CARL VON OSSIETZKY universität OLDENBURG

Fakultät II – Informatik, Wirtschafts- und Rechtswissenschaften
Department für Informatik

Reasoning on Domain Knowledge and Technical Standards to Support the Development of Safety-Critical Automotive Systems

– Extended Abstract –

Erweiterter Abstract der Dissertation
zur Erlangung des Grades eines
Doktors der Naturwissenschaften

von

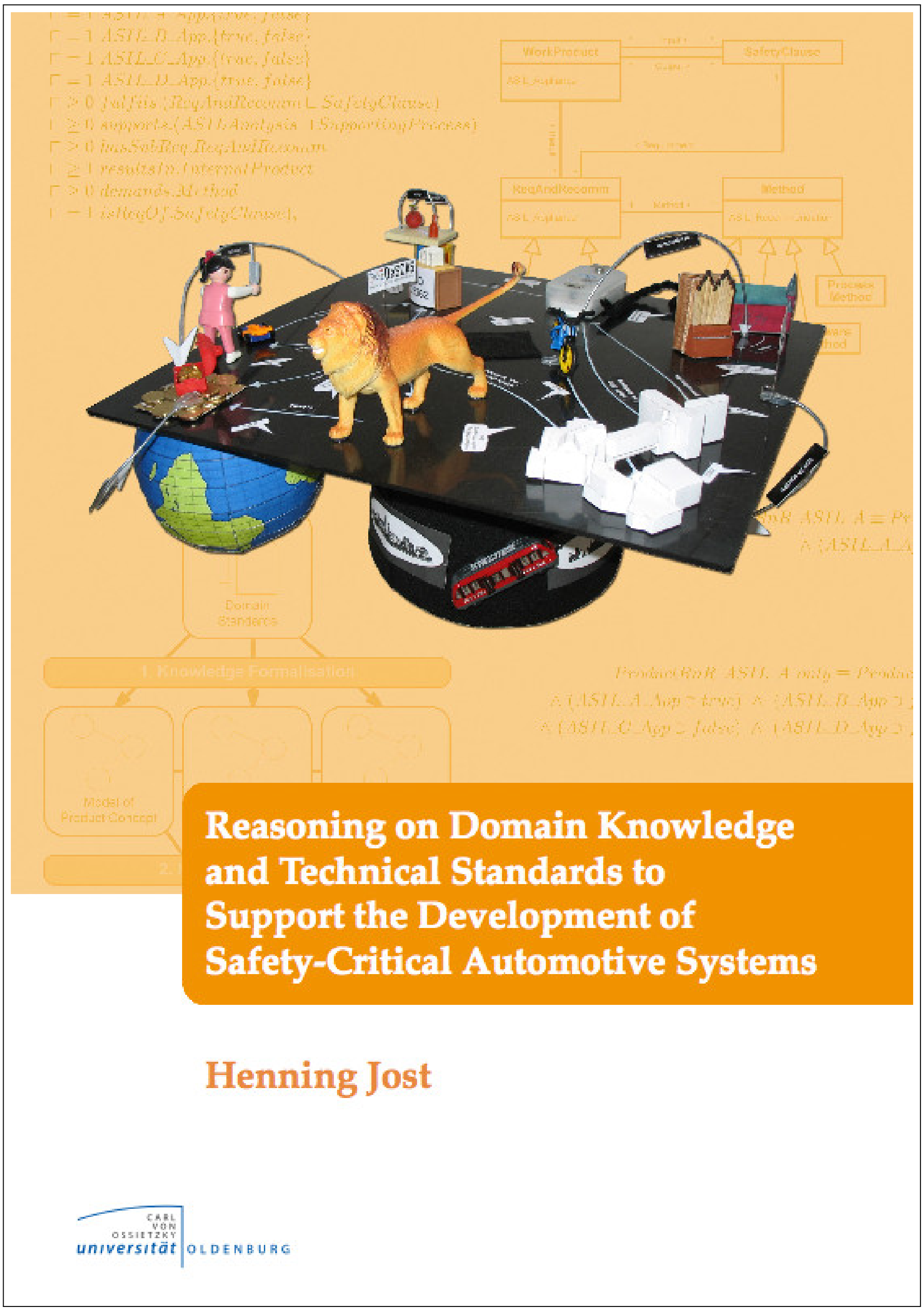
Dipl.-Inform. Henning Jost

Gutachter:

