10 \text{ FIT} - 0.03 \text{ FIT} = 9.97 \text{ FIT} \tag{4.27}$$

$$\lambda_{I2} = (1 - \beta)\lambda_2 = (1 - 0.01) \cdot 3 \text{ FIT} = 2.97 \text{ FIT} \tag{4.28}$$

Resulting in a total failure rate λ of:

$$\lambda = \lambda_{CC} + \lambda_{I1} \cap \lambda_{I2} = 0.03 \text{ FIT} + 9.97 \text{ FIT} \cap 2.97 \text{ FIT} \approx 0.03 \text{ FIT} \tag{4.29}$$

4.12 Safety Measures and Safety Mechanism

Firstly the difference between the terms **safety measure** and **safety mechanism** shall be examined. According to ISO 26262 a **safety measure** is an *activity or technical solution to avoid or control systematic failures and to detect random hardware failures or control random hardware failures, or mitigate their harmful effects.*
Thus, safety measures are all activities which can be applied before, during and after design as well as solutions increasing safety or reliability during operation. Some examples are:

- The end of line tests where each manufactured device is tested and failing samples are scrapped before they are shipped to the customer. Thus, it is a safety measure to avoid random faults caused by the manufacturing process.
- The design rule check reduces the number of systematic faults due to the comparison of the implemented design to rules of the production. This measure reduces the systematic fault caused by designers.
- To only assign educated and qualified staff to certain work products is also a valid measure to reduce the number of systematic failures due to human errors.
- Introduce corner or boundary simulation to be robust against parameter variation.

The safety measure can also include safety mechanism.
A **safety mechanism** is, according to the ISO 26262, a *technical solution implemented by the E/E functions or elements, or other technologies, to detect faults, or control failures in order to achieve or maintain a safe state.*
Thus, safety mechanisms actively maintain safety during operation in the field. Therefore they are part of the system. Examples for safety mechanisms are:

- A parity check for data transmitted via a communication interface.
- Two switches in series to ensure disconnecting even if one switch fails to open (redundancy).
- Indication of a broken wire to the user (detection).

In the context of a safety mechanism, the term **Fault Tolerant Time Interval (FTTI)** is very important. It describes the ability of a system to operate safely for a certain time which is the FTTI. The exact definition provided by the ISO 26262 states the FTTI is the *time-span in which a fault or faults can be present in a system before a hazardous event occurs* which is graphically illustrated in Figure 4.13. The system operates in normal operation until the fault occurs, which is the starting point for the measurement of the FTTI. From this time on, the safety mechanism has to detect the fault and has to react on the detection by initiating the transition to the safe state. In the left diagram, the time needed for the detection of the fault (T_{DTI}) together with the fault reaction time (FRT) are within the FTTI. Thus, the system can reach the state before a possible hazard can occur. However, on the right side, the sum of the diagnostic time intervals and the fault reaction time exceeds the allowed FTTI which lead to a hazard. Thus, the requirement for all safety mechanisms is:

$$FRT + T_{DTI} < FTTI \tag{4.30}$$

Beside the transition to the safe state, it is essential that the system remains in safe state as long as the fault is present [67].

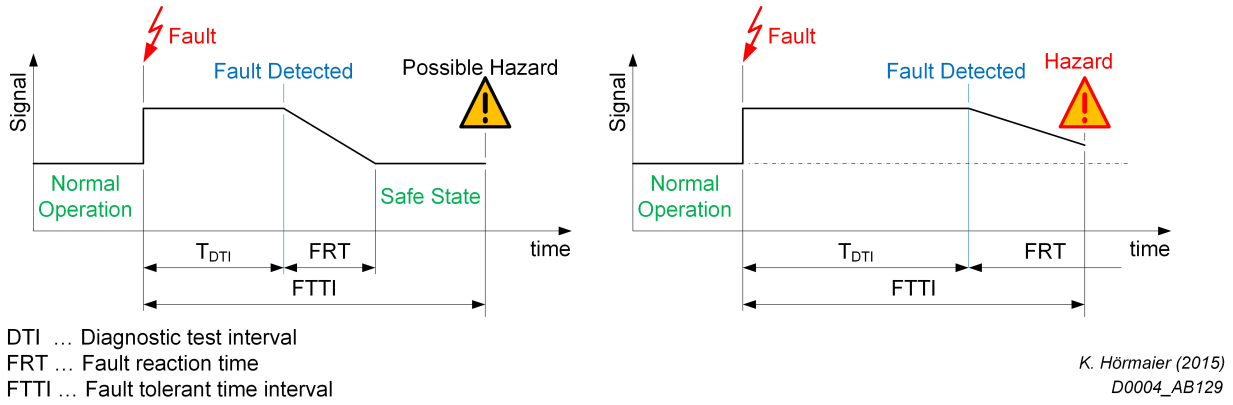


Figure 4.13: Two scenarios with different diagnostic time intervals and fault reaction times are shown. The safety mechanism in the left diagram is sufficiently fast to prevent a hazard in comparison on the right the safety mechanism is not able to bring the system the safe state within the FTTI.

Chapter 5

EMI in the Functional Safety Process

This chapter provides the concepts needed to fully integrate EMI aspects into the FS process. A corresponding process is proposed and explained in detail.
ISO 26262 recommends process steps for FS, but from the EMC point of view not all are relevant (the standard includes steps for e.g., software development, overall safety management). Thus, the process takes the relevant steps into account (see Figure 5.1) and leaves the remaining steps unchanged. The remaining unchanged steps can be gathered from the ISO 26262. In Figure 5.1 both the sequential tasks as well as on the right side the number of elements to be analysed are sketched. Thereby the proposed process consists of six major parts and several subtasks:

- Analysis on victim's side
  - Find all **I**njection **P**oints (IPs) on victim's side
  - Assign IPs to function
  - Fault tree construction and filtering
- Analysis on the aggressor side
  - Extract failure modes
  - Filtering
- Calculation of the coupling paths
- Failure rate calculation
- Safety analysis
- Introduction of safety mechanism

The process is iterative and can be tailored to system's sub blocks.
The basic idea, leading to a smooth integration of EMI into the FS process is considering EMI, not only as an environmental condition but as fault as well. The evidence, together with the root thoughts of EMI as fault are provided in the following section. Necessary adjustments on definitions and methods are introduced when needed.

For the following fault characteristics and analysis methods it is important to clearly distinguish between aggressor and victim. In this thesis, all characteristics are evaluated from the victim's point of view, unless stated otherwise. Generally, fault characteristics of aggressor systems are of interest only if they can influence the victim system. Each E/E system assembled in a car

can be considered as victim, influenced by one or several aggressors. In this thesis only one victim at a time is considered for analysis.

5.1 EMI Treated as an Environment Condition or as a Fault

Before an EMI analysis is performed, it has to be decided whether EMI is treated as an environmental condition or as a fault, since this strongly impacts the used approach. A simple assignment of EMI to the environmental conditions or to faults is not constructive. Standardization here is ambiguous, ISO 26262 continuously treats EMI as an environmental condition[1], however IEC 61508 treats EMI at least partially as a random fault[2] but also as an environmental condition[3].
IEC 61508-2 7.4.5.1:

> *For controlling systematic faults, the **E**lectrical/**E**lectronic and **P**rogrammable **E**lectronic **S**ystems (E/E/PES) design shall possess design features that make the E/E/PE safety-related systems tolerant against environmental stresses, including **electromagnetic disturbances**.*

This clause suggests treading EMI as an environmental condition and thus as a contribution to systematic faults. In this context, a developed system only includes a systematic fault if the robustness against the environmental stress conditions (EMI) is insufficiently low. The clause IEC 61508-2 7.4.3.2.2 h states a different view on the EMI classification:

> *The probability of failure of each safety function, due to random hardware failures shall be estimated taking into account the probability of undetected failure of any data communication process. Failures due to common cause effects and data communication processes may result from effects other than actual failures of hardware components (e.g. **electromagnetic interference**, decoding errors, etc). However, such failures are considered, for the purposes of this standard, as random hardware failures.*

In this clause EMI is seen at least as cause of random faults. In the broadest sense EMI can also be seen as fault. The context focuses on common cause failures, which additionally directly indicates that EMI can be the root cause of a common cause failure. In contrast, the ISO 26262 treats EMI continuously as an environmental condition and never as a fault:
ISO 26262-5 6.4.6

> *The criteria for design verification of the hardware of the item or element shall be specified, including environmental conditions (temperature, vibration, **EMI**, etc), specific operational environment (supply voltage, mission profile, etc) and component specific requirements.*

ISO 26262-5 7.4.1.7

[1] see e.g., ISO 26262-5 6.4.6, ISO 26262-5 7.4.1.7
[2] see IEC 61508 7.4.3.2.2 h
[3] see e.g., IEC 61508 7.2.3.2, IEC 61508 7.4.5.1

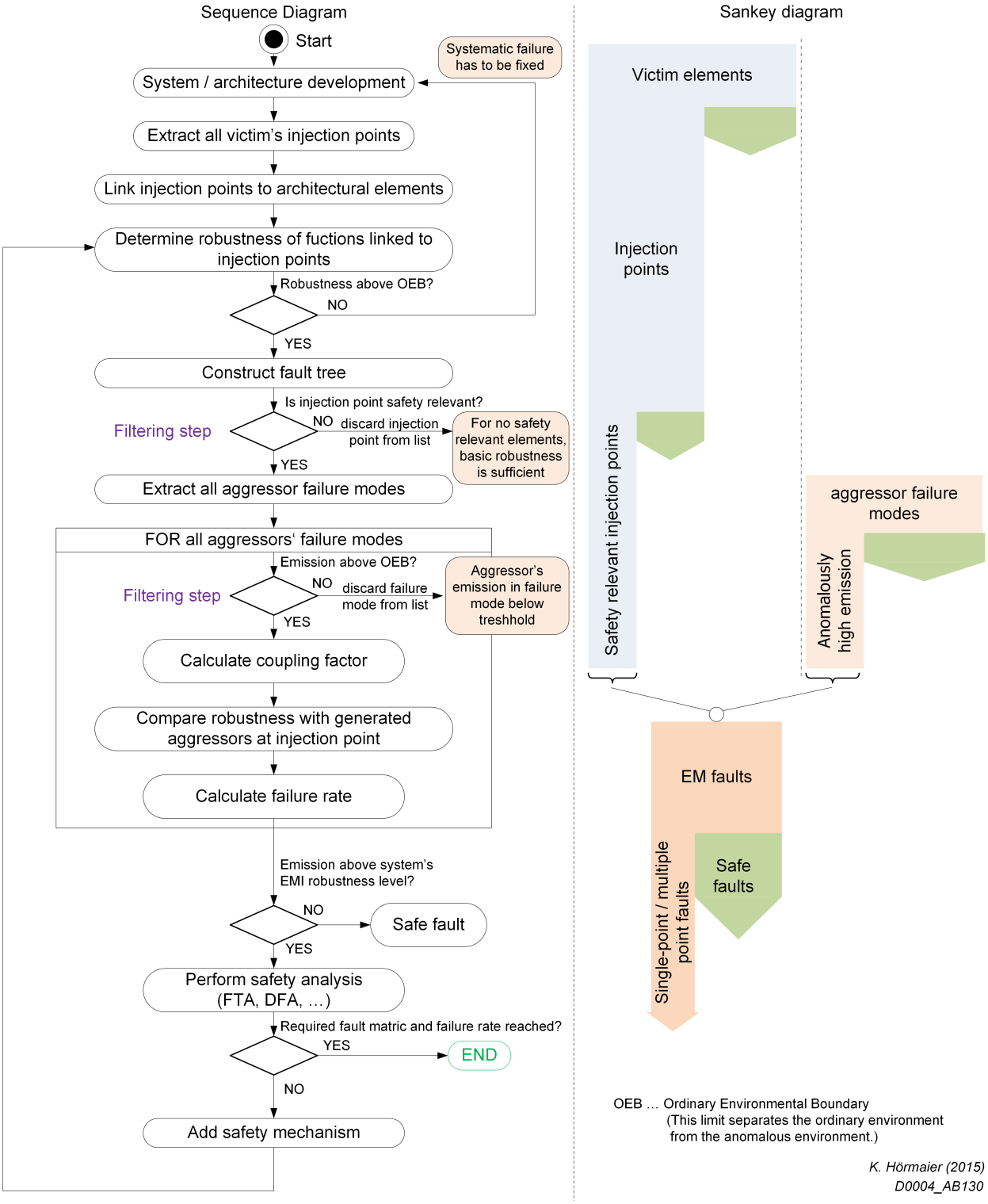


Figure 5.1: Overview of the proposed process incorporating EMI into the FS. On the left side the necessary process steps are expressed in a sequence diagram. On the right side, the corresponding number of elements to be analysed are sketched in the diagram.

Non-functional causes for failure of a safety-related hardware component shall be considered during hardware architectural design, including the following influences, if applicable: temperature, vibrations, water, dust, ***EMI****, cross-talk originating either from other hardware components of the hardware architecture or from its environment.*

The example provided in Figure 5.2 shows a vehicle where EMI is treated as an environmental condition as well as a fault. From the OEM's point of view, the vehicle is placed

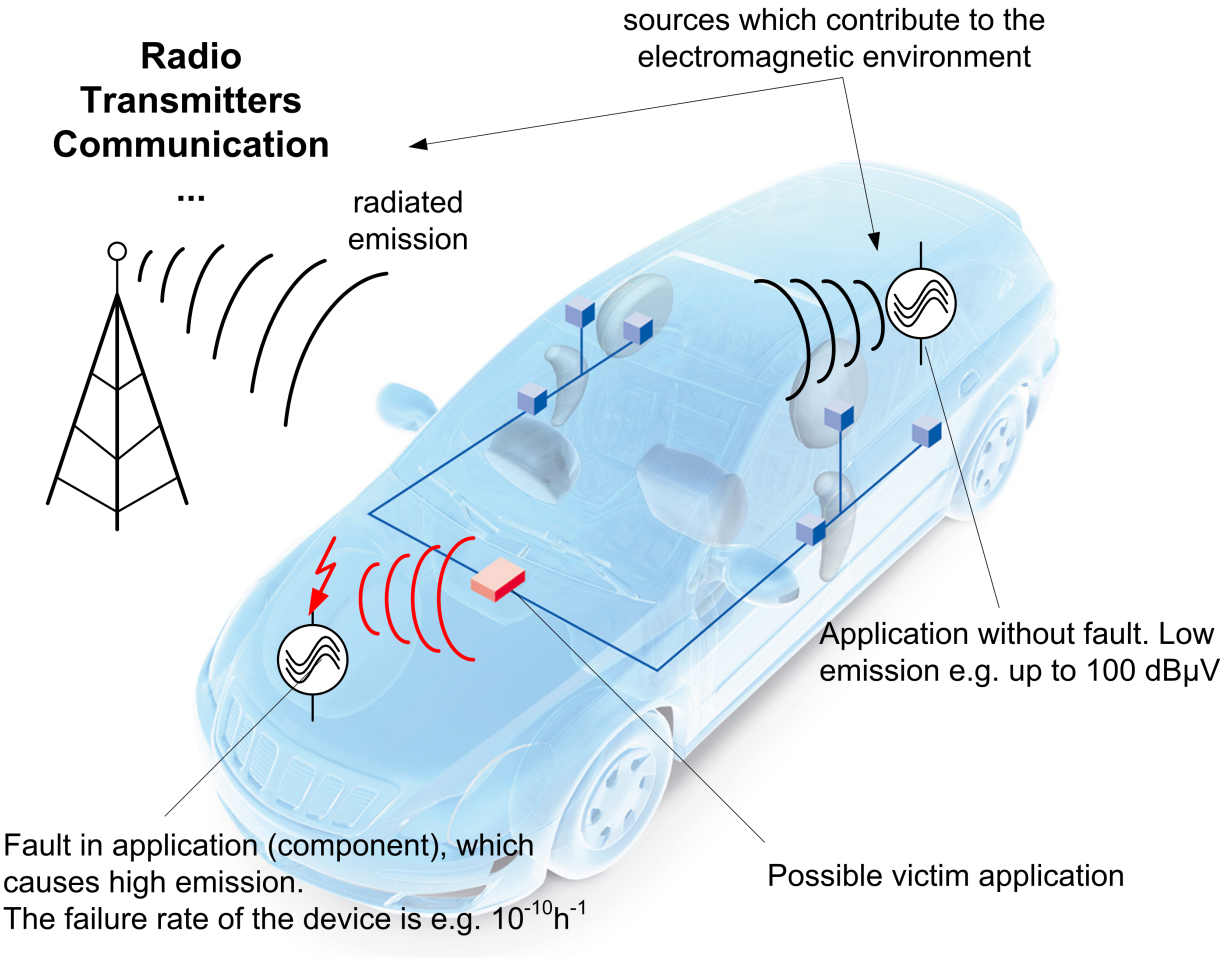


Figure 5.2: Sketch of the interference sources in the automotive environment.

in an uncontrolled EM environment[4]. This EMI is generated by e.g., telecommunication, radio stations and others. All those disturbance sources are stationary and permanently present and therefore have to be considered as systematic[5]. All the different configurations $\theta = \{time, location, connectivity\}$ form the permissible parameter space Θ. A possible example configuration θ could be a permanently activated (= time) radio station in Klagenfurt (Austria) (= location) which emits an EM field (= connectivity) to the street on which the car is located. Since all parameters of the parameter space Θ are permitted we have to evaluate the worst

[4]Even the outside environment is not uncontrolled. National regulation authorities limit the EMI by law. Thus, the EM environment is monitored and the originators of violations are penalised and the sources are turned off.

[5]Very unusual electromagnetic phenomena like nuclear electromagnetic pulses and others are excluded from this work.

case scenario. The probability of the external worst case EM environment $\hat{Pr}_{EM}(A_{EM} < A|\Theta)$ which has to be considered for safety analysis can be calculated using Equation 5.1.

$$\hat{Pr}_{EM}(A_{EM} < A|\Theta) = max_{\Theta}\left(Pr(A_{EM} < A)\right) \tag{5.1}$$

Thereby, A is a random amplitude variable and A_{EM} is the amplitude of the EM phenomena. The maximum probability of all EM phenomena creates the external EM environmental probability distribution.
Inside the vehicle, several electrical and electronic systems are operating which contribute to, or generate the inner EM environment. Disturbance generated by these systems is strongly limited and known. Emission is generally strongly regulated, and admitted emission levels are very low. An example is the emission of integrated circuits, measured with the 150 Ω measurement method [4], are in the range of several tens of dBµV. Only in case of faults, systems tend to produce high emission. E.g., the loss of shielding increased emitted emission or increase of emission because a switch switches against a short circuit conduction high current. The emission is therefore related to faults (leading to failure modes) and not to normal operation. Note: Only a small subset of all possible system failure modes tend to generate high emission. If, for example the light module stops working, generated emission could even decrease, because e.g., the current stops flowing.
Summarizing, the EM environment can be classified into the following three categories:

- external environment,
- internal normal environment and
- internal fault caused environment.

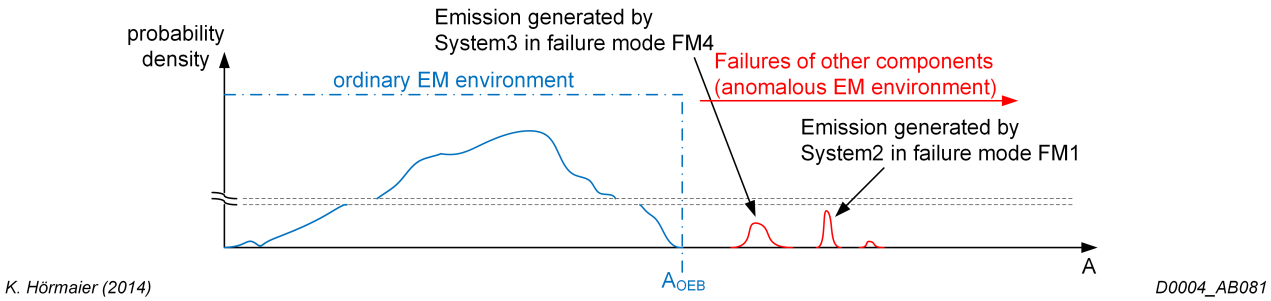


Figure 5.3: Sketched probability density of EMI amplitudes (A) in a vehicle. In the area which is treated as an ordinary EM environment the probability is high. In the region of anomalous EM environment caused by faults of other components the probability of these EM phenomena with high amplitude is very low.

In Figure 5.3 the probability density of EM disturbance in an automotive application is sketched. It presents the distinction of the EM environment between the ordinary (systematic) and anomalous (due to faults) EM environment. It shows that low amplitude EM disturbance is more probable than disturbance with very high amplitude. The disturbance is an amplitude-depending function. In this approach, therefore the **O**rdinary **E**nvironmental **B**oundary (OEB) (A_{OEB}) has been introduced. This limit separates the ordinary environment from the anomalous environment. The probability of the disturbances for the ordinary environment is set to one, but above this limit the probabilities of the EM phenomena caused by faults are used (see Figure 5.4). If the robustness of a system is below this limit, then there is a systematic

failure demanding a redesign of the system. However, if the robustness of a system is above the probability limit, the probability information of the anomalous environment will be used in further safety analysis.
The OEB is not a single value, but a collection of values which are properties of EMI models. The EMI models and their properties will be described in Section 5.4.2. For illustration purposes, only the amplitude of the EMI signal at frequency x has been chosen in this instance.
From a physical perspective, both the ordinary environment as well as the anomalous environment are environmental conditions since the system is surrounded by both. However, from a FS point of view, the anomalous environment is a collection of faults, and therefore shall be treated as a fault and not as an environment.
In conclusion, the ordinary environment is a combination of the external environment and the internal normal environment. The EM environment generated by faults inside the vehicle is called anomalous environment, which is treated as a fault.
Since EMI can be seen as a fault, the fundamentals described in 4 have to hold for "EMI faults" as well. Thus, the next section provides evidence of a valid Fault-Error-Failure propagation.

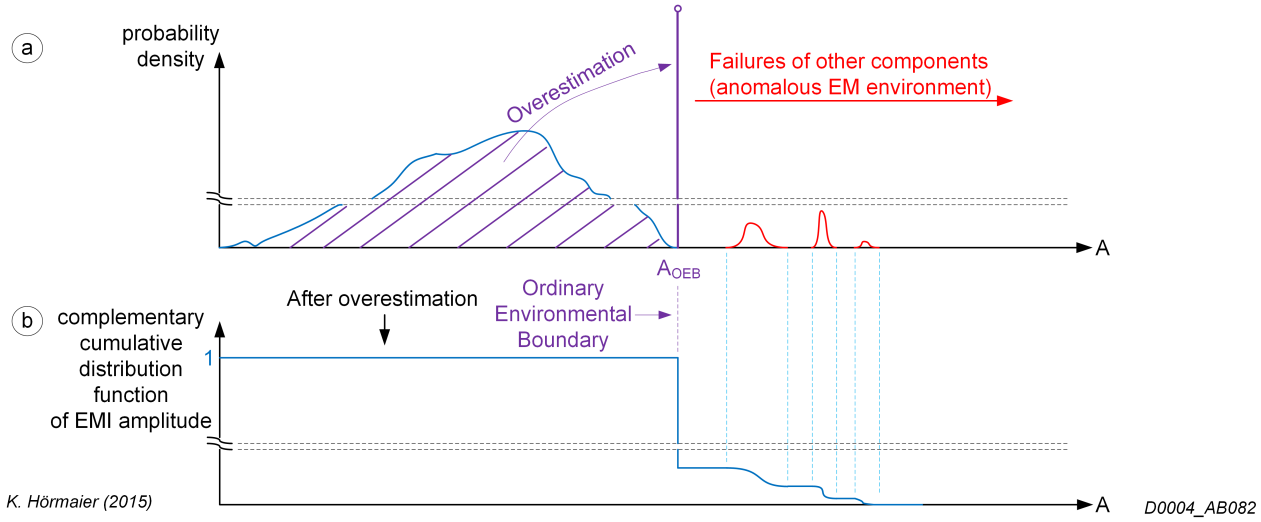


Figure 5.4: In graph a, the probability density function (pdf) of the EMI amplitude is sketched. Hereby, the probability below A_{OEB} is composite in an Dirac at A_{OEB}. In graph b, the complementary cumulative distribution function of the pdf after composition is sketched below. Until the A_{OEB} interference is seen as permanently present and therefore systematic.

5.1.1 EMI Fault-Error-Failure

Since EMI can be seen as a fault, the concept of EMI shall fit to the definitions of the fault propagation as previously described in section 4.5. From the EMI point of view, the fault propagation has to be slightly adapted. A fault in the aggressor causes an error in a function leading to a failure (Figure 5.5). Beside the aggressor malfunction, which is out of scope from the victim's point of view, the violation of the emission limitation is an additional failure. Up to this point there is no difference to the standard fault-error-failure considerations described in 4.5. The aggressor emits EMI, which might couple to the victim as shown in Figure 5.5. If the emission is still below the OEB, no fault is added on the victim's side. Thus, the victim is in normal mode, no fault is present. If the aggressor emits EMI, exceeding the environmental amplitude limit, a fault is present in the victim system. Depending on the robustness of the

victim, the fault might propagate and cause a failure. Further fault propagation now follows the procedure as described in 4.5. In addition, the term **e**lectro**m**agnetic **f**ault (EMF) is introduced which describes the fault introduced in the victim by EMI. The EMF can be handled in analysis the same as a random hardware fault, even if it is caused by EMI fault-mode in a neighbouring system.

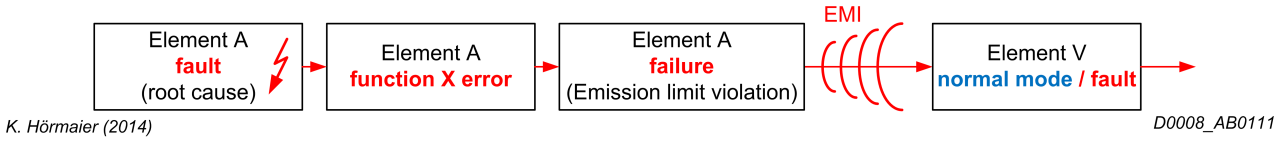


Figure 5.5: Fault propagation starting with a fault in the aggressor element (Element A), which leads to an emission increase, possibly further influencing the victim element (Element V).

5.2 Analysis on Victim's Side

The first step of the process is the analysis on victim's side. The vehicle consists of several E/E systems, where each of them can be a victim. Safety assessment concentrates on one victim at a time. Thus, in the following all considerations are based on one victim. For all other remaining victims exactly the same steps have to be performed. Before the analysis can take place, a general description of the victim's environment will be provided.

5.2.1 Environment

The environment inside the vehicle is neither constant nor homogeneous, neither from a time perspective nor from a location's perspective. Since each assembled system has its own location, it has its own environment. Thus, theoretically the environment for each system has to be assessed independently. From an economical as well as technical point of view it is not feasible to determine the exact EM environment at each location inside the vehicle. Simulation time and the complexity to set up the simulations exceed the possibilities of state of the art development processes. Thus, the evaluation of the environment has to be performed on an abstract level. The major abstraction originates from the introduction of a threshold, which represents a slight overestimation of the local environment. This threshold is set to the **O**rdinary **E**nvironmental **B**oundary avoiding the need to analyse all ordinary sources. Since the ordinary environment is fully covered by the threshold, all the ordinary sources and their couplings with the victim do not need to be analysed. Unfortunately the simplification tends to overestimate the environment leading to, in some cases, unnecessary robustness (over-engineering) of the developed product. Nevertheless, this approach is still a good compromise between overestimation and analysis effort. Consequently, the robustness analysis or tests can only be considered as pass if the robustness level of the victim exceeds the OEB amplitude (A_{OEB}).

5.2.2 Injection Points

Within the analysis of the victim, the first part is the elicitation of the injection points. As described in Chapter 3.1, EMI can only couple into a system if an effective coupling mechanism exists. Thus, the coupling mechanism can be considered as the system's entrances which have to be elicited. These points of entrance will further be called IPs. The number of possible entrances of the system is typically limited as the following example illustrates.

Assuming an IC with a silicon die size of 10 mm times 10 mm, the maximal wire length between two points is 20 mm.[6] The EM far-field's ability to couple directly into the IC can be calculated as follows. For the EM far-field's minimal wave length, in the frequency range of interest from 150 kHz to 1 GHz [4], Equation 3.8 can be used leading to the following result[7]:

$$\lambda_{min} = \frac{c}{f_{max}} = \frac{3 \cdot 10^8 \text{ m/s}}{1 \text{ GHz}} = 300 \text{ mm} \tag{5.2}$$

And k as the ratio of the minimum wave length λ_{min} and the maximal wire length l_{max} can be calculated as:

$$k = \frac{\lambda_{min}}{l_{max}} = \frac{300 \text{ mm}}{20 \text{ mm}} = 15 \tag{5.3}$$

Due to inserting the maximal frequency (= minimal wave length), the worst case value for k has been calculated. For lower frequencies the ratio k further increases. The ratio higher than 10 means that such a wire has a very bad antenna characteristic, which implies an inefficient coupling mechanism [41]. Thus, an EM far-field cannot couple directly into the IC, which strongly reduces the possible coupling points.

Instead of analysing the robustness of all single components or elements in a system, first only the IPs are analysed. For example, an **E**lectronic **C**ontrol **U**nit (ECU) assembled inside the vehicle consists of ICs (die size below e.g. 10 mm), passive elements and an interface to the wiring harness. The wiring harness itself includes connections to sensors and resistive loads as well as to the battery supply line and a ground connection. The wires of the wiring harness typically build efficient antennas. Thus, all pins connected to the wiring harness have to be classified as IPs, as they represent efficient coupling paths. Additionally long wires on the PCB, exceeding a certain length, as well as components of large shape (e.g., heat sink [68], [69]) are added to the list of IPs.

For the galvanic coupling, the system's interfaces have to be analysed. Only if an interface is commonly connected with another system, coupling can take place. Which, in the example is the ground and supply connection with aggressors connected to the same ground. Lastly, the near-field coupling is elicited.

Elements which resemble, due to their geometrical structure and material properties, a coil or a part of a capacitor are included in the list of IPs.

In the next step, all IPs are associated or linked to architectural elements, which is needed for safety analysis later on. Such a linking allows performing the safety analysis on a logical perspective, but also taking the specific information of the physical view into account.

Seen from a logical perspective, the previously gathered IPs are located at the system's boundary. But, as indicated in Figure 5.6, EMI can propagate also within the system, possibly interfering with other architectural elements. Thus, in addition to the architectural elements (logically connected to the IPs) the propagation of EMI to neighbouring architectural elements have to be analysed as well. The coupling between the affected elements / components can be estimated or calculated using the basics provided in 3.1. A simple example is the coupling between two wires which are routed on top of each other. The first wire is connected to the IP and the second line is within a different architectural element. The capacitive coupling (C) can be approximated by dividing the overlapping area of the two wires (A_1, A_2) with their distance d to each other multiplied by the dielectric coefficient of the PCB (ε_r).

$$C = \varepsilon_0 \varepsilon_r \frac{A_1 \cap A_2}{d} \tag{5.4}$$

[6] Under the assumption that the designer does not build an extra long trace or even an antenna by purpose. The 20 mm results due to the sum of the two 10 mm edges.

[7] For the calculation, vacuum has been chosen as material (speed of light in vacuum).

