Anne Elisabeth Haxthausen - DTU Orbit (23/12/2017)

Anne Elisabeth Haxthausen

Organisations

Associate Professor, Department of Informatics and Mathematical Modeling
04/07/2003 → 07/04/2016 Former
ah@imm.dtu.dk
VIP

Computer Science and Engineering
25/02/2012 → 18/02/2013 Former
VIP

Software Engineering
25/02/2012 → 18/02/2013 Former
VIP

Associate Professor, Department of Information Technology
04/07/2003 → 07/04/2016 Former
ah@it.dtu.dk
VIP

Associate Professor, Department of Applied Mathematics and Computer Science
27/12/2012 → present
aeha@dtu.dk
VIP

Software Engineering
18/02/2013 → present
VIP

Publications:

A Domain-Specific Language for Generic Interlocking Models and Their Properties
State-of-the-art railway interlocking systems typically adhere to the product line paradigm, where each individual system is obtained by instantiating a generic system with configuration data. In this paper, we present a domain-specific language, IDL, for specifying generic behavioural models and generic properties of interlocking systems. An IDL specification of a generic model consists of generic variable declarations and generic transition rules, and generic properties are generic state invariants. Generic models and generic properties can be instantiated with configuration data. This results in concrete models and concrete properties that can be used as input for a model checker to formally verify that the system model satisfies desired state invariants. The language and a configuration data instantiator based on the semantics have been implemented as components of the RobustRailS tool set for formal specification and verification of interlocking systems. They have successfully been applied to (1) define a generic model and generic safety properties for the new Danish interlocking systems and to (2) instantiate these generic artefacts for real-world stations and lines in Denmark. A novelty of this work is to provide a domain-specific language for generic models and an instantiator tool taking not only configuration data but also a generic model as input instead of using a hard-coded generator for instantiating only one fixed generic model and its properties with configuration data.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, University of Bremen
Authors: Vu, L. H. (Intern), Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Pages: 99-115
Publication date: 2017

Host publication information
Title of host publication: Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification
Volume: 10598
Publisher: Springer

Series: Lecture Notes in Computer Science
Volume: 10598
ISSN: 0302-9743
Compositional Model Checking of Interlocking Systems for Lines with Multiple Stations

In the railway domain safety is guaranteed by an interlocking system which translates operational decisions into commands leading to field operations. Such a system is safety critical and demands thorough formal verification during its development process. Within this context, our work has focused on the extension of a compositional model checking approach to formally verify interlocking system models for lines with multiple stations. The idea of the approach is to decompose a model of the interlocking system by applying cuts at the network modelling level. The paper introduces an alternative cut (the linear cut) to a previously proposed cut (border cut). Powered with the linear cut, the model checking approach is then applied to the verification of an interlocking system controlling a real-world multiple station line.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering
Authors: Macedo, H. D. D. S. (Intern), Fantechi, A. (Intern), Haxthausen, A. E. (Intern)
Pages: 146–162
Publication date: 2017

Host publication information
Title of host publication: Proceedings of NASA Formal Methods Symposium 2017
Publisher: Springer
Series: Lecture Notes in Computer Science
Volume: 10227
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: NASA Formal Methods Symposium 2017, Moffett Field, United States, 16/05/2017 - 16/05/2017
Railway interlocking, Compositional verification, Model checking
DOIs: 10.1007/978-3-319-57288-8_11
Source: PublicationPreSubmission
Source-ID: 132971040
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Compositional Verification of Interlocking Systems for Large Stations

Railway interlocking systems are responsible to grant exclusive access to a route, that is a sequence of track elements, through a station or a network. Formal verification that basic safety rules regarding exclusive access to routes are satisfied by an implementation is still a challenge for networks of large size due to the exponential computation time and resources needed. Some recent attempts to address this challenge adopt a compositional approach, targeted to track layouts that are easily decomposable into sub-networks such that a route is almost fully contained in a sub-network: in this way granting the access to a route is essentially a decision local to the sub-network, and the interfaces with the rest of the network easily abstract away less interesting details related to the external world. Following up on previous work, where we defined a compositional verification method that started considering routes that overlap between sub-networks in interlocking systems governing a multi-station line, we attack the verification of large networks, which are typically those in main stations of major cities, and where routes are very intertwined and can hardly be separated into sub-networks that are independent at some degree. At this regard, we study how the division of a complex network into sub-networks, using stub elements to abstract all the routes that are common between sub-networks, may still guarantee compositionality of verification of safety properties.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering
Authors: Fantechi, A. (Intern), Haxthausen, A. E. (Intern), Macedo, H. D. D. S. (Intern)
Pages: 236-252
Publication date: 2017
Formal Development and Verification of Safe Railway Control Systems

