A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems

Marko Wolf, ESCRYPT GmbH, Munich, Germany (marko.wolf@escrypt.com)
Michael Scheibel, TÜV Informationstechnik GmbH, Essen, Germany (m.scheibel@tuvit.de)

Abstract: By now, security engineering is an accepted challenge in the development of most vehicular IT systems. However, even though many vehicular security threats and effective protection measures are known in general, automotive engineers have difficulties to realize efficient security solutions such that the costs for certain protection measures are appropriate to the actual security threats in order to avoid "under- protection" as well as "over-protection", which both are unacceptable particularly in the automotive domain.

By applying a thorough security risk analysis, which incorporates the special characteristics of the automotive domain, we would have a qualified taxonomy to make well-founded decisions about the security measures effectively required. We therefor present a methodical approach for conducting a meaningful security risk analysis, which focusses particularly on vehicular IT systems. This approach applies systematic estimations for the two mandatory factors of any risk analysis, the potential damages and the probability of a successful security attack, both based on industry-proven methods and taxonomies carefully adapted to vehicular IT security scenarios.

1 Motivation

Strong IT security measures are often mandatory to enforce vehicular business models, liability, legal issues, warranty issues, and in particular to ensure the dependability of many of the next generation vehicular safety systems [An03, Br04, Wo09]. The automotive security protection measures, which will become actually implemented, should be determined by a well-founded costs benefit analysis, which prevents undersized, but also oversized security solutions. Consequently, we need a reliable taxonomy to be able to balance the costs and the complexity added for realizing a vehicular security measure against the potential damage caused by a potential security breach of the particular vehicular IT system. By applying a well-founded security risk analysis, which systematically evaluates the "difficulty" for realizing a certain security attack and the damage caused by this attack, we would have a qualified taxonomy to make well-founded decisions about the security protection measures effectively required. A meaningful security risk analysis thus particularly enables the realization of so-called *economic security* solutions that means that the total cost of a successful attack shall exceed the potential economic gain and shall be proportional to the potential damage, respectively. Finally yet importantly, a meaningful risk analysis would act as the underlying "security business model" to argue and prove for the necessity and necessary strength of appropriate IT security measures.

1.1 Our Contribution

Even though some general approaches and simple taxonomies for IT risk analyses already exist (e.g., [TVRA]), there is so far no systematic approach for IT security risk assessment adapted to vehicular IT scenarios, which are different to standard IT systems, for instance, regarding the attack paths (e.g., internal physical attacker) or regarding potential attack impacts (e.g., driving safety). Hence, this work provides a carefully adapted, four-step methodical approach for calculating the IT security risks especially for vehicular IT scenarios. Our approach therefor provides a systematic evaluation scheme together with an appropriate taxonomy, which enables a quantified rating for the two underlying factors, the "difficulty" for realizing a certain security attack, and the damage that can be caused by this attack, both well-adapted to the special characteristics of the automotive domain. The practical feasibility of our proposed approach will be demonstrated and illustrated by a real-world automotive security application example.

The paper is organized as follows: First, we give some background information on the methods we use for developing our risk analysis approach (Section 2). After that, we describe how these methods can be systematically combined to form a risk analysis method and give an example of its application (Section 3). We then discuss how to get relevant input data for risk analyses and how to use it in our risk analysis model (Section 4). We finally close our contribution with a short note about a helpful tool implementing our approach and assisting the systematic acquisition of all relevant input data (Section 4.3) together with a short summary of our results by giving an outlook and an overview of open questions (Section 5).

1.2 Related Work

Various authors have identified the need for information security and software protection in vehicles [An03, Br04, Wo09]. They present different security vulnerabilities and threats and propose a range of security measures for existing and upcoming vehicular IT systems. However, except for some completely (legally) mandatory security requirements, there are no systematic cost-benefit analyses for efficiently thwarting other security threats. On the other hand, there are already first systematic security risk evaluation approaches for standard IT systems such as telecommunication networks or industry automation [Fi05, TVRA, VDI2182]. However, these approaches are only limitedly applicable to the special security environment of a vehicular IT system due to the completely different attacker incentives, attacker capabilities (e.g., internal physical attacks) and different potential damages (e.g., human injuries, scalability). Moreover, both approaches mentioned remain quite inexplicit and generic especially regarding the identification and estimation of potential damages. After all, [GL02, Wi06] analyze the optimal investment level in information security as the relation of investments to protected assets. As opposed to this universal view to economic security our approach provides a very concrete, quantified view clearly adapted to the special characteristics of the automotive domain.

2 Preliminaries

The following sections give some background information on the risk definition within an IT security context, the Common Criteria for IT Security Evaluation (CC) and the

Safety Integrity Levels (SIL) used in our approach. These are methods from different IT disciplines, not only from the automotive domain. However, they later become specially adapted and linked together to enable a well-founded vehicular security risk evaluation.