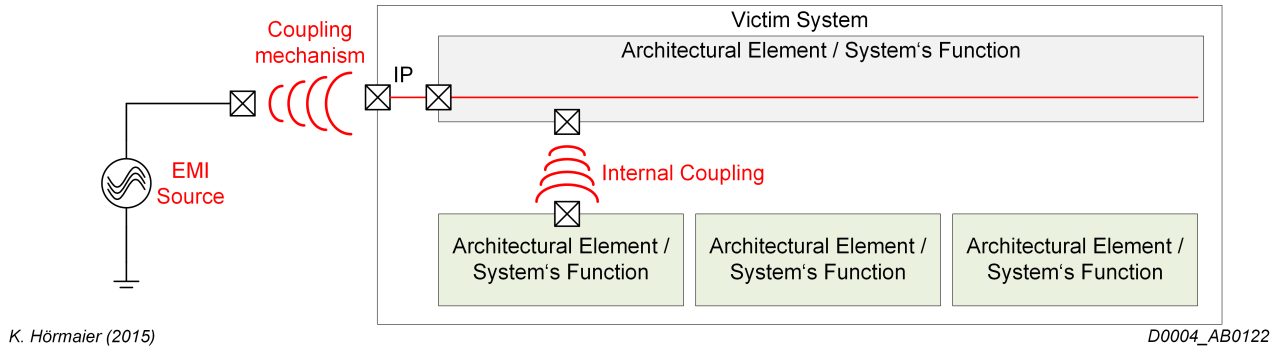


Figure 5.6: EMI entering the system via an IP, might couple via various coupling paths into other sub components which are logically independent from the component directly connected to the injection point.

The damping of the EMI signal inside the architectural element, which is directly connected to the IP, has to be included in the coupling impedance as well.

5.2.3 Basic Robustness

The elicitation of the IPs is followed by the characterisation of the victim's robustness without safety mechanisms. Thereby the robustness against possible interferences, coupling through the IPs into the system, is analysed. The robustness of the victim determines whether injected EMI leads to systems failure or not. With the robustness of the system against EMI, which is present in the ordinary environment, the system can be seen with respect to EMI as free of systematic faults. If the contract is not satisfied, counter measures have to be put in place. The victim's robustness can be evaluated by calculation or simulation or testing. The robustness depends on the realised function and its specification. Thus, the robustness evaluation "stresses" the victim until a specification violation can be observed. For simple calculations, e.g., the maximum voltage ratings of assembled components are compared to the maximum induced voltage. The testing description can be found in Chapter 3, and for simulation an overview will be given later in in Chapter 6.
Contrarily, for the analysis of the random faults the information of the anomalous environment is needed, which can be gathered by the analysis of the aggressors.

5.3 Analysis on the Aggressor's Side

The analysis of the aggressors starts with the characterisation of their generated emission. All aggressors' normal operation modes have to be evaluated to get its contribution to the ordinary environment. As explained before, the environment is composed of the ordinary environment as well as by an anomalous environment generated by faults of various E/E systems inside the vehicle. Thus, beside the normal operation modes, also the failure modes of the aggressor systems have to be analysed. As shown in Figure 5.7 a fault in an aggressor system can propagate via diverse coupling paths to various victim systems. By fault injection into the aggressor system, the emission caused by the aggressor's failure mode can be characterised. The characterised emission gives the EM environment at the aggressor which has to be further transferred to the victim. Therefore, all the coupling paths between the aggressors and the

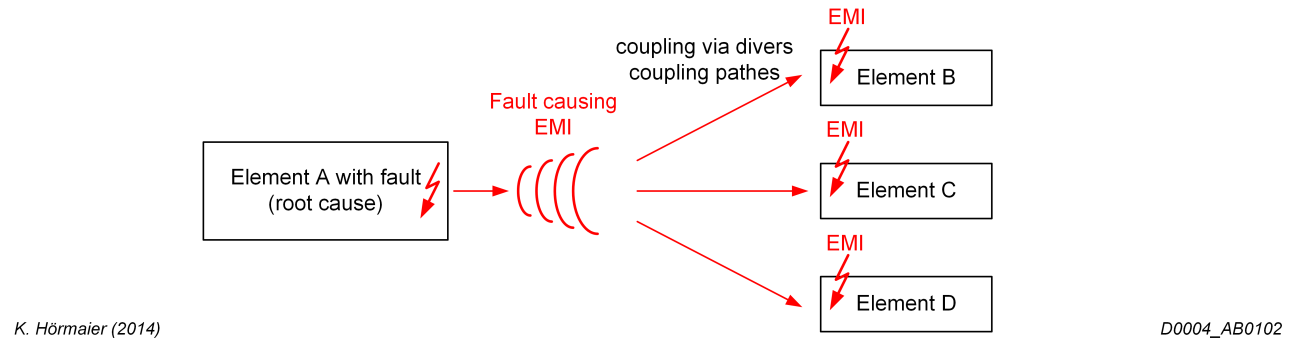


Figure 5.7: A fault of a element in the vehicle can cause EMI. The generated EMI propagates via diverse coupling paths to other elements in the vehicle causing them to fail.

victim have to be analysed. The indiscriminate use of methods to achieve a complete analysis of the components increases the effort dramatically. Thus, rigorous analysis will inevitably fail. To overcome this problem, filtering to reduce the number of aggressors is highly advisable. Initially, a fast filtering method, but with lower accuracy, is used to reduce the possible combinations for analysis, followed by an accurate analysis. Thereby, the filtering screens-out those EMI sources which, independently from the coupling path, cannot interfere with the victim. The coupling is overestimated by setting the coupling factor to one, which means that the full EMI amplitude reaches the victim. This results in an environment at the victim equal to the aggressor's emitted emission. Since all victims have to resist EMI up to the OEB, it is advisable to use the OEB as filtering threshold. Thus, all aggressors which cannot generate EMI above the OEB are filtered out and do not have to be considered. If the emitted EMI of the aggressor exceeds this limit, this does not imply that the victim system will fail for sure. Depending on the coupling path, the EMI at the victim can be already damped to a level so that the victim can withstand the EMI stress. To eliminate false verdicts caused by the overestimation, in the next step the coupling paths between the remaining aggressors and the victim are evaluated in detail.

5.3.1 Coupling path

Accurately determining the coupling requires an extensive undertaking, which can be found in e.g. [70], [71]. This thesis will therefore only explain the effects of the coupling path. The coupling path does not only propagate the EMI but can also change its characteristics. For example for far-field as well as near-field coupling the amplitude is reduced with increasing distance. Thus, the coupling path properties are determined and summarized in a variable coupling factor ξ. With the coupling factor, the transformation of the EMI between the aggressor with its amplitude A_{FM} and the IP with the amplitude A_{IP} can be calculated as follows:

$$A_{IP} = A_{FM} \cdot \xi \tag{5.5}$$

Not only the amplitude but also various properties might be changed. For example, depending on the inductance of the wiring harness, the shape and therefore the timing of pulsed interference can change. The symbol A_{IP} stands for a bulk of parameters which can be assigned to the time domain as well as frequency domain.

5.4 Properties of EMI as Fault

This section aims at describing, how to integrate EMI into the nomenclature, definitions described in the Chapter 4, and therefore provide evidence of the applicability of the proposed concept.

5.4.1 Failure Modes

The definition of the failure mode (see Section 4.6) also applies to EMI. The victim has as well as the aggressors show failure modes. The aggressor's failure modes can, but do not have to generate EMI. The aggressor's failures that cause an increase of EMI, will be called **e**lectro**m**agnetic **f**ailure **m**odes (EMFMs). For further analysis, the failure modes of the aggressor have to be assigned to one **S**tandardized **e**lectro**m**agnetic **F**ailure **M**ode (SEMFM). Since several aggressor systems may exist, and some of their failure modes may be equal or similar, they are assigned to the same SEMFM. E.g., a window lifter motor as well as the motor for changing the seating position might have a failure mode with the same characteristic EMI. Thus, the failure mode characteristics can be combined in one SEMFM. The SEMFMs have to be measurable on the aggressor's side, and able to be stimulated on the victim's side. An SEMFM example is a sinusoidal interference which is measurable on the aggressor's side by for example, the 150 Ω method [4] with the frequency and the amplitude as its characteristic. On the victim's side, the equivalent interference can be generated using the DPI setup with the transformed frequency and amplitude values of the aggressor's measurement. For the analysis on the victim's side, the SEMFM are used to describe faults (see 5.1.1).

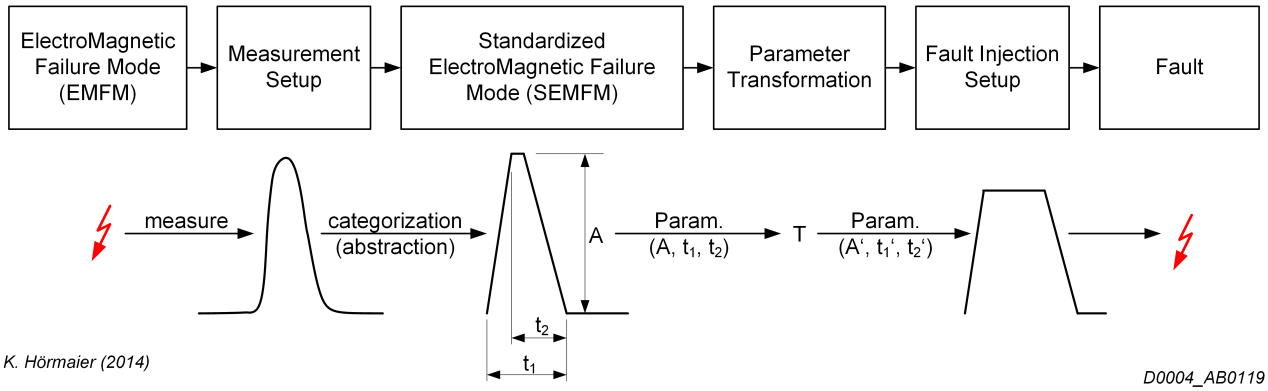


Figure 5.8: The failure behaviour of the aggressor is represented by its EMFM. The failure behaviour can be measured and the parameters of the SEMFM are matched to the measurement results. The parameters on the aggressor's side are transformed considering the coupling path to victim's side. At the end, the victim can be stressed by using the SEMFM with the transformed parameters.

5.4.2 Fault Model

As already described, the emitted EMI characteristic can be similar between aggressors. Thus, also the fault models shall be unified and reusable. Additionally important is the fact that the automotive development process is a parallel process. Several systems inside a vehicle are developed in parallel. In order to achieve a good time to market performance, it is not possible to wait until all components are characterised regarding their possible emission. Thus,

fault models with which both, aggressor as well as victim sides can be tested, have to be used. Not necessarily all fault models already exist but at least a majority of them can be covered by existing test methods (see Chapter 3). From different points of view the usage of standardized test methods is preferred compared to new specific test methods. The most important advantages of standardized test methods are listed as follows:

- Availability of equipment
- Equipment costs
- Use of past data
- Understood, practised and routine work with setups
- Commonly agreed
- Proven by use - fault free

5.4.3 EMI Fault Classification

EMI can be of all fault types explained in Section 4.8. The following three examples illustrate the classification of EMI in this context.
A short in a supply line might cause a fast current change ($\gg di(t)/dt$), resulting in a transient interference. But the constant high current in steady state will not cause problematic radiation. Thus the EMI can be seen as a transient fault, whereas the supply's short is classified as a permanent fault. The source of an EMI as intermittent fault could be a loose connection of a supply node and a load, causing a fast change of voltage ($\gg dV/dt$) each time the connection breaks. The resulting repetitive emission can then be seen as an intermittent fault.
A permanent EMI fault is for example caused by the loss of the EMI filter of a motor whose function is to suppress the emission caused by the motor.

5.4.4 Failure Rate

For quantitative safety analysis, the system's failure rate $h_V(t)$ (at the victim's side) has to be determined. The victim's failure rate is composed of the failure rate due to random hardware faults (caused by elements integrated in the victim) and the failure rate originated by EMI of the anomalous EM environment. The failure rate originated by the anomalous environment depends on the failure rate of the aggressors and their failure modes. With the following example the calculation of the failure rate considering only one aggressor's failure mode will be explained. The failure rate of the corresponding aggressor is given as $h_A(t)$ and the contribution to the FMD of the **e**lectro**m**agnetic **f**ailure **m**ode (EMFM) is determined as d_{EM}. Entering these values into Equation 4.16 leads to the failure rate of the EMFM:

$$h_{EM}(t) = h_A(t) \cdot d_{EM} \tag{5.6}$$

The characteristics of the emitted EMI are typically not constant due to manufacturing process parameter variations. Thus, for example the amplitude of the emitted EMI varies statistically over the amplitude range. This on the other hand, makes it necessary to use the amplitude's probability density function $f(A_{EM})$. As illustrated in Figure 5.9 the failure rate of the aggressor's EMFM does not necessarily translate one to one into the victim's failure rate. Thus, the aggressor's electromagnetic failure rate can contribute to the following categories:

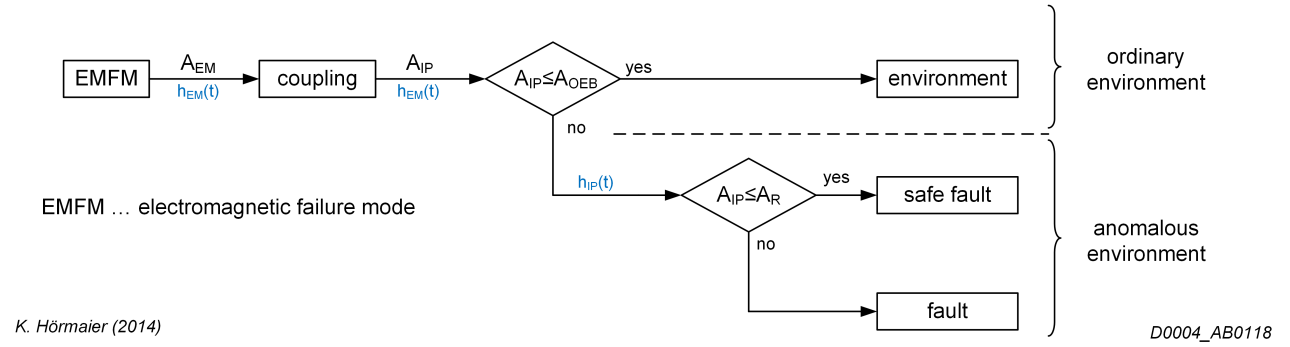


Figure 5.9: Distribution of the aggressor's failure rate (h_{EM}) to the three different classes (environment, safe faults and fault). An aggressor's electromagnetic failure mode (EMFM) does not necessarily lead to a victim's fault.

- EM environment
- safe faults, and
- faults.

The need for the distinction will be described in more detail in Section 5.5. To get the portion of the failure rate $F_{IP}(t)$, which does not contribute to the environment, the following equation can be applied:

$$h_{IP}(t) = h_{EM}(t) \cdot \xi \int_{A_{OEB}}^{\infty} A_{EM}(a \cdot \xi) da \tag{5.7}$$

In the equation A_{OEB} represents the amplitude of **O**rdinary **E**nvironmental **B**oundary (OEB), ξ represents the coupling factor and A_{EM} represents the pdf of the emitted emission in the EMFM. Also the victim's robustness varies statistically due to manufacturing process variations, leading to a pdf of failure, depending on the interference amplitude. In Figure 5.10 the pdfs of the generated interference amplitude, the resulting EMI amplitude at the victim and of the victim's robustness amplitude are sketched. Their distribution can be of any kind and need not to be normally distributed as shown in the example figure.
A fault arises only if the amplitude of the generated interference at the IP (A_{IP}) is higher than the component's robustness against this type of interference. The component's robustness is given by the amplitude (A_R) which is represented as random variables as well. Consequently, the component fails if $A_R \leq A_{IP}$. Since both amplitudes $(A_R; A_{IP})$ are uncorrelated random variables the probability of failure has to be calculated according to Equation 5.8. The pdf of A_R is given by the function $f_{A_R}(a_R)$ and by the function $f_{A_{IP}}(a_{IP})$ for A_{IP}. Here f is the pdf of the amplitudes and not the probability of failure which is also denoted by f.

In the next step, the conditional probability $Pr\{A_R \leq A_{IP}|H_{EM}\}$ of the victim's failing due to an EMI at the IP (due to the aggressor's failure) can be calculated. In this case, H_{EM} represents the event (the aggressor's electromagnetic failure mode). First, a joint random variable Z is introduced which is $Z = A_R - A_{IP}$. To get the pdf $f_Z(z)$ of Z, the convolution of $f_{A_{IP}}(a_{IP})$ with $f_{A_R}(a_R)$ can be calculated using the convolution integral as shown in Equation 5.9.

$$f_Z(z) = f_{A_R}(a_R) \otimes f_{A_{IP}}(a_{IP}) \tag{5.8}$$

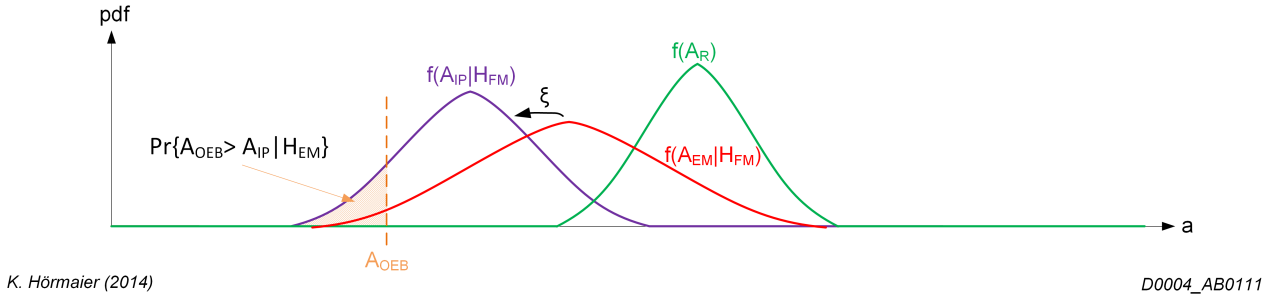


Figure 5.10: Three different amplitude probability density functions are shown. On the right side, the components susceptibility $f(A_R)$ is plotted. The middle curve visualizes the generated interference caused by a failure mode $f(A_{EM})$ and the left one shows the interference signal's probability density at the injection point $f(A_{IP})$ (after transformation by the coupling factor ξ). The area of the IP's amplitude probability density function, left of the ordinary environmental boundary (A_{OEB}), is rated for the safety analysis as environmental condition. The intersecting area of $f(A_{IP})$ and $f(A_R)$ shows the probability of a systems failure due to the interference.

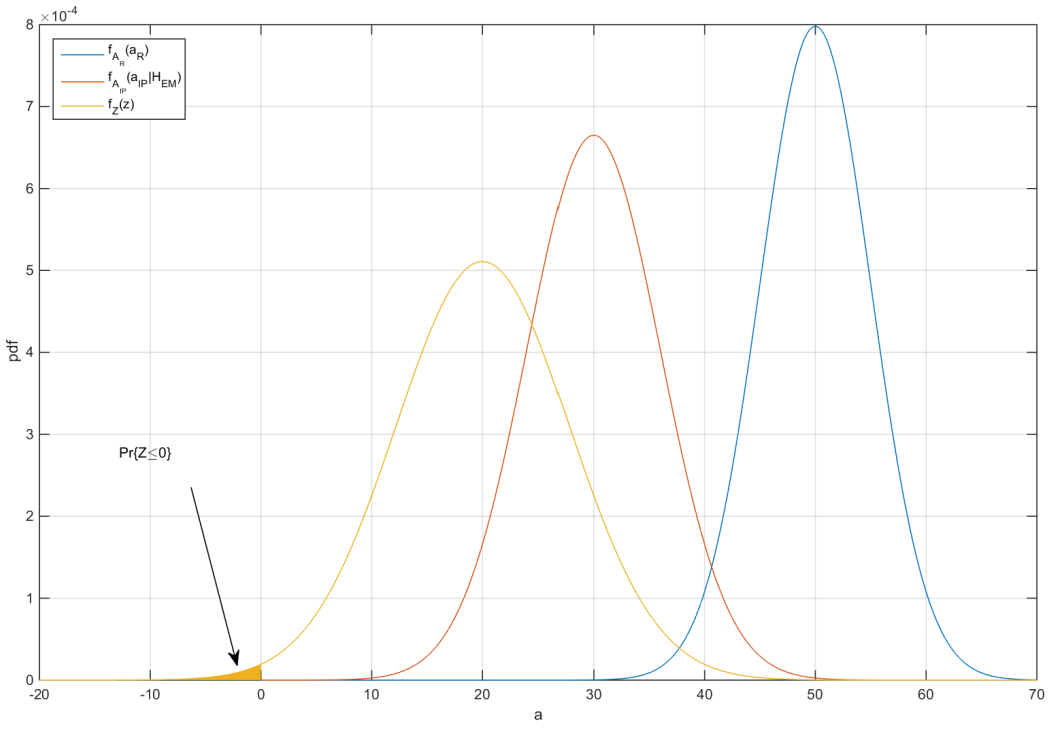


Figure 5.11: The convolution of the two amplitude probability functions $f_{A_R}(a_R)$ and $f_{A_{IP}}(a_{IP})$ resulting in $f_Z(z)$ are shown. The area bellow $f_Z(z)$ from $-\infty$ to 0 provides the probability that A_{IP} is higher than f_{A_R}.

$$f_Z(z) = \int_{-\infty}^{\infty} f_{A_R}(z - a_{IP}) f_{A_{IP}}(a_{IP}) da_{IP} \tag{5.9}$$

The probability that the random variable Z is below zero ($Pr\{Z \leq 0$) can be calculated as follows:

$$Pr\{Z \leq 0\} = \int_{-\infty}^{0} f_Z(z) dz \tag{5.10}$$

The probability of EMI exceeding the victim's robustness is $Pr\{A_R \leq A_{IP} | H_{EM}\}$. As $Pr\{A_R \leq A_{IP} | H_{EM}\}$ is equal to $Pr\{Z \leq 0 | H_{EM}\}$ ($A_R - A_{IP} \leq 0$), Equation 5.10 can be used to calculate the probability $Pr\{A_R \leq A_{IP} | H_{EM}\}$. Inserting Equation 5.9 in Equation 5.10 leads to:

$$Pr\{A_R \leq A_{IP} | H_{EM}\} = Pr\{Z \leq 0 | H_{EM}\} = \int_{-\infty}^{0} \left[\int_{-\infty}^{\infty} f_{A_R}(z - a_{IP}) f_{A_{IP}}(a_{IP}) da_{IP} \right] dz \tag{5.11}$$

Thereby it is assumed, that the aggressor's failure H_{EM} has occurred. H_{EM} occurs with the frequency (failure rate) of $h_{IP}(t)$ (see Equation 5.7) and lead to an unreliability $F_{IP}(t)$.
The victim fails if H_{EM} occurred and the victim's robustness is insufficient ($A_R \leq A_{IP}$). Thus the victim's unreliability $F_V(t)$ can be calculated as:

$$F_V(t) = Pr\{A_R \leq A_{IP} | H_{EM}\} F_{IP}(t) \tag{5.12}$$

Expanding Equation 5.12 with Equation 5.11 and replacing a_{IP} by $a_{EM} \cdot \xi$ leads to:

$$F_V(t) = F_{IP}(t) \int_{-\infty}^{0} \left[\int_{-\infty}^{\infty} f_{A_R}(z - a_{EM} \cdot \xi) f_{A_{EM}}(a_{EM} \cdot \xi) da_{EM} \right] dz \tag{5.13}$$

Finally replacing $F_{IP}(t)$ in Equation 5.13 as in Equation 5.7 gives:

$$F_V(t) = F_{EM}(t) \xi \int_{A_{OEB}}^{\infty} A_{EM}(a \cdot \xi) da \int_{-\infty}^{0} \left[\int_{-\infty}^{\infty} f_{A_R}(z - a_{EM} \cdot \xi) f_{A_{EM}}(a_{EM} \cdot \xi) da_{EM} \right] dz \tag{5.14}$$

5.4.5 Systems to System

A vehicle contains multiple systems or arrays of systems. All of these systems can fail and thus they might contribute to a victim system's EM fault. In Figure 5.12 an overview of the systems assembled in the vehicle is shown. Each aggressor system can contribute to the victim's failure rate. Thus, the failure rate of a victim's fault is composed of several aggressor systems. Therefore, the failure rate can be calculated for each SEMFM as:

$$h_{V\_SEMFM}(t) = \sum_{i=1}^{M} \left[\frac{\frac{dF_{Vi}(t)}{dt}}{1 - F_{Vi}(t)} \right] \tag{5.15}$$

with the number of contributing aggressor systems M, and the unreliability $F_{Vi}(t)$ for certain SEMFMs. As explained in Equation 4.2 the probability calculation of the logical "OR" ($A \cup B$) connection of two random variables (A, B) contains a multiplication part which can be neglected if the failure rates of A and B are much lower than one. Since this is also true for this equation the cut-set term has been neglected. As illustrated more than one fault of the same aggressors can contribute to one victim's fault.

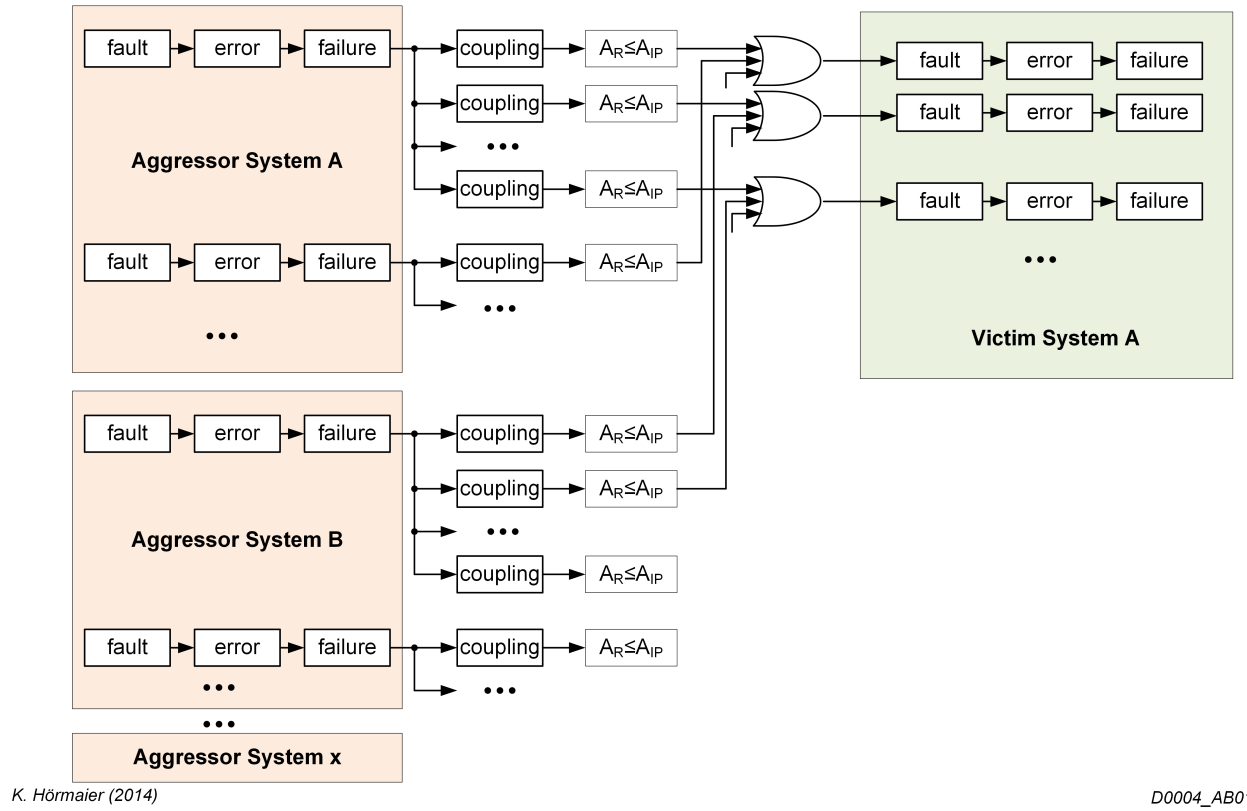


Figure 5.12: Contribution overview of the various aggressor systems to the victim's EM related faults.

5.4.6 Common Cause Failures

The analysis of common cause failures is one of the most difficult undertakings during safety analysis. It is often very difficult to gather the needed information in order to analyse it afterwards, since one single source of emission couples via various ways to several injection points of the system (Figure 5.13). But a common cause might not only have its source outside the system. Also inside the system EMI might couple from one location to several functional blocks simultaneously. Thus, faults inside the system can be common cause faults as well.

5.5 Fault Metric

The proposed method introduces new EMI caused faults into the system, impacting the fault metrics. Adding new faults might hinder the development due to an increase of for example, the single-point fault metric. Including only the EMI caused faults leading to failures would increase fault metrics and therefore would lead to more challenges in design. Thus, in addition, EMI safe faults, which decrease the fault metric, shall be introduced. However by introducing a large number of safe faults the fault metric would be distorted. Therefore, it is proposed to distinguish between safe faults that are safety related and not safety related faults caused by EMFM, that contribute only to the environment and thus do not impact the metrics. Thus, additionally to the faults also EMI safe faults (decreasing the fault metric) and not safety related faults (increasing the fault metric) have to be introduced.

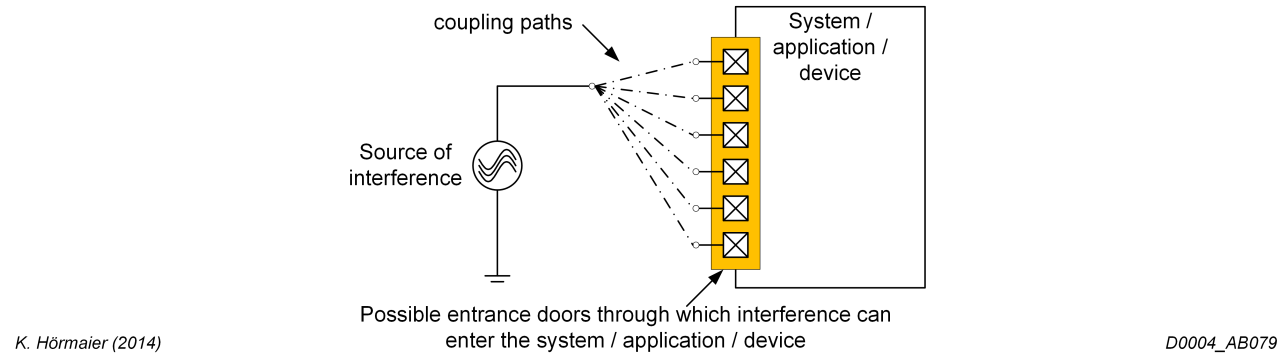


Figure 5.13: A single interference source couples via different paths into the system. The interference is therefore present at different locations in the system and interferes with several functional blocks simultaneously. Thus several components might fail due to the same (common) cause.

5.6 Safety Measures and Safety Mechanism

In the following, the safety mechanism targeting EMI will be discussed. In this context, the safety mechanism prevents, in case of EMI, the victim system to fail.
The implemented functions have typically certain robustness due to their architecture or design. Thereby, the robustness is not achieved due to additional components but by the components needed to build the function. A failing of one of these components will inevitably lead to a failure of the function. Thus from an EMI point of view those components have not to be considered because their influence is already covered by their own failure rate. On the other hand, all included components which do not contribute directly to the functionality have to be considered separately.
Here again, the differences between the ordinary environment and EMI as fault have to be stressed. Components which are additionally built in to increase the robustness to handle the ordinary environmental stress are part of the normal functionality but all mechanisms which further increase the robustness have to be classified as safety mechanisms. The failure rates of the components, included to sustain the ordinary environment stress, directly contribute to the functions failure rate. The failure rate of the component $h(t)_{COMP}$, included to sustain the anomalous environment, has only a negative influence in combination with an EMI event $h(t)_{EMFM}$. Thus, the resulting failure rate is the multiplication of the two failure rates $h(t)_{COMP} \cdot h(t)_{EMFM}$.
Thus, safety mechanisms can be built in, but not recognised by the safety engineer, which are called hidden safety mechanisms by the author. If the hidden safety mechanism is not recognised, and therefore is not assigned to an IP a failing of this mechanism is not considered in the safety analysis. This will inadvertently decrease the overall failure rate, which has to be avoided.
The robustness of the victim can be increased, the coupling can be weakened and the emitted emission of the aggressor can be reduced. From a global perspective, it is useful to reduce abnormally high emission generated by the aggressors. Nevertheless from a victim's point of view this approach is not a safety mechanism but reduces the failure rate of the corresponding EMFM.