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Software Engineering
Authors: Haixthausen, A. E. (Intern)
Publication date: 2017
Event: Poster session presented at Transport Summer Summit DTU 2017, Lyngby, Denmark.
Main Research Area: Technical/natural sciences
Electronic versions:
Transportday2017V2.pdf
Source: PublicationPreSubmission
Source-ID: 140539598
Publication: Research › Poster – Annual report year: 2017

Formal modelling and verification of interlocking systems featuring sequential release
In this article, we present a method and an associated toolchain for the formal verification of the new Danish railway interlocking systems that are compatible with the European Train Control System (ETCS) Level 2. We have made a generic and reconfigurable model of the system behaviour and generic safety properties. This model accommodates sequential release - a feature in the new Danish interlocking systems. To verify the safety of an interlocking system, first a domain-specific description of interlocking configuration data is constructed and validated. Then the generic model and safety properties are automatically instantiated with the well-formed description of interlocking configuration data. This instantiation produces a model instance in the form of a Kripke structure, and concrete safety properties expressed as invariants. Finally, using a combination of SMT based bounded model checking (BMC) and inductive reasoning, it is verified that the generated model instance satisfies the generated safety properties. Using this method, we are able to verify the safety properties for model instances corresponding to railway networks of industrial size. Experiments show that BMC is also efficient for finding bugs in the railway interlocking designs. Additionally, benchmarking results comparing the performance of our approach with alternative verification techniques on the interlocking models are presented.

General information
State: Published
Organisations: Software Engineering, Department of Applied Mathematics and Computer Science , University of Bremen
Authors: Vu, L. H. (Intern), Haixthausen, A. E. (Intern), Peleska, J. (Ekstern)
Pages: 91-115
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: Science of Computer Programming
Volume: 133
ISSN (Print): 0167-6423
Model Checking Geographically Distributed Interlocking Systems Using UMC

The current trend of distributing computations over a network is here, as a novelty, applied to a safety critical system, namely a railway interlocking system. We show how the challenge of guaranteeing safety of the distributed application has been attacked by formally specifying and model checking the relevant distributed protocols. By doing that, we obey the safety guidelines of the railway signalling domain, that require formal methods to support the certification of such products. We also show how formal modelling can help designing alternative distributed solutions, while maintaining adherence to safety.
Comparing formal verification approaches of interlocking systems

The verification of railway interlocking systems is a challenging task, and therefore several research groups have suggested to improve this task by using formal methods, but they use different modelling and verification approaches. To advance this research, there is a need to compare these approaches. As a first step towards this, in this paper we suggest a way to compare different formal approaches for verifying designs of route-based interlocking systems and we demonstrate it on modelling and verification approaches developed within the research groups at DTU/Bremen and at Surrey/Swansea. The focus is on designs that are specified by so-called control tables. The paper can serve as a starting point for further comparative studies. The DTU/Bremen research has been funded by the RobustRailS project granted by Innovation Fund Denmark. The Surrey/Swansea research has been funded by the SafeCap and the DITTO research projects granted by EPSRC and RSSB. The authors would like to thank Linh Hong Vu for providing the benchmark of scheme plans and the drawings of the track plans.
Compositional Verification of Multi-Station Interlocking Systems

Because interlocking systems are highly safety-critical complex systems, their automated safety verification is an active research topic investigated by several groups, employing verification techniques to produce important cost and time savings in their certification. However, such systems also pose a big challenge to current verification methodologies, due to the explosion of state space size as soon as large, if not medium sized, multi-station systems have to be controlled.

For these reasons, verification techniques that exploit locality principles related to the topological layout of the controlled system to split in different ways the state space have been investigated. In particular, compositional approaches divide the controlled track network in regions that can be verified separately, once proper assumptions are considered on the way the pieces are glued together.

Basing on a successful method to verify the size of rather large networks, we propose a compositional approach that is particularly suitable to address multi-station interlocking systems which control a whole line composed of stations linked by mainline tracks. Indeed, it turns out that for such networks, and for the adopted verification approach, the verification effort amounts just to the sum of the verification efforts for each intermediate station and for each connecting line.