2.1 Risk Definition

In most engineering disciplines (e.g., [EN50126]), risk is generally defined as follows.

risk = (probability of an accident) x (expected losses through that accident) (2.1)

For IT security scenarios, the *probability of an accident* can be mapped to the *attack potential* (cf. Section 3.2) required to successfully mount a certain attack, which means to carry out an existing security threat and to misuse a security vulnerability. In our case, the attack potential describes (amongst others) the accumulated technical, financial, and intellectual resources that are required to successfully mount a certain attack. This approach is based on the meaningful assumption that the probability of an accident – which in our IT security scenario means a successful security attack – is decreasing with the increase of the attack potential required. The *expected losses* in turn can be mapped to the *damage potential* (cf. Section 3.3) that means the global sum of all financial and operational damages and particularly of all potential damages regarding vehicular driving safety (if applicable).

2.2 Common Criteria

Most security evaluations of IT (security) products today are done based on the *Common Criteria for Information Technology Security Evaluation* (CC) [CC07]. These criteria basically consist of a catalogue of pre-defined security functional requirements that the evaluation target claims to fulfill as well as pre-defined levels of assurance that give insight on how deep the evaluation of this claim has been done. Custom functional requirements and assurance packages can be added. The evaluation is carried out by an evaluation laboratory and supervised by a governmental institution. As such, evaluations up to a certain evaluation assurance level (EAL) are internationally accepted [CCRA]. The criteria are accompanied by the *Common Methodology for Information Technology Security Evaluation* [CEM] describing the methodology behind a CC security evaluation. The CEM includes a method for calculation the potential of attacks on the evaluation target, which we use for our risk analysis taxonomy.

2.3 Safety Integrity Levels (SIL)

The *Safety Integrity Levels* (SILs) represent a discrete, systematic classification for the functional reliability of safety relevant electronics. There are four SILs, with SIL 4 having the lowest risk for a malfunction (and thus the highest reliability) and SIL 1 in comparison having a “higher” risk for a malfunction (and thus a “lower” reliability). The SILs are defined in [IEC61508] and can be directly referenced to the abbreviated injury scale (MAIS) from the Association for the Advancement of Automotive Medicine (AAAM) [AAA05] that classifies the severity of injuries from car accidents (cf. Table 1). There have been very recent standardization efforts to translate the more generic SIL definitions into specialized *Automotive Safety Integrity Levels* (ASIL) in order to have a more precise adaption of SIL for passenger car vehicular electronics. The corresponding

standard [ISO26262] eases and harmonizes the determination of automotive-specific risk classifications for potential safety hazards caused by malfunctioning vehicular electronics. The metrics and proportions provided by SIL (cf. Table 1) will be directly adapted by our safety damage potential taxonomy, which is described in Section 3.3.

Maximum Abbreviated Injury Scale		SIL reference [IEC61508]	Risk reduction factor (SIL)	ASIL reference [ISO26262]
S0	No injuries	1	10 – 100	A
S1	Light and moderate injuries	2	100 – 1000	B/C
S2	Severe and life-threatening injuries (survival probable)	3	1000 – 10,000	C/D
S3	Life-threatening injuries (survival uncertain), fatal injuries	4	10,000 – 100,000	– (not applicable)

Table 1: Safety integrity level metrics and corresponding proportions

3 Vehicular IT Security Risk Analysis

This section describes our approach to carry out a vehicular IT security risk analysis that is required within virtually all (e.g., [TVRA, VDI2182]) security design cycles (cf. Figure 1). A vehicular IT security risk analysis hence starts with an identification of the actual security assets and their high-level security objectives, which are exposed to certain security threats from potential attack paths (cf. Section 3.1). We then motivate and describe our approaches for calculating the attack potential (AP) and the vehicular damage potential (DP) for a certain attack path (cf. Sections 3.2 and 3.3). Based on AP and DP, we finally motivate and describe our approach to assess and classify the respective vehicular IT security risk. The section closes with a practical example using our approach for a vehicular IT security risk analysis.

3.1 Identification of Security Objectives, Security Threats, and Attack Paths

Before we can evaluate any vehicular attacks, we have to identify the high-level *security objectives* sometimes also referenced as *security goals* or *security aims*. Security objectives accumulate all relevant security assets (e.g., critical data, functionality, or resources) and *security policies* (e.g., "Only authorized personnel may change function parameters of this vehicular component.") together with potential misuse cases and issues to be resolved on a very high-level basis. A security objective for a certain vehicular electronic control unit (ECU) could be, for instance, preventing IP theft or counterfeiting of ECU's software by preserving the confidentiality of the corresponding ECU software. The next step in our approach is to identify possible *security threats* against each of the security objectives we have identified before. A threat is hereby defined by an attacker, an adverse action, and the attacked asset [CC07, Part 1, A.6.2]. A community-developed set of relevant security objectives, security threats, and generic security evaluation criteria for a given family of IT products or IT systems is called a *protection profile* (PP). A PP typically covers all important, known security issues (independently from potential security solutions) that at least have to be verified for

proper counteracting in a security evaluation for evaluation targets of this family. Hence, PPs are often created in context of CC evaluations and are currently available for many IT products and IT systems, but unfortunately not for automotive IT components such as ECUs (Electronic Control Units). By then, we refer to general approaches for identifying security objectives, threats and attack paths (e.g., [Fi05, TVRA, VDI2182]) in combination with corresponding vehicular IT security work (e.g., [An03, Br04, Wo09]).

