

Freiberger, Stefanrger; Albrecht, Matthias; Käufl, Josef

Article

Reverse engineering technologies for remanufacturing of automotive systems communicating via CAN bus

Journal of Remanufacturing

Provided in Cooperation with:

Springer Nature

Suggested Citation: Freiberger, Stefanrger; Albrecht, Matthias; Käufl, Josef (2011) : Reverse engineering technologies for remanufacturing of automotive systems communicating via CAN bus, Journal of Remanufacturing, ISSN 2210-4690, Springer, Heidelberg, Vol. 1, pp. 1-14, <https://doi.org/10.1186/2210-4690-1-6>

This Version is available at:

<https://hdl.handle.net/10419/108884>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<http://creativecommons.org/licenses/by/2.0/>

RESEARCH

Open Access

Reverse Engineering Technologies for Remanufacturing of Automotive Systems Communicating via CAN Bus

Stefan Freiberger^{*}, Matthias Albrecht and Josef Käußl

Abstract

Nowadays, as mechatronic and electronic systems have found their way into vehicles, the technological knowledgebase of traditional remanufacturing companies erodes rapidly and even the industrial principle of remanufacturing is at risk. Due to the fact that modern cars incorporate up to 80 of these mechatronic and electronic systems that are communicating with each other e.g. via the vehicle controller area network (CAN), remanufacturing of these automotive systems requires innovative reverse engineering knowhow, methodological innovations and new technologies, especially focusing on the tasks testing and diagnostics of systems and their subassemblies. The European research project "CAN REMAN", conducted by Bayreuth University in cooperation with two other universities and eight industrial partners, focuses on these needs in order to enable companies to remanufacture modern automotive mechatronics and electronics with innovative reverse engineering skills as well as to develop appropriate and affordable testing and diagnostics technologies.

In order to operate and test the mechatronic device with CAN interface outside the vehicle environment, an appropriate simulation of the vehicle network and all connected sensors of the device under test (DUT) is essential. This implies an electrical analysis of the connectors of the DUT, a content-related analysis of the CAN-bus, a sensor hardware simulation and a CAN-bus simulation.

All electrical measurements and results were taken using conventional multimeters or oscilloscopes. The CAN-bus analysis and simulations were conducted using the Vector Informatics software tool "CANoe" (Version 7.1) and a suitable CAN-bus hardware, e.g. the CANcardXL and the IOcab8444opto. All hardware simulations were executed with a conventional wave form generator or a microcontroller evaluation board (Olimex AVR-CAN) and an appropriate electric setup.

In order to initially readout the failure memory and to investigate the diagnostic communication of the DUT, garage testers such as "Bosch KTS 650" or "Rosstech VAG-COM" were used.

The results of the project are application-orientated methods, test benches and skills for remanufacturing companies to find out the working principles of the CAN-bus communication between automotive mechatronic and electronic systems within vehicles.

The knowhow presented in this article enables remanufacturing companies to remanufacture modern automotive mechatronic and electronic systems which are communicating via the CAN-bus and similar communication types.

Keywords: Remanufacturing, Mechatronics, Electronics, CAN-bus, Reverse Engineering, Testing, Diagnosis, Vehicle Network Topology

^{*} Correspondence: stefan.freiberger@uni-bayreuth.de
Chair of Manufacturing and Remanufacturing Technology, Bayreuth University, Universitaetsstrasse 30, 95447 Bayreuth, Germany

1. Introduction

Raising requirements on occupant safety and comfort on the one hand and the introduction of new emission regulations on the other hand, forces the automotive manufacturers to enhance their products continuously. In order to achieve these improvements, electronic systems, based on microcontrollers, have found their way into modern cars and they contributed considerably to many new advantages in terms of safety and comfort such as Electronic Stability Program (ESP), Anti-lock Brake System (ABS), Parking Assist System (PAS), Electro Hydraulic Power Steering (EHPS) or Electro Assisted Steering (EAS). Nevertheless, the new trend of modernization has an immense impact on the remanufacturing business. It can be seen that new branches in electronic remanufacturing arise. In contrast to that, the knowhow of traditional remanufacturing companies has eroded rapidly and even the industrial principle of remanufacturing is at risk [1]. Due to the fact that modern cars incorporate up to 80 of these mechatronic and electronic systems that are communicating with each other e.g. via the CAN-bus, remanufacturing of these automotive systems requires innovative reverse engineering knowhow, methodological innovations and new technologies especially focussing on the tasks testing and diagnostics of systems and their subassemblies. Since, traditional remanufacturing companies do not have much capacity to build up the appropriate knowhow, the Chair of Manufacturing and Remanufacturing Technologies at Bayreuth University assists these companies in reverse engineering, as well as finding new methodologies and technologies for remanufacturing [2,3].

In the following chapters, reverse engineering methodologies, technologies and results for automotive components will be presented on the example of an EHPS pump. The results have been obtained within the European research project "CAN REMAN" which is conducted by Bayreuth University, Linköping University (Sweden), the University of Applied Sciences Coburg, Fraunhofer Project Group Process Innovation and eight industrial partners. The target of this project is to enable independent aftermarket (IAM) companies to remanufacture modern automotive mechatronics and electronics with innovative reverse engineering skills as well as to develop appropriate and affordable testing and diagnostics technologies [4]. The described, close to industry results, will contribute to the remanufacturing research theory by the upcoming PhD-thesis of engineers of the Chair of Manufacturing and Remanufacturing Technology.

2. Automotive Mechatronics Change Today's Remanufacturing

The term "mechatronics" was formulated in 1969 in Japan and it is an artifice that describes a system which

combines mechanics, electronics and information technologies. A typical mechatronic system gathers data, processes the information and outputs signals that are for instance converted into forces or movements [5].

