(ATINER)

Athens Journal of Technology & Engineering

(ATINER)

Volume 6, Issue 4, December 2019

Articles

ATHENS INSTITUTE FOR EDUCATION AND RESEARCH
A World Association of Academics and Researchers
8 Valaoritou Str., Kolonaki, 10671 Athens, Greece.
Tel.: 210-36.34.210 Fax: 210-36.34.209
Email: info@atiner.gr URL: www.atiner.gr
(ATINER) Established in 1995 (ATINER)

Mission

ATINER is a ***World Non-Profit Association*** of Academics and Researchers based in Athens. ATINER is an independent **Association** with a **Mission** to become a forum where Academics and Researchers from all over the world can meet in Athens, exchange ideas on their research and discuss future developments in their disciplines, **as well as engage with professionals from other fields**. Athens was chosen because of its long history of academic gatherings, which go back thousands of years to *Plato's Academy* and *Aristotle's Lyceum*. Both these historic places are within walking distance from ATINER's downtown offices. Since antiquity, Athens was an open city. In the words of Pericles, **Athens*"...is open to the world, we never expel a foreigner from learning or seeing".*** ("Pericles' Funeral Oration", in Thucydides, *The History of the Peloponnesian War).* It is ATINER's **mission** to revive the glory of Ancient Athens by inviting the World Academic Community to the city, to learn from each other in an environment of freedom and respect for other people's opinions and beliefs. After all, the free expression of one's opinion formed the basis for the development of democracy, and Athens was its cradle. As it turned out, the Golden Age of Athens was in fact, the Golden Age of the Western Civilization. *Education* and *(Re)searching* for the 'truth' are the pillars of any free (democratic) society. This is the reason why *Education* and *Research* are the two core words in ATINER's name.

The Athens Journal of Technology & Engineering
ISSN NUMBER: 2241-8237- DOI: 10.30958/ajte
Volume 6, Issue 4, December 2019
Download the entire issue (PDF)

Athens Journal of Technology & Engineering
Editorial and Reviewers' Board

President's Message

All ATINER's publications including the e-journals are open access without any costs (submission, processing, publishing, open access paid by authors, open access paid by readers etc.) and are independent of the presentations made at any of the many small events (conferences, symposiums, forums, colloquiums, courses, roundtable discussions) organized by ATINER throughout the year. The intellectual property rights of the submitted papers remain with the author.

Before you submit, please make sure your paper meets some basic academic standards, which include proper English. Some articles will be selected from the numerous papers that have been presented at the various annual international academic conferences organized by the different divisions and units of the Athens Institute for Education and Research.

The plethora of papers presented every year will enable the editorial board of each journal to select the best ones, and in so doing, to produce a quality academic journal. In addition to papers presented, ATINER encourages the independent submission of papers to be evaluated for publication.

The current issue of the Athens Journal of Technology & Engineering (AJTE) is the fourth issue of the sixth volume (2019). The reader will notice some changes compared with the previous volumes, which I hope is an improvement. An effort has been made to include papers which extent to different fields of Technology and Engineering.

Gregory T. Papanikos, President
Athens Institute for Education and Research

Athens Institute for Education and Research

A World Association of Academics and Researchers

10th Annual International Conference on Civil Engineering
20-25 June 2020, Athens, Greece

The Civil Engineering Unit of ATINER is organizing its **10th Annual International Conference on Civil Engineering, 22-25 June 2020, Athens, Greece** sponsored by the Athens Journal of Technology & Engineering. The aim of the conference is to bring together academics and researchers of all areas of Civil Engineering other related areas. You may participate as stream leader, presenter of one paper, chair of a session or observer. Please submit a proposal using the form available (https://www.atiner.gr/2020/FORM-CIV.doc).

Academic Members Responsible for the Conference

- **Dr. Dimitrios Goulias**, Head, Civil Engineering Unit, ATINER and Associate Professor & Director of Undergraduate Studies Civil & Environmental Engineering Department, University of Maryland, USA.

Important Dates

- Abstract Submission: **18 November 2019**
- Acceptance of Abstract: 4 Weeks after Submission
- Submission of Paper: **25 May 2020**

Social and Educational Program

The Social Program Emphasizes the Educational Aspect of the Academic Meetings of Atiner.

- Greek Night Entertainment (This is the official dinner of the conference)
- Athens Sightseeing: Old and New-An Educational Urban Walk
- Social Dinner
- Mycenae Visit
- Exploration of the Aegean Islands
- Delphi Visit
- Ancient Corinth and Cape Sounion

Conference Fees

Conference fees vary from 400€ to 2000€
Details can be found at: https://www.atiner.gr/2019fees

8th Annual International Conference on Industrial, Systems and Design Engineering, 22-25 June 2020, Athens, Greece

The Industrial Engineering Unit of ATINER will hold its **8th Annual International Conference on Industrial, Systems and Design Engineering, 22-25 June 2020, Athens, Greece** sponsored by the Athens Journal of Technology & Engineering.The aim of the conference is to bring together academics, researchers and professionals in areas of Industrial, Systems, Design Engineering and related subjects. You may participate as stream leader, presenter of one paper, chair of a session or observer. Please submit a proposal using the form available (https://www.atiner.gr/2020/FORM-IND.doc).

Important Dates

- Abstract Submission: **18 November 2019**
- Acceptance of Abstract: 4 Weeks after Submission
- Submission of Paper: **25 May 2020**

Academic Member Responsible for the Conference

- **Dr. Theodore Trafalis**, Director, Engineering & Architecture Division, ATINER, Professor of Industrial & Systems Engineering and Director, Optimization & Intelligent Systems Laboratory, The University of Oklahoma, USA.

Social and Educational Program

The Social Program Emphasizes the Educational Aspect of the Academic Meetings of Atiner.

- Greek Night Entertainment (This is the official dinner of the conference)
- Athens Sightseeing: Old and New-An Educational Urban Walk
- Social Dinner
- Mycenae Visit
- Exploration of the Aegean Islands
- Delphi Visit
- Ancient Corinth and Cape Sounion

More information can be found here: https://www.atiner.gr/social-program

Conference Fees

Conference fees vary from 400€ to 2000€
Details can be found at: https://www.atiner.gr/2019fees

Estimating the Success of IT Security Measures in Industry 4.0 Environments using Monte Carlo Simulation on Attack Defense Trees

By Till Hänisch[*] & Christoph Karg[†]

The choice of defense strategies in IT-security is often guided by qualitative methods only. For common scenarios like securing desktop computers, web servers, or extranets, there are well accepted best practices for establishing a secure environment. For other scenarios like computers in production environments (often referred as "Industry 4.0") this is not the case. To secure such systems, there are a number of options, but their relevance for a certain application is less clear and is specific for the situation. Especially, for small and medium enterprises it is often unclear, which security measures to apply in their production. This paper describes a method based on attack defense trees, which allows to assess the value of defense measures based on simulated attacks.

Keywords: *IT-security, Industry 4.0, Attack Tree.*

Introduction

Examples like the ransomware attacks of the last years, show that high profile cyber-attacks like advanced persistent threats (APTs) are not only targeting large multinational enterprises or governments, but also small and medium enterprises. Unfortunately, there is no clear consensus on how small and medium enterprises should protect their IT systems in production environments, for example in "Industry 4.0" scenarios. The general best practices published by institutions like the BSI in Germany or the CPA (Axelsen 2018) are not targeted to production environments and therefore of little help. The most prominent security measure, which is separating the production systems from the internet ("air gap"), is no longer realistic. Current trends like using Big Data, Industrial Internet of Things, and especially remote maintenance need a network connection between production IT and the outside world. Because of this, the choice of adequate security measures is increasingly important. To address this question, we conducted a survey among a number of larger companies, aiming to identify best practices for IT security in production (Hänisch and Rogge 2017). But it was unclear, how to prioritize them for each different small or medium company.

While there is little doubt that common techniques like network segmentation, firewalls, virus scanners, intrusion detection systems, or enhanced employee awareness against social attacks make sense, and should be used by any means, allocation of budget or assigning priorities to more sophisticated techniques is not so obvious.

[*]Professor, DHBW Heidenheim, Germany.
[†]Professor, Hochschule Aalen, Germany.

To decide, if adding a certain countermeasure makes sense in a given environment, a tool is needed, which allows to answer the question "Does countermeasure X stop the threat Y?" To decide, if the countermeasures currently in use in a given environment make sense, the question "Which countermeasure stops which threats?" also has to be addressed.

Attack Defense Trees (ADT) are a well-established way to structure the complex interdependencies of threat steps and countermeasures (Roy et al. 2010). But since there are many possible paths through the Attack Defense Tree, the questions given above can't be answered directly. A Monte Carlo simulation is used: a (large) number of attacks is simulated as a random walk through the tree. By counting, which countermeasure stops which attack, the above questions can be answered.

One problem remains: For every node in the ATD, the success probability has to be defined. Since there are many nodes, it is too much effort to build a new individual tree for every environment; for example a new tree for every company. If a common standardized tree is used, it has to be defined without knowing the details of the actual (difficulty of the) attack: standard attack trees neither compensate for local specialties of the target, like the awareness level of employees, the degree of standardization or the response times of a CERT team, nor do they incorporate knowledge about the attacker. While the latter is hard to specify (usually you don’t know the attacker in advance) it might be possible to define attacker groups by giving an upper limit of the knowledge (or for example the resources available) of an attacker.

The contribution of this paper is the definition of a method that allows specifying the assumptions about the success probabilities of an attack given a set of countermeasures in a way that is accessible to humans and allows adapting to a certain situation. The most important adaption is the analysis of a specific company without having to build a new tree. Intuition needed for finding the relevant defense measures can be replaced by interviews; selection of relevant attacks can be based on published data and/or attack trees and might be extended by case specific expertise. With the described method, the specification of success probabilities is simplified by splitting the probabilities in two parts; one that is common to all scenarios and can be reused, and a second, which might be different for each company.

In summary: This paper describes a method based on attack defense trees which allows to assess the value of defense measures based on simulated attacks. The goal is not to provide an automatic strategy generator or tool selector, but to make the importance of specific measures transparent and help guide decisions by supporting human security specialists.

Related Work

While attack trees are normally used to find out which way an attacker will choose, we assume that we already know about the possible threats, but want to find the best measures to stop them.

One problem[1] of prioritizing countermeasures is to assess the probability of a successful attack, without the countermeasure in question. Because intuition is a questionable way of computing probabilities of rare events (Taleb 2007), a quantitative approach is advantageous. Methods for calculating probabilities of success for an attack are quite old: Attack trees were developed in the sixties (Ericson 1999), and have been used in IT security for more than twenty years (Amoroso 1994, Schneier 2000).

Roy et al. (2010) propose an extension of Attack-Defense-Trees called Attack-Countermeasure-Trees, which includes defense nodes at any level in the tree. Our formalism could be applied to this type of tree too, but we put our focus on trees as simple as possible to keep the effort of adaption to a special case like a company as low as possible. They also use ROI-type calculations to find an optimal set of countermeasures. While cost is a well-accepted way of measuring the value of things, real costs are often not that easy to define for all events. To do that, it is necessary to rely on assumptions about possible threats, possible attackers, and their motivation and the effectiveness of the defense measures deployed. While assumptions are certainly necessary to a certain extent, one has to be aware that assumptions are no facts, and have to be treated accordingly. In our opinion, a good method is one that needs as few assumptions as possible.

Probabilities, required in many methods, especially in attack trees, can either be based on the past (that means counting), or on assumptions. Extrapolating the past into the future is risky, especially with rare events and impossible for events never seen before (Taleb 2007). Guessing probabilities is hard too, especially for the same kind of events as above: while humans have a good intuitive understanding of the probability of common events, the human brain is particularly bad assessing rare events. That makes sense from an evolutionary point of view, but is very bad for IT-security, where especially the rare and/or new attacks might be very dangerous in terms of damage. It is necessary to use a method for specifying the possible damage in a way that is accessible to humans.

There are attempts to generate Attack Trees automatically, see for example (Paul 2014). But these are not adapted to a specific environment, company specific aspects like the awareness of employees are not considered.

Attacks can be modeled in other forms like UML diagrams, which allow to model not only a static state space but can also show dynamic interactions, which are especially useful to analyze the behaviour in case of failed defense measures. But, the complexity of these models limits their use to general cases where their use is to understand general attack and defense mechanisms and not to analyze a specific environment for example a company (Löhner 2018).

The separation of the probability in two parameters can be used for other purposes, like (Fen et al. 2012) proposing a two part definition of the possibility of an attack using a difficulty of an attack and the attack detection possibility to define the success probability but doesn't use the difficulty parameter to adapt to special situations but to select the path an attacker chooses to select the attack steps using multi-attribute utility theory.

[1]The one investigated in this paper. There are more, like estimating the damage of a successful attack.

A common approach in IT security management is the assessment of risk by qualitative means. For example, the OWASP risk rating methodology (OWASP 2019) assesses the risk of a threat by correlating its likelihood and its impact. Both the likelihood and the impact of the threat are rated with the value LOW, MEDIUM, or HIGH, respectively. The likelihood rating is derived by analyzing factors of the threat agent such as his or her skill level and motive and analyzing factors of the vulnerability such as the ease of its discoverability and the ease of its exploitation. Factors relevant for the assessment of the impact are technical impacts such as the loss of availability or confidentiality and business impacts such as financial damage or non-compliance. Depending on the rating of the likelihood and the impact, the overall risk severity of the threat is rated with None, Low, Medium, High, or Critical, respectively.

Another popular framework is the Common Vulnerability Scoring Framework (CVSS) (FIRST 2019). The goal of CVSS is the communication of characteristics and severity of software vulnerabilities. Similarly to the OWASP approach, CVSS rates a vulnerability with the value None, Low, Medium, High or Critical, respectively. The rating is derived by assessing the vulnerability with three metric groups. The Base metrics group addresses intrinsic properties of the vulnerability which do not change over time and are not dependent on the user's environment. Metrics of the group rate the exploitability of the vulnerability and the respective impact in terms of confidentiality, availability, and integrity. The Temporal metrics group considers aspects of the vulnerability which might change over time such as the existence of exploitation tools or security patches. The Environment metrics group allows the customization of the score with respect to the requirements of a particular company or organization. While the assessment of the base group is mandatory to determine the vulnerability's score, the assessment of the temporal and environment is optional. An advantage of CVSS over other risk assessment frameworks is the world wide support by certs and organizations. For example, the U.S. National Institute of Standards and Technology runs the National Vulnerability Database[2] which provides a comprehensive and up-to-date list of vulnerabilities with CVSS scores.

Methodology

ADTs are an extension of attack trees, which include countermeasures as leaf nodes (Kordy et al. 2014). While these trees and especially their evaluation can be made complex, see for example (Bistarelli 2007), a very simple version is used in our proposed method.

[2]Website: https://nvd.nist.gov.

Figure 1. *a) Simple Attack Tree with Different Node Types. To Achieve the Goal (N0009) there are Three Alternatives (N0005, N0006, N0007) from which the Attacker might choose one. b) The Corresponding Attack Defense Tree Shows N0005 having one Countermeasure N0001 which might stop this Attack. N0006 Needs Two Measures N0002 and N0003 to be Successful to Stop the Attack*

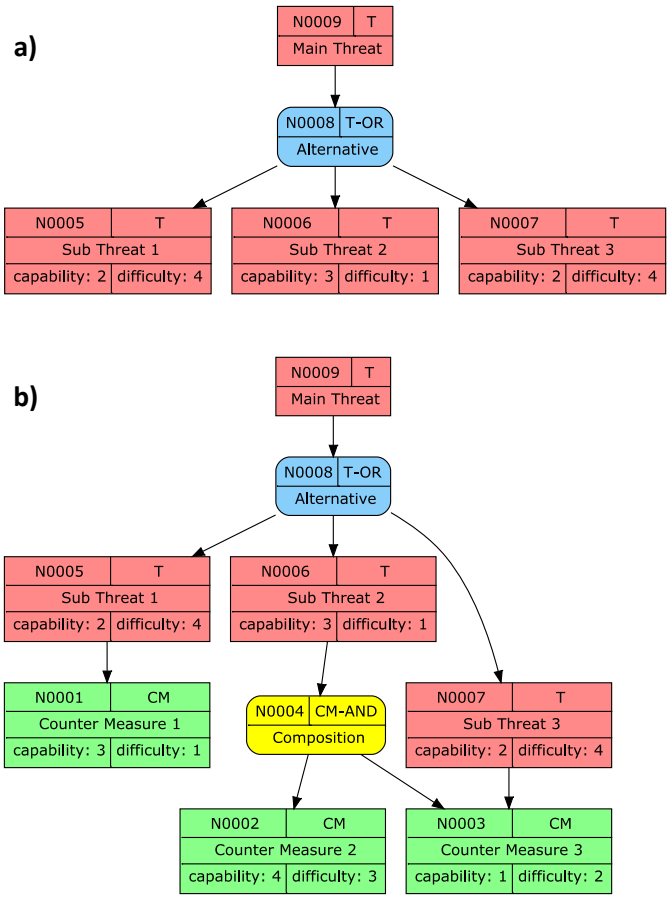


Figure 1a shows a simple attack tree. The attack is modeled as a hierarchy of simpler steps. Threat nodes in Figure 1 may have groups of children (Roy et al. 2010) where either all have to be successful (Composition, AND), or where it is sufficient that one is successful (Alternative, OR). To keep the design of the tree simple, we do not use selections out of a group of events. If this way of modeling is needed, it can be converted into nested structures of AND and OR.

In addition to these combinations, we suggest a group of actions, which have to be successful in a given sequence (SAND); for an overview see (Kordy et al. 2015). This is interesting for example in cases, where security incidents can be detected in an early stage of an attack and, if detected, be used to prevent following steps to be successful. Using a sequence allows to clarify, which attack steps shall be blocked and which can be ignored due to blocking of measures in earlier steps. This does not change the overall probability of success, but is important information for the prioritization of defense measures.

A second use of a sequence is to make the intent of the modeler explicit, when in reality the order of steps is not arbitrary. Assume we want to model the following attack steps:

1. Spear phishing Office-IT
2. Put Drive-by Malware in place
3. Infect control panel app

In step 2, maybe an XSS attack of a trusted website could be used. When specifying the difficulty of this step, it will highly depend on the website, which has to be used. In general, it is not difficult to infect a random site with an XSS attack vector. But, if for example we want to attack an office application in the controlling department of a large company with good employee awareness, it will be very difficult to exploit one of the few websites, an employee will use during his work. Because of this, the actual difficulty for this attack step cannot be defined without knowing in which context (and the order of the steps is part of this context) the steps will be executed. But since the usefulness of this additional modeling tool has not been validated in our practical experiments, in this paper we will focus on the more common grouping methods of "AND" and "OR".

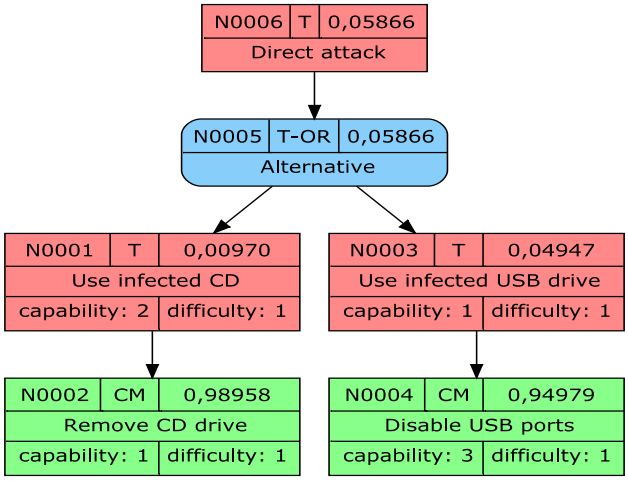
Figure 1b shows the same tree extended by countermeasures shown as green nodes. Countermeasures can also be modeled as subtrees containing logical groupings, exactly like attack steps.

The construction of trees can be based on real examples found in the wild, for example from interviews. The initial attack tree we used for our work was based on interviews with a number of companies about their defense measures used to secure their production sites (Hänisch and Rogge 2017). Additionally, it was used to understand implications on security architecture for industry appliances (Hänisch 2018).

The success probabilities of the individual nodes are defined by an empirical equation. The success probability of an attack step like "Use infected CD" to place malware is defined in terms of the capabilities the attacker must have and the actual difficulty of making the attack successful in a certain situation. Required capabilities in this example are "Be able to produce an innocent looking but interesting DVD" and "Physically put the disc to a place where it is taken and put into the machine to be attacked". Both of these are simple, if the attacker has physical access, and are pretty difficult, if not. How hard it is in a certain situation, e.g. for a certain company facility, to guess, what looks innocent and interesting to the people in the company to be attacked, and to get physical access to a relevant place depends heavily on the company[3]. That means, the capability level is at least in a first approximation common to all targets but the difficulty is different for every situation. That means, the capability part has to be defined only once, while the difficulty part must be defined specifically for every situation.

[3]And maybe on the type of attacker, like insider, motivated kid or member of an intelligence agency.

Figure 2. *Part of a larger Attack Defense Tree. To Attack a Computer without going over the Network, an Infected CD or an Infected USB Stick could be used. The Attack via the CD could be prevented by Removing the Drive, the Attack via USB by Disabling All (Accessible) USB ports. The Success Probabilities of the Different Nodes are given by their Respective Capability and Difficulty Value. The Resulting Success Probability is shown in the Top Right Corner of Each Node*



The probability of success for an attack step is therefore separated in two parameters

$$p = p(c, d)$$

If c and d are assumed to be independent sub-probabilities, p is the product of both, so our implementation uses

$$p = 1 - c * d$$

as a starting point. This can be modified by a frequency component providing (empirical) information about how "popular" this attack (step) is:

$$p = f * (1 - c * d)$$

From an economic perspective it makes more sense to deploy measures, which help against common attacks, instead of rarely used ones. But, this might depend on the attacker. An intelligence agency with unlimited resources might choose a rare and complex way to attack a target hoping that no-one will focus on preventing rare attack vectors. In this paper, we will only discuss the simple form with $f \equiv 1$.

