

# VEHICLE ECU CLASSIFICATION BASED ON SAFETY-SECURITY CHARACTERISTICS

Dennis K. Nilsson, Phu H. Phung, and Ulf E. Larson

Department of Computer Science and Engineering  
Chalmers University of Technology  
SE-412 96 Gothenburg, Sweden  
{dennis.nilsson,phu.phung,ulf.larson}@chalmers.se

**Keywords:** In-vehicle networks, ECU classification, safety, security, attacks

## Abstract

An upcoming trend for automotive manufacturers is to perform remote diagnostics and firmware updates over the air, which allows identifying hardware problems and correction of software flaws with minimal customer inconvenience. These procedures require that the previously isolated in-vehicle network permits external communication, which introduces a number of security risks, e.g., cyber attack threats. In this paper, we identify cyber attack threats and classify the electronic control units (ECUs) in the in-vehicle network to assist in determining which ones to protect and restrict access to. We divide the ECUs into five categories: powertrain, vehicle safety, comfort, infotainment, and telematics. We then use four safety integrity levels to classify the ECU categories. Moreover, we define safety effect levels of security threats which are used to classify identified attacks in the remote diagnostics and firmware updates over the air procedures. The safety and security levels are combined to classify the ECU categories. From the results we conclude that ECU categories such as powertrain and vehicle safety require further protection prior to introducing remote connectivity. As a conclusion, we suggest that automotive manufacturers should emphasize security or restrict the remote diagnostics and firmware updates over the air procedures to certain ECUs.

## 1 Introduction

A vehicle is accelerating when the airbag suddenly triggers. The driver loses control of the vehicle, resulting in a crash that seriously injures the driver. Possible explanations to this event have historically been hardware faults and software malfunction; however, in the near future this event could be the result of a *cyber attack*, deliberately seeking to affect the operation of the vehicle and the safety of the driver.

Modern vehicles contain an in-vehicle network of embedded electronic control units (ECUs) responsible for most of the functionality in the vehicle. The

functionality ranges from small tasks such as opening a window and unlocking a door to more advanced functionality such as automatic brake systems and collision warning systems. The ECUs are therefore highly plausible targets for future attacks. To provide the specific functionality, each ECU operates using its own independent firmware. An upcoming trend for automotive manufacturers is to perform *remote diagnostics* and *firmware updates over the air* (FOTA) [12], which allows identifying hardware problems and rectifying software flaws with minimal customer inconvenience and shorter correction cycles [19].

Diagnostics can be performed on the ECUs to detect software errors or to determine the root cause of malfunctions. It allows finding errors in an early phase and aids in creating better and safer firmware. As new improved firmware versions are developed, the new firmware is downloaded to the vehicle and flashed to the ROM of the corresponding ECU, overwriting the old firmware. Thus, remote diagnostics and FOTA allow the firmware on the ECUs to be up-to-date to provide better and safer functionality.

However, allowing external communication with the previously isolated in-vehicle network introduces a number of security risks, as indicated by our introductory example.

As presented in [5,13], cyber attacks on the in-vehicle network could have serious consequences, and as shown in [9,14] there is a need for detecting and tracing such attacks. To assist in designing security to know what to protect, we perform an ECU classification based on safety and security. To our knowledge there exists no such classification for vehicles. Based on our classification we suggest that automotive manufacturers should emphasize the security or restrict the remote diagnostics and FOTA procedures to certain ECUs.

The main contributions of this paper are presented below.

- We have analyzed the functionality of individual ECUs and categorized them into groups based on safety integrity levels.

- We have analyzed cyber attacks introduced by allowing wireless communication with vehicles for performing remote diagnostics and firmware updates over the air. In addition, we have defined safety effect levels of security threats to classify the attacks.
- By combining the safety classification of the ECUs and the security classification of attacks, we have classified the ECUs according to safety-security characteristics.

The paper is outlined as follows. Section 2 describes related work. Section 3 gives background information on the in-vehicle network, and the remote diagnostics and FOTA procedures. Section 4 presents the analysis and method, and Section 5 gives the results of the safety-security classification. Section 6 discusses the classification, and Section 7 presents future work. The paper is concluded in Section 8.

## 2 Related work

Previous research related to safety and security in ECUs and in-vehicle networks includes the following.

Wolf et al. [24] describe several confidentiality and authenticity weaknesses in the CAN [1] and FlexRay [3] network protocols but do not suggest which ECUs to protect. Nilsson et al. [13] describe simulated attacks on the CAN bus and introduce the notation of vehicle virus.