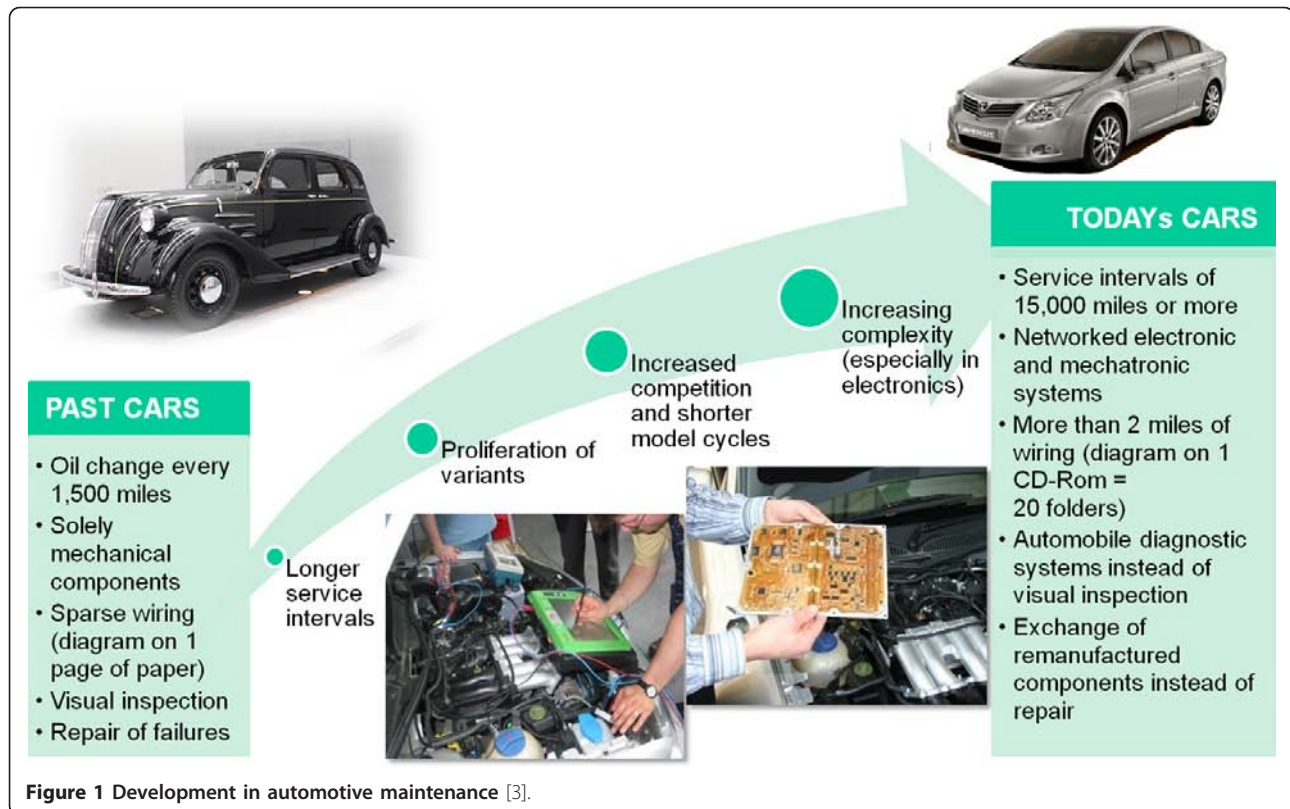
2.1. Technological Change of Vehicles

Automotive parts should not longer be seen as isolated standalone applications with few mechanical and electrical inputs and outputs. Now, they have the capability to communicate to each other and to share the same information. Subsequently, the communication of the different automotive subsystems helps the original equipment manufacturers (OEMs) to reduce weight and cost by sharing the same sensors and reducing cable doubling (cable length) in modern vehicles. For the driver the network and communication within the car remains invisible and he feels the car behaving like ten years ago despite of some additional comfort functions. Figure 1 demonstrates the radical shift in the automotive technological development.

But if we take a closer look, nowadays modern vehicles resemble more or less a distributed system. Several embedded computers - often referred to electronic control units (ECUs) - communicate, share information and verify each other over the vehicle network. One of the commonly used communication networks in vehicles is the CAN-bus. Within this network structure, each control unit has at least one unique identifier (ID) on which it broadcasts messages that again incorporate different signals and information [6]. Easily speaking, in case of a missing or faulty participant in the network, all other controllers will notice the participant as they have a lack of information. The lack of information or errors on the CAN-bus can force other systems to operate in a "safe mode" or cause that these systems never start their operation. In reverse, a controller not connected to the specific vehicle network will not start its regular operation patterns.

2.2. Difficulties for Remanufacturers

As stated before, the introduction of electronic networks into modern cars entails enormous problems for remanufacturers. Modern electronic and mechatronic vehicle components cannot be tested as easily as traditional electrical and mechanical ones [7-9]. While it was usually sufficient to link electrical systems to the power supply (battery), modern mechatronic and electronic systems gather a lot of information from the vehicle environment and driving conditions using plenty of sensors and the CAN-bus network of the vehicle. As a consequence, connecting all sensors and the power plug to the DUT is insufficient unless the device is connected to the network of a real car or an adequate simulation of the communication in the vehicle.



Following these statements, the key for successful remanufacturing and testing of a certain automotive system lies in the simulation of the complete network communication in the vehicle. In each case, the car matrix (CAN database) of the specific vehicle model is required to build a simulation of the CAN communication in a vehicle. However, the OEMs will not release any information on the communication parameters to non-OEs and therefore they will not support the independent remanufacturing business. As a consequence, the independent remanufacturers - onto which this paper focuses - have to do a lot of reverse engineering themselves or in cooperation with others in order to design their remanufacturing process chain and to come up with test solutions to ensure the quality of their products [10-12]. These reverse engineering activities focus on the system, its components, the system behavior in the vehicle and the vehicle CAN-bus communication.

2.3. The Remanufacturing Process Chain for Automotive Mechatronics

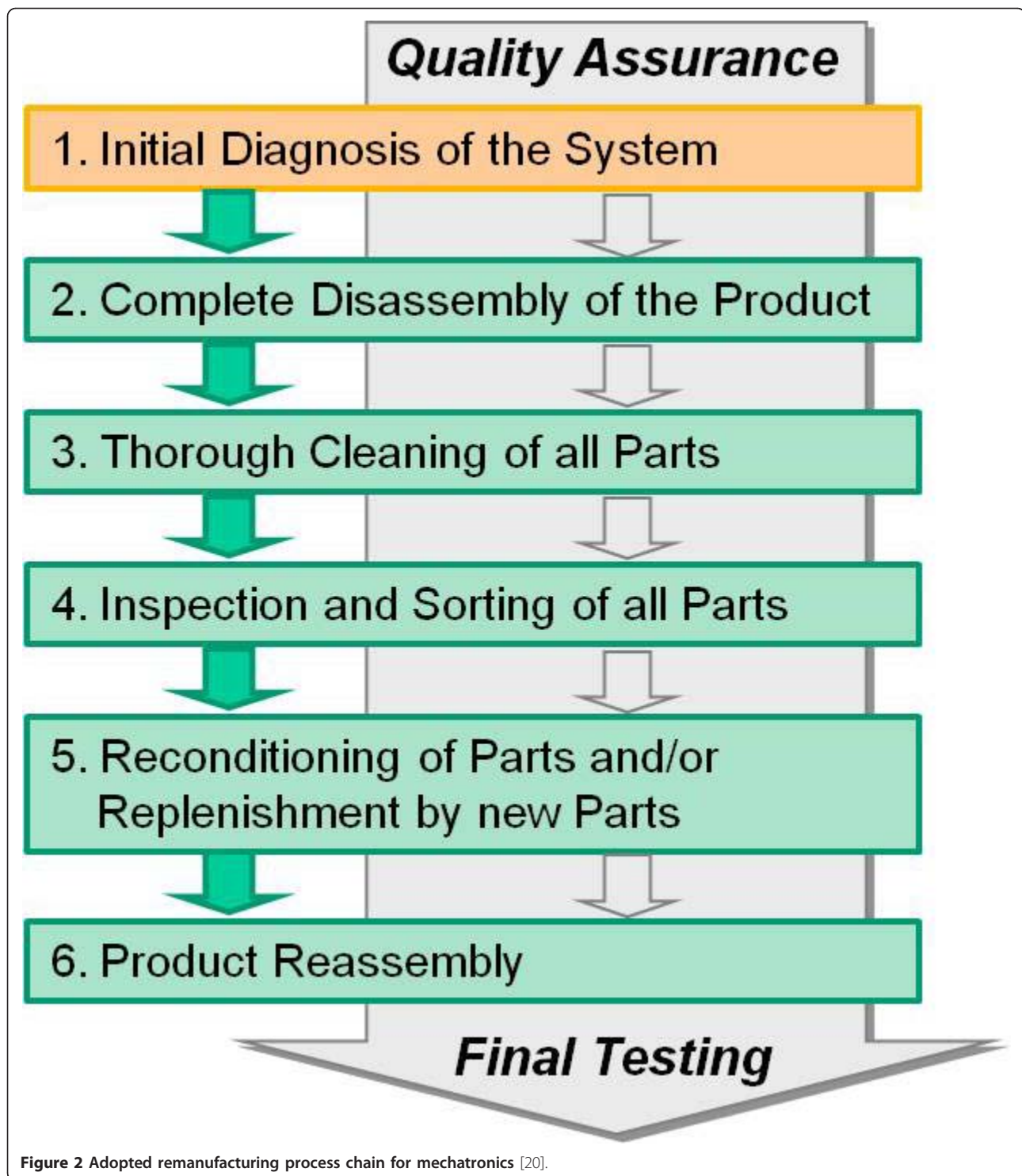
Following the previous aspects, the state-of-the-art process chain for remanufacturing, needs to be reconsidered when it comes to mechatronics, as shown in Figure 2. Regarding the process steps, disassembly, cleaning and reassembly, great progress has been made on mechanic systems, as it can be found in the literature