Since we need probabilities and it is difficult to select values, especially for very rare and very common cases, we use a scale from 1 to 6, borrowing and simplifying[4] ideas from the OWASP risk rating model (OWASP).

[4]From OWASP Threat Agent Forces we borrow "Skill Level" and "Opportunity" as somewhat similar to our "capability" and "difficulty". Instead of the OWASP likelihood level scale with three groups of three, we use 3 groups of 2, in total 6 levels.

Table 1. *Definition of Probability Scale Values. The Same Values are used for Attacks and Countermeasures*

Scale value	Definition	Probability value
1	very low/very easy (e.g. everyone)	0.1
2	low/easy (e.g. some skills required/some problems)	0.3
3	middle (well, middle)	0.5
4	high (e.g. expert level)	0.8
5	very high/very difficult (e.g. highly motivated hacker/ criminal)	0.9
6	extremly high/extremly difficult (e.g. government agency level)	0.99

To rank the measures, a Monte Carlo simulation is applied. This is a random walk over the state space of the tree: We walk down the tree till we are at the leaf. While going back, we check how things work: if a measure catches, the attack has failed. If the measure succeeds this is logged. If the measure succeeds, the threats on the way back have failed as a consequence.

If the measure has not succeeded (or we have no measure), we make random attempts with the threats on our way up. If for example in Figure 1b "countermeasure 1" fails, we try, if "Sub Threat 1" is successful.

If a threat fails, everything up to the next "OR" on our way back has also failed. The probability for choosing an (OR) alternative is weighted by the required capability. As a first approximation we chose the associated probabilities from the Capability - Probability table defined above (see Table 1). Then we shuffle the alternatives to avoid dependence on the (artificial) sequence of the definition. Then we add the probabilities of the alternatives for normalization. Next, we generate a random number and add up the probabilities until we reach this number. The corresponding alternative is the one we choose. This is basically a roulette wheel selection as used in genetic optimization; see for example (Lipowski and Lipowska 2012) or (Goldberg 1989). More details on the final implementation can be found in (Karg and Hänisch 2019).

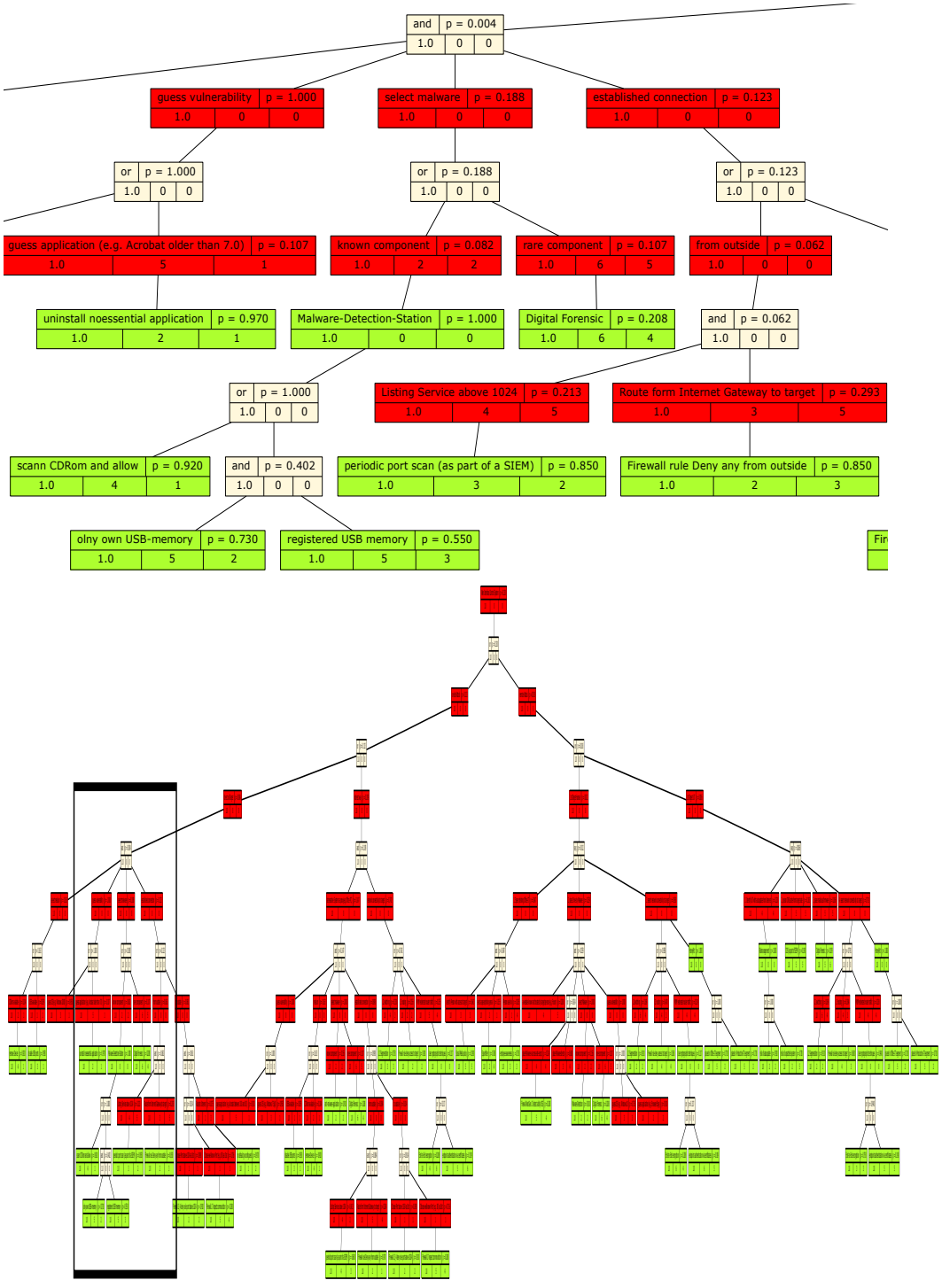
This process is repeated a (large) number of times. Since we logged, which measures were successful in stopping an attack, we can sort the measures by this number. The ones which prevented many attacks are the more important ones. This is the central assumption in our model

Findings/Results

To evaluate our method, we created an example tree, part of which is shown in the following Figure 3. The complete tree is available on github[5], along with the source code. Other examples for the construction of Attack Defense Trees can be found in (Edge 2007).

[5]https://github.com/TillHaenisch/ATD.git.

Figure 3. *Part of the Example Tree, here Placing Malware. The Lower Graphic Shows the Complete Tree with the Rectangle Defining the Border of the Graphic Above*



The tree was constructed from interviews with a number of companies to find out about the countermeasures used in their production IT. These were matched with a model-threat that tries to compromise a machine in a production

environment. The respective success probabilities were assigned using the scheme described above. This tree consists of 70 attack steps and 54 countermeasures. Even for this limited attack scope, the tree is pretty big and hard to oversee and understand. In our experience, a much larger tree is not manageable. This makes the use of very general attack trees rather difficult to say the least.

To find out, if the results of the Monte-Carlo-Simulation of the attack-defense-mechanisms are consistent with real-life strategies from our interviews, we simulated 10.000 attacks and analyzed, which threat steps were successful, and which measures successfully caught attacks. Table 2 shows some of the results.

Table 2. *Simulation Results: The Most and Least Successful Countermeasures and Attack Steps; there are shown the Type of Node (Threat or Countermeasure), the Actual Countermeasure or Threat Step and the Number of Successful Events in the Simulation in Absolute Numbers for 10000 Simulated Attacks*

ID	type of node	name	# successful
1	measure	spamfilter	1020
2	measure	increase employee awareness	970
3	measure	anti-malware-application	501
4	measure	remove Device	911
6	measure	uninstall nonessential application	374
7	measure	L2 segmentation	366
8	measure	no default gateway configured	266
		…	
48	measure	endpoint authentication via certificates	0
49	measure	End-to-End encryption	0
50	measure	use cryptographic techniques	0
1	threat	identify IoT with autoupdate from internet	1347
2	threat	poison DNS cache from target site	474
3	threat	rare component	388
4	threat	MitM redirected router traffic	333
5	threat	identify Person with access to target	227
		…	
32	threat	USB available	0
55	threat	L3 routing	0
57	threat	first target IoT device	0
65	threat	place malware directly	0

Since most of the attacks require the unintentional cooperation of a human, it is reasonable that a spam filter catches a large number of attacks by blocking the

required phishing mails. The same holds for increasing the awareness of employees.

Measures like “endpoint authentication via certificates” or “L2 segmentation” didn’t stop a single attack in this experiment.

The intended use of the described method is to check, if certain measures might be superfluous, because other measures catch all relevant attack. In Table 2 for example, the measure "End-to-End encryption" does not catch a single attempt. Of course, that does not mean, that this measure is worthless, but only that other measures seem to be more important for the specific threat under consideration.

A second benefit is to check, if a measure considered to be implemented is useful. If it does not catch (many) attacks, it might be superfluous. These checks are not meant to be absolute in the way, that they are used to decide which measures should be implemented or not, but should be considered as indicators that further investigation is needed.

In addition, looking at the successful measures, we also log successful threats. Every successful threat step, meaning it is not blocked by a measure and was found to be successful in a random walk through our tree, is logged too. With this information we can again sort by this number to get an idea which ways into our system are easy to take. For example, the threat step "poison DNS cache from target site" shown in Table 2 was successful in a large number of cases. That does not necessarily mean, that this is a real problem, because the related problems might be caught by measures not modeled in the tree, but that has to be evaluated.

If it is a real problem, meaning this threat step is not caught by other measures, action is necessary. To reduce the success probability of a critical threat step, either additional measures can be deployed or the difficulty of the threat step can be increased by techniques not modeled in the tree.

Conclusions

Based on interviews with companies, an attack defense tree for a machine in a production environment was built. The success probabilities for its threat steps and countermeasures were assigned according to the scheme described in the article at hand. The Monte Carlo simulation of the overall success probability of attacking a machine gives results for the effectiveness of common countermeasures, which are compatible with the best practices found in the interviews. It seems reasonable, that the described model for specifying probabilities can be used in practice to assess the effectiveness of countermeasures. The model described should be tested with a number of specific practical problems to identify possible issues.

Acknowledgments

Special thanks to Stephan Rogge from certerius for helpful discussions.

References

Amoroso EG (1994) *Fundamentals of Computer Security Technology*. USA, Upper Saddle River, NJ: Prentice-Hall, Inc.

Axelsen M (2018) *It Checklist for Small Business, CPA Australia.* Retrieved form https:// bit.ly/2tzKEaV.

Bistarelli SM, Aglio D, Peretti P (2007) Strategic Games on Defense Trees. *LNCS* 4691: 1-15.

Edge K (2007) *A Framework for Analyzing and Mitigating the Vulnerabilities of Complex Systems via Attack and Protection Trees.* Ph.D. Dissertation, Air Force Institute of Technology. Retrieved from https://bit.ly/2lMxMNW.

Ericson II, Clifton A (1999) *Fault Tree Analysis – A History*. Proceedings of the 17th International System Safety Conference, 1999.

Fen Y, Xinchun Y, Hao H (2012) A Network Attack Modeling Method Based on MLL-AT. *Physics Procedia* 24(C): 1765-1772.

Goldberg DE (1989) *Genetic Algorithms in Search, Optimization, and Machine Learning*. Boston, MA: Addison-Wesley Longman Publishing.

Hänisch T, Rogge S (2017) IT-Sicherheit in der Industrie 4.0. [IT Security in the Industry 4.0]. In VP Andelfinger, T Hänisch (Eds.), *IT-Sicherheit in der Industrie 4.0.* Germany, Wiesbaden: Springer.

Hänisch T (2018) An Architecture for Reliable Industry 4.0 Appliances. *Athens Journal of Technology and Engineering* 5(1): 7-18.

Karg C, Hänisch T (2019) *Using an Extended Attack Defense Graph Model to Estimate the Risk of a Successful Attack on an IT Infrastructure.* Presented at 15th Annual International Conference on Information Technology & Computer Science, 20-23 May 2019, Athens, Greece.

Kordy B, Mauw S, Radomirovi´c S, Schweitzer P (2014) Attack–Defense Trees. *Journal of Logic and Computation* 24(1).

Kordy B, Jhawar R, Mauw S, Radomirovic S, Trujillo-Rasua R (2015) *Attack Trees with Sequential Conjunction,* Presented at the 30th IFIP International Information Security Conference (SEC).

Lipowski A, Lipowska D (2012) Roulette-Wheel Selection via Stochastic Acceptance. *Physica A: Statistical Mechanics and its Applications* 391(6): 2193-2196.

Löhner B (2018) *Attack-Defense-Trees and Other Security Modeling Tools, Network Architectures and Services*. Network Architectures and Services, September 2018.

OWASP Risk Rating Methodology. Retrieved from https://bit.ly/1BJAUe8.

Paul S (2014) *Towards Automating the Construction & Maintenance of Attack Trees: A Feasibility Study*. First International Workshop on Graphical Models for Security (GraMSec 2014).

Roy A, Kim D, Trivedi KS (2010) *Cyber Security Analysis using Attack Countermeasure Trees.* CSIIRW '10 Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research Article No. 28, 2010.

Schneier B (2000) *Secrets and Lies: Digital Security in a Networked World*. USA, NY: John Wiley and Sons, Inc.,

Taleb N (2007) *The Black Swan: The Impact of the Highly Improbable.* USA, NY: Random House.

Using an Extended Attack Defense Graph Model to Estimate the Risk of a Successful Attack on an IT Infrastructure

By Christoph Karg[*] *& Till Hänisch*[±]

Nowadays, securing the IT infrastructure is an ongoing task in every company and organization. For small and medium-sized enterprises, this task is challenging because of its complexity and the related costs. Especially the risk assessment of threats and the choice of appropriate countermeasures is hard to handle by this kind of enterprises. Using the example of a ransomware attack, this paper describes how to use a method for risk assessment on the basis of attack defence graphs and Monte Carlo simulations. The details of the simulation algorithm are explained and formal aspects are considered.

Keywords: *IT security, attack defense graph, risk assessment, threat modeling.*

Introduction

In a commercial environment, the goal of each security measure is the protection of the company's or organization's assets. In the context of information security, the measures focus on computer systems and the data stored on them. Usually, the financial budget to be spent on security measures is limited. As a consequence, not all of the available measures can be applied because of monetary restrictions. Hence, a choice must be made on how much money to spend on which security measure in order to use the financial resources in an optimal manner.

The selection of the measures to secure a company's IT infrastructure is usually based on best practices. In the case of office IT environments, many of the choices are based on the experience which was gathered in the last decades. In the case of industrial production environments, the situation is quite different, since the process of digitalization just begins to find its way into these environments. According to IT security experts, there is the need of a quantitative assessment of a security measure with respect to the environment it shall be applied to (Blakley et al. 2002, Cremonini and Martini 2005). This kind of assessment may assist decision makers in choosing and prioritizing appropriate security measures.

This paper describes an approach to assess the effectiveness of security measures on the basis of Monte Carlo simulations. The approach builds on the well-known model of attack defense graphs. An attack defense graph is a directed acyclic graph whose nodes represent threats which arise from existing vulnerabilities and countermeasures to mitigate the respective threats. The nodes are grouped in compositions (and) or alternatives (or) in order to specify the dependencies. Each sink of the graph represents an attack which may be the result of successfully exploiting the vulnerabilities which are located on the paths

[*]Professor, Aalen University of Applied Sciences, Germany.
[±]Professor, DHBW Heidenheim, Germany

towards the sink. The attack may be prevented by successfully applying the counter measures which lie on the paths towards the sink.

In order to estimate the risk of a successful attack, the model is extended with additional information. In particular, both a capability and a difficulty value are assigned to each node representing a threat or a countermeasure. The capability of a threat or a countermeasure describes the skill level of an attacker to successfully implement the threat or the skill level of a defender to successfully deploy a countermeasure, respectively. It is assumed that the capability value is independent of the environment to be analyzed. The difficulty value of a node measures the difficulty of implementing a threat or of deploying a countermeasure in a given environment, respectively. To enable Monte Carlo simulation techniques, probabilities are derived from the capability and the difficulty values.

To answer questions such as "How does the usage of security measure A influence the risk?" or "Is security measure A better than security measure B with respect to the mitigation of the risk?", several Monte Carlo simulations are performed and analyzed. The simulation results can help the decision makers to select these countermeasures which fit the best to their IT environment. Another application of the approach is the computation of an cost-optimal selection of security measures which minimize the risk of a successful attack. The use case of a ransomware attack is used in order to illustrate the application of the model.

The paper is organized as follows. The section *Related Work* contains a summary of the papers which were relevant for this work. The section *Findings/ Results* contains our contributions to the topic. At first, the model of attack defense graphs is introduced briefly. Then the model is applied to the use case of a ransomware attack. After describing the algorithm behind the simulation system, the use case is analyzed. Furthermore, formal aspects of the model are presented and insights into the implementation are provided. The paper closes with the section *Conclusion*.

Related Work

Analyzing the safety of a technological system with the mathematical model of graphs is a well-known and acknowledged methodology in systems engineering. The roots go back in the 1960s where Watson and Mears at Bell Labs developed a tree-based technique to analyze the Minuteman Launch Control System. Hassl from Boeing recognized the potential of this approach and promoted it as a significant system safety analysis tool. The tool became popular as fault tree analysis (FTA) in the aerospace industry and was adopted from other industries such as the nuclear power industry and the robotics industry. In 1981, the U.S. Regularity Commission published a handbook on the application of the fault tree analysis and its mathematical foundations (Vesely et al 1981). Over the last six decades, fault tree analysis was developed further by a worldwide scientific community. More details on the history of the fault tree analysis can be found in (Ericson, 1999). An approach to utilize attack-fault trees for quantitative analysis in the area of cyber physical systems is given in (Kumar and Stoelinga 2017).

In the year 1999, Bruce Schneier introduced the concept of attack trees as a (Schneier 1999a, 1999b). According to Schneier, most people do not have a detailed understanding in computer security. Especially, for decision makers in companies and organizations it is hard to figure out the consequences of a cyber security threat. Attack trees are a formal method to describe attacks on computer systems in a manner which is understandable for non-experts. Schneier proposed to assign attributes to the nodes in order to enrich the attack tree with additional information. Examples of such attributes are the success possibility of the attack represented by an node, the equipment needed to perform the attack, or the costs of the attack to be paid by the threat agent. Schneier's model of attack trees is a simplistic one and lacks the concepts of countermeasure nodes and success probabilities.

Schneier's concept influenced the work of many researchers on the field of computer security. For example, Mauw and Oostdijk (2005) studied formal aspects of attack trees and provided a denotional semantics. To do this, they formalized the notion of an attack tree and studied transformations on attack trees and their respective consequences (Mauw & Oostdijk, 2005). Kordy et al. (2014) extended the model to so-called attack defense trees by adding countermeasures to the tree (Kordy et al. 2014). The idea behind their approach is to model a game between an attacker and a defender of a computer system. On the one hand, the attacker has the goal to successfully realize the threat by applying the steps represented by the attack nodes. On the other hand, the defender tries to prevent the attacker from being successful by applying the countermeasures described in the defense nodes. The authors gave a formal representation of the attack defense tree model and prove several semantic aspects of the model.

Edge et al. (2006) used attack and protections trees to analyze attacks against computer networks (Edge et al. 2006). They created the concept of threat logic trees. These are trees where metrics are associated to the leaf nodes of the tree. The metrics are probability of success, impact to the system, the cost to attack, and risk. The metrics are used to analyze the tree and to estimate the risk of a successful attack. They use their model to analyze a distributed denial-of-service attack to the servers of Homeland Security. In contrast to the above approaches, the modelling is split in two trees: the attack tree and the protection tree.

The usage of attack defense trees in threat modelling and risk assessment is a widely recognized methodology in information technology. For example, Fraile et al (2016) used attack defense trees to analyze the security of automated teller machines (ATM) (Fraile et al. 2016). Based on their practical work, the authors attest attack defense trees a high potential to produce good results in risk assessment.

The quality of the modelling with attack defense trees is strongly related to the experience of the persons which are involved in the analysis process. Experts on the field of cyber security apply methodologies from risk assessment such as the OWASP risk rating methodology (OWASP 2019) or the CORAS approach (Lund et al. 2011). Another useful tool is the common vulnerability scoring system (CVSS) which is a worldwide accepted standard to describe the characteristics of vulnerability (Forum of Incident Response and Security Teams 2019). CVSS is

used to classify known vulnerabilities in a standardized way. The findings are published in publicly available databases such as the U.S. National Vulnerability Database[1].

Hänisch and Karg (2019) introduced a method for cyber security risk assessment on the basis of attack defense graphs and Monte Carlo simulations (Hänisch and Karg 2019). Their goal was to make the importance of specific measures transparent to decision makers and to support security specialists without requiring the effort of a complete risk analysis.

Findings & Results

The Model

The model to be used in following is a combination of attack defense graphs and Monte Carlo simulations. For a detailed introduction to the model, we refer to (Hänisch and Karg 2019).

In this model, attack defense graphs are used to analyze the risk of a threat. Such a graph is a directed acyclic graph. The nodes of the graph consist of threats, countermeasures, or selections of them. A selection can be either a composition (and) or an alternative (or). The root of the graph represents the main threat to be analyzed. The leafs of the graph are the atomic actions to be performed by the attacker and the defender, respectively. Each leaf is assessed with two values, the *capability* and the *difficulty*. The meaning of the values is as follows:

- The capability measures the fundamental complexity of successfully applying the threat or the countermeasure. The value is integral and ranges from 1 (simple) to 6 (very complex).
- The difficulty rates the environment the system is located and the respective effects on implementing the threats and countermeasures. The value is integral and ranges from 1 (simple) to 6 (very complex).

The success rate of a threat or a countermeasure is derived by its capability and difficulty assessment according to (Table 1). In the following, we refer to the contents of this table as the risk assessment model.