Formal Development and Verification of Safe Railway Control Systems

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering
Authors: Haxthausen, A. E. (Intern)
Number of pages: 1
Publication date: 2016
Event: Poster session presented at Kick Off for Transport DTU, Kgs. Lyngby, Denmark.
Main Research Area: Technical/natural sciences
Electronic versions:
Transportday2016HandOut.pdf
Source: PublicationPreSubmission
Source-ID: 127608288
On the Feasibility of a Unified Modelling and Programming Paradigm

In this article, the feasibility of a unified modelling and programming paradigm is discussed from the perspective of large scale system development and verification in collaborative development environments. We motivate the necessity to utilise multiple formalisms for development and verification, in particular for complex cyber-physical systems or systems of systems. Though modelling, programming, and verification will certainly become more closely integrated in the future, we do not expect a single formalism to become universally applicable and accepted by the development and verification communities. The multi-formalism approach requires to translate verification artefacts (assertions, test cases, etc.) between different representations, in order to allow for the verification of emergent properties based on local verification results established with different methods and modelling techniques. It is illustrated by means of a case study from the railway domain, how this can be achieved, using concepts from the theory of institutions. This also enables the utilisation of verification tools in different formalisms, despite the fact that these tools are usually developed for one specific formal method.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, University of Bremen
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Pages: 32-49
Publication date: 2016

On the Use of Static Checking in the Verification of Interlocking Systems

In the formal methods community, the correctness of interlocking tables is typically verified by model checking. This paper suggests to use a static checker for this purpose and it demonstrates for the RobustRailS verification tool set that the execution time and memory usage of its static checker are much less than of its model checker. Furthermore, the error messages of the static checker are much more informative than the counter examples produced by classical model checkers.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, Technical University of Denmark
Authors: Haxthausen, A. E. (Intern), Østergaard, P. H. (Ekstern)
Pages: 266-278
Publication date: 2016
SaRDIn - A Safe Reconfigurable Distributed Interlocking

Current computer-based interlocking systems most often have a centralized design, with all logic residing in a single computer. Centralized interlockings are complex to design. Following the general trend in Cyber-Physical Systems, the SaRDIn (Safe Reconfigurable Distributed Interlockings) concept promises a radically simpler solution. The novelty of the SaRDIn concept is a fine-grained distribution of the logic over all processors deployed at the sensors and actuators along the track layout, i.e. within the track circuits, point machines, signals, etc. The advantages and drawbacks of such a solution are discussed, together with strategies to address the main challenges introduced by this concept, namely configuration, re-configuration and certification.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, University of Florence, CNR Institute of Informatics and Telematics, University of Twente, Fondazione Bruno Kessler, University of Surrey
Authors: Fantechi, A. (Intern), Gnesi, S. (Ekstern), Haxthausen, A. E. (Intern), van de Pol, J. (Ekstern), Roveri, M. (Ekstern), Treharne, H. (Ekstern)
Number of pages: 8
Publication date: 2016

Host publication information
Title of host publication: Proceedings of 11th World Congress on Railway Research (WCRR 2016)
Publisher: Ferrovie dello Stato Italiane
Main Research Area: Technical/natural sciences
Conference: 11th World Congress on Railway Research (WCRR 2016), Milan, Italy, 29/05/2016 - 29/05/2016
Source: PublicationPreSubmission
Source-ID: 125543800
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016
Formal Development and Verification of Railway Control Systems - In the context of ERTMS/ETCS Level 2

This dissertation presents a holistic, formal method for efficient modelling and verification of safety-critical railway control systems that have product line characteristics, i.e., each individual system is constructed by instantiating common generic applications with concrete configuration data. The proposed method is based on a combination of formal methods and domain-specific approaches. While formal methods offer mathematically rigorous specification, verification and validation, domain-specific approaches encapsulate the use of formal methods with familiar concepts and notions of the domain, hence making the method easy for the railway engineers to use. Furthermore, the method features a 4-step verification and validation approach that can be integrated naturally into different phases of the software development process. This 4-step approach identifies possible errors in generic applications or configuration data as early as possible in the software development cycle, and facilitates debugging/troubleshooting if errors are discovered. The proposed method has successfully been applied to case studies of the forthcoming Danish railway interlocking systems that are compatible with the European standardized railway control systems ERTMS/ETCS Level 2. Experiments showed that the method can be used for specification, verification and validation of systems of industrial size.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering
Authors: Vu, L. H. (Intern), Haxthausen, A. E. (Intern)
Number of pages: 276
Publication date: 2015

