Security requirements for automotive on-board networks

Olaf Henniger*, Ludovic Apvrille†, Andreas Fuchs*, Yves Roudier§, Alastair Ruddle¶, and Benjamin Weyl‖
*Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany
†Institut Telecom, Telecom ParisTech, CNRS LTCI, Sophia Antipolis, France
§EURECOM, Sophia Antipolis, France
¶MIRA, Nuneaton, Warwickshire, England
‖BMW Group Research and Technology, München, Germany

***Abstract*—This paper considers security requirements for automotive on-board networks and describes the processes used for identifying and prioritizing such requirements. The security engineering process starts from use cases for automotive on-board networks that require wireless communication interfaces and involves an investigation of security threat scenarios and the assessment of the relative risks associated with the threats.**

***Index Terms*—Security risk management; in-vehicle communications**

I. Motivation and outline

Future automotive safety applications based on vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication (jointly referred to as V2X communication) are regarded as a means for decreasing the number of fatal traffic accidents. While these functionalities herald a new era of traffic safety, new security requirements need to be considered in order to prevent attacks on these systems.

Modern cars are equipped with up to 70 embedded ECUs (electronic control units) and electronic sensors and actuators for a diversity of functions. These components are connected via various communication buses, forming a complex distributed system. So far, there has been little incentive and opportunity for tampering with automotive on-board networks. This will change with the advent of new wireless communication interfaces. The on-board electronics will be threatened by attacks originating both outside and inside the vehicle, resulting for instance in illegitimate message injection.

Trust anchors and secure storage of secret keys and secure, trustworthy communication within individual vehicles is the basis for the secure deployment of electronic safety aids based on V2X communication. Therefore, security-relevant components of automotive on-board networks need to be protected against tampering and sensitive data need to be protected against compromise [1]. A careful analysis of the security requirements is important in order to devise security measures that are both effective and cost-effective.

This paper outlines the security requirements analysis process that we have applied to automotive on-board networks with V2X communication interfaces [2] within the European research project EVITA, which deals with on-board network protection. Section II characterizes the systems under investigation. The security requirements analysis process involves the following steps [3]:

- Identification of threats (Section III);
- Identification of security requirements to counter the threats (Section IV);
- Assessment of the risks associated with the threats and prioritization of the security requirements based on the risks addressed (Section VI).

Section V outlines the security requirements derived by applying these processes to example use cases, and Section VII gives an outlook on further work.

Contact: Olaf Henniger, Fraunhofer Institute SIT, Rheinstr. 75, 64295 Darmstadt, Germany; olaf.henniger@sit.fraunhofer.de

II. System under investigation

A. Network architecture

The system under investigation is an automotive on-board IT system consisting of embedded ECUs, sensors, and actuators that are connected with each other through several busses. Fig. 1 shows the assumed architecture based on [4].

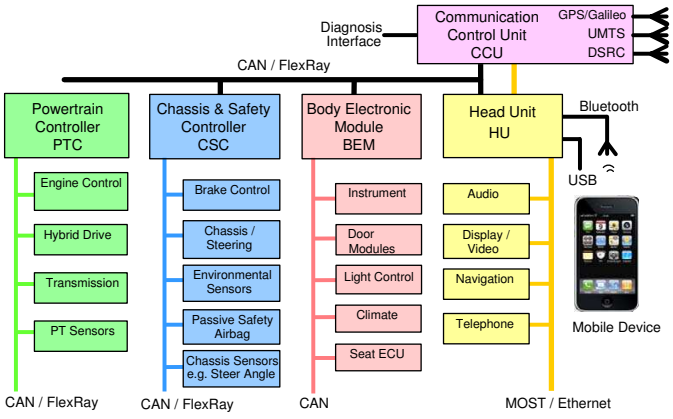

Fig. 1. Assumed automotive on-board network architecture

The communication control unit (CCU) and the head unit (HU) possess accessible interfaces to the outside. There are

- wireless interfaces such as GPS, UMTS and DSRC,
- wire-bound diagnostic interfaces, and
- interfaces such as Bluetooth for connecting with mobile devices.