A vehicle ECU classification based on software architecture is presented in [18]; however, no safety or security implications are mentioned. Instead, the classification assists in identifying the focus for embedded system application domain and in exploring the possibilities for software reuse in the automotive ECU domain.

In [7] a hazard analysis for safety critical systems in the automobile domain is presented. The analysis describes controllability of various safety failures but does not consider security threats.

The Global System for Telematics project [20] provides a reference standard for vehicle systems. The standard is J2ME/OSGi based, describes how a telematics client application can be downloaded and installed over the air from a control center, and specifies an interface for receiving vehicle data. In the context of security for the OSGi framework, some researches have investigated secure bundle deployment [10,16]. The solutions help certify the origin and the integrity of code. More relevant to this work is [6] which is a rule-based runtime monitor integrated into the OSGi to detect and prevent certain security violations.

Jonsson [8] presents a framework for security and dependability and describes the link between security and dependability (safety). Since the areas are related it

is necessary to take both safety and security into consideration when creating the classification.

## 3 Background

In this section, we describe the basics of an in-vehicle network and briefly explain the procedures of the two administrative functions remote diagnostics and FOTA. Furthermore, we develop an attacker model for this scenario.

### 3.1 In-vehicle network

A modern vehicle contains an in-vehicle network typically consisting of 50-70 ECUs. A conceptual model of the network is illustrated in Figure 1. There are several networks using different protocols in the in-vehicle network [21]: *Controller area network (CAN)*, *local interconnect network (LIN)*, and *media-oriented systems transport (MOST)*. The different networks are connected through gateways. CAN is the most common network in a vehicle, and there are often several CAN networks such as powertrain and comfort CAN [22]. LIN is a low-speed communication protocol used for non-safety critical sensor and actuator systems. The MOST protocol allows high bandwidth and is used to carry audio and video data.

There exists a wireless gateway on the in-vehicle network that allows external communication. The remote diagnostics and FOTA procedures use the wireless gateway to access the ECUs in the in-vehicle network.

Each ECU runs a specific firmware and is responsible for a certain functionality in the vehicle. For example, one ECU is responsible for the brake lights, and one ECU handles the driver door functionality. For more complex functions such as the engine system, a number of ECUs are cooperating.

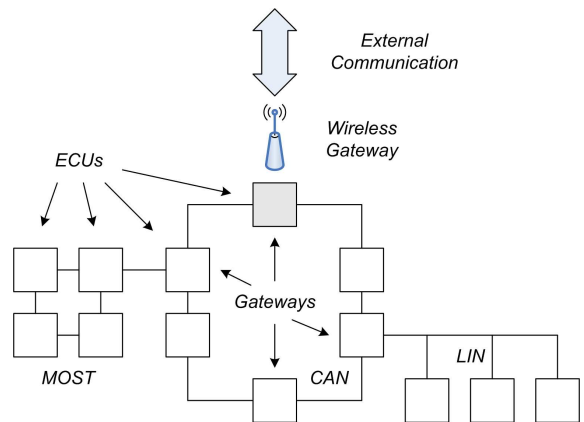


Figure 1: Conceptual model of an in-vehicle network consisting of CAN, LIN, and MOST networks, and a wireless gateway.

### 3.2 Remote diagnostics

Diagnostics is used to affect single data parameters in the ECUs [23], and is used for reading or controlling the ECU functionality.

*Read requests* are sent to read a specific parameter value. For example, the status value of the passenger door can be read to determine if the door is locked or the value of the engine temperature could be read.

*Control requests* are sent to control the ECU functionality. For example, actuators on a door locking mechanism could be controlled to unlock the door.

Both read and control requests are sent over a wireless communication link to perform remote diagnostics.

### 3.3 Firmware updates over the air (FOTA)

The firmware update procedure involves flashing a new firmware over an existing firmware in an ECU. It is used to install a new firmware version, e.g., when software flaws are discovered. The new firmware is sent over a wireless communication link to perform FOTA [19]. Protocols for secure FOTA are presented in [11,15].

Once the firmware has been downloaded to the vehicle, the firmware is transmitted in the in-vehicle network and received at the target ECU. The ECU flashes the new firmware to its ROM and reboots. The ECU functionality is then controlled by the new firmware.

