Adv. Radio Sci., 9, 297–302, 2011
www.adv-radio-sci.net/9/297/2011/
doi:10.5194/ars-9-297-2011

Advances in Radio Science

Fault tree analysis for system modeling in case of intentional EMI

E. Genender[1], M. Mleczko[1], O. Döring[1], H. Garbe[1], and S. Potthast[2]

[1]Institute of Electrical Engineering and Measurement Technology, Leibniz Universität Hannover, Hannover, Germany
[2]Bundeswehr Research Institute for Protective Technologies and NBC-Protection Munster, Germany

Abstract. The complexity of modern systems on the one hand and the rising threat of intentional electromagnetic interference (IEMI) on the other hand increase the necessity for systematical risk analysis. Most of the problems can not be treated deterministically since slight changes in the configuration (source, position, polarization, ...) can dramatically change the outcome of an event. For that purpose, methods known from probabilistic risk analysis can be applied. One of the most common approaches is the fault tree analysis (FTA). The FTA is used to determine the system failure probability and also the main contributors to its failure. In this paper the fault tree analysis is introduced and a possible application of that method is shown using a small computer network as an example. The constraints of this methods are explained and conclusions for further research are drawn.

1 Introduction

The complexity of modern electronic systems such as IT networks does not allow to examine the susceptibility of that systems against intentional EMI (IEMI) solely deterministically (Garcia, 2008; Mansson et al., 2009; Holland and John, 1999). The reason for this are the uncertainties associated with the analysis:

- Sources: There are a lot of different types of sources with different characteristics (Giri and Tesche, 2004). To each source the system might respond differently.
- Coupling paths: Depending on the position of the source or its orientation different coupling paths are dominant.
- System behavior: For the same source, same position and same orientation the system might fail or not, which is a random event regarding the huge number of internal states of the system (Camp et al., 2004).

The aspects described above are typically out of analysts control. It is not possible to determine which type of source the attacker is going use or how he is going to position it. Hence, these uncertainties need to be treated statistically. Furthermore, there are aspects which can be determined exactly however because of the complexity of the system have to be estimated. The electromagnetic field inside a shielded room depends on so many factors that the deterministic calculation becomes impossible. The application of worst case scenarios and safety factors will make the system overprotected and thus too expensive. That is why simple hardening against all sources and all possible situations cannot be done. Furthermore, the question about the risk that the systems is exposed to remains still unanswered. Hence, the system needs to be analyzed statistically taking the uncertainties into consideration.

Methods for analyzing the system reliability and risk have been developed and used for many years. Especially the nuclear and the aerospace industries have made a lot of progress in this area (Stamatelatos, 2002). When analyzing the risk of a complex system it is important to proceed systematically. For that, the fault tree analysis (FTA) is an important tool. In Sect. 2 a short introduction to fault tree analysis is given. Then in Sect. 3 a computer network is introduced for which the reliability analysis is carried out. Section 4 is the main section and discusses how the fault tree for the computer network can be developed. First the functional and then IEMI specific dependencies are modeled. The restrictions of FTA associated with that are discussed.

2 Fault tree analysis

It is difficult to predict the failure probability of the whole system in a certain electromagnetic environment at once. By decomposing its failure behavior in smaller scenarios the description becomes possible. This principle is also used in

Correspondence to: E. Genender (genender@ieee.org)

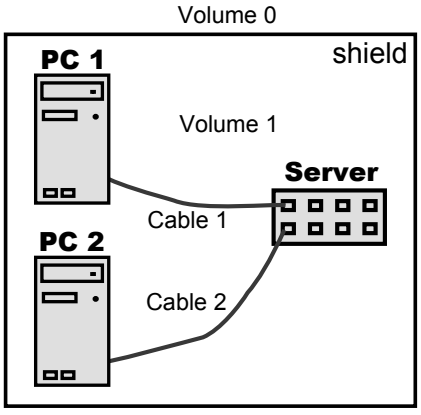

Fig. 1. Network which reliability is to be determined.