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English

Series: DTU Compute PHD-2015
Number: 395
ISSN: 0909-3192
Main Research Area: Technical/natural sciences

Electronic versions:
phd395_Hong_LV.pdf
Publication: Research › Ph.D. thesis – Annual report year: 2015

Formal Modeling and Verification of Interlocking Systems Featuring Sequential Release

In this paper, we present a method and an associated tool suite for formal verification of the new ETCS level 2 based Danish railway interlocking systems. We have made a generic and reconfigurable model of the system behavior and generic high-level safety properties. This model accommodates sequential release – a feature in the new Danish interlocking systems. The generic model and safety properties can be instantiated with interlocking configuration data, resulting in a concrete model in the form of a Kripke structure, and in high-level safety properties expressed as state invariants. Using SMT based bounded model checking (BMC) and inductive reasoning, we are able to verify the properties for model instances corresponding to railway networks of industrial size. Experiments also show that BMC is efficient for finding bugs in the railway interlocking designs.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, Universität Bremen
Authors: Vu, L. H. (Intern), Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Pages: 223-238
Publication date: 2015

Host publication information
Publisher: Springer
Editors: Artho, C., Csaba Ölveczky, P.
ISBN (Print): 978-3-319-17580-5
ISBN (Electronic): 978-3-319-17581-2

Series: Communications in Computer and Information Science
Volume: 476
ISSN: 1865-0929
Main Research Area: Technical/natural sciences
Model Checking and Model-based Testing in the Railway Domain

This chapter describes some approaches and emerging trends for verification and model-based testing of railway control systems. We describe state-of-the-art methods and associated tools for verifying interlocking systems and their configuration data, using bounded model checking and k-induction. Using real-world models of novel Danish interlocking systems, it is exemplified how this method scales up and is suitable for industrial application. For verification of the integrated HW/SW system performing the interlocking control tasks, a model-based hardware-in-the-loop testing approach is presented. The trade-off between complete test strategies capable of uncovering every error in implementations of a given fault domain on the one hand, and on the other hand the unmanageable load of test cases typically created by these strategies is discussed. Pragmatic approaches resulting in manageable test suites with good test strength are explained. Interlocking systems represent just one class of many others, where concrete system instances are created from generic representations, using configuration data for determining the behaviour of the instances. We explain how the systematic transition from generic to concrete instances in the development path is complemented by associated transitions in the verification and testing paths.

A SysML Test Model and Test Suite for the ETCS Ceiling Speed Monitor: Technical report, Work Package 4

In this technical report a detailed model description of a train control system application is given. The application consists of the ceiling speed monitoring (CSM) function for the European Vital Computer which is the main onboard controller for trains conforming to the European Train Control System specification. The model is provided in SysML, and it is equipped with a formal semantics that is consistent with the (semi formal) SysML standard published by the Object Management Group (OMG). The model and its description are publicly available on http://www.mbt-benchmarks.de, a website dedicated to the publication of models that are of interest for the model-based testing (MBT) community, and may serve as benchmarks for comparing MBT tool capabilities. The model described here is of particular interest for analysing the capabilities of equivalence class testing strategies. The CSM application inputs velocity values from a domain which could not be completely enumerated for test purposes with reasonable effort. We describe a novel method for equivalence class testing that – despite the conceptually infinite cardinality of the input domains – is capable to produce finite test suites that are exhaustive under certain hypotheses about the internal structure of the system under test.
A Domain-Specific Language for Railway Interlocking Systems
This paper presents a domain-specific language (DSL) for describing route-based interlocking systems which are compatible with European Train Control System ETCS Level 2. The abstract syntax and static semantics of the language are formally defined using the RAISE Specification Language (RSL). Furthermore, the paper describes an interlocking table generator (ITG) that generates automatically a well-formed interlocking table from a well-formed railway network layout. Experiments with the DSL and ITG using the RAISE tools and the C++ implementation show that the use of the DSL and ITG can increase the productivity and significantly reduce errors in the specifications of railway interlocking systems.