In the next section, the victim's robustness improvement and the coupling optimization are targeted. Generally, different solutions to improve the performance are possible. Beside the changing of the material properties a separation of the system's function from the EMI can be achieved by modification of the:

- Location
- Frequency
- Time
- Amplitude

In the following, all four concepts will be discussed in detail.

5.6.1 Material Properties

The material can be changed to weaken the coupling path. For capacitive coupling paths the material's permittivity can be decreased or a conduction material can be introduced (shielding). For inductive coupling, the material's permeability can be decreased by for example, building an air gap. For galvanic coupling, the resistivity of the common current path can be increased. Especially, small signal traces in ICs built with sub micron technologies, have high resistance wires. A 1 mm long (l) copper wire with the minimum width and height of both 200 nm has a resistance of:

$$R = \rho \frac{l}{A} = 1.7 \cdot 10^{-2} \frac{\Omega \text{ mm}^2}{\text{m}} \cdot \frac{1 \text{ mm}}{200 \text{ nm} \cdot 200 \text{ nm}} = 425 \ \Omega \tag{5.16}$$

with $\rho = 1.7 \cdot 10^{-2} \frac{\Omega \text{ mm}^2}{\text{m}}$ the conductivity of copper.
For interference coupling into the system which uses a differential input, the input impedance shall be matching. If the input impedance is symmetric common mode interference has no influence because both interfaces will see the same voltage which is cancelled out.

5.6.2 Separation in Location

Changing the victim's location will change the coupling path, thus influences the EMI propagation. With increasing distance, the interference will be reduced. Besides the increase of distance, filters can be used to bypasses or conduct the EMI at another location, before the EMI reaches the sensitive parts of the victim. This approach needs additional components. Not only can the distance by itself, but also the material between the aggressor and the victim change depending on the location (see Section 5.6.1).

Barriers
One concept of location separation is the insertion of barriers. Barriers separate areas with a high density of EMI from other locations. Thereby, the barriers ensure weak coupling between the locations. The additional separation of the location into classes can ease the amount of work for safety analysis. Components in zones of a certain EMI class do not have to be analysed regarding their EMI robustness. Figure 5.14 shows a possible realisation of the approach. EMI might couple from outside into the system and influences signals or components within the area shown as Class 1. In the whole area labelled with Class 1 an EMI amplitude is permitted complying with the definition of Class 1. The permitted amplitudes have to be defined by the designer.

Introducing barriers on the other hand, should not be done after development of the project but in the early product concept phase. To ensure independency of functional blocks, barriers have to be defined which will be implemented later on.

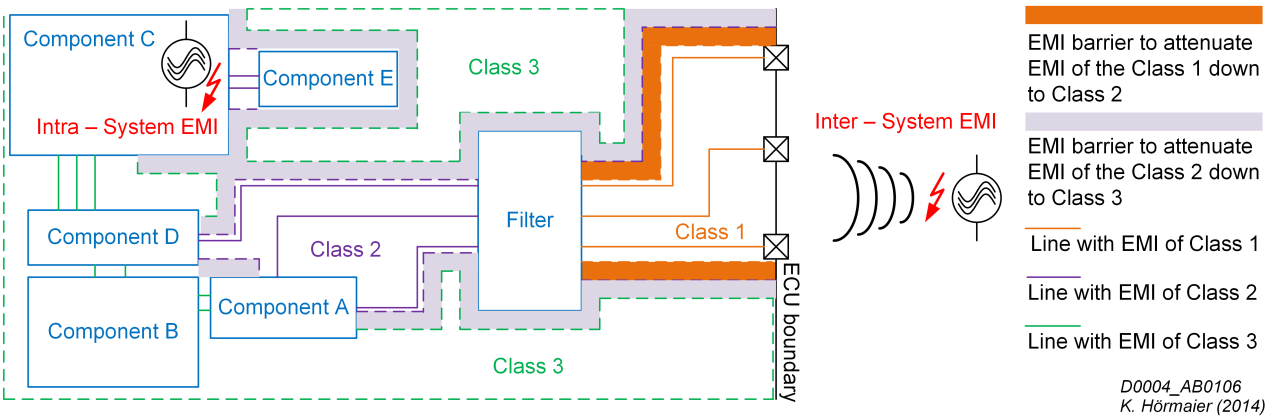


Figure 5.14: Interference enters the system and propagates depending on the placement of barriers. Traces, in a dedicated class, have to be considered as be influenced by EMI up to the classes defined ratings. This analysis is conducted on the physical perspective.

In the early design phase, measurement results are typically not available. Thus, to be able to perform a safety analysis, assumptions have to be made. Assuming that EMI can couple into all elements is theoretically valid, but impractical since the number of elements to be analysed increases dramatically. To overcome the problem, the approach of introducing barriers shall be taken.
The analysis of coupling paths is not completed at the systems boundaries. Further propagation EMI can occur inside the system. An already affected line, which carries the EMI, can couple to a line beside itself. Thus, the systems designer shall analyse possible coupling or directly include barriers which omit the propagation of EMI within the system. If any lines are crossing a class area they shall be treated as part of this class as well.

5.6.3 Separation in Time

The separation in time accounts for the fact, that EMI can be of the fault type "transient fault" which has a limited time span (T_{EMI}). However, not only transient faults, but also intermittent faults might be limited in time, even if they are recurrent. The idea is to separate the operation of the function from the occurrence of the fault. An example is a repetitive measurement which takes $T_{SS} = 30$ ms and which has to be performed at least every 150 ms. Considering as basis test pulses of the type 3a of ISO 7637-2 which are active for $T_{FS} = 10$ ms and deactivated $\overline{T_{FS}} = 90$ ms for uncorrelated pulses the following probabilities can be derived. The probability $Pr(S)$ of success is:

$$Pr(S) = \frac{\overline{T_{FS}} - T_{SS}}{T_{FS} + \overline{T_{FS}}} = \frac{90\text{ ms} - 30\text{ ms}}{10\text{ ms} + 90\text{ ms}} = 0.6 \tag{5.17}$$

But if the fault can advertently be synchronised with the measurement (correlated), the starting time of the measurement can be placed in the time where no fault is present which leads to a 100% success rate. On the other hand, an inadvertent synchronisation of the measurement with the fault can lead to continuous problem-filled measurements, which have to be avoided. Nevertheless, the function can possibly resist the fault for a certain period of time. This time is called FTTI as described in Section 4.12.

Fault Tolerant Time Interval

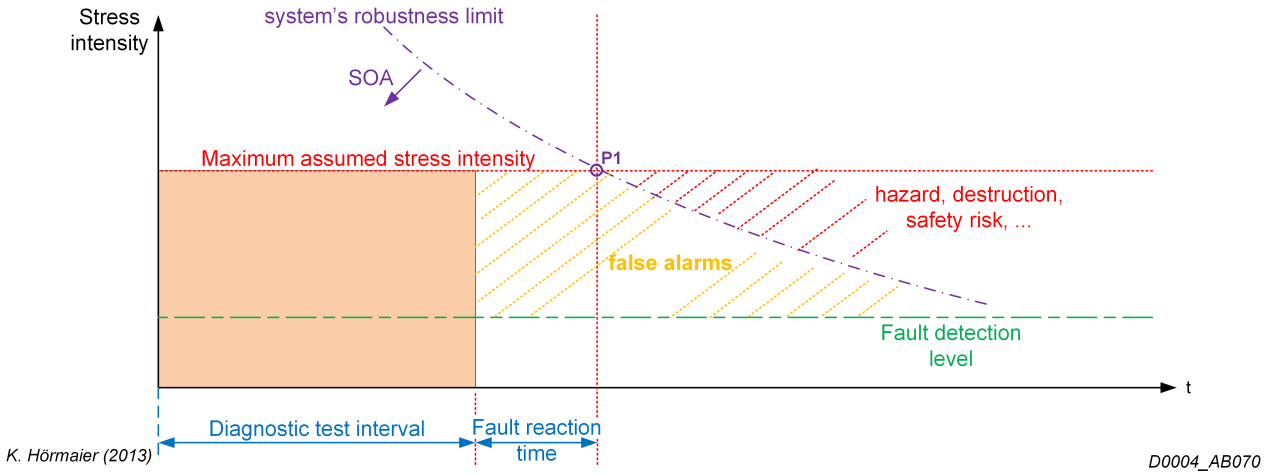


Figure 5.15: Separation of the operation area into the hazardous area and the Safe Operating Area (SOA) which is further divided into the area of false alarms and the robust area.

As required in Section 4.12, the safety mechanism has to bring the system into the safe state within the FTTI. In Figure 5.15 the red chain dotted line indicates the boundary of the **S**afe **O**perating **A**rea (SOA). Within the SOA, which is a function of time and stress amplitude, the system can handle the stress event without disturbance. Thus, the FTTI depends on the stress amplitude as well.
The engineer has some degree of freedom to design the system and the corresponding safety mechanism. Firstly, the engineer might be able to increase the robustness of the system and therefore increase the FTTI. In addition the engineers might be able to influence the maximal possible stress intensity for example, by limiting the current with a resistor between the supply and the system. And finally, the engineer can influence the detection level, the diagnostic test interval and the fault reaction time. These parameters can be varied to get an optimal design. A detection mechanism is often not able to take the real boundary of the SOA into account due to effort in implementation. Instead, a fixed stress intensity is used as detection level. If the stress intensity exceeds this limit the safety mechanism has to detect this excess and brings the system into safe state. From a functional safety view, very short reaction and detection times are the targets to aim for, but this will lead to a high number of false alarms. False alarms are these events where the safety mechanism forces the transition of the system into safe state even if the stress event would not cause a risk. These false alarms have to be avoided from the point of availability as well as for a good reputation of the product (company). Thus the engineer has to build the system and its safety mechanism in a manner that the ordinary environmental stress conditions do not lead to hazard or to a false alarm. As shown in Figure 5.15 the stress events like pulses defined in (ISO 7637) shall be part of the orange area, in which no alarm is triggered and the system is not damaged. With it, the robustness and the maximum stress intensity can be set. In the next steps, the remaining parameters will be defined (optimized).
In Figure 5.16 two different detection mechanisms are sketched. They differ in their complexity of realisation and their accuracy. The left mechanism uses a physical behavioural model of the system to predict the SOA. It represents a line parallel to the real SOA boundary. If the stress amplitude in combination with the stress time exceeds this line a failure flag is raised and the transition into safe state is executed. The detection mechanism on the right side, which can be realised more cheaply, compares the stress event's amplitude with a defined fault

detection level. If the stress event's amplitude exceeds the fault detection level for a defined time span, a fault flag is set. The fault detection level shall be below the SOA but to avoid false alarms, it shall be as high as possible. Thus the optimal value is the DC maximal rating of the component. The optimum regarding the sum of diagnostic test interval and the fault reaction time is the point P1 drawn in Figure 5.16. It has the lowest number of false alarms for a certain design. For the fault reaction the optimum can be reached by minimizing the fault reaction time, thus the diagnostic test interval shall be maximised to reach P1. The diagnostic test interval additionally consists of the diagnostic itself and a possible idle time. Form the point of false alarms, the idle time shall be minimised as well leading to a maximisation of the diagnostic within the boundaries.

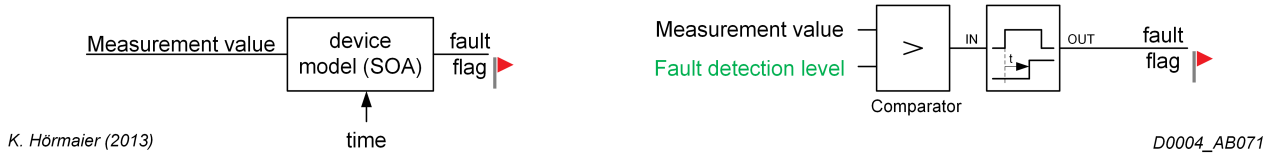


Figure 5.16: Two different realisations of detection mechanism to detect stress possibly exceeding the SOA. On the left side the device model is used to predict the boundary of the SOA which is used for minimal false alarms. On the right side, the easy to implement comparison with a fixed limit is shown. If the stress exceeds for the defined time span the defined fault detection level, a fault flag is raised.

The previously considerations are only valid for single pulses, because the SOA is only valid for typical start conditions. If for example the start temperature is higher due to previous stress events, the capability of resisting stress might be temporarily be reduced.

5.6.4 Separation in Frequency

The separation in frequency is commonly known and often used [72]. Hence this work will give only a rough overview.
Filters are used to separate the desired signal from the interference in the frequency domain. Depending on the properties, these filters can be low-pass, band-pass or high-pass filters with various damping. The filter allows the desired signal to pass but the power of the interference signal is rejected. For all of these approaches, it is necessary that the interference has another frequency as the desired signal's frequency. However, if the interference's frequency is the same, an alternative method is needed. It is possible to change the operation frequency depending on the interference frequency as for example, in a capacitive measurement device, the carrier frequency has to be changed depending on the EMI frequency [73].

5.6.5 Separation in Amplitude

EMI signals and desired signals may be distinguishable by their specific signature of amplitude over time. For a function untypical changes of the amplitude can be detected and filtered. For example, a thermal sensor provides a temperature proportional voltage at its output (V_{OUT}). High EMI can couple (e.g., capacitive) into this sensor interface and change the output voltage. The change due to for example pulses defined in (ISO 7637), is very fast. A step function can be seen at the output. On the other hand, the temperature at the sensor cannot jump that fast. Thus, depending on the change rate of the amplitude a distinction between a real

temperature increase and an increase due to EMI can be detected. By limiting the change rate of the amplitude, EMI can be filtered.
For measurements, typical counter measures as for example correction of outliers, to erase the effects of EMI are taken. Depending on the measurement values, some values can be discarded for calculation. For example, for the DC value of a signal not the mean but the median shall be calculated.
High voltages can be clamped by for instance zener diodes. Also active clamping is possible, such as by switching on the output transistor to regulate the interference.

5.6.6 Safety Measures

Safety measures consist of the previously described safety mechanism in addition to all activities improving safety which are not directly implemented in the product. The safety measures, which improve the robustness of the product regarding EMI, shall be elicited during FMEA. The list of safety measures can be long and strongly depends on the design and verification process. Some examples of valid safety measures targeting EMI are stated in what follows.
Measures like a design rule check, which targets cross coupling, can be included as well as rules limiting the maximum impedances of nodes inside the system. Also EMI testing and EMI simulation as well as EME simulations should be included in the list. As previously explained contracts, consisting of a promise and an assumption, have to be checked for their consistency. If a pair of contracts or a combination of several contracts are inconsistent a systematic fault might be in the system. Tools support the analysis of contracts and high automation is possible [74]. Also test case generation out of contracts is possible and even methods to trace down the source of a fault in the **S**ystem **U**nder **T**est (SUT) is possible [75].

5.7 Safety Analysis Methods

This section describes the modifications and extensions of the safety analysis methods originally described in Section 4.11. Furthermore, all aspects regarding EMI will be explained in detail.

5.7.1 Hazard Analysis and Risk Assessment (HARA)

The steps to be performed for a HARA considering EMI are the same as described in Section 4.11.1. However, the context of the analysis might be influenced by EMI. As in the ISO 26262 Chapter "Scope" the following statement is given, suggesting that the HARA shall consider the possible risk of high radiation:

> *ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards unless directly caused by malfunctioning behaviour of E/E safety-related systems.*

If a risk of harming humans by unacceptable high power EMI exists, then this risk has to be assessed by the HARA. To do so, the hazard *EMI* has to be added to the catalogue of possible hazards and has to be further analysed and compared to the EMI exposure limits on humans. If a potential risk of EMI directly harming humans is accounted, a safety goal has to be formulated which aims the avoidance of this hazard. Guidance and limits regarding the exposure on humans to radiation (magnetic, electric, electromagnetic) can be found in [76].

Consequently, the emission generated by the developed system has to be determined for safety analysis as well and not only the emission generated by systems acting as aggressors.

5.7.2 Fault Tree Analysis

The fault tree, in its origin explained in Section 4.11.2, can incorporate EMI differently. Depending on the outcome of the HARA (see Section 5.7.1), EMI has to be represented by a top event. So the top event can be formulated as for example "Generated electric field exceeds the limit of XX V/m for a duration longer than XX s in the frequency range from XX MHz to XX MHz."[8]. The fault tree is further developed, top down, by connecting the top event via a logic gate with a sequence of primary events as known from the typical FTA.
The second part, of EMI incorporation in the fault tree, is including EMI as primary event. An integration of standardized EM phenomena into the fault tree was already proposed in [77] but the publication did not take safety mechanisms into account. For this reason, primary events were connected only via OR gates making a cut set analysis obsolete. Secondary, for all base events no failure rate was assigned, leading to an only qualitative analysis of the fault tree hindering to use the FTA's full potential.
As described in Section 4.11.2 the fault tree development starts with the top event and is further developed top down to the primary events, without including safety measures. For EMI, the primary events can be additional to the typical component's faults, either SEMFM or EMFM. The newly added primary events and the typical primary events can be distinguished by additional properties (like amplitude or timing behaviour) of the new events.
Since EMI events are linked to IPs and the IPs are linked to architectural elements of the system, the EMI represented by SEMFM or EMFM can be allocated to architectural elements, with which the FTA can be constructed. In Figure 5.17, the primary events representing EMI

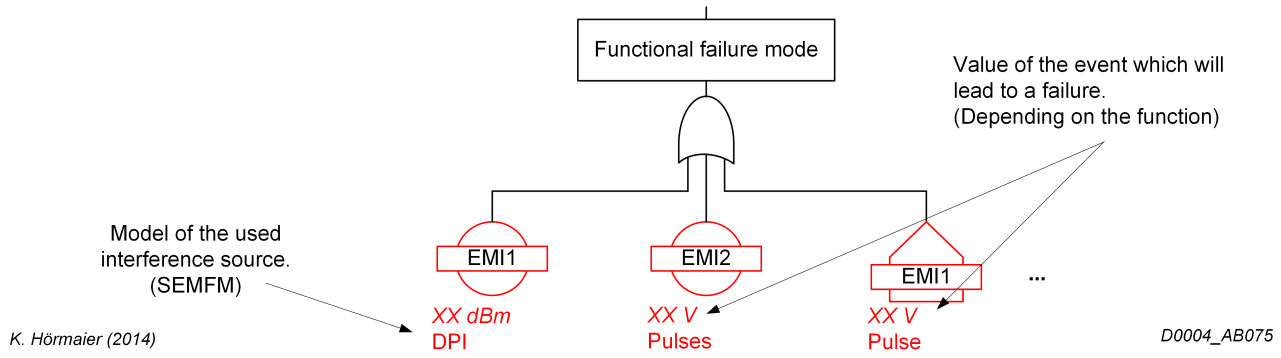


Figure 5.17: The functional failure mode can be caused by several EMFM, which can be either represented by base events or trigger events. In addition, the model and the robustness level of the architectural element is annotated.

in the fault tree are shown. In the fault tree, EMFMs can be accomplished by base events as well as trigger events. Base events are used for permanent or intermittent events and trigger events are chosen for transient events. Each of these primary events are annotated by the EMFM and the level of robustness of the architectural element. For a qualitative analysis, the fault tree is sufficiently developed but to perform a quantitative analysis, the failure rate has to be appended. The failure rate, depending on the robustness of the architectural element, can be taken from the calculations provided in Section 5.4.4 and can further be assigned to the

[8]The author disclaims to provide values. Instead XX is used as a place holder

corresponding primary event.
By performing the previous step, the initial fault tree construction is completed. In the next step, the fault tree analysis can be performed as described in Section 4.11.2. The analysis will lead to failure rates assigned to the top event. Depending on the results, it might be neces-

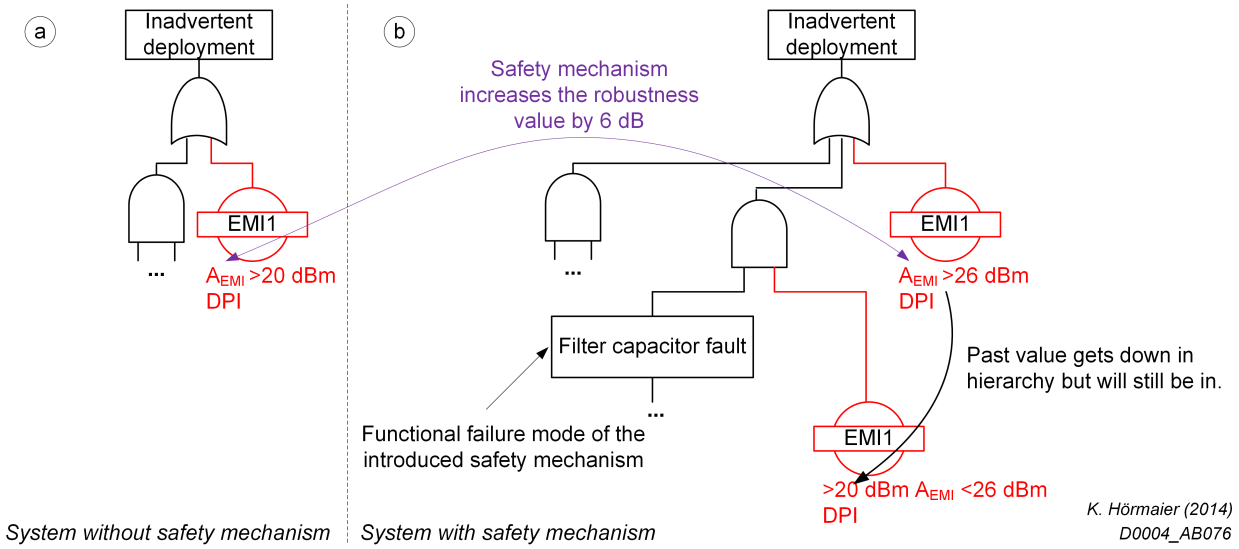


Figure 5.18: Detail of two fault trees, one without safety mechanism and one with safety mechanism regarding EMI faults. On the left side (a) an EMI fault represented by the SEMFM DPI with an amplitude of >20 dB is shown. On the right side (b) the same system is sketched but with included safety mechanism. The safety mechanism increases the robustness of the system but still a remaining susceptibility is present. Also the failure mode of the safety mechanism is included which is in parallel with the previous value of the SEMFM of the system on the left side.

sary to additionally introduce safety mechanisms which increase the robustness regarding EMI. The safety mechanisms are connected via logical "AND" gates with the EMFMs, as shown in Figure 5.18. On the left side of the figure, the system without the safety mechanism is shown and on the right side of the figure the safety mechanism is included. The safety mechanism, which is in the example a capacitor, can also fail which is taken into account in the fault tree by connecting the safety mechanism's failure mode logically with the EMFM. Since, as described in Section 5.6, a safety mechanism might not eliminate the weakness of the system completely, an EMFM at the original position will still remain. But, due to the increased robustness of the component against EMI, the annotated robustness value of the EMFM has to be adapted. In the example, the robustness has been increased by 6 dB, thus the robustness indicator and therefore also the failure rate of the initiator at the origin position have to be updated. In the case of the example, the new level of robustness is 26 dBm instead of 20 dBm. The calculation of the resulting failure rate of the new primary event can be performed according to Equation 5.13 but for the adaption of the failure rate of the original primary event the dependency to the new primary event has to be considered. In the example, the probability of EMI level higher than 26 dBm is covered by the new prime event and thus shall not be included in the probability of the original primary event anymore. Thus, the failure rate of the original component shall only represent the probability range between 20 dBm and 26 dBm. From a physical perspective, there is only one EMI fault in the example, this single fault is only split for illustration purposes and calculation. On the other side, in addition to the EMFM also the failure mode of the capacitor is added which has also an impact on the over all failure rate.

The undeveloped event, which is used for faults which are negligible but on the other side which shall be visible for documentation in the fault tree, can be used for EMI events which are so rare that they will not be part of robustness analysis. Up to now, the fault tree does not take dependent faults into account. In the next chapter dependent faults will be analysed.

5.7.3 Dependent Fault Analysis

Especially EMI is one of the most important factors regarding the analysis of dependent faults. As EMI can be the root cause of several simultaneously occurring faults, EMI can be a common cause failure. Since the DFA is typically based on previous analysis tasks or takes them into account, here the analysis refines the FTA. In the FTA of previous steps, EMI related primary events were introduced all of which, possibly have the same cause. Up to now, these primary events are treated independently, which is sometimes incorrect. Thus, the common cause effects have to be added.
In practice, an often used approach includes a base event called EMI as common cause initiator directly leading to a violation of the safety goal (see Figure 5.19). This is formally correct, but leads to difficulties in arguing why the system is, even with this initiator, safe enough to bring it onto the market. It is possible, to argue that the risk of the common cause initiator as shown in Figure 5.19 can be mitigated by testing. However increased test levels would therefore be necessary and would unavoidably lead to a increase of product costs. Another drawback is that, this approach makes it practically impossible to assign a failure rate to the newly introduced common cause event. In addition it would eliminate the benefits gathered by including EMI related faults into the FTA for example.

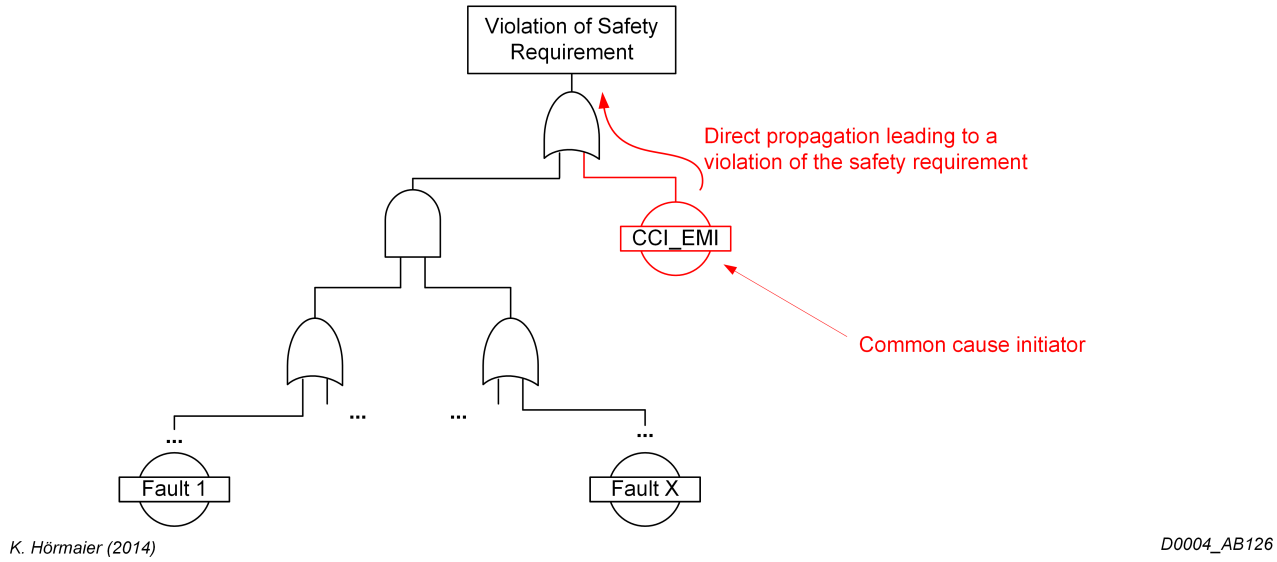


Figure 5.19: In the fault tree the base event CCI_EMI *representing EMI as a common cause initiator is included at the highest level. The base event directly propagates through the logical "OR" gate leading to a violation of the safety goal.*

As presented in Section 4.11.3 other methods are more appropriate for handling common cause failures. Typically, the reason for adding an EMI common cause initiator at the top of the fault tree is due to the gap of information of the EMI sources. However, in the presented approach this information has already been elicited and can be further used. Since the coupling paths

between one single source and the EMFs are known, this dependency can be added as a common cause to the FTA. As shown in Figure 5.20 the EMFs can be tracked back to the EMFM of the source. To calculate the failure rate of the two events, the propagation within the fault tree has to be taken into account.
At first glance, the easiest approach to use, for all initiators with the same common cause, is to have one global primary event. Yet, this approach has a major drawback. A global fault is one single fault with one failure rate. But, as shown in Figure 5.20, the initiators have different failure rates, although they are connected to the same common cause. Therefore, the global fault cannot be efficiently used to represent EMI as common cause fault.
A better approach is the usage of the β-factor, which additionally is fully supported by available FTA tools. Each of the EMFs, with the same common cause, gets assigned a β-factor of one. Since the failure rates of the EMFs vary due to the different coupling paths, the calculation of the fault propagation has to follow the Equations 5.18:

$$\lambda_{CC} = \beta \cdot \min(\lambda_1 \dots \lambda_N) \tag{5.18}$$

and 5.19

$$\lambda_{In} = (1 - \beta \cdot \min(\lambda_1 \dots \lambda_N)) \cdot \lambda_n \tag{5.19}$$

By replacing the β by one, the equations can be reduced to:

$$h_{CC}(t) = \min(h_1 \dots h_N(t)) \tag{5.20}$$

which means that the common portion ($h_{CC}(t)$) is equal to the failure rate of the EMF with the lowest failure rate. As a result, also the individual failure rates are updated according to the following equation:

$$h_{In}(t) = h_n(t) - \min(h_1(t) \dots h_N(t)) \tag{5.21}$$

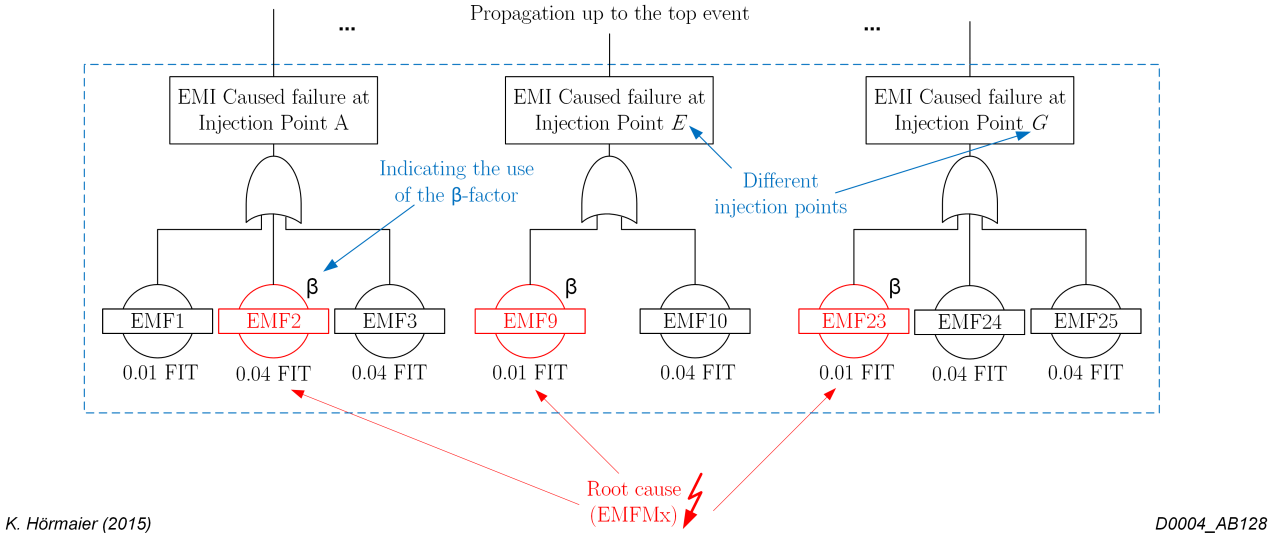


Figure 5.20: The bottom line of the fault tree with the EMFs.