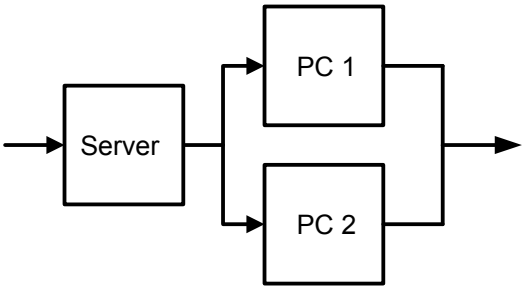

Fig. 2. Reliability block diagram for the network from Fig. 1.

the electromagnetic topology concept. In order to analyze the system reliability the fault tree analysis (FTA) can be applied (Vesely, 2002). Using the FTA for analyzing a system exposed to an EMP was first mentioned by National Research Council (1984). However, as far as the authors know, FTA has never been applied for that purpose. The FTA is a deductive method: beginning with an undesired event (also called the top event) the FTA is used to find the causes for this top event. When determining the causes, a fault tree is constructed from top to bottom. For its construction several symbols are used that indicate the relation between different events. The main symbols are presented in Table 1.

3 Computer network under test

In order to present the application of FTA, a computer network is introduced in Fig. 1. The network is placed in a (shielded) room and consists of one server and two computers (PCs). The two PCs are connected to the server. Both PCs fulfill the same function and are thus redundant. Now the task is to analyze the system reliability when it is exposed to an electromagnetic interference. It is assumed that the interference source is outside of the shielded room.

The first step of the analysis is to determine the functional dependencies of the system. A reliability block diagram is used to visualize the dependency of the overall system on the functionality of its elements. Each element of the system is represented by a block. The blocks are connected depending on their function in the system. A serial connection of two blocks means that both blocks are needed for the successful operation of the system. A parallel connection of blocks means that at least one of the blocks is needed. The system operates successfully if a path between the left and the right end of the reliability block diagram exists in which all blocks are functioning. The reliability block diagram for the introduced computer network is shown in Fig. 2.

Table 1. Fault tree symbols.

Symbol	Name	Meaning
	Intermediate Event	An event is caused by combination of other events
	Basic Event	A basic event requiring no further development
	AND Gate	Output occurs if all of the input events occur
	OR Gate	Output occurs if at least one of the input events occurs

4 Fault tree analysis of the computer network

4.1 Fault tree for system failure

At the beginning of each FTA the top event is defined. For this event the causes are then determined successively. For the network under test different events might be defined. The determination of all possible top events cannot be done with FTA. For that other tools need to be used. Possible top events could be permanent damage of the network, degradation of the performance, temporal uncontrollability of the network and so on. In this paper the top event is simply defined as the failure of the whole system which is denoted as F_{Sys}.

From the reliability block diagram in Fig. 2 it is concluded that the system fails, if the server fails or the redundant (parallel) system consisting of the two PCs fails. That relation is depicted in Fig. 3 by the OR connection of the events *Server fails* F_{Ser} and *Redundant system (PC1&2) fails* $F_{\mathrm{PC1\&2}}$. The event $F_{\mathrm{PC1\&2}}$ is further developed as the AND connection of the events F_{PC1} and F_{PC2}. Using Boolean algebra the system failure event can be described as:

$$\begin{aligned} F_{\mathrm{Sys}} &= F_{\mathrm{Ser}} \cup F_{\mathrm{PC1\&2}} \\ &= F_{\mathrm{Ser}} \cup (F_{\mathrm{PC1}} \cap F_{\mathrm{PC2}}) \end{aligned} \quad (1)$$

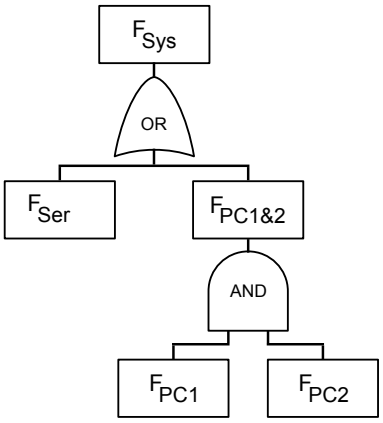

Fig. 3. Fault tree for the top event *System fails* F_{Sys}.

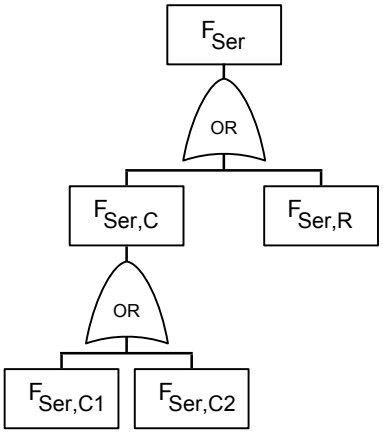

Fig. 4. Fault tree for the top event *Server failed*.

