Opponent's Report on Final Thesis (dissertation)

Dissertation topic

New design methodology - Using VHDL-AMS models to consider aging effects in automotive mechatronic circuits for safety relevant functions

Student: M. Eng. Gerhard Hofmann

A new methodology for design of safety relevant functions in automotive mechatronic circuits is proposed by the student in his dissertation. The new methodology uses computer simulation tools namely the VHDL-AMS language. The methodology is intended as an add-on of the current design processes of the mentioned safety relevant functions and is focused on improvement of the early project development phases. Improvement consists in consideration of the aging effects on functional safety thereby potential lack of design related to components aging in their life cycle can be eliminated for equipment which implement the safety relevant functions.

The student states that the current practice during design of the safety relevant functions in automotive mechatronic circuits is to examine the environmental effects when real equipment prototypes are validated. Whereas the new proposed methodology can enable to examine the aging effects from the early equipment design phases. Although this statement provides, to certain extent, reasons why the student dealt with the dissertation topic it can be stated that a clear and easy identifiable reason(s), why the current processes used to design the safety relevant functions in automotive mechatronic circuits are not sufficient and should be supplemented by the new methodology, is missing. The student mentions the reasons why to improve the current status separately in different parts of the dissertation and this fact leads to doubts if a reader understood well or did not omit the main author's arguments.

When certain uncertainty concerning reasoning, why to elaborate the dissertation topic, is omitted it can be stated that the dissertation has a contribution to the field of study and is original one. The student defines step by step the goals of the dissertation and specifies and substantiates logically by the consequential theoretical parts how the new methodology will look like and how it will be practically verified. As a part of the methodology proposal quite extensive theoretical analytic activity is focused also on description of the relevant standards which are related to realization of the safety relevant functions in automotive.

To verify practically the methodology the student selected quite simple case and focused on the aging effects concerning resistors. Among other things the student states that suitable formulas describing aging of the resistors are not available. Therefore one part of the dissertation describes results of the practical tests which were performed by the student to examine aging of 8 resistor samples. Unfortunately the dissertation does not contain results for all examined samples. This fact has a negative effect in the final parts of the dissertation where the student demonstrates application of the proposed method on two examples. In the first case the data acquired from the student's practical tests are used to create the resistor aging model. In the second case the data from previous investigation of another author is taken over. The formulas modelling resistor aging differ

significantly in the mentioned examples. As a consequence different outcomes are obtained when the formulas are applied to the same model case. However the student does not comment if his experiments with 8 different resistor samples helped him somehow to decide which formula corresponds better to reality. There is only a general statement in the dissertation that just availability of quality (credible) aging models is a limiting factor of the proposed methodology. And that in the current state the proposed methodology cannot replace the existing environmental validation procedures.

It can be stated from the opponent point of view that quite extensive theoretical preparation and new methodology proposal are not, in the final dissertation parts, balanced by more exhaustive evaluation of the achieved practical results and deeper discussion about the limits which are related to the new methodology - namely in the sense how quality of the models used to examine aging of the components can influence results obtained from the proposed methodology.

The dissertation is elaborated quite understandable and in a systematic way. On the level of the dissertation some grammar deficiencies, particular text format deficiencies and, unfortunately, also bad readability of some figures can be commented.

During the dissertation defence the student should explain the following questions:

1. How is evidenced that the existing processes used in automotive for design of the safety relevant functions are not sufficient?
2. From the student point of view how realistic is a possibility that quality (credible) validated aging models for components used in automotive will be obtained?
3. The student states in the dissertation that he deals with the end part of the bath-tub diagram for the failure rate. How is this fact/assumption evidenced? A comparison which would compare the required life time of the circuits for the safety relevant functions with the time when the bath-tub diagram changes from the part with constant failure rate to the wear out failures part is missing.

Student's publications are on the lowest acceptable level.

The submitted dissertation is recommended to be defenced.