[13-16]. This progress on the mechanical systems can also be transferred to the mechanic components inside of mechatronic systems. However, the diagnostics and testing differs to a certain extent from the traditional (final) testing of mechanics, as it has already been discussed before. In addition to this, it was found that a lot of failures of parts and its subassemblies can only be detected or isolated with a test of the completely assembled mechatronic system [2,17], e.g. by utilization of the onboard-diagnostics and readout of the fault memory inside a mechatronic system. This means that the process chain for remanufacturing of mechatronic systems should be extended by an additional first step as it is shown in Figure 2.

In the initial entrance diagnostics of the system to be remanufactured all communication patterns have to be reverse engineered in order to simulate the vehicle network and get access to the fault memory of the system. An appropriate vehicle network simulation will also prevent new fault memory records to be stored in the DUT.

3. Reverse Engineering an Automotive Mechatronic System

The term "reverse engineering" has its origin in the mechanical engineering and describes in its original meaning the analysis of hardware by somebody else



than the developer of a certain product and without the benefit of the original documentation or drawings. However, reverse engineering was usually applied to enhance your own products or to analyze the competitor's products [18]. According to Cifuentes and Fitzgerald (2000), an analog term is "*reengineering*" (of software)

which does not refer to the process of analyzing software only, but which also intends to translate software into a new form, either at the same or a higher level of abstraction. In addition to this, the two authors summarize the different types of software reverse engineering. It can be differentiated between black and white

box reverse engineering. While black box reverse engineering only looks at the behavior of a program and its documentation (if it's available) without examination of the internals of the program, white box reverse engineering involves looking at the internals of a program so that its working can be understood [19].

Chikovsky and Cross (1990) describe reverse engineering in the context with software development and the software life cycle as an analysis process of a system, in order to identify the system (sub-) components, to investigate their interaction and to represent the system at a higher level of abstraction [18]. In this context, they also clarify the terms "redocumentation" and "design recovery".

"Redocumentation" is the generation or revision of a semantically equivalent description at the same abstraction level. This means, that the results are an alternative representation form for an existing system description. However, redocumentation is often used in the context of recovering "lost" information [18].

The term "design recovery" defines a subset of reverse engineering that includes domain knowledge, external information (of third parties) and conclusions additionally to the original observations and analyses in order to derive meaningful abstractions of the system at a higher level [18].

Overall, reverse engineering of software in the field of software development focuses on the following six targets [18-20]:

- Coping with the system complexity
- Generation of alternative views
- Recovery of lost information
- Detection of side effects
- Synthesis of higher abstractions
- Facilitation of reuse

These targets, that have originally been defined for software reverse engineering, can also be transferred to a certain extent to the reverse engineering of automotive mechatronic systems and hence to the remanufacturing of these systems.

First, remanufacturers will have to cope with the complexity of mechatronic systems as stated before. "Cope" means in this context, that it must be possible to operate an automotive mechatronic system independently from its original environment (the vehicle).

Second, universal taxonomies have to be detected in order to transfer the gained knowledge to similar mechatronic systems or to other variants of the system. Especially the high degree of variation of similarly looking mechatronic systems and control units makes it difficult for the remanufacturers to manage the complexity of automotive components that usually differ by a slight detail [21].

Third, recovery of missing, rather than lost, information will be one of the most important aspects for the remanufacturing.

The following chapter demonstrates how a reverse engineering analysis can be conducted for an automotive mechatronic system.

4. Analyzing an Automotive System in Five Steps

After a reference system (a reference system in this case is a commonly used automotive subsystem; for example an electro-hydraulic power steering pump) for the analysis has been chosen it is necessary to procure at least one, ideally brand-new, system to grant correct functionality, for all following investigations. In order to analyze the system in its normal working environment, the original vehicle, in which the reference system commonly is built in, should be procured as well.

This investment might be unavoidable, because a mechatronic system communicating via CAN, detached from all other vehicle communication will not work anyway, because essential input information, transmitted via CAN, is missing otherwise (refer to chapter 2). In this case it is very difficult to understand the ECU communication and put up the system into operation isolated from the vehicle.

A cheaper way to investigate the communication between vehicle and reference system is to create a CAN recording using a software tool such as "CANoe" from Vector Informatics. This tool allows easily recording of the complete vehicle communication for instance while doing a test drive with a vehicle that may be available only once. But this procedure requires careful planning prior the test drive is carried out, in order to record every driving condition which is needed for further analyses without having the vehicle available.

Whatever strategy is chosen, it is essential to figure out which input information (CAN data) is necessary to start, operate and control the system.

The following subsections will describe the five most important steps of the analysis process more in detail.

4.1. Electrical Wiring

After having obtained a reference system, it is essential to know the pinout of all connectors of the system. Therefore, the very first step is to find out which pin belongs to which wire and signal.

First of all, the power connector (ground and positive terminal), including ignition, must be identified. One opportunity to obtain this information is the utilization of wiring diagrams or similar credentials. If such documents are not available, for example a visual inspection of the connectors and wire harness in the vehicle or continuity measurements can be beneficial.

Afterwards, it is indispensable to identify the CAN connection pins. These can easily be recognized by inspecting the cable harness (in most cases two twisted wires, but single wire CAN connection is possible, too) or by measuring a terminating impedance of 60 Ω between to cables.

Finally, all connectors for sensors and actuators (auxiliary power and sensor/actuator signal) must be known as well to go further in the analysis process.

4.2. Vehicle Network Topology

The investigation of the structure of all bus systems in the vehicle is placed in front of the proper CAN-bus analysis step. It is necessary to determine how many (CAN-bus) networks are established and in which network the reference system is located. Additionally, the network speed, the presence of a separate diagnosis network (e.g. K-Line), and all ECUs of the specific networks must be found out, especially those ECUs that provide essential input as mentioned before. Furthermore, possible gateway ECUs, which are linking different networks, should be identified.

A feasible solution to gain this information can be for example a web inquiry, documents from the manufacturer of the vehicle or the system, third party documents or technical journals (e.g. ATZ, MTZ ...).

4.3. CAN Bus Communication

In order to understand the vehicle communication more in detail, all ECUs and its associated CAN message IDs must be determined. For this purpose CANoe can be used. First of all, a physical connection to access the CAN-bus using CANoe has to be installed in the vehicle, ideally nearby the reference system ECU. With the "trace functionality" of CANoe the bus communication and all CAN messages of all ECUs can be displayed easily (Figure 3). Beside of the CAN IDs, the cycle time and the length of each message can be analyzed. This information is relevant later on for a rest bus simulation of all participating ECUs to ensure correct functionality of the reference system.

The assignment of CAN ID and the associated ECU is more difficult. In the following, two options are described in detail.

One possibility to gather this information is to record the CAN communication initially with all ECUs connected to the bus using CANoe. Afterwards, each ECU is disconnected from the bus one after another and a CAN trace is stored again. Next, all recordings are compared to each other. Those IDs that are missing in the recording can be assigned to the disconnected ECU.