The fault propagation within the fault tree is done as sketched in Figure 5.20. The two EMFs (*EMF1*, *EMF2*), which are connected via different logical operators, have the same common cause and therefore a common β-factor of one. Thus, the resulting failure rates for the logical OR connection and the logical AND connection can be calculated. The calculation of the logic OR gate does not differ from the typical calculation because still the upper boundary defines the

OR gate's result but the common factor influences the calculation of the logical AND gate. The calculation of the resulting failure rate $h_R(t)$ can be done for the AND connection as follows: To calculate the failure rate resulting from the AND connection, first the unreliabilities $F_x(t)$ for all contributing failure rates $h_x(t)$ have to be calculated as:

$$F_x(t) = 1 - e^{-\int_0^t h_x(\tau)d\tau} \tag{5.22}$$

This leads to unreliabilities $F_{CC}(t)$, $F_{IEFM1}(t)$ and $F_{IEMF2}(t)$. Taking those unreliability information, the unreliability of the system $F_R(t)$ can be calculated as:

$$F_R(t) = F_{CC}(t) + F_{IEFM1}(t) \cdot F_{IEMF2}(t) = F_{CC}(t) + (F_{EFM1}(t) - F_{CC}(t)) \cdot (F_{EMF2}(t) - F_{CC}(t)) \tag{5.23}$$

The resulting failure rate $h_R(t)$ can be obtained by:

$$h_R(t) = \frac{\frac{dF_R(t)}{dt}}{1 - F_R(t)} \tag{5.24}$$

In the previous description the EMI faults were assumed to be correlated, which is true from the stress amplitudes view[9], but might be incorrect from a time perspective. Considering a source of a transient fault which couples via different paths to the two IPs and considering a time shift of the EMI event at the IPs due to the different coupling paths the transient EMI faults might not occur simultaneously. If the functions recover after the transient fault, and the shift in time between two EMI events is large enough, redundant functions might not be simultaneously interfered.
Beside externally caused EMFs, EMI can also be caused within the system itself. A fault within the system causes the function to generate interference which might couple to neighbouring blocks / functions. As shown in Figure 5.21 a fault in function block one has an influence on a neighbouring, logically independent functional block. The fault possibly propagates via various coupling paths, thus the analysis of those paths is a need for the DFA. Functions, which generate high interference due to an internal random hardware fault, have to be considered for analysis. For those functions the coupling paths (IPs) to other components have to be elicited as described in Section 5.2.2

5.8 EMI as Stress Factor

EMI introduces power or current / voltage into the system. Both, power leading to a temperature increase as well as high voltage might pose stress. As described in Section 4.9.2, stress can lead to pre-aging and therefore might increase the failure rate. Temporary stress usually contributes little to pre-aging and might be neglected. But other EMI events, which are supposed to be permanently present, have to be considered as a stress factor. Thereby, the OEB is used as an easily applicable but pessimistic value. The OEB has to be converted into the proper quantities for stress representation. An example for an injected power P, the stress and therefore the acceleration factor AF can be calculated based on 4.17 as follows:

$$AF = e^{\frac{\Delta E}{k}\left(\frac{1}{T_{Ref}} - \frac{1}{T_{Amb.} + P \cdot R_{th}}\right)} \tag{5.25}$$

with the ambient temperature $T_{Amb.}$ and the thermal resistance R_{th}.
The gained acceleration factor can further be used to calculate the resulting failure rate.

[9]The amplitude dependency is already covered by the failure rate calculation which takes the coupling factor and therefore the amplitude dependency into account.

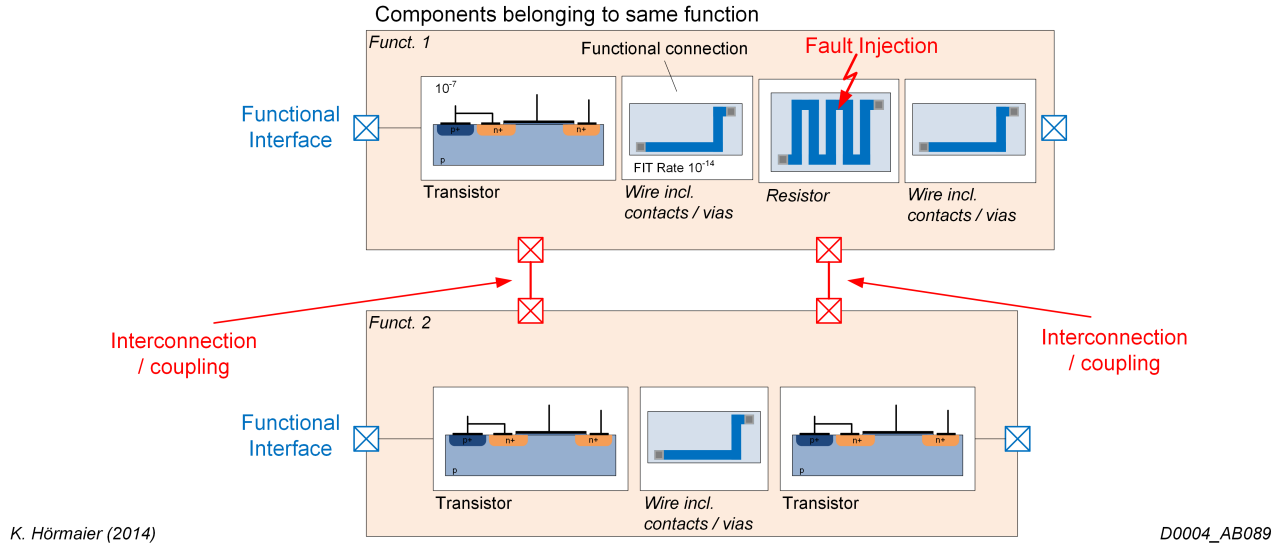


Figure 5.21: Two logically independent functions are shown. One of the functions includes a fault influencing the other function. Thus, the internal coupling mechanisms have to be added in the safety analysis. These dependent faults might eliminate the benefits of redundant functions.

5.9 Verification

The verification of the safety mechanisms is a difficult undertaking because the safety mechanism controls the system only in case of a fault. Thus, in verification these faults have to be introduced into the system which is done by fault injection.

5.9.1 Fault Injection

The robustness of the system regarding random hardware faults has to be verified also with regard to the effectiveness of the safety mechanisms. During the occurrence of the fault, the system's functions have to be observed and deviations from the expected behaviour are recorded. Random faults have typically a very low probability of occurrence. The failure rate is in the range of 10^{-9} failures in one hour (or 1 failure in 10^9 h = 114.000 years). Waiting for the natural occurrence of those faults is therefore impractical. Thus, fault injection allows to speed up the process by increasing the fault occurrence [78]. In the context of the ISO 26262, fault injection techniques regarding hardware faults are used to evaluate the effectiveness of safety mechanisms in the design.

Fault injection is a verification method, which inserts representational fault models into the DUT, in order to observe their influence on the DUT's functionality (see Figure 5.22). A correctly working component is replaced by a faulty variant of it.
There are various methods of injecting faults into the system. Faults can either be injected randomly or guided. A random fault injection method arbitrarily selects the component (component model) to be replaced by the faulty model. In the guided approach the user (verification engineer) selects specific components which, in the engineer's expert judgment, have an impact on the DUT's safety. The guided approach allows minimising the number of injected faults, but leaves responsibility and work to the user. Additionally, fault injection can be carried out at different levels of abstraction. The faults can be injected on a physical level (e.g. using a transistor fault model) up to the highly abstract functional level (e.g. controller fault model).

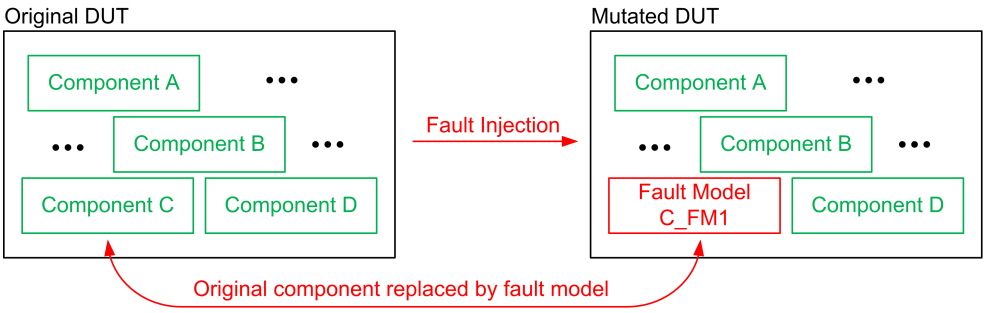


Figure 5.22: Principle of the fault injection. At least one component of the original design is replaced by a fault model(s). The process of exchanging the original component by the fault model is called fault injection.

The choice of the appropriate abstraction level is a non-trivial challenge. The main advantage of choosing a high detail level is that the fault models can be picked from a standard fault library. Thus, fault injection can be highly automated. In addition, several effects can be considered which might not be visible at higher abstraction levels (e.g. common reference voltage for two functional independent blocks). A further benefit is the accuracy of the resulting failure modes. An example is the abstract functional failure mode "oscillation", which would need at least the properties / values frequency and amplitude. It can be difficult for the verification engineer to define these values without a deep knowledge of the underlying circuits. For low level injection this knowledge is unnecessary because those parameters are automatically obtained by the evaluation of the low level faults. The main drawback of the injection at low abstraction level is the possibly huge number of faults to be injected resulting in long test times (simulation or physical testing time).
The second approach models the faults on high abstraction level. The functional blocks are used as a basis for the fault injection. The main benefit is based on the fact that, the high abstraction level strongly reduces the number of faults to be injected. The high abstract view consists of only a few blocks and functions compared to the low level. In most cases it is quite easy to build an equivalent model which describes the fault. For instance, a communication interface can transmit wrong date or no data. A disadvantage can be in addition the possibly pessimistic failure rate. The assessed failure rate is typically based on the block area and thus might be higher than the real failure rate, because components might be included which are safe faults.

The following calculations highlight the scalability problem of low abstraction level fault injection. Calculation of the number of necessary simulations $\#_{Sim}$ for single-point faults:

$$\#_{Sim} = \sum_{n=1}^{N} \#_{FM,\chi_n} \tag{5.26}$$

with the number of components N at the actual abstraction level and the number of **F**ailure **M**odes (FMs) $\#_{FM,\chi_n}$ of the component χ_n. Therefore, the simulation time is proportionally increasing with the number of components. Assuming a nearly equal number of component failure modes, the simulation time increases linearly with the number of components. Taking multi-point faults into account will increase the simulation effort dramatically. More than one fault has to be injected in each fault simulation. The following equation shows the approximate

calculation of all possible fault simulations:

$$\#_{N,k} = \binom{N}{k} = \frac{N!}{k!(N-k)!} \tag{5.27}$$

Here k is the number of considered faults occurring at the same time and N is the number of components. The ISO 26262-5: 7.4.3.2 requires considering multiple-point faults up to an order of two. Using Equation 5.27 for dual-point faults leads to Equation 5.28.

$$\#_{N,2} = \binom{N}{2} = \frac{N!}{2!(N-2)!} = \frac{N(N-1)}{2} \tag{5.28}$$

The activation of the faults requires additional DUT's inputs, which have to be controlled by the user. Inserting fault can be done by two main methods. In the first method, a copy of the design at a new storage location place is generated. This copy is modified to include one of the faults. The simulation is performed using this new model. The main advantage is that no extra functionality has to be added to the main model. Adding faults into the original design can bear the risk of implementing the "injected" fault into the build system. Thus, a strict separation of the original and the modified design is advisable.

Functional Monitoring

Injecting a fault covers only a part of the work to be done. The remaining part consists of the monitoring of the functionality. The function has to be monitored and deviations from the expected behaviour have to be recorded. The monitoring can measure the generated emission or focus on the functional behaviour of the DUT. Monitoring the functionality can be difficult, because typically the resulting behaviour is unknown in advance. Additionally, the time between the fault injection and a possible failure can vary. In Figure 5.23 a couple of significant examples illustrate some of the possible effects. In the first plot, the fault product violated the specification after a certain time. The monitoring of the signal's slope would indicate to wait until the spec violation. In the second plot, the signal's slope changes also without a fault but in addition, a trend can be observed which can be used as an indicator. In the last plot the fault leads to an error, but not to a failure. Thus, the simulation time shall always be as long as a failure occurs or the signal settles. In addition also a dead-time might exist, in which no change from outside of the system can by observed. Thus, the defining of the minimum observation time is a challenging task which is product dependent and has to be considered carefully.

Fault injection on module level

EMI faults have to be injected at each IP. For large scale products it is often unfeasible to include the whole DUT in the simulation, due to limitation of simulation time. Thus, the component has to be divided into modules (blocks) where each of the blocks build for them self an entity. These modules can be simulated individually with the benefit of quicker simulation time compared to a complete simulation of the whole component. The module itself might have some injection points, which the verification engineer tests. During fault injection the verification engineer observes the module's functional behaviour and depending on the observations decides whether the module passes or fails the test. As a result, engineers often miss an important aspect. The module, they are verifying, might not be directly the victim, but an entrance for the interference coupling into the component. To take this into account, not

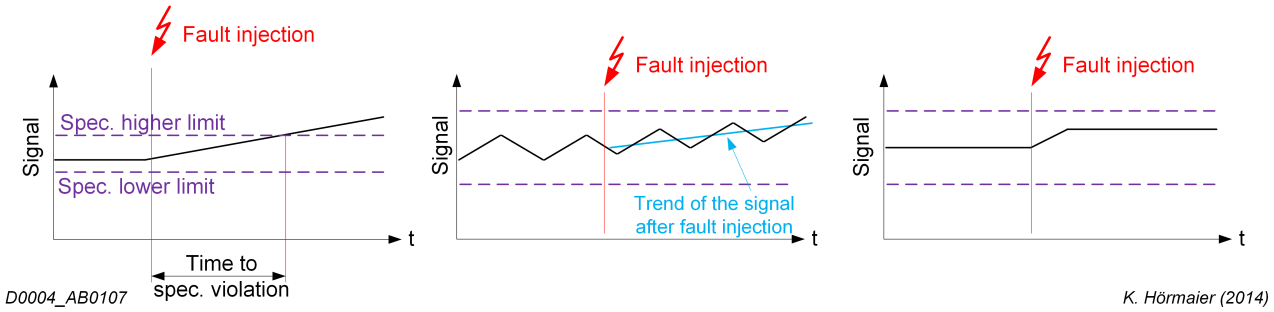


Figure 5.23: An injected fault might not directly be visible as a violation of the specification. Thus the observation time shall be dependent on the reaction of the system. In the first graph the specification is violated after a certain time. In the second graph, a signal tends to violate the specification. Here, the observation time shall be increased. The last plot shows a change of the observed signal but in this scenario the fault does not lead to a specification violation.

only the functionality but all remaining interfaces have to be monitored as well. It is assumed, that usually engineers do not monitor input signals because they themselves had defined same. Engineers suppose that the system's inputs are not influenced. In Figure 5.24, a simulation setup verifying one module is sketched. The input interface might have a parasitic feedback on the input's source, which might get influenced by the interference. Examples for such interfaces are reference signals or power supply nets coming from other modules.
Typically, the connected modules are replaced by ideal components like voltage sources or current sources, which are not expected to fail. But real sources might fail. Even if the source does not directly fail, which means the support for the module under test is still sufficient, other modules connected to the same supporting source might fail due to the coupled EMI. In order to consider this topic, the simulation test bench has to be modified.
Firstly, the ideal sources have to be decoupled (see Section 6.3.1). In the second step, monitors and equivalent impedances have to be added at all inputs. The monitors are used to store the maximum EMI rating at the input and the equivalent impedance is necessary in order to avoid over-engineering. Generally, the standard decoupling is effective, but sometimes better than required. The monitored amplitude at the input can be lower, depending on the source impedance or other connected modules. Thus, the additionally connected impedance (Z_M) controls the load of the block (see Figure 5.24).
The load impedance at the interface can be controlled by the decoupling impedance, but for the designers understanding the additionally introduced impedance better illustrates the dominant impedance.
Before the victim's safety analysis regarding EMI can be performed, some prerequisites are necessary. Specifically, the interference emitted by the aggressors has to be characterised, including aggressors' failure modes which might lead to increased emission. To analyse the possible emitted emission, methods like fault injection might be used. This means that a fault is injected into the aggressor and the emission is characterised.

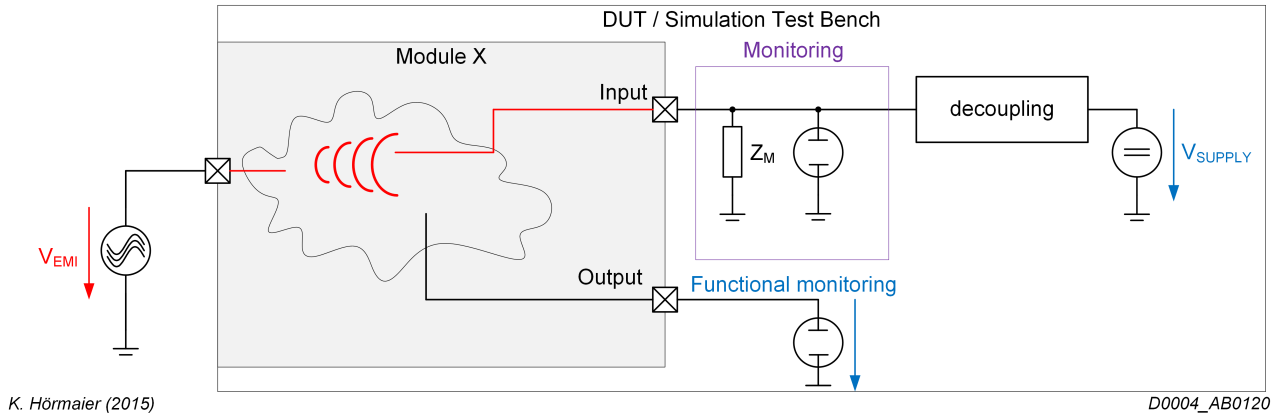


Figure 5.24: A component's module as entrance of interference into the component. All interfaces including supporting interfaces have to be monitored.

Chapter 6

EMI Simulation

The previous chapter (5) builds upon the knowledge of EMFMs. The EMFMs are aggressor's failure modes which generate high EME. Therefore, methods to gather the emission information are needed. These methods have to estimate or measure the generated emission in case of faults. To obtain the EMFMs as early as possible, emission simulation provides an adequate method to identify the generated EMI. Thus, this chapter will provide the necessary method of evaluating emission by simulation.
Emission simulation as well as immunity simulation are recommended to support product quality. As a reminder, EMC is not only a safety requirement but also a minimum EMC is required for all other functions (for product quality). Thus, investigating the product's EMC performance shall be carried out independently of the safety relevance of the product. EME simulations shall be applied for product quality as well as for functional safety. In order to avoid carrying out work twice, the methods for evaluation of the EMFMs shall be applicable for product quality measures and vice versa. This can be achieved by applying the same setup with one small difference. The only difference is due to fault injection for obtaining the EMFM's emission spectrum. Thus, in this chapter no distinction between emission generated in normal operation mode and emission generated in a failure mode will be made except the fault injection. The emission simulation delivers the EMFM, thus in the following the term EME simulation is used instead of EMFMs evaluation.

Typically the simulation's execution times can be very long, hindering the broad acceptance of these simulations. This chapter will also take the efficiency of simulations regarding effort and simulation time into account.

EMC simulations can be complex and as a result tend to be prone to errors. Since a simulation relies on the used models and the solver which calculates the output, its correctness has to be ensured. Measures have to be put in place which could detect incorrect simulations. The most reliable solution is to perform measurements on hardware to confirm or fine trim the simulation results. The measurement task can also be difficult, and might not be carried out like an ideal simulation. In simulation an ideal setup or environment is easy to build but it should be comparable to measurement setup. In the measurement each individual wire has an additional impedance, capacitors have a series inductance and series resistance and so on which can be seen as parasitic elements. If the simulation setup cannot be rebuilt based on the measurement setup, a comparison often fails. Thus, as early on as the simulation, the real behaviour of the measurement setup has to be included. Therefore, the pre-silicon verification engineer has to include the components which are mandatory for the measurement task. To support the pre-

silicon verification engineer who carries out the simulation, the post-silicon verification engineer in the lab has to deliver his setup information in advance. The main impacting properties depending on the test have to be extracted in advance and shall be provided as contracts. Besides the parasitic conditions originating from the non-ideal measurement setup, the measurement setup might include intended components which originate as a result of standards, which could have an even stronger influence on the results.

EMC standards (e.g. CISPR 25 [79] for products, IEC 61967 [4] for ICs) limit the EME of electric and electrical products. The compliance to the standards is verified by emission measurements. But these measurements have to be done with a defined test setup (e.g. according to CISPR 25 [79], IEC 61967 [4]) and defined measurement equipment (defined in CISPR 16-1-1 [80]) to make them comparable, reproducible and reliable. One of these standards, the IEC 61967, defines the setup for emission measurement by the 150 Ω method for conducted emission measurement. Without following the setup, a judgement or comparison against the allowed emission limits is not possible. Thus, the same setup shall be applied for simulation to make them meaningful.

The proposed method shall be applicable on simulation of larger blocks or complete ICs where more than one source of emission might exist or the generated emission is a time variant. The described guideline will provide the designer with an overview as well as an easy process to debugging the design by means of locating the source of emission in the time domain. In order to get interpretable emission simulation results, EMC specifics (like measurement setup, measurement devices, impedances, ...) have to be taken into account. Thus, this work shows guidance for setting up an EME simulation.
In the following, first a detailed description of an EMI Receiver Model will be provided. Thereafter, the detailed process of performing EME simulations using these EMI receiver basics will be shown.

6.1 EMI Receiver Model

The model of the EMI receiver is an important part of the simulation setup. Discarding the EMI receiver characteristics in simulation leads to an EME spectrum error. This error can be up to several orders of magnitude. Before the new approach of the model will be shown, the principles of the EMI receiver are given. Detailed explanations can be found in [81].

6.1.1 Swept-Tuned Analyzer Basics

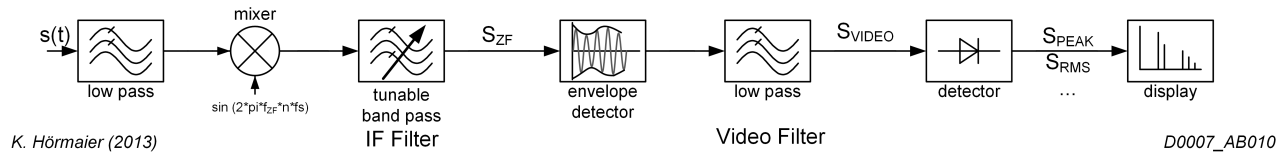


Figure 6.1: Simple block diagram of a swept analyser including the mixer, IF filter, envelope detector, video filter, a detector and the display. [81]

The structure of the swept-tuned analyzer (swept analyser) realizing an EMI receiver, shown in Figure 6.1, consists in principle of the following blocks:

- a low pass filter implementing anti-aliasing,
- a mixer to shift the frequency into the base band,
- a band pass filter depending on the current band (**I**ntermediate **F**requency filter),
- an envelope detector,
- a low pass filter which is called "Video filter",
- an EMI detector (Peak, Quasi-Peak, RMS, ...) for evaluating the interference, and
- a display block with a logarithmic diagram.

In the first stage, the swept analyser low-pass filters the input signal to avoid aliasing effects when mixing the frequency components into base band.
The mixing step's purpose is to ease the technical realisation of located after the mixer (e.g. band pass filter). Nevertheless, this has no influence on the result and can be neglected for modelling. The mixer is followed by the IF filter, which implements the **R**esolution **B**and **W**idth (RBW) by band pass filtering the input signal. Only frequency components which are within the RBW are passed through this filter. Depending on the selected band the CISPR 16-1-1 defines values for the RBW as for example, 9 kHz, 120 kHz. The filtered output signal is fed to the envelope detector demodulating the signal followed by the video filter which is for an EMI receiver set to 3 times the RBW and therefore has also no influence on the output. The video filters output is weighted by the different detectors which deliver the emission result. Following those steps the emission power at one center frequency can be measured. To obtain the whole frequency range of interest the mixer-frequency is changed stepwise. The resulting spectrum consists of several discrete frequency bins, where each frequency bin includes the power of the input signal filtered by the RBW.
The swept analyser stepwise changes the frequency at which it measures. Thereby, the swept analyser stays on one frequency for a certain time (dwell time). In the CISPR standard, a minimum dwell time is defined. Nevertheless, the analyser shall stay at least three input signal's periods on the same frequency.

Modelling Basics

The structure of the swept analyser (Figure 6.1) can be modelled in a straightforward fashion, but this leads to a long execution time. Nevertheless, the simulation speed is an important factor because the number of different frequency bins that have to be assessed for emission measurement is relatively high. For the bands B (150 kHz - 30 MHz), C (30 MHz - 300 MHz) and D (300 MHz - 1 GHz), which have to be assessed for automotive products, this sums up to a total number of e.g. 11401 frequency bins. Even if a simulation for one frequency bin with a swept analyser algorithm takes only one second, the total simulation time for the entire spectrum would still require more than 3 hours ($11401\ frequency\ bins \cdot 1\ s/3600 \approx 3h$). Consequently, there is a strong need for a fast but standard conform implementation of an EMI receiver model.
Often a **F**ast **F**ourier **T**ransformation (FFT) is used to calculate the emission spectrum. The advantages are the easy implementation and the faster calculation time. Several simulation tools support the calculation of the FFT directly in their **G**raphical **U**ser **I**nterface (GUI). On the other hand, only a subset of signals can be correctly calculated with the FFT, as the FFT is a linear operation which cannot cope with the nonlinear effects caused by the

EMI receiver's detectors. Thus the FFT can only be used for a periodic signal with a period (T) much smaller than the reciprocal of the RBW ($T < 1/RBW$). In all other cases (e.g. pulses with a repetition rate f of $f < RBW$ or time variant signals) the FFT will show lower emission compared to the measurement. Covering the large number of emission simulations needs a general valid approach. A therefore fast and standard conform implementation of an EMI receiver for emission calculation using the **S**hort **T**ime **D**iscrete **F**ourier **T**ransformation (STDFT) was presented in [82]. But also this approach needs some prerequisites in order to be applicable. Mainly a simulation time longer than $1/RBW$ is required. For signals with a repetition frequency higher than the RBW several periods have to be simulated possibly leading to high simulation execution time. Nevertheless, guidance to avoid errors by using the single FFT will be needed and therefore will be provided later on.

6.1.2 EMI Receiver Processing Overview

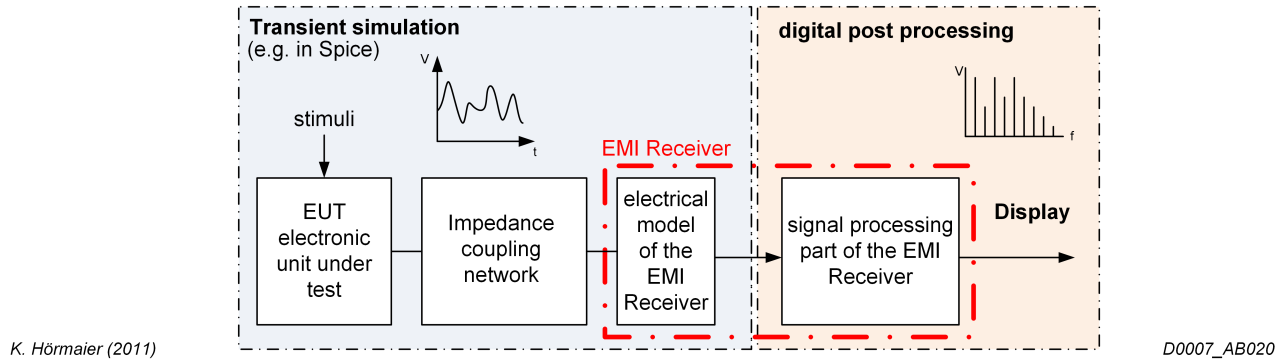


Figure 6.2: Principle of an emission simulation with an analog circuit simulated in Spice and a post processing with the EMI receiver.

In Figure 6.2 the principle of the EMI receiver within the simulation setup is shown. The implementation of this EMI receiver model consists of two parts, the feedback of the receiver's input to the test setup due to its 50 Ω input impedance and the digital post processing part. The first part is the analog part (receiver input impedance), which has to be included in the transient simulation. In detail a 50 Ω resistor has to be connected to the signal-line under consideration which emulates the 50 Ω input impedance of the EMI receiver. The second, from the transient simulation decoupled part, represents the signal processing unit including the detectors. The post processing itself consists of several steps as shown in Figure 6.3. Starting from the signal obtained by the transient simulation the spectrum and optionally the spectrogram can be gained. Depending on the simulation time steps the input signal $s[q]$ might require a resampling, which is followed by the decision whether to perform a single FFT or to apply the STDFT. Only if the STDFT path is chosen, the zero padding option can be used. Zero padding allows to gain as much information as possible also at the start and the end of the signal, which will be described in Section 6.1.4. Afterwards the STDFT, including an additional step of combining frequency bins, will be performed. In the final step of the STDFT path, detectors evaluate the spectrogram leading to the weighted spectrums $S_D[k]$.
Or in the parallel path, the FFT together with the combination of frequency bins is used to calculate the spectrum directly. To note, for the FFT no differentiation, due to different detectors, is possible and necessary. For the signal period, which is permitted when using

the FFT method, is very short, all detectors will deliver the same value. Thus no detectors functions are needed for the FFT method.

6.1.3 Resampling

The obtained transient signal $s(t)$ is represented by the quantized simulation output signal $s_O[q]$, which can either be uniformly or non-uniformly sampled. To use the latter on the FFT instead of a **D**iscrete **F**ourier **T**ransformation (DFT), which has high impact on processing time, the simulated signal has to be uniformly sampled (equidistant time steps). Therefore, the solver (of the simulation) can be set to a fixed time step. But fixing the time step typically slows down the simulation. Thus, the solver is permitted to use a variable time step, which makes post processing of the simulator output signal $s_O[q]$ necessary. The post processing resamples the signal $s_O[q]$ to gain a uniformly sampled signal $s_N[n]$. Figure 6.4 shows in plot (a) the original non-uniformly sampled signal $s_O[q]$ and the expected resampled result with equidistant time steps $s_N[n]$. To avoid aliasing effects, the easiest approach would be to resample the signal to the highest sampling rate contained in the original signal, but this will lead to a high amount of data and unnecessary high calculation times for the FFTs later on. Typically, the frequency range of interest is limited according to the measurement standards, such as for ICs in the automotive domain the frequency range of interest is 150 kHz to 1 GHz. Thus, the maximal required frequency components can be limited to the highest frequency of interest (e.g., 1 GHz). Therefore, higher frequency components can be filtered out, but adding a safety margin to take non-ideal filtering effects into account for accuracy is necessary (e.g., the filter cut of frequency of 5 GHz). For filtering out high frequency components, a moving average filter can be used which builds the average of the original samples between two target signal time steps as shown in Figure 6.5. By using a zero order hold, the average between two samples can be calculated as

$$s_N[n] = \frac{1}{T_{ab_n}} \sum_{q=a_n}^{b_n} s_O[q] \Delta t_q \tag{6.1}$$

with $\Delta t_q = t_{q+1} - t_q$ (the time between two none uniform samples), and the T_{ab_n} is approximately the inverse resampling rate ($1/F_S$).
For the time steps which are below the target sampling rate, linear interpolation is used to obtain the new samples, as shown in Figure 6.4 plot (c). An appropriately accurate solver has to control the time step size in order to control the maximal error. High order effects between two samples are therefore not permitted. Thus, it can be assumed that linear interpolation delivers sufficiently accurate results. Even if the signal does not include frequency components below the highest frequency of interest (according to the standards) an up sampling is not useful because no additional information can be gained. Thus, the target sampling frequency is limited to the maximum contained frequency component in the original signal.

$$f_{max} = min\left[max\left[\frac{1}{\Delta t_q}\right], F_S\right] \tag{6.2}$$

In addition for the single FFT the sampling rate shall be chosen to get the power of 2 samples, which is generally required for a FFT.

Signals with unnecessary high sampling rates (of signals with variable step size) increase the workload for the computer. Thus, a low pass filter in the simulator helps to reduce the number of values quickly.