### 3.4 Attacker model

In our attacker model, we assume that an attacker has access to the wireless communication link to perform cyber attacks on the vehicle. We adopt the Dolev-Yao attacker model [2] where an attacker can eavesdrop, intercept, modify, and inject messages into the communication link. Thus, we assume that the attacker deliberately aims to disrupt the communication between the automotive manufacturer and the vehicle. The attacker could, e.g., cause the communication to fail or modify the messages to perform arbitrary actions.

For remote diagnostics, the attacker could modify the read and control requests and cause them to *fail*. In addition, the attacker could modify and inject read and control requests to cause *arbitrary* actions. Replies sent from the vehicle are not considered since an attacker modifying or injecting replies does not affect the vehicle safety. The arbitrary actions are bound to the functionality of the corresponding ECU. Examples of attacks performed on the CAN bus are found in [13].

For FOTA, we assume that the attacker can disrupt the communication when the vehicle is downloading the firmware to cause the *download to fail*. Moreover, the attacker could modify the firmware in transit such that the download is successful but the *flashing of the firmware fails*. We assume that a failed flashing has

partially overwritten the existing firmware such that the functionality is partially or fully disabled. Last, the attacker could issue *arbitrary firmware* which is successfully downloaded to the vehicle and flashed to the corresponding ECU.

If an attacker compromises an ECU, the attacker can perform the functionalities that the corresponding ECU is responsible for or control. For example, an attacker compromising an ECU controlling the brakes could disable the brake capability or apply the brakes.

Furthermore, we assume that an attacker reading the firmware does not affect the vehicle safety, and thus this attack is not considered further.

## 4 Analysis method and classification

In this section, we discuss safety integrity levels (SIL) and introduce the notation of safety effect levels of security threats (SEL). We classify the ECUs into categories based on their functionalities and assign a SIL value to each category based on the controllability of a failure. We also assign SEL values to the identified attacks in the remote diagnostics and FOTA procedures.

### 4.1 Safety and security levels

We first discuss how SIL values are assigned based on controllability. Next, we develop SELs based on how severe the safety effect is from a particular cyber attack.

#### Safety integrity levels (SIL)

<i>Controllability</i>	<i>Acceptable failure rate</i>	<i>Safety integrity level (SIL)</i>
Uncontrollable	Extremely improbable	4
Difficult to control	Very remote	3
Debilitating	Remote	2
Distracting	Unlikely	1

Table 1: SILs according to controllability and probability of failures.

Safety integrity is defined as “the probability of a safety-related system satisfactorily performing the required safety functions under all stated conditions within a stated period of time” [4]. A SIL is a discrete level, ranging from level 1 as the lowest to level 4 as the highest, for specifying the safety requirements of the safety functions to be allocated to the safety-related systems. The levels of SIL are primarily designed for *probability of failures* and *controllability* by humans. We classify the ECU categories using the SIL levels. The

designation of SIL levels according to controllability and probability of failures is given in Table 1.

**Safety effect levels of security threats (SEL)**

Inspired by SIL in [4], we introduce safety effect levels of security threats (SEL). We specify four levels for identifying the safety effect of a specific security threat. Level 4 is the highest value indicating a security threat resulting in a disastrous safety effect. Correspondingly, level 1 is the lowest value representing a security threat which is merely distracting. The levels are presented in Table 2. Since we focus on deliberate cyber attacks, the probability of failures is neglected.

<i>Safety effect</i>	<i>Safety effect level (SEL)</i>
Disastrous	4
Severe	3
Mediocre	2
Distracting	1

Table 2: SELs according to safety effect of security threats.

**4.2 ECU categorization and classification**

We categorize the ECUs based on how a failure of the functionality may affect the safety of a driver.

We divide the ECUs into five categories: powertrain, vehicle safety, comfort, infotainment, and telematics, and for each category we assign a SIL value. The categories and respective SIL values are provided in Table 3.

<i>ECU Category</i>	<i>SIL</i>
Powertrain	4
Vehicle safety	4
Comfort	2
Infotainment	1
Telematics	1

Table 3: SIL values for ECU categories.

**Powertrain**

The powertrain category consists of critical resource controls such as engine management and transmission control. Examples of systems belonging to this category

are the brake system that helps the driver to prevent wheel skidding and the electronic brake force distribution that maintains the vehicle stability. These ECUs are highly safety critical since a failure of the functionality might cause the driver to lose control of the vehicle.