Plzeň, 31st January 2019

Opponent: Karel Běneš
Výzkumný ústav železniční, a.s.
Technical manager of the subsystem Control-Command and Signalling

External Examiner's Report on the Doctoral thesis of Ph.D. student Gerhard Hofmann

A) Evaluation of the importance of the dissertation for the field

The automotive industry is currently influenced by four megatrends - the so-called CASE trends - where CASE stands for **c**onnected, **a**utonomous, **s**hared, and **e**lectrified. These megatrends are largely based on additional electronics. Particularly in the field of electrification and autonomous driving, mechatronics plays a major role because of an additional number of sensors and actuators. The resulting complexity requires additional effort to master it. In particular, the aspect of functional safety (see ISO 26262) is becoming more important. Among other things, this is taken into account by the fact that the relevant standard ISO 26262 is currently being revised and a 2nd edition has been published 2018.

For example, in the 2nd Edition an extension to buses, trucks and motorcycles took place. Also, a part about semiconductor has been added. However, the area of aging has not been explicitly dealt with, so the dissertation deals with a new area.

The ISO 26262 attempts to minimize systematic and random failures both during the development phase and during operation. The proposed methodology aims at improving early detection of systematic errors in the aspect of aging.

The methodology is a supplement to the existing processes and combines proven methods such as the failure mode and effect analysis (FMEA) and the hardware description language (VHDL-AMS) simulation to a new and meaningful methodology.

The benefits are primarily in early detection of systematic design failures, which can help to reduce future warranty cost or avoid redesign.

B) Comments on the procedure of the proposed solution, the methods used and the achievement of the intended objective

First the state of the art of the wide field reliability, aging, Functional Safety and simulation are described. Then G. Hofmann focus on the problem,

that in the automotive industry still validation qualification tests are performed in a late design phase to prove the function over lifetime. He suggests, that a new methodology should be derived to detect aging influences in an earlier design phase.

The new methodology combines input from the VDI 2221/2222 (general guideline for development), VDI 2206 (guideline for mechatronic development) and the ISO 26262 (road vehicle - Functional Safety for electric/electronic). It focuses on an early development phase and uses only the system design path of the V-Model.

The proposed methodology starts with the choice of a suitable safety-related function, continues with performing the Functional Safety activities according ISO 26262. After a technical safety concept is set up a failure mode and effect analysis is used to identify aging relevant hardware components – here the term "aging FMEA" is introduced. Further an VHDL-AMS model for the aging behavior is developed. The source for the aging relevant information can either be out of data sheets, scientific papers, field data or own measurements. The VHDL-AMS language is chosen in order to stay open to other physical disciplines in the car and this is a reasonable choice. Finally, the models are applied in the relevant electrical circuit and the simulation results are evaluated.

In the practical part the proposed methodology is demonstrated on a simplified function of the electronic throttle device for combustion engines (E-GAS). The work product of the Functional Safety activities including the safety goal of "prevention of unintended acceleration" for an ASIL B function is described. With the FMEA a critical component is identified. Different sources for the aging behavior of resistors are demonstrated, including own experiments which do not confirm older results of a paper. A VHDL-AMS model is used with ANSYS Simplorer. Two different models which represent the own measurements and the results of the paper are used in a simplified resistor bridge circuit to evaluate the throttle valve input signal. Here different scenarios are investigated and evaluated. The practical part is focused on demonstrating the methodology and therefore acceptable simplifying assumptions are chosen. In the evaluation it is concluded that the plausible check is capable of coping with the aging effects or additional plausible checks with absolute values. The applied example is understandable and logical.

C) Opinion on the results of the dissertation and the original concrete contribution of the dissertation submitter

The results of the dissertation show that the inclusion of aging effects already at the design stage represents a new and meaningful approach. In this respect, the goal of the dissertation was achieved. The work can thus make a valuable contribution to improving the reliability of safety-related systems. The experimental proof was indicated by a simple but practical example (ohmic resistance).

D) Statement on the systematic, clear, formal and linguistic level of the dissertation

The structure of the dissertation is clear and appropriate. The linguistic style is good. The quality of some pictures (resolution, sharpness, readability) should be enhanced for the published version of the thesis after the oral disputation.