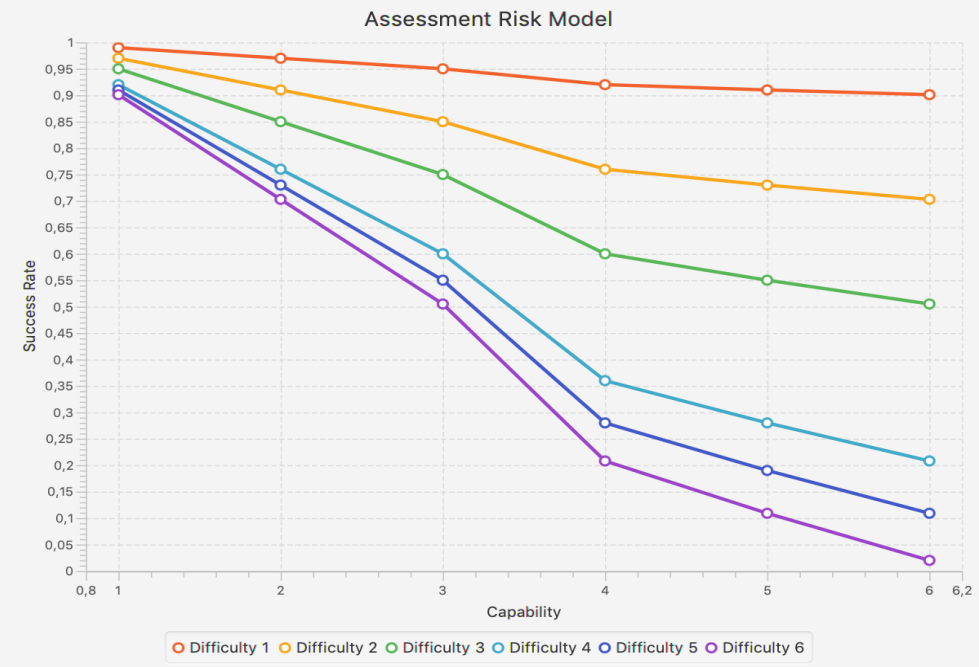
[1]Webpage: https://nvd.nist.gov

Table 1. *Risk Assessment Lookup Table*

		capability					
		1	2	3	4	5	6
difficulty	1	0.99	0.97	0.95	0.92	0.91	0.90
	2	0.97	0.91	0.85	0.76	0.73	0.70
	3	0.95	0.85	0.75	0.60	0.55	0.51
	4	0.92	0.76	0.60	0.36	0.28	0.21
	5	0.91	0.73	0.55	0.28	0.19	0.11
	6	0.90	0.70	0.51	0.21	0.11	0.02

Figure 1 provides a chart of the success rates of the capabilities with respect to the difficulties.

Figure 1. *Risk Assessment Chart*

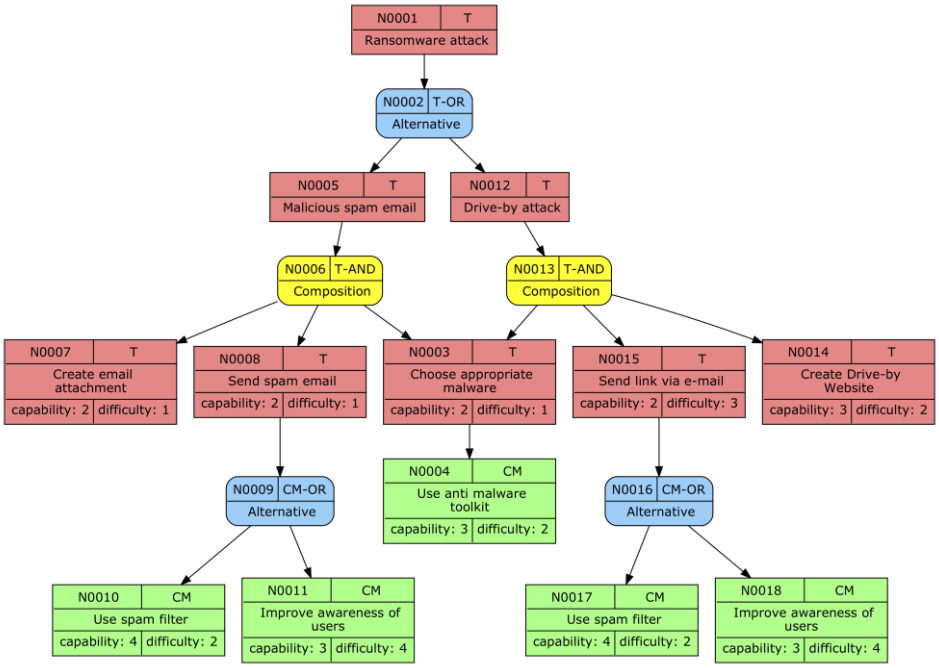


Use Case: Ransomware Attack

In the following, the attack defense graph model is used to analyze the threat of a ransomware attack. The respective graph is displayed in Figure 2.

The root (N0001) of the graph represents the risk of a successful ransomware attack. An assumption in this use case is that the attacker is not able to get physical access to the company site. Hence, he cannot place malicious USB sticks or hack the company's computers directly.

Figure 2. *An Attack Defense Graph modeling the Threat of a Ransomware Attack and the Respective Countermeasures.*



Without direct access, the attacker needs to the malware via the internet. He has two alternatives: sending a spam email which contains the malware as an attachment or performing a drive-by attack where the victim downloads the malware from a well-prepared web page. This alternative is modeled with the nodes N0002, N0005, and N0012.

Independently of the attack path, the attacker needs to choose a ransomware malware which is feasible for a successful attack (node N0003). This can be done quite easily by searching the internet or the darknet. A countermeasure is the deployment of an anti-malware toolkit within the company's IT infrastructure (node N0004). The challenge is to keep this toolkit up to date in order to detect the latest malware.

The next step of the attack path is the creation of an attachment containing the malware (node N0007). Usually, this is a PDF or a Microsoft Office document. From the defender's point of view, this cannot be prevented. Finally, the spam email needs to be sent (node N0008). The attacker can choose a service offered in the darknet or can use a public email service provider. The defender can act against this threat by using a spam filter (node N0010) or improving the awareness of the employees (node N0011).

After choosing the malware, the attack path continues with the setup of a website which is used to distribute the malware (node N0014). In the internet, there exist various hosting platforms for this purpose. It is not difficult to create a well-designed website. Finally, the attacker needs to send the link to the website via email (node N0015). The defender can take care on this threat by using a spam filter (node N0017) or improving the awareness of its employees (node N0018). In

contrast to the previous attack path, we assume that for a spam filter it is more difficult to detect malicious links in an email than to detect bad attachments. This results in an higher capability value of node N0017.

Monte Carlo Simulation

After modeling the use case, the resulting attack defense graph is analyzed by performing a Monte Carlo simulation. The algorithm behind this simulation is depicted in Figure 3.

In the first step of the algorithm, the success rates of the leafs are initialized with the values of the risk assessment model. Then, the parameters of the simulation are initialized. All in all $\texttt{total} = 100000$ simulation steps are performed. The number of successful simulation steps is stored in the variable cntr.

A simulation step is computed by a recursive procedure which performs a depth-first walk through the attack defense graph beginning at the root node. The steps of the computation depend of the type of visited node.

If the visited node is a countermeasure node, then the procedure chooses the success rate p depending on the countermeasure's capability and the difficulty (see (Table 1)) and determines its success by a random trial, this is, a Bernoulli experiment with success probability p.

If the visited node is a threat node, there are two cases:

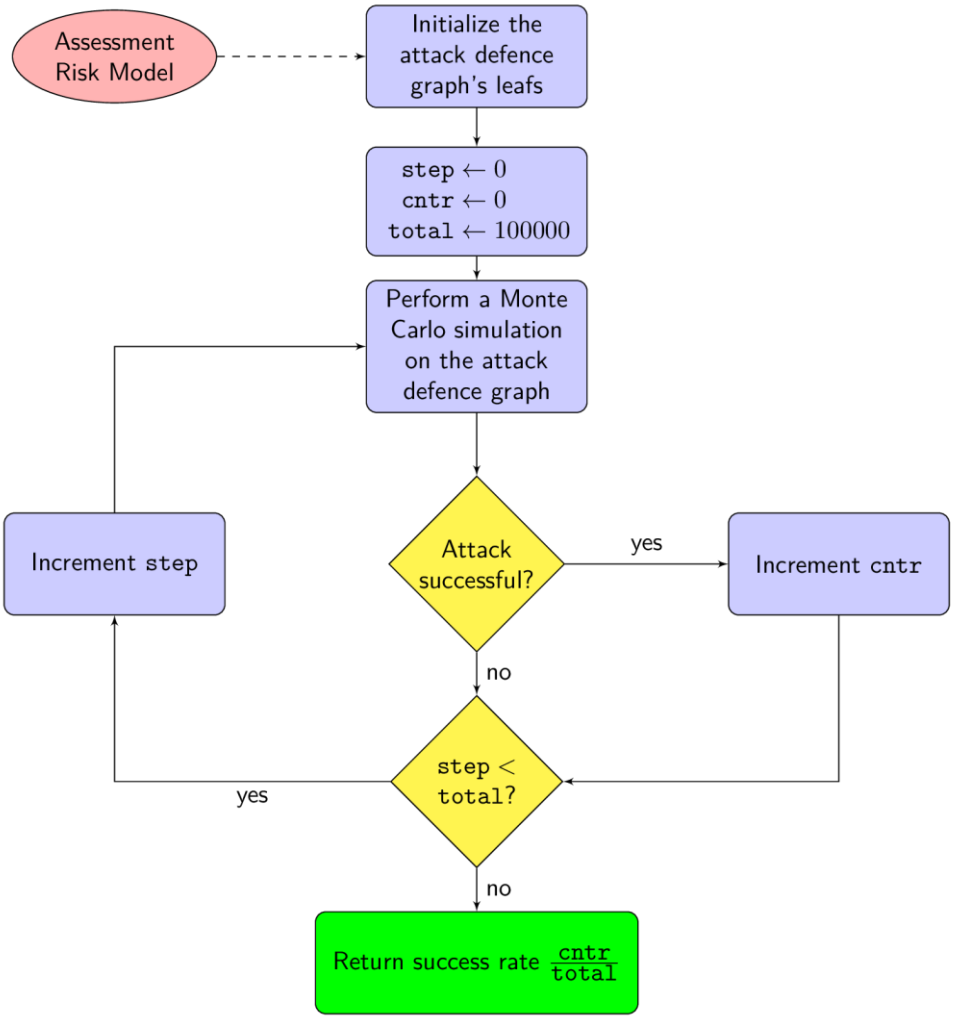
- The node is a leaf: In this case, the procedure guesses the result b_T of the threat uniformly at random according to its capability and difficulty.
- The node has a child threat: In this case, the procedure computes the result of the child threat recursively and stores it as the result b_T of the node.

If a countermeasure is assigned to the threat node, then the procedure furthermore computes the result b_C recursively and sets the result of the node to $b_T = b_T \ and \ not \ b_C$. This is, if the countermeasure is successful, then it prevents the success of the threat.

If the node is a composition (and) or an alternative (or) of threats or countermeasures, then the procedure recursively computes the result of the node's children and then sets the value of the node as the logical and or the logical or of its children, respectively.

In the case of a successful attack, the variable cntr is increased. As the result, the algorithm returns the ratio of successful attacks with respect to the total number of simulations, this is, the fraction $\frac{\texttt{cntr}}{\texttt{total}}$.

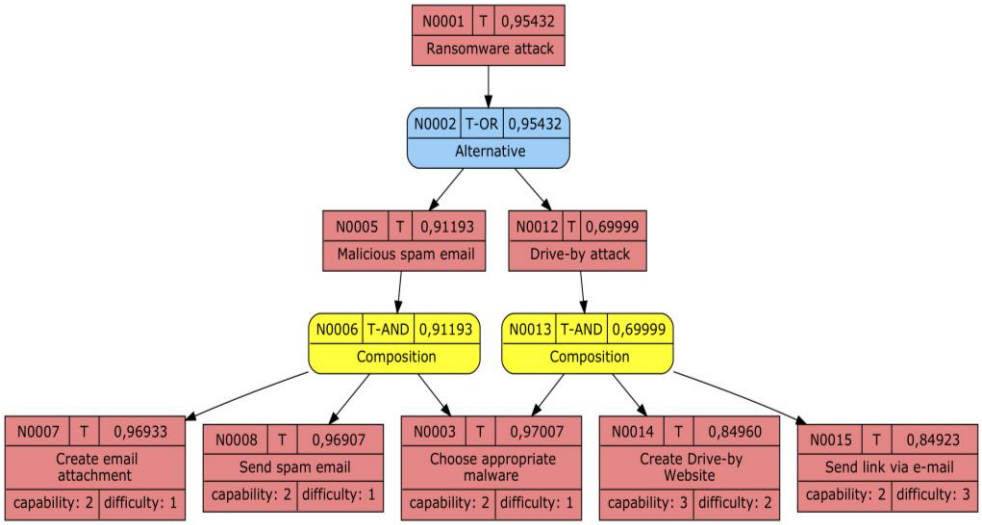
Figure 3. *Simulation Approach*



Analysis of the use Case

The analysis of the use case starts with two basic simulations. The first simulation runs on a variant of the attack defense graph where all countermeasures are disabled (see Figure 4). According to the simulation, the success rate of threat without countermeasures is approximately 95.432%. The success rate is too high to be neglected.

Figure 4. *The Simulation of the use Case without Countermeasures Delivers a Success Rate of 95.432%.*



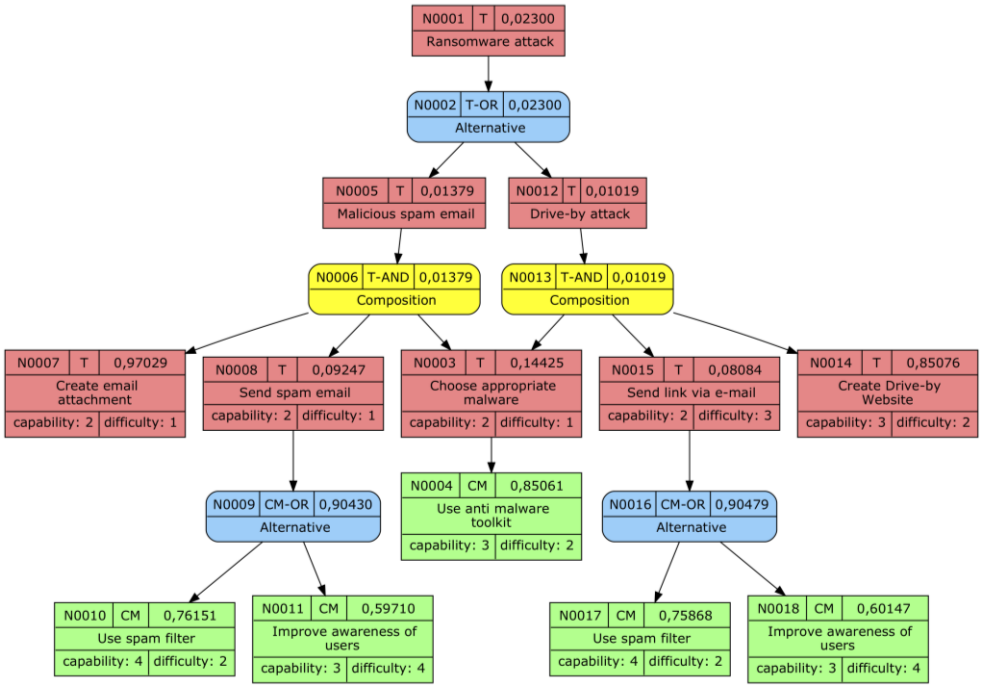
The second simulation runs on the graph with all countermeasures enabled (Figure 5). The result is that the countermeasures reduce the success rate to 2.3%. Interpretation: the risk of a ransomware attack can be effectively minimized by applying all countermeasures.

Table 2. *Sensitivity Analysis of the Usage of an anti-Malware Toolkit (node N0004)*

capability	difficulty	success rate
6	6	0.14551
6	5	0.13320
5	6	0.13051
5	5	0.11903
6	4	0.11720
4	6	0.11690
5	4	0.10623
4	5	0.10619
4	4	0.09512
3	6	0.07384

capability	difficulty	success rate
6	3	0.07324
5	3	0.06768
3	5	0.06725
4	3	0.05908
3	4	0.05903
6	2	0.04496
5	2	0.03836
3	3	0.03646
4	2	0.03437
3	2	0.02187

Figure 5. *Applying the Countermeasures Lowers the Success Rate to 2.3%.*



The usage of an anti-malware toolkit (node N0004) is a central countermeasure in the sense that it influences both attack paths. Hence, it is important to analyze the consequences of a wrong assessment of this node. This is done by changing both the capability and the difficulty of the node and performing another Monte Carlo simulation on the modified attack defense graph. The result is displayed in [tab: anti-malware-sensitivity]. The simulation shows that in the worst case the success rate of the ransomware attack is seven times higher (capability 6, difficulty 6) than in the initial assessment.

From an economic point of view, the deployment of IT security mechanisms results in costs such as license fees or working time of the IT department. A legitimate question is which of the counter measures can be omitted without significantly increasing the risk of a successful attack. These kind of questions can be answered by modifying the attack defense graph. In the use case of the ransomware attack, the implementation of the countermeasures (nodes N0011 and N0018) might cost a non-negligible amount of money. What happens if these countermeasures are omitted? Changing the attack defense graph and performing a Monte Carlo simulation shows that this results in a success rate of 5.233%.

Formal Aspects

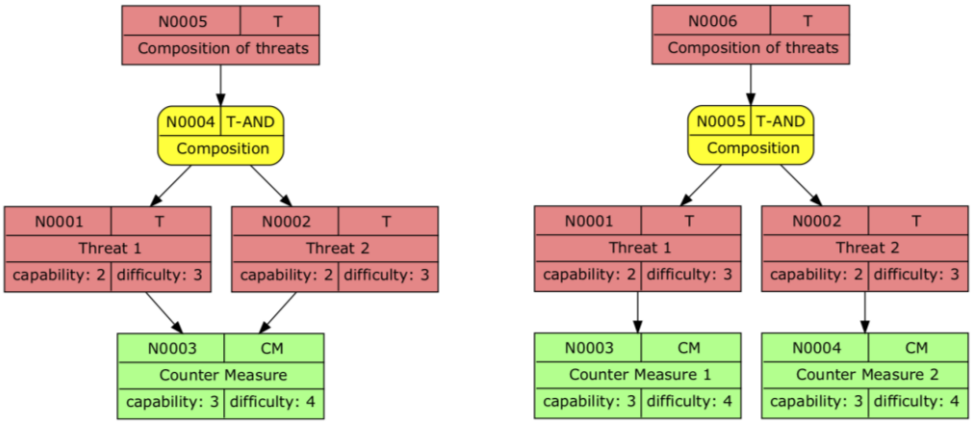
A fundamental assumption of the model is the independence of the leaf nodes. Using this assumption and a pocket full of mathematics, several facts can be derived which help to understand the behaviour of the model. These facts help to find errors in the implementation of the simulation system.

In the following T_1 and T_2 denote the event that the threat T_1 or the threat T_2 is successful, respectively. The events C, C_1, and C_2 are defined analogously with respect to countermeasures.

Fact 1. If T_1 and T_2 are independent, then
$\Pr[T_1 \cap T_2] = \Pr[T_1] \cdot \Pr[T_2]$,
and
$\Pr[T_1 \cup T_2] = 1 - \Pr[\overline{T_1}] \cdot \Pr[\overline{T_2}]$.

The first equation represents a composition of threats, the second one represents an alternative of threats. The fact applies to countermeasures too and can be extended to any number of independent events.

Figure 6. *Two ways to apply Countermeasures to a Composition of Threats*



a) One countermeasure for both threats b) one countermeasure per threat

A common situation during the modeling phase of a threat assessment is choice of preventing two threats together with one single countermeasure or with one countermeasure per threat (see (Figure 6)). The following two facts model the situation in the case of a composition (and) of two threats. Fact 2 addresses the first case ((Figure 6) a), fact 3 addresses the second case ((Figure 6) b).

Fact 2. If the events T_1, T_2 and C are independent, then
$\Pr[(T_1 \cap T_2) \cap \overline{C}] = \Pr[T_1] \cdot \Pr[T_2] \cdot \Pr[\overline{C}]$.

Fact 3. If the events T_1, T_2, C_1 and C_2 are independent, then
$\Pr[(T_1 \cap \overline{C_1}) \cap (T_2 \cap \overline{C_2})] = \Pr[T_1] \cdot \Pr[\overline{C_1}] \cdot \Pr[T_2] \cdot \Pr[\overline{C_2}]$.

If $\Pr[C] = \Pr[C_1] = \Pr[C_2]$, then the following inequality can be derived from fact 2 and fact 3:

$$\Pr[(T_1 \cap \overline{C}) \cap (T_2 \cap \overline{C})] < \Pr[(T_1 \cap \overline{C_1}) \cap (T_2 \cap \overline{C_2})].$$

This inequality can be interpreted as follows: in the case of a composition of two threats, it is better to mitigate the risk of each threat with a separate countermeasure than to handle both threats together with one single countermeasure.

The next two facts consider the two cases in the case of an alternative (or). Fact 4 addresses the usage of one countermeasure for both threats, fact 5 addresses the treatment of each threat with one separate countermeasure.

Fact 4. If the events T_1, T_2 and C are independent, then
$\Pr[(T_1 \cup T_2) \cap \overline{C}] = (1 - \Pr[\overline{T_1}] \cdot \Pr[\overline{T_2}]) \cdot \Pr[\overline{C}]$.

Fact 5. If the events T_1, T_2, C_1 and C_2 are independent, then
$\Pr[(T_1 \cap \overline{C_1}) \cup (T_2 \cap \overline{C_2})] = 1 - (1 - \Pr[T_1] \cdot \Pr[\overline{C_1}])(1 - \Pr[T_2] \cdot \Pr[\overline{C_2}])$.