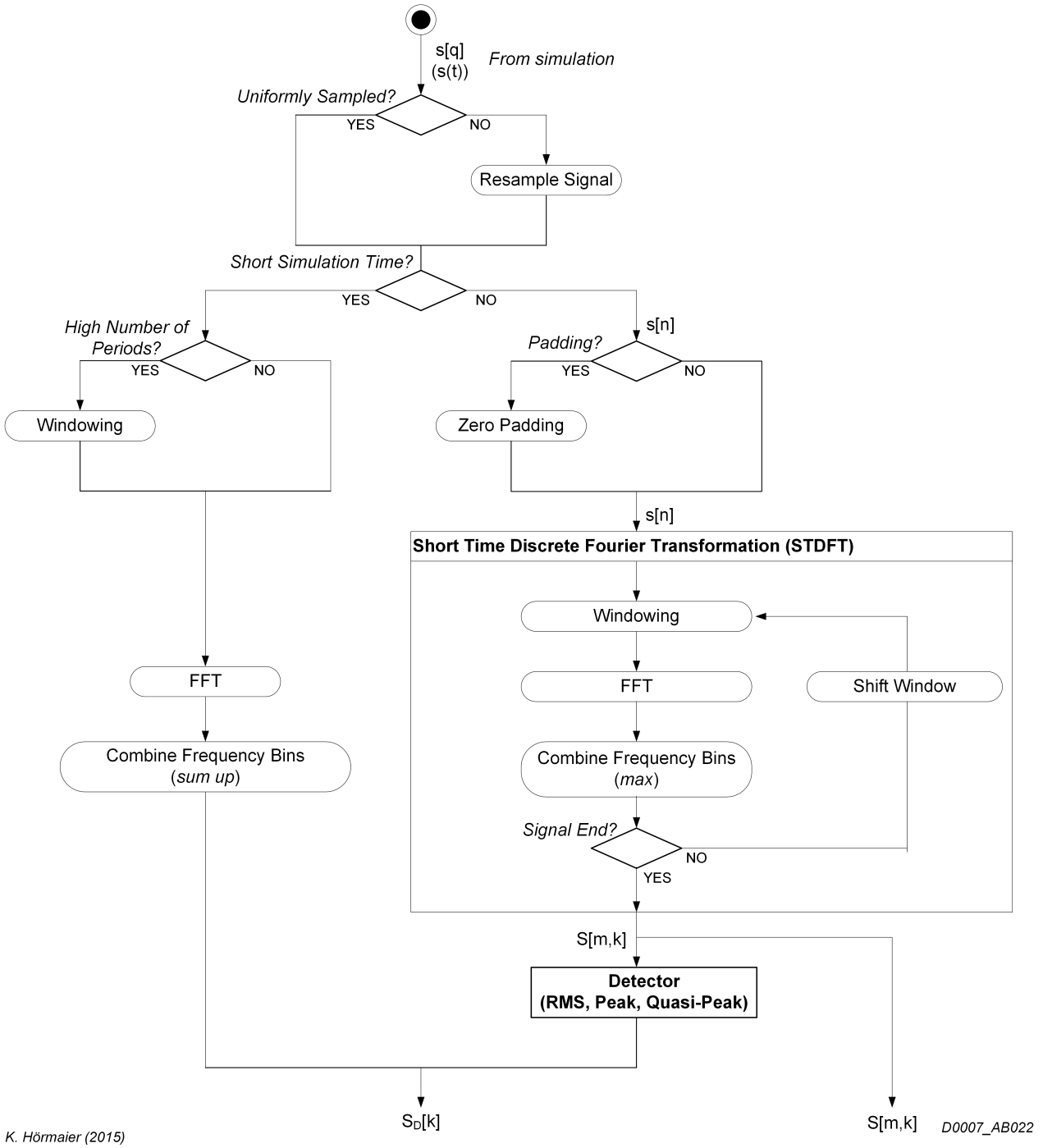


Figure 6.3: EMI receiver post processing steps used to calculate the spectrogram and the spectrum of the simulator output signal.

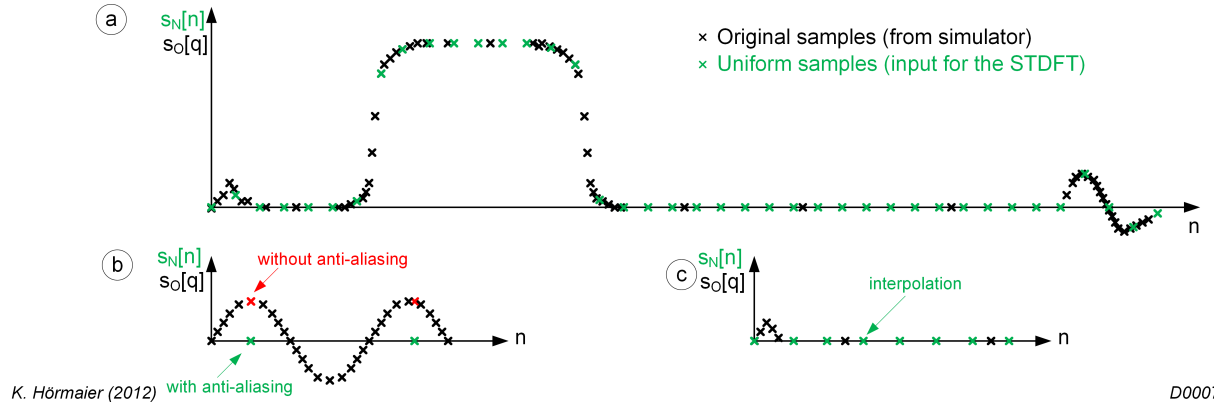


Figure 6.4: All three subplots show the output signal of the simulator s[q] as well as the resampled output signal s[n] having a equidistant time steps (uniformed sampled). The plot (a) shows a typical signal with very long time steps and very short time steps and the resulting resampled signal. In plot (b) the original signal s[q] has a higher sampling rate as needed, but down sampling without anti-aliasing would lead to wrong results. In plot (c) the time step size of the original signal is large, thus the resulting signal is interpolated.

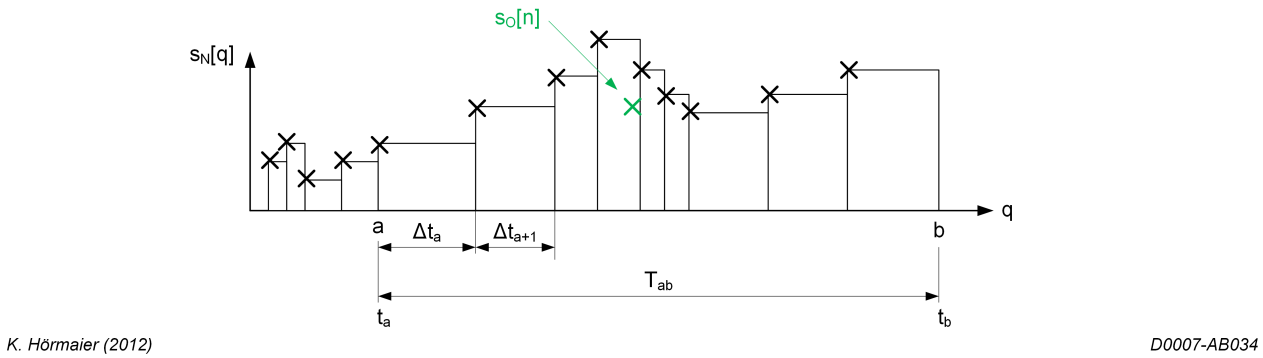


Figure 6.5: Down sampling of a signal with non-uniform samples by calculating the moving average over the sampling time span. A zero order hold is used for calculation.

6.1.4 Zero Padding

After the optional resampling, zero padding can be used to extend the signal. Thereby, the signal can be extended by adding zero value samples before the original signal starts and after the original signal ends. Thus, zero padding helps analyzing the very beginning and the very end of a signal. It is mainly used for signals which generate pulsed emission. The details of padding the signal and the rational, why to perform padding at all, will be described in detail in Section 6.4.2.

6.1.5 Short Time Discrete Fourier Transformation (STDFT)

The optional resampled and zero padded signal $s[n]$ is transformed by the STDFT obtaining the spectrogram $S[n,k]$. The STDFT is given by

$$S[n,k] = \sum_{m=0}^{L-1} s[m+n] \cdot w[m] e^{-j\frac{2\pi}{N}km} \tag{6.3}$$

where n represents the discrete time variable, k represents the discrete frequency variable and w represent the window function of the length L. Solving this equation results in the spectrogram with discrete time and frequency steps S[n,k]. In the equation, the windowing function emulates the **I**ntermediate **F**requency (IF) filter characteristic, inherently seen as the IF filter model. As shown in Figure 6.6 the window function is shifted by discrete time steps over the signal. Each windowed part of the signal is transformed by the FFT generating a slice of the spectrogram.

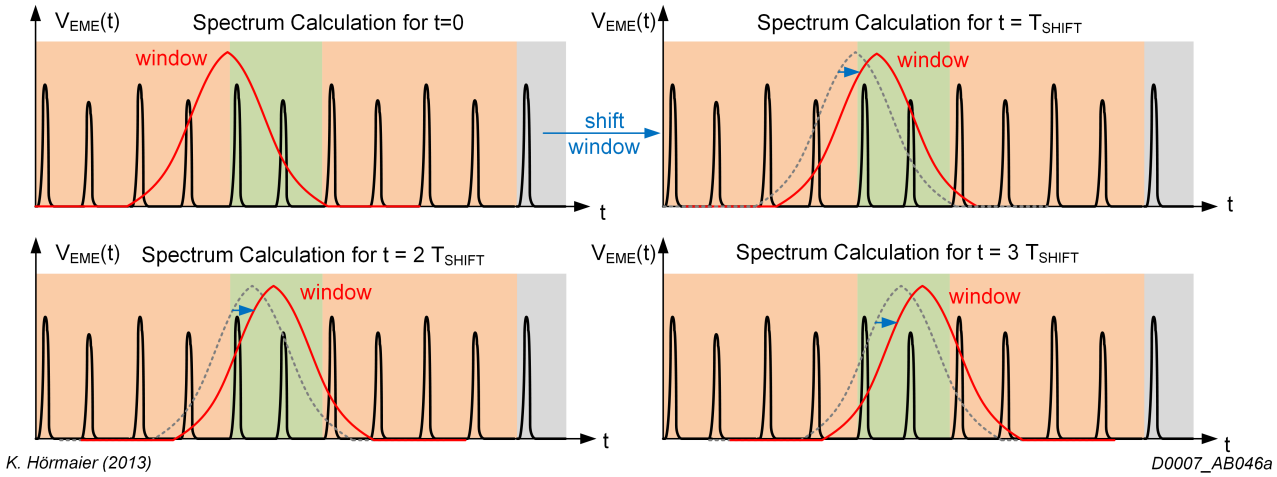


Figure 6.6: The window is shifted over the input signal. Each windowed signal part is afterward transformed by an FFT.

6.1.6 Model of the IF Filter

By using a Gaussian window with the appropriate parameter, the band pass filter (IF filter) defined in CISPR 16-1-1 can be obtained [83]. For different bands defined in CISPR 16-1-1, different values for the RBW have to be used. Thereby, the RBW represents the -6 dB attenuation of the IF filter. Several filter topologies can fulfil this task, but practically a Gaussian window is used. With the Gaussian window the best compromise between time and

Table 6.1: Values for the standard deviation (typical and conservative) of the Gaussian window matching the IF filter characteristic defined in CISPR 16-1-1.

Band	Frequency Range	RBW	σ_{typ}	σ_{wc}
A	9 Hz - 150 kHz	200 Hz	$1.87 \cdot 10^{-3}s$	$1.72 \cdot 10^{-3}s$
B	150 kHz - 30 MHz	9 kHz	$4.16 \cdot 10^{-5}s$	$3.78 \cdot 10^{-5}s$
C/D	30 MHz - 1 GHz	120 kHz	$3.12 \cdot 10^{-6}s$	$2.70 \cdot 10^{-6}s$
E	1 GHz - 18 GHz	1 MHz	$3.74 \cdot 10^{-7}s$	$3.40 \cdot 10^{-7}s$

frequency resolution can be achieved [84]. The Gaussian window $w(t)$ can be formulated in continuous time as:

$$w(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t}{\sigma}\right)^2} \tag{6.4}$$

Hereby σ is the standard deviation of the Gaussian window function and t is the time. For the digital realisation of the window the discrete time representation $w[n]$ is given as:

$$w[n] = \frac{L-1}{\sigma F_S\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{n}{\sigma F_S}\right)^2} \tag{6.5}$$

where σ is the standard deviation, F_S is the sampling frequency and L the length of the Gaussian window. Since the IF filter characteristic is defined in the frequency domain, the window function in the frequency domain $W(f)$ is needed. By transformation $w(t) \multimap W(f)$ the frequency behaviour $W(f)$ can be calculated as:

$$W(f) = e^{-2\pi^2\sigma^2 f^2} \tag{6.6}$$

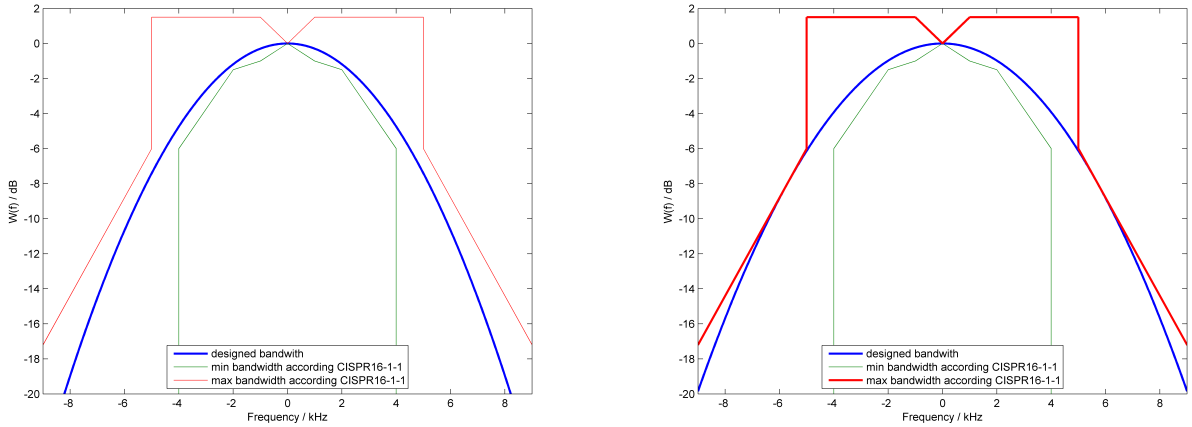
with the standard deviation σ and the frequency variable f. Since the input signal is multiplied in the time domain with the windowing function a convolution is performed in the frequency domain.
The measurement standard CISPR 16-1-1 defines the RBW as the frequency span at which the IF filter has a damping of $-6dB$. Taking this point as filter design target, the following equation can be used to obtain the required standard deviation σ:

$$\sigma = \frac{1}{\pi RBW}\sqrt{-2ln\left(10^{\left(\frac{d_{dBV}}{20}\right)}\right)} \tag{6.7}$$

with RBW the defined resolution bandwidth (e.g., 9 kHz) and d_{dBV} which is the required damping (-6 dBV). Table 6.1 gives the possible standard deviation values σ_{typ} for different bands as defined in the standard CISPR 16-1-1.
Since the measurement equipment is confirmed as long as its characteristic is within the boundaries shown in Figure 6.7 and the measurement equipment is not known in advance a more conservative approach shall be used. Thus, for the standard deviation σ of the Gaussian window function instead of the previously obtained values, the conservative filter characteristic shall have the maximum width as shown in Figure 6.7. By numerical optimization, the conservative values σ_{wc} of σ have been obtained and are listed in Table 6.1 as well.

Window length optimization

During the EME assessment, measurements at a discrete number of frequencies bins is performed. For each of these bins the standard defines how the frequency components, corresponding to the bin, should be weighted. Ideally, all frequency components corresponding to



(a) Typical filter design for Band B ($RBW = 9\ kHz$)

(b) Conservative design for Band B ($RBW = 9\ kHz$)

Figure 6.7: Filter characteristic of the IF-filter in frequency domain, for a RBW of 9 kHz. According CISPR 16-1-1 the frequency response of the filter is required to be within the limits indicated by the red and green lines. For both views, the center frequency of the filter has been set to 0 Hz.

the bin should obtain the same weight. However, it is not possible to design such filters. Therefore, the standards define certain limits for the weights. This implies that frequency components that do not coincide with the center frequencies of the bins get lower weights. However, when EME is assessed during simulation this effect should be avoided because a small change of for example, the time basis will lead to a shift of the frequency components. Thus, the variation of the weights must be minimised while keeping the number of bins and in turn, the simulation time low. The distance between two frequency bins of an FFT can be calculated by:

$$\Delta f = \frac{1}{T_W} = L \cdot F_S \tag{6.8}$$

where T_W is the time length of the window equal to the length L of the windowing function multiplied by the sampling frequency F_S. If the frequency bins of the FFT have a large distance compared to the windowing function (frequency response of the IF filter) an amplitude error e_{AMP} or even gaps in the frequency spectrum will occur (compare Figure 6.8). In order to find the optimum window length for a given amplitude error e_{AMP} the following equation has to be solved:

$$W(f) = \max_{i=1:M} \left[e^{-2\pi^2\sigma^2(f-f_{C,i})^2} \right] \tag{6.9}$$

$W(f)$ represents the attenuation of a signal component at frequency f during the integration of the signal power within the evaluation bins.
The equation shows the convolution of the frequency response of the window function with the frequency bins f_C of the FFT. The maximal amplitude error can be calculated by following equation:

$$e_{AMP,max} = \frac{W\left(f_{C,i} - \frac{\Delta f}{2}\right)}{W\left(f_{C,i}\right)} \tag{6.10}$$

Solving Equation 6.10 leads to following equation which states the minimal frequency Δf_{min} between two frequency bins of the FFT for a given amplitude error $e_{AMP,max}$.

$$\Delta f_{min} = 2\sqrt{-\frac{ln\left(e_{AMP,max}\right)}{2\pi^2\sigma^2}} \tag{6.11}$$

Finally, with the Δf_{min}, the length L of the window can be calculated according to equation 6.8.

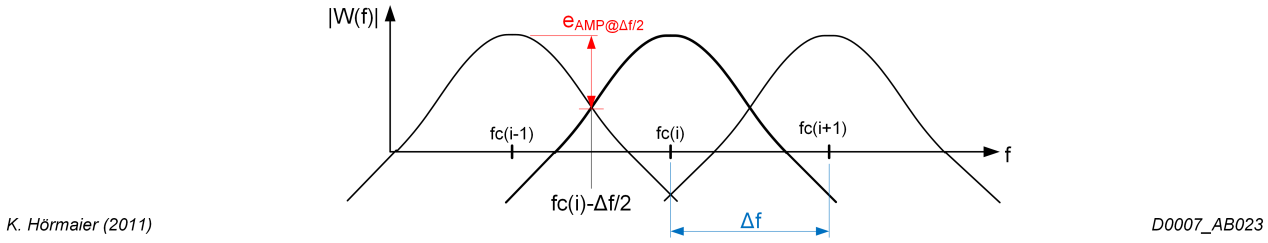


Figure 6.8: The frequency response of the IF filter convolved with discrete frequency bins. Apparently, not all frequency components obtain the same weight. However, with a sufficient number of frequency bins, the drop between them can be kept low, and a maximum amplitude error of $e_{AMP,dB@\Delta f/2}$ is achieved.

Time resolution

Not only in the frequency domain an error can arise, but also in the time domain. In Equation 6.3 the signal s[n] is shifted over the window function. Thereby N FFTs have to be performed to get the result. This adds up to a high resolution in time but also leads to a long computation time. The computation time can be dramatically reduced by skipping short shifts of the signal ($T_{Shift} \gg 1/F_S$). To avoid gaps in the time domain (to not miss a short event) the maximum allowed time shift (T_{Shift}) has to be limited. As described in [85] an overlapping of the window functions in time domain is therefore necessary. Similar to the optimization of the window length, the time shift can also be optimized. As shown in Figure 6.9 the maximum error is given at half of the distance between two window functions.

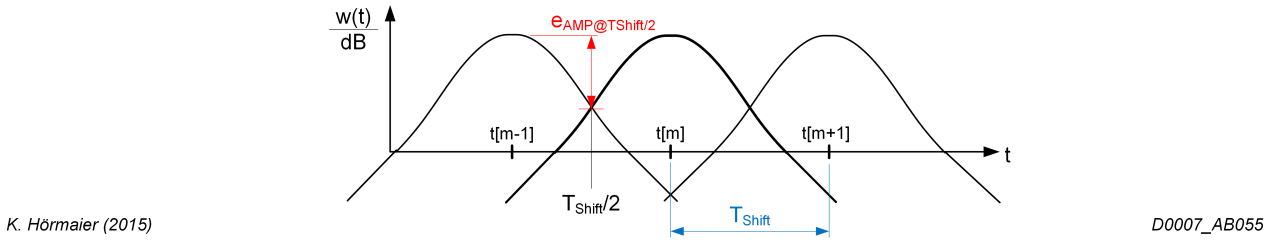


Figure 6.9: The window function is shifted by the time T_{Shift} over the input signal. Due to the shift emission events which are not concurrent with the center of the window function are weighted lower. Thereby an error e_{AMP} arises, which has its maximum in the center between two window functions ($T_{Shift}/2$).

Again the maximum error $e_{AMP@TShift/2}$, which is the ratio of the window function at the time zero $w(0)$ and the window function $w(T_{Shift}/2)$ at the time $T_{Shift}/2$, has to be limited and can be calculated as:

$$e_{AMP@TShift/2} = \frac{w(T_{Shift}/2)}{w(0)} = e^{-\frac{1}{2}\left(\frac{T_{Shift}}{2\sigma}\right)^2} \tag{6.12}$$

Table 6.2: Values for the maximal time shift dependent on the standard deviation (typical and conservative) of the Gaussian window matching the IF filter characteristic defined in CISPR 16-1-1

Band	Frequency Range	RBW	$T_{Shift} \forall \sigma_{typ}$	$T_{Shift} \forall \sigma_{wc}$
A	9 Hz - 150 kHz	200 Hz	1.79 ms	1.65 ms
B	150 kHz - 30 MHz	9 kHz	39.9 μs	36 μs
C/D	30 MHz - 1 GHz	120 kHz	2.99 μs	2.59 μs
E	1 GHz - 18 GHz	1 MHz	359 ns	326.4 ns

The transformation of the equation leads to the maximum allowed time shift for the maximum allowed error:

$$T_{Shift} = \sqrt{-8\sigma^2 ln\left(e_{AMP@TShift/2}\right)} \tag{6.13}$$

The Table 6.2 lists values for the time shift T_{Shift} depending on the IF filter's standard deviation σ and the filter design strategy (typical σ_{typ} or conservative σ_{wc}).

Combine Frequency Bins

The number of frequency bins obtained by the FFT depends on the sampling rate F_S and the simulated time span. Up to now, in the single FFT path the IF filter was not considered. As a reminder, the IF filter passes only the power of the signal in a defined frequency span. In comparison the FFT maps the "continuous" frequency components into discrete frequency bins, which typically are not coherent with the IF filter characteristic. Thus, the power is distributed over a couple of frequency bins obtained by the FFT. Therefore, the frequency bins have to be combined into the desired frequency bins f_C. This can be achieved by summarizing the frequency bins obtained by the FFT as shown in Figure 6.10.
To consider the fact, that the IF filter characteristics of two neighbouring frequency bins overlap for summing up the frequency components an overlap is also needed. To mitigate over estimation, the region of overlapping frequency components are weighted accordingly to the frequency characteristic of the IF filter.
In comparison, the STDFT performs a convolution of the frequency bins with the characteristic of the IF filter in the frequency domain. Thus, each frequency bin already contains the power within the given RBW. To reduce the number of frequency bins and to set them to the wanted frequencies (f_{Ci}), always the maximum value out of a certain frequency range is taken. An overlapping of the regions is not necessary and would even lead to an unintended increase of emission amplitude. Thus the spectrum component at f_{Ci} can be calculated as:

$$S(f_{Ci}) = \max_{f_{Ci-\Delta f/2} < f_{Ci} < f_{Ci-\Delta f/2}} (S(f)) \tag{6.14}$$

The Figure 6.11 shows the spectrum at the time k and the combination of frequency bins.

Detectors

The spectrogram $S[n,k]$ is weighted by detectors resulting in the spectrum of emission $S_D[k]$, which can be directly compared with the emission limits $L_{EME}[k]$ and the measurement results. The implementation is straightforward and can be found for the peak detector, the RMS and the average detector in [86]. In addition, in [87] the modelling of the quasi-peak detector has been presented.

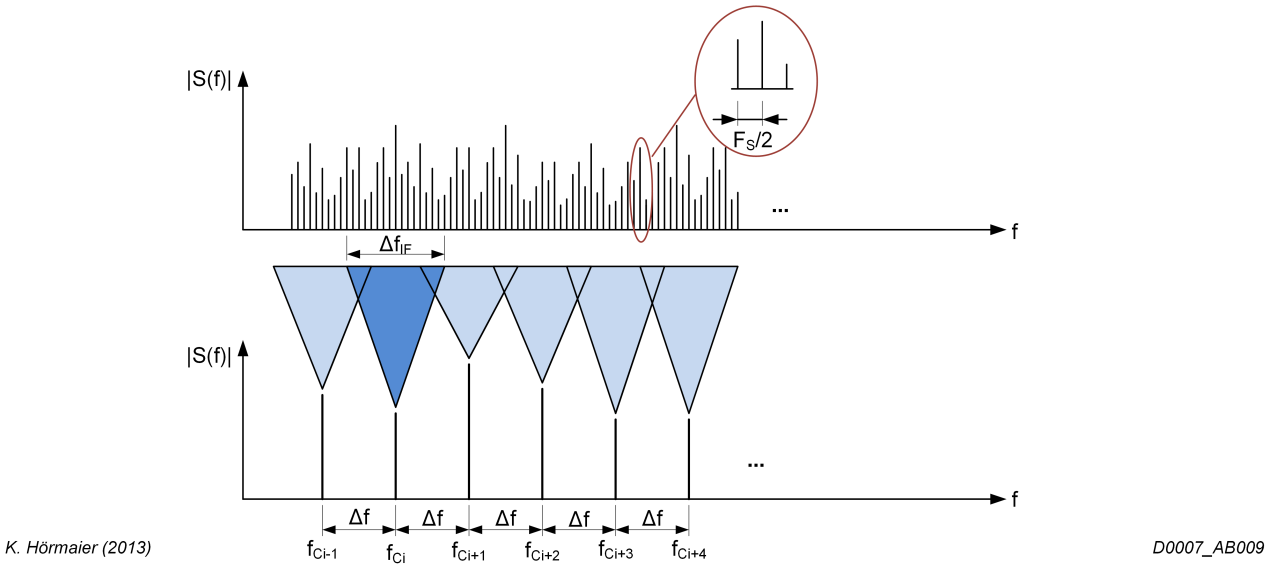


Figure 6.10: To consider the effect of the IF filter and its RBW, frequency bins obtained by the single FFT have to be combined. All bins which are within the span of the RBW have to be summed up, while considering the filter characteristic at the same time.

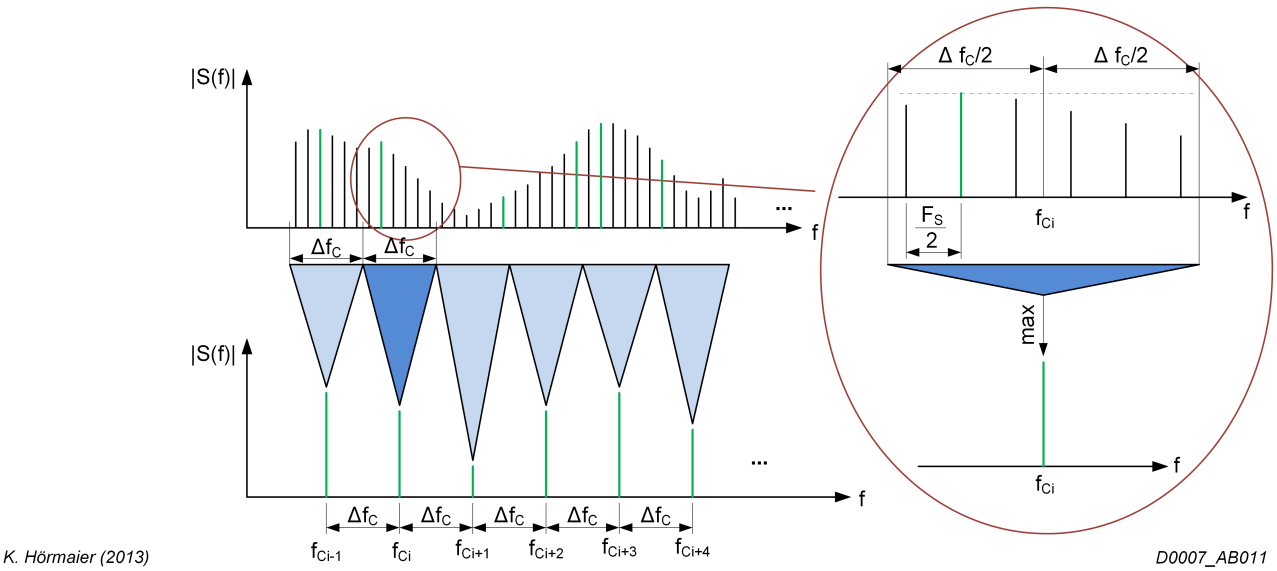


Figure 6.11: For the STDFT for each time slice a data reduction has to be performed. Thereby, the data reduction is performed by selecting the maximum amplitude within the frequency span of Δf_C.

The single FFT result only represents the RMS detector, nevertheless, if the signal is short enough (signal period ¡ 1/RBW), the RMS value equals the peak, average value and the quasi-peak value as well.

6.1.7 Decision FFT vs. STDFT

This section provides guidance when to use the single FFT and when the single FFT cannot be used due to high probability of faulty results.
If simulation execution time is circumstantial, the STDFT shall always be used together with a signal of sufficient long simulation time. The user needs only to consider a few settings leading to a decrease in human failure probability. The appropriate length will be described in detail in Section 6.4.2. In comparison, the single FFT approach bears a high risk of usage errors.
The power, calculated by a single FFT, is the effective power which is distributed over the whole time span. Thus, the FFT result depends on the selected time span. In contrast, the STDFT only requires a minimum selected time span but no further dependency on the selected time span is present. If the single FFT path is taken, due to simulation execution time limitations, significant errors can arise depending on the signal's period. Only the **R**oot **M**ean **S**quare (RMS) detector result is time independent and will deliver correct results. However the peak, quasi-peak and average detector might deliver incorrect results depending on the signal's period. The following example will illustrate the unwanted dependency of the FFT on the signal's period.

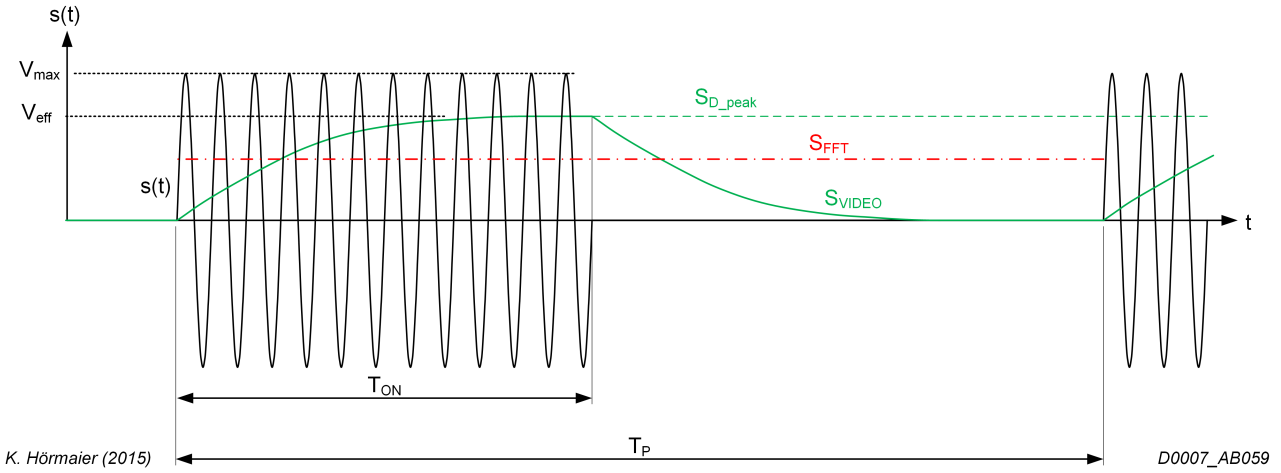


Figure 6.12: A sinusoidal signal is switched on and off repetitively. Due to the long on time, the swept analyser will deliver the effective value of the pure sinusoidal signal but the FFT delivers a value S_{FFT} which is below the peak value S_{D_peak} which depends on the signal's period T_P.