Most vehicular on-board IT systems operate in an uncontrolled environment where they are exposed to a variety of threats, against which their assets must be protected.

B. Assets

The main components of an automotive on-board network that may become targets of attacks are

- on-board electronic components such as ECUs, sensors, and actuators,
- the communication links between these components and within ECUs, and
- the software running on the ECUs.

C. Use cases

Use cases describe a system's behavior as it responds to various stimuli from the outside. We consider use cases of the following categories, covering a range of future vehicle functions with possible security implications [5]:

- V2V communication,
- V2I communication,
- Use of nomadic devices, USB sticks, or MP3 devices,
- Aftermarket, and
- Workshop/diagnosis.

The following possible future use cases of V2V communication serve as examples:

- Sending messages that lead to safety reactions: If a vehicle has to slow down suddenly, e.g. at the tail end of a traffic jam, then it should broadcast an emergency notification message including position data in order to warn other vehicles.
- Safety reaction – active braking: If a vehicle receives an emergency notification message, then it should first check the plausibility of the danger by comparing the received information with information from its own global positioning system (GPS or other) receiver and from own radar, lidar or video sensors. Then, if a dangerous situation is recognized and braking deemed the best solution, the vehicle should notify and support the driver to initiate an instant brake manoeuvre and itself broadcast an emergency notification message.

Such systems are intended to provide some preliminary braking ahead of the driver's response. Obviously, an active braking should not happen without a real danger, and the vehicle must always stay controllable by the driver.

III. Threats

The first step is to find a comprehensive list of threats, the source of which is largely general experience. Possible motivations for attacks on automotive on-board networks are

- to gain advantages (e.g. by identity theft, information theft, fraudulent commercial transactions, enhancing traffic privileges, avoiding liability for accidents) or
- just to harm others (e.g. drivers, passengers).

Possible attacks range from jamming the wireless communication over replaying wireless messages to "chip tuning". Threats by attacks that require direct physical manipulations of the hardware of other vehicles are excluded here as they do not depend on new communication interfaces. They are already now feasible and will probably always be. However, manipulations of the own hardware of the attacker are within scope since attackers may modify their own vehicles to use them as a means of attack.

We use attack trees [6] for structuring. The root of an attack tree represents the goal of an attack. Child nodes represent subgoals that could satisfy the parent attack goal. Child nodes may have children themselves. The tree is truncated where the efforts required for a successful attack can be estimated. If a node is labeled with a logical AND operator, then all its child nodes need to be achieved to achieve the superior attack goal. Otherwise, an attack goal can be achieved by achieving any one of its subgoals (logical OR relation). Fig. 2 shows part of the attack tree for "unauthorized active braking".

IV. Identification of security requirements

A. Overview

Based on models derived from the use cases, we systematically identify security requirements using different approaches:

- Abstract functional path approach: based on a purely functional representation of the use cases, providing authenticity and confidentiality requirements,
- Detailed functional path and mapping approach: based on mapping a functional representation of the use cases to an architecture, providing both functional and architectural (availability, timing) requirements.

Merging the results of these approaches should ensure that the security requirements are sufficiently comprehensive to support subsequent design activities.

B. Abstract functional path approach

As a basis for the security requirements analysis, a compact functional model is derived from the use case descriptions. As use case descriptions do not identify internal system details, the functional model describes only actions happening at the system borders and interactions with other systems. Each information flow from inputs to outputs of the overall system is associated with requirements for

- authenticity of incoming data and their origins and
- an appropriate level of confidentiality for outgoing data.

The abstract functional path approach [7] provides a compact description of V2X communication-related security requirements. Based on these, security measures for the on-board system can be designed.