If $\Pr[C] = \Pr[C_1] = \Pr[C_2]$, then the following inequality can be derived from fact 4 and fact 5:

$$\Pr[(T_1 \cup T_2) \cap \overline{C}] < \Pr[(T_1 \cap \overline{C_1}) \cup (T_2 \cap \overline{C_2})].$$

This inequality can be interpreted as follows: in the case of an alternative of two threats, it is better to handle both threats together with one single countermeasure than to mitigate the risk of each threat with a separate countermeasure.

Implementation Aspects

This section provides some details on the lessons learned from the implementation of the simulation system.

Rapid Prototyping with Python

The first step in the implementation process was a rapid prototyping approach with Python[2]. The application was designed in an object oriented fashion. As expected, the development was done in short period of time.

While working with Python, we benefited from the simplicity of this programming language. Especially the dynamic typing of the variables during run-time and the required formatting of the code with indentations supported to make a good progress. Another advantage are the built-in data structures such as lists and dictionaries which simplify the implementation of common algorithms such as graph algorithms.

The Python ecosystem consists of lots of additional packages which can be installed easily with the Package Installer for Python (PIP). Two of these packages turned out to be very useful in our software protect and are described briefly in the following.

[2]Webpage: https://www.python.org

In the development of the simulation system the possibility of cloning an attack defense graph was needed. This is, an exact copy of the graph had to be created which is in a different memory location than the original one. Thy Python module *copy*[3] provides with the command deepcopy() exactly the required functionality. The command recursively creates a copy of an object and all the objects it does contain.

In order to simulate an attack defense graph with different node assessments, it is necessary to iterate through a given range of capability or difficulty values. For example, in the above use case, the impact of an anti-malware toolkit (node N0004) was analyzed by simulating the attack defense graph for each of the capability difficulty pairs from in the set $\{3,4,5,6\} \times \{2,3,4,5,6\}$. Programming in Python, this can be done easily by using the module *itertools*[4] which provides building blocks for iterators based on a given set of values. This module helped a lot in creating different simulation scenarios.

After the prototype of the simulation system was completed, it was used to analyze several use cases. While working with the software, several drawbacks of the Python language did arise. At first, since Python is an interpreted programming language, many errors in the code pop up during the execution of the program. Furthermore, the execution of the interpreted code is slow compared to the code of a compiled programming language such as C++ or Java.

Another disadvantage is the Python global interpreter lock (GIL), which controls the execution of threads in such a way that only one thread is executed at a point of time. As a consequence, implementing a multi-threaded simulation approach does not improve the performance of the simulation system, since at a time only one thread can be executed. The power of a multi core CPU is not maxed out because only one core is used. A solution is the implementation of a multi process approach with interprocess communication which is more complex compared to multithreading. For more details, we refer to (Gorelick and Ozsvald, 2014).

Besides of its drawbacks, rapid prototyping with Python was the right decision, because the simulation tool could be put into work within a very short period of time. It provided a lot of knowledge which turned out be useful in further progress of this project.

Re-Implementation with Java

The major drawback of the Python implementation was its mediocre performance and the restricted support of multithreading. Hence, we decided to do a re-implementation with the programming language Java[5]. Java was chosen because of its platform independence and the large availability of third party software packages. The re-implementation started with Java 8. Later, we switched to Java 11, the current version with long term support.

[3]Webpage: https://docs.python.org/3/library/copy.html.
[4]Webpage: https://docs.python.org/3/library/itertools.html.
[5]Webpage: https://www.oracle.com/technetwork/java/index.html.

The project was designed as a multi-module architecture which made use of the Java Platform Module System (JPMS) which was introducted in Java 9. Simply spoken, JPMS enables the separation of the code into several modules. Each module must have an unique name and must specify the dependencies on other modules. In particular, it must be specified which elements of the module are accessible. The benefit of this approach is an increase of reliability of the software and a better encapsulation of the software packages. The interested reader finds more information on Java modules in chapter 12 of (Flanagan and Evans 2018).

Since the Java SE Development Kit does not include a build tool which automatically takes care of module dependencies, Maven[6] was chosen as the software management and build toolkit. The layout of the project was a multi-module one. For each module, a project object model (POM) had to be created. The POM includes, among other things, the dependencies of the module and the instructions to build and package the module. The format of a POM file is XML.

The re-implementation with Java resulted in a software with improved running times and proper multithreading support. Compared to Python, the development in Java was more time-consuming. Since Java did not provide modules with the functionality of Python's copy and itertools modules, additional work had to be spent on implementing these features.

Conclusion

This paper describes the application of a risk assessment model to the use case of a threat induced by ransomware attack. The model is based on attack defense graphs and Monte Carlo simulations. The model was successfully implemented with Java. The analysis of the ransomware use case demonstrated how to apply the model to practical problems arising in the area of cyber security risk assessment. The use case shows how the model can help security specialists to find out appropriate countermeasures to mitigate common threats on computer systems. The effort of applying this model is moderate compared to other risk assessment methods. As a consequence, the model is appealing to small and medium-sized enterprises which can use the model for decision-making on it security solutions with moderate costs.

References

Blakley B, McDermott E, Geer D (2002) Information Security is Information Risk Management. *Proceedings of the 2001 Workshop on New Security Paradigms*.

Cremonini M, Martini P (2005) Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). In *4th Workshop on the Economics on Information Security.*

[6]Webpage: https://maven.apache.org.

Edge KS, Dalton GC, Raines RA, Mills RF (2006) Using Attack and Protection Trees to Analyze Threats and Defenses to Homeland Security. *Military Communications Conference, Milcom 2006*, IEEE.

Ericson CA (1999) Fault Tree Analysis - a History. In *17th International System Safety Conference*.

Flanagan D, Evans B (2018) *Java in a Nutshell* (7th ed.). O'Reilly Media, Inc.

Forum of Incident Response and Security Teams (Ed.). (2019). *Common Vulnerability Scoring System v3.1: Specification Document*. Retrieved from https://bit.ly/2m8c Ssz.

Fraile M, Ford M, Gadyatskaya O, Kumar R, Stoelinga M, Trujillo-Rasua R (2016) Using Attack-Defense Trees to Analyze Threats and Countermeasures in an atm: A Case Study. In *The Practice of Enterprise Modeling, Poem 2016:* 326–334. Springer.

Gorelick M, Ozsvald I (2014) *High Performance Python*. California: O'Reilly.

Hänisch T, Karg C (2019) *Using Monte Carlo Simulation to Estimate the success of it Security Measures in Industry 4.0 Environments*. Presented at 15th Annual International Conference on Information Technology & Computer Science, 20-23 May 2019, Athens, Greece.

Kordy B, Mauw S, Radomirović S, Schweitzer P (2014) Attack–Defense Trees. *Journal of Logic and Computation* 24(1): 55–87.

Kumar R, Stoelinga M (2017) Quantitative Security and Safety Analysis with Attack-Fault Trees. *18th International Symposium on High Assurance Systems Engineering*, IEEE.

Lund MS, Solhaug B, Stølen K (2011). *Model-Driven Risk Analysis: The CORAS Approach*. Berlin, Heidelberg: Springer.

Mauw S, Oostdijk M (2006) Foundations of Attack Trees. In: Won D.H., Kim S. (eds) *Information Security and Cryptology - ICISC 2005*. ICISC 2005. Lecture Notes in Computer Science, vol 3935. Berlin, Heidelberg: Springer.

OWASP (Ed.). (2019, June 27). *OWASP Risk Rating Methodology*. Retrieved from https://bit.ly/1BJAUe8 [Accessed 13 July 2019].

Schneier B (1999a). Attack Trees. *Dr. Dobb's Journal of Software Tools* 24(12): 21–29.

Schneier B (1999b) *Attack Trees*. Retrieved from https://bit.ly/2IcpbcC

Vesely W E, Goldberg FF, Roberts NH, Haasl DF (1981). *Fault tree handbook* (No. NUREG-0492). U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Division of Systems; Reliability Research.

Evaluation of Human Exposure owing to Wireless Power Transfer Systems in Electric Vehicles

By Adel Razek[*]*, Lionel Pichon*[±]*, Abelin Kameni*[♠]*, Ludovic Makong*[♦] *& Sahand Rasm*[•]

This paper presents a general overview of wireless power transfer systems (WPT) for charging batteries in electric vehicles (EV), focusing on human exposure surveys. After describing the schematics and strategies of the two WPT problems, static (stationary parking) and dynamics (road travel), we examined the problem of exposure to radiation fields attributable to WPT systems in humans and more generally living tissues. We first study how to predict these radiated fields and examined their compliance with international standards. A model used the human body derived from magnetic resonance imaging and high resolution. It was also developed a mode by numerical computations with the method of the finite elements. An exposure assessment of a characteristic wireless inductive charging system was provided to estimate the induced electromagnetic fields. We counted the worst configuration for the exposure assessment of the wireless charging system. In a second step, we studied the sensitivity of the exposure level, taking into account the uncertainty of the parameters characterizing the electromagnetic problem. Stochastic models, helped study exposure level of an inductive power transfer system. Two non-intrusive approaches were associated with a 3D finite element method to construct adequate meta-models: the Kriging and Polynomial Chaos extensions. These two techniques proved to provide powerful tools for characterizing human exposure at 85 kHz, which is a typical frequency of inductive charging of electric vehicles.

Keywords: *Electric Vehicles, Wireless Power Transfer, Battery Charging, Human Exposure, Stochastic Approaches.*

Introduction

The automotive industry is currently undergoing profound technological change in a context where environmental concerns are at the forefront. Constraints in terms of CO_2 emissions have pushed the manufacturers to develop a "cleaner" concept such as electric vehicles (EV). Such a vehicle currently uses a standard cable connection for charging that may include annoying and/or inconvenient items for the user. In this context, the non-contact inductive power transfer (IPT) charger is an interesting substitute.

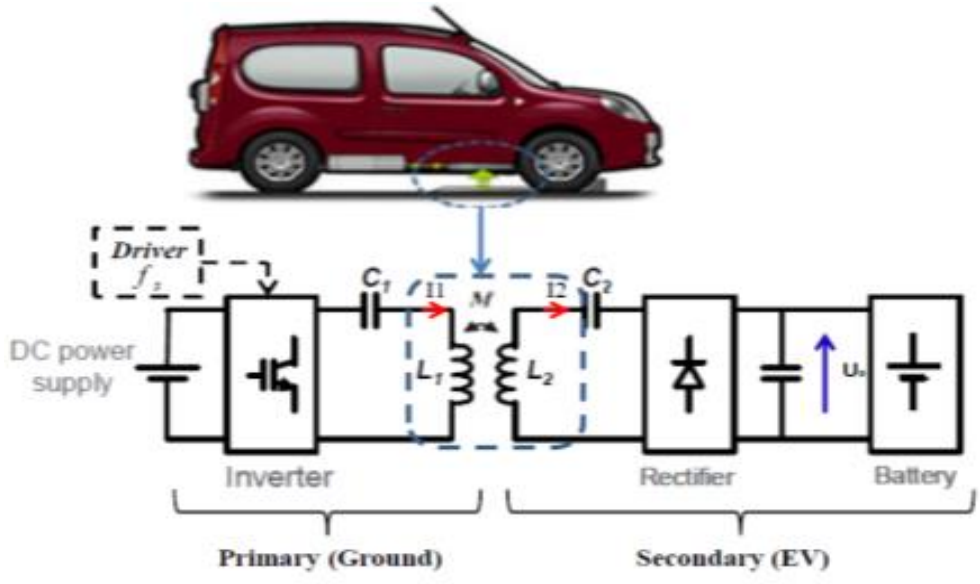
The two essential theories that manage the IPT are the Ampere's law of 1820 and the principle of magnetic induction found by Faraday in 1831. While Ampere

[*]Emeritus Research Director, C.N.R.S. & Honorary Professor, CentraleSupelec, GeePs, University of Paris-Saclay and Sorbonne University, France
[±]Research Director, C.N.R.S., GeePs, University of Paris-Saclay and Sorbonne University, France
[♠]Associated Professor, GeePs, University of Paris-Saclay and Sorbonne University, France.
[♦]PhD, Research Engineer, GeePs, France
[•]MSc Student, GeePs, France.

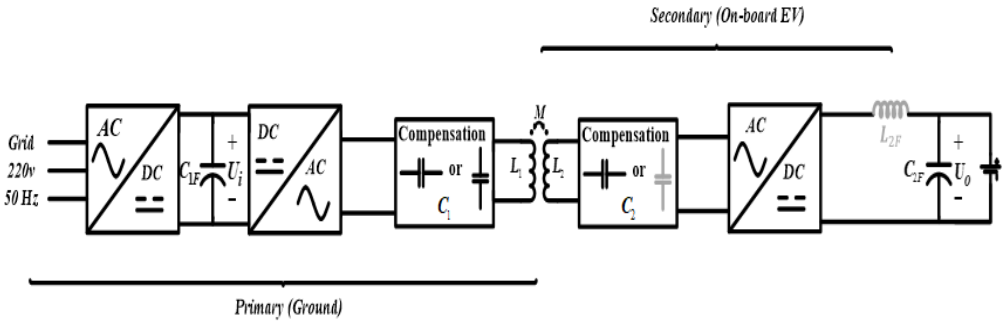
showed that a current could produce a magnetic field, Faraday revealed the duality between the magnetic and the electric field demonstrating that a time-varying magnetic field can be interacting with an electrical circuit in order to induce into it an electromotive force. These two principles are allowing abundant applications commanding the development of the modern energy conversion devices. The first real improvement in the direction of IPT arrived with Tesla's studies.

Nikola Tesla (1856-1943) first introduced wireless power transfer in the 1890s (Tesla 1904), but it was only recently that this technology has been widely exploited for societal applications. In particular, the extension of resonant wireless energy technology can be used for the charging of many everyday devices. Various terms, including inductive power transfer (IPT), inductive coupling, and resonant power transfer, are generally referred as wireless power transfer (WPT). These different terms are designated to the same essential procedure - the transfer of energy from a power source to a load, without contact, through an air gap. A wireless energy transfer system consists essentially of two coils - a transmitter and a receiver.

Figure 1. *IPT Charging System for EV: (a) System Arrangement (b) Electric Circuit*



(a)



(b)

This solution offers in the case of EV simplicity of use, a speed and a decent resistance to damage of cables. The objective was to transfer energy from the ground to the vehicle (on board battery) by an inductive loop system (a transformer), as shown in Figure 1 (Ibrahim et al. 2015). This device required reaching a good performance and positioning tolerance (transmitter - receiver coupling). The coupling between the transmitter, which was placed on the ground, and the receiver, which was placed under the floor of the vehicle, was functioning through a large gap. This large space implies a high level of parasitic field near the coils, which can pose a problem of exposure to magnetic fields for passengers or persons likely to approach the vehicle during charging operations. It is therefore necessary to evaluate the level of exposure in order to comply with international safety instructions (ICNIRP 2010).

The use of wireless inductive power transfer (IPT or WPT) is becoming an effective technology for the growth of electric mobility (Cirimele et al. 2018). In addition, with the increasing number of current research attractions and the expected intensification of the practice of such wireless charging systems for electric vehicles, it is important to initiate research efforts to wireless charging systems and the human body (Ding et al. 2014).

WPT systems could be used in static, parking mode (Ibrahim 2014) or when moving the vehicle dynamically (Cirimele 2017). The dynamic mode, even more complicated in its operational control and the need for specific infrastructures, offers the possibility of overcoming the barriers represented by the heavy storage of the battery on board, the long charging time and the limited autonomy in the case of static mode. The parasitic field level near the coils due to the large air gap can be different between static and dynamic modes, and is due to the nature and operation of the coils in both cases. In addition, the constraints of field exposures differ between the two modes; however, the exposure assessment strategies are more or less similar.

Two features mainly motivate the research efforts to interact between the wireless charging systems and the human body. One has to estimate the induced electromagnetic fields in the human body at the frequency of the wireless charging system, i.e., magnetic flux density, electric field, and current density, to evaluate the potential health effects, as well as to examine the compliance with standards defined by International Commission on Non-Ionizing Radiation Protection (ICNIRP), see (ICNIRP 2010). The other aspect was to examine the impact of the input current of the wireless charging system on the radiation levels and make available the valid data for determining the extent of design liberty of IPT systems. Much research has been dedicated to the investigation of human exposure to the electromagnetic environment, such as handset antennas and the wireless resonance power system, see for example (Okoniewski and Stuchly 1996, Shiba and Higaki 2009, Christ et al. 2013). The operating frequency derived mainly from megahertz to gigahertz.

However, due to electromagnetic compatibility and energy efficiency, the IPT system for electric vehicles, generally operates in lower frequency range (from a few kilohertz to around 100 kHz). In this frequency range, exposure studies to wireless inductive charging systems have not been enough so far. Since fields

close to the IPT system can engender high fields in the body tissues of nearby humans, we need to identify the conditions under which the IPT system can demonstrate compliance with international safety guidelines (ICNIRP 2010, IEEE Standard 2005). The evaluation of exposure of human tissues to magnetic fields needs usually suitable and sufficient modeling methodologies, based on 3D computations applied for solving the electromagnetic problem involving the wireless system, the vehicle, and the human body (ie. in the vehicle or located beside), see for example (Ding et al. 2014). In this work, an assessment focuses on the electromagnetic fields induced by a representative inductive wireless charging system in the human body. Constructed MRI (Magnetic Resonance Imaging) models produced human anatomical models with high resolution compatible with the numerical approach. A 3D numerical approach providing a scientific estimate of human exposure to this system was developed. In addition, an evaluation of the electromagnetic exposure presented both normal and unfavorable configurations.

In order to assess human exposure near WPT systems in automotive applications, adequate systematic modeling methodologies have to be developed. Recently 3D computational models have been studied and applied for solving the electromagnetic problem involving the wireless system, the vehicle, and the human body in the vehicle or located beside vehicle, see (Park 2018, Cirimele et al. 2017, Cimala, et al. 2017 and Campi et al. 2017). Such full wave computational approaches give reliable results about the radiated fields around the system or induced quantities in the human body; however, this may lead to heavy computations that need to be repeated for each new configuration. A key point in such problems is that the level of exposure is highly dependent on various parameters: shape or size of coils, geometrical characteristics of the system (structural parts of the vehicle and shielding plates), materials properties (ferrites and chassis of vehicle), possible misalignment between transmitter and receiver while charging, and position of the human body. Moreover, some uncertainty can affect each physical or geometrical parameter. Therefore, during the design of the IPT system, the consideration of level of exposure cannot only rely on deterministic full 3-D solvers. In this situation, the introduction of stochastic tools allows to deal with the variability of all the parameters which are describing the electromagnetic problem. Such approaches can be very efficient in the framework of the determination of specific rate absorption (SAR) in biological tissues due to mobile phones at microwave frequencies.

The first objective of this article was to present a general overview of wireless energy transfer systems in electric vehicles, focusing on human exposure surveys. After having illustrated the problems and strategies of the two WPT categories, static (stationary parking), see for example (Ibrahim et al. 2015) and dynamic (road travel), see for example (Cirimele et al. 2016), we examine the problem of exposure to radiation fields attributable to WPT systems in humans and more generally in living tissues.

In the second objective of this work, we studied the sensitivity of the exposure level taking into account the uncertainty of the parameters characterizing the electromagnetic problem. Due to this aim, we compared different stochastic methods during the investigation of the compliance of IPT systems with

international standards, regarding the human exposure. We focused on so-called non-intrusive methods that use 3D finite element computations with a limited set of realizations. Kriging and Polynomial chaos have already shown their interest in numerical dosimetry and optimization in the case of extremely low frequency (50 Hz), see (Lebensztajn et al. 2004 and Gaignaire et al. 2012) or wave propagation problems, see (Voyer et al. 2008 and Kersaudy et al. 2014). In this paper, the two techniques provided powerful tools to characterize the human exposure at 85 kHz, which is a typical frequency for inductive charging of electrical vehicles.

Wireless Power Transfer WPT

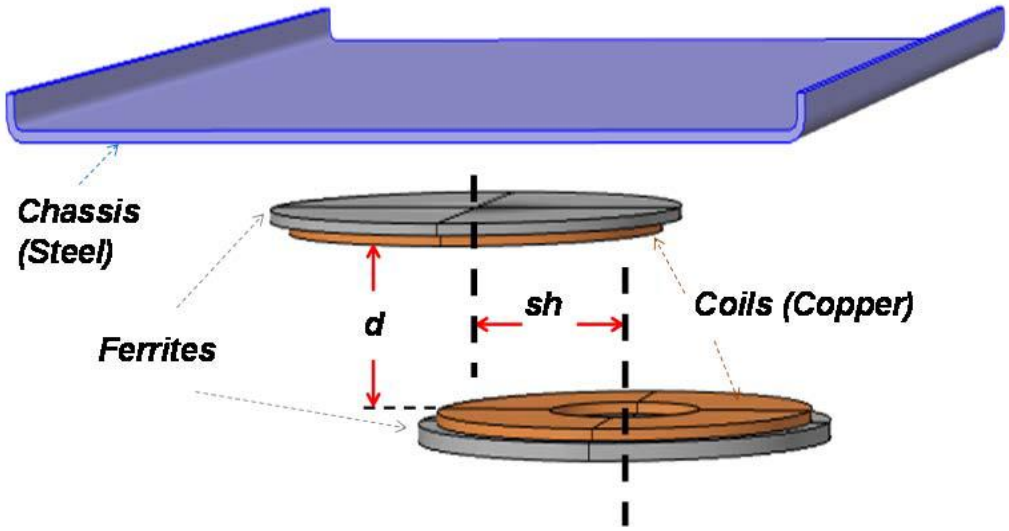
Static WPT

An IPT system for charging battery of a static EV, is represented in Figure 1. It is composed of an electrical source, a load (battery) and in between an inductive coupler transformer (ICT) with shielded coils. Planar parallel axes shielded coils could produce concerning the ICT structure, one of the most proficient magnetic flux transfers. In such a situation, the energy transfer functions overall receiver surface and shielding that is used to improve the mutual inductance (M) by increasing the magnetic flux between the two coils. The shielding is accomplished by a magnetic almost none conducting material and ferrite is usually used.

