An Approach to Predictive Risk Analysis of Manipulation of Electric Vehicles

Stefan Matthias Müller,
Alexander Pohl and Markus Lienkamp
Technische Universität München
Institute of Automotive Technology
Garching b. München, Germany
Email: Mueller@ftm.mw.tum.de

Carsten Reinkemeyer

AZT Automotive GmbH
Allianz Zentrum für Technik
Ismaning, Germany

***Abstract*—In the current vehicle market, there are hardly any possible types of manipulation available for electric vehicles. However, it is only a matter of time until the market situation changes. For the new field of electric vehicles, it is therefore necessary to perform risk analysis at an early stage. Due to the currently non-existent market, it is necessary to estimate a possible future market. This paper outlines an analytical approach, which allows the systematic evaluation of risks of manipulation involving core components of electric vehicles, based on currently available information. The approach is basically founded on two main factors, probability of occurrence and potential damage. These categories have been specified up to a complete taxonomy for the whole risk analysis.**

Keywords—Risk Analysis; Manipulation; Electromobility

I. Motivation

There is already a well-organized market for manipulation of conventional vehicles, especially for unauthorized manipulation of odometers. Vehicle manufacturers, insurers and car buyers have to bear damages in the billions every year in Germany alone [1]. At the same time, a trend of moving steadily towards an individualized market is becoming apparent [2]. This leads to an increasing demand for manipulation in order to personalize vehicles, which favors changes setting the vehicle apart from the masses. A very common example is chip tuning to improve performance or to optimize fuel consumption (eco tuning) [3].

Electric cars represent a new class of vehicles entering the market. These vehicles are primarily characterized by new technologies particularly in the area of the drive train as well as the energy storage. Due to the expensive electric energy storage, the situation worsens when it comes to manipulation of electric vehicles. The used battery cells are subject to aging mechanisms [4] what in turn has a negative impact on the already comparatively low electrical storage capacity as well as on the residual value. This offers new lucrative targets for manipulation, such as changing the logged aging state towards a better value, similar to the manipulation of the odometer.

The current storage technology limitations, furthermore, lead to restrictions for users of electric vehicles. For example, due to the often very limited electrical capacity, these vehicles can only cover comparatively short distances and the top speed is often electronically limited by the manufacturer as well. On the other side, the used technologies are continually being improved, for example cells with a higher energy density. Both factors can lead to an increased demand for subsequent modifications.

Currently there is hardly a market for electric vehicle manipulation. This is probably due to the still low number of electric vehicles in the market, the new technologies and the market penetration among private customers which is still low. Nevertheless, it is possible to expect an increasing number of types of manipulation available on the market in the future. For the young field of electric mobility, it is therefore advisable to consider possible types of manipulation at an early stage and to evaluate them especially with regard to risks.

A. Objectives

Based on the suggestion of an early risk evaluation for electric vehicles the overall goal is to determine the relevance of different types of possible manipulation in order to detect hot spots. The analysis shall, furthermore, be used to identify specific protective measures early on and to lay the foundation for focused safety concepts. This information can be used to work out future research priorities.

As a result, this paper presents an approach to a mainly qualitative risk analysis. At the moment, almost no electric vehicle is being manipulated. Therefore, the major challenge is to predict the relevance of possible types of manipulation for a future market, including manipulation of software, electronics and mechanics of core components of electric vehicles. In order to evaluate the risks of specific types of manipulation, it is necessary to define a complete taxonomy with adapted categories and classifications. In this context, the analysis is not intended to represent a mere snapshot, but rather a continuous process. It has to be possible with regard to the taxonomy to optimize the results and adapt them to new circumstances by selectively enhancing and refining scores. Consequently, the evaluation scheme must also allow the update of each sub-region, without the need to adapt other rating areas.

B. *Outline*

The paper is laid out as follows: First some background information is provided about the regarded field of manipulation, electric mobility and related risk analyses from the automotive domain (Section II). The next section covers the combination of existing approaches to the definition of risk and the description of the resulting analysis structure (Section III). Afterwards, the entire risk analysis approach is described with taxonomy and suitable sources of information to obtain relevant data. The method for calculating the total risk factor is moreover described together with the corresponding classification (Section IV). At the end, a short summary of the results, an overview of outstanding issues and an outlook is provided (Section V).

II. Constraints and Related Work

This section, first of all describes the area and circumstances under which the risk analysis is to be implemented, especially in terms of types of manipulation and the electromobility environment. In addition, two relevant existing approaches of risk analyses from the automotive domain are briefly described.

A. *Constraints*

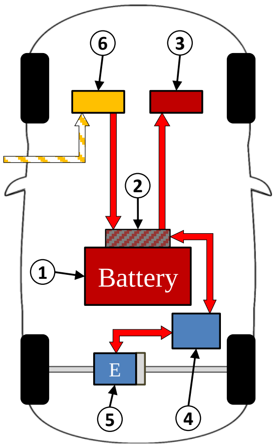
There are numerous possibilities for manipulating a vehicle. In this paper, the following two general approaches are grouped together under the central term of "manipulation" [3]:

- *Modification* includes all actions in which existing components or functions of a system are changed.
- *Retrofitting (unprofessional)* includes all actions where additional components or functions are inserted into an existing system.