E) Comments on the student's publications

G. Hofmann has published his research results sufficiently. He has published three IEEE-papers and presented his findings in other publications and at conferences. His publications can be regarded as reasonable and adequate.

F) Final Statement

With his work, Gerhard Hofmann has shown that he can independently work on an important technical research field in vehicle technology with current engineering methods, tools and application-oriented questions.
I recommend the Faculty of Electrical Engineering of the University of Pilsen to accept the dissertation of Mr. Hofmann.

Esslingen, 7.1.2018

(Prof. Dr.-Ing. J. Haag)

OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Prof. Ing. Georg Scharfenberg
Ostbayerische Technische Hochschule
Fakultät Elektro- und Informationstechnik
PO Box 120327
93025 Regensburg

Regensburg, december 19th, 2018

Examiner's Report

Doctoral thesis Ph.D. student Gerhard Hofmann

Cover of the thesis:

New design methodology- Using VHDL-AMS models to consider aging effects in automotive mechatronic circuits for safety relevant functions

The automotive industry is the global engine of economic growth. Development in the automotive industry is driven by the growing global demand for units, the need for greater functionality and the parallel efforts required to reduce energy and fuel consumption and to reduce pollutants while utilizing vehicles. This development will be accompanied by the conversion to new drive concepts and by social changes that require new business models in the direction of networked vehicles (big data) with new service tasks.

A global challenge is the number of 1.35 million annual road accident fatalities (WHO Global Status Report on Road Safety 2018). Modern automotive concepts must provide solutions to reduce the number of fatalities.

The automobile has developed into a mechatronic system, with most of the functions being implemented in software-supported electronics. The number of electronic control units (ECUs) has now significantly exceeded 50. This fact requires the networking of components in the vehicle combined with a high level of sensor technology and communication requirements.

Most of the electronic control units have to perform safety tasks. These tasks (active safety functions) combine with passive vehicle safety functions with the aim of protecting the vehicle occupants and road users outside the vehicle from serious damage in the event of an accident.

Evaluation of importance

Hazards in the environment of the automobile can be caused by malfunctions in the technology but in particular by wrong actions of the driver or other road users.

Incorrect decisions by the driver or other road users should be reduced and/or revealed in real time by available assistance functions. Active intervention of the vehicle system (braking, maintaining distance, counter-steering) is partly provided for.

Malfunctions that can occur in the electronic components (random failures) are detected by checks and coped with architectural measures for secured safety objectives of the defined safety functions. Diagnostic intervals, fault reaction times and an assigned "safe state" are defined for this purpose.

Systematic errors represent a considerable risk factor, which must be assumed throughout the entire life cycle from specification, design and production to decommissioning.

This dissertation refers to the field of functional safety and addresses the E/E/PE systems in the vehicle. E/E/PE systems are "electrical/electronic/ programmable electronic safety-related systems". Normative references to this are the international standard IEC 61508 as generic basic standard and the industry-specific automotive standard ISO 26262 which has been derived from IEC 61508. The automotive standard ISO 26262 provides specifications for safety-critical functions throughout the entire life cycle of a vehicle. The aim of these specifications is to ensure that the process to be controlled or monitored does not pose a hazard in the event of a malfunction when a safety function is required. The standard enables a systematic, risk-based approach to safety-relevant tasks in automobiles.

The core of this dissertation deals with an important part of the possible systematic errors that can occur due to aging.

The automotive standard ISO 26262 was first published in 2011. This issue explicitly does not deal with aging of hardware components. A standard is checked for topicality at the latest after five years. This check was also carried out for the ISO 26262 standard and is scheduled to be completed in 2018. The further development takes into account the increasing complexity of assistance systems, the use of highly integrated semiconductor components and the treatment of motorized two-wheeled vehicles.

Future challenges, which are not yet dealt with in the present ISO 26262:2018, concern the worldwide existing developments in the direction of autonomous driving in level 4 "fully automated" and level 5 "driverless" driving. With the implementation of autonomous driving, the

interception of a malfunction by a driver will no longer be necessary in the future and thus represents a decisive challenge to avoid this type of error, especially for systematic errors as the largest group of possible errors.

