Pan-European Training, research and education network on Electromagnetic Risk management (PETER)

PETER Deliverable 1.1 (D3)– Basic description statistical electromagnetic risk assessment

Authors: Samikshya Ghosalkar[1], Heyno Garbe[1]

[1]Leibniz Universität Hannover

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No. 812.790

Deliverable Number	**D1.1 (D3)**
Deliverable Name	**Basic description statistical electromagnetic risk assessment**
Deliverable Duration	April 1, 2019 to October 31, 2020
Due Date of Deliverable	October 31, 2020
Actual Submission Date	October 30, 2020
Deliverable Lead Partner	LUH
Dissemination Level	Public
Work Package	WP1
No of Pages (Annex not included)	32
Keywords	WP1, electromagnetic risk assessment

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Deliverable 1.1

Basic Description Statistical Electromagnetic Risk Assessment

Faculty of Electrical Engineering and Computer Science

Gottfried Wilhelm Leibniz University of Hanover

Submitted By

Ms. Samikshya Ghosalkar

under the Guidance of

Prof. Dr. -Ing. Heyno Garbe

MSc Samikshya

Prof. Dr.-Ing. Heyno Garbe

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No. 812.790

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Table of Content

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

List of Figures

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Abstract

The increasing number of wireless communication devices leads to an increased risk of (Intentional) Electromagnetic Interference ((I)EMI) which threats to disturb or even destroy electronic systems.

In the past, many researchers have proposed different approaches to estimate the whole risk of a system. Despite this, there is no direct or well-established approach available to estimate the risk related to (I)EMI, nor to combine this with other available information. In our work, we propose to use different statistical approaches to analyze the system behavior and estimate the (I)EMI-related risk and the failure probabilities, combined with technical and non-technical parameters.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

1 Introduction

Ongoing trends like Smart Grid (SG), Industry 4.0 (I4.0) and Internet of Things (IoT) are all based on widely networked communication between multitudes of electronic systems. Especially the developments in the area of IoT show a rapid development and spread in the area of wireless networks between electronic devices.

The field of electromagnetic compatibility (EMC) is concerned with the prevention of unintentional interference. Unfortunately, the danger of intentional disturbance or destruction of a system through Intentional Electromagnetic Interference (IEMI) is growing. Criminal aggressors in particular could attempt to use an artificial source of electromagnetic disturbances to impair, manipulate or destroy an electrical system. The sources which are mainly used differ in their bandwidth, power, size, signal shape and other non-technical aspects. Therefore, the process of electromagnetic interference interaction can be considered as a statistical problem. In the context of our work, knowledge or estimates on the statistical sensitivity to electromagnetic interference are expanded from the component level and subsystem level to higher levels in order to assess the vulnerability at system and even infrastructure level.

1.1 Electromagnetic Interference at Subsystem Level

The section summarizes the first approaches for statistical modelling of the failure behavior of electronic components, considering electromagnetic disturbances. Early studies on the interference sensitivity at component level by Bäckström et al. [1, 2] showed impairment depending on the angle of incidence of the deliberate electromagnetic interference, which used narrowband signals. Further investigations of the failure behavior with broadband pulses followed by Camp et al. [3] and Nitsch et al. [4]. Camp [5] introduced a first statistical approach in which the failure behavior of microcontrollers with a defined disturbance variable

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

was estimated and predicted by a distribution function. For the statistical description of the failure behavior depending on the pulse amplitude, Camp introduced the terms breakdown failure rate (BFR) and destruction failure rate (DFR). Nitsch demonstrated that the BFR introduced by Camp was dependent on the interference pulse shape used. The transfer to other pulse forms takes place via the lowest amplitude dropout threshold and the width of the measured BFR curve for typical system lengths. A prediction using a statistical approach was carried out by Magdowski and Genender [6,8]. Their approach starts from the findings presented by Bäckström on the dependence of the effect that the interference has on the angle of incidence of the electromagnetic disturbance. In addition, they expanded the statistical approach of Camp to predict the failure behavior of subsystems by a random angle of incidence. Compared to Camp, this represents a more precise model for predicting the failure probability, but is nevertheless is still based on a rather simple case of coupling, compared to real life.

1.2 System Level Electromagnetic Interference

An attempt to analyse the electromagnetic interference effect at the system level, led Baum [9] in 1974 to describe the system behavior using electromagnetic shielding zones with propagation and coupling paths between them. Later, Lo Vetri and Costache [10] picked up this approach of electromagnetic topology (EMT) in 1991 and extended it with an estimate of the failure probability of the individual sub-components with a defined electromagnetic disturbance variable. The resulting disturbance variable is compared with the system's probability of failure taking into account the damping evaluation of the coupling paths. Further building upon this, Mao worked on the topic of a statistical forecasting model and combined it with a Bayesian Network (BN) exploiting statistical data analysis. For systems of relatively small size, Mao showed in 2015 that an assessment of the vulnerability of a core system that depends on other subsystems is possible. Mao’s analysis takes into account environment, coupling mechanisms, sensitivity of the components and the system state.

This project has received funding from the European Union’s EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

In 2012, Genender picked up parts from the classic risk analysis and developed a statistical approach for the system analysis of the vulnerability of electronic systems at the system level. The approach took into account both to the electromagnetic sensitivity of electronic systems, as well as non-technical parameters that were previously introduced by Sabath and Garbe in 2008 [11, 12]. Sabath and Garbe extended the classification according to the physical properties of electromagnetic interference sources – according to Giri and Tesche – to also include non-technical aspects, such as mobility, the technological challenge, the development costs and the probability of occurrence. Genender used these parameters in his risk analysis to determine the vulnerability of a system. In addition, Genender combined thiw with the work of Mansson from 2009 to assess the accessibility of an infrastructure as a zone model.

An approach introduced in 2015 by Sabath and Garbe [13] used the results of a survey of an expert panel to predict the risk of occurrence and the hazard potential of possible electromagnetic interference sources to assess the risk.