It should be noted that intervention in software and electronic and mechanical components are considered for the regarded risk analysis. Based on the listed types of manipulation, there are potential threats, which have to be taken into account. These can be classified according to the underlying motivation [3]:

- *Tuning* refers to individually made modifications and retrofits with the aim of increasing a subjective benefit for the vehicle user.
- *Unauthorized manipulation* describes all changes that are sanctioned by manufacturers, insurance companies, legal regulations or other authorized third parties.
- *Abuse* refers to the use of components or functions in a way that is not intended in their use context.

Besides the theory, real threats depend heavily on the components or functions that can be manipulated. It is therefore important for the analysis to consider the regarded environment, which involves just the field of electric mobility. Only those components that are used solely in electric vehicles or are used in a different way than in conventional vehicles with combustion engines are considered for the analysis. These core components and their energetic links are illustrated in Fig. 1. The graphic is used to provide an overview of the relevant environment, but does not claim to be complete.



Components:
1: Electric energy storage
2: Periphery
- Battery management system
- Cooling
- Insulation monitor
- Contactors
- Sensors
- Fuses
3: Voltage converter (12V)
4: Power electronics
5: Electric motor
6: Onboard charger

Fig. 1. Core components of electric vehicles and their energetic links

During the entire analysis, particular attention is placed on the electrical energy storage, which is an expensive component in the vehicle and is classified as critical to safety. In addition, each cell ages and thus has a limited life, which depends, among other things, on usage conditions [4]. It moreover appears that all the core components taken into consideration are energetically or functionally connected to the battery. For this reason, it is necessary to consider all influences on the energy storage, caused by the regarded manipulations - especially with regard to possibly resulting aging effects.

B. *Relevant Risk Assessments*

There are currently no appreciable publications on the topic available with regard to the special case of electric vehicles. Therefore, two publications [3, 5] from the automotive IT environment have been taken into consideration and used as a basis. For the intended analysis, this environment is appropriate because attention is already focused on this area, caused by the limitation to the core components of electric vehicles. Subsequently, the approaches for the risk analyses of the mentioned publications are described:

J. Dittmann [3] presents a complete risk analysis of common types of electronic manipulation of vehicles and infrastructure systems, with the aim to gain an overview of their distribution and relevance. The analysis is focused mainly on road safety. The probability of occurrence of manipulation is compared with the associated risks for road safety. The assessment is carried out along automotive subsystems that have been identified as targets for manipulation. Extensive research, particularly in new media and literature, is used as a basis in this regard. In the process, the probability of occurrence is initially estimated, based on the demand for individual changes and the exploitable vulnerabilities in the system. The outcome is compared with the potentially resulting dangers – in particular safety critical damage. A calculative combination of the two areas into an overall ranking does not take place. Thus, a specific point in time is observed without providing a continuous update and the analysis relies heavily on the existing market. However, the starting point, the general procedure and the aim of the observation can be used as basis for the planned analysis. Furthermore, it is possible to take the results into account and to compare them to the ones for electric vehicles.

M. Wolf [5] describes an approach for analyzing the safety protection objectives of IT systems in vehicles. The goal is to balance the security costs of implemented security functions and the security risks of corresponding attacks (economic security). A risk analysis is presented for this purpose, in which the probability mapped to the effort needed to successfully implement an attack and the potential damage are regarded. The starting points of the analysis are security threats that are determined by previously identified security objectives. To carry out the analysis, the effort to misuse a vulnerability is assessed according to [6] and the potential damage based on a developed classification. The combination within the main categories is done additively and the resulting numerical values are classified and linked through a risk matrix to the final risk score. The advantage of the described approach is the ordinal and numerical rating and categorization that enable a continuous update cycle. The used categories allow reducing the subjective influence on the evaluation by experts. Moreover, the entire taxonomy is already adapted to the vehicle surroundings and can therefore be used as a good basis. However, the pursued goal does not fit with the objective of the planned analysis, so the results need to be treated carefully.

Both described approaches have several advantages which can be used for the planned risk analysis. But due to the specific constraints, none meets the requirements sufficiently. Therefore, an adapted and extended evaluation method is necessary.

III. RISK DEFINITION

Appropriate evaluation categories are necessary to carry out a risk analysis. Like in many engineering disciplines, in this approach the risk is defined by the probability of occurrence of an incident and the potentially resulting damage [7, 8, 9]. The mathematical risk calculation is done multiplicatively, shown in (1):

$$Risk = Probability \text{ x } Consequences \tag{1}$$

The consequences can be evaluated in terms of potential damage, caused by a successful manipulation. Since there is still no notable market for manipulation of electric vehicles, there is no information available with regard to occurrence frequencies. For this reason, it is necessary to further break down the probability criterion. Templates for this purpose are included, among others, in [7, 9, 10]. Regardless of nomenclature, all three approaches can be traced back to the definition for the probability of occurrence, formulated in (2):

$$Probability = Vulnerability \text{ x } Attractiveness \tag{2}$$

The vulnerability describes the estimated effort needed to perform a desired manipulation. Note that a small effort causes a large occurrence probability and vice versa. The criterion attractiveness evaluates how much a manipulation is considered in the market.