Another appropriate and more sophisticated way is to locate all ECUs which provide relevant data on the

CAN bus and to separate the CAN wires out of the cable harness. Each end of the CAN wires in the vehicle must be connected to a computer via CAN hardware. Afterwards, a kind of software gateway (Figure 4) is installed in between the DUT and the other ECUs using CANoe and a simple CAPL (CAN Access Programming Language) program.

By this means, it is now possible to detect the messages on the bus as well as the transmit direction - receive or transmit. This step is repeated for each ECU which provides relevant input data for the reference system. Obviously, the time exposure for this kind of CAN-bus analysis is much higher due to fact that the gateway has to be placed in between every ECU which is connected to the CAN network. The higher the complexity level of the reference system (more inputs), the more time is needed to identify all ECU messages which transmit relevant data via CAN.

The second way is more satisfying, although it may be more time-consuming than the first one. The first option offers a good overview of all CAN messages and its original ECU, but it may be fault-prone and incomplete. No matter which way is chosen, the result is a complete CAN message structure. Both ways are targeting.

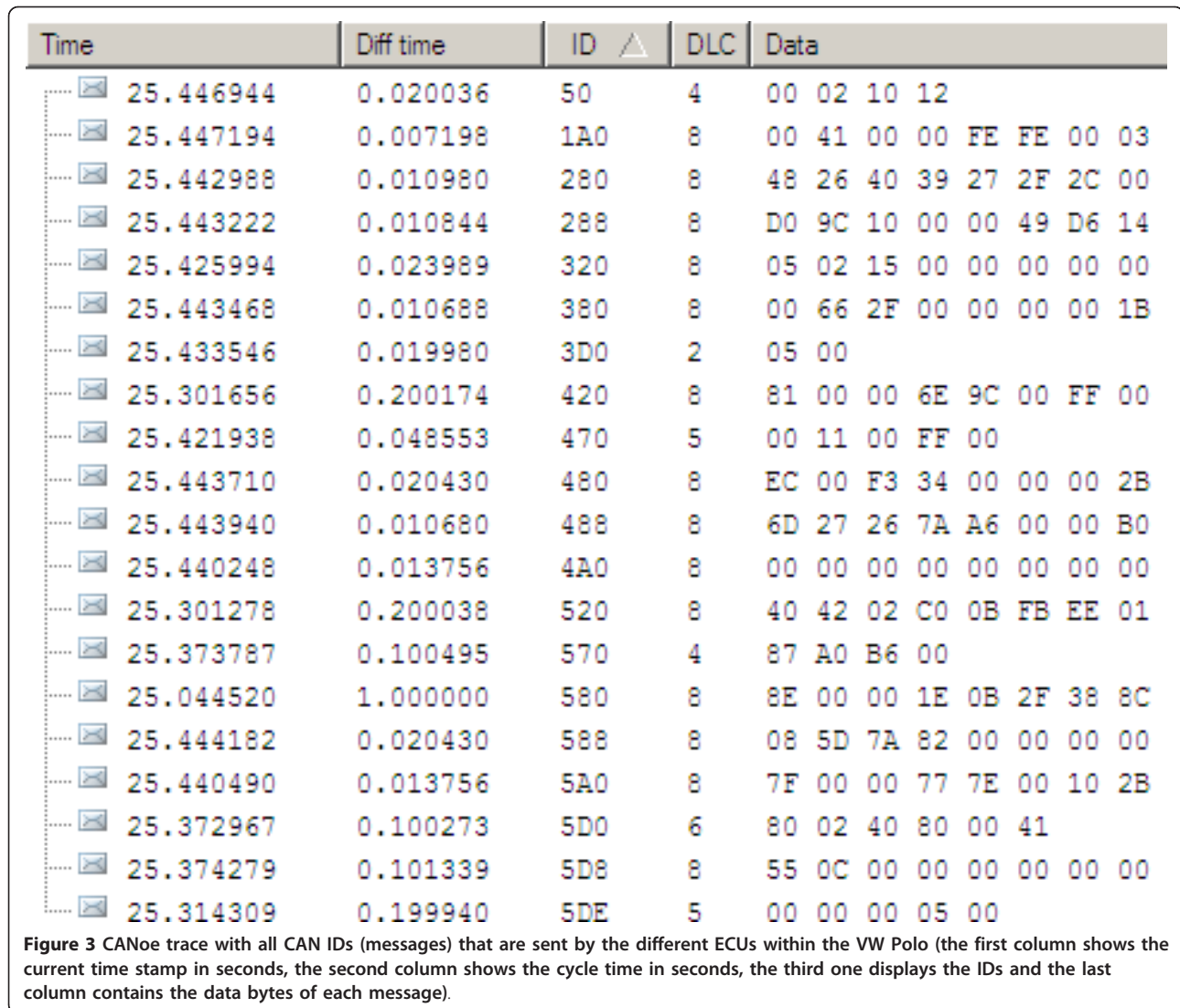
But not all identified messages are relevant for the DUT. Some are not recognized by the DUT and can be disregarded for further investigations. By adding filters for single messages in the gateway CAPL program or simply disconnecting whole ECUs from the network, an empty fault memory of the DUT will reveal unnecessary messages/ECUs and hence reduce data complexity. Hereby, an external garage tester can be used in most cases in order to readout the fault memory and in order to determine whether a failure was caused by removing certain data information.

After having identified the relevant CAN messages, it is inevitable to examine the message data bytes in detail to determine the physical signals. This can be achieved by generating physical inputs manually (e.g. open the throttle, drive, break ...) and observe the particular CAN messages as well as its bytes in parallel. After that, a correlation between a CAN message, its CAN data and a physical input value can be established.

Having performed the steps above, it is possible to setup the desired restbus simulation for the reference system.

4.4. Sensors

Besides the CAN data, analog inputs of sensors and analog outputs of actuators are important in order to ensure correct functionality of the reference system. Therefore, each sensor and nearly each actuator has to be analyzed and simulated, too.



The sensors can be analyzed using an oscilloscope and a multimeter in order to characterize current consumption, supply voltage and signal transmission. Typically, sensor output signals are analog to:

- Current/voltage, amplitude
- Frequency/cycle time
- Pulse width/duty cycle

Or they are discrete in the following forms:

- Binary
- Multi-staged (different scaled)
- Multi-staged (equidistant) → digital

For the simulation, the measured values must be interpreted and emulated. For example, the internal resistance of a sensor (load) can be calculated from the sensor current consumption. Afterwards, the presence of the sensor can be simulated using a (simple) resistor.

The simulation of the sensor signal can be realized using a waveform generator, an analog circuit, a micro-controller or a combination of them, depending on the signal characteristics.

4.5. Diagnostics

Finally, to test the reference system completely detached from the vehicle, it is necessary to know how the diagnosis communication works in order to check the fault memory and to read internal sensor information of the ECU (e.g. for temperature).