An Institution for Imperative RSL Specifications
The RAISE Specification Language (RSL) is a wide-spectrum specification language having a very complex semantics. This paper defines an institution for an imperative subset RSLI of RSL such that this subset can be given a much simpler semantics in terms of that institution. The subset allows model-oriented type definitions, declaration of state variables, axiomatic specification of values (including functions), and explicit function definitions. Functions may be imperative. The semantics of an RSLI specification is defined to be the loose semantics of a theory presentation consisting of a signature Σ and a set of sentences E that can easily be derived from the specification.
Applied Bounded Model Checking for Interlocking System Designs
In this paper the verification and validation of interlocking systems is investigated. Reviewing both geographical and route-related interlocking, the verification objectives can be structured from a perspective of computer science into (1) verification of static semantics, and (2) verification of behavioural (operational) semantics. The former checks that the plant model – that is, the software components reflecting the physical components of the interlocking system – has been set up in an adequate way. The latter investigates trains moving through the network, with the objective to uncover potential safety violations. From a formal methods perspective, these verification objectives can be approached by theorem proving, global, or bounded model checking. This paper explains the techniques for application of bounded model checking techniques, and discusses their advantages in comparison to the alternative approaches.

Automated generation of formal safety conditions from railway interlocking tables
This paper describes a tool for extracting formal safety conditions from interlocking tables for railway interlocking systems. The tool has been applied to generate safety conditions for the interlocking system at Stenstrup station in Denmark, and the SAL model checker tool has been used to check that these conditions were satisfied by a model of the relay circuits implementing the interlocking system at Stenstrup station.
Complete Model-Based Equivalence Class Testing for the ETCS Ceiling Speed Monitor

In this paper we present a new test model written in SysML and an associated blackbox test suite for the Ceiling Speed Monitor (CSM) of the European Train Control System (ETCS). The model is publicly available and intended to serve as a novel benchmark for investigating new testing theories and comparing the capabilities of model-based test automation.
tools. The CSM application inputs velocity values from a domain which could not be completely enumerated for test purposes with reasonable effort. We therefore apply a novel method for equivalence class testing that, despite the conceptually infinite cardinality of the input domains, is capable of producing finite test suites that are complete (i.e. sound and exhaustive) for a given fault model. In this paper, an overview of the model and the equivalence class testing strategy is given, and tool-based evaluation results are presented. For the technical details we refer to the published model and a technical report that is also available on the same website.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, University of Bremen, University of Hamburg
Authors: Braunstein, C. (Ekstern), Haxthausen, A. E. (Intern), Huang, W. (Ekstern), Hübner, F. (Ekstern), Peleska, J. (Ekstern), Schulze, U. (Ekstern), Vu, L. H. (Intern)
Pages: 380-395
Publication date: 2014

Host publication information
Title of host publication: Formal Methods and Software Engineering: Proceedings of the 16th International Conference on Formal Engineering Methods, ICFEM 2014
Publisher: Springer
ISBN (Print): 978-3-319-11736-2
ISBN (Electronic): 978-3-319-11737-9

Series: Lecture Notes in Computer Science
Volume: 8829
ISSN: 0302-9743

BFI conference series: International Conference on Formal Engineering Methods (5010548)
Main Research Area: Technical/natural sciences
Model-based testing, Equivalence class partition testing, SysML, European Train Control System ETCS, Ceiling Speed Monitoring
Electronic versions:
main.pdf
DOIs:
10.1007/978-3-319-11737-9_25
Source: PublicationPreSubmission
Source-ID: 100853350
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

FM-RAIL-BOK organizers' message
General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, University of Pretoria, McMaster University, Swansea University
Authors: Gruner, S. (Ekstern), Haxthausen, A. E. (Intern), Maibaum, T. (Ekstern), Roggenbach, M. (Ekstern)
Pages: XI-XII
Publication date: 2014

Host publication information
Title of host publication: 11th International Conference on Software Engineering and Formal Methods, SEFM 2013: Collocated Workshops: BEAT2, WS-FMDS, FM-RAIL-Bok, MoKMaSD, and OpenCert
Publisher: Springer
ISBN (Print): 978-3-319-05031-7
ISBN (Electronic): 978-3-319-05032-4

Series: Lecture Notes in Computer Science
Volume: 8368
ISSN: 0302-9743
BFI conference series: Conference on Software Engineering and Formal Methods (5000403)
Main Research Area: Technical/natural sciences
Computer Science (all), Theoretical Computer Science
Source: FindIt
Formal Modeling and Verification of Interlocking Systems Featuring Sequential Release