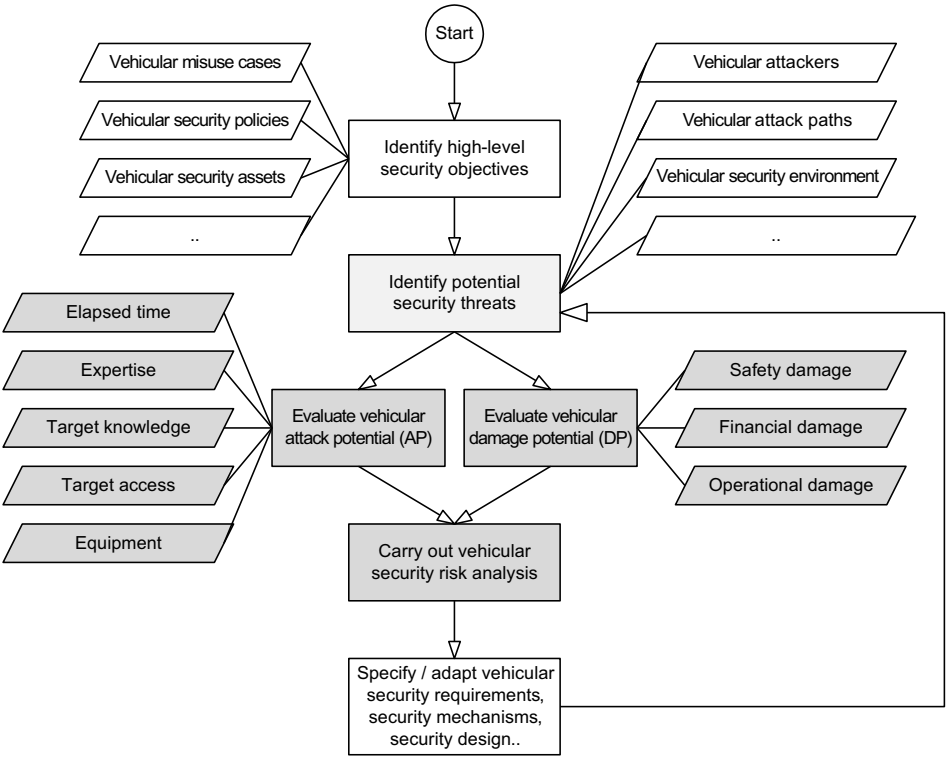

Figure 1: Security risk analysis (gray) as part of the vehicular security design process

The security threats on a security objective can then be organized in an attack tree as shown in Figure 2. Please note that any attack tree is by no means (and cannot be) complete. In contrast to the original attack tree proposal that uses the attacker's goal as the root node [Sc99], we put the security objective at the top. A successful attack on the security objective can then be described by a path from a leaf to the root. Please see [ABD06] and [MSR04] for other applications of attack trees and similar techniques in automotive contexts. We can now calculate the attack potential required to successfully carry out each of the attack paths on our security objective.

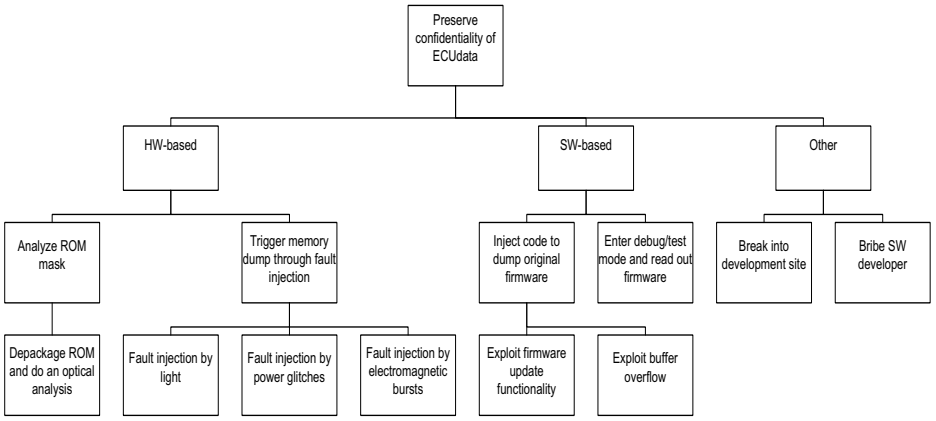

Figure 2: Incomplete attack tree against an ECU security objective regarding data confidentiality

3.2 Attack Potential Calculation

To calculate the attack potential for an identified attack path we follow the industry-proven, standardized CC approach as described in [CEM, B.4] and hence estimate the resources needed to successfully mount the attack in terms of time required for identification and exploitation[1], specialist expertise, knowledge of target, and access and equipment required. This approach can include both known and assumed to be (at least medium-term) possible security attacks (cf. for instance RSA factoring challenges) whereas the latter yields to a higher attack potential. The individual factors are shown in Table 2, which has been taken from [CEM, B.4.2.3] with only minor modifications[2]. All estimations have to consider the worst-case scenario from the security perspective. In case, the attack reference estimation is in-between two categorizations, it is also possible to take an appropriate intermediate value for the corresponding factor.

