Fuzzy-Based Risk Analysis for IT-Systems and Their Infrastructure

Tim Peikert, *Student Member, IEEE*, Heyno Garbe, *Fellow, IEEE*, and Stefan Potthast

Abstract—This paper introduces a procedural method based on the fuzzy logic and set theory, which analyzes the risk of an IT-System in a facility and its surrounding area. The method analyzes the susceptibility of an electronic system with respect to intentional electromagnetic interferences and classifies the intentional electromagnetic environment (IEME). It extends the well-known statistical-based models fault tree analysis, electromagnetic topology and Bayesian networks (BN) with imprecise data, uncertainness with linguistic terms, and opinions of experts. In a final step, the critical scenarios and the elements and the location that contribute most to the risk are identified, which can be used to enhance the protection level.

Index Terms—Decision making under risk, electromagnetic (EM) effects, fuzzy logic, fuzzy rules, fuzzy sets, intentional electromagnetic environment (IEME), intentional electromagnetic interference (IEMI), probabilistic risk analysis.

I. INTRODUCTION

THE vulnerability of failures of modern electronic systems has increased in the last decades by intentional electromagnetic interference (IEMI). One reason is the increasing dependence on computer networks, wireless communications, microelectronics, other sensitive electronic systems, and the strong interconnection between these different electronic devices. Partial failures of a system are able to lead to a malfunction of the total function based on that strong interconnection. Another reason is the growing risk of occurring of such high-power electromagnetic (HPEM) sources that range from simple homemade devices to advanced military sources.

The hazard of such IEMI scenarios is adopted by the "Resolution on criminal activities using electromagnetic tools" in 1999 by the URSI [1]. Later the scenario of IEMI is investigated in several scientific reports [2], [3]. Due to this

T. Peikert is with the Institute of Electrical Engineering and Measurement Technology, Leibniz Universität Hannover, Hannover 30167, Germany (e-mail: peikert@geml.uni-hannover.de).

H. Garbe is with the Institut fuer Grundlagen der Elektrotechnik und Messtechnik, Leibniz University of Hannover, Hanover 30167, Germany (e-mail: heyno.garbe@ieee.org).

S. Potthast is with the GF 330, Wehrwissenschaftliches Institut für Schutztechnologien-ABC-Schutz, Munster 29633, Germany (e-mail: stefanpotthast@bundeswehr.org).

situation, a protection from IEMI threats is necessary and therefore a systematic protection concept is needed.

To handle the risk assessment with its complexity and the strong interconnection of the IT infrastructure a statistical mathematical approach is needed for the risk analysis. Probabilistic risk analysis is a well-known method from the aerospace, chemical, and nuclear industries [4]. In 2013, a concept of stochastic modeling for HPEM risk at system level was introduced by Sabath [5] and Genender [6]. Therein, a procedural method for systematic analysis of these risks is presented.

The used statistical mathematical approaches to calculate the risk susceptibility of electronic systems under the condition of electromagnetic radiation are the fault tree analysis (FTA) by Genender [6], the electromagnetic topology (EMT), and the Bayesian networks (BN) by Mao [7].

These methods are limited by processing crisp data, which have to be set exactly and the probabilities have to be known. The risk analysis are often specified only vaguely and their probabilities are based on experts estimations. According to the complexity of IT-Systems and their dependent interconnection and the inherent uncertainty of all possibilities, the fuzzy numbers are an appropriate mathematical description of nonprecise data. Often only linguistic terms are used to describe the risk of systems, such as the HPEM risk assessment cube from Sabath [8], which is defined by the threat level, mobility (ML), and technological challenge. These terms could be transformed into fuzzy sets with different kinds of boundaries and membership functions. These soft or crossing boundaries are an advantage of the fuzzy probability theory. The fuzzy logic and set theory is used to determine the risk of a target system in a facility and its surrounding area. The approach (see Section II) turns every data into a computational mathematic. For that, the failure propagation is estimated for series and parallel circuits (see Section III) and the fuzzy rules (see Section IV) to combine the linguistic terms. The risk analysis based on the fuzzy theory (see Section V) divides the complexity in three parts: the breakdown failure probability of the victim system, the hazard of IEMI sources in zones of accessibility and a classification of the whole environment. An exemplary scenario (see Section VI) is used to discuss the approach to improve the protection against IEMI threats.

II. FUZZY APPROACH

The approach [9] is based on the set theory and the Boolean algebra. In 1965, Zadeh [10] introduced the fuzzy set as a model to deal with imprecise, inconsistent, and inexact information.
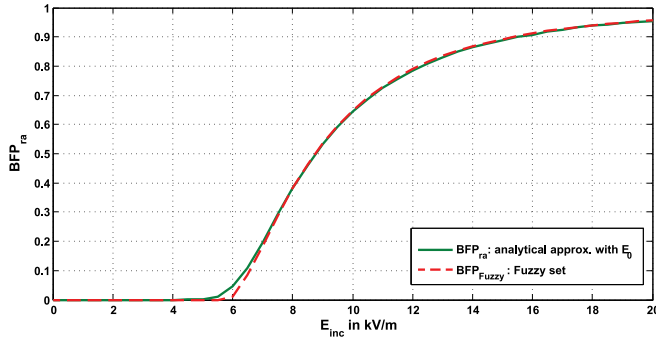
Fig. 1.   Breakdown failure probability with fuzzy sets [9].