This is where the presented new model for the design methodology using VHDL-AMS comes in and provides a new way to systematically analyze the aging of components.

The current revision of the automotive standard ISO 26262 also explicitly addresses the problem of aging for the first time. General hints are mentioned which do not reach the depth of the design methodology presented in the dissertation.

In the following paragraphs three references of the automotive standard ISO 26262 are listed, which is currently in the output state DIS "Draft International Standard". All references can be found in the newly amended Part 11, which was published under the title "Guideline on application of ISO 26262 to semiconductors".

A) ISO DIS 26262-11:2016

Table 22 — Systematic dependent failures initiators due to environmental conditions

DFI examples	Measures to prevent dependent failures from violating the safety goal	Measures to prevent the occurrence of dependent failures during operation
Temperature Vibration Pressure Humidity / Condensation Corrosion EMI Overvoltage applied from external Mechanical stress Wear Aging Water and other fluids intrusion	Diversification of impact (e.g. clock delay between master & checker core, diverse master and checker core, different critical paths) Direct monitoring of environmental conditions (e.g. temperature sensor) or indirect monitoring of environmental conditions (e.g. delay lines used as dependent -failure sensors)	Fault avoidance measures (e.g. conservative specification / robust design) Physical separation (e.g. distance of the die from a local heat source external of the die) Adaptive measures to reduce susceptibility (e.g. voltage/operating frequency decrease) Limit the access frequency or limit allowed operation cycles for sub-parts (e.g. specify the number of write cycles for an EEPROM) Robust design of semiconductor packaging

B) ISO DIS 26262-11:2016

4.7.5.2 Verification of mitigation measures

This clause introduces exemplary methods to evaluate the effectiveness to control or avoid dependent failures. The methods can be based on:

- Analytical approach using known principles;

  EXAMPLE 1 Reference [4] and similar provide analytical approaches that can be used as a basis to evaluate the effectiveness of the provided safety mechanisms addressing dependent failures

- Pre-silicon simulation using documented test protocols to provide evidence of robustness against the identified DFI;

  EXAMPLE 2 Test protocols that allow simulation of clock or power supply disturbances, EMI simulations etc. The simulation can be based on different levels of abstraction (based on the fault model to be targeted) and use adequate fault injection techniques to produce the intended disturbance.

- Post-silicon robustness tests (e.g. EMI test, burn In studies, accelerated aging test, electrical stress tests); and

- Expert judgment supported by documented rationale.

A combination of measures can be used, e.g. references [24], [21] and similar provide a mix of analytical, fault injection and expert judgment based approaches that can be used as a basis to evaluate the effectiveness of the provided safety mechanisms addressing dependent failures.

C) ISO DIS 26262-11:2016

5.2.5 About avoidance of systematic faults during the development phase

Analogue and mixed signal components are developed based on a standardized development process.

The general requirements and recommendations related to hardware architecture and detailed design are defined in ISO 26262-5:2018, Clause 7.

The guideline in 5.1.9 applies to the analogue and mixed signal components well if:

- Table 30 is replaced by Table 40; and

- the usage of 3rd party validated macro blocks and to comply with each constraint and procedure defined by the macro core provider, if practicable, is restricted to hard cores only.

NOTE Wear and aging are considered during development with proper verification and validation procedures.

In summary, it can be stated that the dissertation on systematic errors that can be caused by aging focuses on an important core area and provides a proven method for analysis in the design phase.

As shown above, the automotive standard ISO 26262 explicitly recognizes the significance of this systematic error for the first time. However, no appropriate analysis methods for electronic components are mentioned.

Procedure of the proposed solution, the methods used and the achievement of the intended objective

The procedure in the dissertation combines the two VDI guidelines VDI 2221/VDI 2222 and VDI 2206 with the standard ISO 26262. The focus of the VDI 2221/VDI 2222 guidelines is a general method for the implementation of a systematic development and is divided into seven steps from the planning up to the validation of the development result. The guideline VDI 2206 provides a design methodology for mechatronics systems. This guideline supports three core approaches: the use of a general problem-solving cycle on the micro-level, application of the V-model and usage of predefined process modules. The sequential approach is derived from these core approaches, as described in Chapter 5.3 in six steps, and provides the rationale for simulation models.