Thus, the structure of the overall risk analysis follows the scheme shown in Fig. 2. The three main evaluation criteria *vulnerability*, *attractiveness* and *consequences* are described in detail in the Sections IV.B to IV.D.

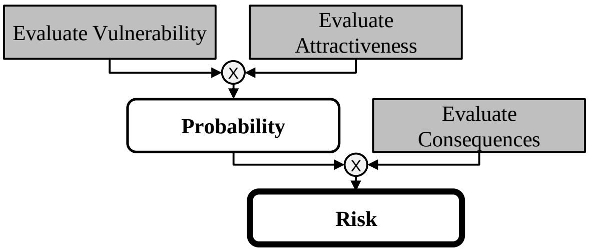


Fig. 2. Basic scheme of the risk analysis

Independent sources of information are recommended in order to clearly define the individual ratings of each evaluation criterion. The criteria can be viewed in a chronological sequence, shown in Fig. 3. The *first step* is the market and the perceived *attractiveness* of a specific type of manipulation resulting in a possible implementation. In this case, the market itself can be used as a basis for the assessment of this criterion. Each influence that affects the demand is of particular interest. The *second step* is the actual technical realization of a certain manipulation. The implementation effort depends largely on the modified system and its resistance against the manipulation process (*vulnerability*). For this reason, the evaluation takes place on a technical level. Through the change process, different *damage* may occur (*step 3*). In the evaluation, all primary damage can be taken into account, which may result from specific types of manipulation.

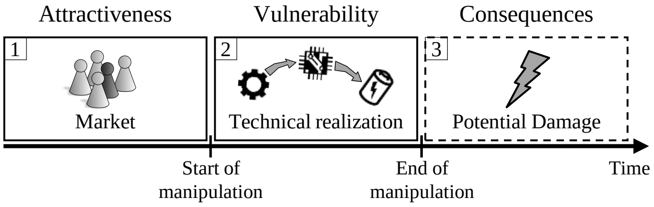


Fig. 3. Chronical sequence of a manipulation related to the risk analysis

IV. RISK ANALYSIS

This section covers a complete approach for a risk analysis regarding manipulation of electric vehicles. It is based on the categories, which have already been defined in Section III and the related existing risk analyses, described in Section II.B. Furthermore, the given constraints are taken into account by focusing on the core components of electric vehicles, see Section II.A. The approach starts directly at the lowest level, the systematic identification of the starting points of the whole analysis. Following this is the individual description of the three main evaluation categories (vulnerability, attractiveness and potential damages) including appropriate subcategories and corresponding classifications. The overall risk calculation and classification is finally described.

A. Identification of Potential Attack Paths

The starting point of a risk analysis contains the elements, which shall be evaluated and is therefore essential for the desired results. In this paper the possible attack paths for implementing specific types of manipulation are chosen as starting points to evaluate the relevance of these types. An attack path describes the chosen path along involved subsystems up to the implementation of a specific manipulation. This means that all types of manipulation which shall be considered in the analysis need to be captured already at this point, together with all relevant associated attack paths. In order to achieve a sufficient coverage, a systematic procedure is recommended (Fig. 4).

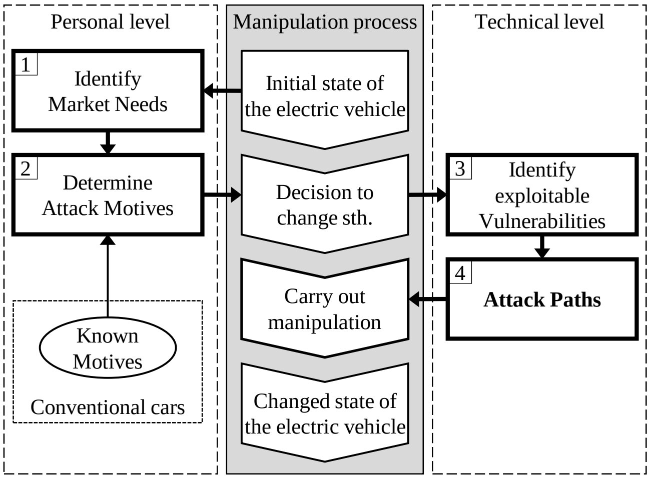


Fig. 4. Systematic identification of attack paths based on the manipulation process

The basis of the schematic approach, shown in Fig. 4, is a conceptual model of the events that take place during manipulation. Starting directly at the initial state of electric vehicles, possible needs of their users are derived in the *first step* of the concept. They can occur, for example, due to unsatisfactory vehicle attributes, like the limited range or top speed. The sources of information listed below can be used for data acquisition - the focus lies on generating a wide range of needs.