(a)

(b)

Fig. 2.   Comparison of the membership for an element in the (a) classical (b) and fuzzy set theory.

(a)

(b)

Fig. 3.   (a) Serial and (b) parallel compound of a system.

A fuzzy set is a class of objects with a continuum of grades of membership. Zadeh [10] defines that a set $\tilde{A}$ of X is characterized by a membership function $\mu_A(x)$ that associates with each point in X a real number in the interval $[0, 1]$, with the values of $\mu_A(x)$ at x representing the grade of membership of x in $\tilde{A}$. The degree of x belonging to A is expressed with the following equation:

$$\tilde{A} = \{(x, \mu_A(x))|x \in X\} \text{ with } \mu_A : X \to [0, 1]. \quad (1)$$

Typical membership shapes are triangle, trapezoid, sigmoidal, or Gaussian bell. Further, more flexible classes of membership functions are possible [9], for example, the distribution density functions to describe the breakdown failure probability (BFP) or destruction failure probability [11] (DFP) of electronic systems. For example, the beta density function is used to estimate the BFP with a random angle of incident of a system and is written as follows:

$$\mu_{\text{BFP}}(x; \alpha, \beta) = \begin{cases} 0 & x \leq 0, \\ \int_0^x f(t; \alpha, \beta)dt & 0 < x \leq 1 \\ 1 & x > 1 \end{cases} \quad (2)$$

where $f(t; \alpha, \beta)$ is the standard beta probability density function (PDF)

$$f(t; \alpha, \beta) = \begin{cases} \frac{1}{B(\alpha, \beta)}t^{\alpha-1}(1-t)^{\beta-1} & 0 \leq t \leq 1 \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

and $B(\alpha, \beta)$ is the beta function with both the shape factors α and β, which defines the form of the shape, and x is the electromagnetic field strength normalized on the maximum (20 kV in Fig. 1), which is shown in Fig. 1.

The fuzzy logic is a multivalued logic and the known operator from the typical Boolean operations from the two-valued logic is not directly transferable, as similar aggregation operators, the union (maximum), intersection (minimum), and complement (negation) from the classical set theory, are used to combine the different fuzzy sets. Based on the Takagi and Sugeno model [12], the typically aggregation operators of two sets A as $\mu_A(x)$ and B as $\mu_B(x)$ are defined as follows:
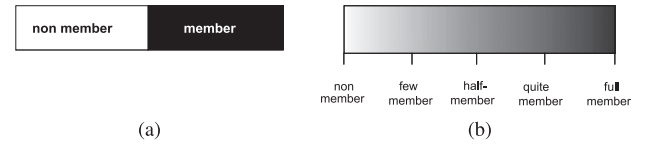
union : $A \cup B \Leftrightarrow \mu_{A \cup B}(x) = \mu_A(x) \cup \mu_B(x) =$
$\max\{\mu_A(x), \mu_B(x)\}$

intersection : $A \cap B \Leftrightarrow \mu_{A \cap B}(x) = \mu_A(x) \cap \mu_B(x) =$
$\min\{\mu_A(x), \mu_B(x)\}$

complement : $\hat{A} \Leftrightarrow \mu_{\hat{A}}(x) = 1 - \mu_A(x).$

The membership for an element differs between the classic and the fuzzy set theory. In Fig. 2, both types of membership of an element to a set are presented. In the classic set theory [Fig. 2(a)], an element is a member or not a member of the set. Instead the fuzzy set theory [Fig. 2(b)] defines a degree of membership to that set.

III. FAILURE PROPAGATION

The BFP of a single device is shown in Fig. 1, in which the breakdown depends on the magnitude of the electric field and for a typical waveform adopted from Genender [11]. Typical waveforms are damped sine wave pulse, double exponential pulse, burst, and continuous wave. Each of them leads to a different BFP and has to be considered for the estimation.

The failure of this system can propagate in a network to another device and can lead to a misbehavior or its malfunction. To estimate this effect of the failure propagation from one to another system, the different membership functions have to be combined.

Two different kinds of interconnection between two or more systems are possible. The first one is the serial circuit shown in Fig. 3 (a) and the second one is the parallel circuit shown in Fig. 3(b). The BFP of a compound of series interconnected systems is estimated with the maximum operator as follows:

$$\mu_{\text{series}}(x) = \max\{\mu_1(x), \mu_2(x), ..., \mu(x)_n|x \in X\}. \quad (4)$$

A failure of one subsystem leads to the breakdown of the entire system. The BFP for a parallel circuits of two or more
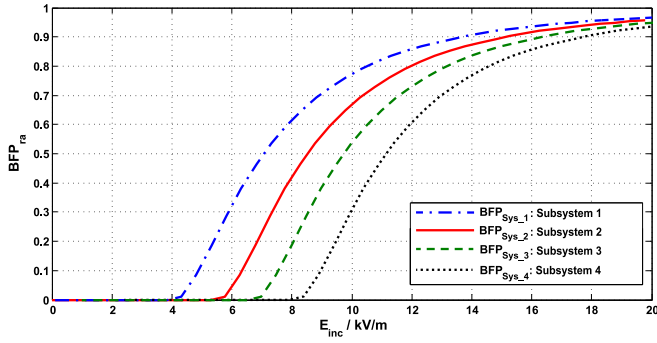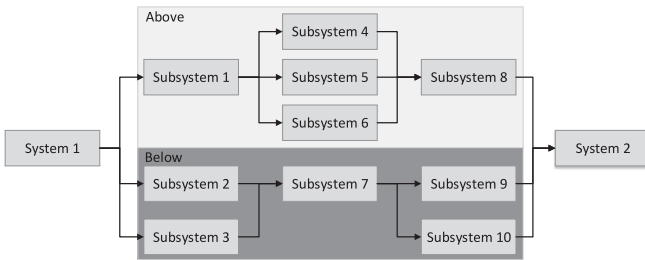
Fig. 4.   Four different BFPs.