Category	[CEM, B.4.2.3] Reference	More detailed automotive domain related reference (if applicable)	Factor
Elapsed time	Hours	(none)	0
	Days	(none)	1
	Weeks	(none)	3
	Months	(none)	7
Specialist expertise	Layman	Ordinary vehicle owner/driver; Knows only very simple attacks (e.g., Internet feature activation code generators; simple dip switches or simple shortcuts)	0
	Proficient person	Experienced owner, ordinary garage personnel; Knows simple, popular attacks (e.g., odometer tuning, installing counterfeit parts)	3

[1] Note that CC from version 3.1 no longer distinguishes between identification and exploitation phase.
[2] For example, the category "Elapsed Time" has been carefully reduced from ten to four references.

Category	[CEM, B.4.2.3] Reference	More detailed automotive domain related reference (if applicable)	Factor
	Expert	Specially experienced garage personnel (e.g., <20%); Knows also some more sophisticated, but established attacks (e.g., installing pirate smartcards)	6
	Multiple expert	Highly experienced (garage) personnel (e.g., <1%); Knows also very recent state-of-the-art (academic) attacks (e.g., side-channels, cryptanalysis, zero-day exploit)	8
Knowledge of the target	Public information	Everything that can be found in book stores or in the Internet; Information shared without non-disclosure agreements; "secret" shortcuts (e.g., hot key)	0
	Restricted information	Information shared between different organizations (e.g., OEM and supplier) only under non-disclosure agreements (e.g., source code, internal documentation)	3
	Sensitive information	Information shared only under non-disclosure agreements only within an organization, i.e., exclusive to OEM or to a supplier (e.g., key parameters)	7
	Critical information	Information (traceable) exclusively accessible to only a few persons within an organization (e.g., secret root signing key)	11
Access	Unnecessary or unlimited	Logical or remote access without physical presence, for instance, wireless or via Internet (e.g., V2X or cellular interface, critical vehicle IT backend vulnerability)	0
	Easy	Physical access to interior or exterior but without using any special tools (e.g., opening the hood to access wires, simple removing some car interior lining)	1
	Moderate	Complex disassembly of vehicle parts to access deep internals (e.g., ECU flash memory access) but without breaking sophisticated tamper-protection boundaries (e.g., more than special screws and similar "unsophisticated" measures)	4
	Difficult	Disassembly on microelectronic level (e.g., micro probing/cutting, chemistry) including breaking some sophisticated tamper-protection boundaries	10
Equipment	Standard	Readily available, e.g., common IT device such as notebooks up to simple OBD diagnosis devices; everything a common amateur mechanic could have at home	0
	Specialized	Professional garage equipment, but still (somehow) freely available, e.g., in-vehicle communication devices (e.g., CAN cards) up to costly garage diagnosis equipment	4
	Bespoke	At least one equipment item not freely available such	7

Category	[CEM, B.4.2.3] Reference	More detailed automotive domain related reference (if applicable)	Factor
		as manufacturer-restricted special equipment or equipment with costs > 50,000€ (e.g., electron microscope)	
	Multiple bespoke	More than one bespoke equipment item	9

Table 2: Reference classification for the attack potential factors

The overall attack potential AP is then calculated by estimating and adding the factor for each category as shown in equation (3.1).

$$AP = AP_{time} + AP_{expertise} + AP_{knowledge} + AP_{access} + AP_{equipment} \quad (3.1)$$

Thus, AP represents the accumulated attack potential that merges all resources required for successfully mounting a certain attack path. The total AP value can now be translated into an attacker classification as shown in Table 3. The classification puts AP into the categories as defined by the Common Criteria [CEM, B.4].

AP	Total attack potential classification
0 – 9	Basic
10 – 13	Enhanced Basic
14 – 19	Moderate
20 – 24	High
> 24	Beyond high

Table 3: Attack potential (AP) classification

3.3 Damage Potential Calculation

Our calculation of the damage potential is based on three damage types a successful attack against a certain vehicular security objective can yield to, namely safety damage, financial damage, and/or operational damage (cf. Table 4).

Safety damages include any unfavorable incident that might cause injuries to vehicle passengers as result of a successful security attack. For the safety damage classification, we use the industry-proven ASIL classification from [ISO26262] (cf. Section 2.3). For the quantitative classification of the corresponding factors, we also transferred the (A)SIL decimal power scaling. However, note that the proposed safety damage factors solely represent arithmetical values without any ethical rating (e.g., in comparison with the financial damage factors).

Financial damages include the global sum of all losses as result of a successful security attack that do not directly reflect a safety issue. Therefore, financial damages include all *direct financial losses*, for instance, all financial losses from broken business models (e.g., broken after-sales feature activation), legal implications (e.g., penalties), product liability issues (e.g., penalties or callbacks), counterfeiting, but also estimations for all *indirect financial losses*, for instance, regarding business reputation damages or loss of

market shares. However, since the meaning of some concrete sums of money, can be very different for every company, the given financial damage classifications are related to the general financial damage classifications from the "IT-Grundschutz" [BSI-100-4] issued by the German Information Security Agency. To account the – in contrast to most safety damages – again comparatively smaller consequences properly, we shifted the corresponding factors in proportion to the safety damage classes downwards by one magnitude (while keeping the decimal power scaling).