The complete scheme is composed of two major parts: the ICT that allows the wireless transfer through the magnetic induction and that ensures a galvanic insulation between the source and the load. The second feature comprises the capacitive compensations and the power electronics connected to ICT, which manages the arrangement to operate at resonance. The whole system practices IPT system. Between the grid and the ICT, there are two conversion steps: grid low frequency AC to DC, and DC to AC high frequency. These conversions allow regulating the power quantity by controlling the input voltage and the frequency. Between the ICT and the battery, a finishing conversion from high frequency AC to DC permits granting energy to the battery. The air gap of the ICT is large and then the coupling is weak. Therefore, administering the high reactive power is required in order to reach the required transferred power, and the use of resonant elements in both sides of the ICT is indispensable as compensation to guarantee good efficiency. In addition, control of the output parameters at the load side is needed in order to monitor the battery charging profile and to insure its protection.

A structure of the ICT coupler is shown in Figure 2. It consists of a transmitter coil, a receiver coil and two ferrites plates that completely cover the coils. The design included a steel plate that represented the EV chassis. The two ICT coils with their ferrites (pads) are identical with an air gap distance (d), and axes shift (sh), in the case of Figure 2, which corresponds to the EV position on the ground. In societal applications situation, the two coils (and generally pads) forms may be different depending on constructors of EVs and IPTs. Therefore, in such case, we need to perform an interoperability analysis (Ibrahim et al. 2016).

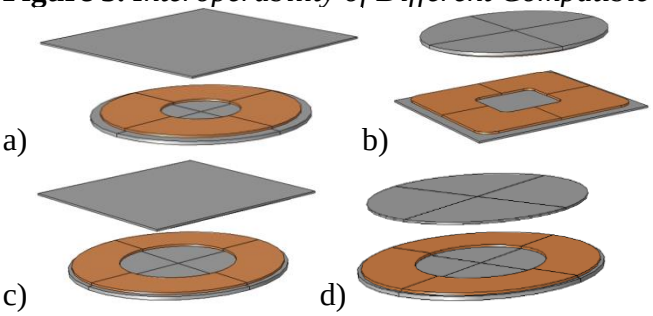
Figure 2. *3-D Structure of an ICT with Shielding, Simple EV Chassis*



Generally, we can use 3D electromagnetic field computations, forexample the finite elements method (FEM) simulations, for the ICT considering the whole structure of the IPT (see Figure 2) for the determination of its mutual coupling and inductances (see Figure 1). The effect of shielding using coil-closed ferrites to reduce the leakage fields and to border the penetration of the field within the vehicle required consideration in such simulations. Moreover, in the structure of the IPT system the EV chassis was modeled (Ibrahim 2014). In fact, the presence of the EV chassis modifies the field values, and hence the matching inductances of the power system and the electromagnetic compatibility (EMC) radiation level. After deducing the mutual coupling and inductances of the ICT, accounting for the IPT structure from the field values, an electrical circuit model of the whole system including the resonance topology was established (Figure 1).

As mentioned before, in practice we need an interoperability analysis concerning the forms and surfaces of the pads (coils/ferrites) of ground regarding those of EVs. This analysis concerns the position of EV pad in the vehicle (middle or backend), the tolerance to positioning of vehicle, the human exposure recommendations, the efficiency, the sizes of power components of the IPT. A detailed analysis of this question is presented in Ibrahim et al. (2016). Figure 3 shows different examples of compatible pads.

Figure 3. *Interoperability of Different Compatible Prototypes*



Dynamic WPT

In the last section, we discussed static IPT. Such technology indicated as static, when the vehicle parked or motionless during charging, will likely replace the wired systems. However, the absence of mechanical stresses, in the course of charging, suggests the possibility of using the inductive transfer when moving the vehicle that uses the dynamic IPT. In such a case, the receiver of the IPT installed on the bottom of the vehicle will move over successive transmitters fixed on the ground infrastructure (Figure 4).

The putting in place of dynamic IPT systems in the road infrastructure will abolish the need for charging stops and, in the short term, this appliance could result in a significant reduction in the size of the battery installed on-board. The successful demonstration of the feasibility of this technology may indicate a concrete approach to improve the acceptance of electric mobility and to solve the most critical aspects of the use of electric vehicles.

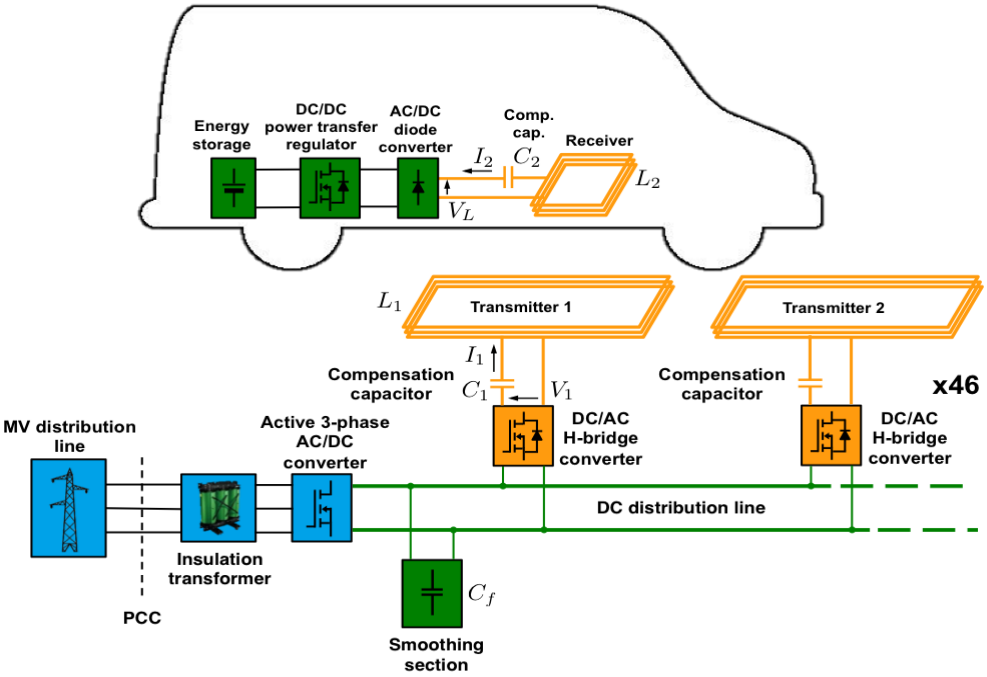
An important technical problem for the dynamic IPT is the identification of the vehicle when it approaches a transmitter and the management of the passage between the successive transmitters. Moreover, as in the case of static IPT, there is the aspect of protection against exposure to magnetic fields generated in the dynamic IPT.

Figure 4. *Dynamic IPT*

Finally, there is the vast quantity of defies represented by all the aspects related to the establishment of the road infrastructure. In particular, the insertion of the emitting portion in the pavement, the choice of material for the coating, the management of the rainwater, the need to communicate with the relating management infrastructure.

Different recent works are concerned by these aspects, see for example (Cirimele 2017) – Figure 5.

Figure 5. *Scheme of the General Architecture of the IPT System Developed for On-the-Road Prototype (Cirimele, 2017)*



Human Exposure

As mentioned before, the large space between the two coils of IPT in either of static or dynamic cases implies a high level of parasitic field near the coils. This situation posed a problem of exposure to magnetic fields for passengers or persons likely to approach the vehicle during charging operations. Therefore, to comply with societal health safety, it was necessary to evaluate the level of exposure concerning the international safety instructions (ICNIRP 2010).

Prediction of Radiated Fields

The evaluation of exposure of living tissues to magnetic fields needs generally adequate modeling methodologies based on 3D computations applied for solving the electromagnetic problem involving the wireless system, the vehicle and the human body (in the vehicle or beside vehicle). In such computations, the considered human body model is very important. The most critical aspects governing the choice of such a model are fidelity to physical biological characteristics of realistic situation and the adaptability to the used computational methodology. There are considerable research efforts devoted to the construction of human body models. Usually, the computations of electromagnetic fields in human body require computer-adapted models of the human body and a comprehensive information of the dielectric properties of human tissues for a given frequency. These models are of two categories, homogeneous and non-

homogeneous. For homogeneous ones, the dielectric properties of the human body are generally attributed to a 2/3 equivalent muscle model (Harris et al 2011). For non-homogeneous human models, ghost models of layered tissue are founded on magnetic resonance imaging (MRI), computed tomography and digital imaging techniques, offering precision of tissue shape to the nearest millimeter (Gjonaj et al. 2002, and Steiner et al 2006). The dielectric properties of biological tissues are described in Hasgall et al. (2012) and Gabriel et al. (1996). A comprehensive description of the accessible measurement data for dielectric permittivity and electrical conductivity for any specified frequency was specified by Gabriel et al. (1996).

Conformity with International Standards

The fields close to the IPT systems can produce high fields in the body tissues of nearby humans and we need to characterize the conditions under which the IPT system can validate agreement with international safety guidelines (ICNIRP 2010, IEEE Standard 2005). The evaluation of exposure of human tissues to magnetic fields needs suitable and complete modeling methodologies based on 3-D computations for solving the electromagnetic problem involving the wireless system, the vehicle and the human body (Ding et al. 2014).

Figure 6. *Vertical Body and Wireless Inductive Charging System*

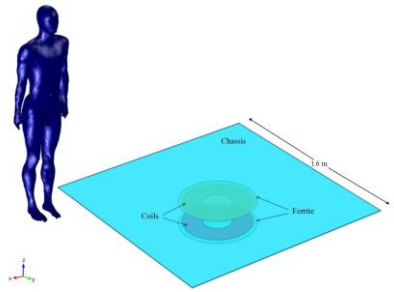
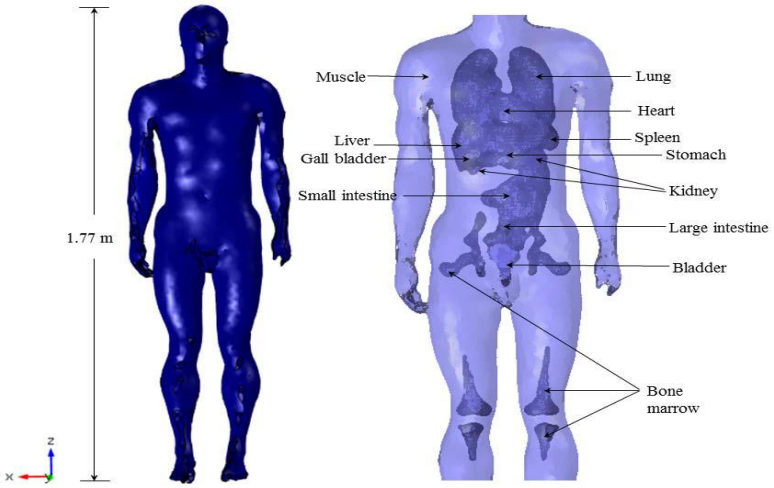


Figure 7. *Anatomical whole Body Model and its Different Tissues and Organs of Interest*



The configurations studied involving the human body, the IPT coils with ferrites and the chassis shown schematically in Figure 6. The study considers the two cases of vertical and horizontal positions of human body. The high-resolution human anatomical model compatible with the numerical approach constructed from human MRI models, as shown in Figure 7. Examples of results obtained in (Ding et al. 2014) are shown in Figures 8 and 9 corresponding to positions: vertical and horizontal (laying the ground) respectively. The obtained results confirm the agreement with international safety guidelines (27 μT for the magnetic induction B and 4.05 V/m for electric field E).

Figure 8. *Distribution of Induced Fields inside the Anatomical Human Body for the Configuration of Figure 6. (a) Magnitude of Magnetic Flux Density B (T), (b) Magnitude of Electric E-field (V/m) (Ding et al 2014)*

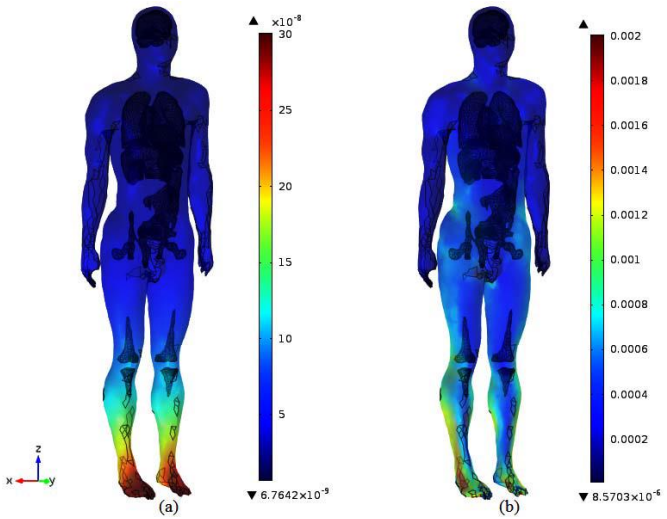
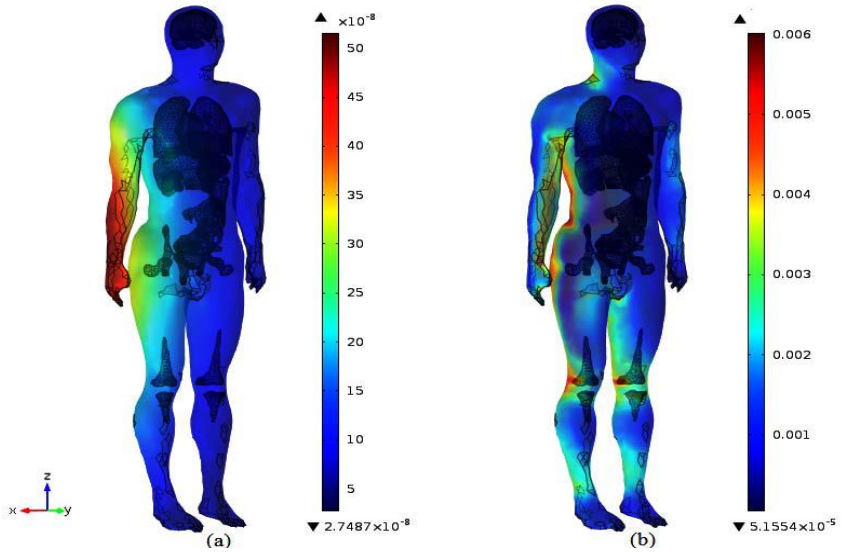


Figure 9. *Distribution of Induced Fields inside the Anatomical Human Body for the Configuration of Horizontal, Ground Lying Body. (a) Magnitude of Magnetic Flux Density B (T), (b) Magnitude of Electric E-field (V/m). (Ding et al 2014)*



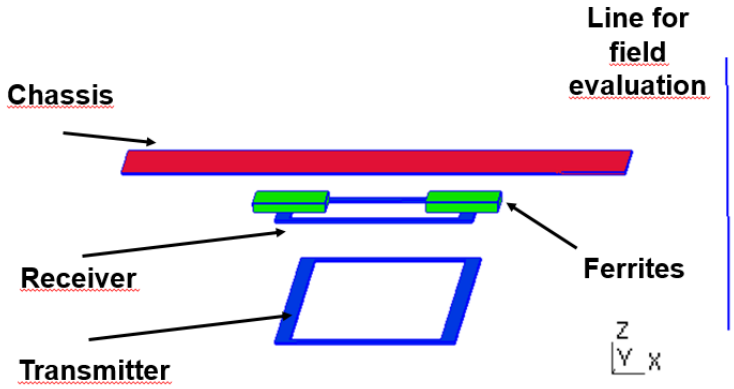
Non-Intrusive Stochastic Approaches

As mentioned before, the objective of this work was to compare different stochastic methods when investigating the compliance of IPT systems with international standards regarding the human exposure. We focused on so-called non-intrusive methods that use 3-D finite element computations with a limited set of realizations.

Wireless Power Configuration

The structure model of the system considered in this work contains two rectangular coils (transmitter and receiver), and two ferrites plates (Cirimele, 2017). The design also includes a steel plate that represents the chassis of the electric vehicle (Figure 10).

Figure 10. *Studied Configuration of Wireless Transfer System (Cirimele, 2017)*



The dimensions of the system are shown in Table 1.

Table 1. *Dimensions of Figure 10*

	Width (m)	Length (m)
Transmitter	0.5	1.5
Receiver	0.525	0.3
Ferrites	0.2	0.25
Chassis	1.5	0.5

The relative permeability of ferrites is 2000. Each coil has 10 turns. A 3-D vector potential formulation has solved the magneto-dynamic problem. This system has been designed for dynamic charging but in the present work, only a static charging scenario was considered. The power electronics controls and keeps the *rms* value of the current in the transmitter at 36 A, and the current in the receiver at 75 A, respectively. The electromagnetic quantities were evaluated along the vertical line located at 1m from the axis of the transmitter (Figure 10).

Stochastic Models

In this work investigated two non-intrusive stochastic methods: Kriging and Polynomial Chaos.

Kriging

Kriging is a stochastic interpolation algorithm that assumes that the model output M(x) is a realization of a Gaussian process indexed by the inputs x. A Kriging meta-model was described by the following equation:

$$M(x) \sim M^K(x) = \beta^T f(x) + \sigma^2 Z(x, \omega) \qquad (1)$$

The first term in (1), is the mean value of the Gaussian process (trend) and it consists of the regression coefficients βj (j = 1…P) and the base functions fj (j = 1,…P). The second term in consists of σ^2, the (constant) variance of the Gaussian process and Z(x, ω), a zero mean, unit variance, stationary Gaussian process. The underlying probability space was represented by ω and was defined in terms of a correlation function R and its hyper-parameters θ The correlation function R = R(x; x_0; θ) described the correlation between two samples of the input space, *e.g.* x and x_0 and depends on the hyper- parameters θ. In the context of meta-modelling, it is of interest to calculate a prediction M^K(x) for a new point x, given X = (x_1…x_n), the experimental design, and y = (y_1 =M(x_1),…, = M(x_n)), the corresponding (noise-free) model responses. A Kriging meta-model (Kriging predictor) provided such predictions based on the Gaussian properties of the process.

Polynomial Chaos Expansion

The polynomial chaos is a spectral method and consists in the approximation of the system output in a suitable finite-dimensional basis Ψ(X) made of orthogonal polynomials. A truncation of this polynomial expansion can be as follows:

$$M(x) \sim M^{PC}(x) = \sum_{0}^{P-1} \propto_j \Psi_j(X) \qquad (2)$$

where M(x) is the system output, X is the random input vector made of the input parameters x_i, Ψ_j are the multivariate polynomials belonging to Ψ(X), α_j are the coefficients to be estimated, ε is the error of truncation, and P is the size of the polynomial basis Ψ(X). Each multivariate polynomial Ψ_j was built as a tensor product of univariate polynomials orthogonal with respect to the probability density function of each input parameter x_i. In the present work, the value of P around 15 provided reliable results. Here, inputs used Gaussian distributions, and the corresponding polynomial families were the Hermite polynomials families.

The coefficients in (2) are estimated from spectral projections or least-square regressions.

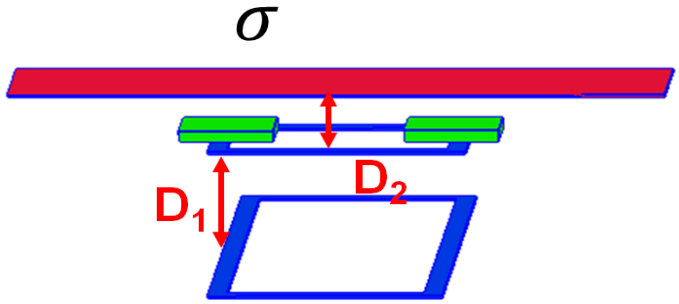
Results

Marelli and Sudret (2014) developed the two stochastic models described above and used in this paper. The models were proposed in the framework for uncertainty quantification in UQLab (www.uqlab.com) and are freely available. Configurations were applied in the two previous approaches (refer to Figure 10) to check the compliance regarding the references levels of radiated magnetic field. For the frequency of interest (85 kHz), the maximum admissible value of the magnetic flux density was 27 µT according to the ICNIRP Guidelines (ICNIRP 2010).

First Configuration

In a first example, investigation of uncertainties included three major parameters: the conductivity of the chassis σ, the distance between the two coils D_1 and the distance between the secondary coil (receiver) and the chassis D_2 (Figure 11).

Figure 11. *Studied Configuration and Relevant Parameters*



The range of variation, mean, and standard deviation of the parameters are shown in Table 2. Two bounds took into account different kinds of steel material for the conductivity. The bounds for the two distances D_1 and D_2 exceed standards values of existing systems in order to evaluate the worst cases. The 3D finite element mesh includes between 10^5 and 3.10^5 elements depending on the geometrical configuration of the system. The method used first order nodal elements.

Table 2. *Parameters of the Electromagnetic Problem*

Parame-ter	Min	Max	Mean	Standard Variation
σ (S/m)	10^6	5.10^6	3.10^6	10^6
D_1 (m)	0.2	0.6	0.4	0.05
D_2 (m)	0.1	0.5	0.3	0.01

A total number of 30 computations performed by FEM based on a Gaussian distribution of samples over the whole range of variations in order to check the efficiency of the two meta-models. In the first case, only three FEM computations (learning samples) were used to build the meta-models. The other 27 computations have been used as a validation of the meta-model. Figure 12 shows the magnitude of the magnetic field density on the evaluation line obtained by Kriging and Polynomial expansion when the values of the parameters are σ = 1.89 106 S/m; D_1= 0.405 m; D_2= 0.312 m. It clearly appears in this case with only three samples that the agreement between the results from the polynomial expansion was very close to the finite element predictions. The accuracy was significantly better than that provided by Kriging. Figure 13 underlines the differences between the results obtained by finite elements (horizontal axis) and by the meta-models (vertical axis) when considering the 27 finite element computations as validation.