4.2 Fault tree for the server failure event

The fault tree which is developed until here is not directly related to IEMI problems and the main focus is on functional dependencies. The causes of the bottom events in Fig. 3 however are related to IEMI. For each of the bottom events a fault tree needs to be developed. In this paper we take a closer look at the failure behavior of the server F_{Ser}. Hence, the new top event is defined as *Server failed* (F_{Ser}). The fault tree which is going to be developed for this event can later just be attached at the corresponding position of the fault tree in Fig. 3.

Typically, electric equipment can be disturbed by radiated or conducted interference. Hence, the next step is to model the failure of the server as an OR connection of the events *Server failed through conducted disturbance* ($F_{\mathrm{Ser,C}}$) and *Server failed through radiated disturbance* ($F_{\mathrm{Ser,R}}$), see Fig. 4.

Those two events require further analysis. In Fig. 1 it can be seen that two cables are connected to the server. Hence, the event *Server failed through conducted disturbance* ($F_{\mathrm{Ser,C}}$) can be developed as the combination of the events *Server failed through conducted disturbance on cable 1* ($F_{\mathrm{Ser,C1}}$) and *Server failed through conducted disturbance on cable 2* ($F_{\mathrm{Ser,C2}}$). The top event has been decomposed into lower level events that are easier to analyze for themselves. Using Boolean algebra the server failure event can be described as:

$$\begin{aligned} F_{\mathrm{Ser}} &= F_{\mathrm{Ser,C}} \cup F_{\mathrm{Ser,R}} \\ &= F_{\mathrm{Ser,C1}} \cup F_{\mathrm{Ser,C2}} \cup F_{\mathrm{Ser,R}} \end{aligned} \tag{2}$$

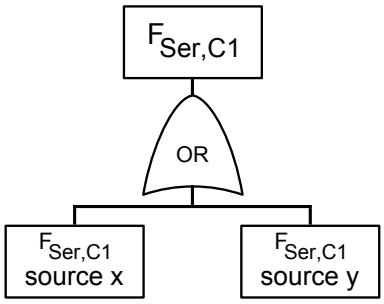

Fig. 5. Fault tree for the event *Server failed through conducted disturbance on cable 1*.

4.3 Fault tree for the server failure through disturbance on cable 1

At this point there is a need to know how susceptible the server at different ports is. The susceptibility of each port depends on the type of the source. In Brauer et al. (2009) it is shown that different types of cables are susceptible to different types of pulses. For example in Brauer et al. (2009) it is shown that, an ultra wideband (UWB) source couples well to network cables, damped sinusoid (DS) source to power supply and high power microwave (HPM) into the casing of the analyzed equipment. Hence, at this point of the fault tree failures through different sources are distinguished. For each cable only those sources need to be taken into consideration, which are important for this type of cable. In this paper the event *Server failed through conducted disturbance on cable 1* ($F_{\mathrm{Ser,C1}}$) is further developed. It is assumed that the server is susceptible on cable 1 to source x and sources y, which is depicted in the fault tree in Fig. 5.

In order for the server to fail through source x this source needs to occur and given the presence of the source x the server has to fail. Let's assume that the source is a high-altitude EMP (HEMP). This event has a very low probability, let's say 1%. However, given the occurrence of the source the probability that the server fails is very high, let's say 80%. Then the probability of the server to fail through a HEMP is $0.01 \cdot 0.8 = 0.008$. This relation can be depicted as an AND connection as can be seen in Fig. 6.

As both events at the bottom of the fault tree are basic events the fault tree development for this branch is finished

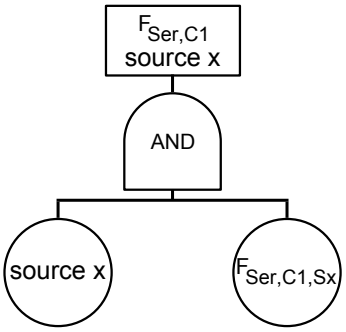

Fig. 6. Fault tree for the event *Server failed through conducted disturbance on cable 1 through source X*.

and has to be continued for other branches. When all branches are finished the fault tree can be solved.

5 Solution and restrictions of the fault tree

The fault tree is developed top-down and solved bottom-up. This means that the probabilities of the basic events have to be defined and then propagated through the fault tree. In the fault tree in Fig. 6 the basic events are the probability of the source and the failure probabilities of the elements given a certain source. These basic events are analyzed in the following.