We assign the powertrain category SIL 4 since a failure could affect vehicle control and maneuverability resulting in an uncontrollable effect on safety.

**Vehicle safety**

The vehicle safety category contains systems that provide safety assistance to the driver such as anti-lock braking systems, tire pressure monitoring, adaptive cruise control, airbag, and collision avoidance systems. These ECUs are also highly safety critical since a failure of the functionality could lead to driver injuries.

The vehicle safety category is also given SIL 4 since a failure of safety functionality could have an uncontrollable impact on safety.

**Comfort**

The comfort category includes ECUs that provide driver assistance such as electronic suspension, thermal management and parking assistance. Since the category aims to assist the driver, failures of the ECU functionality might not immediately affect the safety of the driver.

This category is assigned SIL 2 since failures are not directly related to safety but a combination of failures could lead to debilitating effects.

**Infotainment**

The infotainment category consists of systems for audio and video support in the vehicle. Such systems include digital broadcasting TV, audio streams, and TFT displays [18]. In addition, systems that receive data from external sources, e.g., traffic and weather information systems are included in this category. These systems provide information and entertainment to the driver and the passengers and are not directly related to vehicle system control.

The infotainment category is assigned SIL 1 since failures of systems in this category do not immediately affect safety but are considered distracting.

**Telematics**

The telematics category involves systems that integrate telecommunications and informatics. Such systems are used to provide networked software applications to the vehicle. In addition, this category contains ECUs that provide mobile communication such as GPRS.

We assign the telematics category SIL 1 since a failure of functionality in these systems does not directly affect the safety of the driver but could be considered distracting.

### 4.3 Cyber attack classification

The identified cyber attacks (Section 3.4) are discussed and the four SEL values are used to classify the effect of safety as a result of each attack.

#### Remote diagnostics attacks

We assign SEL 1 to attacks that cause the read and control requests to fail, since these failures are not harmful to the vehicle system. SEL 1 is also assigned to arbitrary read requests since read actions are not safety related. On the other hand, arbitrary control requests could allow an attacker full control of ECU functionality which would allow an attacker to execute malicious actions [13]; therefore, we assign SEL 4 to this type of attack. Table 4 shows the SEL classification for remote diagnostics attacks.

<b>Remote diagnostics attacks</b>		<b>SEL</b>
Read request	<i>Fail</i>	1
	<i>Arbitrary</i>	1
Control request	<i>Fail</i>	1
	<i>Arbitrary</i>	4

Table 4: SEL values for remote diagnostics attacks.

#### Firmware updates over the air attacks

An attacker causing the FOTA download process to fail does not directly affect the safety of the vehicle; therefore, it is given SEL 1. Moreover, causing a firmware flashing failure could result in ECU malfunction which could affect the safety of the vehicle and driver considerably. As a result, we assign the flashing fail attack SEL 3. Last, arbitrary flashing of the ECU allows an attacker to perform any actions which could have disastrous effects on safety; therefore, it is assigned SEL 4. The SEL classification for FOTA attacks is given in Table 5.

<b>FOTA attacks</b>	<b>SEL</b>
<i>Download fail</i>	1
<i>Flashing fail</i>	3
<i>Arbitrary flashing</i>	4

Table 5: SEL values for FOTA attacks.

## 5 ECU safety-security classification

We use the SIL and SEL values as a basis to determine the safety criticality of security threats. We combine the SIL values for respective ECU category with the SEL values for each attack type in remote diagnostics and FOTA. We add the SIL and SEL values together to achieve a safety criticality level of a specific security threat in the corresponding ECU category. Thus, the resulting classification is based on safety and security characteristics. The combined values, ranging from 2 to 8, are presented in a matrix. In Table 6, the safety-security ECU classification for remote diagnostics attacks is shown.

<b>ECU categories</b>	<b>Remote diagnostics attacks</b>			
	<b>Read request</b>		<b>Control request</b>	
	<i>Fail</i>	<i>Arbitrary</i>	<i>Fail</i>	<i>Arbitrary</i>
Powertrain	5	5	5	<b>8</b>
Vehicle safety	5	5	5	<b>8</b>
Comfort	3	3	3	<b>6</b>
Infotainment	2	2	2	5
Telematics	2	2	2	5

Table 6: Safety-security levels for ECU categories based on remote diagnostics attacks.

In Table 7, the safety-security ECU classification for FOTA attacks is provided.