Figure 12. *Variation of Magnetic Flux Density Predicted by Meta-Models in the Case of the Three Learning Samples*

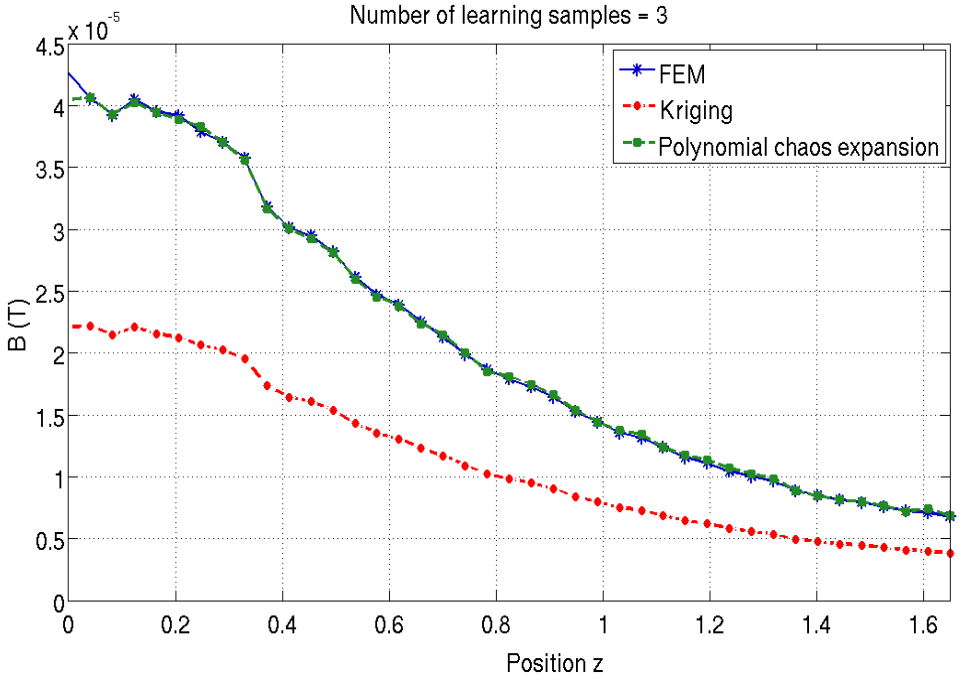
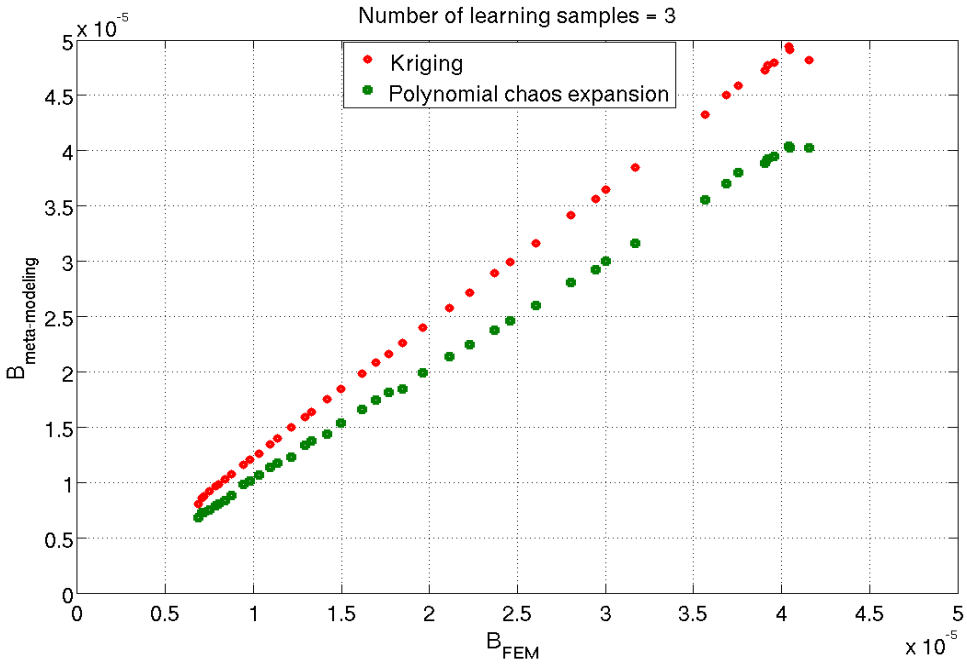
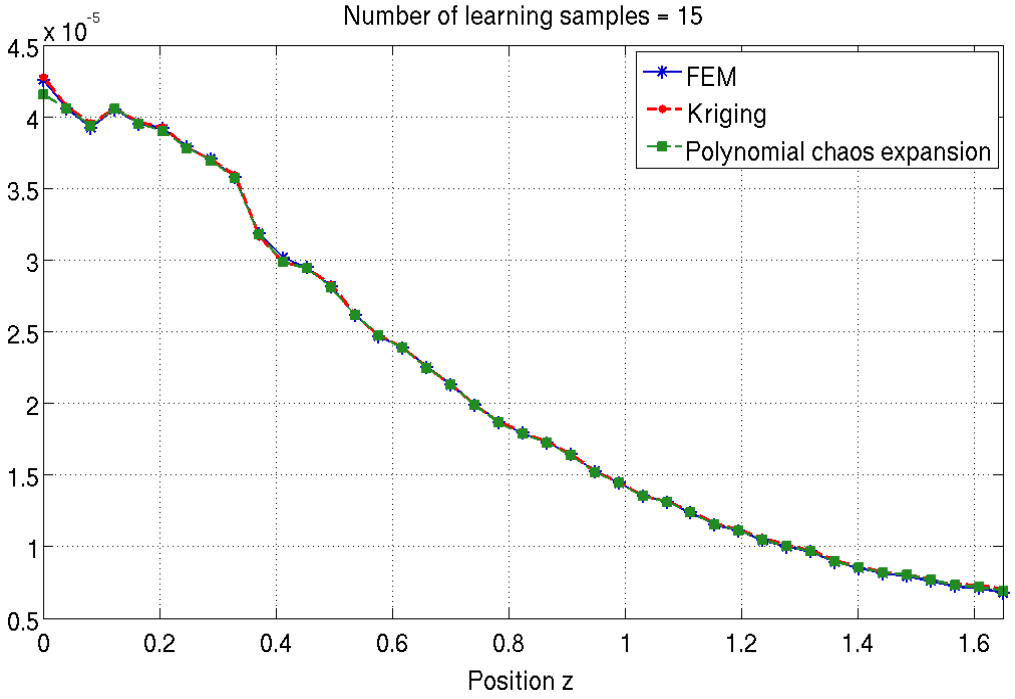


Figure 13. *Differences between Finite Element Results and Meta-Modeling Results in the Case of the Three Learning Samples*



1.

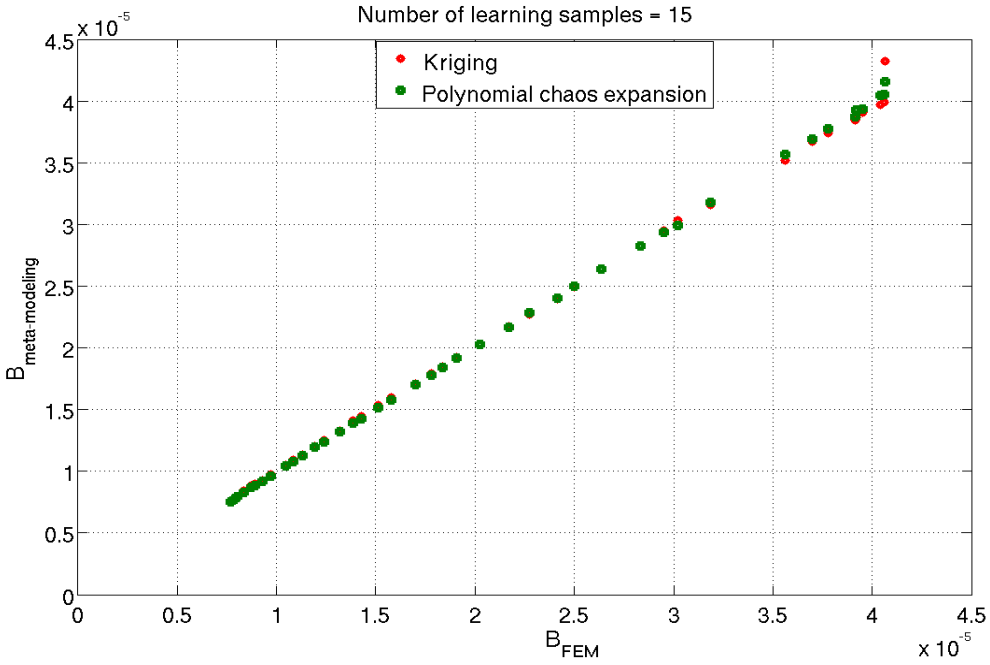
Figure 14. *Variation of Magnetic Flux Density Predicted by Meta-Models in the Case of the 15 Learning Samples*



In a second case, 15 FEM computations were used as learning samples. The other 15 computations were used for the validation. Figure 14 shows that the agreement between the results from the two meta-models was very good. This can

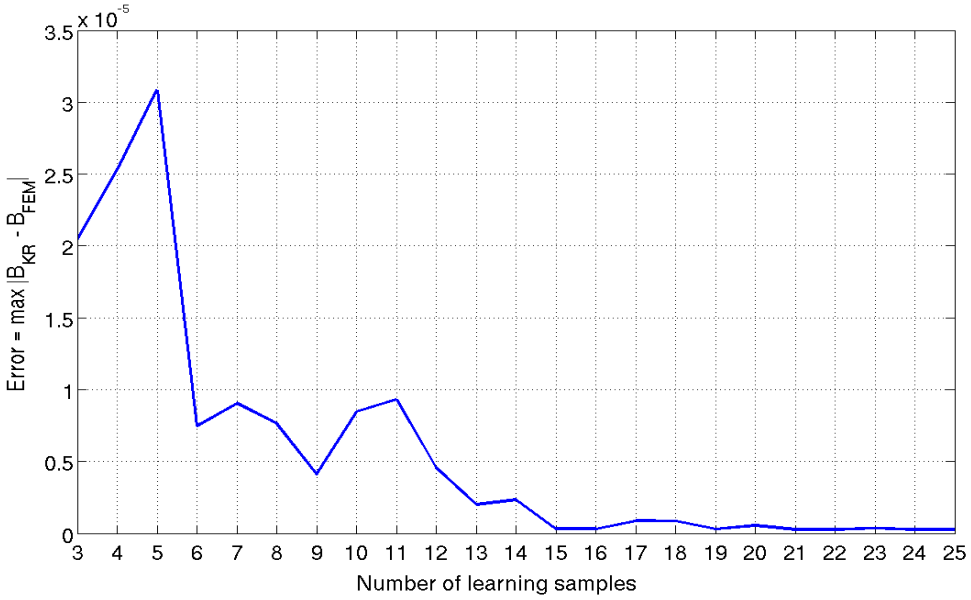
also be noted on Figure 15 where were plotted the differences between the results obtained by finite elements (horizontal axis) and by the meta-models (vertical axis) when considering the 15 finite element computations as a validation. The accuracy of each meta-model can be observed on Figures 16 and 17 showed the maximum error obtained along the evaluation line versus the number of learning samples. High errors for high values of flux density were obtained but it was worth noting that this error was decreased significantly with Kriging if the number of learning samples was greater than 10.

Figure 15. *Differences between Finite Element Results and Meta-Modeling Results in the Case of the 15 Learning Samples*



Regarding the computational time needed by the meta-models, Kriging required two or three times faster than Polynomial chaos expansion depending on the number of learning samples. Whatever the meta-model and the number of learning samples this computational time remains negligible compared to the FEM calculation for all the samples.

Figure 16. *Variation of Error versus the Number of Learning Samples (Kriging)*



Second Configuration

In this second configuration, the two parameters σ and D_1 were the same as those shown in Figure 11; however, D_2 was the distance between the two axes of the coils. This configuration may appear in case of large misalignment or if the receiver is located in the rear of the vehicle. The range of variation, mean and standard deviation for the parameters are shown in Table 3. Figure 18 illustrates the mean value obtained by Kriging along the evaluation line.

Figure 17. *Studied Configuration and Relevant Parameters*

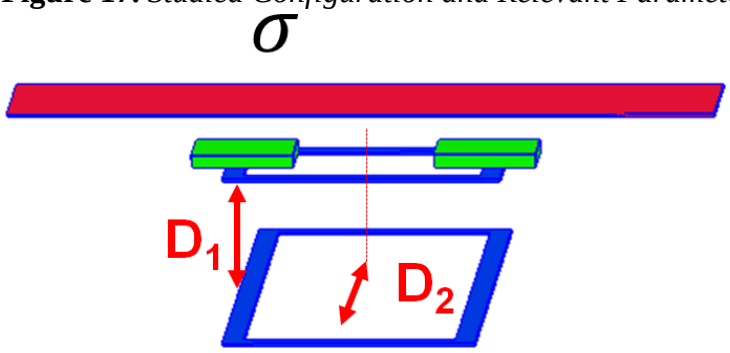
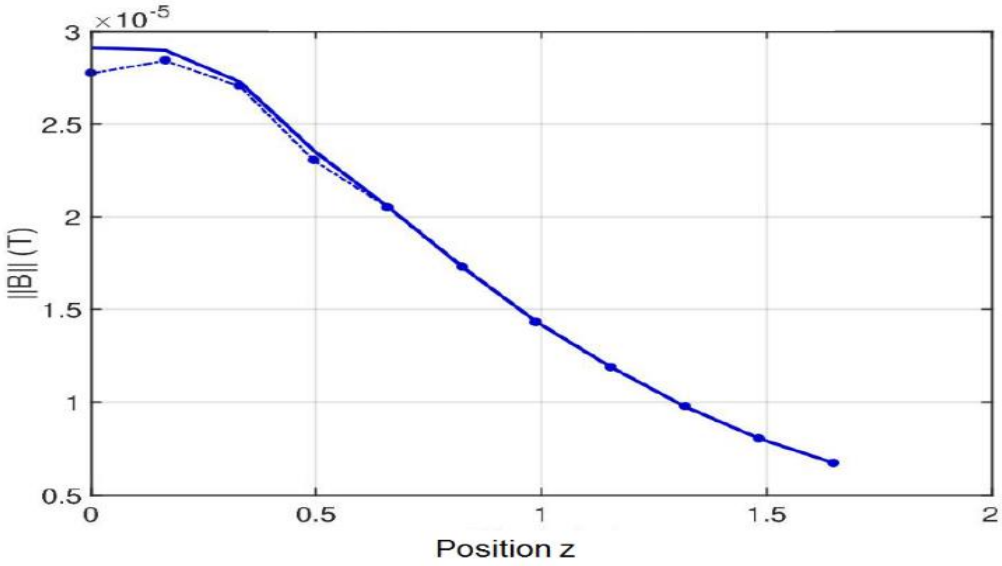


Table 3. *Parameters of the Electromagnetic Problem*

Parameter	Min	Max	Mean	Standard Variation
σ (S/m)	10^6	5.10^6	3.10^6	10^6
D_1 (m)	0.2	0.6	0.4	0.05
D_2 (m)	-1.5	1.5	0.	0.1

Figure 18. *Mean Value of the Magnetic Flux Density obtained by Kriging (Dots) and by Finite Elements (Continuous Line)*



Conclusions

In the first part of this paper we presented a general overview of wireless power transfer systems (WPT) for charging batteries in electric vehicles (EV), focusing on human exposure surveys. After describing the schematics and strategies of the two WPT problems, static (stationary parking) and dynamics (road travel), we examined the problem of exposure to radiation fields attributable to WPT systems in humans living tissues. We reviewed how to predict these radiated fields and examined their compliance with international standards.

In the second part of the paper, predictions of radiated magnetic field have been obtained from two non-intrusive stochastic models in case of a simplified but there is also realistic wireless power transfer system for electric vehicle. Kriging and Polynomial chaos expansions provided efficient meta-models to take into account uncertainties of different physical or geometrical parameters. From the work, it comes out that Kriging allowed a faster prediction than a polynomial chaos expansion. If the number of learning samples was sufficient, Kriging can be used as an efficient predictor to check if reference levels fit the guidelines for human exposure. The work has to be extended the investigation of configurations that are more complex with a detailed anatomical human body model located in the vehicle or beside.

References

Tesla N (1904) The Transmission of Electrical Energy without Wires. *Electrical World and Engineer* 1: 21-24.

Ibrahim M, Bernard L, Pichon L, Razek A, Houivet J, Cayol O (2015) Advanced Modeling of a 2-Kw Series–series Resonating Inductive Charger for real Electric Vehicle. *IEEE Transactions on Vehicular Technology* 64 (2): 421-430.

ICNIRP: International Commission on Non-Ionizing Radiation Protection (2010) Guidelines for Limiting Exposure to time-Varying Electric, Magnetic, and Electromagnetic Fields (1 Hz to 100 kHz). *Health Physics* 99(6): 818-836.

Cirimele V, Diana M, Freschi F, Mitolo M (2018) Inductive Power Transfer for Automotive Applications: State-of-the-Art and Future Trends. *IEEE Transactions on Industry Applications* 54(5): 4069.

Ding PP, Bernard L, Pichon L, Razek A (2014) Evaluation of Electromagnetic Fields in Human Body Exposed to Wireless Inductive Charging System. *IEEE Transactions on Magnetics* 50(2): 1037-1040.

Ibrahim M (2014) *Wireless Inductive Charging for Electrical Vehicles: Electromagnetic Modelling and Interoperability Analysis*. PhD Thesis, University of Paris-Sud.

Cirimele V (2017) *Design and Integration of a Dynamic IPT System for Automotive Applications*. PhD Thesis, Politecnico di Torino and Université Paris-Saclay (GeePs).

Okoniewski M, Stuchly MA (1996) A Study of the Handset Antenna and Human Body Interaction. *IEEE Transactions on Microwave Theory and Techniques* 44(10): 1855-1864.

Shiba K, Higaki N (2009) Analysis of SAR and Current Density in Human Tissue Surrounding an Energy Transmitting Coil for a Wireless Capsule Endoscope. *20th International Zurich Symposium on Electromagnetic Compatibility*.

Christ A, Douglas MG, Roman JM, Cooper EB, Sample AP, Waters BH, Smith JR,

Kuster N (2013) Evaluation of Wireless Resonant Power Transfer Systems with Human Electromagnetic Exposure Limits. *IEEE Transactions on Electromagnetic Compatibility* 55 (2): 265-274.

IEEE Standards (2005) *IEEE Standard for Safety Levels with respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz*. Retrieved from https://bit.ly/2LmeA2q.

Park S (2018) Evaluation of Electromagnetic Exposure during 85 kHz Wireless Power Transfer for Electric Vehicles. *IEEE Transactions on Magnetics* 53(1): 1-8.

Cirimele V, Freschi F, Giaccone L, Pichon L, Repetto M (2017) Human Exposure Assessment in Dynamic Inductive Power Transfer for Automotive Applications. *IEEE Transactions on Magnetics* 53(6): 1-4.

Cimala C, Clemens M, Streckert J, Schmuelling B (2017) Simulation of Inductive Power Transfer Systems Exposing a Human Body with a Coupled Scaled-Frequency Approach. *IEEE Transactions on Magnetics* 53(6): 1-1.

Campi T, Cruciani S, Maradei F, Feliziani M (2017) Near Field Reduction in a Wireless Power Transfer System using LCC compensation. *IEEE Transactions on Electromagnetic Compatibility* 59(2): 686-694.

Cirimele V, Ruffo R, Guglielmi P, Khalilian M (2016) A Coupled Mechanical-Electrical Simulator for the Operational Requirements Estimation in a Dynamic IPT System for Electric Vehicles. *2016 IEEE Wireless Power Transfer Conference (WPTC)*: 1-4.

Lebensztajn L, Marretto CAR, Caldora Costa M, Coulomb JL (2004) Kriging: A Useful Tool for Electromagnetic Device Optimization. *IEEE Transactions on Magnetics* 40(2): 1196-1199.

Gaignaire R, Scorretti R, Sabariego RV, Geuzaine C (2012) Stochastic Uncertainty Quantification of Eddy Currents in the Human Body by Polynomial Chaos Decomposition. *IEEE Transactions on Magnetics* 48(2): 451-454.

Voyer D, Musy F, Nicolas L, Perrussel R (2008) Probabilistic Methods Applied to 2D Electromagnetic Numerical Dosimetry. *COMPEL* 27(3): 651-667.

Kersaudy P, Mostarshedi S, Sudret B, Picon O, Wiart J (2014) Stochastic Analysis of Scattered Field by Building Facades Using Polynomial Chaos. *IEEE Transactions on Antennas and Propagation* 62(12): 6382-6392.

Ibrahim M, Bernard L, Pichon L, Laboure E, Razek A, Cayol O, Ladas D, Irving J (2016) Inductive Charger for Electric Vehicle: Advanced Modeling and Interoperability Analysis. *IEEE Transactions on Power Electronics* 31(12): 8096-8114.

Harris LR, Zhadobov M, Chahat N, Sauleau R (2011) Electromagnetic Dosimetry for Adult and Child Models within a Car: Multi-Exposure Scenarios. International Journal of Microwave and Wireless Technologies 3(6): 707-715.

Gjonaj E, Bartsch M, Clemens M, Schupp S, Weiland T (2002) High-Resolution Human Anatomy Models for Advanced Electromagnetic Field Computations. *IEEE Transactions on Magnetics* 38(2): 357-360.

Steiner T, De Gersem H, Clemens M, Weiland T (2006) Local Grid Refinement for low-Frequency Current Computations in 3-D Human Anatomy Models. *IEEE Transactions on Magnetics* 42(4): 1371-1374.

Hasgall P, Neufeld E, Gosselin MC, Kingenböck A, Kuster N (2012). *IT'IS Database for Thermal and Electromagnetic Parameters of Biological Tissues.* Retrieved from: https://bit.ly/30KwoL9.

Gabriel C, Gabriel S, Corthout E (1996) The Dielectric Properties of Biological Tissues: II. Measurements in the Frequency Range 10 Hz to 20 GHz," *Physics in Medicine & Biology* 41(11): 2251-2269.

Marelli S, Sudret B (2014) UQLab: A Framework for Uncertainty Quantification in Matlab. *2nd International Conference on Vulnerability, Risk Analysis and Management (ICVRAM2014)*.