5.1 Source likelihoods

In order to determine the source likelihoods (Sabath and Garbe, 2009) suggest to evaluate the mobility and the technological challenge of a source. The smaller and lighter the source is the higher is its mobility. The technological challenge combines quantities such as the level of knowledge needed to design or operate the system, availability of components and costs. The lower the technological challenge and the higher the mobility of a source is, the higher is its likelihood.

5.2 Failure probability of components

The failure probability of single elements can be estimated from the knowledge of strength (failure threshold) of the equipment and the stress which the equipment is exposed to.

5.2.1 Estimation of the strength of the components

The strength can be measured or estimated in a separate arrangement by inducing different voltages on the cable and then collecting the failure statistics of the device. Another option is to estimate the strength from the experience of the EMC engineer or from the known strengths of similar equipment.

In previous research, Camp et al. (2004) have shown that the strength (breakdown failure rate (BFR)) can be described by the Weibull distribution. The parameters of that distribution are however dependent on the shape of the radiated electromagnetic pulse. For different pulse shapes different breakdown behavior is expected. Using the window norms in frequency domain the energy- and amplitude efficiency factors (Nitsch et al., 2004) can be calculated. With the help of the energy- and amplitude efficiency factors the breakdown behavior for one pulse shape can be estimated from the knowledge of the breakdown behavior for another pulse shape.

5.2.2 Estimation of the stress

Besides the strength of the components the knowledge of the stress that the elements are exposed to is required. For that the principles of the electromagnetic (EM) topology can be applied (Baum, 1980). The main idea of EM topology is the same as in fault tree analysis: a complex system is decomposed into smaller subsystems. That way, the subsystems can be analyzed independently. In order to analyze the EM topology the whole system is divided into subvolumes which are separated by surfaces. A surface can be represented by a transfer function from one volume to another. Having the absolute knowledge of the situation including information like the exact positions of the objects, material parameters, angle of incident of electromagnetic wave, there would be no need to analyze the system statistically. In reality, we don't posses the absolute knowledge of the situation but a certain degree of belief or expectation about the true situation and thus we have uncertainties. Statistical analysis of coupling on cables in shielded environments is well described by Holland and John (1999). In the classical EM topology concept however, the uncertainties are not taken into account.

In order to take the uncertainties into consideration, the classical topological concept needs to be extended. Not only the transfer functions need to be considered but also the uncertainties of these transfer functions.

In order to analyze the system statistically there are two conceivable ways. The first way is to extend the topology concept in order to include the uncertainties and then to use the results as input data for the fault tree. The second way is to further extend the fault tree and to include the effects of shielding and propagation in this fault tree. By choosing the fault tree analysis, the whole system can be described by one model. There are however restrictions of the fault tree. The events in the tree are binary. Continuous values, such as field strength or shielding effectiveness, can be included if the symbols of the fault tree are extended. However the more serious restriction is that a disturbance in the electromagnetic topology graph can take several paths to each system element. Trying to implement this parallel paths in the fault tree is difficult and for some cases even impossible. Because of that the classical topology should be used in order

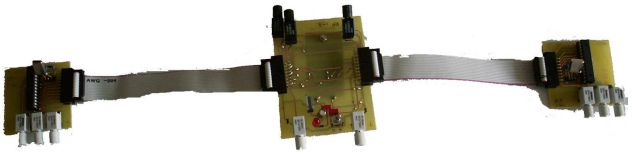

Fig. 7. Redundant two component system.

to describe the stress which the components are exposed to. For that the classical topology needs to be extended in order to include the uncertainties. This can be achieved by assigning the transfer function between two volumes uncertainties. This uncertainty can be described by single values such as the standard deviations or by whole probability density function. For example, instead of using just a shielding effectiveness value of 40 dB, a pair consisting of the expected shielding value and its standard deviation can be used and propagated through the topology tree such as (40 dB, $\pm$ 10 dB).

6 Common cause failures

In our previous research we have measured the failure probability of a redundant two component system depicted in Fig. 7. It was observed that depending on the wiring of the system there was a strong dependency between the two components. This dependency has a very strong influence on the redundancy and thus on the failure probability of the whole system. In classical risk analysis this type of failure is called Common Cause Failures (CCF). There are several models that try to include the CCF into the overall model (Bedford and Cooke, 2001, pp. 140–152). In order to include the common cause failures in our model the fault tree can be extended. However, before that the common cause have to be analyzed. It is part of our future work to predict the dependencies of the failures in interconnected systems.