This section summarized approaches from classic risk analysis and statistical models for predicting vulnerability to electromagnetic interference from electronic systems. The approaches are based either on purely physical quantities or additionally use non-technical parameters for prediction. A combination of the physical and non-technical parameters was introduced in some methods of risk analysis. So far, these have not been combined in a common system-level model. On the one hand, the complex process of obtaining physical data, which is additionally burdened with uncertainties to estimate the vulnerability of larger networks from systems, is a key problem. On the other hand, how to link the non-technical parameters, i.e. the linguistically formulated terms from the expert knowledge, with the physical relevant quantities within the methods described above is an open question. Therefore, in this work a statistical approach is to be worked out, which combines the objective and subjective knowledge in formulated terms with the uncertainties of the measured values and non-technical parameters in one approach. In particular, the uncertainties and expert opinions must be linked to the complexity of networked electromagnetic systems in a holistic stochastic approach.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

2 Statistical methods

When analyzing complex systems, the analytical considerations, numerical calculations and experimental investigations quickly reach their limits in terms of the effort required. Due to the complexity, an analytical view is only possible with great simplifications. A complete numerical analysis is complicated by the huge number of possible states and electrical quantities to take into account. Similarly, the large number of electrical signals and quantities prevents an experimental investigation, since only a limited time is available for measurements. Finally, the location of the source of the interference should be assigned a certain probability.

To overcome the above, various statistical methods and approaches for IEMI risk analysis are presented in the following sections. One of the first methods in risk analysis is the fault tree analysis and is explained in section 2.1 and, based on this, the event tree analysis is detailed in section 2.2.

Section 2.3 examines the approach of electromagnetic topology (EMT) to investigate the propagation path of electromagnetic interference signals and the classification of shielding levels for risk analysis. Then the Markov analysis (section 2.4) and the risk analysis according to Genender (section 2.5) and its procedures are presented.

For more complex problems, a procedure based on the Bayes Theorem follows in Section 2.6. An approach based on unsharp quantities is introduced in Section 2.7, which is further pursued in this work. Section 2.8 describes an expansion of the fuzzy theory to include neural networks.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

2.1 Fault tree analysis (FTA)

Fault tree analysis (FTA) is one of the deductive risk-analysis methods and serves as a procedure for the reliability and/or safety analysis of technical systems. FTA uses a graphical approach to analyze the relationship between a top event (system failure, hazard) and investigates the causes that can lead to this top event. The causes can occur either alone or in combination with others. The process of the FTA has been defined since 1981 by the standards DIN 25424-1 / -2 (1981/1990) and DIN EN 61025 (2007) and was originally developed for Boeing at Bell Laboratories in New Jersey (USA) in the 1960s. After being used for probabilistic safety analysis in nuclear power plant technology, the approach found its way into many technical areas, including software development.

The aim of the FTA process is to model the system realistically on a component basis, to detect possible failure types and causes, to establish the functional connections to the occurrence of the failures and to describe the effects of these failures on the system. FTA is mainly used for preventive quality assurance, system analysis and problem solving for new errors.

FTA is a suitable method for examining sub-components. If the failure probabilities of the individual components are available, it can also be applied to more complex systems. In the case of electromagnetic interference in complex systems, the failure probabilities are not known and for the most part can only be determined with extremely complex measurement campaigns. There are many uncertainties to determine the risk, so that the method quickly reaches its limits and can only be used as an aid.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

2.2 Event tree analysis (ETA)

Event Tree Analysis (ETA) is an inductive approach in risk analysis which describes an initiating hazard event and examines the possible consequences of this event. In contrast to FTA, the event tree is usually constructed from an event to an error (see **Figure 2.1**). The tree starts on the left with the initiating event, the root node, and branches over a number of decision nodes. These nodes represent decision-making situations that may or may not occur, similar to FTA. The tree ends on the right in the effect of the initiating event.

Figure 2.1 shows a general example of an ETA analysis. The root node is the EMI exposure, which can lead to a disruption of the system under consideration. The first subsequent event is the coupling of an interference voltage into the system. Either this event occurs or not. The non-entry leads to the upper branch, indicating that no interference voltage is coupled in and the system is not disturbed, which directly represents the end of this branch. When an event occurs, the second event follows, which results in the failure of a module. This continues by considering the failure of a subsystem up to the final impact. In this example it would be conceivable that either there is no malfunction, that the system's performance is reduced, that it leads to a partial failure or to a complete system failure.

The ETA approach in itself is not a stochastic approach aimed to calculate the probability of a failure, but is aimed to be a clear, structured graphical representation for possible states and events. **Figure 2.1** shows a general example of an ETA analysis. The root node is the EMI exposure, which can lead to a disruption of the system under consideration. The first subsequent event is the coupling of an interference voltage into the system. Either this event occurs or not. The non-entry leads to the upper branch, that no interference voltage is coupled in and the system is not disturbed, which directly represents the end of this branch. When the event occurs, the second event follows, which results in the failure of a module.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

This continues by considering the failure of a subsystem up to the final impact. In this example it would be conceivable that either there is no malfunction, the system's performance is reduced, it leads to a partial failure or to a complete system failure.