<b>ECU categories</b>	<b>FOTA attacks</b>		
	<b>Download fail</b>	<b>Flashing fail</b>	<b>Arbitrary flashing</b>
Powertrain	5	<b>7</b>	<b>8</b>
Vehicle safety	5	<b>7</b>	<b>8</b>
Comfort	3	5	<b>6</b>
Infotainment	2	4	5
Telematics	2	4	5

Table 7: Safety-security levels for ECU categories based on FOTA attacks.

## 6 Discussion

According to the results from our analysis, ECU categories such as powertrain and vehicle safety

require further protection prior to introducing remote connectivity. Unwanted effects in any of these categories may render the vehicle uncontrollable and cause disastrous consequences for the driver. Furthermore, the remote diagnostics and FOTA procedures should be prohibited for ECU categories where the safety-security level value is six or higher. This restriction would allow safety-critical actions on non-safety-critical ECUs, such as remotely updating the mp3-player in the infotainment system with new device drivers. It would also allow non-safety-critical actions on safety-critical ECUs, including reading status information from the powertrain ECU to find out whether the latest required firmware version is installed. However, safety-critical actions on safety-critical ECUs would not be allowed since they would allow an attacker to directly affect the safety of the driver. These are indicated with bold text in Tables 6 and 7.

Furthermore, allowing external parties to issue control requests to and performing FOTA on the comfort, infotainment and telematics ECUs require a strong security perimeter around the powertrain and vehicle safety ECUs. This separation is required to, e.g., prevent a compromised comfort ECU to communicate with a powertrain ECU. Security protection, such as packet filtering, should be added to the gateway ECUs, and access policies need to be developed for allowing network traffic to enter and leave the powertrain and vehicle safety ECUs.

## 7 Future work

The safety-security classification introduced in this paper can be used to define access control policies for ECU categories and remote procedures interacting with vehicles.

Traditional security solutions, such as digital signatures, could be applied to ensure that a firmware is correctly downloaded and that it originates from a trusted third party. However, if a third party issues a firmware that contains a bug or malicious code, the traditional solutions will not prevent the bug from causing problems or the malicious code from executing. Therefore, there exists a need for finer-grained access controls which could be employed by defining security policies. Recent studies in security policy enforcement show that language-based security mechanisms such as inlined reference monitors [17] provide a potential solution for security in such systems. As future work, we plan to investigate the approach of language-based security mechanisms in an automotive context.

## 8 Conclusion

Since safety and security are two closely related concepts [8], we have provided a vehicle ECU category classification based on safety and security char-

acteristics. We suggest that automotive manufacturers should emphasize the security or restrict the remote diagnostics and firmware updates over the air procedures to certain ECUs.

The presented safety-security ECU classification assists in designing security for remote diagnostics and firmware updates over the air. We emphasize a security level that allows a safety-critical action on a non-safety-critical ECU and a non-safety-critical action on a safety-critical ECU to achieve an adequate level of security.

## 9 Acknowledgments

This material is based upon work supported by the Swedish Governmental Agency for Innovation Systems (VINNOVA), Volvo Car Corporation, and Volvo IT under the Vehicle-ICT program. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of VINNOVA, Volvo Car Corporation, or Volvo IT.

## References

- [1] Bosch. CAN Specification 2.0. <http://www.dcd.pl/dcdpdf/can2spec.pdf>, 1991. Visited August, 2007.
- [2] Danny Dolev and Andrew C. Yao. On the Security of Public Key Protocols. In *IEEE 22nd Annual Symposium on Foundations of Computer Science*, Stanford, CA, USA, 1981.
- [3] FlexRay Consortium. FlexRay Communications System Protocol Specification 2.1 Revision A.
- [4] Health Innovation Electronics (UK) Ltd and Safety Laboratory. A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines.
- [5] Tobias Hoppe and Jana Dittman. Sniffing/Replay Attacks on CAN Buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy. In *Proceedings of the 2nd Workshop on Embedded Systems Security (WESS)*, Salzburg, Austria, 2007.
- [6] Chi-Chih Huang, Pang-Chieh Wang, and Ting-Wei Hou. Advanced OSGi security layer. In *Proceedings of AINAW '07*, pages 518–523, USA, 2007. IEEE Computer Society.
- [7] Per Johannessen, Fredrik Torner, and Jan Torin. Actuator Based Hazard Analysis for Safety Critical Systems. In *Proceedings of the 23rd International Conference on Computer Safety, Reliability and Security (SAFECOMP)*, 2004.
- [8] Erland Jonsson. An integrated framework for security and dependability. In *NSPW'98: Proceedings of the 1998 workshop on New security paradigms*, New York, NY, USA, 1998.
- [9] Ulf E. Larson, Dennis K. Nilsson, and Erland Jonsson. An Approach to Specification-Based