Operational damages in turn, include all other unfavorable incidents, which do not directly cause any injuries and do not have any meaningful measurable financial dimension. This includes, for instance, damages to the vehicle functionality (e.g., breakdown of the air-condition system) up to potential damages to vehicular infrastructures (e.g., traffic management systems). The classification is again based on a shortened, but industry-proven estimation as used in vehicular defect severity categorization already such as FMEA (Failure Mode and Effects Analysis) [AIA08]. To account the – in contrast to the safety damages and the chosen financial categories – comparatively smaller consequences, we shifted the corresponding factors again downwards by one magnitude (while keeping the decimal power scaling).

Damage category	**Damage reference**	**Factor**
Safety severity classes	Life-threatening injuries (survival uncertain), fatal injuries	10,000
	Severe and life-threatening injuries (survival probable)	1,000
	Light and moderate injuries	100
	No injuries	0
Finance severity classes (global sum)	Existence-threatening financial damage (e.g., monetary damage is >30% of annual sales)	1,000
	Substantial financial damage, but yet not existence-threatening (e.g., monetary damage is 20% – 30% of annual sales)	100
	Undesirable financial damage (e.g., monetary damage is 5% – 20% of annual sales)	10
	No or tolerable financial damage (e.g., monetary damage is <5% of annual sales)	0
Operational functionality severity classes	Vehicles unusable, i.e., one or more fundamental functions are affected. The vehicle usage is infeasible. This can be compared with FMEA severity rating above 8.	100
	Service required, i.e., an important function is affected. The vehicle can be used only with massive restrictions. This can be compared with FMEA severity rating 6 to 8.	10
	Comfort affected, i.e., a function is affected. The vehicle can be used with some restrictions. This can be compared with FMEA severity rating 2 to 5.	1
	No relevant effects, i.e., at most, an unimportant function is affected and the vehicle can be used without restrictions. This can be compared with FMEA severity rating 1.	0

Table 4: Reference classification for the damage potential factors

The total damage potential DP can then be calculated by estimating and adding the values of the three individual factors (cf. Section 4 on estimation methodology) as shown in equation (3.2). Similar to the attack potential calculations, all estimations have to consider the worst-case scenario. In case, the damage reference estimation is in-between two categorizations, it is also possible to take an appropriate intermediate value for the corresponding damage factor.

$$DP = DP_{safety} + DP_{financial} + DP_{operational} \quad (3.2)$$

Thus, DP represents the accumulated damage potential that merges all potential financial and non-financial consequences caused by a successful security attack against a certain security objective, regardless of the occurrence likelihood / difficulty for such an attack. The underlying decimal power weighting of the evaluation intervals of the three damage categories (i.e., safety, financial, and operational) is shown in Figure 3.

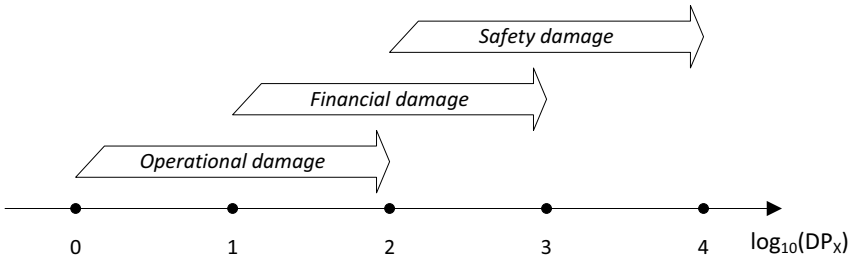

Figure 3: Damage interval relations

Note that a successfully violated security objective through a successfully accomplished security attack often may yield to different autonomous consequences regarding safety, finance, or vehicle operation in parallel. However to ease application, we suggest to consider from all potential consequences only the worst consequence for each category, which includes all other "lower damages". For example, a successful security attack, which violates a security objective that "only authorized personnel may modify the ECU firmware" and hence enables unauthorized modifications, may have three individual, autonomous consequences. It could yield to two independent safety damages (e.g., due to two potential ECU malfunctions) but it could also yield to a certain financial damage independent from the two safety damages (e.g., due to an unauthorized feature activation). For calculating the corresponding damage factor, we would first look for the consequence with the worst-case safety damage and would take only this consequence for determining DP_{safety}. We would then look for the consequence with the worst-case financial damage and would take this consequence for determining $DP_{financial}$. Similarly, we would look for the worst-case operational damage consequence and would take this consequence for determining $DP_{operational}$. The sum of all worst-case factors would then determine the total DP caused by the corresponding security objective violation.

Finally, the total DP value can be translated into damage categories as shown in Table 5. These classifications use the well-established decimal power scaling (cf. Table 1),

realized in such a way that severe injuries and very high financial damages result in a classification of catastrophic.