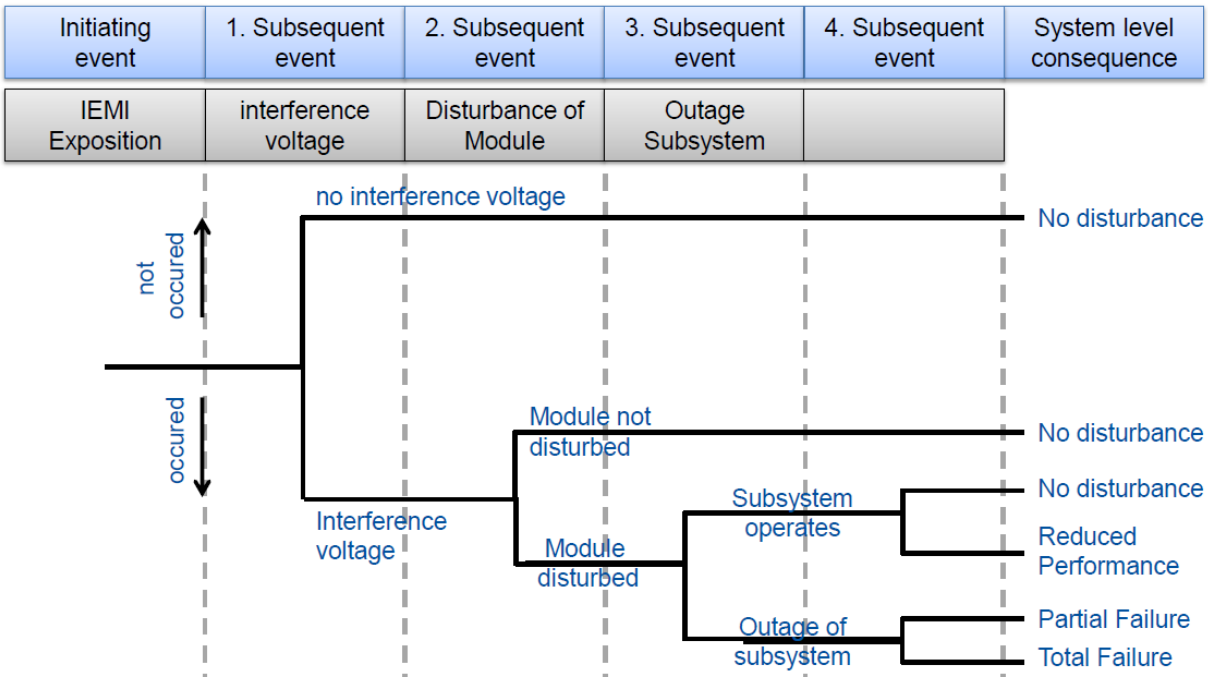
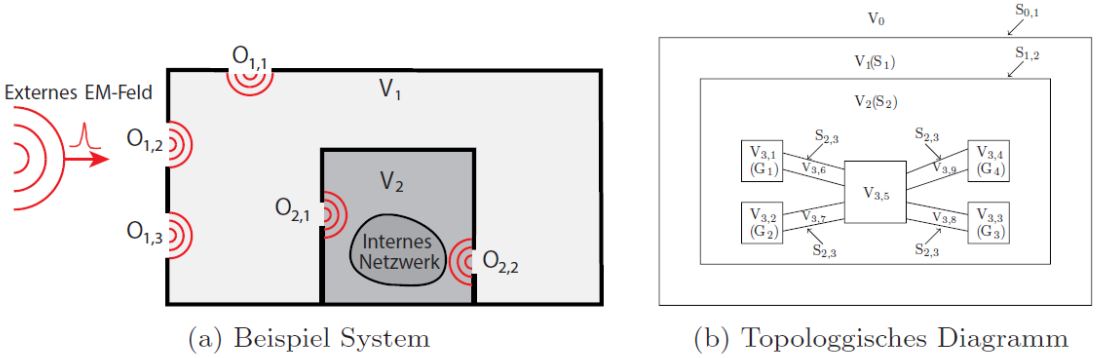


Fig 2.1: Example of a typical event tree

2.3 Electromagnetic Topology (EMT)

The concept of EMT was developed by Baum [9] to describe the electromagnetic shielding of complex systems. More specifically, the method for characterizing the electromagnetic property of one or more shielding levels is used.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/



(a) Beispiel System (b) Topologgisches Diagramm

Fig 2.2: Example system and the topological diagram

For this purpose, the complex system is broken down into its individual coupled subsystems (partial volumes). Each subsystem is examined and the partial results are combined with the EMT. The interactions of the individual partial volumes are shown using the topological diagram (see **Fig. 2.2 b**) and the interaction graph (see **Fig. 2.3**). The graph is based on the top-down principle and thus only considers how the disturbance flows towards volumes of equal or lower order.

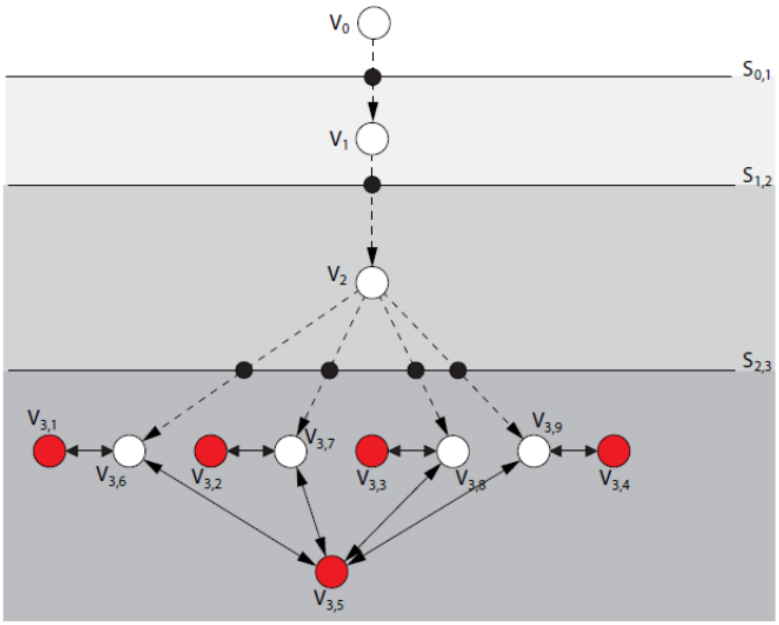


Fig 2.3: Interaction graph for Fig. 2.2

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Using EMT, the propagation of the electromagnetic interference can be sketched, considering possible coupling mechanisms and graphically depicting the dependencies on subsystems. However, this requires extensive prior knowledge of the scenario under consideration. A classification of the sources of interference and the calculation of the failure probability is not possible in EMT.

2.4 Markov analysis

Markov analysis is suitable for the modeling and calculation of complex systems with several states that can be traced back to stochastic processes. For this purpose, the behavior is transformed into states S_i, state transitions p_{ij} and rules for the state transitions, which are called Markov chains. A system is assumed to be in one specific state at any time t. States are therefore exclusive and mutually exclusive. Another characteristic is that the next state of the process may depend on the current state, but not on the previous one from which the current state was reached. Therefore, an essential feature is the lack of memory within this approach. The probability of reaching a certain state X at a future time t_{n+1} depends only on the state at the current time t_n and is defined as follows:

$$P\{X(t_{n+1}) = S_{n+1} \mid X(t_n) = S_n\}$$
$$= P\{X(t_{n+1}) = S_{n+1} \mid X(t_n) = S_n, X(t_{n-1}) = S_{n-1}, \ldots, X(t_0) = S_0\}$$
$$(t_{n+1} > t_n > t_{n-1} > \ldots > t_0). \qquad (2.1)$$

Depending on the choice of the parameter space, continuous Markov chains (tn € R+) or discrete-time Markov chains (tn € N0) exist. The discrete-time case for an example system is considered below. A system is analyzed which is subjected to an interference signal and can assume the following four states:

- Normal state S1,
- System is loaded S2,
- System is faulty S3 and
- System drops out S4.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

For this example, the graphical representation of the Markov chain is shown in **Fig. 2.4**.