Prof. Dr. Werner Damm
PD Dr. Frank Köster

Ort/Datum der Disputation: Oldenburg, 18. Juni 2012

Die vollständige Dissertation ist erschienen als Buch
im **Verlag Dr. Hut** unter der **ISBN 978-3-8439-0570-1**.



http://www.dr.hut-verlag.de/9783843905701.html

Extended Abstract

The development of safety-critical systems in the automotive domain, e.g. *Advanced Driver Assistance Systems* (ADAS), is exposed to an increasing product and process complexity. Assisting the driver and automating driving manoeuvres imply a complex functionality which demands an elaborated design process to guarantee the functional safety of such systems. Representing the state of the art of the application domain, technical standards define complex development procedures and thus play a major role in automotive engineering activities. One example is the forthcoming introduction of the safety standard ISO 26262 for functional safety of road vehicles.

However, these standards comprise an informal representation in natural language text. As a consequence, inconsistencies and flaws regarding the use of technical terms as well as concerning the dependencies between the elements of the standard become evident and may lead to a misinterpretation of the standard's content. With respect to a specific system under development, manually extracting the relevant requirements and development activities out of the extensive standard is error-prone and time-consuming. This also refers to performing analysis methods imposed by the standards, especially the *Hazard Analysis and Risk Assessment* (HARA) of ISO 26262. Heavily relying on domain knowledge (e.g. environmental conditions or general system properties), such analysis methods can be objectified and automated as far as a generic (i.e. product independent within a specific domain) and computer-readable (thus formal) representation is available. Knowledge models specified by the *Web Ontology Language* (OWL) are appropriate to handle generic domain concepts and methods in a formal way. The challenge is to integrate the heterogeneous content of the various domain standards into homogeneous ontology models with a sufficient level of detail. Using OWL's logical base, reasoning engines can be applied to check the models' consistency (ensuring an unambiguous and consistent knowledge representation) as well as to perform knowledge deduction (for automating analysis techniques and extracting development measures).

Addressing the standard-compliant development of automotive ADAS, a proposed methodology comprises the modelling of automotive domain knowledge and related standards, especially ISO 26262, by means of OWL ontologies. These knowledge models are further processed to conduct a preliminary HARA that enables the automatic derivation of product-relevant measures compliant to the ISO standard, thus tailoring the reference process of ISO 26262 to a specific development. Illustrated by Figure 1.1, the proposed methodology of the thesis consists of the following individual steps that require or generate several artefacts:

1. **Knowledge Formalisation** – Technical *domain standards*, such as ISO 26262, or other domain guidelines are informal documents that contain but are not limited to domain requirements (e.g. a safety lifecycle) and domain concepts (e.g. generic system properties) in natural language. In a manual step, this domain knowledge is formalised by means of OWL ontology models providing a basis for further processing steps. Although this is a manual and time-consuming task, the modelled knowledge of the formal ontologies can later be reused in other projects of the application domain.