C. Detailed functional path and mapping approach

The detailed functional path and mapping approach allows aspects such as availability and timing, and dependencies between requirements, to be considered at an early stage. The following steps are used:

1) From use cases, a functional view of the system is derived, i.e. various functions, inputs/outputs (sensors,

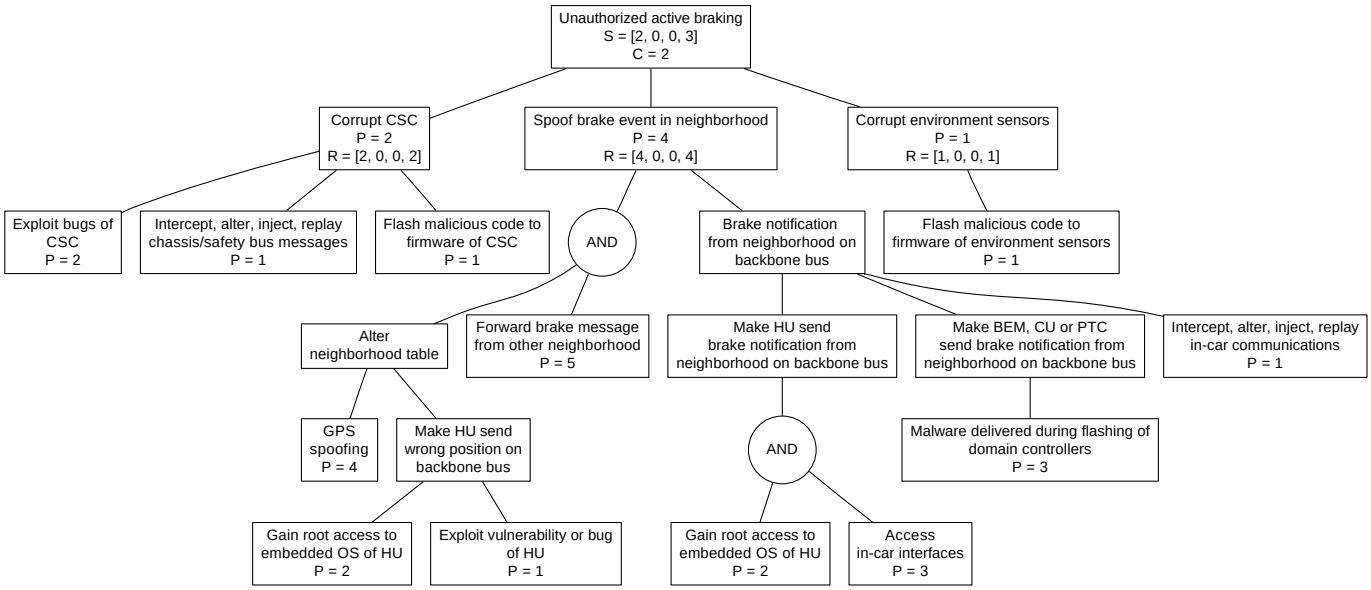

Fig. 2. Attack tree for unauthorized active braking

actuators, I/O operations), as well as data and event flows between functions are identified.

2) A candidate hardware architecture is proposed, built upon abstract parameterized hardware nodes (e.g. CPUs, buses, memories, etc.).
3) Functions and their communication links are mapped onto the candidate architecture. Functions are mapped onto hardware devices (ECUs, sensors, or actuators), with assumptions on where code is stored.
4) Security requirements are listed so as to provide a full coverage of attack tree nodes. They are found considering the use case descriptions, functional and mapping views as well as attack trees.

The approach can be applied using TTool [8], an open-source UML toolkit supporting several UML profiles.

V. Resulting security requirements

A. Overview

At the highest level, the security objectives are:

- to ensure the functional safety of the vehicle occupants and other road users;
- to protect the privacy of vehicle drivers, and the intellectual property of vehicle manufacturers and their suppliers;
- to maintain the intended operational performance of all vehicle and ITS functions;
- to prevent fraudulent commercial transactions and theft of vehicles.