- Disadvantages of electric vehicles compared to conventional vehicles
- Surveys, studies and statistics
- Literature and new media [3]

In the *second step*, possible attack motives behind the different types of manipulation are derived from the identified needs. These motives are additionally supplemented with known manipulation motives based on the current vehicle market including especially targets with fraudulent intentions.

In the manipulation process, the decision to pursue a manipulation is made depending on the attack motives, which represents the transition from the personal level to the technical level. In the *third step*, vulnerabilities, which can be exploited for this purpose, are identified at a technical level, along with the involved subsystems and functions. For a single attack motive, there are usually several possible variations. According to this, the types of possible manipulation and the exploitable vulnerabilities are directly derived from the vehicle components.

The systems considered are basically very similar to those of current conventional vehicles and thus comparable in this case. This enables to transfer existing knowledge into the evaluation of electric vehicle systems. In cases where this is not possible, a detailed technical examination is required.

Each reasonable and purposeful combination of vulnerabilities identified in step three, equals one attack path. The starting points for the risk analysis, determined in the *fourth step*, comprise an attack motive and an associated specific attack path - collectively referred to as an *attack path.*

After identifying a suitable manipulation possibility, defined by a specific attack path, the implementation towards a new vehicle condition takes place.

B. *Evaluation of Vulnerability*

This section outlines an assessment method for evaluating the vulnerability along an attack path from a technical perspective based on predefined criteria. The aim is to generate a corresponding ranking system, which is intended to reflect the necessary effort to implement the different types of considered manipulation.

IT security products are often evaluated today using Common Criteria [11]. These contain in [6] a method for assessing and calculating the necessary effort to execute a manipulation based on a security vulnerability. In this approach this method is used, with the minor adjustments, described in [5], in order to adapt to the automotive environment. The rating categories and the associated numerical factors are listed in Table I. A detailed description of the automotive domain related reference can be found in [5].

TABLE I. REFERENCE CLASSIFICATION FOR THE VULNERABILITY FACTORS [5, 6]

Category	**CEM, B.4.2.3** [6]	
	Reference	***Factor***
Elapsed time describes the overall time required for a manipulation, including planning, preparatory work, implementation and rework.	Hours	0
	Days	1
	Weeks	3
	Months	7
Specialist expertise describes the required expertise of a manipulator, which is necessary for carrying out a manipulation.	Layman	0
	Proficient person	3
	Expert	6
	Multiple expert	8
Knowledge of the target includes the necessary information about the features and condition of the vehicle system and the difficulty of obtaining information.	Public information	0
	Restricted information	3
	Sensitive information	7
	Critical information	11
Access describes how difficult the access to the system is which is to be manipulated (software and hardware).	Unnecessary or unlimited	0
	Easy	1
	Moderate	4
	Difficult	10
Equipment describes the necessary equipment and tools (software and hardware) which are required for a manipulation	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

The categories of the risk analysis taxonomy from Table I can be used directly for the desired analysis, even if they relate to IT systems in conventional cars [5]. This is possible, since the focus is directed almost exclusively to electronic components with the constraint on the core components of electric vehicles. Their basic structure and the protection systems used differ usually not from the systems in conventional vehicles. Because of the restriction in this particular case, the proposed categories can also be applied to mechanical changes without further adjustments.

To carry out the assessment based on the proposed categories, it is necessary to have expert knowledge about the observed types of manipulation. Since a lot of information on the vulnerabilities of the included systems is already available for conventional vehicles, it is possible to apply reviews relating to similar systems. Cases of manipulation where this is not possible have to be individually assessed by experts and optionally in specific studies. The approach described allows a vulnerability assessment of the regarded systems, although the market for manipulation in this area is still almost non-existent.

The combination of categories and the overall effort is done accordingly to [6], by summarizing the corresponding factors of each category, as shown in (3).

$$AP = AP_{\text{Time}} + AP_{\text{Expert.}} + AP_{\text{Knowl.}} + AP_{\text{Access}} + AP_{\text{Equip.}} \quad (3)$$

A suitable classification for the calculated vulnerability score is defined in [6], shown in Table II. It can be applied for the intended purpose without modification. But it is necessary to consider that an effort is classified, not directly the vulnerability. A high effort implies a low vulnerability and vice versa. Taking this fact into account, there are logical inverse numeric values in brackets, assigned to the classes shown in the table. These display the corresponding vulnerability and can consequently be used for the risk calculation.

TABLE II. ATTACK POTENTIAL CLASSIFICATION [6]

Values	Total attack potential classification
0 - 9	Basic (5)
10 - 13	Enhanced Basic (4)
14 - 19	Moderate (3)
20 - 24	High (2)
> 24	Beyond High (1)

C. Evaluation of Attractiveness

This section describes a possible evaluation method for estimating the perceived market attractiveness of individual manipulation of electric vehicles. The challenge is again the market itself. Due to the lack of types of manipulation available for electric vehicles, there is currently no assessable demand. Because prices depend on supply and demand, a monetary consideration is not possible either. So, a predictive analysis of the market is necessary for assessing the perceived attractiveness of a manipulation.