First, the applied protocols for transport and application layer must be identified. Often, standardized communication protocols for ECU diagnostics are used (e.g. ISO TP, KWP2000 or UDS). In some cases OEMs use proprietary self-developed keyword protocols (e.g. KWP1281). Thus, it is more difficult to establish a

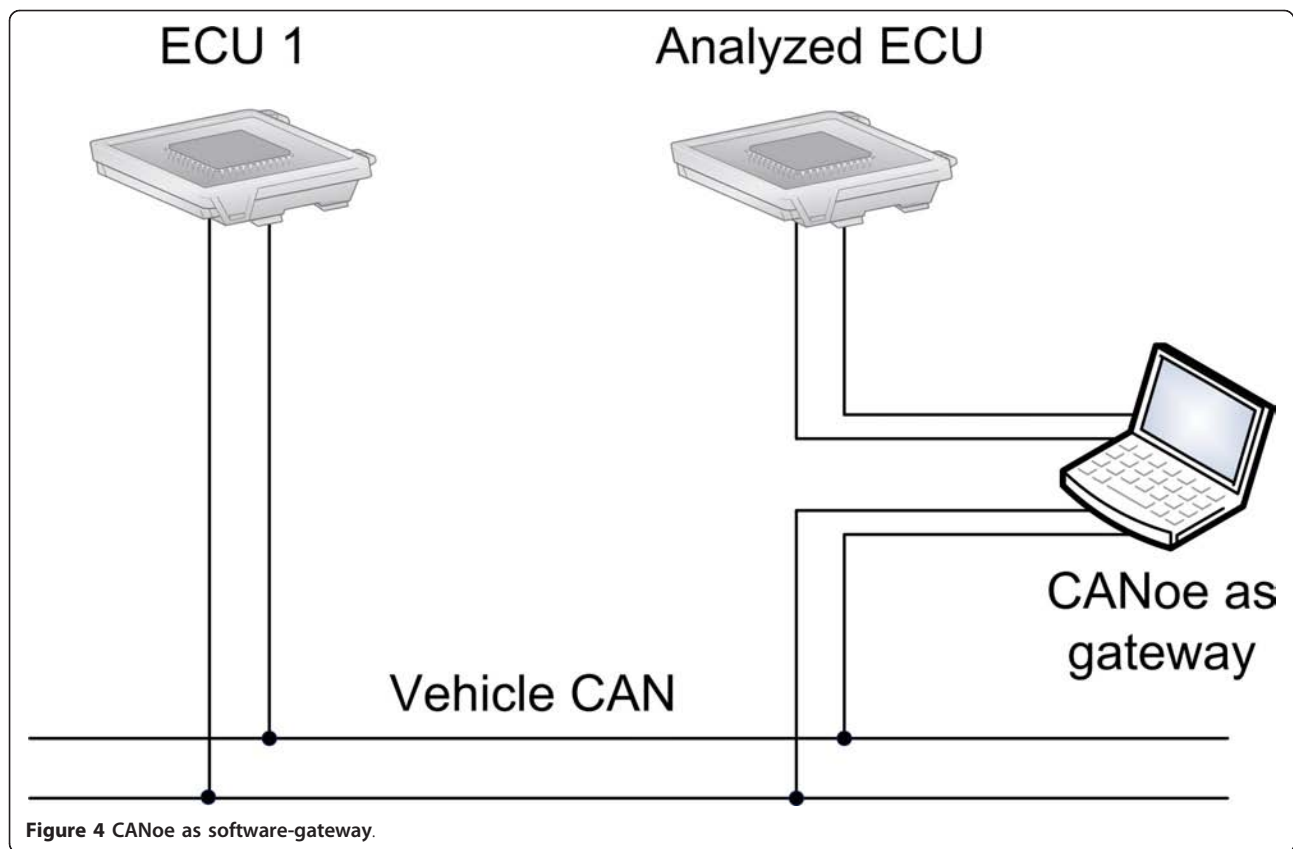


Figure 4 CANoe as software-gateway.

diagnosis connection to the reference system because the protocol specification is unknown to the remanufacturer. Hence, a detailed analysis of the CAN or K-Line communication during a diagnosis session is essential. Sophisticated reverse engineering capabilities are necessary in order to analyze, understand and recreate such a diagnosis communication. The message IDs, used for the communication, must be investigated independently by observing the diagnosis communication with CANoe. If the CAN IDs and protocols are known, the diagnose communication can be reproduced for example in CANoe using the CAPL environment.

After a remanufacturing company has accomplished all mentioned steps for the reference system, it is able to operate this system detached from all analog (sensor signals) or digital (CAN) inputs.

Finally, a test bench can be developed for entrance and final testing in series production scale.

5. Example: Remanufacturing of an Electro Hydraulic Power Steering (EHPS) Pump

An electro hydraulic power steering pump is a rotating oil pump driven by an electro motor. The pump converts electric power to hydraulic power. The hydraulic power is used to reduce the force the driver needs to steer the car. Most steering assistance is needed at low

driving speeds, maybe for parking, which makes it necessary that the EHPS pump has information about the actual driving speed. That information is communicated via CAN-Bus.

The following six steps describe the reverse engineering process on the basis of an EHPS pump that is used in a VW Polo which is seen in Figure 5.

5.1. Physical Analysis and Electrical Wiring of the EHPS

At the beginning, the EHPS has to be perceived as a black box with inputs and outputs. Because of the mechanical design and the general function of a hydraulic power steering, the output can be determined as the flow rate of the fluid [20]. The inputs are composed of an information about the internal combustion engine state (running or not running) and direct or indirect information about the necessary oil flow rate.

To get a first overview about the electrical connections of the device, a reference system (in this case the EHPS of the VW Polo - see Figure 6)) was completely disassembled. Large connector pins were good indicators for the general power supply by reason that the power consumption of the electric motor is supposed to be high. The ground pin of this connector was found by searching for a direct linkage between those pins and the ground plate of the circuit board. The other cable



Figure 5 Examination of the CAN Reman test vehicle.

on the connector is the positive power supply. At this point, the connection of the steering angle sensor, which is directly mounted on the steering shaft, was disregarded. The third connector contained three cables. Two of them were twisted in the following cable harness. That was a perfect indication for CAN cables. The CAN-high cable rises from 2.5 V to 3.5 V and the CAN-low cable falls from 2.5 V to 1.5 V during active communication. When operating the vehicle, the last cable was on 12 V level and therefore it was assumed to be the signal for “ignition on”. At this point the electrical analysis of the device was completed.

5.2. Vehicle Network Topology

On the example of the VW Polo EHPS, all relevant ECUs for operating the DUT have to be in the same CAN-bus network (Figure 7). Unfortunately, the CAN bus is not linked to the on-board diagnosis (OBD) connector of the test vehicle, whereas usually selected CAN bus data is also accessible through this connection. Therefore, the CAN wires in between of the EHPS and

the rest of the vehicle were separated in order to get access to this network for further investigations.

Assigning single messages/IDs to ECUs has simply been done by disconnecting single ECUs and locating missing messages/IDs. By a parallel readout of the internal fault memory of the DUT, relevant ECUs or single messages have been found.

5.3. CAN Bus Communication Investigations

This step can always be split into two parts. The first is the analysis of the communication in order to filter out and understand the relevant messages for the EHPS sent by other ECUs. The second is the simulation of the necessary CAN communication, which is called “rest-bus” in the following.

First, the start signal, transmitted to the EHPS via CAN bus, must be discovered as described in step 2. Therefore, a recording of the in-car CAN communication was made at a stationary test with well defined and reproducible conditions. After that, the recording was replayed to the test device outside the car and it started



Figure 6 Pins of the EHPS of the VW Polo.

its operation. Next, CAN messages were successively filtered out until the motor of the test device stopped. Hence, the last filtered message contained some kind of a start signal. Having performed in depth analyses, this signal was identified to be the RPM signal of the internal combustion engine. In order to eliminate or to find other input parameters, the same study was carried out using a recording of a real-road test. It was found that the vehicle speed is another input parameter for the EHPS.

Second, required input parameters were simulated with CANoe. Using a third party diagnosis garage tester (Bosch KTS 650), it was discovered that the fault memory of the external EHPS can only be erased when at least the presence of the missing messages of the in-car communication is simulated, too. This simulation of messages with and without data content is called restbus.