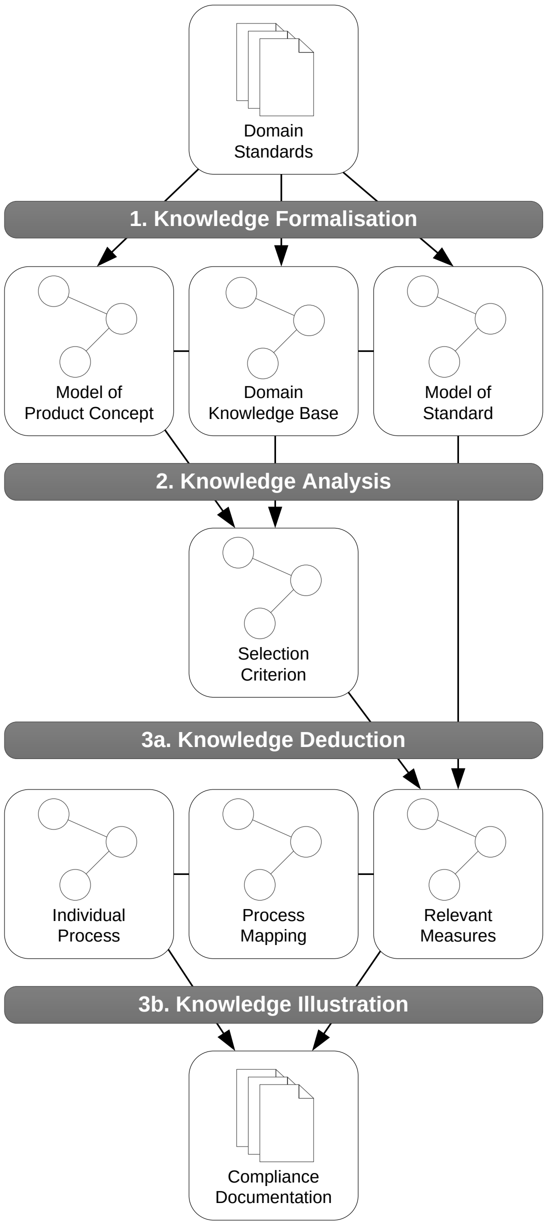


Figure 1.1: Proposed methodology of the thesis

At first, a *domain knowledge base* is established that comprises overall concepts of the application domain. In the case of the thesis, ADAS of the automotive domain (especially an *Adaptive Cruise Control* system) are regarded. The formalised concepts have to be generally applicable across various standards of the considered domain and usually refer to the glossaries of the domain standards or guidelines that specify the domain terminology. In addition, the concepts defined in specific terminological standards are integrated. Consequently, the supplementary parts of technical standards and other domain guidelines as well as terminological standards are typically evaluated to establish the domain knowledge base. In doing so, a terminological basis is created to substantiate the model of a specific standard. This specific *model of a standard* is constituted next.

Within the thesis, the safety standard ISO 26262 has been chosen exemplarily for the model of a specific standard as it will become one of the most important standards of the automotive domain. The ontology model of ISO 26262 focusses on the standard's process and product requirements, work products, methods, and the process model. The appendices and glossaries are not covered by the model of the specific standard as they have been integrated into the domain knowledge base before. Thus, the "main" parts of ISO 26262 are formalised by an OWL ontology.

As a last task of the knowledge formalisation step, a *model of the product concept* (i.e. an ADAS concept) has to be created. This ontology model comprises product requirements which can also be derived from a functional standard, such as ISO 15622, and which are related to the knowledge base concepts relevant for the ADAS under development.

2. **Knowledge Analysis** – Using the formal ontology models, analysis methods proposed by domain standards can be performed automatically by means of reasoning engines applied to the ontologies. This automatic step shall compute a *selection criterion* for deriving relevant measures from the standard model with respect to the system under development.

   Within the thesis, the HARA of ISO 26262 is considered that calculates the risk class of the regarded product. In terms of ISO 26262, this risk class is represented by the *Automotive Safety Integrity Level* (ASIL) which constitutes the required selection criterion. To sum up, the step of knowledge analysis provides the model-based approach of a preliminary risk analysis according to ISO 26262.

3a. **Knowledge Deduction** – By means of the calculated selection criterion, the *relevant measures* for the regarded system can be automatically inferred from the model of the standard as ISO 26262 classifies its measures according to the ASIL. The ASIL-related process and product requirements, work products, and methods of ISO 26262 are linked to the ISO's process steps so that a reference process compliant to ISO 26262 can be obtained, tailored to the system under development.

   The ISO-compliant reference process shall be combined with an *individual process* that represents a company-specific process model. The individual process has to be available as an OWL ontology as well. Within the thesis, the DeSCAS process model demonstrates the company-specific process due to its formal base. A *process mapping* (in terms of an OWL ontology) connects the relevant measures with the individual process by relating process elements of the tailored ISO process to corresponding elements of the DeSCAS process model. At this point of the methodology, the thesis is embedded into the work of the DeSCAS project[1] and the PhD thesis *Zur interdisziplinären Entwicklung sicherheitskritischer Assistenz- und Automationssysteme im Automobil*[2] of Jan Gačnik (2012) where the DeSCAS process model and its further processing have been elaborated.