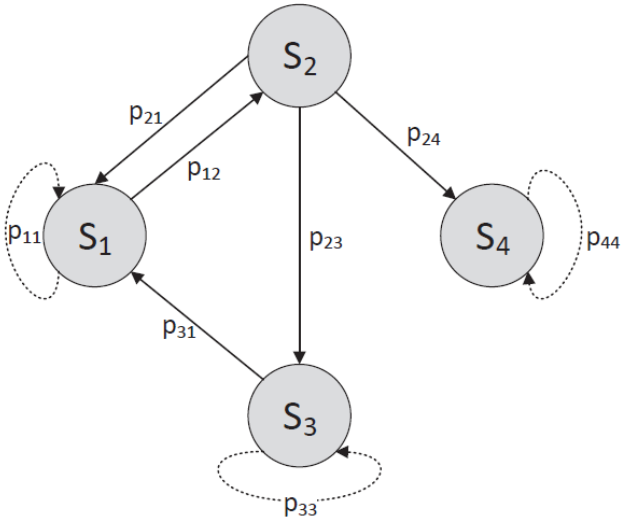


Fig 2.4: Example of a Markov chain

The probability of occurrence of a certain condition can be calculated using the Markov analysis. In this example, it would be the failure due to electromagnetic interference. The result of this consideration in earlier states is completely neglected. Previous damage to the system is thus ignored and not considered in the calculation. This can be corrected by introducing additional states Si. This makes the graph in **Fig. 2.4** more extensive. This method is therefore only of limited use for complex systems.

2.5 Risk analysis according to ISO 31000

The risk analysis defined in ISO 31000 is a systematic analysis for the identification and assessment of risks. This method was used by Genender to analyze the risk of electronic systems related to electromagnetic interference. The method itself is not a stochastic approach, but a process step in the overall risk management.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

2.5.1 Definition of risk according to ISO 31000

The ISO 31000 standard defines risk as the combination of the probability of occurrence of a damage and the associated extent of damage. Genender formulated the risk R as a combination of the negative consequences Ci and determined the probability p (Ci) as a set of pairs of these consequences:

$$R = \{Ci, p(Ci)\}, \text{ with } i = 1,., N \quad (2.2)$$

If the probabilities are available as quantitative values, the total risk results from the sum of the products:

$$R = \sum_{i=1}^{N} Ci \,.\, p(Ci) \quad (2.3)$$

The resulting result can be used to compare the risks of different scenarios.

2.5.2 Risk Management and Analysis

The risk management process (see Fig. 2.5) includes all measures to identify, analyze, evaluate, monitor and control the risks.

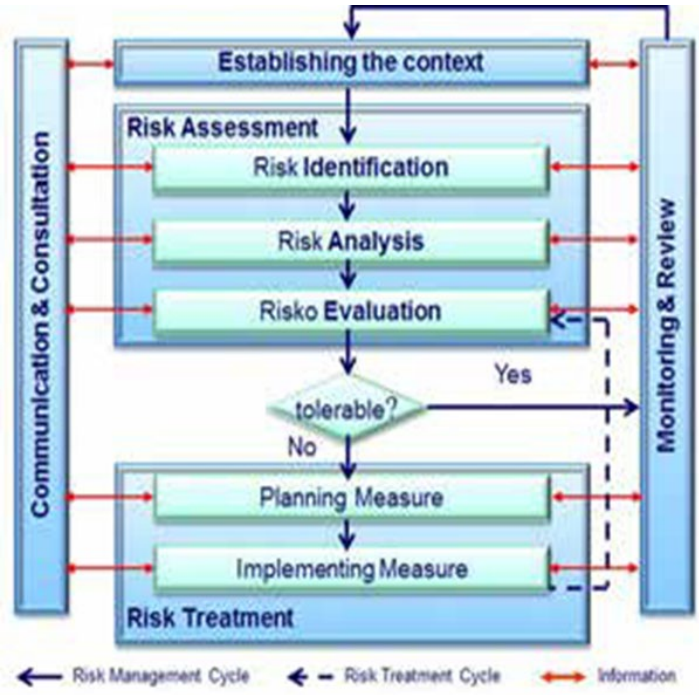


Fig 2.5: Risk management process according to ISO 31000 [14]

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

The procedure and definition of the process are described differently in the specialized literature. On the one hand, this depends on the area of application. On the other hand, the process is subject to constant change. In the IEMI application, risk management is divided into three areas:

- Risk analysis / assessment,
- Risk control and
- Risk communication.

The analysis should identify the risks and assess the consequences and probability. The probability of occurrence, the potential effects and their priorities (e.g. low, medium and high risk) are determined for the identified risks. Control means risk management, in which measures for reduction are planned and developed. In the final step, risk communication, risk information is exchanged between analysts, experts and other stakeholders. The entire management process is a repetitive process to minimize risk.

2.5.3 Methods in Risk Analysis

In this section various methods in risk analysis are described. Only methods that are of interest for assessing the risk of electromagnetic interference are considered.

2.5.3.1 Failure Mode and Effects and Criticality Analysis (FMECA)

FMECA is an inductive method and is an extension of the Failure Mode and Effects Analysis (FMEA) to additionally assess the criticality of an error event. The structure of the FMECA is explained in MIL-STD-1629A and is mainly used for reliability and security analysis (e.g. in the automotive industry or aerospace). At the heart of this method is the assessment of the impact and criticality of individual error events on the overall functionality of the system under consideration. The process focuses on internal system error states and their effects on system behavior and is structured as follows:

- Definition of the system,
- Development of a structural model,
- Identification and analysis of errors and causes,

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

- Classification of the severity of the error,
- Identification of methods for error detection and compensation and
- Documentation of the analysis.

Due to the focus on internal error states, the method is only conditionally applicable in the application of the EMI risk analysis, since environmental influences are not considered from the outset. By expanding the basic structure of FMECA to consider electromagnetic ambient conditions, the method for EMI scenarios can be used to analyze the risk. This is described in the following subsection 2.5.3.2.