Fig. 5.   Parallel compounds of a system.

subsystems is estimated with the minimum operator

$$\mu_{\text{parallel}}(x) = \min\{\mu_1(x), \mu_2(x), ..., \mu_n(x)|x \in X\}. \quad (5)$$

The entire system still works without any errors until every subsystem is disturbed. In Fig. 4, four different BFP functions are shown, with the result for the maximum operator $\text{BFP}_{\text{Sys}-1}$ and the minimum operator $\text{BFP}_{\text{Sys}-4}$. With the combination of serial and parallel elements, it is possible to estimate the failure propagation and its effect to complex systems composed of different subsystems, which are shown in Fig. 5.

The propagation path is divided into the above and below path and both are combined with the minimum operator (8). The first path (6) is composed of three serial elements, where one element is a parallel subsystem consisting of three devices. The below path in Fig. 5 is also composed of three elements connected in series in which the first and the last one is a parallel subsystem consisting of two elements

$$\mu_{\text{Above}}(x) = \max\{\mu_{\text{Sub1}}(x), (\min\{\mu_{\text{Sub4}}(x), \mu_{\text{Sub5}}(x),$$
$$\mu_{\text{Sub6}}(x)\}), \mu_{\text{Sub8}}|x \in X\} \quad (6)$$

$$\mu_{\text{Below}}(x) = \max\{(\min\{\mu_{\text{Sub2}}(x), \mu_{\text{Sub3}}(x)\}), \mu_{\text{Sub7}}(x),$$
$$(\min\{\mu_{\text{Sub9}}(x), \mu_{\text{sub10}}(x)\})|x \in X\} \quad (7)$$

$$\mu_{\text{System}}(x) = \min\{\mu_{\text{Above}}(x), \mu_{\text{Below}}(x)|x \in X\}. \quad (8)$$

IV.   FUZZY RULES

The combination of measurement data, PDFs and expert opinions defined in linguistic terms are achieved with the fuzzy rules. It is possible to combine these different kinds of input data in one mathematical model. This rules can be considered

TABLE I
EXAMPLE OF TWO RULES WITH THE MAMDANI METHOD [13]

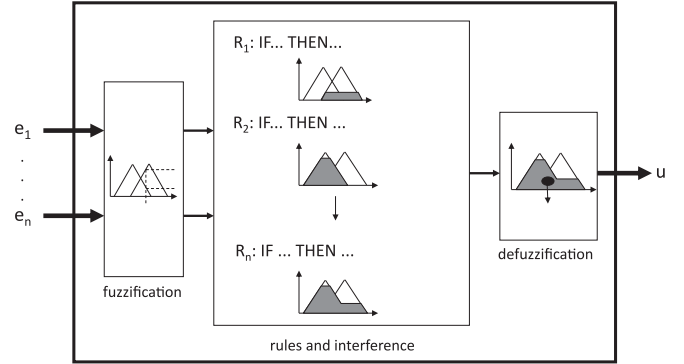| No.	Rule
R_1	IF x is A_1 AND y is B_1 THEN z is C_1
R_2	IF x is A_2 AND y is B_2 THEN z is C_2

Fig. 6.   Fuzzy rules with fuzzification and defuzzification [14].

as the knowledge of an expert who knows exactly the system behavior. These rules are represented by a sequence of the form IF-THEN and they associate a condition described by linguistic variables and/or fuzzy sets with a conclusion or an output. More than one input could be combined by the mentioned operators of Section II. The IF part is used to capture the knowledge by using the input conditions and the THEN part can be utilized to obtain the conclusion or output in linguistic variable form. An example for two typical fuzzy rules with two inputs is shown in Table I.

An example of using the rules to estimate risk with different inputs is shown in Fig. 6. The inputs (e_1 to e_n) are mapped on membership functions (fuzzification), the rules estimate the dependencies, and the defuzzification mapped, for example, the results on a risk-level metric.

V.   RISK ANALYSIS BASED ON FUZZY

The expression "risk" has different and misleading meanings; Genender [6] defines the risk as the probability of a hazardous and severity event. Sabath [15] categorizes the criticality of the IEMI effect in five linguistic categories that are as follows:
1) no effect or no consequence (undisturbed);
2) interference (limited);
3) degradation (severe);
4) loss of main function/mission kill (very severe); and
5) loss of system (catastrophically).