In this paper, we present a method and an associated tool suite for formal verification of the new ETCS level 2 based Danish railway interlocking systems. We have made a generic and reconfigurable model of the system behavior and generic high-level safety properties. This model accommodates sequential release - a feature in the new Danish interlocking systems. The generic model and safety properties can be instantiated with interlocking configuration data, resulting in a concrete model in the form of a Kripke structure, and in high-level safety properties expressed as state invariants. Using SMT based bounded model checking (BMC) and inductive reasoning, we are able to verify the properties for model instances corresponding to railway networks of industrial size. Experiments also show that BMC is efficient for finding bugs in the railway interlocking designs.

Formal Verification of the Danish Railway Interlocking Systems

In this paper, we present a method for formal verification of the new Danish railway interlocking systems. We made a generic and reconfigurable model of the behaviors and high-level safety properties of non-collision and nonderailment. This model accommodates sequential release – a new feature in the new Danish interlocking systems. Instantiating the generic model with interlocking configuration data results in a concrete model and high-level safety properties. Using bounded model checking and inductive reasoning, we are able to verify safety properties for model instances corresponding to railway networks of industrial size.

Formal Verification of the Danish Railway Interlocking Systems

In this paper, we present a method for formal verification of the new Danish railway interlocking systems. We made a generic and reconfigurable model of the behaviors and high-level safety properties of non-collision and nonderailment. This model accommodates sequential release – a new feature in the new Danish interlocking systems. Instantiating the generic model with interlocking configuration data results in a concrete model and high-level safety properties. Using bounded model checking and inductive reasoning, we are able to verify safety properties for model instances corresponding to railway networks of industrial size.

Formal Verification of the Danish Railway Interlocking Systems

In this paper, we present a method for formal verification of the new Danish railway interlocking systems. We made a generic and reconfigurable model of the behaviors and high-level safety properties of non-collision and nonderailment. This model accommodates sequential release – a new feature in the new Danish interlocking systems. Instantiating the generic model with interlocking configuration data results in a concrete model and high-level safety properties. Using bounded model checking and inductive reasoning, we are able to verify safety properties for model instances corresponding to railway networks of industrial size.
Applied Bounded Model Checking for Interlocking System Designs

In this article the verification and validation of interlocking systems is investigated. Reviewing both geographical and route-related interlocking, the verification objectives can be structured from a perspective of computer science into (1) verification of static semantics, and (2) verification of behavioural (operational) semantics. The former checks that the plant model – that is, the software components reflecting the physical components of the interlocking system – has been set up in an adequate way. The latter investigates trains moving through the network, with the objective to uncover potential safety violations. From a formal methods perspective, these verification objectives can be approached by theorem proving, global, or bounded model checking. This article explains the techniques for application of bounded model checking techniques, and discusses their advantages in comparison to the alternative approaches.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, Universität Bremen, Siemens
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern), Pinger, R. (Ekstern)
Pages: 21-26
Publication date: 2013

A Rigorous Methodology for Analyzing and Designing Plug-Ins

Today, GUI plug-ins development is typically done in a very ad-hoc way, where developers dive directly into implementation. Without any prior analysis and design, plug-ins are often flaky, unreliable, difficult to maintain and extend with new functionality, and have inconsistent user interfaces. This paper addresses these problems by describing a rigorous methodology for analyzing and designing plug-ins. The methodology is grounded in the Extended Business Object Notation (EBON) and covers informal analysis and design of features, GUI, actions, and scenarios, formal architecture design, including behavioral semantics, and validation. The methodology is illustrated via a case study whose focus is an Eclipse environment for the RAISE formal method’s tool suite.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, Technical University of Denmark
Efficient Development and Verification of Safe Railway Control Software

In this book, the authors present current research on the types, design and safety issues of railways. Topics discussed include the acoustic characteristics of noise in train stations; monitoring railway structure conditions and opportunities to use wireless sensor networks as tools to improve the monitoring process; hydraulic absorbers as dampers to dissipate the energy of oscillations in railway electric equipment; development of train fare calculation and adjustment systems using VDM++; efficient development and verification of safe railway control software; and evolution of the connectivity of the Portuguese broad gauge railway network (1948-2012).