The following subsections outline some of the security requirements needed to satisfy the security objectives, focussing on the example use cases described in Section II-C. Other requirements considered include non-repudiation, availability, and freshness requirements.

The security requirements are determined using the approaches outlined in Section IV. The security requirements are based on the use cases and attack trees. Their level of detail depends on the level of detail of the underlying use case descriptions.

Security requirements are constraints arising from security concerns. We do not specify here how to satisfy the constraints, but only what they are. Designing possible secure measures is subject of forthcoming work.

B. Authenticity

1) Certain information originating within a vehicle (such as the vehicle's environment sensor information, vehicle-dynamics sensor information, or position information) shall be authentic in terms of origin, content and time if the vehicle performs actions based on that information (such as active braking).
2) Certain information that a vehicle receives from other vehicles (such as other vehicles' position information, vehicle-dynamics sensor information, or position information) shall be authentic in terms of origin, content and time if the vehicle performs actions based on that information (such as active braking).

C. Anonymity

1) The identity of the vehicle shall be confidential in wireless communication.[1]

VI. Risk assessment and prioritization

A. Introduction

In order to identify the most relevant security requirements, we need to assess the level of risk posed by potential attacks and to prioritize the identified security requirements based on the results of the risk assessment.

[1]Anonymity may later be weakened to pseudonymity in order to accommodate competing requirements.

The risk of an attack is seen as a function of the possible severity (i.e. the gain and loss) of the attack for the stakeholders and the estimated probability of occurrence of a successful attack. In case of threats to safety, the risk assessment also includes an additional controllability parameter.

It is hard to exactly quantify all factors influencing the risk of an attack. However, the relative severity, success probability, and controllability of attacks can be assessed, allowing a ranking of attacks based on their relative risk.

B. Severity

The severity of an attack is considered in terms of four aspects that may be associated with harm to the stakeholders:

- Safety of the vehicle occupants and other road users;
- Privacy of vehicle drivers and the intellectual property of vehicle manufacturers and their suppliers;
- Financial losses that may be experienced by individuals or ITS operators;
- Interference with operational performance of vehicle and ITS (intelligent transport system) functions.

Based on the severity classification used in vehicle safety engineering [9], a range of qualitative severity levels is defined in Table I.

The severity of the outcome is estimated for attacks with high-level attack goals. For instance, the root node in Fig. 2 is labeled with the following severity estimate: $S = [2, 0, 0, 3]$. There may be significant safety implications ($S_S = 2$). No financial or privacy aspects are associated with this attack. The operational impact for unauthorized active braking is $S_O = 3$ (significant impact for multiple vehicles).

C. Probability of success

To be on the safe side, we must assume that each attack that is possible and promises whatsoever small benefit will be carried out by someone. The probability that an attack, once launched, will succeed depends on the attack potential of the attacker and the attack potential that the system under investigation is able to withstand.

The attack potential is well defined in [10], [11]. Essentially, it corresponds to the minimum effort required to create and carry out an attack. The higher the attackers' motivation, the higher efforts they may be willing to exert. The following factors are considered during attack potential evaluation [11]:

- Time taken by an attacker to identify a vulnerability, to develop an attack method, and to mount the attack;
- Specialist expertise required;
- Knowledge of the system under investigation;
- Window of opportunity to access the target of attack;
- IT hardware/software or other equipment required to identify and exploit a vulnerability.

In many cases these factors are not independent, but may be substituted for each other in varying degrees. For instance, expertise or equipment may be a substitute for time. Table IV identifies the factors discussed above and, based on [10], [11], associates numeric values with each level. Intermediate values to those in the table can also be chosen.