To analyze the risk of an IEMI scenario we need information about the victim system, the area plan of the infrastructure, and the possible IEMI sources that can harm the investigated system. For the last point, many data are published, for example by Mora [16] and Sabath [17]. The last one is mostly bonded to their places and is highly improbable to disturb the victim system. Sabath [8] classifies the sources in ML, technology challenge

TABLE II
HL OF SOURCES AND ML LEVEL [9]

HL	Description	Amplitude	ML	Description
XL	low	$< 0{,}1\,\text{kV/m}$	1	stationary
L	little	$0{,}1\text{–}1\,\text{kV/m}$	2	transportable
M	middle	$1\text{–}10\,\text{kV/m}$	3	mobile
H	high	$10\text{–}100\,\text{kV/m}$	4	very mobile
XH	very high	$> 100\,\text{kV/m}$	5	highly mobile
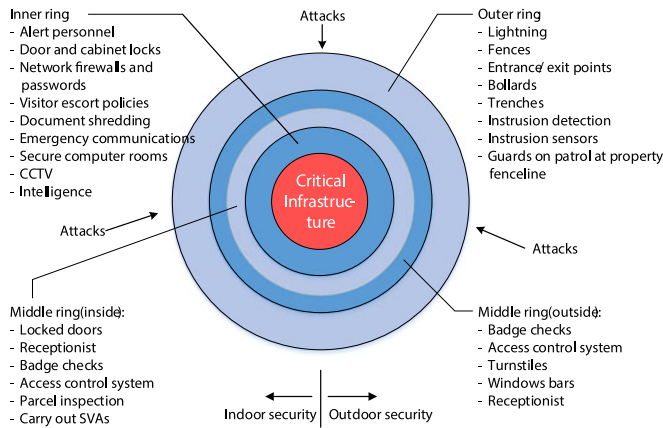
Fig. 7. Security rings of protection [9].
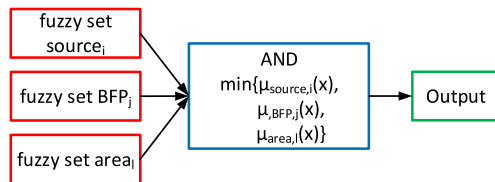
Fig. 8. Combination of the three main fuzzy sets [14].

Fig. 9. Fuzzy Sets for the probability of occurrence for IEMI sources [9]: (a) membership function and (b) $\min\{\mu_{\text{TC}}, \mu_{\text{HL}}, \mu_{\text{FoE}}, \mu_{\text{ML}}\}$.
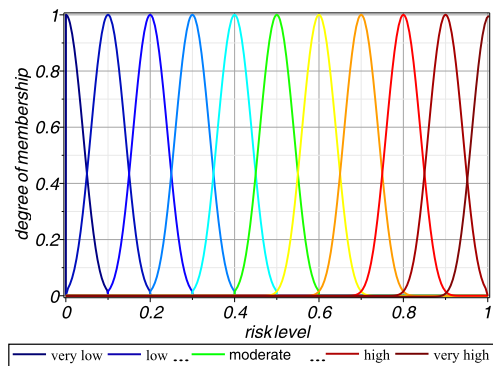
Fig. 10. Fuzzy set for the risk-level membership functions [14].

(TC), availability, and its hazard level (HL). The classification for the ML and the HL is shown in Table II .

The ML of an IEMI source is described as the capability of that source to come close to the victim system. Genender [6] defined the aspect ML as the compiled aspects such as dimensions, weight, need of special supplies, integrability into platforms systems or shelters, and the ability to operate in motion.

The area plan of the infrastructure with the surrounding area and the buildings have to be studied and divided into zones of accessibility. The security rings of protection in Fig. 7 by Peikert [9] are used for the zoning of the area.

The last important point is the breakdown failure behavior of the desired system. Therefore, measurements (see Fig. 1) and expert opinions are needed to classify the BFP of the system.

If every data and terms are obtained, everything has to be turned into fuzzy membership functions. In the beginning, the three categories, the area plan, the intentional electromagnetic environment (IEME) sources, and the BFP of the whole system are calculated and everything is combined at the end with the intersection operator, as shown in Fig. 8 . The susceptibility of the whole system has to be estimated. Therefore, the victim

system is divided into subsystems and the dependencies between each subsystem have to be determined. The result for the whole system is obtained with the union of each subsystem BFP, n and is expressed as follows:

$$\mu_{\text{BFP,total}} = \max\{\mu_{\text{BFP},1}, \mu_{\text{BFP},2}, ..., \mu_{\text{BFP},n}\}. \tag{9}$$

The probability of occurrence of an IEMI source is determined by the TC of such sources, the availability, the ML, its HL, and the frequency of event (FoE). The estimation with the fuzzy theory approach is shown by Peikert [9] and in Fig. 9 , where one combination of the each membership function and its intersection result is presented.

Finally, an outline of the surrounding area with its buildings is required. The location of the system under consideration has to be determined and the zones of accessibility have to be integrated into the plan. At the end, each result has to be mapped onto the risk-level membership function. The risk level, shown in Fig. 10 , is divided into 11 parts, it starts with no risk, passes in the middle the moderate risk, and ends with very high risk.

VI. SCENARIO FOR THE FUZZY APPROACH

A map with accessibility zones and classified ML levels [Fig. 11(a)] for these zones by Genender [6] are used as a scenario for the risk analysis approach. The analysis of the scenario is divided into the analysis of the target system, the sources of disturbance and the environment.
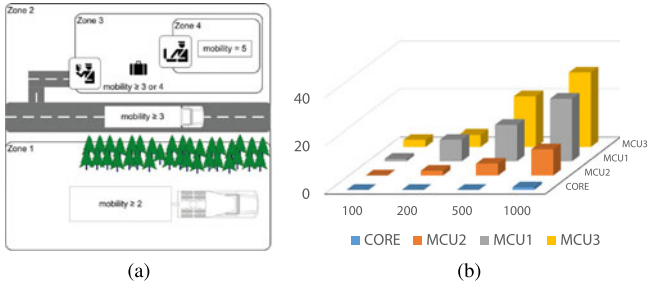
Fig. 11. (a) Accessibility zones and classified ML levels for these zones needed by Genender [6] and (b) failure rate of an MCU compound by Peikert [14].