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, Universität Bremen
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Pages: 127-148
Publication date: 2013

Host publication information
Title of host publication: Railways: Types, Design and Safety Issues
Publisher: Nova Science Publishers, Incorporated
Editors: Reinhardt, C., Shroeder, K.
ISBN (Print): 978-1-62417-139-0
Main Research Area: Technical/natural sciences
Electronic versions: Read only
Publication: Research - peer-review › Book chapter – Annual report year: 2013

Formal Development and Verification of Railway Control Systems

This paper presents work package WP4.1 of the RobustRails research project. The work package aims at suggesting a methodology for efficient development and verification of safe and robust railway control systems.

1 Project background and state of the art
Over the next 10 years all Danish railway signalling systems are going to be completely replaced with modern, computer based railway control systems based on the European standard ERTMS/ETCS [3, 4] by the Danish Signaling Programme [1]. The purpose of these systems is to control the railway traffic such that unsafe situations, like train collisions, are avoided. Central parts of these new systems consist of safety-critical software the functional correctness of which is one of the key requisites for a reliable operation of the traffics and in particular for the safety of passengers. Until now the development of railway control software has typically been done applying conventional methods where requirements and designs are described using natural language, diagrams and pseudo code, and the verification of requirements has been done by code inspection and non-exhaustive testing. These techniques are not sufficient, leading to errors and an ineffective and costly development process. The railway sector and in particular Rail Net Denmark (Banedanmark) therefore call for improved software development methods.

2 Original contribution and expected results
In order to avoid the problems mentioned in previous section, it is strongly recommended by the CENELEC standards [2] for railways to use formal (i.e. mathematical) logic and models for the unambiguous description of requirements and designs as well as for exhaustive verification as they give a higher assurance of safety compared to conventional methods. The use of domain-specific methods is another trend in software development, suggested to make the construction of software more efficient by generating the software automatically from domain-specific descriptions. Hence, to combine these two approaches is expected to be very attractive. The project will examine how domain-specific methods and formal methods can be combined and used for an efficient development and verification of new fail-safe systems. The
expected result is a methodology for using domain-specific, formal languages, techniques and tools for more efficient development and verification of robust software for railway control systems. The hypothesis is that domain-specific, model-based system development methods will lead to a more efficient construction with fewer errors and these errors will be found earlier in the system development.

3 Acknowlegments
This work is part of the research project RobustRails funded by the Danish Council for Strategic Research. The work is affiliated with a number of partners: DTU Compute, DTU Transport, DTU Management, DTU Fotonik, Bremen University, Banedanmark, Trafikstyrelsen, DSB, and DSB S-tog. More information about RobustRails project is available at http://www.dtu.dk/subsites/robustrails/English.aspx

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Software Engineering, University of Bremen
Authors: Vu Hong, L. (Intern), Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Number of pages: 1
Publication date: 2013
Event: Abstract from Strategisk forskning i transport og infrastruktur, Kongens Lyngby, Denmark.
Main Research Area: Technical/natural sciences
Electronic versions:
Pages_from_slot_10_2.pdf
Publication: Research - peer-review › Conference abstract for conference – Annual report year: 2013

Formal Development and Verification of Safe Railway Control Systems

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Software Engineering
Authors: Haxthausen, A. E. (Intern), Vu Hong, L. (Intern)
Number of pages: 1
Publication date: 2013
Event: Poster session presented at Danish Railway Conference 2013, Copenhagen, Denmark.
Main Research Area: Technical/natural sciences
Electronic versions:
Banekonference2013_wp41.pdf
Source: dtu
Source-ID: u::10127
Publication: Research - peer-review › Poster – Annual report year: 2013

The Overture Approach to VDM Language Evolution
The Overture Language Board (LB) has a strategic role in the development of the VDM-10 Languages, VDM-SL, VDM++ and VDM-RT, and deals in particular with Requests for Modifications (RMs) to the language. Such requests come usually from participants in the Overture project. This paper describes how the LB uses a well-defined process with several phases to deal with the RMs, from when they are requested until they are either rejected or accepted and implemented. The paper also gives an overview of language changes that have been accepted and implemented in the period April 2009 – June 2013.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Software Engineering
Authors: Battle, N. (Ekstern), Haxthausen, A. E. (Intern), Hiroshi, S. (Ekstern), Jørgensen, P. (Ekstern), Plat, N. (Ekstern), Sahara, S. (Ekstern), Verhoef, M. (Ekstern)
Pages: 8-15
Publication date: 2013