- Attack Detection for In-Vehicle Networks. In *Proceedings of the 12th IEEE Intelligent Vehicles Symposium (IV)*, 2008.
- [10] Hee-Young Lim, Young-Gab Kim, Chang-Joo Moon, and Doo-Kwan Baik. Bundle Authentication and Authorization Using XML security in the OSGi Service Platform. In *Proceedings of ICIS '05*, pages 502–507, Washington, DC, USA, 2005. IEEE Computer Society.
- [11] Syed Masud Mahmud, Shobhit Shanker, and Irina Hossain. Secure Software Upload in an Intelligent Vehicle via Wireless Communication Links. In *Intelligent Vehicles Symposium*, 2005.
- [12] Radovan Miucic and Syed Masud Mahmud. Wireless Multicasting for Remote Software Upload in Vehicles with Realistic Vehicle Movement. Technical report, Electrical and Computer Engineering Department, Wayne State University, Detroit, MI 48202, USA, 2005.
- [13] Dennis K. Nilsson and Ulf E. Larson. Simulated Attacks on CAN Buses: Vehicle virus. In *Proceedings of the Fifth IASTED Asian Conference on Communication Systems and Networks (ASIACSN)*, 2008.
- [14] Dennis K. Nilsson and Ulf E. Larson. Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks. In *Proceedings of the First ACM International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics)*, 2008.
- [15] Dennis K. Nilsson and Ulf E. Larson. Secure Firmware Updates over the Air in Intelligent Vehicles. In *Proceedings of the First IEEE Vehicular Networking & Applications Workshop (Vehi-Mobi)*, 2008.
- [16] Pierre Parrend and Stephane Frenot. Supporting the Secure Deployment of OSGi bundles. In *Proceedings of WoWMoM*, 2007. IEEE Computer Society, June 2007.
- [17] Fred B. Schneider, Greg Morrisett, and Robert Harper. A language-based approach to security. In *Informatics 10 Years Back, 10 Years Ahead, LNCS 2000*, pages 86–101, 2000.
- [18] Win-Bin See. Vehicle ECU Classification and Software Architectural Implications. Technical Report, Feng Chia University, Taiwan, 2006.
- [19] Moshe Shavit, Andy Gryc, and Radovan Miucic. Firmware Update over the Air (FOTA) for Automotive Industry. In *Asia Pacific Automotive Engineering Conference*, Hollywood, CA, USA, August 2007.
- [20] The Global System for Telematics (GST) project. <http://www.gstforum.org>. Visited November, 2007.
- [21] Vector Informatik. Serial Bus Systems in the Automobile: Part 1. [http://www.vector-scandinavia.com/portal/medien/cmc/press/PTR/SerialBusSystems\\_Part1\\_ElektronikAutomotive\\_200611\\_PressArticle\\_EN.pdf](http://www.vector-scandinavia.com/portal/medien/cmc/press/PTR/SerialBusSystems_Part1_ElektronikAutomotive_200611_PressArticle_EN.pdf), 2007.
- [22] Vector Informatik. Serial Bus Systems in the Automobile: Part 2. [http://www.vector-scandinavia.com/portal/medien/cmc/press/PTR/SerialBusSystems\\_Part2\\_ElektronikAutomotive\\_200612\\_PressArticle\\_EN.pdf](http://www.vector-scandinavia.com/portal/medien/cmc/press/PTR/SerialBusSystems_Part2_ElektronikAutomotive_200612_PressArticle_EN.pdf), 2007.
- [23] Vector Informatik. Vehicle Diagnostics: The whole story. [http://www.vector-scandinavia.com/portal/medien/cmc/press/PDG/Diagnostics\\_Congress\\_ElektronikAutomotive\\_200703\\_PressArticle\\_EN.pdf](http://www.vector-scandinavia.com/portal/medien/cmc/press/PDG/Diagnostics_Congress_ElektronikAutomotive_200703_PressArticle_EN.pdf), 2007.
- [24] Marko Wolf, Andre Weimerskirch, and Christof Paar. Security in Automotive Bus Systems. In *Workshop on Embedded IT-Security in Cars*, 2004.