The approach is based on the analysis of the existing electric vehicle market. Therefore, the motivation behind a manipulation and the resulting benefits are taken into consideration [3, 6]. Since the attractiveness depends as well on the size of the market share of electric vehicles having the necessary components and systems installed for a specific manipulation, the market penetration of components is also included in the evaluation [3].

The underlying valuation basis can be adopted to a limited extent from [3], because their analysis relies heavily on the market, not existing for the regarded case. The three evaluation criteria and their adaption to the circumstances are as follows:

1) Criterion - Motivation

The objective of this evaluation category is a classification, regarding the severity of the motives behind different types of manipulation. Since a manipulation is carried out to realize a motive, not a specific attack path, the motives from Section IV.A can serve as an assessment basis. These motives are separately derived from the markets of electric cars and conventional cars. This fact has to be considered in the evaluation of the corresponding motivation, illustrated in Fig. 5.

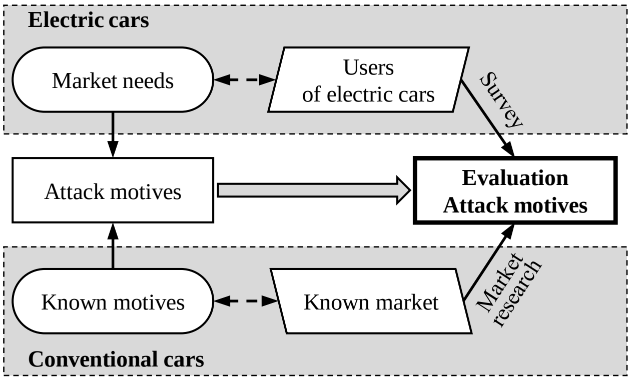


Fig. 5. Diagram outlining the evaluation of attack motives

For the attack motives, derived from the known market for *conventional cars*, the evaluation is directly based on the published assessments from [3]. These are already available for many types of manipulation and are qualitatively classified into five nominal classes. If necessary, an extended examination on the same basis can be aligned.

In the field of *electric cars*, the observation is focused on their users. Even if there is currently no offer for manipulation, the demand arises based on the needs of these users. Their needs are directly linked with the corresponding motives and therefore, the severity of the needs can serve as an assessment basis. For the evaluation, a survey by questionnaire is to be implemented, in which the users of electric vehicles are directly asked about relevant needs. For example, by rating a specific need based on grades from one to five. The results can be supplemented by existing surveys and studies on perceived disadvantages of electric vehicles. The whole database provides a ranking system, which can be classified. For this purpose, five discrete classes are used, which are carefully adapted to the categorization for the motives of the conventional market. The proposed rating classes and the related detailed references are listed in Table III.

It should be noted that the motives based on conventional vehicles are only used as a supplement. If a case occurs, in which a combined evaluation does make sense, each individual case has to be assessed by experts. Moreover, in this approach, all attack paths associated with a motive have the same score in this category. But the assessment can also be systematically refined for particularly critical attack paths.

2) Criterion - Benefit

The aim of this criterion is to evaluate, to what extent a manipulation along a specific attack path contributes to the satisfaction of the corresponding attack motive. In order to perform the assessment of benefits from an objective point of view, a technical analysis of the considered core components of electric vehicles is used. The regarded systems are from actual vehicles, which are probably the first ones to be manipulated.

To classify the benefit on a technical basis, a reference value is used, illustrated in Fig. 6. Within this approach, this value represents a reasonable limit for the possible benefit, from which an attack motive is regarded as completely fulfilled. This value must be specified by experts, for every regarded motive at the very beginning of the risk analysis. In conclusion, a manipulation gets the highest rating if the created benefit reaches the reference value for the underlying motive. If the benefit is below this value, the classification is based on the detailed references in Table III.

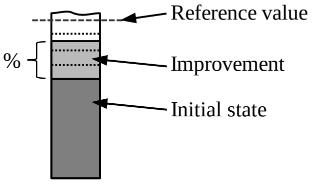


Fig. 6. Reference value used to evaluate benefits

If a manipulation also causes significant losses in other areas, it has to be considered in the evaluation by reducing the rating accordingly. The evaluation is based on the worst-case scenario, which means that a regarded manipulation is always executed in a perfect way. Gradations, for example due to an unqualified implementation, are not considered.

The reference value is crucial for evaluating the benefits. If differences to reality are recognized, then the limits have to be adjusted. This may especially be the case when new manipulation possibilities are available.

3) Criterion - Market Penetration of Components

If an attack path contains a component that is installed in only very few vehicles on the market, the overall attractiveness of the path is correspondingly lower. It is necessary to analyze in this category the market penetration of observed components and systems, including their different versions. As valuation basis the current market of electric vehicles is used again.