TABLE II
RATING OF ASPECTS OF ATTACK POTENTIAL

Factor	Level	Value
Elapsed time	$\leq$ 1 day	0
	$\leq$ 1 week	1
	$\leq$ 1 month	4
	$\leq$ 3 months	10
	$\leq$ 6 months	17
	$>$ 6 months	19
	not practical	∞
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge of system	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Window of opportunity	Unnecessary/unlimited	0
	Easy	1
	Moderate	4
	Difficult	10
	None	∞
Equipment	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

To determine for each path in an attack tree the attack potential required to identify and exploit it, sum up the appropriate values from Table IV and apply Table III to classify the attack potential. Note that once an attack scenario has been identified and exploited, it may be exploited repeatedly with less effort than for the first time. Both phases, identification and exploitation, are considered in conjunction.

TABLE III
RATING OF ATTACK POTENTIAL AND ATTACK PROBABILITY

Values	Attack potential required to identify and exploit attack scenario	Attack probability
0–9	Basic	5
10–13	Enhanced-Basic	4
14–19	Moderate	3
20–24	High	2
$\geq$ 25	Beyond High	1

A high probability of successful attack is assumed to correspond to a low attack potential, since many possible attackers will have the necessary attack potential. Conversely, a high attack potential suggests a low probability of successful attacks, since the number of attackers with the necessary attack potential is expected to be comparatively small.

The probability of success is estimated for the leaf nodes of the attack trees. For instance, each leaf node in Fig. 2 is labeled with a probability estimate P based on the attack potential rating given in Table IV. The estimates are based on as-is automotive on-board networks, prior to the introduction of security measures.

For higher attack goals, the individual probabilities of their child nodes can be combined using the tree logic. If an attack goal can be achieved using any one of a number

TABLE I
SEVERITY CLASSIFICATION SCHEME FOR SECURITY THREATS

Security threat severity class	Aspects of security threats			
	Safety	**Privacy**	**Financial**	**Operational**
0	No injuries	No unauthorized access to data	No financial loss	No impact on operational performance
1	Light or moderate injuries	Anonymous data only (no specific driver of vehicle data)	Low-level loss ($\approx$ €10)	Impact not discernible to driver
2	Severe injuries (survival probable); light/moderate injuries for multiple vehicles	Identification of vehicle or driver; anonymous data for multiple vehicles	Moderate loss ($\approx$ €100); low losses for multiple vehicles	Driver aware of performance degradation; indiscernible impacts for multiple vehicles
3	Life threatening (survival uncertain) or fatal injuries; severe injuries for multiple vehicles	Driver or vehicle tracking; identification of driver or vehicle for multiple vehicles	Heavy loss ($\approx$ €1000); moderate losses for multiple vehicles	Significant impact on performance; noticeable impact for multiple vehicles
4	Life threatening or fatal injuries for multiple vehicles	Driver or vehicle tracking for multiple vehicles	Heavy losses for multiple vehicles	Significant impact for multiple vehicles

TABLE IV
EXAMPLES OF ATTACK POTENTIAL ESTIMATES

Attack	**Elapsed time**	**Expertise**	**Knowledge of system**	**Window of opportunity**	**Equipment**	**Required attack potential**	
						Sum	**Rating**
Forward brake message from other neighborhood	1	3	0	0	4	8	Basic
GPS spoofing	4	3	0	0	4	11	Enhanced-Basic
Access in-car interfaces	0	6	3	1	4	14	Moderate
Gain root access to embedded OS of HU	10	3	0	4	4	21	High
Flash malicious code to firmware of CSC or of environment sensors	17	6	7	4	7	41	Beyond High

of attacks (i.e. OR relationship), then the combined attack probability is taken to be the highest of the attack probabilities for the attack options. Where the attack method requires a conjunction of attacks (i.e. AND relationship), the combined attack probability is taken to be the lowest of the probabilities of success associated with the contributing attack steps. For instance, for the "Corrupt CSC" attack in Fig. 2 the combined probability of success is $P = 2$.