2.5.3.2 Threat Scenario, Effect and Criticality Analysis (TSECA)

The Threat Scenario, Effect and Criticality Analysis (TSCEA) is one of the inductive methods of EMI risk analysis and builds up the FMECA (see **Chapter 2.5.3.1**) and extends it by considering electromagnetic environmental conditions (threat scenarios). Instead of only describing the system in the first analysis step, the entire threat scenario is also defined. This means that the structural model of the system is supplemented by the modelling of the EMI environment and the electromagnetic coupling. The basic structure of the TSCEA method is shown in **Fig.2.6** and is identical to the structure of the FMECA. The determination of possible error states can be reduced in step three to the error states caused by the EMI environment. Like the FMECA, the TSCEA represents a structured procedure for risk assessment of a system. However, this method is not suitable as a stochastic model; other methods must be used for this.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

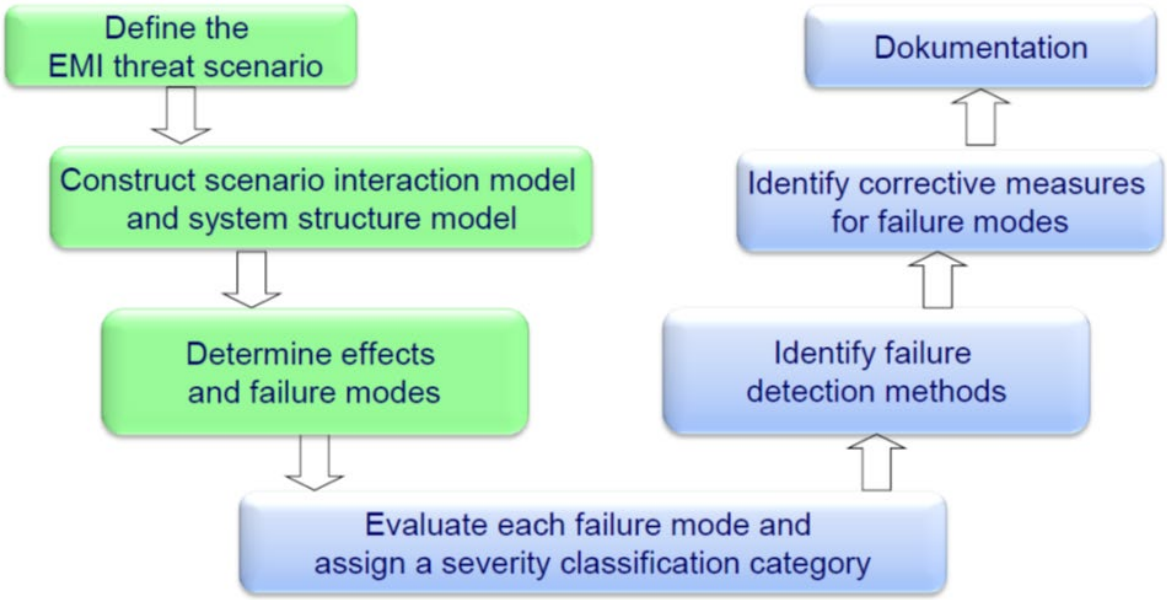


Fig 2.6: Basic structure of the TSCEA method [15]

2.5.3.3 Bow Tie Analysis (BTA)

Bow Tie Analysis (BTA) represents a further qualitative analysis method, which, similar to EMT (see **Chapter 2.3**), graphically represents the path of action from the cause of a risk to the effect. The structure of the BTA is more or less a combination of FTA (see **Chapter 2.1**) and ETA (see **Chapter 2.2**). The focus of the risk diagram is the considered error event, which is related to the causes and consequences.

Fig. 2.7 shows an example for the analysis of an EMI scenario. The causes of risk are listed on the left-hand side and linked to the error event. Protective measures (e.g. filters, shielding) can be entered as a barrier on the connecting lines. To the right of the fault event are all possible effects that would follow without further action. This method is suitable for the analysis of simpler relationships, because this method quickly reaches its limits in complex systems. Furthermore, temporal relationships are not shown, which makes it difficult to analyze overlapping effects of simultaneously occurring hazards.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

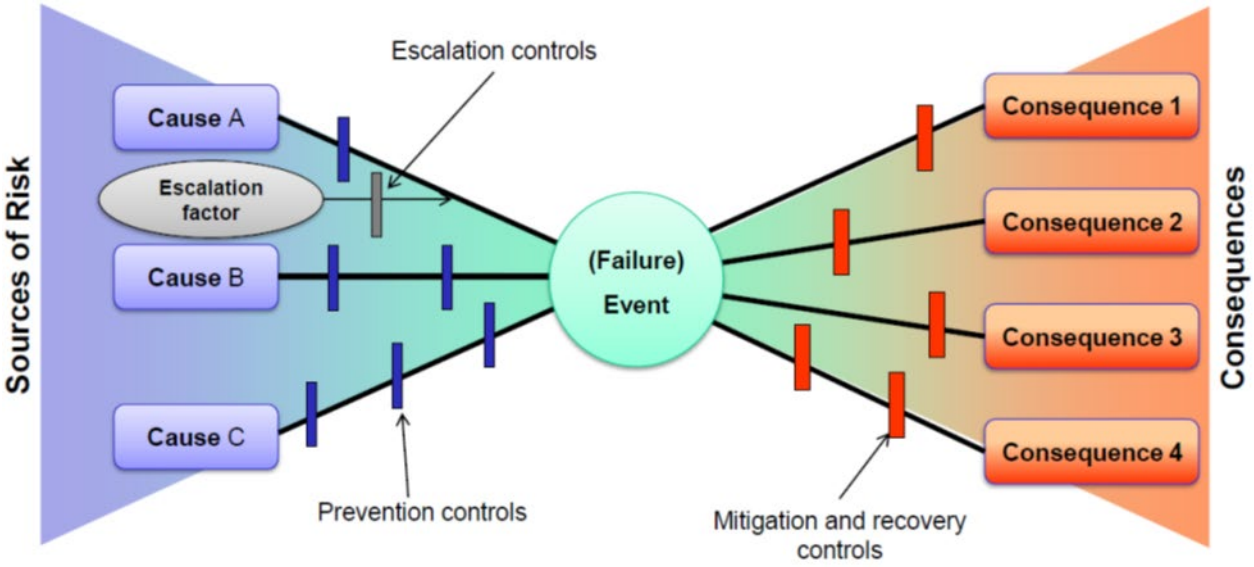


Fig 2.7: Example of a bow tie diagram

2.5.3.4 Preliminary Hazard List or Analysis (PHL or PHA)

The Preliminary Hazard List (PHL) is used for the early structured identification of sources of danger and as a preliminary stage of the Preliminary Hazard Analysis (PHA). Starting with the cause of a risk, possible causes of danger are systematically recorded. In the case of EMI risk analysis, all potential EMI sources from the area are listed. The resulting list of PHL is used in the PHA to assess the risk. The aim of the assessment is to assess the possible effects, severity and frequency of an event and determine starting points for measures to manage risk. This methodology from PHL and PHA is based on the knowledge of the system and is used for the preliminary assessment of the risk. A concern is an incomplete list of hazards.