The analysis takes place primarily based on a secondary market research of new media and publications. Sales figures or vehicle registration statistics of currently available electric cars can be linked to the relevant installed components in order to receive an estimate of the market penetration of the components at a specific time. To take a possible future market into account, it is possible to include forecasts relating to future sales figures or the use of different components. The described procedure can be realized with reasonable effort, because there are currently only a manageable number of series-production cars available on the German market, with only a few derivatives [12, 13].

The final evaluation is based on the part of the market, which is practically able to perform a manipulation. In case of modification this means every car with a specific component or function – i.e., the market penetration. In case of retrofitting, it is of interest, which part of the market does not already have the regarded component or function – the inverse market penetration [3]. The proposed classification is based on [3] and therefore divided into five classes. These classes and the corresponding detailed references, as shown in Table III, are thereby related to the modification case.

TABLE III. Reference Classification for the Attractiveness Factors

Category	**Attractiveness**		
	Reference	***Detailed Reference***	***Factor***
Level of motivation	Very low	Among the users of electric vehicles, there is (almost) no need for a change (Guideline: Ø 1 Pt. / 5 in survey)	0
	Low	There is a low need for a change (Guideline: Ø 2 Pts. / 5 in survey)	1
	Moderate	There is a moderate need for a change (Guideline: Ø 3 Pts. / 5 in survey)	2
	High	There is a great need for a change (Guideline: Ø 4 Pts. / 5 in survey)	3
	Very high	Among the users of electric vehicles, there is a very great need for a change (Guideline: Ø 5 Pts. / 5 in survey)	4
Benefit	Very small	Negligible / no increase to the initial state in relation to the reference value (Guideline <10%)	0
	Small	Small increase in relation to the reference value (Guideline 10-40%)	1
	Moderate	Moderate increase in relation to the reference value (Guideline >40-70%)	2
	High	Significant increase in relation to the reference value (Guideline >70%)	3
	Very high	Increase reaches / exceeds the reference value (Guideline = >100%)	4
Market penetration	Very small	Component is present in (almost) no vehicle (Guideline 0-20%)	0
	Small	Component is present in a few vehicles (Guideline 20-40%)	1
	Average	Component is present in a average amount of vehicles (Guideline 40-60%)	2
	High	Component is present in many vehicles (Guideline 60-80%)	3
	Very high	Component is present in (almost) every vehicle (Guideline 80-100%)	4

Note: The shown classification is a proposal that must still undergo practical testing. Some adjustments may still be necessary.

4) Attractiveness Calculation and Classification

In order to calculate with the qualitative evaluation results of the three described categories, they need to be assigned to numeric factors. [3] basically uses the same categories and some results are already included in the attractiveness evaluation scheme. For the approach outlined in this paper, the qualitative classification of [3] based on five levels from low to high is directly transferred to discrete, numerical factors from zero to four and applied to the attractiveness categories. The resulting factors are listed in the last column of Table III. However, these factors are just based on a reference analysis and not yet verified. If necessary, they can be scaled to change the relation between the categories or replaced with non-linear values.

To calculate the final value for the perceived attractiveness of a manipulation, the corresponding factors of the three described evaluation categories are combined additively (4). The reason for the additive combination is that the categories are independent of each other, regarding the attractiveness. An increase of one category will not affect the attractiveness more than the local increase.

$$AT = AT_{\text{Motivation}} + AT_{\text{Benefit}} + AT_{\text{Penetration}} \tag{4}$$

The proposed classification for the calculated attractiveness values is shown in Table IV. The value ranges are based on an average value approach [3]. This implies for example that the combination of a *very low*, a *moderate* and a *very high* rating leads to a *moderate* score. This gradation is possible for the regarded case, since the three categories have an identical classification, according to the factors. If this needs to be changed, for example in favor of non-linear factors, mentioned above as a possibility, then the classification of the attractiveness (TABLE IV) has to be adapted as well. The numeric values in brackets, assigned to the classes, are used as factors for the final risk calculation.

TABLE IV. ATTRACTIVENESS CLASSIFICATION

Values	Total attractiveness classification
11 - 12	Very high degree of interest (5)
8 - 10	High degree of interest (4)
5 - 7	Moderate degree of interest (3)
2 - 4	Low degree of interest (2)
0 - 1	No interest (1)

D. *Evaluation of Potential Damage*

This section outlines an assessment method for evaluating the potential primary damage that may occur due to a manipulation of an electric vehicle. For the assessment, the taxonomy of [5] is used (TABLE V), which is already adapted to the automotive environment regarding categories and factors. The possible damage is split into safety-critical, economic and functional parts:

- The *safety-critical damage* includes all incidents that may cause injuries to persons, triggered by manipulation. The classification corresponds to the ASIL classes [14], including the relevant factors. For the evaluation, the results of analyses on the basis of functional safety of electric vehicles can be taken into account.
- In [5] the *economic damage* are the total costs that can be caused by manipulation, including e.g. reputation damage. This approach is too extensive for the restricted area of core components of electric vehicles, so the attention is placed mainly on the primary financial loss. The reference, shown in Table V, have therefore been changed to the original descriptions of [15]. The factors for evaluating the economic damage stay unchanged.
- The *functional damage* contains all remaining damage that does not cause notable injuries or significant financial losses. These primarily include sacrifices relating to vehicle comfort functions. The classification, selected by [5], comes from the common practice of Failure Mode and Effects Analyses (FMEA) [16]. For that reason, known FMEA results for electric vehicles can be used directly for the evaluation.