3b. **Knowledge Illustration** – The qualification of ADAS is usually accomplished in a document-oriented manner. Reusing the traceability provided during the *Knowledge Analysis* and *Knowledge Deduction* step, *compliance documentation* can be automatically generated in

[1] `http://www.descas.org/`
[2] `http://www.digibib.tu-bs.de/?docid=00043460`

order to support qualification and certification activities. Within the thesis, HTML documentation will export the tailored and mapped development process applicable for the regarded system under development by using the DeSCAS prototype toolchain developed in the thesis of Jan Gačnik (see above). This documentation may demonstrate that the standard's measures have been integrated into the product development, thus implying standard compliance.

All in all, the proposed methodology provides an integrated approach for supporting the standard-compliant development of automotive ADAS. As the domain knowledge base of the *Knowledge Formalisation* provides a practicable fundament of modelled domain concepts to be used by the other knowledge models, its completeness and level of detail heavily affects the results of the subsequent *Knowledge Analysis* and *Knowledge Deduction*. For this reason, the knowledge base shall be regarded as an evolving expert system that can be easily enhanced by further domain concepts necessary to detail the examination of a (new) automotive system. This aspect is supported by using open ontology models. The model of a specific standard mainly covers the composition and the elements of ISO 26262 as well as the relations of the standard's elements instead of formalising the content of the standard's requirements. Thus, an objective modelling of ISO 26262 can be achieved by directly representing the structure of the standard. Concerning the *Knowledge Analysis*, the model-based approach of the risk analysis of ISO 26262 builds upon the knowledge base (especially a generic hazard list for automotive systems) so that the analysis results depend on the quality of the modelled domain knowledge available in the knowledge base. The analysis results can be validated by evaluating the traceability information provided by the related ontology models. These traceability information can further be used for validating the process derivation of the *Knowledge Deduction* step. The process itself is assessed by checking for executability using consistency checks and model checking as well as by showing compliance to the underlying standard. Finally, *Knowledge Illustration* summarises the obtained results in a comprehensible form for demonstrating standard compliance.

The appliance of open OWL ontologies supports reuse and easy enhancement of the knowledge modelling. The high complexity in reasoning on the OWL models can be counteracted by separating the ontology content and applying rule or query languages (such as SWRL and SPARQL) to the OWL ontologies instead of complex OWL axioms. However, long computation times in reasoning do not necessarily obstruct the appliance of the proposed methodology as real-time criticality is not an issue when conducting the methodology.

Finally, the proposed methodology improves the efficiency in the development and qualification of safety-critical systems by reducing development times via automated analyses and process tailoring in contrast to manually accomplished development tasks. Further, the manageability of demanded standards (e.g. ISO 26262) and applicability of the standard's analysis methods (e.g. a preliminary HARA) are also improved by reasoning on the ontology models. Thus at an early stage of development, a concept of a (new) automotive system can be assessed in terms of the development effort to be expected. On the other hand, it might happen that the development effort is rather shifted to other development activities than really reduced. The inherent complexity, high modelling effort and maintenance of the OWL ontologies as well the continuous examination of modelling results may decrease the saved development effort that has been achieved by means of the knowledge models. However, if a high level of reuse of the ontologies is enabled, the benefit of the thesis's approaches will become evident. For this purpose, the knowledge models have to be developed in such a way that they can be applied to many different classes of automotive systems.

Acknowledgements

Many people have supported and accompanied the writing of my PhD thesis so that I want to express my gratitude to them explicitly at this point.

First of all, I would like to thank Prof. Dr. Werner Damm and PD Dr. Frank Köster for being the supervisors of this thesis. Having equipped me with a lot of technical knowledge during my studies at university, Prof. Dr. Werner Damm offered me a position at his division that enabled me to work on this thesis. Apart from his valuable impulses and comments, I want to thank him for his trust in my work and for giving me the freedom and opportunity to develop my scientific ideas. Equally, I have to thank PD Dr. Frank Köster for his intensive supervision. Besides his technical feedback on the thesis's content, he has always accompanied my work from the start of elaborating basic ideas up to final considerations. As the speaker of the DeSCAS project, he has further participated in common publications that helped me in substantiating my ideas and results. Moreover, I am very grateful that Prof. Dr. Martin Fränzle took over the chair of my PhD commission since he has been heavily involved in the DeSCAS project and thus provided beneficial input to my thesis. Completing my PhD commission, Dr. Alfred Mikschl is one of the first persons of the SES group I have met during my studies so that he kindly represents the continuous factor of my time at the University of Oldenburg.