2.5.3.5 Importance Analysis

The aim of this analysis method is to identify the elements that make the greatest contribution to the risk of the system. This results in a ranking of the hazard elements, which is an important result of the risk analysis. Various methods exist for the calculation. Birnbaum Importanz is the most common form in which the change in the overall failure probability p(Sys) is related to the change in the selection probability A of the components A under consideration.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

I_B (A) = δp (Sys) / δp(A) = p(Sys). δ/ δp(A) (2.4)

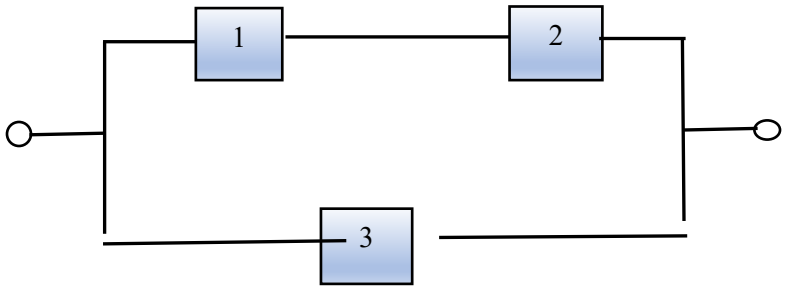


Fig 2.8: Example system for Importance Analysis

In order to use the importance analysis, the overall failure probability and the failure probabilities of the subsystems are required for the system under consideration. If this information is known, this is a suitable method for optimizing the system against vulnerabilities. This will often not be the case with larger and complex systems, so this method is unsuitable for such systems.

2.5.3.6 Risk Matrix

One method for risk assessment is the risk matrix. It is similar to risk assessment using the risk priority number (RPZ), in which the probability of occurrence (A), the severity (S) of the effects and the detectability (E) of risks are multiplied. The probability of occurrence means the probability that a corresponding event occurs and its impact on the system is understood under the term severity. The fact that this event is detected by surveillance measures reflects its discoverability. In the event that further dependencies are added, the resulting risk cube consists of n dimensions for n factors.

RPZ = A.S.E. € {1, 1000} (2.5)

In the risk matrix, the various probabilities are classified using scales. These characteristics are plotted against each other in an assignment matrix, the risk matrix. The individual cells of this matrix are assigned scale values of the risk. A typical scale for subdivision is derived from the traffic light.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

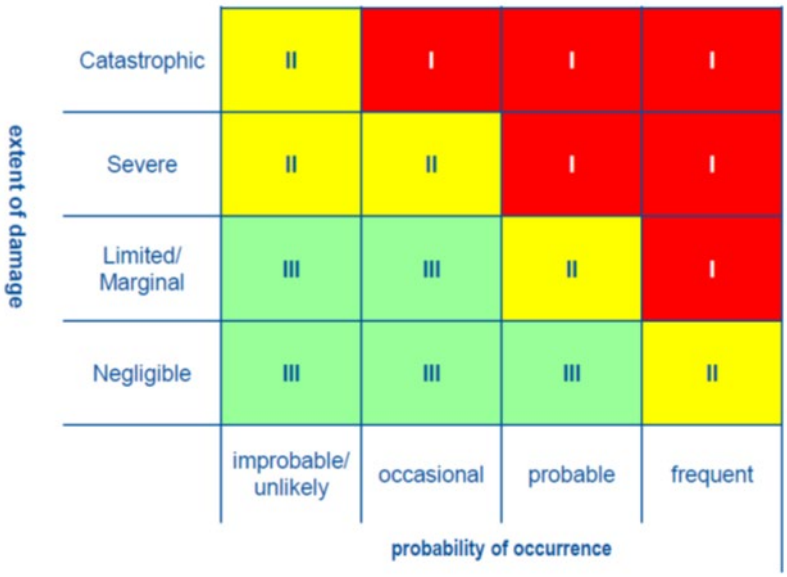


Fig 2.9: Example of a risk matrix

The three areas for risk assessment would be:

- that the risk is acceptable (green),
- action is required (yellow) or
- the risk is not acceptable (red).

The methods considered in this section 2.5 require the knowledge of an expert group to carry out the risk assessment. The composition of this group directly determines the success of the rating. Therefore, success depends on the level of expertise in each area. In the case of EMI risk assessment, an interdisciplinary and system-oriented approach is required.

2.6 Bayesian Statistics and Networks

According to the risk theory, a risk consists of events and their effects together with the probabilities. The Bayesian concept of probability is suitable for calculating these probabilities. The strength of this approach is based on the processing of large amounts of data, the consideration of previous knowledge and the use of assumptions.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Two approaches based on Bayes' concept of probability for determining the probability of failure of complex systems are presented below. The method of Bayesian statistics is presented in Chapter 2.6.1 and the Bayesian networks in Chapter 2.6.2.

2.6.1 Bayesian Statistics

In order to use Bayesian probability as a measure of uncertainty, a person with experience and understanding of the topic is required. A probability is therefore always a function not only depending on events, but also on information (assumptions, knowledge and data).

Bayesian statistics are characterized by the use of distribution functions to calculate the probability. The accuracy and reliability of the results depend on these functions. Another advantage of Bayes' theorem is an existing knowledge to combine the variable to be examined (a priori distribution) with new knowledge (likelihood), from which improved results of the probability result (a posteriori). Thus, newly acquired information or knowledge can subsequently be used to optimize the failure characteristics of a complex system.

2.6.2 Bayesian Networks

Bayesian networks are used to represent systems with uncertainties. This is achieved using directed acyclic graphs (DAG). The nodes of the DAG present the random variables and directed edges represent direct stochastic dependencies. The edges of the DAG describe the causal influence of the start node (cause) to which the edge refers (effect).