DP	Total damage potential classification
0 – 2	Insignificant
3 – 21	Medium
22 – 210	Critical
> 210	Catastrophic

Table 5: Damage potential (DP) classification

3.4 Risk Assessment

To conclude our risk analysis, we finally create a so-called *risk matrix*, which combines the probability of a successful security attack path (attack potential AP) and the expected losses of that incident (damage potential DP) to a meaningful risk classification.

Unfortunately, both, [IEC61508] as well as its automotive derivation [ISO26262] (currently) do not provide any obligatory risk assessment method or risk acceptance values. This has mainly political reasons, since every industry (or even each manufacturer) that applies the generic [IEC61508] standard would have its own individual definitions of acceptable and non-acceptable risks. However, we found that the risk matrix and the corresponding risks assessments according to [EN50126] – originating from the railway safety engineering – satisfactorily fits our needs. Hence, Table 6 serves as at least as a basis for an individually adaptable automotive IT security risk acceptance matrix. A further, however general security risk taxonomy from the research perspective can be found in [Fi05].

AP↓	Probability reference	Risk assessment			
Basic	Certain	Undesirable	Inacceptable	Inacceptable	Inacceptable
Enhanced Basic	Likely	Tolerable	Undesirable	Inacceptable	Inacceptable
Moderate	Possibly	Tolerable	Undesirable	Inacceptable	Inacceptable
High	Unlikely	Negligible	Tolerable	Undesirable	Inacceptable
Beyond High	Rare	Negligible	Negligible	Tolerable	Inacceptable
	Practically infeasible	Negligible	Negligible	Negligible	Undesirable
DP →		Insignificant	Medium	Critical	Catastrophic

Table 6: Exemplary automotive IT security risk matrix

3.5 Application Example

We now illustrate our approach by giving a brief example. We consider a customer modifying a safety-critical ECU firmware for an unauthorized performance manipulation of his car's engine (i.e., "*chip tuning*"). This attack aims at violating the security objective that the integrity of the ECU firmware shall be protected. In our example,

uploading custom code to the ECU is a protected capability, which means, only authentic original and – for IP protection reasons – encrypted code will be accepted by the ECU. We assume that the protection mechanism is not enforced by a security chip, but solely through software security measures. Thus, the attacker is able to reverse-engineer the firmware and/or gets to know non-public information in order to do the custom code software update. This attack path could result in the following attack potential rating according to method described in Section 3.2.

The time elapsed to collect necessary knowledge, to obtain necessary equipment, and to actually execute the attack probably will be between *days* and *weeks* (Factor 2). Note that it is perfectly alright two choose intermediate factors for an estimation of an AP category, such as factor 2 for a rating which is between the two references "days" and "weeks". The expertise required to identify and carry out such an attack for the first time would be *expert* (Factor 6). The necessary knowledge of the target will be rated *restricted* (Factor 3), since at least basic knowledge of the internal software structure and functionality will be required to succeed between days and weeks. As the attacker usually is also the legitimate owner of the vehicle, he has full access to his car all the time such that the window of opportunity is practically unlimited. However, the attacker has to communicate somehow with the ECU, which requires at least *easy* physical access (Factor 1). Finally, standard equipment plus some additional software/cables may be required to carry out the attack. However, those specialized parts can be easily obtained via the Internet so that the necessary equipment is rated to between *standard* and *specialized* (Factor 3). The calculation of the total AP is summarized in Table 7 and results in a required AP of *moderate*. However, once an attack can be automated and the required code (a so-called "exploit") is published on the Internet, its rating usually decreases significantly and results in a new attack path.

We now analyze the damage potential if the corresponding security objective has been violated by this attack path. If some safety-critical code has been modified in an unauthorized way, its execution may lead – from the worst-case safety perspective – to severe accidents even with injuries (Factor 100). From the worst-case financial perspective, which are not safety-related, (undetected) custom software installations may lead to spurious warranty claims or false liability issues yielding to a financial damage is rated to be at most 5% to 20% of the related annual sales (Factor 10). Finally, an unauthorized modified software code may also – independently from any safety or financial consequences – lead to some impacts or failures of certain vehicular functionality, since it has not been verified by the manufacturer (Factor 5). As can be seen in Table 7 the overall damage potential is calculated and categorized as *critical*.

For the final IT security risk assessment of this attack path, we apply our vehicular IT security risk matrix as defined in Table 6 that rates this attack path as an *undesirable* security risk (i.e., 1/*moderate* x *critical*). Implementing better security measures into the ECU such as a hardware-based integrity protection mechanism [SSW08] as opposed to a software-only mechanism may significantly increase the attack potential required and thereby decrease the overall risk for instance to a *tolerable* level.

Please note that there may be several reasonable calculations of the attack potential because the prerequisites for the attack may differ. As an example, there usually is a trade-off between expertise and time that means an attacker needs either much expertise

or much time. In these cases, it is safe to choose the lowest total AP factor from the set of attack scenarios. Moreover, some attacks cannot be countered directly by the IT component for which the risk analysis is being done (e.g., security during development). These attacks may be non-technical, such as social engineering, or target technical systems that are out-of-scope for the manufacturer of the IT component. A formal way of incorporating these attacks into the risk analysis is to define assumptions under which the risk analysis holds, for instance, to assume the development site is secure.