Fig. 12. (a) Mapping of the availability on the probability of occurrence and (b) the mapping of the cost on the probability of occurrence by Sabath [20] (gray bar: expert valuation; dashed line: approximated function).

TABLE III
SCALE FOR AVAILABILITY (SfA) (COMPONENTS AND/OR SOURCE) BY SABATH [20]

| AV_c^a	Availability category	Description
1	Off-the-shelf	Available in the commercial marketplace (e.g., department stores); can be bought by anyone
2	Commercially available	Available in specialty stores; can be bought by anyone
3	Specialized trade	Available only in specialized trading companies; acquisition is limited to commercial customer
4	Limited acquisition	Limited acquisition under conditions or to registered buyer, special designed components
5	Restricted acquisition	Trade or acquisition prohibited by law

A. Target System

As a victim system, a complex compound of microcontroller (MCU) are used, in which breakdown failure probability is studied by Peikert [14]. In Fig. 11(b), the number of failures are shown for the compound after exposing with a double exponential pulse. As a pulse generator, the PBG7 from the company Kentech is used as an IEMI source. The compound in Fig. 11(b) is exposed in a GTEM cell for one minute with 100, 200, 500, or 1000 pulses and the level of each column stands for the number of breakdowns. This measurement setup is used to determine the BFP for the MCU compound. The setup comprises a core unit, which communicates and analyzes every other unit (MCU1, MCU2, and MCU3). MCU1 is used as a system of three in series, which needs the calculation result from the unit before. MCU2 is designed as a redundant system and MCU3 works with different communication protocols (twi, spi, and ethernet). BFP of the whole system is calculated from the measurements of each subsystem and every result is combined with the union operator:

$$\mu_{\text{BFP,MCU1}} = \max\{\mu_{\text{BFP,MCU1}-1}, \mu_{\text{BFP,MCU1}-2},$$
$$\mu_{\text{BFP,MCU1}-3}\} \qquad (10)$$

$$\mu_{\text{BFP,MCU2}} = \max\{\mu_{\text{BFP,MCU2}-1}, \mu_{\text{BFP,MCU2}-2},$$
$$\mu_{\text{BFP,MCU3}-3}\} \qquad (11)$$

$$\mu_{\text{BFP,MCU3}} = \max\{\mu_{\text{BFP,MCU3}-1}, \mu_{\text{BFP,MCU3}-2},$$
$$\mu_{\text{BFP,MCU3}-3}\} \qquad (12)$$

$$\mu_{\text{BFP,total}} = \max\{\mu_{\text{BFP,core}}, \mu_{\text{BFP,MCU1}},$$
$$\mu_{\text{BFP,MCU2}}, \mu_{\text{BFP,MCU3}}\}. \qquad (13)$$

B. Classification of the IEMI Source

Mora [16] published a list of existing IEMI sources and gathered the information of peak field, rise-time, technology level by Giri [18], the cost level by Sabath [8], the probability level of ITU [19], and more for the most available sources. The fuzzy theory approach to classify the probability of occurrence and the risk level is shown in the work of Peikert [9]. These classifications consider the four categories of HL, ML level, availability, and TC. Sabath [20] discusses a technique that enables the assessment of key parameters of various IEMEs. With his technique, Sabath estimates the likelihood that an offender has access to such an IEMI source. Some of the experts' opinions for the availability are shown in Fig. 12 (a) and the costs are shown in Fig. 12(b). The used categories and the meanings of the availability are shown in Table III .

Extending the approach of Peikert [9], with the additional experts opinion from Sabath [20], delivers a new rate of the risk level of an IEMI source. Therefore, the fuzzy sets for the kind of sources that are possible (14) are combined with the achievable values of field magnitude next to the target system (15) and the sets for the expert opinions (16)

$$\tilde{A}_{\text{field}} = \{(x, \mu_{\text{field}}(x)) | x \in X\} \qquad (14)$$

$$\tilde{A}_{\text{source}} = \{(x, \mu_{\text{source}}(x)) | x \in X\} \qquad (15)$$

$$\tilde{A}_{\text{expert}} = \{(x, \mu_{\text{expert}}(x)) | x \in X\}. \qquad (16)$$

As an example, the combination of the SfA, scale for required knowledge (SfrK), cost scale (CS), and the level of sophistication (LoS) lead to the TC of an IEMI source shown in Fig. 13 . The results are the linguistic terms low tech., medium tech., high tech., and highly sophisticated systems according to Sabath [5] and are used to estimate the HL of this combination for such source. An example for the used fuzzy rules to combine the inputs are shown in Table IV .

With the different fuzzy systems of the TC, IEMI sources, and some more according to the published characteristics of Sabath [5], Mansson [21], [22], and Giri [18], the type of the IEMI source and its possible output power range can be estimated. The used MATLAB–Simulink model is shown in Fig. 14 . This model combined the results of the three fuzzy systems: ML and

Fig. 13.   Fuzzy system for the TC.