There are no cycles with a DAG, so the networks consist of the following three basic elements: series, divergent and converging connection (see **Fig. 2.10**). The series connection represents the continuous influence of the start node A on C via B. A diverging connection means that the start node has a direct influence on the two nodes B and C. In the last example, the two nodes A and B act on node C

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

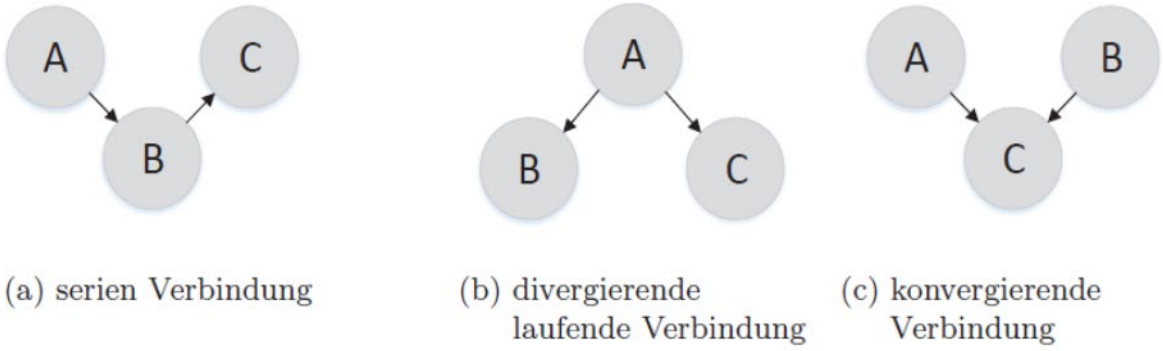


Fig 2.10: Basic elements for building a Bayesian Network

Once the Bayesian network is known, a wide variety of scenarios can be calculated with it. Despite the many possibilities of Bayesian networks, this knowledge storage approach nevertheless shows some weaknesses as well. With a known order of cause and effect, setting up a Bayesian network is still relatively simple. If, however, too few dependencies are known, densely populated Bayesian networks can result from unfavorable indexing, which in turn leads to a high effort when calculating probability distributions. So, the probabilities needed must be all at least partially known, which is not the case when considering an IEMI scenario with a more complex system structure.

Another disadvantage is the directional structure of a Bayesian network. So, the conditional dependence can only be shown with respect to all of its predecessors. In addition, cyclical dependencies cannot be described, since they must not appear in the Bayes graph. Thus, it is generally not possible, without auxiliary models, to use and display all existing dependences of the distribution of origin in Bayesian networks.

2.7 Fuzzy Theory

The two-valued, Boolean logic refers to clear, sharp statements, which are often represented by the states "true" and "false". This contrasts with the theory of fuzzy logic, which is a multi-valued logic. With fuzzy logic [7], on the one hand, as with classic binary logic, sharp

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

statements with sharp boundaries can be processed. In this case, overlapping limits mean that a statement can be "true" to one degree and "false" to the other degree. Another advantage is the processing of uncertainties, which can be expressed, for example, using linguistically formulated terms.

2.7.1 Fuzzy Sets

The definition of fuzzy sets was published by Zadeh in 1965 and has been the basis of today's fuzzy logic since then. Compared to the classical set theory, the membership of elements in a set is not described by "0" for not and "1" (see **Fig. 2.11a**) for belonging, but any number is possible as a degree of belonging (see **Fig.2.11b**).

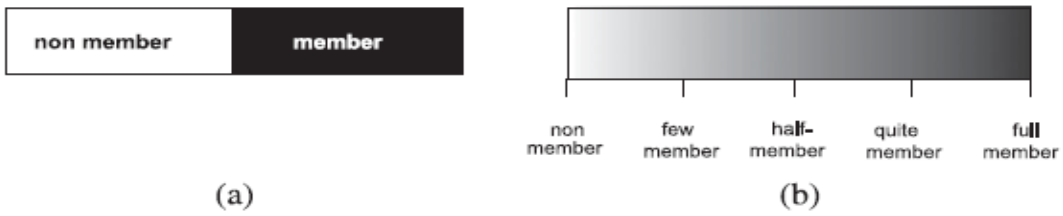


Fig 2.11: Comparison of the classic set with the fuzzy set

2.7.2 Fuzzy Systems

Fuzzy inference systems are used to reproduce a static, non-linear functional relationship y = f (x). An input vector x = {x1, x2, ... xn} serves as the input parameter, which leads to the output of the fuzzy system y (see **Fig. 2.12**).

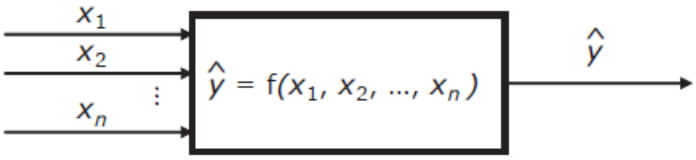


Fig 2.12: Fuzzy functional context

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Such systems are used for various tasks:

- as developing a model that describes a section of a real process,
- as a system with action knowledge to control a process (fuzzy controller)
- or to diagnose a technical system.

2.8 Neural Networks

Neural fuzzy systems are a coupling of the artificial neural networks with fuzzy systems, mainly with fuzzy controllers. The artificial neural networks (KNN) simulate the neuronal networking of the brain and spinal cord. This is mainly used for the development of artificial intelligence in neuroinformatic. They can also be used to calculate probabilities using fuzzy systems or to develop rules for fuzzy controllers.

Fig. 2.13 shows an example of the basic structure of a three-layer neural network. The input units take up the information and passes it on to the intermediate units. This process information depends on the network configuration.

Such KNNs are of interest for applications in which there is little explicit knowledge to solve the problem at hand. Areas of application are typically image processing, pattern recognition development, classification, IT, robotics, medical diagnostics and Control engineering.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

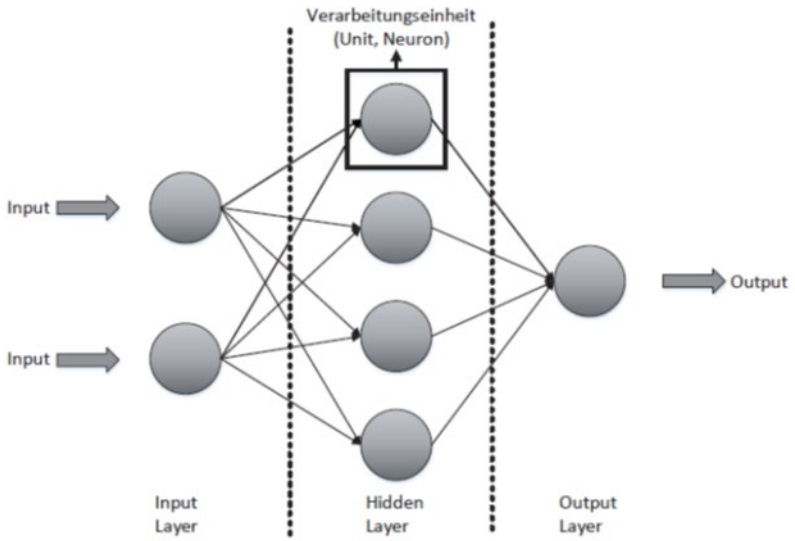


Fig 2.13: Example of a three-layer neural network

2.9 Summary

In summary, there are many different approaches for calculating the risk probability of systems. For complex and extensive tasks, the methods FTA (**Section 2.1**), ETA (**Section 2.2**), EMT (**Section 2.3**) and the Markov analysis (**Section 2.4**) reach their limits. The methods of risk analysis (**Section 2.5**) usually require a panel of experts for the assessment and there is no mathematical description for this. Only the BN and Fuzzy approaches offer the possibility to use expert knowledge. The latter can formulate this in linguistic terms and process fuzzy knowledge. By coupling with KNNs, fuzzy systems can be taught in and therefore represent the mathematical approach in this work.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