AP/DP category	**Reference**	**Factor**
Elapsed time	*Between days and weeks*	2
Specialist expertise	*Expert*	6
Target knowledge	*Restricted information*	3
Access	*Unlimited*	1
Equipment	*Standard/specialized*	3
Total AP	*Moderate*	15
Safety severity	*In worst case up to light and moderate injuries*	100
Finance severity	*Undesirable, i.e., at most 5% – 20% of related annual sales*	10
Operational severity	*Vehicle operable, but increased chance for inherent failures*	5
Total DP	*Critical*	115
Sec. Risk = 1/AP x DP	***1/moderate*(15) x *critical* (115) = *Undesirable***	

Table 7: Exemplary calculation of attack potential, damage potential, and resulting security risk

4 Getting Relevant Data

An important question is how to get all the relevant data in order to (i) identify possible attacks and potentially resulting damages and (ii) to classify damage factors and attack factors accordingly. For the identification of potential security objectives and possible attack paths, we suggest the use of security questionnaires (cf. Section 4.1). For the identification and classification of attacks, we apply the approach as described in Section 4.2. Lastly, for the estimation of potential damages according to Section 3.3, we suggest the use of more detailed security questionnaires that include also analyses of former similar security incidents.

4.1 Security Questionnaire

In the following, we provide a draft proposal for a security questionnaire in order to collect the information necessary to conclude a meaningful security risk analysis. This includes a basic understanding of application usage (1), the identification of potential security objectives (2), collection of potential attacks and misuse cases known (3), and identification of already existing security measures (4). This approach is similar to the Common Criteria model of defining a "Security Target" describing the evaluation target, its security environment, its security objectives, and its functional security requirements.

(1) Please give a short description of your vehicular IT application including all involved entities (e.g., driver, OEM, service, third parties) and all (security) relevant use cases!

Main components, available interfaces, general functionalities, entities, security environment, and corresponding use cases
(2) Please provide data, resources, or functionality where certain entities may have certain security objectives!
Entity requirements on data regarding confidentiality, integrity, authenticity, availability, freshness, or access control. Entity requirements on functionality and resources regarding correctness, availability, access control, or quality-of-service control
(3) Please describe shortly any attacks, misuse cases and attack intentions you know for this vehicular IT application!
Attack goal, misuse case, attack path, attacker model, attack tree
(4) Please describe shortly any security measures that possibly already exist to enforce a security objective from (2)!
(a) Security objective 1: Security protection measure 1, Security protection measure 2 (b) Security objective 2: Security protection measure 1 (c) …
(5) Please provide estimations about the preliminaries and costs for each attack identified in (4)!
Reference to: Table 3: Attack potential (AP) classification
(6) Please provide estimations about the potential damages for each attack identified in (4)!
Reference to: Table 5: Damage potential (DP) classification

Table 8: Exemplary IT security questionnaire for risk analyses

For a fine-grained estimation of attack and damage potentials, the security questionnaire should use the categories provided by our estimation method as proposed in Section 3.2 and Section 3.3, respectively. In case of a new security-relevant application, the damage categories can be estimated only on approximations of the corresponding experts. In case the security-relevant application is already target of security attacks, the estimations would be much more precise as they can include the severity and frequency of already existing incidents. Thus, we recommend that the responsible developer completes this questionnaire together with a security expert and with experts capable to estimate the safety, financial, and operational consequences caused by a security breach of the analyzed vehicular application.

4.2 Identification and classification of attacks

The Common Criteria require the evaluator to examine public sources as well as evaluation evidence (i.e. internal documentation) to identify potential vulnerabilities and to assess the possibility of their exploitation. If a potential vulnerability is exploitable in the intended operational environment of the evaluation target, and the attack potential required for a successful identification and exploitation is beyond the level the evaluation target claims to resist, a security solution has to be implemented. The assessment of the attack factors are done in accordance with the CC and the knowledge and experience of the evaluator. Thus, once an IT product has been CC-certified, reliable statements about the resistant to attacks on its security objectives can be made. The identification and classification of possible attacks, which has to be done in context of our risk analysis methodology, can be based on CC certification results. Furthermore, a CC certification of a security-critical vehicular system gives internationally accepted

assurance that the manufacturer has put serious efforts on averting damages resulting from an attack on the system.

4.3 Implementation

We have implemented our approach as a simple spreadsheet application that allows a systematic acquisition of security targets, their possible attack paths, and their individual damage consequences. It enables estimations of attack and damages potentials according to our proposed approach, and provides an automatic risk assessment according to our adapted [EN50126] security risk matrix.

In doing so, our approach has already been successfully applied in several security analysis and consulting projects for several well-known automotive OEMs.