TABLE V. REFERENCE CLASSIFICATION FOR THE DAMAGE POTENTIAL FACTORS [5]

Category	Damage	
	Damage Reference	***Factor***
Safety severity classes	Life-threatining injuries (survival uncertain), fatal injuries	10000
	Severe and life-threatining injuries (survival probable)	1000
	Light and moderate injuries	100
	No injuries	0
Finance severity classes	Existence-threatening effects	1000
	Significant effects	100
	Noticable effects	10
	Low, barely noticable effects	0
Operational functionality severity classes	Vehicle unusable (FMEA > 8)	100
	Service required (FMEA 6 – 8)	10
	Comfort affected (FMEA 2 – 5)	1
	No relevant effects (FMEA 1)	0

In order to carry out the assessment based on the proposed categories, expert knowledge about the observed changes and the correct classification of the possible damage is necessary. Because different experts may be needed for this purpose, the classification is performed in several steps (Fig. 7).

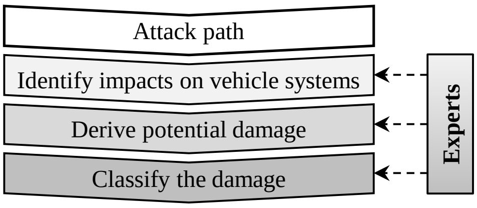


Fig. 7. Steps of damage assessment by experts

First, the impacts of a manipulation, based on a specific attack path, to all systems in the vehicle are determined. This is done on the basis of physical quantities. During the examination, it is important to consider effects on the energy storage device especially with regard to aging effects. Based on the determined impacts, the resulting potential damage can be derived. If not enough information is available from real cases, then new studies are necessary. According to the evaluated damage, the concluding classification can take place. Once again, the worst-case scenario is taken into consideration. If there are multiple kinds of damage within a category, the damage with the highest factor is chosen.

In order to calculate the total damage potential, an additive combination of the ratings is used [5], formulated in (5).

$$DP = DP_{\text{Safety}} + DP_{\text{Financial}} + DP_{\text{Operational}} \qquad (5)$$

An appropriate classification of the calculated damage potential is already given in [5], shown in Table VI. The assigned values in brackets are used as factors for the risk calculation.

TABLE VI. POTENTIAL DAMAGE CLASSIFICATION [5]

Values	Total damage potential classification
> 210	Catastrophic (4)
22 - 210	Critical (3)
3 - 21	Medium (2)
0 - 2	Insignificant (1)

E. Risk Calculation and Classification

The final step in the risk analysis is the calculation and the subsequent classification of the final risk-score. The calculation takes place sequentially (due to intermediary classifications) on the basis of (1) and (2). First, the occurrence probability is calculated using the second equation. The vulnerability and attractiveness criteria are multiplicatively combined and then classified according to Table VII. In [3], the same major and minor criteria are considered. For this reason and in order to achieve comparability, the classification is based on the one used in [3], which is carried out only qualitatively without underlying numerical values. Therefore, it is not possible to transfer into the multiplicative rating system without slight adjustments. Fortunately, shrinking the very large mean area (possibly) is a possibility in favor of the two smaller adjacent regions (unlikely and likely), what leads to a satisfactory result.

TABLE VII. PROBABILITY CLASSIFICATION

Values	Total Probability Classification
> 16	Certain (5)
12 - 16	Likely (4)
5 - 11	Possibly (3)
3 - 4	Unlikely (2)
1 - 2	Rare (1)

To complete the analysis, the risk value is calculated according to (1) by multiplying the rating of the probability of occurrence and the potential damage. The resulting value indicates the risk of an observed attack path. Together with the ratings of other attack paths, a ranking system can be created. The relevance of individual elements can therefore only be assessed in relation to the ranking.

In order to categorize risk ratings independently, an additional classification is necessary. For this purpose, there are many approaches from different areas [8, 9, 17], but there are currently no mandatory risk acceptance values available for the automotive sector. However, the classification of [18] matches the requirements satisfactory. It origins from the field of public transport networks and can be applied without modification. The final risk classification and the corresponding risk matrix are shown in Table VIII.