Finally, the design methodology is adopted from the international automotive standard ISO 26262. The individual work steps are the item definition, the hazard and risk analysis, the definition of safety targets and the resulting derivation of the functional safety concept through to the technical safety concept.

The FMEA (Failure mode effect analysis) is chosen as the method for identifying the critical age-dependent hardware components.

Results of the dissertation and the original concrete contribution of the dissertation submitter

The result is a methodology that can be used for safety-relevant functions in the automotive sector in an early design phase. It considers aging effects on electronic components which are mapped in a simulation model. The proactive usage of a FMEA serves as an additional supplement to the existing validation methods of the functional safety standard ISO 26262.

To prove the applicability of the methodology, a simplified representation of the automotive functional system E-Gas is used, in which part of the safety-relevant sensor technology is subjected to an ageing simulation.

For this purpose, both data from existing papers or own measurements are used. The measurements are carried out with the aim of identifying ageing effects. The collected data were evaluated and mapped in a VHDL model. With the simulation of the VHDL model two scenarios could be considered. And it is also shown how easily different data sources (existing papers or own measurements) can be evaluated by the proposed methodology.

In scenario 1 the ageing of a single component is investigated, while in scenario 2 two components are subjected to ageing simultaneously.

The simulation results provide recommendations for the further development of a safety-relevant function.

Statement on the systematic, clear, formal and lingual level

The work is well organized and structured. After the basic part, the problem description follows. The derivation of the methodology is detailed, solution-oriented and comprehensible. The presented methodology is also discussed critically regarding benefits and limitation. With the example of the simplified EGAS function the proposed methodology is applied to prove the applicability. The practical part of the thesis serves to prove the applicability of the methodology. In the final analysis, the emphasis is placed that the methodology is a supplement to existing procedures and most beneficial in an early design phase. The thesis ends with an outlook on further research fields.

The work contains all directories, such as glossary, list of figures and tables and bibliography. Based on the contents, the structure of the work is recognizable und logical. The figures used are adequately and support the understanding of the text. Only the schematic of the multiplexer board is hard to read.

It was extensively and correctly cited by the harvard method. The literature consists of both standard works and conference contributions. Internet sources are explicitly marked and mostly refer to datasheets.

The English is in good quality and readable. It has to be considered that English is not the native language of the author.

The thesis itself is on an average quality level with a good structure and readable English.

Comments on the publications

The List of publication includes three IEEE papers, which were presented in the IEEE international conference of Applied Electronics. These papers deal with different aspects of Functional Safety, aging of Electronics and simulation with VHDL.

Further two other papers with new aspects of Functional Safety were published in German conferences and one of these papers was published in the magazine „Elektronik automotive" 03/2016.

The new methodology itself is turned in at the international Journal of automotive technology.

Statemement of the examiner

The complexity of the topic is high and the proposed methodology is acceptable and fulfills the standard requirements on a scientific work. The thesis provides a new approach for evaluating aging aspects in Functional Safety and provides a proactive methodology to be used as an additional complement to the existing validation methods of the functional safety standard ISO 26262.

I recommend the defense of this thesis at the state examination committee.

Questions to the thesis:

1. How was the methodology derived?
2. Why was VHDL-AMS chosen as simulation language?
3. What is the most benefit of the methodology?

Review protocol author:
Prof. emer. Ing. Georg Scharfenberg

OTH Regensburg- Ostbayerische Technische Hochschule Regensburg
Co-Partner in Func. Safety (www.las3-regensburg.de)
Dozent Master Applied Research
Dozent Master Autom. Electronics
Homepage: https://hps.hs-regensburg.de/scg39074/

Tel. +49 (0)941 943 - 1118 -1101
Email: georg.scharfenberg@oth-regensburg.de

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

Regensburg, 19.12.2018