5 Summary and Outlook

In this paper, we presented a methodical approach to balance the security costs for implementing vehicular security measures against the security risks of corresponding automotive security attacks. This approach is based on well-established methodologies, which have been carefully adapted and combined for efficient, meaningful application in vehicular IT security scenarios. By integrating the special characteristics of the automotive domain, the proposed approach, provides automotive developers and manufacturers with a quantified assessment methodology for vehicular IT security measures where the trade-off between costs and security risks can be clearly analyzed to enable well-founded decisions. Our approach is based on the assumption that the probability of a successful attack on a security measure is decreasing with the increase of the attack potential required (see Table 6). This is only true for most but not all real-world scenarios. As an example, imagine a car manufacturer that – no matter the cost – is willing to reverse-engineer the software of a brand-new competitors' product. How to get rid of this assumption by extending our taxonomy will be subject of further research. Having more fine-grained factors or a better weighting of the individual factors and categories, would be another subject of further research. Especially, first practical results from our proposed security questionnaires could provide valuable input for verifying or adjusting our scales to current automotive industry real world scenarios. As mentioned in Section 3.1, an automotive-specific Protection Profile (PP) covering all important, known ECU security issues (independently from potential security solutions) evaluation, would clearly ease and systematize the identification of vehicular security objectives, threats, and attack paths. Another interesting question is how our results relate to the discussions of [GL02] and [Wi06] who try to determine the optimal level of investments in information security. According to their work and given requirements, 36.8% to 50% of total cost of protected assets should be invested in security measures. Does our approach yield similar results? In our special context of vehicle mass production, the total investment costs are significantly influenced by the cost per production unit. To (amongst others) get answers on this question, our approach for vehicular IT risk analysis is currently (independently) applied and evaluated for two individual security solutions of two German car manufacturers. Finally, we would like to stress that – even if based on well-found analyses – a risk analysis remains a statistical estimation that inherently includes uncertainties.

References

[AAA05] American Association for Automotive Medicine (AAAM), „The Abbreviated Injury Scale (AIS)", 2005.

[ABD06] Amer Aijaz, Bernd Bochow, Florian Dötzer, Andreas Festag, Matthias Gerlach, Rainer Kroh and Tim Leinmüller, "Attacks on Inter-Vehicle Communication Systems – An Analysis", In *3rd International Workshop on Intelligent Transportation (WIT 2006)*, March 2006.

[AIA08] Automotive Industry Action Group (AIAG), "Potential Failure Mode and Effects Analysis (FMEA)", 2008.

[An03] Ross Anderson, "Electronic Safety and Security – New Challenges for the Car Industry. In *1st Workshop on Embedded Security in Cars (escar)*, Bochum, Germany, November 2003.

[Br04] Manfred Broy, "Sichere Software im Automobil – Potenziale, Herausforderungen, Trends", In *2nd Workshop on Embedded Security in Cars (escar)*, Bochum, Germany, November 2004.

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

[CC07] Common Criteria for Information Technology Security Evaluation, continually maintained as ISO 15408.
"Part 1: Introduction and general model", V.3.1, Revision 1, September 2006,
"Part 2: Security functional components", V.3.1, Revision 2, September 2007,
"Part 3: Security assurance components", V.3.1, Revision 2, September 2007.

[CCRA] Common Criteria Recognition Agreement, www.commoncriteriaportal.org/theccra.html, 2006.

[CEM] Common Methodology for Information Technology Security Evaluation, V.3.1, Revision 2, September 2007, Continually maintained as ISO 18045.

[EN50126] EN 50126, "Railway applications – The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)", 1999.

[Fi05] Donald G. Firesmith, "A Taxonomy of Security-Related Requirements", 2005.

[GL02] Lawrence A. Gordon and Martin P. Loeb, "The economics of information security investment". In *ACM Transactions on Information and System Security*, November 2002.

[IEC61508] IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems", 2005.

[ISO26262] ISO 26262, "Road vehicles – Functional safety", November 2011.

[MSR04] Stephan Merk, Kathrin Scheidemann, Michael Rudorfer, Thomas Stauner, Johannes Grünbauer, Gerhard Popp, Guido Wimmel, "Security for Downloadable Automotive Services", In In *2nd Workshop on Embedded Security in Cars (escar)*, Bochum, November 2004.

[SSW08] Michael Scheibel, Christian Stüble, Marko Wolf, "An Interoperable Security Architecture for Vehicular Software Protection", In International Workshop on Interoperable Vehicles (IOV 2008), ETH Zürich, Switzerland, March 2008.

[Sc99] Bruce Schneier, "Attack trees – Modelling security threats", In Dr. Dobb's journal, http://www.schneier.com/paper-attacktrees-ddj-ft.html, December 1999.

[TVRA] ETSI TS 102 165-1, "Method and proforma for Threat Vulnerability and Risk Analysis (TVRA)", December 2006.

[VDI2182] VDI/VDE 2182, "IT-security for industrial automation - General model", August 2007.

[Wi06] Jan Willemson, "On the Gordon&Loeb Model for Information Security Investment", In *5th Workshop on the Economics of Information Security (WEIS 2006)*, June 2006.

[Wo09] Marko Wolf, "Security Engineering for Vehicular IT Systems — Improving Trustworthiness and Dependability of Automotive IT Applications", Dissertation, Vieweg+Teubner-Verlag, 2009.