At this point the EHPS can completely be operated outside the car, but with a real steering angle sensor.

5.4. Simulation of Sensors

In order to operate the EHPS in a completely simulated environment, the angular velocity sensor had to be simulated.

Analog to step one, VCC and GND were identified on the sensor terminal using a multimeter. The third cable transfers the information about the angular velocity of the steering wheel. This signal was analyzed using an oscilloscope (Figure 8) and identified as a pulse width modulated signal. This signal was simulated by a

waveform generator. Furthermore, the sensor presence had to be emulated by a simple 600 Ω resistor matching the power consumption of the original sensor.

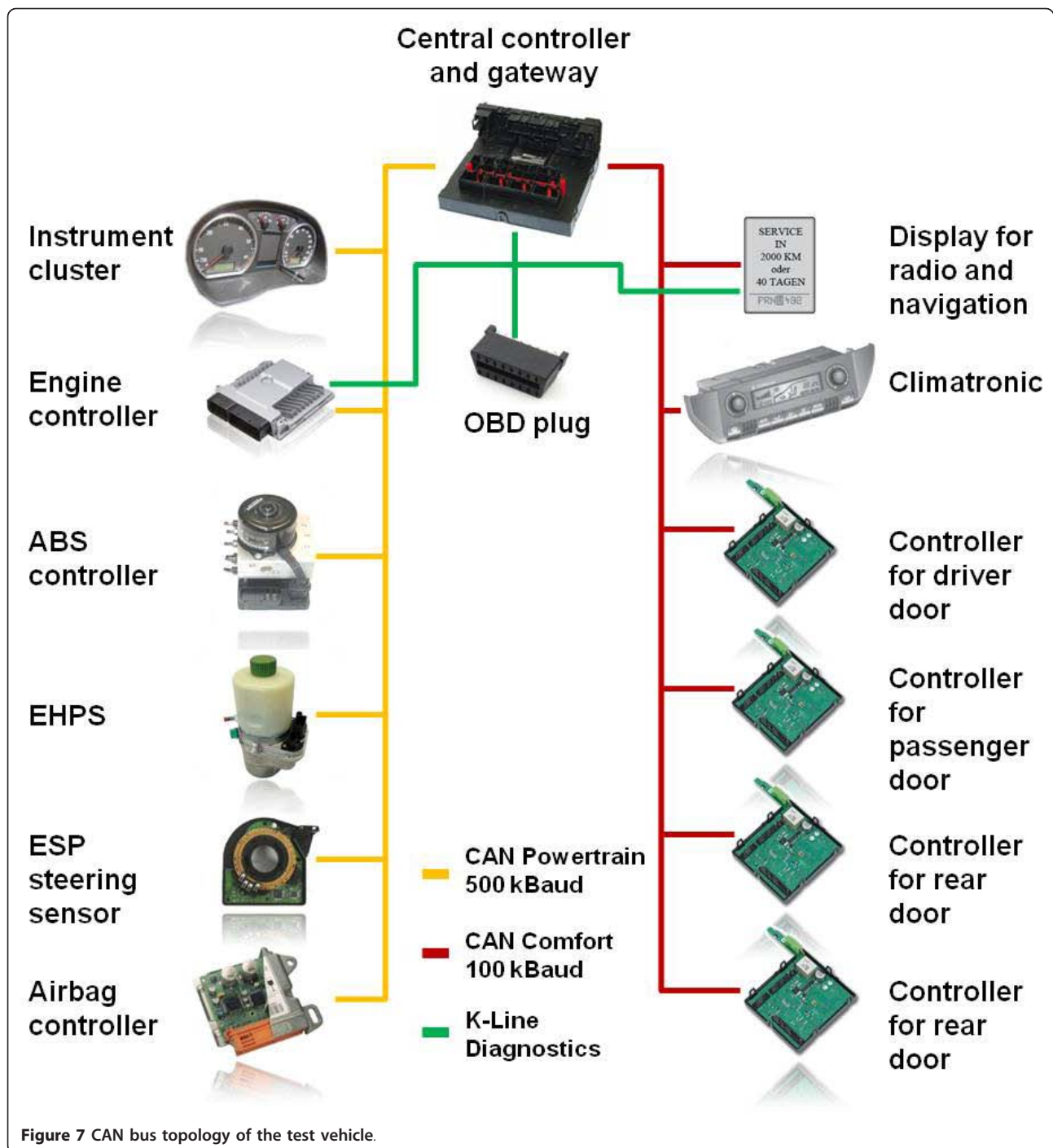
5.5. Diagnostic Functions of the Device

Most devices, including the present EHPS, can be diagnosed over CAN-bus with an external diagnosis garage tester. This tester can, as mentioned above, directly communicate with ECUs using a transport and a keyword protocol. The protocols are only partially defined and the communication differs from brand to brand tremendously. Therefore, the most efficient way to understand how e.g. the fault memory can be erased is to erase the fault memory with one of those testers and to try projecting the sequence onto known standards. In the present case, it were the standards KWP1281 and TP1.6. Even though the understanding of the diagnosis communication was very time-consuming, it was possible to erase and read the fault memory, to read the internal sensor data or duty cycles, to parameterize the device for different car models or even to completely reprogram the software.

Finally, all functions were implemented in CANoe using CAPL which can be controlled by a graphical user interface (GUI).

5.6. Operation Range

At last, the correlations between input and output values were determined in detail. For this reason, the



input parameters angular velocity, vehicle speed, RPM and the outputted oil flow rate were recorded simultaneously.

In this case the RPM signal only started the EHPS and was disregarded for the measurement. The vehicle speed was found in a particular message on the CAN bus as figured out in step 3. The angular velocity value is part of the sensor data provided by the EHPS in a diagnosis

communication session as mentioned in step 5. The resulting oil flow rate was measured by installing an oil flowmeter to the low pressure side of the EHPS in the test vehicle. This flowmeter generates a frequency modulated signal which was converted to a CAN message by a microcontroller and broadcasted to the local in-car CAN network in a separate CAN message. Finally, all necessary input and output values were

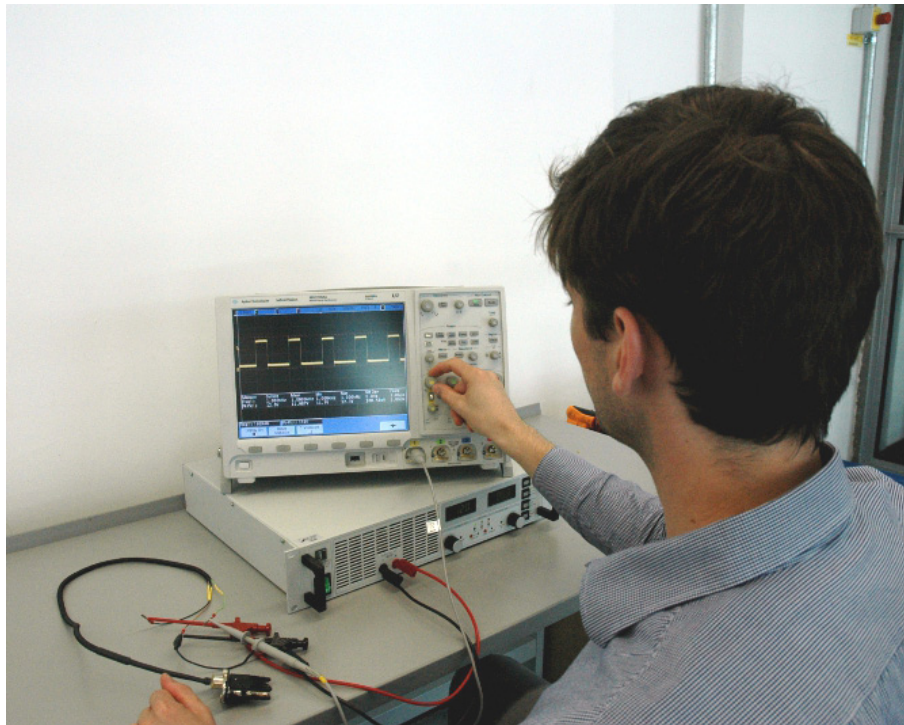


Figure 8 Measuring the sensor signal.

recorded from the CAN network time simultaneously using CANoe. Figure 9 depicts the flow rate of the steering oil as a result of vehicle speed and angular velocity, measured in a real-road test.