TABLE VIII. TOTAL RISK CLASSIFICATION AND RISK MATRIX [18]

Values	Total Risk Classification	
> 14	Intolerable	█
8 - 14	Precaurious	▓
4 - 7	Tolerable	▒
1 - 3	Neglible	░

Probability	Risk Matrix			
Certain (5)	(5)	(10)	(15)	(20)
Likely (4)	(4)	(8)	(12)	(16)
Possibly (3)	(3)	(6)	(9)	(12)
Unlikely (2)	(2)	(4)	(6)	(8)
Rare (1)	(1)	(2)	(3)	(4)
	Insignif. (1)	Medium (2)	Critical (3)	Catastr. (4)
	Damage potential			

V. SUMMARY AND OUTLOOK

A comprehensive approach for a specific risk analysis for electric vehicles is presented to estimate the relevance of a particular manipulation or attack path for a future market. The approach is based on different established methodologies and procedures. These are combined and systematically adapted to provide appropriate evaluation categories for each evaluation level. Particular attention is placed on the specific field of electric mobility. An adapted classification was developed and described especially for the rating category "attractiveness" and the corresponding subcategories. As a result, the taxonomy for the complete risk analysis is provided. But the score values are not yet fully validated in scope and depth. They need to be examined accurately and may be adjusted by new objectives of research - this relates particularly to the attractiveness classification. For a first revision of the analysis an initial data set is necessary. The paper outlines procedures for a systematic acquisition of relevant data, as well as practical ways for obtaining such data. The market and a technical assessment based in particular on investigations are used as an information basis. Until the first data set is obtained, many studies, researches and surveys are necessary. To limit the effort and to identify hot spots at an early stage, the first analysis is planned on the level of abstraction of the considered core components, with three possible attack paths each (software, electronics and mechanics). This first analysis can be used to identify the important components in order to assess them afterwards in much greater detail. Due to the mathematical background, existing ratings of the risk analysis can be actualized separately at every part without the need to adapt other ratings. The analysis is designed for electric vehicles, but can be extended to the electrical drivetrain of hybrid electrical vehicles as well.

ACKNOWLEDGMENT

We would like to thank the reviewers for their corrections and helpful suggestions. The work was conducted by basic funding of Allianz SE, Global Automotive.

REFERENCES

[1] A. Thiemel, M. Janke, and B. Steurich, “Tachomanipulation - technisch vorbeugen,” (Deutsch), *ATZ Elektronik*, no. 2, pp. 106–110, 2013.

[2] F. T. Piller, *Mass Customization: Ein wettbewerbsstrategisches Konzept im Informationszeitalter,* 4th ed. Wiesbaden: Dt. Univ.-Verl, 2008.

[3] J. Dittmann, T. Hoppe, S. Kiltz, and S. Tuchscheerer, *Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen: Gefährdungspotentiale für die Straßenverkehrssicherheit; [Bericht zum Forschungsprojekt FE 88.007/2009].* Bremerhaven: Wirtschaftsverl. NW, Verl. für neue Wiss, 2011.

[4] A. Jossen and W. Weydanz, *Moderne Akkumulatoren richtig einsetzen: 36 Tabellen,* 1st ed. Neusäß: Ubooks, 2006.

[5] M. Wolf and M. Scheibel, “A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems,” in *Automotive - Safety & Security 2012: Sicherheit und Zuverlässigkeit für automobile Informationstechnik*, Bonn: Ges. für Informatik, 2012, pp. 195–210.

[6] Common Methodology for Information Technology Security Evaluation, V.3.1, Revision 3, 2009.

[7] C. Eckert, *IT-Sicherheit: Konzepte - Verfahren - Protokolle,* 8th ed. München: Oldenbourg, 2013.

[8] EN 50126, “Railway applications - The specification and demonstration of reliability, availability, and safety (RAMS),” 1999.

[9] Securestation, “Passenger station and terminal design for safety, security and resilience to terrorist attack: D3.1 - Evaluation report of the existing risk assessment methodologies and securestation methodology,” 2011.

[10] C. S. Wright, “A Taxonomy of Information Systems Audits: Assessments and Reviews,” *SANS Institute*, 2007.

[11] Common Criteria for Information Technology Security Evaluation
"Part 1: Introduction and general model, V.3.1, Revision 4, 2012"
"Part 2: Security functional components, V.3.1, Revision 4, 2012"
"Part 3: Security assurance components, V.3.1, Revision 4, 2012".

[12] ADAC Fahrzeugtechnik, *Elektroautos: Marktübersicht / Kenndaten.* Available: http://www.adac.de/_mmm/pdf/27373_46583.pdf (2013, Jan. 28).

[13] Michael Rau (GreenGear), *Marktübersicht 2013: Elektroautos.* Available: http://www.greengear.de/elektroauto-marktuebersicht-2013 (2013, Jan. 28).

[14] ISO 26262, “Road vehicles - Functional safety,” 2011.

[15] German Information Security Agency, BSI-Standard 100-4: Business Continuity Management, 2008.

[16] Automotive Industry Action Group (AIAG), “Potential Failure Mode and Effects Analysis (FMEA),” 2008.

[17] D. G. Firesmith (SEI), “A Taxonomy of Security-Related Requirements,” 2005.

[18] M. Mueth, “EU project COUNTERACT, SSP4/2005/TREN/05/FP6/S07.48891: Generic guidelines for conducting risk assessment in public transport networks,” no. D 3 PT4, 2007.