A sinusoidal signal is switched on T_{ON} and off as shown in Figure 6.12. The output of the video filter of the swept analyser reaches the effective value of the sinusoidal signal which is stored in the peak detector ($S_{D\_peak} = V_{eff}$). The peak detector of the swept analyser will remain at this value independently of the signal's period. However, the output value (for the frequency of the sinusoidal signal) decreases with increasing signal's period $S_{FFT} = V_{eff}\frac{T_{ON}}{T_P}$. Only if the signal's period is sufficiently low, so that the IF filter's characteristic can be approximated as linear function the FFT will deliver the correct value. Limiting again the error e_{AMP} of a single FFT requires the limiting the signal period ($T_{P,max}$) according Equation 6.13 to:

$$T_{P,max} = \sqrt{-8\sigma^2 ln\left(e_{AMP/2}\right)} \tag{6.15}$$

Beside the absolute period dependency, the typical commonly known problems have to be mitigated. Applying a FFT on a signal which does not have an integer multiple of the signal period will lead to phantom spectral components which shall be avoided. Thus, the user has to ensure on his own that the extracted time span is an integer multiple of the signal's period. This effect can be reduced by simulating several periods of the signal.

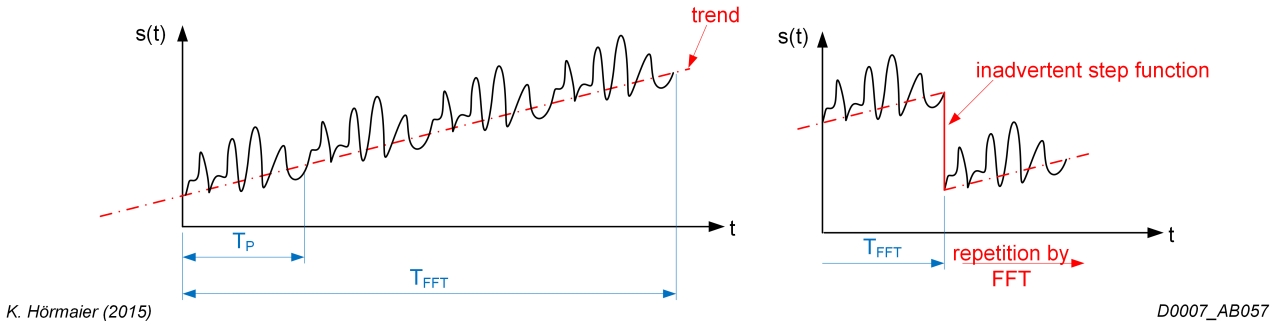


Figure 6.13: If a high frequency signal overlays a low frequency, cutting out some periods can lead to steps (end and start point) is not identical and, therefore, builds a step. This step will lead to phantom broad band emission in the displayed spectrum.

In some cases, the signal of interest is modulated on a lower frequency signal, leading to deviations of the start and end value as shown in Figure 6.13. Thus the FFT, which considers the signal to be repeated infinitely, generates phantom broad band emission. The trend might be corrected by windowing functions such as, Gauss, Butterworth, and so on. But applying these filters on only one period will also distort the spectrum. Thus pre filtering of the signal is only allowed if the number of simulated periods exceeds a certain value depending on the window function. In Figure 6.14 on the left side, the scenario of wrong windowing is shown and on the right side the correct windowing by selecting several periods can be seen.

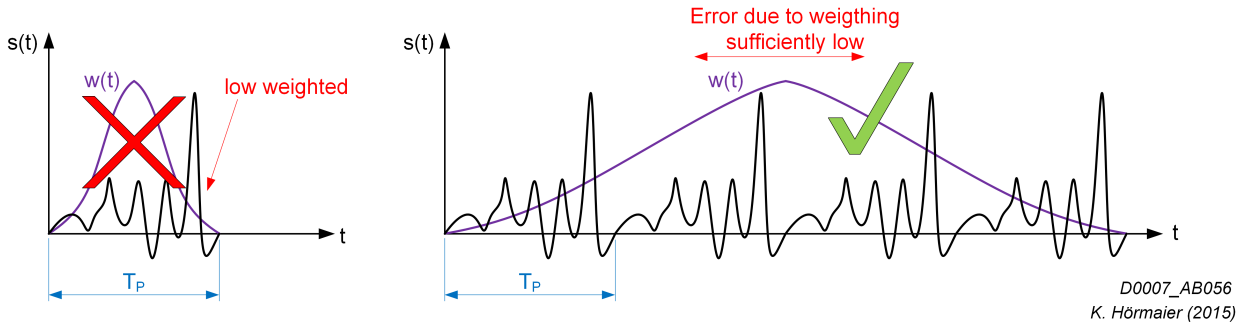


Figure 6.14: Due to the filter characteristic, the left approach would lead to a distort spectrum because the signal outside the center is low weighted by the filter. In contrast, in the right view, one period of the signal is within the center region of the filter and therefore weighted sufficiently accurate.

6.2 Workflow

Figure 6.15 depicts the whole workflow, including modeling, defining the operation modes of the DUT, configuring the simulation, execution of the simulation, post processing of the obtained

signal, and comparing it to the emission limits and finally locating possible emission hot spots.

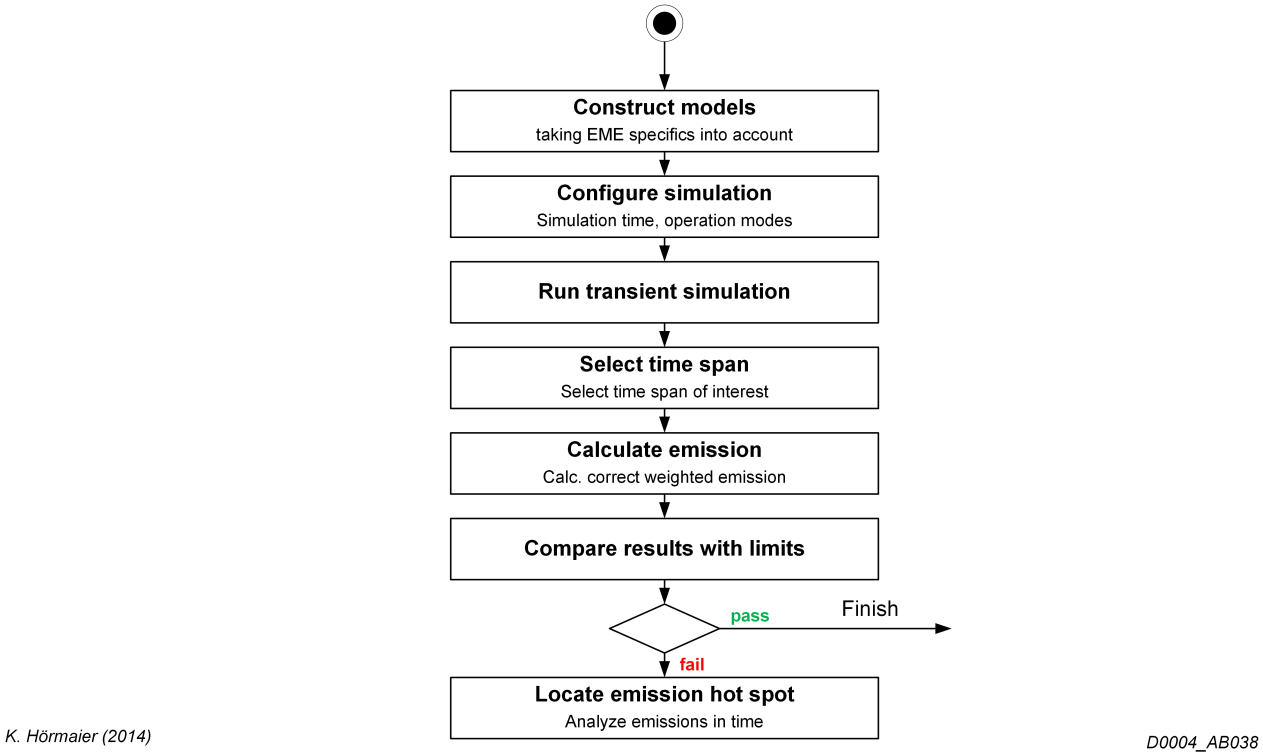


Figure 6.15: Workflow of an EME simulation including all necessary prerequisites.

6.3 Modelling

In order to perform the transient EME simulation three models are needed as shown in Figure 6.16:

- the model of the DUT,
- the application model (including external loads and supplies) and
- the measurement setup model (including impedance controlling networks and the EMI receiver model).

6.3.1 Model of Device Under Test

Emission can be caused by the functionality of the DUT or by parasitic (unintended) physical characteristics. The functionality is generally modelled accurately enough but in contrast the parasitic physical characteristics are inaccurately modelled or even not modelled. Therefore, the DUT has to be modelled including all internal coupling paths which contribute significantly to the overall coupling. The following highly relevant key points provide an overview, but for detailed modeling additional literature, starting from used process technology down to numerical simulation methods, is needed. Especially impedances in common ground connection, high capacitive connections and substrate coupling shall be included. Back annotation can

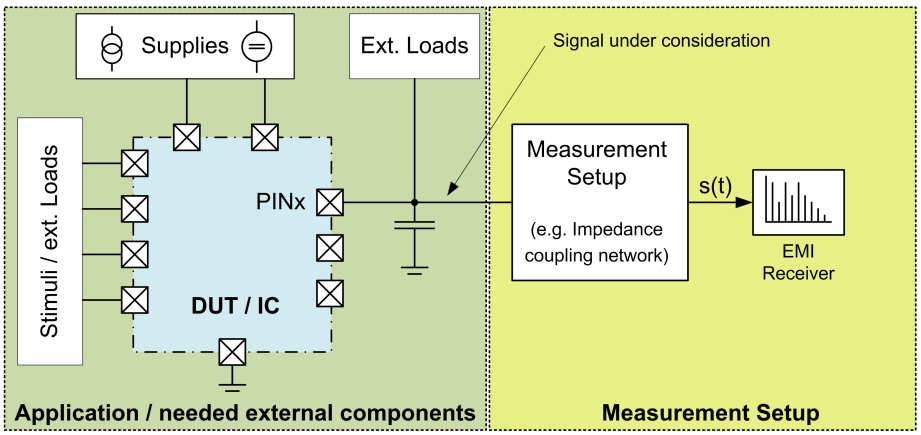


Figure 6.16: Block diagram of the models needed for the EME simulation.

provide a majority of information, which is then added to the schematic.
Constructed models might include ideal sources. Such sources might be used to substitute not yet implemented components or blocks of the DUT or are part of simulation test benches for supply and stimuli generation. Said ideal sources can have a feedback on the emission source leading to an underestimation of the generated emission. In other words, possible emissions are suppressed because the inner impedance of the ideal voltage source is zero. Therefore the ideal sources have to be decoupled as sketched in Figure 6.17. Proper decoupling can be achieved by inserting a serial inductance to the supplies. The inductance defines the impedance in the higher frequency range and does not influence the DC characteristics. As a guide value, the IEC 62132-4 [88] recommends a decoupling impedance, at the frequency range of interest, higher than 400 Ω. Even if the IEC 62132 is a immunity test standard, the proposed value can also be used as a guide value for emission evaluation.

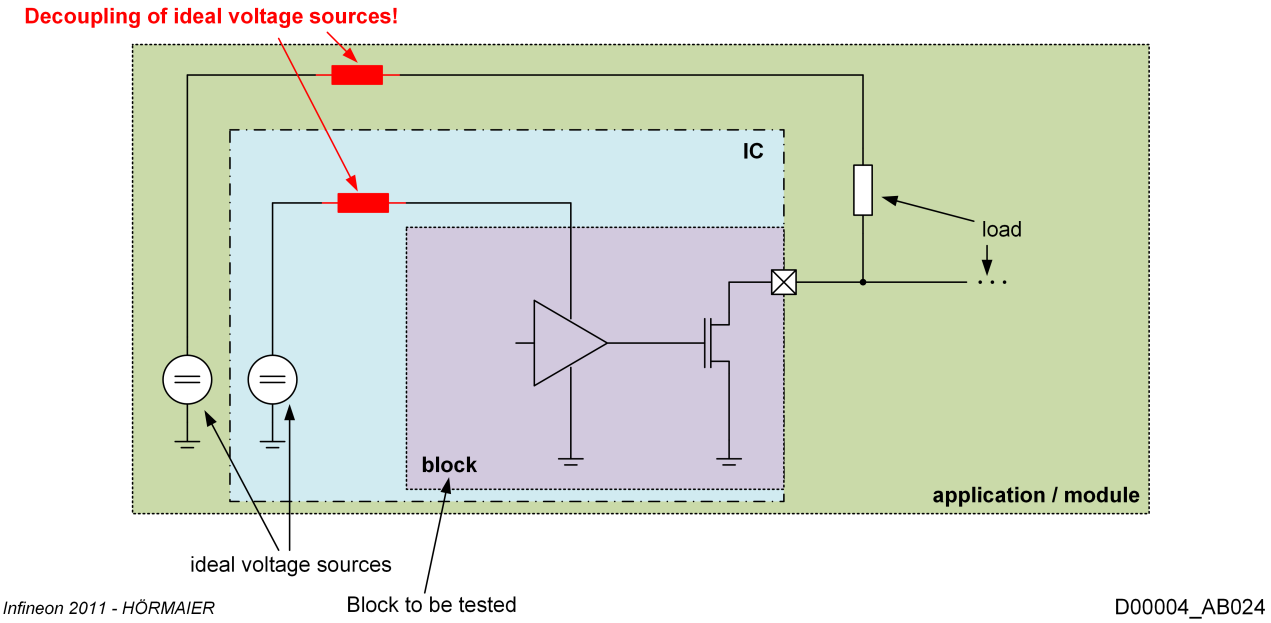


Figure 6.17: All ideal sources have to be decoupled to reduce the risk of underestimating the EME. Decoupling can be realised for example by inserting a serial inductance to the ideal voltage source.

6.3.2 Application Setup Model

The application setup consists of the external components which are mandatory for the operation of the DUT like loads or supplies. The simulation model shall also include the typical load according to the product specification. But attention shall be paid to use the proper equivalent circuit for external components (e.g. RLC equivalent circuit for a capacitor). Ideal components in the external setup model might lead to an underestimation of the evaluated emission and shall thus be decoupled as described in Chapter 6.3.1. If the application circuit is unknown, general recommendations listed in IEC 61967 [4] "*Table 3 – IC pin loading recommendations*" should be followed.

6.3.3 Measurement Setup Model

The measurement setup needs to be modelled as the emission limits are related to a standardized measurement setup. By considering the 150 Ω method required by the IEC 61967-4 [4], two impacting factors exist. The setup itself represents a load connected to the emission source as shown in Figure 6.18. Not considering the measurement network in the analogue simulation will lead to an overestimation of the emission as shown below. The effect can only be neglected if the impedance of the application is much lower than the impedance of the measurement setup $Z_{Source}(f) \ll Z_{Setup}(f)$. In addition, the network can be seen as a voltage divider which reduces the measured voltage. In Figure 6.19 the lower graph shows the attenuation in the frequency range from 150 kHz up to 1 GHz. If not considering the network at 150 kHz, the emission would be overestimated by 23.73 dB.

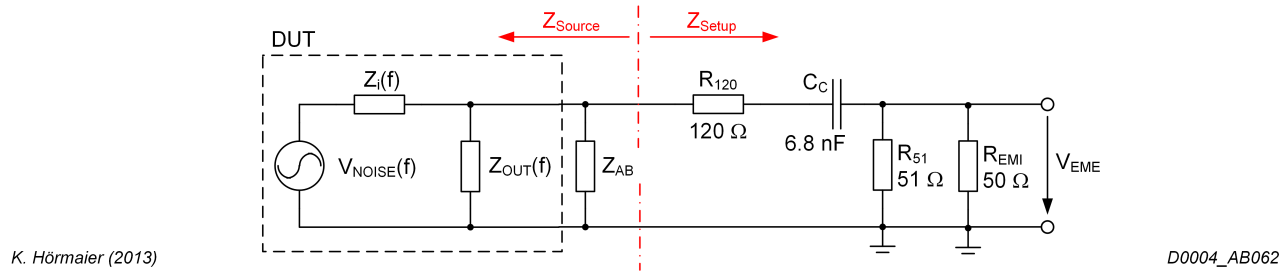


Figure 6.18: The DUT includes the emission source $V_{NOISE}(f)$ with an inner resistance (impedance) $Z_I(f)$ connected to the application board and the measurement setup. The external circuit Z_{Setup} burdens the emission source and therefore reduces the measured emission at the device pin.

The final part of the measurement chain is the EMI receiver, which input impedance has to be included in the measurement. Typically, this input impedance, labeled as R_{EMI} in Figure 6.18, is 50 Ω.

6.4 Simulation settings

As for all simulations, also the EME simulation needs some parameters or signals to be set in advance. Firstly, the signals to activate the different DUT's operation modes have to be defined and secondly the simulation's end time has to be set.

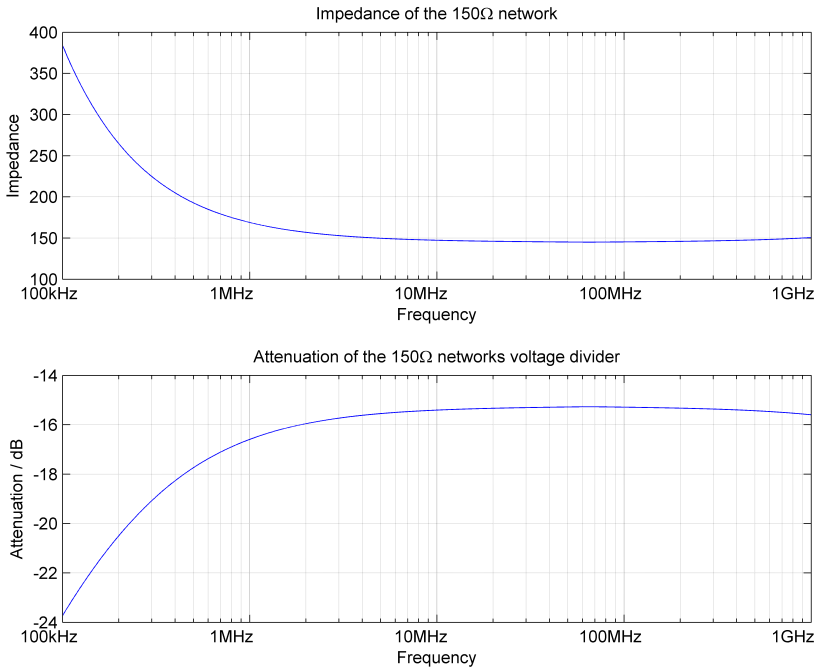


Figure 6.19: Characteristics of the impedance coupling network described by the 150 Ω method [4]. The impedance representing the load of the emission source and the attenuation caused by the voltage divider are plotted.

6.4.1 Operation Modes

The DUT has to be stimulated to activate / trigger implemented functions. These functions / operation modes of the DUT can have a significant influence on the emission. If known, the typical operation profile of the device shall be used. If no operation profile is defined yet, a meaningful profile has to be generated. In order to obtain the supposed emission, all operating modes have to be evaluated. For cycling operation modes the minimum operation repetition period shall be used to obtain the highest emission. Only in some cases, where frequency dependency of the circuit plays a role, the period might be set to the susceptible frequencies.

6.4.2 Simulation Time Consideration

In large mixed signal designs simulation's execution time can become very long and even take up to several weeks. Thus the end time (simulated time) shall be as short as possible. Therefore thoughts about useful simulation time are mandatory. Before starting the transient simulation the simulation time T_{SIM} has to be defined. Considering the signal shown in Figure 6.20 the simulated signal consists of the start up phase followed by continuous operation. So after the start up phase the signal's shape repeats consecutively with the operation period T_P. As we are interested in the emission, only the repetitive part of the signal has to be considered. Not only the operation period T_P but also the window length T_W of the EMI receiver has an influence on the simulation time. For the STDFT the window is shifted over the input signal as shown in Figure 6.6. Due to the fact that the maximum of the window function is at $T_W/2$, a correctly weighted result can only be obtained after $T_W/2$. In other words to get a correct result the maximum of the window function has to be shifted over a complete operation of the signal. As described in Section 6.1.6 a further reduction of time is possible, if an error is allowed. Thus,

the simulation time can be calculated as:

$$T_{SIM} = T_{startup} + \frac{T_W}{2} - \frac{T_{Shift}}{2} + T_P + \frac{T_W}{2} - \frac{T_{Shift}}{2} \tag{6.16}$$

Hereby, $T_{startup}$ is the start up time, T_W is the time length of the window, T_{Shift} is the time shift of the STDFT and T_P is the operation period. The equation can be reduced to:

$$T_{SIM} = T_{startup} + T_W - T_{Shift} + T_P \tag{6.17}$$

It is worth mentioning that $T_W/2$ depends on the band which shall be evaluated. To be precise the lowest band (with the lowest resolution bandwidth) defines the simulation time. Figure 6.21 shows a detailed view of a short operation cycle compared to the window length. The loss of information is illustrated in the regions other than T_P. A detailed explanation of the simulation time consideration can be found in [89].

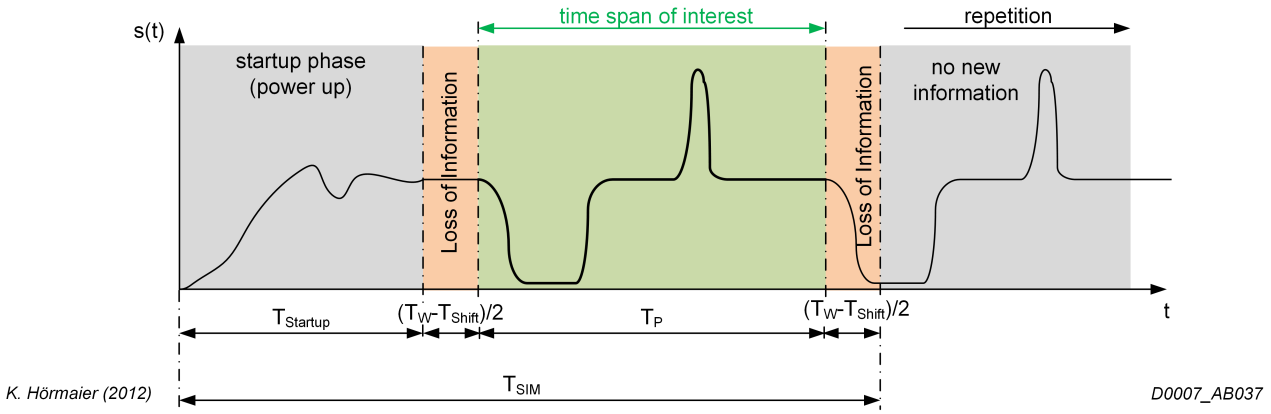


Figure 6.20: Example signal, which is used as the input for the 150 Ω network. The transient simulated signal consists of the start up phase and the continuously repeated operation. For the post processing with the EMI receiver model it has to be considered to take more than the operation cycle so that before and after the time span of interest, signal data is available.

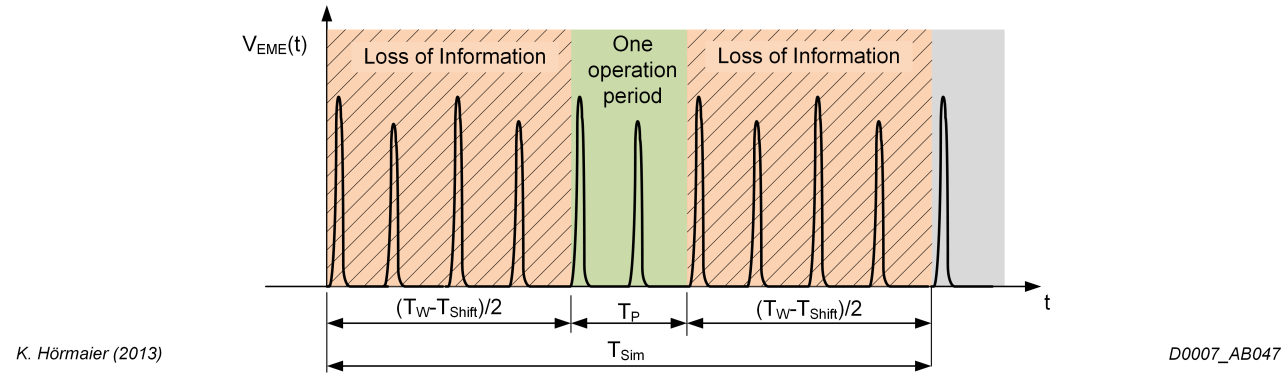


Figure 6.21: Example signal divided into regions where the EMI receiver will deliver highly accurate results and regions of loss of information caused by the window function. For a short operating period compared to the window length several operation periods have to be taken.

Signal Start and Signal End Problem

As previously explained, due to the filter characteristic implemented within the STDFT the signal is low weighted at its start and end. Ideally, the simulation time is increased to include all the signal information but in certain cases the user can decide for reduced simulation's execution time and applies zero padding. First of all expanding the signal with zero values is only useful if the real signal would be zero as well or the real signal would generate only spectral components which are not in the frequency range of the simulated time span. Additionally,

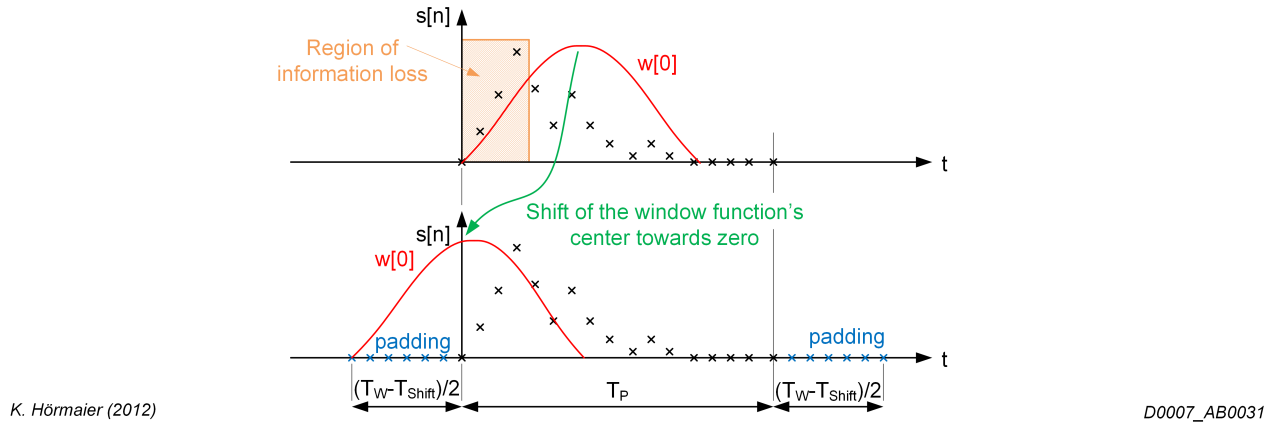


Figure 6.22: To mitigate the loss of information at the signal start and signal end, zero padding can be used extending the signal. Zero values are added before and after the original signal.

the signal has to be approximately zero at the start and the end. In Figure 6.23 different scenarios are plotted. The signal feet to the EMI receiver $s(t)$ is not zero at the start and the end. If zero padding would be applied, at the beginning of the function as well as at the end of the function an unintended step function would be generated, leading to phantom broad band emission displayed in the spectrum. This step exists between the last padded zero value and the start of the simulated signal. At first glance, extending the signal with the first and the last value as shown in the third plot from the top might be a possibility. But, padding with the start and end value does not reflect real behaviour as the derivative (trend) of the signal would be changed, also leading to phantom broad band emission displayed in the spectrum. Thus, the engineer can decide for the reduced simulation time or suppressing phantom broad band emission.

Tighten the Simulation Time

Due to long simulation execution times a reduction of the simulation time shall be targeted. The idea is to reduce intentionally the time between two independent emission generating events without changing the generated emission by taking the EMI receivers IF filter characteristic into account. If two events which are in the typical application separated in time, and the time between the two events is relatively long then the approach is applicable. If between two events as shown in Figure 6.24 no significant emission is generated the latter event can be shifted towards the first event. Thus, all operation modes are covered but the simulation time can be reduced. When are the events independent? The two event can be seen as independent, if the EMI receiver's IF filter output reaches approximately zero after the first event and before the second event occurs. To be able to reduce the simulation time the following conditions have to be fulfilled and the following limitations have to be considered:

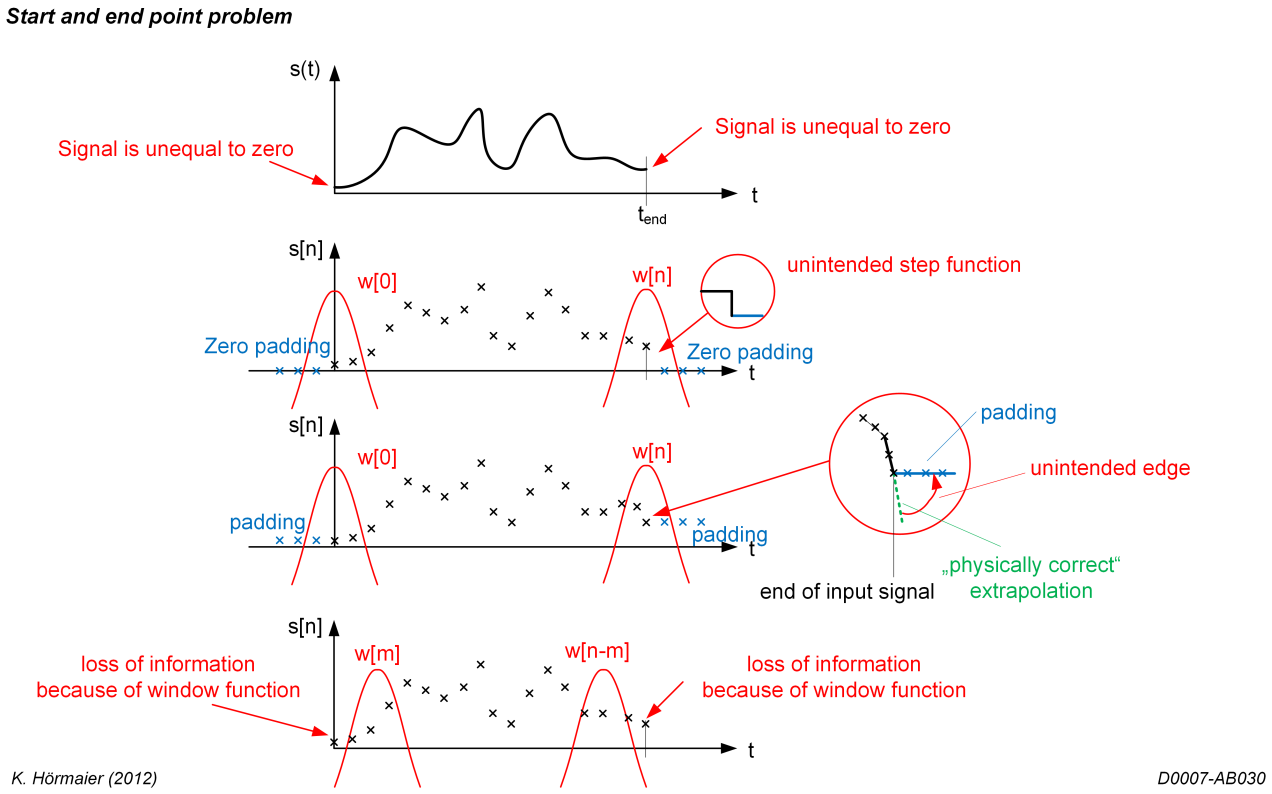


Figure 6.23: Zero padding can introduce severe problems if the signal's start and end do not fulfil certain requirements. The start and the end of the portrayed signal is unequal to zero, leading to unintended step functions generating phantom components in the spectrum.