TABLE IV
EXAMPLE OF FUZZY RULES FOR THE TC

No.	Rule
R_1	IF (SfA is restricted acquisition) AND (SfrK is expert) AND (CS is extreme cost) AND (LoS is de-velopment group) THEN (TC is highly sophisticated)
R_2	IF (SfA is of-the-shelf) AND (Sfrk is novice) AND (CS is low cost) AND (LoS is open literature) THEN (TC is low tech system)
R_3	IF (SfA is commercial available) AND (Sfrk is specialist) AND (CS is increased cost) AND (LoS is technical literature) THEN (TC is medium tech system)

Fig. 14.   MATLAB–Simulink model for the estimation of the risk from the inputs ML, TC, and LoD.

accessibility, likelihood of detection, and the TC. The obtained results imply the risk that arises from that type of HPEM source. These are used to predict the risk level of the investigated system.

The risk level for the target system is addicted to the measured electromagnetic stress level of every MCU and is estimated by beta distribution in (2) and (3). The fuzzy sets for each BFP and

Fig. 15.   Risk level in dependence on the field and probability of occurrence of an IEMI source by Peikert [9].

its dependence on other ones are obtained with the following equation:

$$\tilde{A}_{\text{BFP}} = \{(x, \mu_{\text{BFP}}(x))|x \in X\} \text{ and} \tag{17}$$

$$\tilde{A}_{\text{depending}} = \{(x, \mu_{\text{depending}}(x))|x \in X\}. \tag{18}$$

The risk level of the victim system is addicted to its own electromagnetic stress level, the dependence between all subsystems, the achievable field magnitude, and the probability of occurrence of an IEMI source that can deliver that field magnitude. After mapping the results onto the risk-level membership function in Fig. 10, we obtain that the risk depends on the probability of occurrence and the amplitude of the electromagnetic field, which is shown in Fig. 15 .

C. Classification of the IEME

Now, the estimation for the risk level of the combined target system and sources with their achievable field magnitude have to be combined with the area map with its accessibility zones and required ML shown in Fig. 11(a). The target system is located in the accessibility zone number five with the highest limitation for the ML level. It is located in a building with the ML higher than four. The area is bounded by a fence and is categorized with three or higher. The zone in the line of sight of the building and its surrounding area is categorized with the level equal to three or higher. Everything out of sight has the ML level two or lower. The lowest level needs a stationary building and is disregarded in this scenario.

The zones represented the discoverability of an IEMI sources, which affect the rate of the HL. The higher the rate of ML level of a zone, the more likely the source can be detected by a security measure and the lower the rate of the HL. To integrate the dependence of hazard and ML in the zones, a fuzzy set for the limitation of the five zones is used. Therefore, a trapezoidal membership function with the boundaries a and b is used and expressed as follows:

$$\mu_{\text{zone},i}(x) = \begin{cases} 1 & x \leq a, \\ \frac{b-x}{b-a} & a < x \leq b, \\ 0 & x > b. \end{cases} \tag{19}$$

TABLE V
VALUES FOR a AND b FOR THE AREA MEMBERSHIP FUNCTION

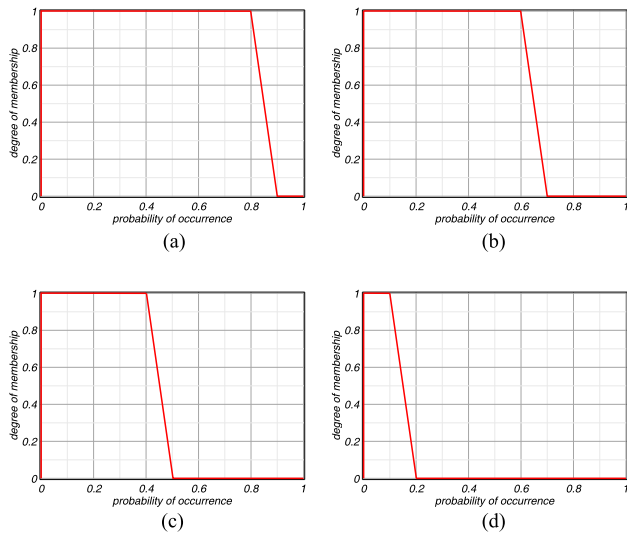|	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
$a =$	1	0.8	0.7	0.4	0.1
$b =$	–	0.9	0.6	0.5	0.2

Fig. 16. Four limitation fuzzy membership functions for the zones of the map. (a) Zone 1. (b) Zone 1. (c) Zone 1. (d) Zone 1.

The used boundary factors a and b for the membership function are shown in Table V. The resulting fuzzy sets for the zone number 1–4 are shown in Fig. 16. In the following step, a grid of squares is added as a layer on the map of the area. For every square, the distance from its center to the center of the target system is estimated. The size of the squares is chosen in order to cover the area well and establish transitions between the accessibility zones as a boundary between two squares. Each square obtained the following data:

1) zone number;
2) boundary to another zone;
3) HL;
4) ML level;
5) distance to target system;
6) resulting field magnitude.

These data are used to assess the field magnitude with the far-field condition that leads to an attenuation of the field strength by a factor of $1/r$, in which r is the distance from the center of the square to the center of the victim system. The result is a matrix of values for the maximum possible peak amplitude which might radiate from a square to the target system. The magnitude values of every square are compared with the breakdown failure probability of the system and are mapped on the risk-level membership function in Fig. 10.