3 Conclusion & Further work

To disrupt wireless connections or electronic systems, artificial sources are used to deliberately disrupt or to destroy them. The intentional electromagnetic interference falls under the term IEMI and poses an ever-increasing criminal danger.

Given the complexity of and many dependencies within systems, in section 2 different statistical methods were examined for their applicability to analyse the risk of electronic systems regarding IEMI. It was found that established processes such as FTA and ETA are only applicable to small circuits. The electromagnetic topology (EMT) turned out to be a suitable way to describe the coupling and propagation paths. At the same time it allows to subdivide the system into shielding levels after which each level can be considered individually. The method reaches its limits with the sources of interference, the failure behavior of the system and the possible transferability to new disruption scenarios.

The analysis of the methodology of the risk analysis showed that there was a procedure for the assessment of complex systems with different approaches (FMECA, TSCEA, BTA, PHL, PHA, Importance Analysis and the Risk Matrix). It was demonstrated that each approach has its pros and cons in the risk analysis. Each of the procedures mentioned require background knowledge of a team of experts. This showed that the methods of risk analysis were only of limited use for a stochastic approach as well as for transferability to new scenarios.

Furthermore, Bayesian statistics consider probabilities of subsystems with uncertainties. As distribution functions have to be used, an expert has to be involved. Moreover, there is no direct approach to integrate linguistically formulated rules.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

As a last procedure, the fuzzy sets and multi-valued logic (fuzzy logic) were examined, which so far have not been applied in the area of IEMI. However, it seems that this is a suitable method to include vague statements from experts, formulated as linguistic terms, as well as probability density functions and to process case probabilities. Especially the fuzzy ones, including transitions from one state to another, seem to be an interesting approach.

There is a continued need to find a different statistical method that can combine both the technical and non- technical parameters. In our future work, we would like to develop methods for Smart Grids that can consider most specifically the non- technical parameters like mobility, accessibility, etc.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

References

[1] M. Bäckström, O. Lundén, and P. Kildal, “Reverberation chambers for EMC susceptibility and emission analyses,” *Review of Radio Science*, pp. 429-452, 1999.

[2] M. Bäckström and J. Loren, “Microwave coupling into a generic object. Properties of measured angular receiving pattern and its significance for testing,” *2001 IEEE EMC International Symposium. Symposium record. International Symposium on Electromagnetic Compatibility (Cat. No.01CH37161)* , pp. 1227-1232, 2001. doi: 10.1109 / I-SEMC.2001.950610

[3] D. Nitsch, M. Camp, H. Friedhoff, J. Maak, F.Sabath, and H.Garbe, “UWB and EMP Susceptibility of modern Microprocessor Boards,” *4th European Symposium on Electromagnetic Compatibility, Belgium,Bruges*, pp. 345-350, Sept. 11-15 2000.

[4] D. Nitsch, M. Camp, F. Sabath, J.-L. ter Haseborg, and H. Garbe,“Susceptibility of Some Electronic Equipment to HPEM Threats,”*IEEE Transactions on Electromagnetic Compatibility* , vol. 46, no.3, pp. 380-389, Aug. 2004. doi: 10.1109 / TEMC.2004.831842

[5] M. Camp, H. Gerth, H. Garbe, and H. Haase, “Predicting the Breakdown Behavior of Microcontrollers Under EMP / UWB Impact Using a Statistical Analysis,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no.3, pp. 368-379, Aug. 2004. doi:10.1109 / TEMC.2004.831816

[6] E. Genender, A. Kreth, D. Zamow, H. Garbe, and S. Potthast, “combination of the Failure Probability with a Random Angle of Incidence of the Radiated Interference,” in *Proceedings of XXX URSI General Assembly 2011*, Istanbul, Turkey, Aug. 2011. doi: 10.1109 / URSI-GASS.2011.6050709. ISBN 978-1-4244-6051-9 pp. 1-4.

[7] T. Peikert, “Predicting Vulnerability of IT systems for Electromagnetic Interference,” dissertation, Leibniz Universität Hannover. ISBN 978-3-86844-990-7 2018.

[8] E. Genender, “Risk Analysis of Systems in Electromagnetic Interference,” dissertation, Leibniz Universität Hannover. ISBN 978-3-8440-1525-6 2012.

[9] C. Baum, “How to think about EMP interaction,” in *Proceedings of the 1974 FULMEN Meeting, Air Force Weapons Laboratory, Kirtland AFB, New Mexico*, 1974.

[10] J. LoVetri and GI Costache, “An electromagnetic interaction modeling advisor,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 33, no.3, pp. 241-251, Aug 1991. doi: 10.1109 / 15.85138

[11] F. Sabath, “Classification of electromagnetic effects at system level,” *2008 International Symposium on Electromagnetic Compatibility - EMC Europe*, pp. 1-5, Sep. 2008. doi: 10.1109 / EMCEURO PE.2008.4786916

[12] F. Sabath and H. Garbe, “Risk potential of radiated HPEM environments,” *2009 IEEE International Symposium on Electromagnetic compatibility*, pp. 226-231, Aug. 2009. doi: 10.1109 / I-SEMC.2009.5284566

[13] ——, “Assessing the likelihood of various intentional electromagnetic environments the initial step of an IEMI risk analysis,” in *Electromagnetic Compatibility (EMC), 2015 IEEE International Symposium on*, Aug 2015. doi: 10.1109 / ISEMC.2015.7256319 pp. 1083-1088.

This project has received funding from the European Union’s EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

[14] ISO 31000, “Risk management - Principles and guidelines,” *International standard*, 2009.

[15] F. Sabath, “Lecture Notes WS2015 / 16 - Risk Analysis, Leibniz Hannover University.”

This project has received funding from the European Union’s EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/