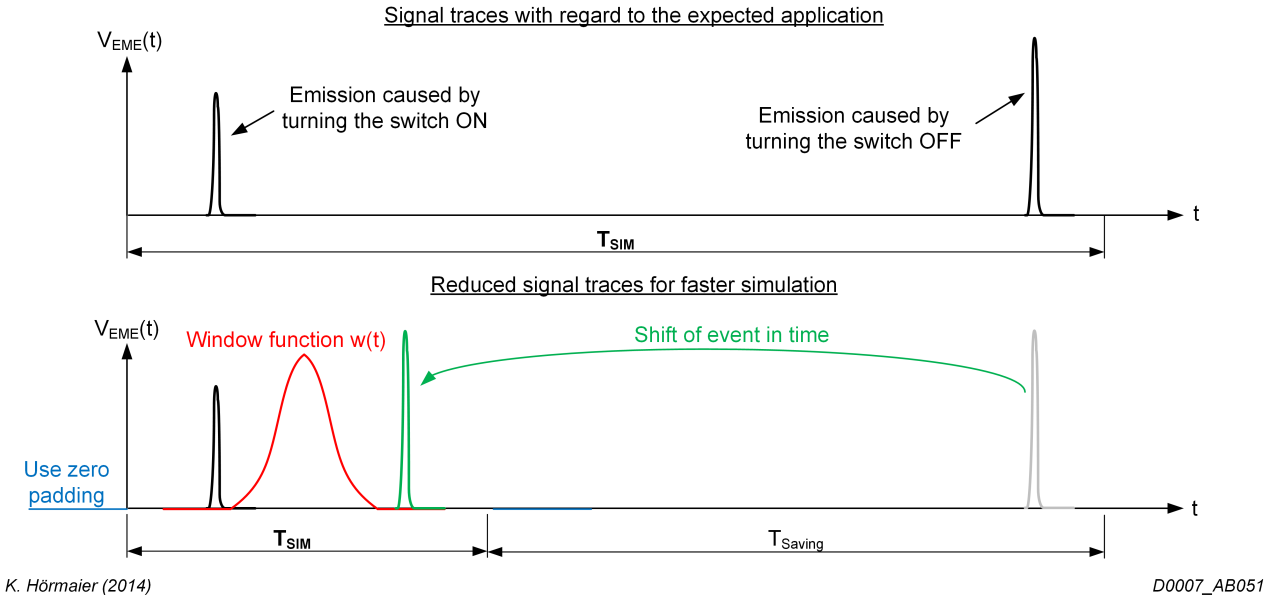
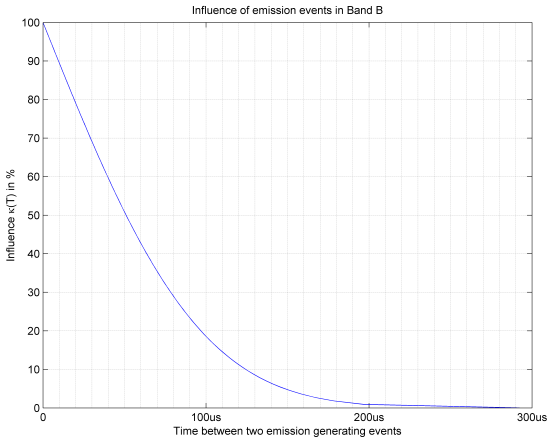
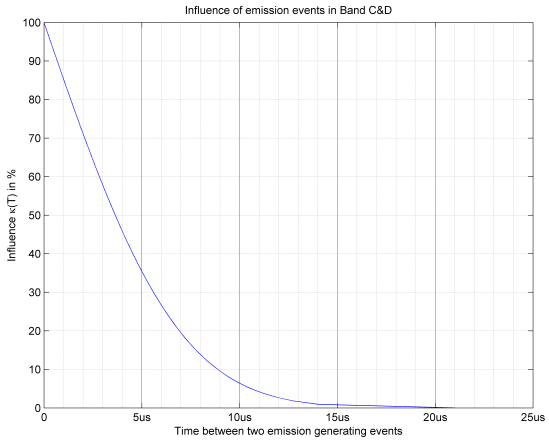


Figure 6.24: By changing the operation profile the simulation execution time can be reduced. The switching events can be brought together up to $1/RBW$ without significantly influencing the generated emission spectrum.



(a) Influence in Band B ($RBW = 9\ kHz$).



(b) Influence in Band C&D ($RBW = 120\ kHz$).

Figure 6.25: Influence of two independent emission-generating events on each other depending on the time between them.

- Only possible for the peak detector
- Only for the STDFT path
- Signal between two events is negligible
- Limited signal period reduction

Unfortunately, only for the peak detector the simulation time can be reduced, for all other detectors the time between the emission-generating events influence the result.
Since the FFT path is already only possible for very short signals this approach cannot be used for the FFT path but for the STDFT path.
In the time between the events which are assumed to generate the emission, no time varying signal generating additional emission shall exist.
The different operation modes or switching events are tightened up and depending on the window and the time between the events an error appears. Events or operation modes which are separated in time more than T_W are independent. Nevertheless, if an error is allowed, a high reduction of simulation time is possible. The worst case influence of two equal events depending on the time between the events can be calculated using Equation 6.18 for $\forall T \in \mathbb{R}^+$, where T is the time between the two independent events and σ is the standard deviation of the IF filter for a given band

$$\kappa(T) = 1 - \int_{-T}^{T} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t}{\sigma}\right)^2} dt \tag{6.18}$$

$$\kappa(T) = 1 - erf\left(\frac{T}{\sigma\sqrt{2}}\right) \tag{6.19}$$

Therefore, in Figure 6.25 the relation between the time between two events and the influence on the emission result is plotted for the Band B and C&D. Obviously the influence is sufficiently small up until approximately $1/RBW$. In Table 6.3 some values for the allowed error due to the shift of independent events are provided.

Table 6.3: Error depended on reduced time between two events.

Maximum allowed error	Time between events Band B	Time between events Band C&D
0.1%	250 µs	18 µs
1%	195 µs	14 µs
5%	150 µs	11 µs
10%	125 µs	9 µs
50%	50 µs	4 µs
75%	25 µs	2 µs

6.5 Interpretation of Simulation Results

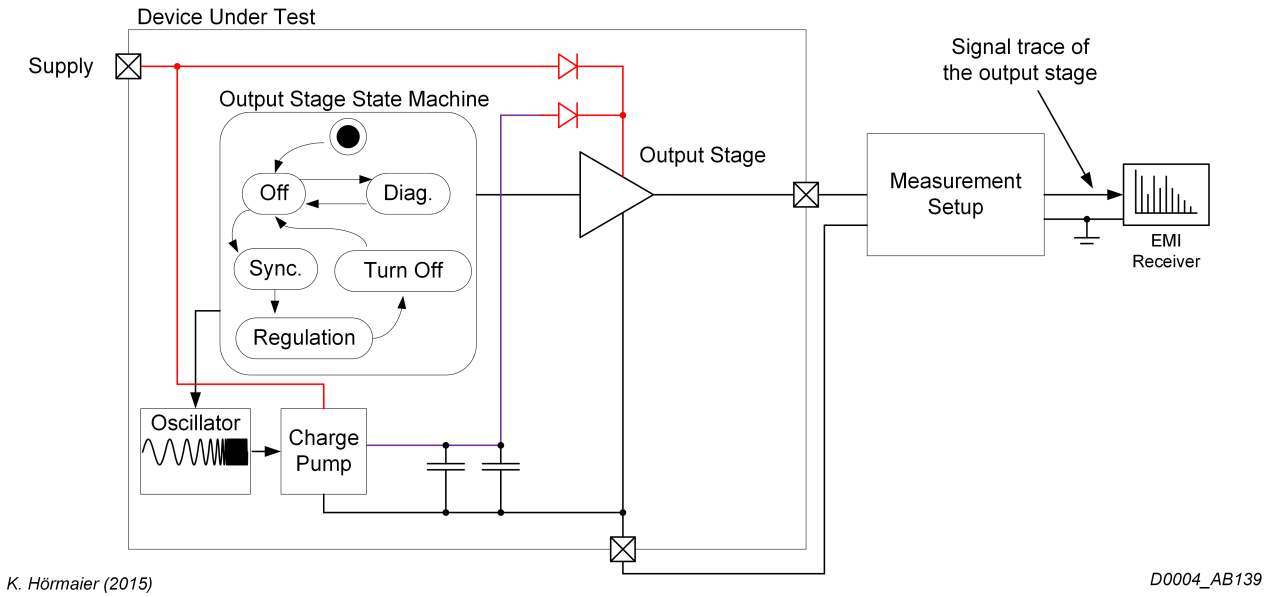


Figure 6.26: Emission measurement example circuit including the DUT. The DUT, in turn, includes an output stage, a charge pump and an oscillator which are controlled by a state machine.

This section will describe an innovative method for supporting designers with the emission root cause analysis. By extracting useful information out of the spectrogram (EMI receiver output) different perspectives are presented to narrow down the source of emission in time domain. A generically exaggerated example, shown in Figure 6.26, shall illustrate the advantages gained using this method. The DUT includes an output stage, charge pump and an oscillator which are controlled by a state machine. The output stage behaves different for the different operation modes illustrated in the sate diagram. Also the charge pump has different modes. In the startup phase, the charge pump frequency is increased starting from 1 MHz to 20 MHz where the operation frequency is reached and the charge pump works in continuous mode with the stable 20 MHz clock. In case the operating voltage is reached, the charge pump is immediately deactivated. The example circuit (DUT) is connected to the measurement setup, measuring the generated emission.

After the transient simulation has finished the simulation result is used as the input for this method. An example for such obtained signals (simulation results) are as shown in Figure 6.27

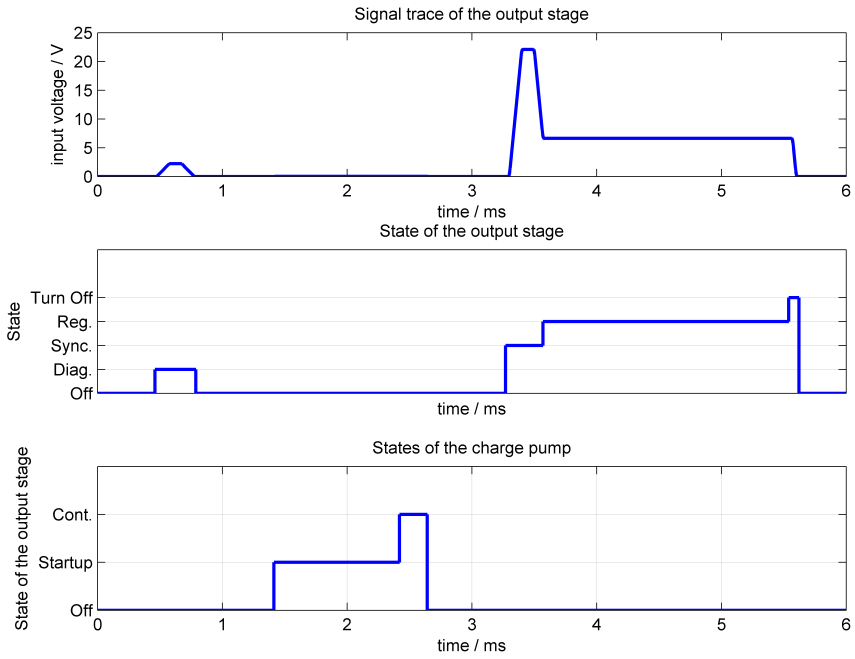


Figure 6.27: Results gained by simulation. The first plot shows the EMI receiver's input signal over time, which is the output stage signal, and the remaining two plots show the corresponding state information of the DUT.

which consist of the driver stage output voltage as well as the actual state information of the driver stage and the charge pump. Thereby, the drive stage output voltage is the signal under consideration which generates the emission. In the next sections the signal is analysed.

6.5.1 Compare results with limits

The emission results calculated by the EMI receiver model can be compared with the specified emission limits shown in Figure 6.28 (the used emission limits are only illustrative). If the emission spectrum stays below the limit (L2) over the whole frequency range, no further work has to be done. But if the limit is violated, the root cause of the emission has to be found and counter measures have to be implemented (e.g., re-design, additional external components). In this example critical violations of the emission limit (L2) in the lower frequency range (150 kHz to 200 kHz) as well as a narrow band interference at 20 MHz is present. An inexperienced designer might assume that the higher pulse (with a voltage up to 20 V) is generating the emission violation in the lower frequency range and that the regulation state (Reg.) is causing the narrow band emission at 20 MHz. On the first glance, the designer might assume that the emission in the lower frequency range is caused by a pulse. Since the first pulse (from 0.5 ms to 0.8 ms) is in its amplitude much lower than the second pulse (from 3.5 ms to 3.8 ms) the designer might assume that the second pulse dominates the emission spectrum. The clock of the regulation loop for the output stage is based on a 20 MHz clock as well. Nevertheless, the regulation algorithms includes a noise shaping mechanism to spread the emission as well. However, the designer might have doubts in the efficiency noise shaping method. The designers assumption can be disproved and results can be visualized using the new method.

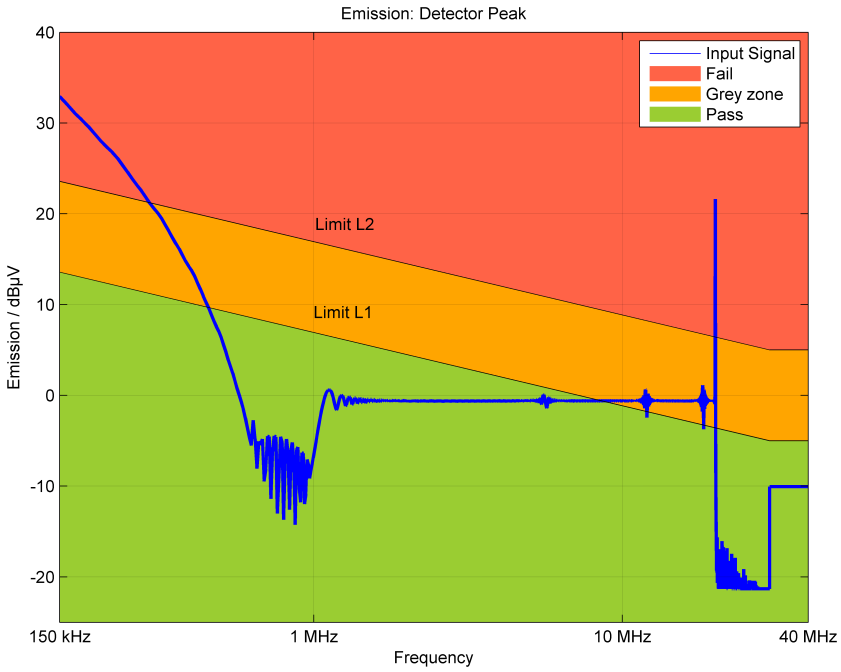


Figure 6.28: Spectrum weighted with the peak detector with the corresponding pass / fail limits.

6.5.2 Locate emission hot spots

Step 1: Step 1 provides an overview. The spectrogram shown in Figure 6.29 shall give the designer an overview of time and frequency. The peak value of emission can directly be seen in the plot, because the spectrogram was calculated considering the RBW of the EMI receiver. To avoid misinterpretation, artifacts of numerical errors have been suppressed. The hiding of these artifacts is done by clipping the spectrogram amplitude Amp_{Calc} to a minimum of -21 dBµV. The following equation is used for clipping:

$$Amp_{Displayed} = \max(-21 dB\mu V | Amp_{Calc}) \tag{6.20}$$

The chosen clipping voltage of -21 dBµV is equivalent to the thermal noise voltage of a 50 Ω resistor at 25 $°C$ with 9 kHz bandwidth. It might still be difficult to orientate oneself in the spectrogram and retrieve accurate information on where improvements can be made.
Step 2: Step 2 goes into detail. Figure 6.30 is the first graph locating the emission sources in time dependency. It helps the user to focus on the points in time where emission is violating the limits. The red areas represent L2 violations and the orange areas violations of L1. In the example one can see that the first smaller pulse generates emissions and violates L2 as well as a signal which occurs at approximately 2.5 ms. This leads to the result that the first (smaller) pulse (from 0.5 ms to 0.8 ms) causes the problem and not the second pulse (from 3.5 ms to 3.8 ms) as assumed before. But it is still unknown what causes the emissions at around 2.5 ms. The next view gives additional information about the bandwidth of the noise signal. Therefore, we define the **V**iol**l**ation **B**and**w**idth (VLBW) which represents the broadness of the generated emission violation. The VLBW can be calculated as follows:

$$VLBW = \sum_{m=1}^{M} \sum_{k=1}^{K_m} \begin{cases} RBW_m & \forall\ A_{m,k} \geq Limit_{m,k} \\ 0 & \forall\ A_{m,k} < Limit_{m,k} \end{cases} \tag{6.21}$$

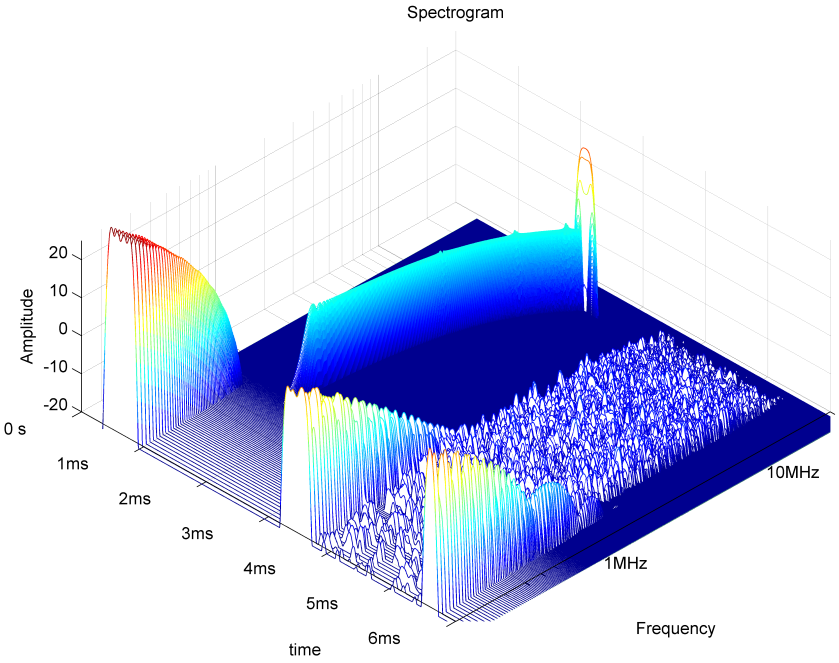


Figure 6.29: The spectrogram shows the generated emission spectrum over time. The peak value of the emission can directly be read from this spectrogram because the filter characteristics of the EMI receiver are included in the calculation.

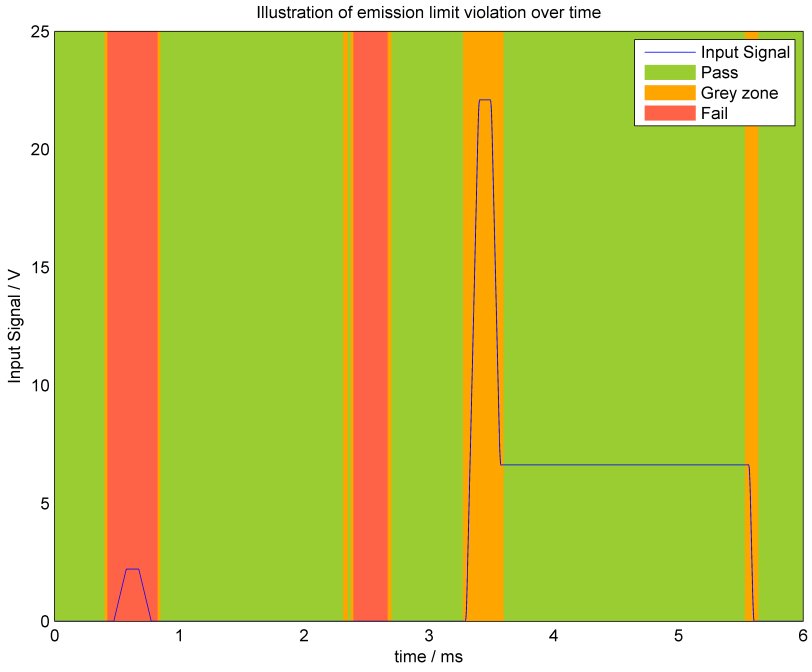


Figure 6.30: Marking the time spans in which the emission limits are violated. The red areas show when L2 is violated and the orange areas show the violation of L1.

were M is the number of calculated bands, K_n is the number of frequency bins in the actual band, RBW_m is the RBW of the corresponding band (e.g. RBW_1=9 kHz, RBW_2=120 kHz), $A_{m,k}$ is the amplitude of emission at the center frequency $f_{Cm,k}$ and $Limit_{m,k}$ the emission limit at the center frequency $f_{Cm,k}$. Figure 6.31 shows the VLBW over time for the two limits (L1, L2) presented in the standard plot. In this example the emission caused at around 2.5 ms has a VLBW of 21 kHz which can be seen as a narrow band interference signal and the first pulse has a VLBW of 117 kHz which indicates the generation of broad band emission. Summarizing the first pulse is causing a broader emission spectrum and the emission at 20 MHz might be generated at around 2.5 ms.

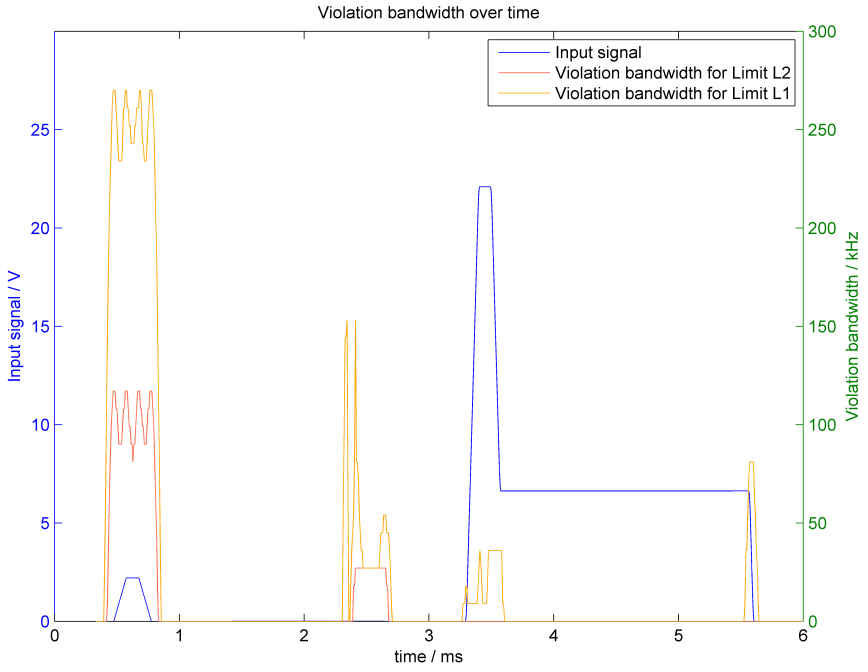


Figure 6.31: Violation bandwidth over time for two limits. The red line shows the violation bandwidth for violation of L2. The orange line shows the violation bandwidth for violation of L1.

In Figure 6.31 the emission seems to be acausal, this is due to an additionally introduced shift of $L/2$ (L is the window length) in the negative time direction. The length has been chosen so that the emission results coincide with the corresponding transition of the input signal. The shift of $L/2$ is due to the lowest attenuation of the windowing function at $L/2$. In this context it shall be remembered that a spectrum can only exist for a time span and not for a point in time. Although it is not correct, in the following sections the term point in time for the time span covered by the window function, has been used. It refers to the time when the window amplitude has its maximum.

Step 3: With the presented graphs designers should already have a good overview of the problems, but in step 3 with two introduced views a more detailed look into the signal is possible. With the

- emission at a fixed time span (constant time) and
- emission over time at a certain frequency (constant frequency)

the user can “zoom into” the spectrogram.

Constant frequency view: With this view, the assumption that the emission at 20 MHz is generated at around 2.5 ms can be proven. The constant frequency view fits well because “narrow” band emissions can be visualized easily. By fixing the frequency to 20 MHz the plot shown in Figure 6.32 can be obtained. The emission violation at 20 MHz (see Figure 6.32) is clearly in the range from 2.3 ms and 2.8 ms. To answer the question which function / block generates the emission additional signals are given in Figure 6.33. As indicated, the active function in this time range is the charge pump, operating in its continuous mode (see Figure 6.33 bottom plot). For easy understanding in this example a sinusoidal signal in the range of several µV has been chosen to represent the charge pump’s behaviour. Thus the charge pump has to be redesigned or counter measures have to be applied to lower the emission. Possible improvement can be achieved e.g. by introducing spread spectrum methods. To underline the features of this view, Figure 6.34 shows the emission at the fixed frequency of 150 kHz.
In this view a weighted spectrum (weighted by the detectors) can additionally be displayed. Thereby the detector output over time for a fixed frequency can be plotted. This can help the designer’s understanding the effects of different detectors.

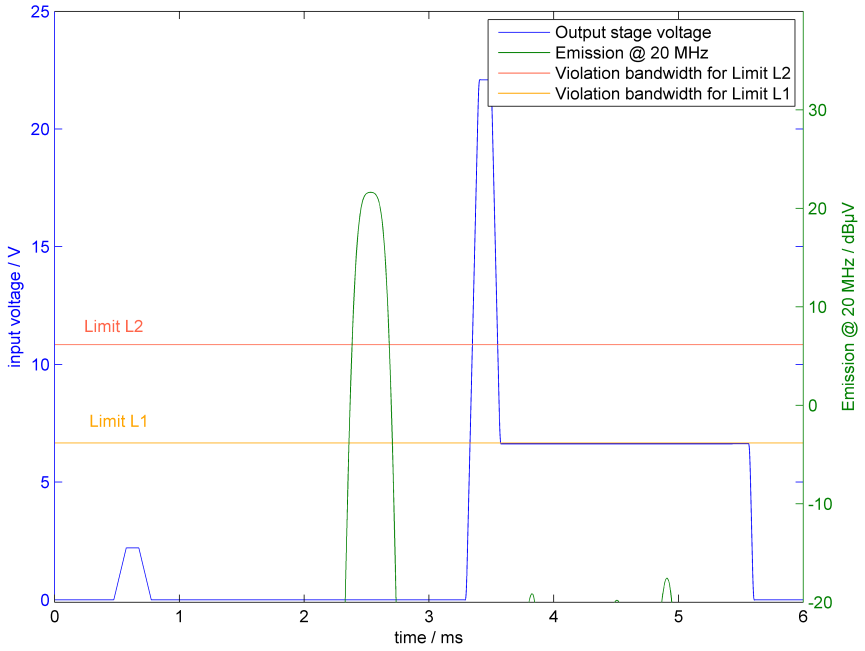


Figure 6.32: The emission over time for frequency components at 20 MHz are plotted. The emission limit violation at 20 MHz is generated in the range from 2.3 ms to 2.8 ms.

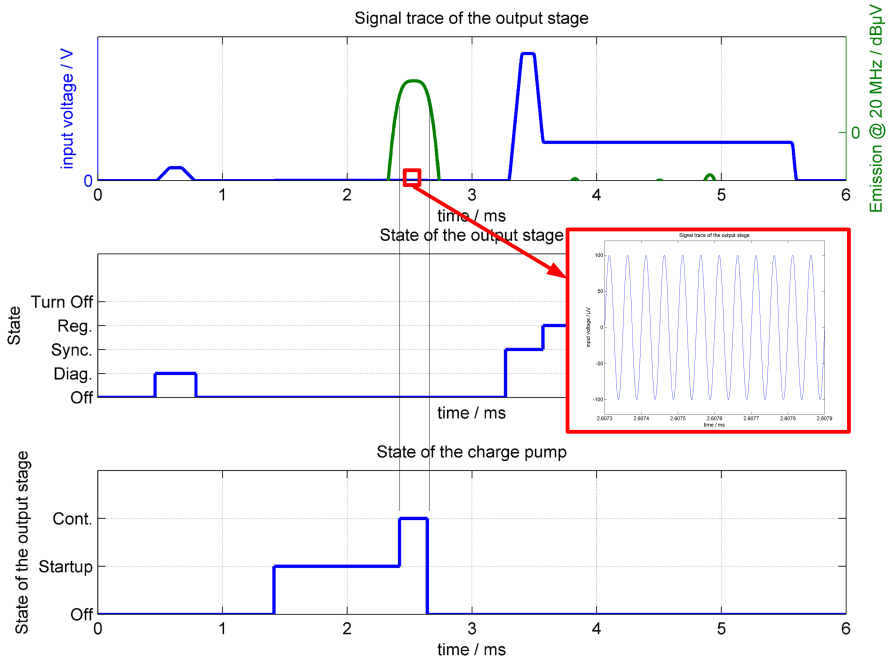


Figure 6.33: Emission at 20 MHz over time. The emissions are generated by the charge pump at around 2.5 ms.

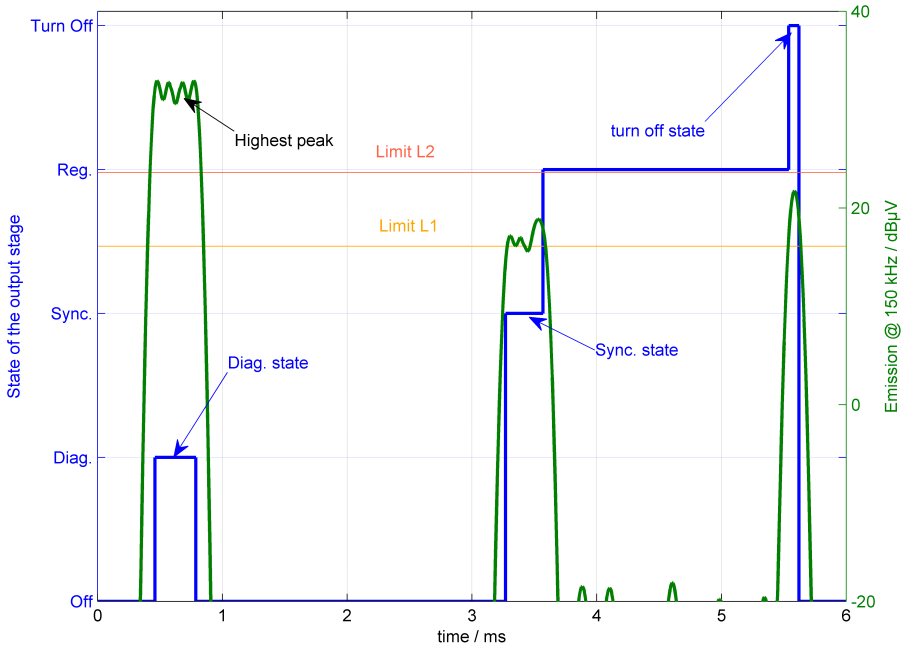


Figure 6.34: The emission over time for frequency components at 150 kHz are plotted. In the diag. state the dominant part of the peak detector emissions is generated, violating L2. In sync. state and turn off state emissions violating L1 are generated.

Constant time view: Now the remaining problem, the broad band emission in the lower frequency range, can be targeted. This can be done by using the constant time view which allows plotting emission generated at a chosen point in time. According to Figure 6.31 the broad band emission is caused by the first pulse (a high VLBW present). To complete the whole picture, the points in time where emissions at 150 kHz were present (see Figure 6.34) shall be also analysed. So the focus is on the three states (diag., sync. and turn off) with higher emission in the lower frequency range. Figure 6.35 shows the driver stage output signal with the state information and overlays it with the window function at the three center times (0.5 ms, 3.6 ms, 5.6 ms). The corresponding spectra and the peak detector results are potted in Figure 6.36. As assumed the emission generated at 0.5 ms dominates the emission spectrum in the lower frequency range and is therefore in the lower frequency range identical with the emission spectrum of Figure 6.28. On the other hand the plot shows if the first pulse is mitigated, the emission will not be below the violet curve (emission at 5.6 ms).