5.7. Practicability of the results

For further mechatronic systems an analysis time of 2 days to 2 month is required, depending on the system complexity. To give some examples for the time required: 2 days for example for another EHPS pump in another VW (each model needs new analyses), 5 days for another EHPS pump in different brand, 1 month for an absolutely new mechatronic system with medium complexity and 2 month or longer for a very complex mechatronic system like an automatic gear box. The costs for the analyses are splitted in the fix costs for the hard- and software of about 40.000 Euro and the costs for the employees for the days they work on. The reliability and safety of a remanufactured mechatronic system is in the same level compared with a new system. A mandatory regulation about standardization of the signals would decrease the costs significantly.

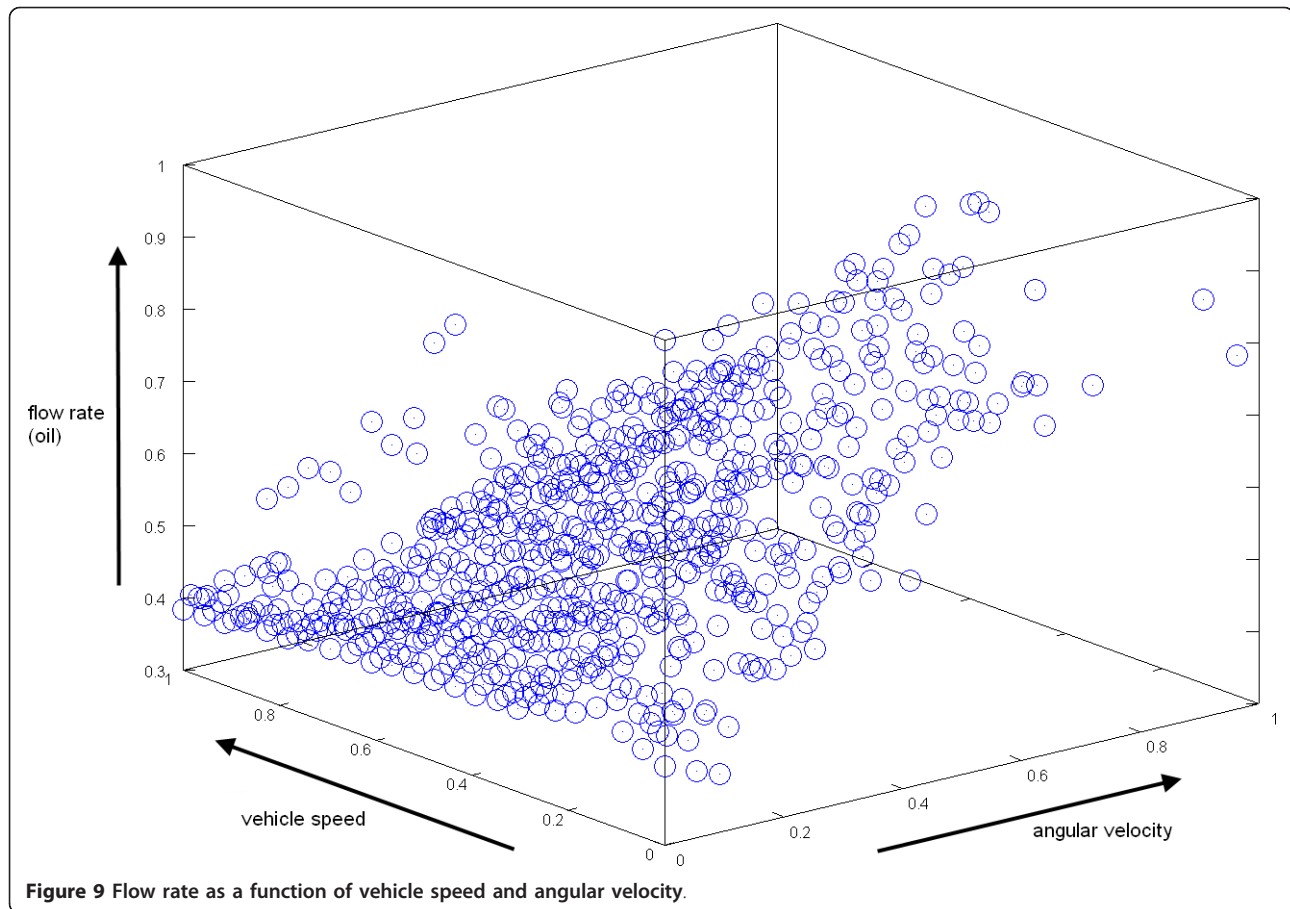
6. Conclusion

A still increasing number of mechatronic and electronic systems is built into today's vehicles. In the future, even more of these systems will be introduced to the cars as

a result of increasing demand for comfort, safety and reduced fuel consumption. Remanufacturing of failing mechatronic systems offers a great opportunity for all, the OEMs and OEs which can save resources and provide spare parts over a long period of time without the demand of long time warehousing; the remanufacturing companies as they can make a growing new business with these systems; and the customers that are benefiting from cheaper, but as good as new, spare parts.

Progress is not possible without its challenges, but it is achievable. The increasing complexity and variety of mechatronic end electronic devices cannot be handled with traditional methodologies. Therefore, remanufacturing companies have to build up new reverse engineering knowhow, find methodological innovations and they need to develop new technologies, especially focusing on the tasks testing and diagnostics of automotive systems and their subassemblies. After having met these challenges, new remanufacturing steps, such as the initial test, can be established and increase the productivity of the remanufacturing businesses e.g. in terms of an automated identification of systems or automated electronic test.

The paper outlines challenges, possible solutions and technological progress for the reverse engineering process of mechatronic automotive systems that are communicating via CAN-bus. In addition to this, the reverse



engineering process is demonstrated on the example of an EHPS which is used in a VW Polo. Obviously, it was possible to completely understand the steering system of the VW Polo by reverse engineering. Now, it is possible to run and test the mechatronic system outside the car as well as to adopt the results for remanufacturing the system in series production scale. The same principle can also be applied to further automotive systems, so that everyone wins, regardless of perspective.

List of abbreviations

ABS: Anti-lock Breaking System; ATZ: Automobiltechnische Zeitschrift (title of an automotive and technical journal); CAN: Controller Area Network; CAPL: CAN Access Programming Language; CRV: Current Replacement Value; DUT: Device Under Test; EAS: Electro Assisted Steering; ECU: Electronic Control Unit; EHPS: Electro Hydraulic Power Steering; ESP: Electronic Stability Program; GND: Ground Connection; GUI: Graphical User Interface; PAS: Parking Assist System; IAM: Independent Aftermarket; ID: (CAN-bus) Identifier; MTZ: Motortechnische Zeitschrift (title of an engine related journal); OEM: Original Equipment Manufacturer; OPI: OEM Product-Service Institute; VCC: Positive Power Supply; VW: Volkswagen.