D. Fuzzy Approach Result

From the results of Sections VI-A–VI-B, with the field strength and breakdown failure behavior of the target system, a

TABLE VI
RISK ESTIMATION OF AN EVENT [9]

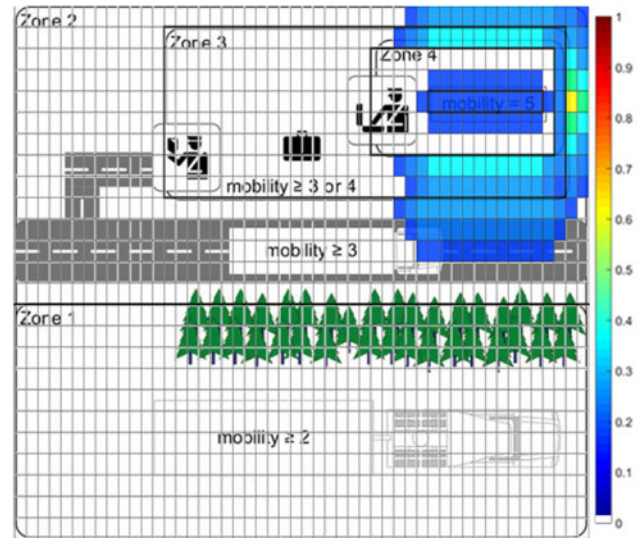| Risk level	Probability of Damage	Criteria
0–1	No risk	Occurrence of the damage is unlikely
2–4	Low	Occurrence of the damage is low
5–7	Moderate	Occasionally occurring damage
8–9	High	Damage occurs in more than half of the exposure
10–11	Very high	Occurs in almost every exposure

Fig. 17. Layer of the risk-level metric overlaid on the area map [14].

risk-level metric is created. The risk-level metric is divided into 11 subregions from zero to one. Zero is the lowest risk level, what represents the IEMI sources that are not able to harm the victim system. The highest rate of the level, specified with one, leads to a damage of the system in almost every exposure. A detailed list is shown in Table VI.

In means of the risk-level metric, a colored square mesh is created. The colorbar starts with white or no color (no risk), it follows blue as low risk, moves to yellow (moderate risk), and ends with dark red (very high risk). This mesh is added as a layer on the area map of the zone of accessibility [Fig. 11(a)] and shown in Fig. 17. This map shows locations in which an IEMI source can harm the victim system. In this example, the victim system is located in the upper right corner of the area and an IEMI source in zone number two, on the right-hand side of the victim system, has a risk level of 0.6 to harm the system. This location is a point of interest for a high protection level of the system and it has to be considered in the EMC shielding of the system.

VII. CONCLUSION

An approach based on fuzzy logic and set theory, which extends the well-known risk analysis method, EMT, FTA, and BN to handle nonprecise data and uncertainness of linguistic terms with the fuzzy set theory, is introduced. The method adds subjective information, uncertain data, nonphysical quantities,

crossing boundaries, and the opinion of experts to the assessment of risk, which can still be simulated with a numerical or analytical math program. The approach divides an IEMI scenario into the breakdown behavior of the target system, categorizes the IEMI sources regarding to the zone of accessibility, and classifies the IEME with its surrounding area and buildings. The combination of these three parts leads to the end of a risk-level metric, which defines locations for sources that can harm the victim system. This information can be used to increase the protection level of the investigated system.

REFERENCES

[1] URSI, "Resolution on criminal activities using electromagnetic tools," URSI resolutions adopted at the Toronto general assembly, 1999. [Online]. Available: http://www.ursi.org/

[2] W. Radasky, C. Baum, and M. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)," *IEEE Trans. Electromagn. Compat.*, vol. 46, no. 3, pp. 314–321, Aug. 2004.

[3] M. Bäckström, B. Nordström, and K. G. Lövstrand, "Is HPM a threat against the civil society?" in *Proc. 27th Gener. Assem. URSI*, Maastricht, The Netherlands, Aug. 2002, pp. 453–456.

[4] T. Bedford and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge, U.K.: Cambridge Univ. Press, 2001.

[5] F. Sabath and H. Garbe, "Concept of stochastic modeling for high-power electromagnetics (HPEM) risk analysis at system level," in *Proc. 2013 IEEE Int. Symp. Electromagn. Compat.*, Aug. 2013, pp. 401–406.

[6] E. Genender, H. Garbe, and F. Sabath, "Probabilistic risk analysis technique of intentional electromagnetic interference at system level," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 1, pp. 200–207, Feb. 2014.

[7] C. Mao and F. Canavero, "System-level vulnerability assessment for EME: From fault tree analysis to Bayesian networks—Part I: Methodology framework," *IEEE Trans. Electromagn. Compat.*, vol. 58, no. 1, pp. 180–187, Feb. 2016.

[8] F. Sabath and H. Garbe, "Risk potential of radiated HPEM environments," in *Proc. 2009 IEEE Int. Symp. Electromagn. Compat.*, Aug. 2009, pp. 226–231.

[9] T. Peikert, H. Garbe, and S. Potthast, "A fuzzy approach for IEMI risk analysis of IT-Systems with respect to transient disturbances," in *Proc. 2015 IEEE Int. Symp. Electromagn. Compat.*, Aug. 2015, pp. 1077–1082.

[10] L. Zadeh, "Fuzzy sets," *Inf. Control*, vol. 8, pp. 338–353, 1965.

[11] 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 *Proc. 2011 XXXth URSI Gener. Assem. Sci. Symp.*, Aug. 2011, pp. 1–4.