Zero Emission Mobility Campus, Using a German Example – Theory to Support a Sustainable Decision-Making by Suggestion

By Rebecca Heckmann[††], Alexandra Mittelstädt[‡‡], Lutz Gaspers[§§] & Jörn Schönberger[♦]

Mobility is a basic human need that needs to be satisfied. However, this need for mobility goes hand in hand with transport, which has negative impacts on people, the environment and the climate. Transport causes different emissions with specific consequences. But not every means of transport causes the same number of emissions. In this way, harmful emissions can be reduced by specifically influencing behaviour. This is done by making suggestions when choosing the means of transport. Suggestion promotes the sustainability aspect in decision-making for or against a means of transport. By strengthening the sustainability aspect, the decision in favour of a sustainable mode of transport should be strengthened. A decision is then no longer based on the priority factors of time, costs, convenience and flexibility, but also on environmental compatibility. In this case, a decision is more likely to be made in favour of a more environmentally friendly mode of transport, as awareness of the consequences of one's own transport behaviour is created. This will reduce transport emissions and help to protect the climate, the environment and people. For precisely this suggestion, a model is going to be developed that shows potential approaches and identifies indicators that describe the potential influence on behaviour. Based on the developed model, a suitable suggestion instrument can be developed which is subject to theoretical principles of consumer behaviour, psychological decision making and the transport choice process.

Keywords: *Behavioural Influence in Mobility, Choice of Mode of Transport, Decision Behaviour in Traffic, Mobility Behaviour of Students, Sustainable Mobility.*

Introduction

Mobility and Choice of Mode of Transport

Mobility is a basic need of mankind. It makes it possible to perceive changes in location between different activities, such as working and living. This is based on developments in urban structures. The separation of functions associated with the Athens Charter, i.e. the local separation of activities, implied necessary changes of location between these.

[††]Researcher, University of Applied Sciences Stuttgart, Germany.
[‡‡]Researcher, University of Applied Sciences Stuttgart, Germany.
[§§]Professor, University of Applied Sciences Stuttgart, Germany.
[♦]Professor, Technical University Dresden, Germany.

These changes of location often take place with motorized individual traffic (Institute for Social Science, 2017). This frequency of motorized individual transport leads to effects of an ecological, urban-structural, social and economic nature.

One of the acute impacts that global mankind is dealing with in the 21st century is climate change, which has to be differentiated into natural and anthropogenic greenhouse gas emissions that favour climate change. Anthropogenic greenhouse gas emissions lead to an increased in total greenhouse gas emissions. "The surge in human greenhouse gas emissions and the observed temperature increase over the last 150 years has led to the conclusion that there is a direct causal link between greenhouse gas concentration and temperature development." (Hollerbach and Berner 2003).

Rudinger and his colleagues believe that this is mainly due to people's mobility behaviour, which in its opposite form is not compatible with environmental protection.

"It is increasingly evident that the corresponding (modern) lifestyles in affluent societies, and the mobility behaviours associated with such life styles, are not consistent with protection of environmental quality, efficient use of human, natural, and financial resources, and promotion of social cohesion and just distributions of opportunities and costs of using transport systems." (Rudinger et al. 2006).

The transport sector is responsible for 14% of global greenhouse gas emissions. Overall, CO_2 emissions have risen sharply by over 90% since 1900 (IPCC 2014). Transportation is the only sector that has not achieved any significant CO_2 reductions since 1990 (Federal Environment Agency, 2018). This can be traced back to the rising number of transport services (Institute for Social Science 2017). Although the specific fuel consumption of passenger cars between 1995 and 2016 led to lower fuel consumption due to improved overall efficiency and the use of more diesel vehicles with lower fuel consumption than a petrol car, the trend towards more efficient vehicles and the increasing use of higher consumption equipment contradicted these improvements (Federal Motor Transport Authority 2017).

Since transport performance is linked directly to economic performance, the traffic problem situation poses a challenge for society as a whole.

In order to achieve declining traffic emissions, it is necessary to separate transport performance from economic performance. Rising traffic volumes as a result of rising economic performance must be handled with lower emissions in order to limit increasing emission burdens and consequences such as climate change (Rhenish-Westphalian Institute for Economic Research 2010).

Environmental developments describe the need to reduce emissions in relation to passenger kilometres if transport performance in passenger kilometres is constant or increases.

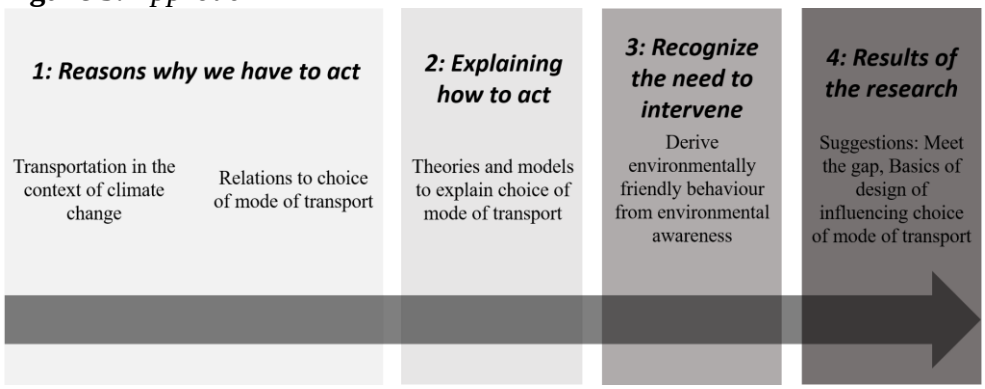
This reduction in emissions is possible by influencing the choice or use of means of transport. Emissions per passenger-kilometre are reduced by switching to a lower-emission means of transport, a Federal Environment Agency means of

transport or by increasing the occupancy rate of a passenger car in order to distribute emissions per kilometre among more people in the vehicle.

A compulsion to change choice or use is not easily possible and not desirable in our social system. Article 1 of the Basic Law describes human dignity, which in the opinion of the Federal Constitutional Court is based on freedom of decision (Federal Republic of Germany, 1949). In order to guarantee this freedom of decision also when deciding on a means of transport and its use, the question of voluntary possibilities to change behaviour arises.

The focus of this work is therefore the theory for the development of a suggestion instrument in the choice of means of transport on a voluntary basis. In order to approach this goal, a four-stage methodological approach was chosen, which is illustrated in Figure 3.

Figure 3. *Approach*



For the sake of clarity, the choice of means of transport in this paper also refers to carpooling or car sharing as an alternative means of transport, i.e. increasing the number of passengers while at the same time reducing the number of individual drivers.

The choice of mode of transport (making a decision) is a complex psychological process, which for example was presented by Pez in 1998 in his model of the choice of means of transport (Pez 1998). Accordingly, different internal and external characteristics influence the choice of means of transport. In the decision-making process, the properties of available means of transport are evaluated. Various factors influence this.

It is generally assumed that younger people are easier to influence than older ones. This for example is based on Busch-Geertsema (Busch-Geertsema 2018). According to her, there is a fixation on traffic behaviour and the development of a transportation routine in the phase between study and professional life. Both students and trainees are regarded as suitable target groups. Since the mobility behaviour among them has often not yet been determined, it is considered possible to influence them. For people in working life, the living conditions and patterns are generally fixed for the longer term and corresponding routines are anchored.

Based on this, research focuses on students and trainees in the first step. In later stages and when the first target groups have been successfully influenced, other groups can also be affected.

First of all, it is important to have an overview of models and principles of decision-making and consumer behaviour as well as theory of choice of mode of transport.

Decisions and also the choice of mode of transport are based on same theoretical models. An important step in these models is the comparison of different factors influencing the decision.

In his model, Pez mentions speed, independence/flexibility, luggage transport and comfort as decisive factors. The representative survey of professors, students and employees of the Stuttgart University of Applied Sciences in 2018 shows that reliability, travel time, costs and flexibility are decisive factors in the choice of means of transport (Heckmann et al. 2019).

The results of Fürst and Oberhofer also verify this impression. In a survey of employees and students at German, Swiss and Austrian universities with a total of over 28,000 evaluated questionnaires, the attributes of the choice of means of transport according to their ranking were perceived as important: Reliability, availability, flexibility, value for money, cost, speed, safety, environmental friendliness and comfort (Fürst and Oberhofer 2012).

In Pez' model as well as in the survey of the Stuttgart University of Applied Sciences and the results of Fürst and Oberhofer it is noticeable that the aspect of environmental compatibility is subordinate.

To influence the choice of means of transport in terms of environmental compatibility is only possible through appropriate measures. Groß describes that the establishment of a change in mobility behaviour is a complex learning process that can only be achieved by forming opinions and changing attitudes and awareness (Groß 1998).

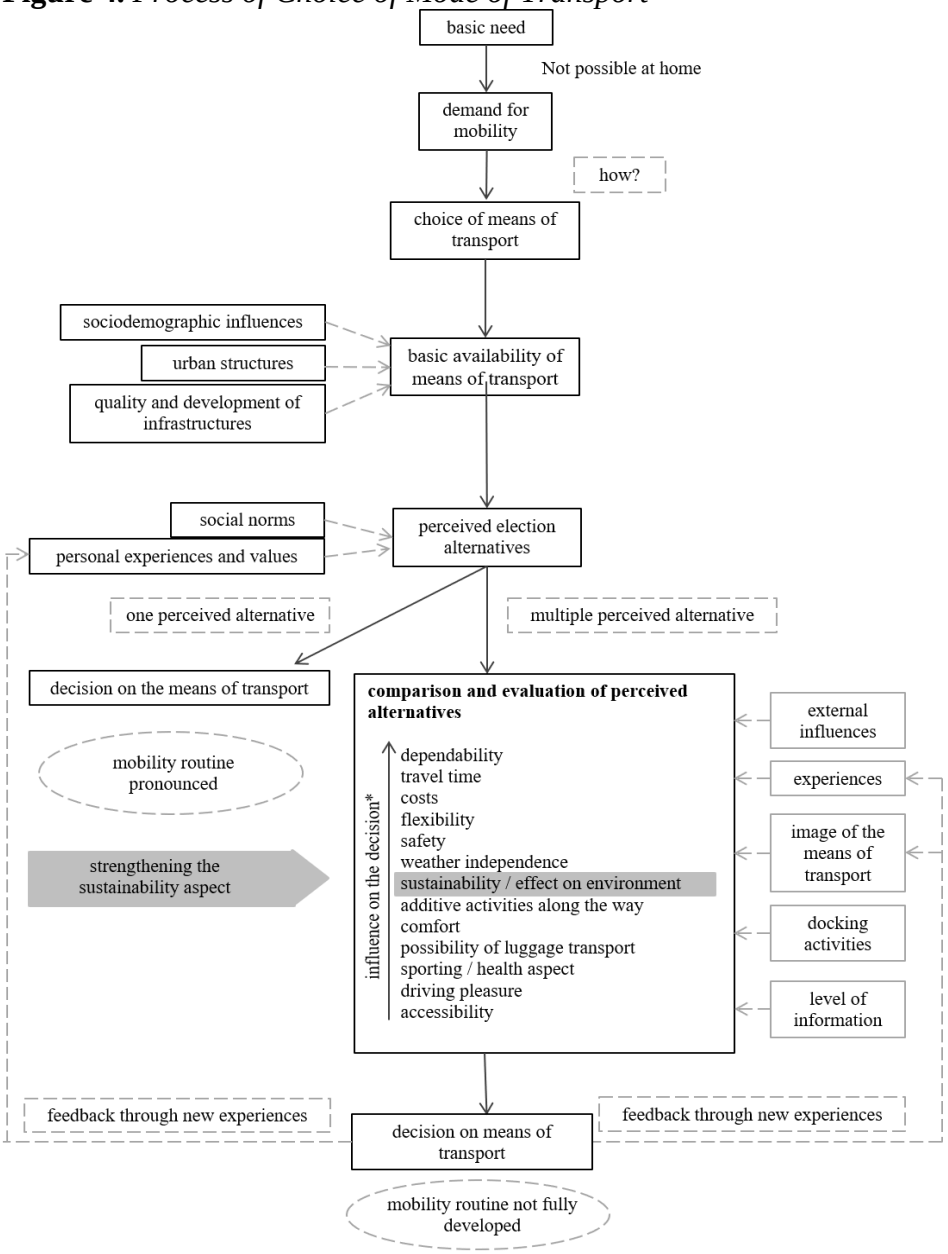
The aim of this work is to develop a medium that leads the user to an environmentally friendly alternative when choosing the means of transport. The focus is on the question of how the environmental aspect can be strengthened as a decision criterion so that users decide on the basis of environmental compatibility and thus choose an environmentally friendly option. At least subjectively and according to the decisive factors of reliability, travel time, costs and flexibility, the environmentally friendly means of transport are perceived as more disadvantageous than a car.

As the study at the Stuttgart University of Applied Sciences has shown, almost 100% of students uses sustainable means of transport (public transport, cycling or walking) (Heckmann et al. 2019). Due to lower fares of public transport for students, it is assumed that the decision for public transport is made by students due to their price sensitivity. Fuji and Gärling also support this view in 2003 and show that: "many have changed means of transport to university or work over the transition [between student and professional life]" (Fuji and Gärling 2003). From this it could be deduced that students use environmentally friendly means of transport during their studies, as these often have cost advantages, but this changes when price sensitivity decreases and cost advantages are possibly eliminated (for example, cheap public transport tickets for students).

In this context, the question arises as how environmental awareness can influence behaviour in order to avoid this upheaval between study and career. This

can be considered sufficient for educational traffic in general. Studies show that pupils and similar groups are particularly frequent users of public transport. This leads to the point that in some places public transport can only be economical at all thanks to pupils. This is the case, for example, in rural areas (Deutsch 2013). Passengers who are undergoing training (apprenticeship or studies) are regarded as a group with homogeneous behaviour. For this group of people, who are in the phase before the transition between training and working life, there is presumably the potential to influence mobility behaviour and establish a mobility routine.

Figure 4. *Process of Choice of Mode of Transport*



* Classification based on the HFTmobil study at the Stuttgart University of Applied Sciences on the question of how decisive the individual factors are for students.

Source: Pez 1998.

Figure 2 shows the process of choosing a means of transport and the starting point for suggesting the environmental aspect. Suggestivity, and thus the potential for reducing traffic emissions, results exclusively from the perception of several alternative choices and the comparison process that results. This comparison process takes place subconsciously on the one hand, and partly consciously and actively on the other, for example by using route planners who compare different driving options with regard to some of the selection factors (mainly driving time, costs, flexibility, comfort).

Fugure 2 shows the suggestion in the phase of comparison and evaluation of the perceived choice alternatives (grey). The aim of the suggestion is to persuade the user to pay more attention to the environmental aspect in the assessment. This should lead to a decision in favour of more sustainable means of transport.

Basics of Choice of Sustainable Mode of Transport

Traffic-relevant decisions have different maturities. Only immediate, short-term decisions can be directly influenced by a suggestion instrument. Nevertheless, the feedback of a decision on experience and routine should also be able to influence medium- and long-term decisions as shown in Table 1. Held differentiates between the following terms and types of choice (Held 1982):

Table 1. *Classification of Transport-Relevant Decisions by Maturity*

Terms of choice	**Type of choice**
Long-term	Choice of workplace Choice of apartment
Medium-term	Car ownership Choice of means of transport for commuting to work
Short-term	driving frequency destination selection Choice of means of transport (other) Choice of time of day route selection

A suggestion tool can influence short-term decisions, as it is assumed that for such decisions a comparison of different options will take place immediately before the action itself. This means that those short-term choices could be influenced. Relevant with regard to emissions are above all the choice of other means of transport, the frequency of travel and the choice of route:

- Other means of transport: Leisure trips and those that do not take place regularly
- Frequency of travel: it is assumed that this can hardly be influenced, since it will probably be established how often the road user drives to a certain activity (example: a road user intends to make a short-term decision on how to get to an event). It is clear that he will drive back and forth to this activity.)
- Route choice: this can have an impact on emissions if different routes have different route lengths or different altitude profiles which affect consumption and therefore emissions.

The aim of the work is to develop a model that shows how decisions that Held believes can be influenced by a suitable instrument.

Methodology

Based on theoretical models of transport choice and consumption theory in relation to sustainable consumption, a theory for influencing sustainable mobility behaviour will be developed.

For this purpose, general models of the transport mode choice like the one of Pez, the Theory of Planned Behaviour of Ajzen, the rational-choice-theory, the norm activation model and a consumption theory will be analysed. In addition, the deficit of environmental awareness and environmentally conscious action will be discussed. The aim is to explain why road users rarely opt for more sustainable means of transport despite a basic awareness of sustainability and the environment.

An approach to possible behavioural suggestion is worked out. Targeted suggestion is intended to encourage road users to transfer environmental awareness into environmentally conscious action.

By opting for sustainable means of transport, the traffic emissions of the road user can be reduced.

Findings/Results

First of all, there are different models that try to explain the decision for a particular means of transport.

At this point, a brief look will be taken at the following models and theories:

- In a nutshell: Aggregated, Behavioural and Attitudinal Models
- Choosing a means of transport as a purchase decision
- Choice of means of transport according to Pez and in comparison to choices under high and low involvement
- Transportation choice in the Theory of Planned Behaviour
- Choice of means of transport within the framework of the norm activation model

- Transportation choice in the Rational-Choice-Theory

In a Nutshell: Aggregated, Behavioural and Attitudinal Models

Historically, 3 classical models for forecasting the choice of means of transport have been developed and evolved.

First, the choice of transport mode was determined using aggregated transport demand models. The choice of means of transport was derived depending on sociodemographic and settlement structural influencing factors. Individual behaviour is not taken into account.

The second generation of transport mode choice models was the disaggregated behavioural models. They also take into account objectively measurable properties of the means of transport and examine the electoral process on an individual level. It is assumed that a road user chooses the alternative with the greatest benefit. The properties travel costs and travel time were used for the decision.

Based on this, attitudinal models go one step further and also include subjective criteria. These include comfort, safety and convenience. It is assumed that there is a clear connection between a user's attitude to a means of transport and later behaviour.

Important Findings for the Suggestion Instrument

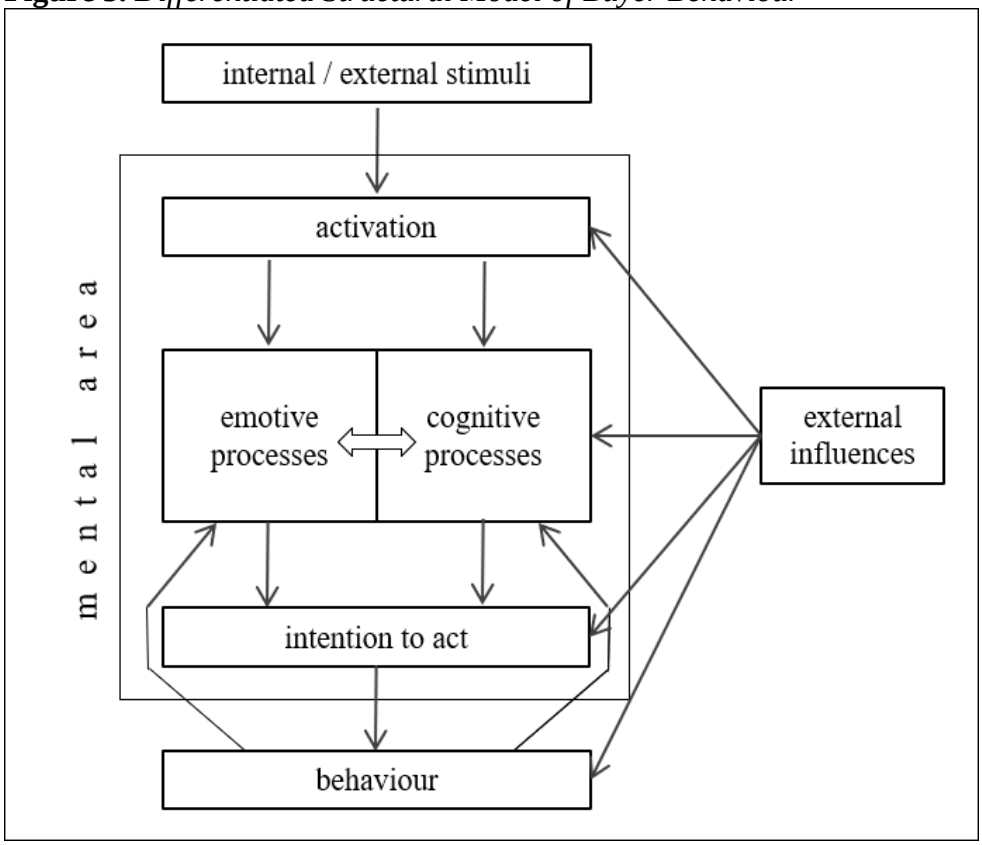
Based on these basic models, different models and theories are now used. What is decisive and remarkable, however, is that the attitudinal models already assume that attitudes to a means of transport influence the decision and behaviour (Research Information Centre 2018).

Choosing a Means of Transport as a Purchase Decision

For example, the choice of means of transport can be regarded as a classic purchase decision.

Based on models for the purchase decision, especially the structural models, as presented by Zemlin, it can be said that the decision for a means of transport, if it is a purchase decision, is influenced by psychological processes. Zemlin distinguishes between cognitive (rational) and emotive processes. In addition, external influences influence these mental processes, as shown in Figure 3 (Zemlin 2005).

Figure 5. *Differentiated Structural Model of Buyer Behaviour*



Source: Zemlin 2005.

This model makes it clear that the psychological process and the external environment are decisive; a first important insight for the development of a suggestion instrument.

Important Findings for the Suggestion Instrument

A transport choice decision can be interpreted as a purchase decision. Thus there are parallels. In purchasing behaviour, emotive and cognitive processes play a decisive role, as does the environment with external stimuli and external influences.

Choice of Means of Transport according to Pez

If we take a closer look at the model of Pez, which has already been presented, we can describe a number of conspicuous features. Sometimes there are parallels to the purchase decision theory mentioned above.