7 Summary and conclusions

In this paper an example is shown of how a fault tree for a complex system exposed to IEMI can be developed. For that, the first step is the analysis of functional dependencies and scenarios that can lead to system failure. In the next step a differentiation is made between the different ways the EM interference can disturb the system. For that, radiated and conducted interference are modeled separately in the fault tree. Furthermore a distinction is made between the different entrance points of conducted interference. Hereafter, a distinction between different IEMI sources is made. It is discussed how the source likelihoods can be estimated and how the breakdown strength can be analyzed and determined in a separate setup. In order to model the disturbance two approaches are possible. The first approach is the classical electromagnetic topology approach. However, the uncertainties associated with modeling and the randomness of events must be included into the topology concept. The second approach is the further development of the fault tree. Because of the restrictions of the fault tree to model parallel propagation of the disturbance a sugestion is made to extend the classical topology concept in order to include statistical aspects.

The calculation of the probability of the top event and of the uncertainties associated with it is one part of the fault tree analysis. The other and not less important parts are the sensitivity and importance analysis. With the help of sensitivity analysis it is possible to determine how sensitive the model (result) reacts regarding changes of the model parameters. That way, it can be determined which model parameters should be modeled more precisely and which model parameters are less important and can thus be estimated roughly. In so doing, the efficiency of modeling time and effort can be improved. The importance analysis (Genender et al., 2010) is closely related to sensitivity analysis. With the help of importance analysis the significance of the system elements can be analyzed in regard to different aspects of the system behavior. Using the quantities like critical importance, risk reduction worth importance or risk achievement worth importance it is possible to determine the elements from which improvement the system will benefit most or the elements from which degradation the system will suffer least. Taking the importance measures into consideration, the system reliability can be improved systematically and cost-efficiently.

References

Baum, C.: Electromagnetic topology: A formal approach to the analysis and design of complex electronic systems, Interaction Notes, 400, 1980.

Bedford, T. and Cooke, R.: Probabilistic risk analysis: foundations and methods, Cambridge University Press, 2001.

Brauer, F., Sabath, F., and ter Haseborg, J. L.: Susceptibility of IT network systems to interferences by HPEM, 2009 IEEE International Symposium on Electromagnetic Compatibility, pp. 237–242, 2009.

Camp, M., Gerth, H., Garbe, H., and Haase, H.: Predicting the breakdown behavior of microcontrollers under EMP/UWB impact using a statistical analysis, IEEE Transactions on Electromagnetic Compatibility, 46, 368–379, 2004.

Garcia, E.: On the Use of Statistics in EMC for Industrial Complex Systems, in: CEM08, 2008.

Genender, E., Mleczko, M., and Garbe, H.: Importnace Analysis to Describe Reliablity of Systems, EMC Europe 2010, International Symposium on Electromagnetic Compatibility, 2010.

Giri, D. V. and Tesche, F. M.: Classification of Intentional Electromagnetic Environments (IEME), IEEE Transactions on Electromagnetic Compatibility, 46, 322–328, 2004.

Holland, R. and John, R. S.: Statistical Electromagnetics, Taylor & Francis Inc, 1999.

Mansson, D., Thottappillil, R., and Backstrom, M.: Methodology for Classifying Facilities With Respect to Intentional EMI,

IEEE Transactions on Electromagnetic Compatibility, 51, 46–52, 2009.

National Research Council: Evaluation of Methodologies for Estimating Vulnerability to Electromagnetic Pulse Effects, NATIONAL ACADEMY PRESS, 1984.

Nitsch, D., Camp, M., Sabath, F., ter Haseborg, J., and Garbe, H.: Susceptibility of some electronic equipment to HPEM threats, IEEE Transactions on Electromagnetic Compatibility, 46, 380–389, 2004.

Sabath, F. and Garbe, H.: Risk potential of radiated HPEM environments, 2009 IEEE International Symposium on Electromagnetic Compatibility, pp. 226–231, 2009.

Stamatelatos, M.: Probabilistic Risk Assessment, Procedures Guide for NASA Managers and Practitioners, NASA, version 1.1 edn., 2002.

Vesely, W.: Fault Tree Handbook with Aerospace Applications, NASA, 2002.