[12] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," *IEEE Trans. Syst., Man Cybern.*, vol. SMC-15, no. 1, pp. 116–132, Jan. 1985.

[13] M. Mizumoto and K. Tanaka, "Fuzzy sets and their operations," *Inf. Control*, vol. 48, no. 1, pp. 30–48, 1981. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0019995881905787

[14] T. Peikert, H. Garbe, and S. Potthast, "Electromagnetic environment and interference risk analysis with a fuzzy-logic approach of a complex installation," in *Proc. U.R.S.I. Landesausschuss in der Bundesrepublik Deutschland e.V. Kleinheubacher Tagung*, 2015, pp. 91–96, doi: 10.5194/ars-14-91-2016.

[15] F. Sabath, "Classification of electromagnetic effects at system level," in *Proc. 2008 Int. Symp. Electromagn. Compat.*, Sep. 2008, pp. 1–5.

[16] N. Mora, F. Vega, G. Lugrin, F. Rachidi, and M. Rubinstein, "Study and classification of potential IEMI sources," System design and assessment (EMP-5), Tech. Rep. 41, Baum Notes 41 and EMC Laboratory, Swiss Federal Institute of Technology in Lausanne (EPFL), Lausanne, Switzerland, Jul. 2014. [Online]. Available: http://ece-research.unm.edu/summa/notes/SDAN/0041.pdf

[17] F. Sabath *et al.*, "Overview of four European high-power microwave narrow-band test facilities," *IEEE Trans. Electromagn. Compat.*, vol. 46, no. 3, pp. 329–334, Aug. 2004.

[18] D. Giri and F. Tesche, "Classification of intentional electromagnetic environments (IEME)," *IEEE Trans. Electromagn. Compat.*, vol. 46, no. 3, pp. 322–328, Aug. 2004.

[19] High-Power Electromagnetic Immunity Guide for Telecommunication Systems, ITU Std. K. 81, 2014. [Online]. Available: https://www.itu.int/rec/T-REC-K.81-201408-I/en

[20] F. Sabath and H. Garbe, "Assessing the likelihood of various intentional electromagnetic environments the initial step of an IEMI risk analysis," in *Proc. 2015 IEEE Int. Symp. Electromagn. Compat.*, Aug. 2015, pp. 1083–1088.

[21] D. Mansson, R. Thottappili, and M. Backstrom, "Methodology for classifying facilities with respect to Intentional EMI," *IEEE Trans. Electromagn. Compat.*, vol. 51, no. 1, pp. 46–52, Feb. 2009, doi: 10.1109/TEMC.2008.2010327.

[22] D. Mansson, M. Backstrom, and R. Thottappillil, "Classifying facilities with respect to intentional EMI," in *Proc. 2009 IEEE Int. Symp. Electromagn. Compat.*, Aug. 2009, pp. 249–254.

Tim Peikert (S'13) was born in Hanover, Germany, in 1981. He received the Dipl.-Ing. degree in electrical engineering from the Leibniz Universität of Hanover, Hanover, Germany, in 2011. He is currently working toward the Dr.-Ing. degree in electromagnetic compatibility in the Department of Electrical Engineering and Measurement Technology from the Leibniz Universität of Hanover.

From 2013 to 2016, he was the Chairman of the IEEE Student Branch Hanover. His research interests include high-frequency measurement techniques with respect to the susceptibility of electronic systems and the risk estimation of the vulnerability of electronic devices. Especially, the investigation of IT networks and other large systems exposed to intentional electromagnetic interference.

Heyno Garbe (M'89–SM'96–F'06) was born in Germany in 1955. He received the Dipl.-Ing. and Dr.-Ing. degrees both in electrical engineering from the University of the Federal Armed Forces, Hamburg, Germany, in 1978 and 1986, respectively.

From 1986 to 1991, he was in the Asea Brown Boveri Research Center, Baden, Switzerland, where he was involved in several research activities on EMC-related topics. From 1991 to 1992, he was the Head of EMC Baden Ltd, Baden, Switzerland. Since 1992, he has been at the Leibniz University of Hanover, Hanover, Germany, where he is currently a Full Professor in the Department of Electrical Engineering and Informatics and Computer Science and holds the Chair of Electromagnetic Compatibility.

Prof. Garbe is very active in several EMC-related national and international standardization committees. He has been elected as an EMP-Fellow. He received the Laurence G. Cumming Award for Outstanding Service, 2003, the Richard R. Stoddard Award for Outstanding Performance, 2010, and the Honorary Life Membership, 2006 from the IEEE Electromagnetic Compatibility Society. Since 1994, he has been a member of the editorial board of the IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY. From 2010 to 2012, he was the Editor-in-Chief of the IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY. In 2015, he was elected as the Vice President of Communication Services for the IEEE Electromagnetic Compatibility Society.

Stefan Potthast was born in Paderborn, Germany. He received the Dipl.-Phys. degree in physics from the University of Paderborn, in 2003, and the Ph.D. degree in physics from the Department of Physics, University of Paderborn, Paderborn, Germany, in 2007, where his research activities included epitaxial growth of cubic GaN and AlGaN and the design of a AlGaN-/GaN-based HEMT.

In 2007, he joined the Federal Office of Defense Technology and Procurement (BWB). Since 2008, he has been in the Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS), Munster, Germany, in the Electromagnetic Effects Branch. His current research focuses on the influence of electromagnetic fields on electronic components and equipment.