Acknowledgements

The research project "CAN REMAN" and the activities described in this paper have been financed by the German Federal Government Department for Education and Research (support code 16INE014). Nobody, beyond the mentioned author's, contributed materials essential for the study.

Authors' contributions

AB carried out the molecular genetic studies, participated in the sequence alignment and drafted the manuscript. JY carried out the immunoassays. MT participated in the sequence alignment. ES participated in the design of the study and performed the statistical analysis. FG conceived of the study, and participated in its design and coordination. All authors read and approved the final manuscript.

Authors' information

Dr.-Ing. Stefan Freiberger

Managing Engineer at:
Bayreuth University
Chair Manufacturing and Remanufacturing Technology and Fraunhofer Project Group Process Innovation
Chairman of the Mechatronics and Electronics Division of APRA (Automotive Parts Remanufacturers Association)
Consultant in the fields of: Remanufacturing, Material- and Energy Efficiency, Process Innovation in Production, Lean Management and Six Sigma
PhD thesis about: "Prüf- und Diagnosetechnologien zur Refabrikation von mechatronischen Systemen aus Fahrzeugen"; „Test and Diagnosis Technologies for Remanufacturing Automotive Mechatronic Systems".

M.Sc., Dipl.-Ing. (FH) Matthias Albrecht

Engineer and research assistant at
Bayreuth University
Chair Manufacturing and Remanufacturing Technology and Fraunhofer Project Group Process Innovation
Field of Activity: Research for remanufacturing of mechanical, electronic and mechatronic components.
Development of test and diagnosis methods for coupled mechatronic and electronic systems with CAN-bus. Transfer of developed technologies and test equipment to different systems and implementation of these systems in

remanufacturing companies. Development of industrial test equipment for mechatronic and electronic automotive components that is application-oriented and easy-to-use.

Dipl.-Ing. (FH) Josef Käufel

Research Engineer at:

Bayreuth University

Chair Manufacturing and Remanufacturing Technology and Fraunhofer

Project Group Process Innovation

Field of activity: Technologies for remanufacturing of mechanical, electronic and mechatronic components. Development of test and diagnosis methods for coupled mechatronic and electronic systems with CAN-bus. Transfer of developed technologies and test equipment to different systems and implementation of these systems in remanufacturing companies.

Competing interests

The authors declare that they have no competing interests.

Received: 30 November 2010 Accepted: 7 December 2011

Published: 7 December 2011

References

1. Freiberger S: **Finding profitable products for Remanufacturing.** *APRA Global Connection, Ausgabe Nr.6 Chantilly* 2010.
2. Steinhilper R, Rosemann B, Freiberger S: **Product and Process Assessment for Remanufacturing of Computer Controlled Automotive Concepts.** *13th CIRP International Conference on Life Cycle Engineering, Leuven, Belgium, May 31st - June 2nd 2006.*
3. Steinhilper R: **Automotive Service Engineering and Remanufacturing: New Technologies and Opportunities.** *15th CIRP International Conference on Life Cycle Engineering, Sidney, Australia, March 17th - 19th 2008.*
4. Freiberger S: **European Research Project "Major European reman project given the green light" Starts Now.** *ReMaTecNews 2/2009, RAI Langfords B. V./RAI Publishing House, Amsterdam 2009.*
5. Roddeck W: **Einführung in die Mechatronik.** B.G. Teubner Verlag/GWV Fachverlage GmbH, Wiesbaden, Germany; 3 2006.
6. Zimmermann W, Schmidgall R: **Bussysteme in der Fahrzeugtechnik.** Vieweg + Teubner/GWV Fachverlage GmbH, Wiesbaden, Germany; 3 2008.
7. Freiberger S, Steinhilper R, Heinrich A, Brüggemann D: **Failure Detection and Isolation through Infrared Thermal Imaging.** In *ReMaTecNews - Automotive Remanufacturing International. Volume 6.* RAI Publishing House, Amsterdam, Dezember; 2006.
8. Freiberger S, Steinhilper R, Stöber R, Fischerauer G: **How to remanufacture partially documented mechatronic systems.** *APRA Global Connection, Ausgabe 16, Chantilly* 2006.
9. Freiberger S: **Remanufacturing of Mechatronics and Electronics.** *APRA Mechatronics and Electronics Division, Harrisburg 2006* [http://www.apra-europe.org].
10. Freiberger S, Landenberger D, Wrobel S: **FMEA in der Refabrikationsindustrie - Erfassen, bewerten, vermeiden.** *Quality Engineering, Ausgabe 04/2006* Konradin Verlag, Leinfelden-Echterdingen; 2006.
11. Freiberger S, Rosemann B, Steinhilper R: **Design for Recycling and Remanufacturing of Fuel Cells.** *Proceedings Eco Design 2005: 4th International Symposium on Environmentally Conscious Design and Inverse Manufacturing, Tokyo 12. bis 14 2005.*
12. Freiberger S, Rosemann B: **State of the Art Application and End-of-Life of Fuel Cell Systems.** *Proceedings 9th International Congress for Battery Recycling, Como, 2. bis 4 2004.*
13. Johnson MR, Wang MH: **Economical evaluation of disassembly operations for recycling, remanufacturing and reuse.** *International Journal of Production Research* 1998, **36(12)**:3227-3252.
14. Seliger G, Hentschel C, Wagner M: **Disassembly Factories for Recovery of Resources in Product and Material Cycles, pp 56 - 67.** In *Life-Cycle Modeling for innovative Products and Processes, Proceedings on life-cycle modeling for innovative products and processes, Berlin, Germany, November/ December 1995.* Edited by: Jansen H, Krause F-L. Chapman 1995:.
15. Seliger G, Grudzien W, Zaidi H: **New Methods of Product Data Provision for a simplified Disassembly.** *Proceedings of the Life Cycle Design 99, Kingston, Kanada 1999.*
16. Westkämper E, Alting Arndt: **Life Cycle Management and Assessment: Approaches and Visions Towards Sustainable Manufacturing.** *CIRP Annals - Manufacturing Technology* 2000, **49(2)**:501-526.
17. Freiberger S: **Selected and Applied Test and Diagnosis Methods for Remanufacturing Automotive Mechatronics and Electronics.** In *Remanufacturing Automotive Mechatronics and Electronics.* Edited by: Fernand J. Weiland, Germany; 2008:.
18. Chikofsky EJ, Cross JH II: **Reverse Engineering and Design Recovery: A Taxonomy.** *IEEE Software, IEEE Computer Society* 1990, 13-17.
19. Cifuentes C, Fitzgerald A: **The legal status of reverse engineering of computer software.** In *Analys of Software Engineering. Volume 9.* Springer Netherlands; 2000:(1):337-351.
20. Freiberger S: **Prüf- und Diagnosetechnologien zur Refabrikation von mechatronischen Systemen aus Fahrzeugen.** *Dissertation, Reihe: Fortschritt in Konstruktion und Produktion, Band 6, Shaker Verlag, Aachen, März 2007.*
21. Haumann M, Köhler DCF: **Coping with complexity in remanufacturing.** *Rematec News* 9(3):32-33.

doi:10.1186/2210-4690-1-6

Cite this article as: Freiberger et al.: Reverse Engineering Technologies for Remanufacturing of Automotive Systems Communicating via CAN Bus. *Journal of Remanufacturing* 2011 1:6.

Submit your manuscript to a SpringerOpen® journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Immediate publication on acceptance
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com