First of all, Pez represents a branching in the decision tree, which in other places in the literature are described comparatively with high and low involvement as well as habitual decisions. First of all, it is crucial whether the road user will make a decision at all. Zemlin describes this by saying that the decrease in involvement also leads to a reduction in the scope of mental processes when

involvement describes the mental commitment to decision making. The less this is noticeable, the less complex the decision-making process becomes, up to and including habitual behaviour, in which de facto no decision-making process takes place anymore.

In the decision-making process, these two extremes (high involvement - extensive decision-making process) and habitualised behaviour (no decision-making process) are represented by a fork in the decision tree. Pez says that a detailed decision can only be made if more than one alternative is perceived. In this case psychological processes follow to compare and evaluate the perceived alternatives. These are influenced by the environment. It is only at the end of these processes that the choice of means of transport is made. If only one alternative is perceived, the decision tree is shortened and psychological processes do not take place.

Important Findings for the Suggestion Instrument

On the one hand, it is important to recognize that a psychological process only takes place if the road user perceives alternative means of transport at all. This limits the potential situations to be influenced. On the other hand, Pez's model clearly shows that a psychological process is a central point in the choice of means of transport and how it takes place. Thus, Pez shows the process stages in which suggestion is possible, namely during the comparison and evaluation process.

Transportation Choice in the Theory of Planned Behaviour

Both the Theory of Planned Behaviour (Ajzen 1991) described here and the Norm-Activations-Model (Onwezen et al. 2013) have proven their worth empirically for the explanation of environmentally friendly behaviour, as well as in the field of choice of means of transport. "What both action models have in common is that they focus on individual internal evaluation processes when explaining environmentally relevant behaviour and not, like behavioural economic and activity-based models, exclusively on individual external requirements and constraints of mobility-related activities." (Hunecke 2015).

The Theory of Planned Behaviour assumes that psychological constructs, subjective norms, attitudes towards cars, public transport and bicycles, and perceived behavioural control influence behavioural intentions. Depending on how strongly the intention is pronounced and the extent of the perceived behavioural controls, the intention is transformed into behaviour. An intention is formed when the behaviour is evaluated positively (attitudes), other persons expect the behaviour (subjective norm) and the behaviour is easy to carry out (perceived behaviour control).

The focus of the Theory of Planned Behaviour is therefore on subjective advantages as motivation for behavioural execution.

Choice of Means of Transport within the Framework of the Norm Activation Model

The norm activation model has a different focus than the Theory of Planned Behaviour. It regards the assumption of personal responsibility for fellow human beings and for the environment as an essential motivation for one's own compliance.

At the centre of the norm activity model is the personal norm, also known as the responsibility norm. If this personal norm is activated, this leads to a feeling of moral obligation, which in turn entails corresponding ecologically responsible behaviour.

In order to achieve this ecologically responsibility, it is essential that road users see themselves as co-responsible for environmental impacts and recognize the link between their actions and the environmental consequences.

Important Findings for the Suggestion Instrument

A decisive finding of the Theory of Planned Behaviour and the norm activation model are two assumed motivations for behavioural executions: on the one hand personal subjective advantages (Theory of Planned Behaviour) and on the other hand, the assumption of responsibility for the environment and fellow human beings. For the suggestion instrument to be developed, both possible motivational bases should be taken up and, if possible, included.

Equally important is the fact that social responsibility only leads to environmentally conscious conduct if one has understood the connection between one's own actions and the ecological consequences.

Transportation Choice in the Rational-Choice-Theory

Economic explanatory models, based on disaggregated behaviour-oriented models, work with the rational choice approach. This is based on the assumption that an individual always chooses the alternative action that promises the greatest personal benefit. Accordingly, objective factors such as time and money dominate the choice of means of transport.

In situations where behavioural costs are low, the theory of benefit maximization cannot be applied, as attitudes and moral convictions gain in importance.

Important Findings for the Suggestion Instrument

According to the rational choice approach, the suggestion instrument should take into account that the user may choose the alternative with the greatest personal benefit. The suggestion instrument must therefore increase the benefit of the environmentally friendly option in terms of hard factors such as time and money compared to the other alternatives.

Conclusions from the Above Models and Theories and the Gap between Environmental Awareness and Environmental Action

The fact that the environmental aspect plays only a minor role in the choice of means of transport is one of the key findings of this work. This fact raises the question of how environmentally sound transport choices can be made.

Similarly, a result of the analyses of theories and models is the determination already made above of the factors and decisive properties that are important for the suggestion instrument. All the important findings should be taken into account in the development of the suggestion instrument.

In order to approach the topic of environmentally conscious behaviour and consumption, it will first be explained why environmental awareness does not lead directly to environmentally friendly behaviour, how the ecological aspect can have an effect as a value, especially against the background of changing values, which approaches are known to promote environmentally friendly presence and which role the aspect of environmental compatibility plays in the choice of means of transport.

On the Discrepancy between Consciousness and Action

It is not always easy for consumers to correctly assess the sustainability properties of products (Schoenheit 2009). Since the decision to use a means of transport is also a consumer behaviour, parallels can be drawn.

"The sustainability properties of products, which in principle range from manufacture to use to disposal, are "not written on the forehead" of the products. As a rule, these are so-called trust properties, which are not really judged by consumers either before or after the purchase, but can essentially only be "believed". Separate and particularly "credible" information offerings are therefore required in order to make the sustainable qualities of products and services visible and recognizable." (Schoenheit 2009).

This raises a crucial question: How can road users be provided with credible information about the sustainability quality of their intended means of transport?

The decision as to which means of transport should be chosen for a necessary change of location is a classic consumer decision. The consumer chooses between different products (the means of transport) the one that seems most optimal for a particular situation. This decision can be explained in more detail using the decision theory. According to this theory, a trader (in this case the road user) would subjectively rationally decide on the best possible course of action by weighing the consequences of action (from the point of view of the trader) (Dierkes et al. 1988). However, it is sometimes not easy to understand based on which influences and within the framework of which psychological processes a road user decides on this or that means of transport. This purchasing decision process (the choice of means of transport) is a complex process. Models can help to describe and explain. Different models try to approach the decision-making process. The next chapter presents all current known models and theories. The same applies to the various influences on the choice of means of transport. First,

however, the connection between environmental awareness and environmentally friendly action will be established in a more specific way and it will be explained how environmental awareness as a value has increased in importance and what this means for a sustainable choice of means of transport.

It remains questionable whether environmental awareness is already important in the area of mobility consumption. This statement should be questioned: "More and more consumers are interested in [...] the CO_2 emissions of their cars". (Heidbrink and Schmidt 2009).

This statement clearly contradicts the data of the previous chapters. The specific emissions of passenger cars have hardly decreased in the past 25 years. There is therefore a discrepancy between the statement that consumers are more interested in the CO_2 emissions of their car and reality. Heidbrink and Schmidt offer an approximation to explain this discrepancy: "A closer look shows, however, that the willingness to consume responsibly is not consistently implemented. Despite buying climate-friendly or fair-trade products, the majority continue to use the car for journeys to work and the plane for long-distance journeys. [...] So there is still a gap between awareness and action." (Heidbrink and Schmidt 2009).

However, this discrepancy does not only seem to exist in the area of mobility, but is also generally valid. Kuckartz and Rheingans-Heintze are of the opinion that the discrepancy between environmental awareness and environmental action depends on the field of action. Thus, you conclude that in the food sector there is still the greatest correlation, whereas in the energy and transport sectors it is much smaller (Kuckartz and Rheingans-Heintze 2006). Prose also describes the fact that although environmental awareness seems to be pronounced in large parts of the population, there does not seem to be a direct connection between people's awareness and behaviour. "The relatively high level of environmental awareness is therefore only inadequately expressed in corresponding energy-relevant (purchasing) decisions and behaviour patterns of the actors". (Prose 1994).

Blake has discovered three barriers that can prevent environmental awareness from leading to environmentally friendly behaviour.

These are individual barriers such as laziness or lack of interest, barriers of responsibility such as lack of efficiency, no need, lack of trust or ownership and barriers of practicality such as lack of time, lack of money, lack of information and the like.

This also partly confirms what has already been mentioned above. Missing information can prevent environmentally friendly behaviour from developing.

However, there are other barriers. These should be tried to overcome when considering how to get people to choose sustainable means of mobility (Blake 1999).

Importance in the Context of Transport Mode Choice Suggestion

The previous findings are important for the development of a suggestion instrument. Sometimes it is possible that the environmental aspect is important for a road user, but it cannot be decisive for the behaviour or the choice of means of

transport, as there is a discrepancy between awareness and behaviour. So the challenge is as follows: how can the suggestion instrument resolve the discrepancy?

Prose believes that one way can be marketing for climate protection and describes it as a strategy of behavioural change. "It is about both reducing environmentally harmful conduction (de-marketing) and strengthening relatively more environmentally friendly behaviour alternatives (marketing). Marketing as a strategy for changing habits requires knowledge of its object, i.e. behaviour and its determinants". (Prose 1994).

Furthermore, the suggestion instrument is more or less a marketing tool, which, following Prose, promotes environmentally harmful means of transport in a negative way (de-marketing) and promotes more environmentally friendly means of transport in a positive way (marketing).

The widespread use of smartphones supports and promotes mobile marketing. Apps are promising marketing instruments. "Apps can be used to address customers on a very intimate, emotional level, as users build a very special personal relationship with their device by constantly keeping their smartphones with them (Tosic 2015).

Therefore, a suggestion instrument in the form of a digital app that is used for marketing and de-marketing of means of transport is considered promising. Marketing should support environment-friendly modes of transport and on the other hand, non-friendly modes could be less attractive caused by de-marketing. A change of mobility decisions is expected.

Based on the theory and model analysis, the suggestion instrument should support the following principles:

It starts with the psychological emotive and cognitive processes in the choice of means of transport. It takes into account that suggestion is only possible if several alternative choices are made. In the absence of perception, for example due to fixed routines, a suggestion is not possible that the psychological decision-making process is not triggered in the first place. Suggestion takes place optimally at the moment of evaluation and comparison of the alternatives with regard to hard and soft factors.

The suggestion instrument offers personal advantages so that the individual chooses the environmentally friendly option. The suggestion instrument appeals to the sense of responsibility for the environment and fellow human beings. In addition, the suggestion instrument for environmentally friendly options maximizes personal benefit.

Based on the Previous Findings: What are Important and Useful Elements of the Suggestion Instrument?

The suggestion instrument starts with the psychological process of the decision.

It can work with a bonus system that offers personal benefits and at the same time increases the use of environmentally friendly means of transport.

At this point, the possibility of gamification features is in discussion. These features help to realize personal advantages and maximize benefits, as well as to

build responsibility for the environment and fellow human beings. Gamification makes it easy to give users an understanding of the relationship between their own behaviour and environmental impacts. Gamification features can be a further step of influencing choice of mode of transport, assuming that gamification features can increase the use and the impact of a suggestion instrument. Different modes of gamification are possible.

Teresa Engel has investigated whether gamification can lead to an intended change in behaviour in the choice of means of transport (Engel 2017). Based on her work, it can be concluded that this is possible if the appropriate gamification elements are selected. With the help of these elements, based on the motivation theory, gamification can support the suggestion instrument in the achievement of its objectives. The corresponding features are therefore included in the planning and development of the suggestion instrument.

Conclusions

It is considered possible for a suggestion instrument to bring about a desired and targeted change in behaviour.

For successful suggestion, the instrument an optimally integration for the specific application is needed.

The following parameters are important when designing the suggestion instrument:

- Simple and unobtrusively use of the instrument
- Influence, without the user consciously or disruptively perceiving it
- Influence by means of simple and intuitive picture language
- Transparent and credible information
- Personal benefits occur
- Compensation for potential disadvantages of environmentally friendly means of transport (maximisation of personal benefit)
- Building a personal connection to the instrument and its contents
- Integration with common systems and processes to increase acceptance and utilization
- Concentration on a target group that is susceptible to influence through marketing or de-marketing
- Orientation and design of the suggestion depending on the target group and the environment
- Gamification as the key to motivation
- Building a sense of responsibility for the environment and fellow human beings

This paper covers basic research. This was necessary for the development of the suggestion app. It provides insights into theoretical models and theories that determine the functionality of a suggestion instrument.

This basic research is therefore important in order to develop a corresponding instrument that takes these models and theories and the principles and modes of action derived from them into account.

Building on the knowledge gained and the parameters worked out, the suggestion instrument can be designed in the next step.

The goal of the research, consisting of the existing basic research and the following application research, divided into development and testing of the instrument, is the goal-oriented, voluntary change of behaviour in traffic behaviour, caused by so-called soft policies, implemented as an app.

The proposal for the suggestion instrument is therefore as follows:

An app that uses a comparison of emission data from different means of transport to make information available to users in a pictorial and easily understandable form. With the help of visual language, gamification and credible data, the user builds up a sense of responsibility, gains an understanding of the environmental impact of his own behaviour and receives incentives to adapt his behaviour to the desired objectives.

The development of the app is a central element of the following application research. The basic research in this paper has shown that a suggestion instrument is suitable for changing mobility behaviour.

Figure 6 and 5 show the original way of decision making for one mode of transport and the principle for the created instrument to support a sustainable decision making.

Figure 6. *Original Way of Decision Making for One Mode of Transport*

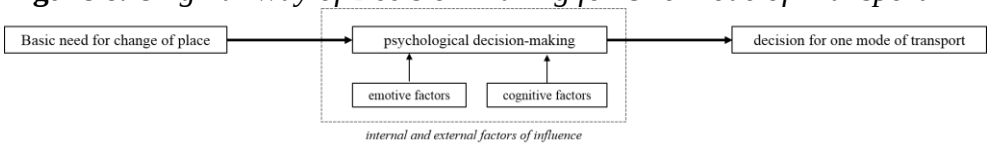
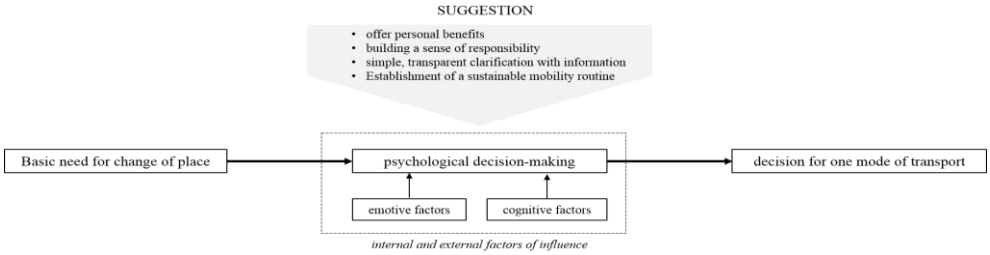


Figure 7. *Created Instruments to Support a Sustainable Decision Making*



With help of the created instrument to support a sustainable decision making, the way of decision making is more complex. The suggestion influences at the stage of psychological decision making. Besides emotive and cognitive factors, the suggestion factors will influence the process. The key influencing factors are the offer of personal benefits, a building of a sense of responsibility, simple and transparent clarification with information and the establishment of a sustainable mobility routine, as it was derived in this paper.

The developed model of suggestion will be realized in an app and evaluated in a field study.

References

Ajzen I (1991) The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes* 50(2): 179-211. DOI=10.1016/0749-5978(91)90020-T.

Blake J (1999) Overcoming the 'Value–Action Gap' in Environmental Policy: Tensions between National Policy and Local Experience. *Local Environment* 4(3). DOI=10.1080/13549839908725599.

Busch-Geertsema A (2018) *Mobilität von Studierenden im Übergang ins Berufsleben.* [Mobility of Students in Transition to Working Life]. Die Änderung mobilitäts-relevanter Einstellungen und der Verkehrsmittelnutzung. DOI=http://dx.doi.org/10.1007/978-3-658-18686-9.

Deutsch V (2013) *Mobil Bleiben in der Fläche: Für einen Integrierten ÖPNV*. [Staying Mobile in Space: For an Integrated Public Transport System]. Köln: Verband Deutscher Verkehrsunternehmen e.V.

Dierkes M, Fietkau HJ (1988) *Umweltbewußtsein, Umweltverhalten.* [Environmental Awareness, Environmental Behaviour]. Kohlhammer, Stuttgart: Metzler-Poeschel.

Engel T (2017) Beeinflussung der Verkehrsmittelwahl durch Gamification [Influencing the Choice of Means of Transport through Gamification]. *ATZ Automobiltechnische Zeitschrift*.

Federal Republic of Germany (1949) *Basic Law for the Federal Republic of Germany*.

Forschungsinformationszentrum – Research Information Centre (2018) *Prognosen zur Verkehrsmittelwahl (Modal Split)* [Forecasts on the Choice of Transport Mode (Modal Split)].

Fuji S, Gärling T (2003) Development of Script-Based Travel Mode Choice after Forced Change. *Transportation Research Part F Traffic Psychology and Behaviour* 6(2):117-124.

Fürst E, Oberhofer P (2012) Trends in der Mobilitätseinstellung von Studierenden und Mitarbeitern Deutschsprachiger Hochschulen. [Trends in the Mobility Attitudes of Students and Staff at German-Speaking Universities and Colleges]. In H Proff, J Schönharting, D Schramm, J Ziegler (eds), *Zukünftige Entwicklungen in der Mobilität*, 455-465.

Groß T (1998) *Mobilitätsverhalten von Jugendlichen. Empirische Untersuchung zur Verkehrsmittelwahl und ihrer Determinanten als Beitrag zur an den ÖPNV in Dortmund.* [Mobility Behaviour of Young People. Empirical Study on the Choice of Means of Transport and its Determinants as a Contribution to Public Transport in Dortmund]. Dortmund: Diplomarbeiten Agentur diplom.de.

Heckmann R, Mentzel B, Gaspers L (2019) *HFTmobil: Untersuchung des Mobilitätsverhaltens von HFT-Angehörigen.* [HFTmobil: Investigation of the Mobility Behaviour of HFT Members]. Stuttgart: Hochschule für Technik Stuttgart.

Heidbrink L, Schmidt I (2009) Die Neue Veranwortung der Konsumenten. [The New Responsibility of Consumers]. *Aus Politik und Zeitgeschehen*, 27-32.

Held M (1982) *Verkehrsmittelwahl der Verbraucher. Beitrag einer Kognitiven Motivationstheorie zur Erklärung der Nutzung Alternativer Verkehrsmittel*. [Choice of Means of Transport by Consumers. Contribution of a Cognitive Motivation Theory to the Explanation of the Use of Alternative Means of Transport]. Duncker & Humblot; Auflage: 1.

Hollerbach A, Berner U (2003) *Klimawandel und CO_2 aus Geowissenschaftlicher Sicht.* [Climate Change and CO_2 from a Geoscientific Point of View]. Presented at the Conference: Tagung Braunkohleverstromung 2003 der VDI-Gesellschaft Energietechnik. Koeln, Germany.

Hunecke M (2015) *Mobilitätsverhalten Verstehen und Verändern.* [Understanding and Changing Mobility Behaviour]. Wiesbaden: VS Verlag für Sozialwissenschaften. DOI=10.1007/978-3-658-08825-5.

Institut für angewandte Sozialwissenschaft GmbH – Institute for Social Science (2017) *Mobilität in Deutschland.* [Mobility in Germany].

IPCC (2014) *Climate Change 2014: Mitigation of Climate Change.* Cambridge and New York.

Kraftfahrt-Bundesamt – Federal Motor Transport Authority (2017) *Downsizing. Nicht in jedem Segment ein Thema*. [Downsizing. Not an Issue in Every Segment].

Kuckartz U, Rheingans-Heintze A (2006) *Trends im Umweltbewusstsein Umweltgerechtigkeit, Lebensqualität und persönliches Engagement.* [Trends in Environmental Awareness. Environmental Justice, Quality of Life and Personal Commitment]. Wiesbaden: VS Verlag für Sozialwissenschaften.

Onwezen M, Antonides G, Bartels J (2013) The Norm Activation Model: An Exploration of the Functions of Anticipated Pride and Guilt in Pro-Environmental Behaviour. *Journal of Economic Psychology* 39(Aug): 141-153.

Pez P (1998) *Verkehrsmittelwahl im Stadtbereich und ihre Beeinflußbarkeit. Eine Verkehrsgeographische Analyse am Beispiel von Kiel und Lüneburg.* [Choice of Transport Mode in Urban Areas and its Influence. A Traffic-Geographical Analysis using Kiel and Lüneburg as Examples]. Kiel: Geographisches Institut der Universität Kiel.

Prose F (1994) Ansätze zur Veränderung vom Umweltbewusstsein und Umweltverhalten aus Sozialpsychologischer Perspektive. [Approaches to Changing Environmental Awareness and Behaviour from a Socio-Psychological Perspective]. *Senatsverwaltung für Stadtentwicklung und Umweltschutz Berlin (Hrsg.). Neue Wege im Energiespar-Marketing, Materialien zur Energiepolitik in Berlin* Heft 16, 14-23.

Rheinisch-Westfälisches Institut für Wirtschaftsforschung (2010) *Verkehrsinfrastrukturinvestitionen - Wachstumsaspekte im Rahmen einer Gestaltenden Finanzpolitik* [Transport Infrastructure Investments - Growth Aspects within the Framework of a Shaping Financial Policy].

Rudinger G, Donaghy K, Poppelreuter S (2006) Societal Trends, Mobility Behaviour and Sustainable Transport in Europe and North America. *European Journal of Ageing* 1(1): 95-101.

Schoenheit I (2009) Nachhaltiger Konsum. [Sustainable Consumption]. *Aus Politik und Zeitgeschehen*, 19-26.

Tosic M (2015) *Apps für KMU. Praktisches Hintergrundwissen für Unternehmer.* [Apps for SMEs. Practical Background Knowledge for Entrepreneurs]. Wiesbaden: Gabler Verlag.

Zemlin B (2005) *Das Entscheidungsverhalten bei der Verkehrsmittelwahl.* [Decision Behaviour in the Choice of Means of Transport]. Wuppertal: Josef Eul Verlag; Auflage: 1.