D. (Un-)controllability

For the safety component of the severity vector, the risk assessment includes an additional probability parameter that represents the potential for the driver to influence the severity of the outcome. In [9] this possibility is reflected in a qualitative measure referred to as "controllability" (see Table V).

TABLE V
CLASSIFICATION FOR CONTROLLABILITY OF SAFETY HAZARDS

Controllability	**Meaning**
1	Avoidance of an accident is normally possible with a normal human response.
2	Avoidance of an accident is difficult, but usually possible with a sensible human response.
3	Avoidance of an accident is very difficult, but under favorable circumstances some control can be maintained with an experienced human response.
4	Situation cannot be influenced by a human response.

The controllability of the outcome is estimated for those attacks with high-level attack goals for which also the severity is estimated. For instance, the root node in Fig. 2 is labeled with $C = 2$ (cf. Table V) as controllability estimate.

E. Risk

Table VI maps severity of outcome, probability of attack, and controllability of the situation to risk level. The risk level is considered to be the higher, the more likely the success of the attacker is, the more severe the outcome is judged to be, and/or the more uncontrollable by the driver the situation is. The risk class "7+" that is used in Table VI for controllability classes $C = 3$ and $C = 4$ denotes levels of risk that are unlikely to be considered acceptable, such as safety hazards with the highest severity classes and threat levels, coupled with very low levels of controllability. For non-safety related risks, however, the mapping for controllability class $C = 1$ of Table VI provides the relative risk level, ranging from 0 (lowest) to 6 (highest).

As the severity of an attack is expressed in the form of a 4-component vector, there is also a 4-component risk vector associated with the attack. The four components may have different ratings. For example, it is possible that an attack could have little or no impact on safety but still presents significant risks in terms of compromised driver privacy or loss of reputation for vehicle manufacturers.

The risk levels are associated with the possible attacks by assessing relative severity at the higher levels of the attack trees and working up relative probabilities from the leaf nodes. For instance, for the "Spoof brake event in neighborhood" attack in Fig. 2 the resulting risk vector is $R = [4, 0, 0, 4]$. The relative safety risk is $R_S = 4$; there are no financial or privacy risks; the relative operational risk is $R_O = 4$.

TABLE VI
SECURITY RISK LEVEL AS A FUNCTION OF ATTACK PROBABILITY P, THREAT SEVERITY CLASS S_i, AND CONTROLLABILITY C

Security risk level		$P=1$	$P=2$	$P=3$	$P=4$	$P=5$
$C=1$	$S_i=1$	0	0	1	2	3
	$S_i=2$	0	1	2	3	4
	$S_i=3$	1	2	3	4	5
	$S_i=4$	2	3	4	5	6
$C=2$	$S_S=1$	0	1	2	3	4
	$S_S=2$	1	2	3	4	5
	$S_S=3$	2	3	4	5	6
	$S_S=4$	3	4	5	6	7
$C=3$	$S_S=1$	1	2	3	4	5
	$S_S=2$	2	3	4	5	6
	$S_S=3$	3	4	5	6	7
	$S_S=4$	4	5	6	7	7+
$C=4$	$S_S=1$	2	3	4	5	6
	$S_S=2$	3	4	5	6	7
	$S_S=3$	4	5	6	7	7+
	$S_S=4$	5	6	7	7+	7+

F. Prioritization of security requirements

The results of the risk analysis are summarized in terms of the frequency of the risk levels found for each threat. This gives an indication of the relative importance of protecting against specific attacks: While a low maximum risk suggests a low priority, a high maximum risk suggests a higher priority for protection. A lower risk that appears in many attack trees, however, might be as important to tackle than a higher risk that appears only once.

Where a number of possible attack subgoals may lead to the same superior attack goal, the subgoal with the highest perceived probability of success is the priority for countermeasures to reduce the risk level for the attack goal. Preventing the attacks judged to have the highest probability of success reduces the risk level for the superior attack goal.