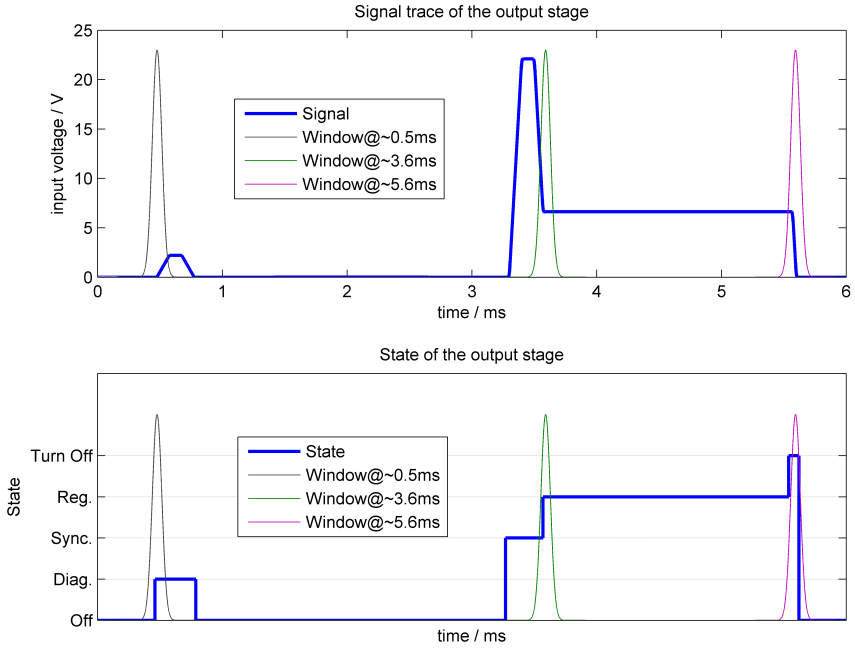


Figure 6.35: The driver output stage signal with the windowing function used for processing the spectrum. The window function for three different time spans is given.

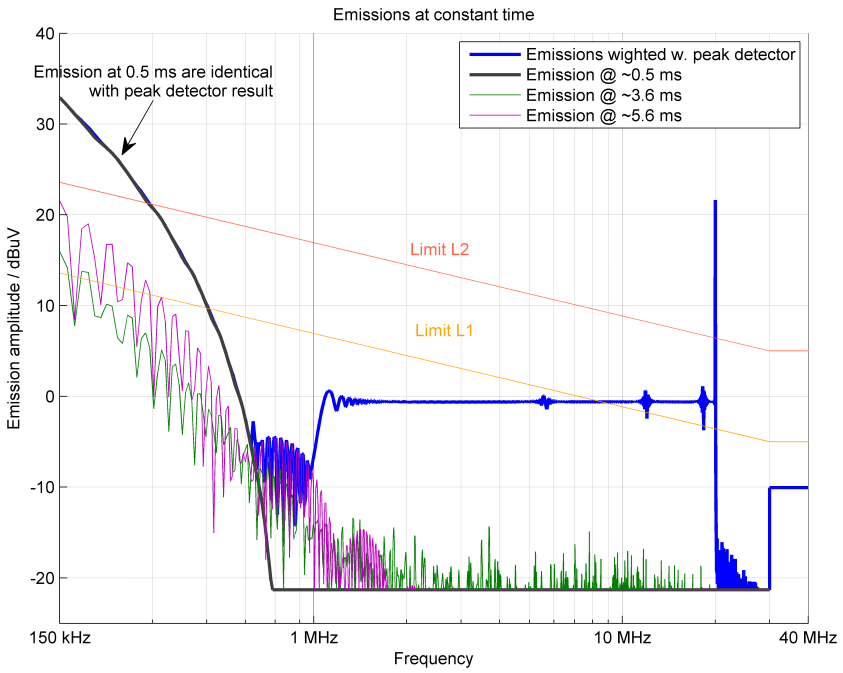


Figure 6.36: Spectrum at certain time span (t=const.). The emission generated at 0.5 ms, 3.6 ms and 5.6 ms are displayed. The emission in the low frequency band generated at 0.5 ms is dominating the peak detector result and is causing the violation of L2.

The previously gathered information are summarized and plotted in Figure 6.37, showing the spectrum of the signal, weighted by the peak detector (see also Figure 6.28 as reference). The spectrum can be separated into six different regions (a to f), as shown in Figure 6.37. The first region (a) is dominated by the diagnostic mode of the output stage. In the second region (b), the emissions caused during the sync pulse phase defines the peak value. The region of constant emission (c) is caused by the linear increasing frequency of the charge pump. At 20 MHz (region d), the constant operation of the charge pump generates the narrow band emission. Region (e) is dominated by broad band emission generated during the shut off of the charge pump. In the last part (f) of the spectrum the generated emissions are below the virtual noise floor and therefore clipped to the virtual noise floor.

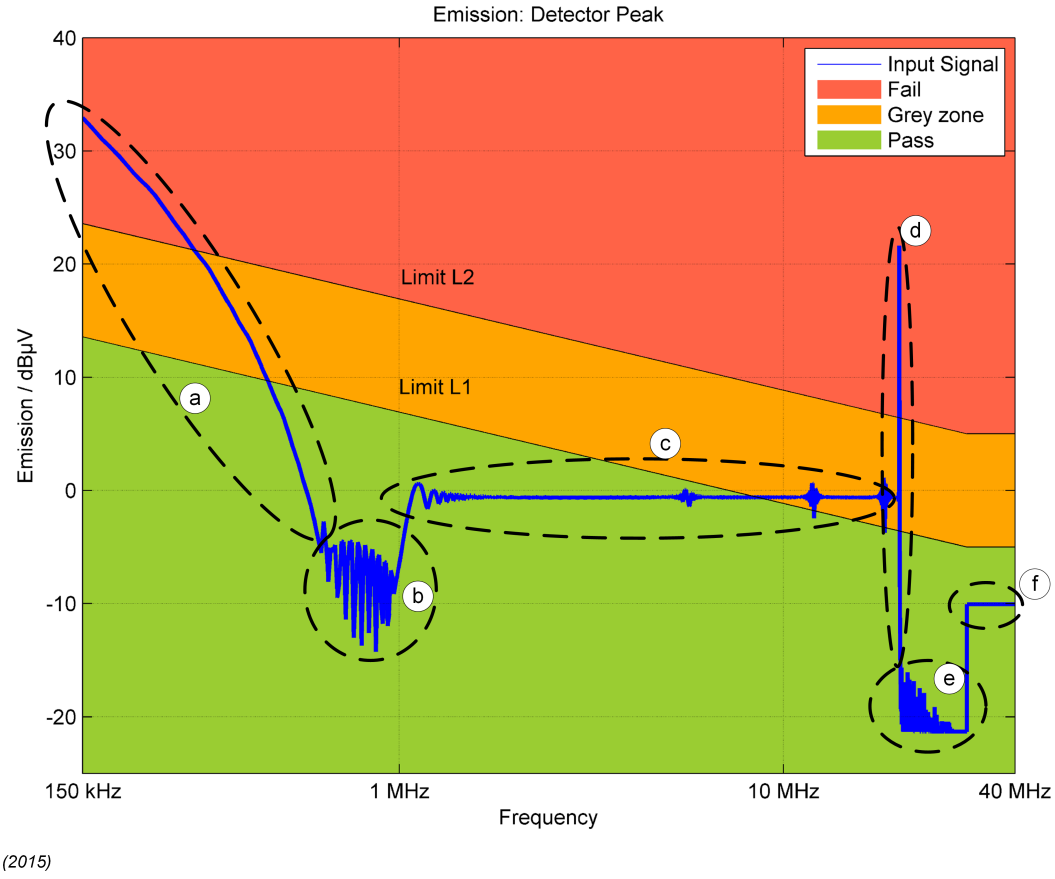


Figure 6.37: Overview of the peak detector weighted spectrum's different ranges. All the ranges are dominated by a certain emission generating mechanism.

An analyser tool was developed based on the methods described above which supports this process. In Figure 6.38 the "Zoom Viewer" interface of the analyser is presented. In this diagram the upper left graph shows the input signal as well as possible other signals which help the user to orientate in time (e.g. an enable signal or the current consumption can be plotted). Additionally, the characteristic of the IF filter (windowing function) is displayed. This window shows the user which time span has been used for the spectrum calculation shown in the bottom left graph. By clicking into the left top graph the corresponding spectrum of this time span will immediately be displayed below. On the top right side, the spectrum weighted with the selected detector is shown. Also the selected frequency point is shown. On the bottom right side, the emission over time weighted by the selected detector is given.

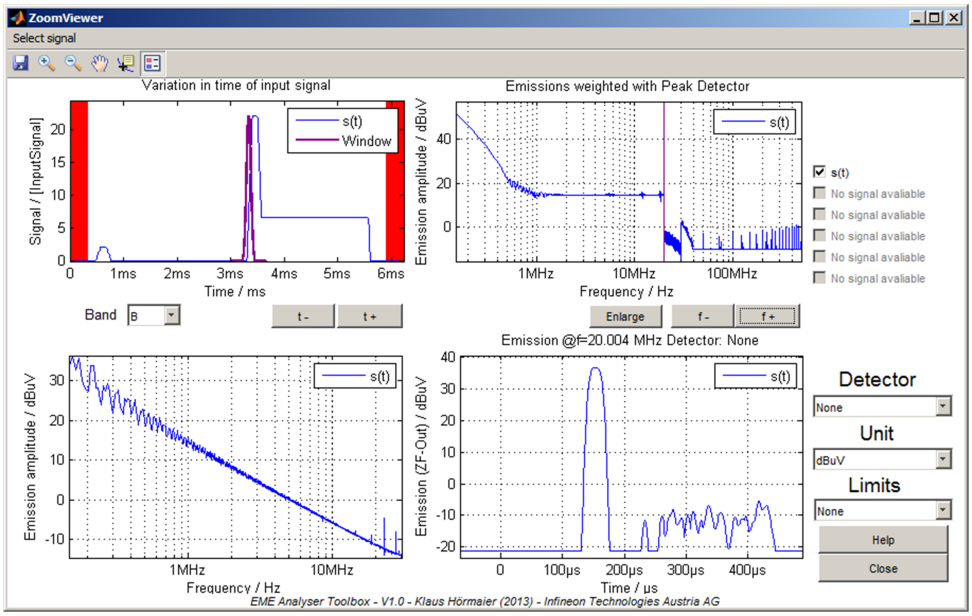


Figure 6.38: One screen shot of the realized EMI Analyzer in "ZoomViewer" mode. In this mode the frequency and time can be fixed and the corresponding spectrum as well as the corresponding variation in time can be displayed.

Chapter 7

Conclusion and Outlook

The presented thesis focuses on a smooth integration of electromagnetic compatibility into the standard conform functional safety process. Therefore, a systematic approach starting with the system / architectural development and ending with quantitative data for fault metrics and failure rates has been introduced. In the first stage, the built victim system has to be analysed and the links between the victim's architectural elements and the victim's elicited so-called injection points have to be established. In the next step the robustness of the victim to electromagnetic interference injected into injection points has to be characterised. The previously obtained information enables to construct the fault tree including electromagnetic events.
In the second stage, the quantitative information regarding electromagnetic failure modes has to be elicited. Therefore, electromagnetic interference (EMI) sources classified as originated by the electromagnetic environment and originated by components' failures. The EMI originated by the environment is permissible and therefore its probability of appearance is rated as 1. In comparison, the EMI caused by a component's failures appears with the probability of the component's failure rate. Since the EMI characteristic changes due to the coupling between the source and the victim system, a transformation of the characterized EMI has to be performed. The transformation EMI characteristic is compared with the robustness of the victim system. If the system's robustness is below the coupled EMI a new failure with the failure rate of the component's failure rate can be added to the victim. This approach allows treating electromagnetic events as fault condition. The main advantage bases on the fact that the victim's required robustness regarding EMC depends on its ASIL (or SIL) rating and therefore the robustness can differ with defined boundaries depending on the safety criticality. Thus, failures due to electromagnetic interference are in principle permitted, but limited by their probability of occurrence. Unnecessary complexity increase due to needless introduction of EMI countermeasures can be reduced, which leads to an improved overall reliability. It allows the optimization of the victim system's reliability taking EMI also into account.
The approach builds upon the knowledge of the failure modes of the components assembled in a vehicle. To be able to characterise the emitted emission in an early development phase, simulations obtaining the possible emissions caused by the component in case of faults shall be used. Firstly a fault has to be injected into the component followed by the evaluation of the generated emission. To limit the effort needed for the emission-simulation, efficient and reproduceable methods were needed. Thus in last part a guideline on how to efficiently simulate the permissible emissions has been provided. The proposed guideline has also taken advantage of reusing existing test and measurement methods because simulation results can better be validated by measurements if they are defined.

With the proposed workflow EMI has been treated as environmental condition and as fault, providing failure rates. This further allows quantitative analysing EMI caused malfunctions and optimizing the system regarding electromagnetic interference.
The systematic and consistent treatment of EMI still remains in its beginning. Extracting and transforming of the electromagnetic events have to be targeted for further research. Also the characterization of systems in case of malfunctions has to be prompted, which has to be driven by the OEMs. Another field of research should target algorithm development which characterize faults or assign them to a standardized electromagnetic failure mode. This might also lead to an enhancement of the EMI receiver model by introducing novel detectors which fit better to the victims' failure models.
Concluding this thesis built the basis for the quantitative analysis of faults, originated by electromagnetic events, in the context of vehicle level.

Abbreviations

ASIL **A**utomotive **S**afety **I**ntegrity **L**evel

CCDF **C**omplementary **C**umulative **D**istribution **f**unction

CDF **C**umulative **D**istribution **F**unction

DFA **D**ependent **F**ailure **A**nalysis

DFT **D**iscrete **F**ourier **T**ransformation

DFTA **D**ependency **F**ault **T**ree **A**nalysis

DPI **D**irect **P**ower **I**njection

DUT **D**evice **U**nder **T**est

E/E **E**lectrical and **E**lectronic

E/E/PES **E**lectrical/**E**lectronic and **P**rogrammable **E**lectronic **S**ystems

ECU **E**lectronic **C**ontrol **U**nit

EM **e**lectro**m**agnetic

EMC **e**lectro**m**agnetic **c**ompatibility

EME **e**lectro**m**agnetic **e**mission

EMF **e**lectro**m**agnetic **f**ault

EMFM **e**lectro**m**agnetic **f**ailure **m**ode

EMI **e**lectro**m**agnetic **i**nterference

FFT **F**ast **F**ourier **T**ransformation

FIT **F**ailure **I**n **T**ime

FM **F**ailure **M**ode

FMD **F**ailure **M**ode **D**istribution

FMEA **F**ailure **M**ode and **E**ffects **A**nalysis

FS **F**unctional **S**afety

FTA **F**ault **T**ree **A**nalysis

FTTI **F**ault **T**olerant **T**ime **I**nterval

GUI **G**raphical **U**ser **I**nterface

HARA **H**azard **A**nalysis and **R**isk **A**ssessment

IC **I**ntegrated **C**ircuit

IF **I**ntermediate **F**requency

IP **I**njection **P**oint

LIN **L**ocal **I**nterconnect **N**etwork

OEB **O**rdinary **E**nvironmental **B**oundary

OEM **O**riginal **E**quipment **M**anufacturer

PCB **P**rinted **C**ircuit **B**oard

pdf **P**robability **D**ensity **F**unction

RFI **R**adio **F**requency **I**nterference

RBW **R**esolution **B**and **W**idth

RMS **R**oot **M**ean **S**quare

SIL **S**afety **I**ntegrity **L**evel

STDFT **S**hort **T**ime **D**iscrete **F**ourier **T**ransformation

SOA **S**afe **O**perating **A**rea

SEMFM **S**tandardized **e**lectro**m**agnetic **F**ailure **M**ode

SUT **S**ystem **U**nder **T**est

VLBW **V**io**l**ation **B**and**w**idth

Bibliography

[1] International Standard Organization (ISO), *ISO 26262 - Road Vehicles - Functional Safety, First edition.* 2011-11-15.

[2] International Electrotechnical Commission (IEC), *IEC61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, First edition.* 12 1998.

[3] National Highway Traffic Safety Administration, "Inadvertent Air Bag Deployment." Online http://www.nhtsa.gov/, 04 2015.

[4] International Electrotechnical Commission (IEC), *IEC61967 - Integrated circuits - Measurement of electromagnetic emissions, 150 kHz to 1 GHz.* 1.0 ed., 2002-03-12.

[5] International Electrotechnical Commission (IEC), *IEC61000 - Electromagnetic compatibility (EMC).* 2.0 ed., 2008-11-27.

[6] Jäkel, B., "Electromagnetic environments - Phenomena, classification, compatibility and immunity levels," *IEEE EUROCON 2009 St.-Petersburg, Russia*, 18-23 May 2009.

[7] Fengying Ma, "Wavelet analysis applied in measurement of coal mining underground EMI and design of filter," in *Automation and Logistics, 2008. ICAL 2008. IEEE International Conference on*, pp. 2691–2695, Sept 2008.

[8] Wilwert, C.; Simonot-Lion, F.; Yeqiong Song; Simonot, F., "Quantitative evaluation of the safety of X-by-Wire architecture subject to EMI perturbations," in *Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on*, vol. 1, pp. 8 pp.–762, Sept 2005.

[9] Andersen, P., "An overview of automotive EMC standards," in *Electromagnetic Compatibility, 2006. EMC 2006. 2006 IEEE International Symposium on*, vol. 3, (Portland, OR, USA), pp. 812–816, Aug 2006.

[10] Fiori, F.; Musolino, F., "Comparison of ic conducted emission measurement methods," *Instrumentation and Measurement, IEEE Transactions on*, vol. 52, pp. 839 – 845, june 2003.

[11] Späth, R., "Elektrische Anforderungen für Fahrzeugkomponenten in 12, 24 und 48V Boardnetzen - Herausforderungen & Lösungen," in *13. EMV-Fachtagung - OVE-Schriftenreihe Nr. 79*, OVE - Österreichischer Verband für Elektrotechnik, 2015. 978-3-85133-085-4.

[12] Musolino, F.; Fiori, F., "Modeling the IEC 61000-4-4 EFT Injection Clamp," vol. 50, pp. 869–875, Nov 2008.

[13] C. P. N. Gallo, D.; Landi, "Experimental evaluation of conducted emissions by variable-speed drives under variable operating conditions," *Instrumentation and Measurement, IEEE Transactions on*, vol. 57, pp. 1350 –1356, july 2008.

[14] Baufreton, Ph; Blanquart, JP; Boulanger, JL; Delseny, H; Derrien, JC; Gassino, J; Ladier, G; Ledinot, E; Leeman, M; Quéré, P, "Multi-domain comparison of safety standards," in *Proceedings of the 5th International Conference on Embedded Real Time Software and Systems (ERTS2), Toulouse, France*, 2010.

[15] Papadopoulos, Y.; Maruhn, M., "Model-based synthesis of fault trees from Matlab-Simulink models," in *Dependable Systems and Networks, 2001. DSN 2001. International Conference on*, pp. 77 –82, july 2001.

[16] Hussain, T.; Eschbach, R., "Automated fault tree generation and risk-based testing of networked automation systems," in *Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on*, pp. 1 –8, sept. 2010.

[17] Vargas, F.; Cavalcante, D.L.; Gatti, E.; Prestes, D.; Lupi, D., "On the proposition of an EMI-based fault injection approach," in *On-Line Testing Symposium, 2005. IOLTS 2005. 11th IEEE International*, pp. 207 – 208, july 2005.

[18] Meixner, A.; Maly, W., "Fault modeling for the testing of mixed integrated circuits," in *Test Conference, 1991, Proceedings., International*, p. 564, oct 1991.

[19] International Electrotechnical Commission (IEC), *IEC61000-1-2 Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*. International Electrotechnical Commission (IEC), 2008.

[20] Ogunsola, A., "EMC and functional safety requirements for integrated electronics systems," in *Electronics System-Integration Technology Conference, 2008. ESTC 2008. 2nd*, pp. 69–74, Sept 2008.

[21] Ogunsola, A., "EMC and Functional Safety requirements - Railway signalling applications," in *EMC in Railways, 2009 IET Seminar on*, pp. 1–8, Feb 2009.

[22] Saitou, H.; Demachi, K., "EMC consideration of safety system," in *SICE, 2007 Annual Conference*, pp. 2906–2909, Sept 2007.

[23] Nelson, J.J.; Taylor, W.; Kado, R., "Impact on EMC for electrical powertrains with respect to functional safety: ISO 26262," in *Electric Vehicle Conference (IEVC), 2012 IEEE International*, pp. 1–7, March 2012.

[24] Armstrong, K., "Why EMC immunity testing is inadequate for functional safety," in *Electromagnetic Compatibility, 2004. EMC 2004. 2004 InternationalSymposium on*, vol. 1, pp. 145–149 vol.1, Aug 2004.

[25] Armstrong, K., "Specifying lifecycle electromagnetic and physical environments - to help design and test for EMC for functional safety," in *Electromagnetic Compatibility, 2005. EMC 2005. 2005 International Symposium on*, vol. 2, pp. 495–500 Vol. 2, Aug 2005.

[26] Armstrong, K., "Validation, verification and immunity testing techniques for EMC for functional safety," in *Electromagnetic Compatibility, 2007. EMC 2007. IEEE International Symposium on*, pp. 1–6, July 2007.

[27] Armstrong, K., "EMC for the functional safety of automobiles why EMC testing is insufficient, and what is necessary," in *Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium on*, pp. –, Aug 2008.

[28] Garcia, E., "Statistics use for radiated high frequency failures," in *Electromagnetic Compatibility (EMC), 2010 IEEE International Symposium on*, pp. 147–152, July 2010.

[29] Helmers, S.; Gronwald, F., "Regelbasierte EMV Bewerung von Fehlerzuständen in Systemen," in *Electromagnetische Verträglichkeit 2012 Messe Düsseldorf*, 2012.

[30] Audone, B.; Amisano, F., "A new approach to immunity testing," in *Electromagnetic Compatibility - EMC Europe, 2008 International Symposium on*, pp. 1–6, Sept 2008.

[31] Baumgart, A; Hoermaier, K; Deuter, G;, "Model-based Method to achieve EMC for Distributed Safety-Relevant Automotive," in *SIMUL2014*, 2014.

[32] Alexandersson, S., "Functional safety and EMC for the automotive industry," in *Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium on*, pp. 1–6, Aug 2008.

[33] Williams, T., *EMC for Product Designers*. Elsevier, fourth edition ed., 2007. ISBN-13: 978-0-75-068170-4.

[34] Franz, J., *EMV - Störungssicherer Aufbau elektronischer Schaltungen*. Vieweg+Teubner Verlag, 2008.

[35] EMCoS Ltd., "EMC Studio." www.emcos.com, 8 2013.

[36] Altair, "FEKO ." www.feko.info, 8 2013.

[37] COMSOL, Inc., "COMSOL Multiphysics." www.comsol.com, 8 2013.

[38] ANSYS, "ANSYS RedHawk." www.ansys.com/products, 05 2015.

[39] CST - Computer Simulation Technology AG, "CST STUDIO SUITE." www.cst.com/products, 05 2015.

[40] Montrose, M.; Nakauchi, E., *Testing for EMC Compliance - Approches and Techniques*. Wiley-Intersience, 2004.

[41] Zentralverband Elektrotechnik- und Elektronikindustrie e.V, *Generic IC EMC Test Specification V2.0*. 3/4/2010. Online: http://www.zvei.org/Publikationen/Generic_IC20EMC_Test_Specification.pdf.

[42] Farfeleder, S.; Hoermaier, K.; Krall, A; Zojer, H.; Rainer, A, "Requirements Specification and Analysis with DODT," in *ICSSEA12 Paris*, 2012.

[43] E. Kreyszig, *Advanced Engineering Mathematics*. John Wiley, 4 ed., 1999. ISBN-10 0-471-33328-X.

[44] Henze, N., *Stochastik für Einsteiger*. 7, Vieweg+Teubner, 2008. ISBN-13: 978-3834804235.

[45] Siemens AG, *Siemens-Norm SN 29500 Part 2 Failure rates of components - Expected values for integrated circuits*. 2004.

[46] EXIDA, *Electrical & Mechanical Component Reliability Handbook, 3rd Edition*. EXIDA, Aug 16, 2012.

[47] International Electrotechnical Commission (IEC), *IEC60721 - Classification of environmental conditions*. 2012-12-13.

[48] Automotive Electronics Council, *AEC-Q200 - Stress test qualification fro passive components*. June 1, 2010. www.aecouncil.com/Documents/.

[49] Parhami, B., "Defect, Fault, Error,..., or Failure?," *Reliability, IEEE Transactions on*, vol. 46, pp. 450–451, Dec 1997.

[50] Nagi, N.; Abraham, J.A., "Hierarchical fault modeling for analog and mixed-signal circuits," in *VLSI Test Symposium, 1992. '10th Anniversary. Design, Test and Application: ASICs and Systems-on-a-Chip', Digest of Papers., 1992 IEEE*, pp. 96 –101, april 1992.

[51] EXIDA, *Electrical & Machanical Component Reliability Handbook, 3rd Edition*, vol. 1. Aug 16, 2012. ISBN-13: 978-1-934977-05-7.

[52] Birolini, A., *Reliability Engineering*. Springer, 7 ed., 27. August 2013. ISBN-13: 978-3642395345.

[53] Hörmaier, K., "Verfahren zur zerstörungsfreien messtechnischen Ermittlung der Belastungsgrenzen von DMOS Leistungstransistoren," in *Tagungsbericht Microelektronik Tagung ME10; Vienna (Austria)*, 2010.

[54] *Systematic and Random Failure*. Safetyengineering Wordpress.com, 08/2014. http://safetyengineering.wordpress.com/2008/04/09/systematic-and-random-failure/.

[55] International Atomic Energy Agency, *IAEA Workshop - Common Cause Failure Analysis*. 10.04.2014. www-ns.iaea.org/.

[56] Goble, William M., *Control System Safety Evaluation and Reliability*. International Society of Automation, Jun 01, 2010. ISBN-13: 978-1-934394-80-9.

[57] Lundteigen, Mary Ann; Rausand, Marvin, "Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing," in *Journal of Loss Prevention in the Process Industries*, 2007.

[58] R. Billinton and R. Allan, *Reliability Evaluation of Engineering Systems: Concepts and Techniques*. Springer US, 1992.

[59] P. H. Seong, *Reliability and Risk Issues in Large Scale Safety-critical Digital Control Systems*. Springer London, 2009.

[60] Karwowski, W, *International Encyclopedia of Ergonomics and Human Factors*, vol. 3. CRC Press, 2001.

[61] I. of Engineering and T. (IET), *Electromagnetic Compatibility for Functional Safety*. IET, 2008. http://www.theiet.org/.

[62] W. Vesley, F. Goldberg, N. Roberts, and D. Haasl, *Fault Tree Handbook*. U.S. Nuclear Regulatory Commision, 1981.

[63] Isograph, *Reliability Workbench 12.0*. 2015. http://www.isograph.com/.

[64] ikv++ technologies ag, "medini analyze." http://www.ikv.de/.

[65] APIS Informationstechnologien GmbH, "APIS IQ-FMEA." http://www.apis.de/.

[66] Wenjing Sun, "Determination of Beta-factor for Safety Instrumented Systems," Master's thesis, Department of Production and Quality Engineering Norwegian University of Science and Technology, 2013.

[67] Jäkel, B.; Kohling, H., "EMV und Funktionale Sicherheit - Bewertungskriterien FS," in *EMV Kongress, Düsseldorf*, pp. 681–688, 2006.

[68] Felic, G.; Evans, R., "Study of heat sink EMI effects in SMPS circuits," in *IEEE International Symposium on Electromagnetic Compatibility, 2001*, 2001.

[69] Xun, Gong; Ferreira, J.A., "Reduction of conducted EMI for SiC JFET inverters by separating heat sinks," in *7th International Power Electronics and Motion Control Conference (IPEMC), 2012*, 2012.

[70] Alexandersson, S., *Automotive electromagnetic compatibility - Prediction and Analysis of Parasitic Components in Conductor Layouts*. PhD thesis, Lund University, 2008.

[71] Darney, Ian B., *Circuit Modeling for Electromagnetic Compatibility*. 2013. ISBN-9781613530283.

[72] Y. Fujishiro, *TDK EMC Technology - Classification of EMC Countermeasure Components and Their Roles*. TDK Corporation, 2011.

[73] Cermak, S.; Brasseur, G.; Zangl, H. ; Fulmek, P.L., "Capacitive sensor for incremental angular measurement," in *2nd Sensors for Industry Conference, ISA/IEEE 2002*, 2002.

[74] Aichernig, B; Hoermaier, K. Lorber, F, "Debugging with Timed Automata Mutations," in *SAFECOMP2014*, 2014.

[75] Aichernig, B; Hoermaier, K. Lorber, F; Nickovic, D; Schlick, R; Simoneau, D; Trian, S;, "Integration of requirements engineering and test-case generation via oslc," in *QSIC2014*, 2014.

[76] International Commission on Non-Ionizing Radiation Protection (ICNIRP), *For Limiting Exposure to Time Varying Electric, Magnetic and Electromagentic Fields (Up to 300 GHz)*. 1998.

[77] Groot Boerle, D.J., "EMC and functional safety, impact of IEC 61000-1-2," in *Electromagnetic Compatibility, 2002. EMC 2002. IEEE International Symposium on*, 2002.

[78] Arlat, J.; Costes, A; Crouzet, Y.; Laprie, J.-C.; Powell, D.;, "Fault injection and dependability evaluation of fault-tolerant systems," *Computers, IEEE Transactions on*, vol. 42, pp. 913–923, Aug 1993.

[79] International Electrotechnical Commission (IEC), *CISPR 25 - Vehicles, boats and internal combustion engines - Radio disturbance characteristics - Limits and methods of measurement for the protection of on-board receivers*. 2008.

[80] International Electrotechnical Commission (IEC), *CISPR 16 - Specification for radio disturbance and immunity measuring apparatus and methods*. 3 ed., 2008.

[81] Rauscher, C., *Grundlagen der Spektrumanalyse*. Rohde & Schwarz, 2000. www.rohde-schwarz.com.

[82] Klaus Hoermaier; Hubert Zangl; Herbert Zojer, "An EMI Receiver Model to Evaluate Electromagnetic Emissions by Simulation," in *Proceedings on IEEE International Instrumentation and Measurement Technology Conference (I2MTC 2012)*, 2012.

[83] Hoffmann, C.; Russer, P.;, "A Time-Domain System for EMI Measurements above 1 GHz with high Sensitivity," in *IEEE German Microwave Conference (GeMIC)*, pp. 1–4, 2011.

[84] *Alfred Mertins; "Grundlagen der Signalbeschreibung, Filterbänke, Wavelets, Zeit-Frequenz-Analyse, Parameter- und Signalschätzung"; Vieweg+Teubner; 2010 ISBN 978-3-8348-0737-3.*

[85] Braun, S.; Frech, A.; Russer, P.;, "CISPR specification and measurement uncertainty of the time-domain EMI measurement system," in *IEEE International Symposium on Electromagnetic Compatibility*, 2008.

[86] Keller, C.; Feser, K., "Non-linear superposition of broadband spectra for fast emission measurement in time domain," in *EMC Zürich*, 2003.

[87] Krug, F.; Russer, P., "Quasi-Peak Detector for a Time-Domain Measurement System," in *IEEE Transactions on Electromagnetic Compatibility VOL.47 NO.2*, 2005.

[88] International Electrotechnical Commission (IEC), *IEC 62132 - Integrated circuits - Measurement of electromagnetic immunity, 150 kHz to 1 GHz*. 1.0 ed., 2006-01-19.

[89] Klaus Hoermaier; Hubert Zangl, "Electromagnetic Emission Simulation Evaluation - A use case," in *Microelectronic Systems Symposium (MESS2014), Vienna, Austria*, 2014.

List of Figures

List of Tables