Then, I want to thank the further DeSCAS mates that supported my work on this thesis. First to name is Dr.-Ing. Jan Gačnik: Our fruitful discussions within and even beyond the scope of the DeSCAS project have enormously contributed to the results of this thesis. Hopefully, our successful collaboration will continue in the near future (*Mighty DeSCAS*). Further, a big thank you to Silke Köhler for discussing topics of my work and writing common publications that also helped me in elaborating my PhD objectives. This also applies to Daniel Beisel in terms of talking about automotive-related standards and the AGHL, as well as Ulf Noyer for discussing the computational complexity of OWL ontologies.

I also don't want to forget to mention the university and DeSCAS associates Jürgen Niehaus (especially concerning funding issues) and Prof. Dr.-Ing. Dr. h.c. mult. Eckehard Schnieder (due to the productive and trans-institutional cooperation). The Helmholtz association of German research centres deserves credit for funding the DeSCAS project and thus supporting the work on my PhD thesis. Further, I want to thank all my colleagues and friends at the University of Oldenburg and OFFIS.

Last but not least, I would like to sincerely thank my girlfriend Cora Stumpe and the entire Jost family for their enduring support in all respects, not only during the writing of this thesis. Thank you for always believing in me and giving me the strength to accomplish this work.

Dipl.-Inform. Henning Jost

List of My Publications

1. Henning Jost, Silke Köhler, and Frank Köster. Towards a Safer Development of Driver Assistance Systems by Applying Requirements-Based Methods. In *Proceedings of the 14th International IEEE Conference on Intelligent Transportation Systems (ITSC 2011)*, October 2011.

2. Jan Gačnik, Henning Jost, Frank Köster, and Martin Fränzle. The DeSCAS Methodology and Lessons Learned on Applying Formal Reasoning to Safety Domain Knowledge. In Eckehard Schnieder and Géza Tarnai, editors, *Proceedings of the 8th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT 2010)*, December 2010. Best Paper Award.

3. Henning Jost, Silke Köhler, Stefan Häusler, Jan Gačnik, Axel Hahn, Frank Köster, and Karsten Lemmer. Supporting Qualification – Safety Standard Compliant Process Planning and Monitoring. In *Proceedings 2010 IEEE Symposium on Product Compliance Engineering (PSES 2010)*, October 2010.

4. Henning Jost. Automating the Risk and Hazard Analysis via Generic Domain Concepts in Formal Ontologies. In Ben J.M. Ale, Ioannis A. Papazoglou, and Enrico Zio, editors, *Reliability, Risk and Safety – Back to the Future, European Safety and Reliability Conference (ESREL 2010)*, September 2010.

5. Jan Gačnik, Henning Jost, Frank Köster, Jürgen Rataj, Karsten Lemmer, Werner Damm, Martin Fränzle, and Eckehard Schnieder. DeSCAS – Formale Ontologien zur Verwebung von interdisziplinären Entwicklungsprozessen. In *AUTOMATION 2009*, number 2067 in VDI-Berichte, long version on CD-ROM. VDI Wissensforum GmbH, June 2009.

6. Jan Gačnik, Henning Jost, Daniel Beisel, Jürgen Rataj, and Frank Köster. DeSCAS Design Process Model for Automotive Systems – Development Streams and Ontologies. In *Safety-Critical Systems 2009*, number SP-2222 in Special Publications. SAE International, April 2009.

7. Jan Gačnik, Henning Jost, Daniel Beisel, and Frank Köster. DeSCAS – Design Process for the Development of Safety-Critical Advanced Driver Assistance Systems. In Géza Tarnai and Eckehard Schnieder, editors, *Proceedings of the 7th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT 2008)*, October 2008.

8. Henning Jost, Jan Behrens, and Ulf Schreier. Architekturbeschreibung mit der UML. In Ralf Reussner and Wilhelm Hasselbring, editors, *Handbuch der Software-Architektur*, chapter Architekturbeschreibung, pages 37-61. dpunkt Verlag, 2nd edition, 2008.