For instance, in case of our example active braking use cases, the probabilities of success of attacks via the wireless communication interfaces, such as GPS spoofing (sending valid but wrong position data) and replaying wireless brake messages, are very high. Therefore, the authenticity of position data and of wireless messages are regarded as the most important security requirements for the active braking use cases. Avoiding reliance on GPS signals alone as a source of position data and measures for detecting tampering with wireless transmissions would help to reduce the risks.

VII. SUMMARY AND OUTLOOK

The identified security requirements for automotive on-board networks form the basis for designing a toolkit of security measures (which may be software, hardware, and architectural) that can be selected for implementation in future automotive on-board systems [12].

The proposed security requirements analysis process may support the development of future automotive applications based on V2X communication. It can be used, in combination with the vehicle manufacturer's security policy, in order to decide whether to accept or transfer the identified security risks or to take measures to reduce or avoid specific risks.

The proposed approach may also be applied beyond the automotive industry in other application domains where embedded, complex communication systems need to be managed.

ACKNOWLEDGMENTS

This work has been part of the collaborative project "EVITA – E-safety vehicle intrusion protected applications" (http://evita-project.org), co-funded by the European Commission under the Seventh Framework Programme. The authors thank the other project participants from BMW Group Research and Technology, Continental Teves AG & Co. oHG, escrypt GmbH, EURECOM, the Fraunhofer Institutes for Secure Information Technology and for Systems and Innovation Research, Fujitsu Services AB, Infineon Technologies AG, Institut Telecom, Katholieke Universiteit Leuven, MIRA Ltd, Robert Bosch GmbH and Trialog for their continuous support.

REFERENCES

[1] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *International Conference on ITS Telecommunications (ITST)*, Sophia Antipolis, France, 2007, pp. 1–6.

[2] A. Ruddle, D. Ward, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gürgens, O. Henniger, R. Rieke, M. Ritscher, H. Broberg, L. Apvrille, R. Pacalet, and G. Pedroza, "Security requirements for automotive on-board networks based on dark-side scenarios," Deliverable D2.3 of EVITA, 2009.

[3] D. Firesmith, "Specifying reusable security requirements," *Journal of Object Technology (JOT)*, vol. 3, no. 1, pp. 61–75, 2004.

[4] M. Hiller, J. Böhm, X. Chen, K. Echtle, T. Eymann, A. Ferre, B. Hedenetz, E. Kelling, V. Lauer, M. Osella, T. Voss, and D. van Wageningen, "Electronic architecture and system engineering for integrated safety systems – General architecture framework," Deliverable D0.2.4 of EASIS, 2004.

[5] E. Kelling, M. Friedewald, T. Leimbach, M. Menzel, P. Saeger, H. Seudié, and B. Weyl, "Specification and evaluation of e-security relevant use cases," Deliverable D2.1 of EVITA, 2009.

[6] B. Schneier, *Secrets and lies – Digital security in a networked world*. New York: Wiley, 2000.

[7] A. Fuchs and R. Rieke, "Identification of authenticity requirements in systems of systems by functional security analysis," in *Workshop on Architecting Dependable Systems (WADS) at the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Estoril, Lisbon, Portugal, 2009.

[8] *TTool: The TURTLE Toolkit*, Institut Telecom, http://labsoc.comelec.enst.fr/turtle/ttool.html.

[9] "Road vehicles – Functional safety," Committee Draft ISO 26262, 2008.

[10] "Information technology – Security techniques – Evaluation criteria for IT security," International Standard ISO/IEC 15408.

[11] "Information technology – Security techniques – Methodology for IT security evaluation," International Standard ISO/IEC 18045.

[12] O. Henniger, A. Ruddle, H. Seudié, B. Weyl, M. Wolf, and T. Wollinger, "Securing vehicular on-board IT systems: The EVITA project," in *25th VDI/VW Automotive Security Conference*, Ingolstadt, Germany, 2009.