Host publication information
Title of host publication: Proceedings of the 11th Overture Workshop
Editors: Pierce, K., Hallerstede, S.
Main Research Area: Technical/natural sciences
Workshop: 11th Overture Workshop, Aarhus, Denmark, 28/08/2013 - 28/08/2013
VDM, Formal specification languages, Language design, Language modification process, The Overture Language Board
Source: Bibtex
Source-ID: urn:991531a4362013b4a7ddaac9cb48bb898
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013
Automated Generation of Safety Requirements from Railway Interlocking Tables
This paper describes a tool for extracting formal safety conditions from interlocking tables for railway interlocking systems. The tool has been applied to generate safety conditions for the interlocking system at Stenstrup station in Denmark, and the generated conditions were then checked to hold by the SAL model checker tool.

On the dimensions of software documents — An idea for framing the software engineering process.

Source: OAI-PMH
A Formal Approach for the Construction and Verification of Railway Control Systems
This paper describes a complete model-based development and verification approach for railway control systems. For each control system to be generated, the user makes a description of the application-specific parameters in a domain-specific language. This description is automatically transformed into an executable control system model expressed in SystemC. This model is then compiled into object code. Verification is performed using three main methods applied to different levels. (0) The domain-specific description is validated wrt. internal consistency by static analysis. (1) The crucial safety properties are verified for the SystemC model by means of bounded model checking. (2) The object code is verified to be I/O behaviourally equivalent to the SystemC model from which it was compiled.

General information
State: Published
Effective Development and Verification of Railway Control Software

This document presents a method for effective development of software for a product line of similar railway control systems. The software is constructed in three steps: first a specifications in a domain-specific language is created, then a formal behavioural controller model is automatically created from the specification, and finally the model is compiled into executable object code. Formal verification is performed automatically by tools at three levels: (1) the specification is checked to follow the rules of the domain, (2) the controller model is checked to ensure safety, and (3) the object code is verified to be a correct implementation of the controller model.

General information
State: Published
Organisations: Software Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern)
Publication date: 2011

Formal Development of a Tool for Automated Modelling and Verification of Relay Interlocking Systems

This paper describes a tool for formal modelling relay interlocking systems and explains how it has been stepwise, formally developed using the RAISE method. The developed tool takes the circuit diagrams of a relay interlocking system as input and gives as result a state transition system modelling the dynamic behaviour of the interlocking system, i.e. the dynamic behaviour of the circuits depicted in the diagrams. The resulting state transition system (model) is expressed in the SAL language such that the SAL model checker can be used to model check required properties of this model of the interlocking system. The tool has been applied to the circuit diagrams of Stenstrup station in Denmark and the resulting formal model has then been model checked to satisfy a number of required safety properties.

General information
State: Published
Organisations: Software Engineering, Department of Informatics and Mathematical Modeling, Technical University of Denmark
Authors: Haxthausen, A. E. (Intern), Kjær, A. A. (Ekstern), Le Bliguët, M. (Ekstern)
Pages: 118-132
Publication date: 2011
Towards a Framework for Modelling and Verification of Relay Interlocking Systems
This paper describes a framework currently under development for modelling, simulation, and verification of relay interlocking systems as used by the Danish railways. The framework is centred around a domain-specific language (DSL) for describing such systems, and provides (1) a graphical editor for creating DSL descriptions, (2) a data validator for checking that DSL descriptions follow the structural rules of the domain, (3) a graphical simulator for simulating the dynamic behaviour of relay interlocking systems, and (4) verification support for deriving and verifying safety properties of relay interlocking systems.

General information
State: Published
Organisations: Software Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern)
Pages: 176-192
Publication date: 2011

Host publication information
Publisher: Springer
ISBN (Print): 978-3-642-21291-8
ISBN (Electronic): 978-3-642-21292-5

Series: Lecture Notes in Computer Science
Number: 6662
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: Monterey Workshop, Redmond, USA, 01/01/2010
DOIs:
10.1007/978-3-642-21292-5

Links:
http://www.montereyworkshop.org/home.html
Source: orbit
Source-ID: 279351
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

An Introduction to Formal Methods for the Development of Safety-critical Applications
This report is a delivery to The Danish Government's railway authority, Trafikstyrelsen, as a part of the Public Sector Consultancy service offered by the Technical University of Denmark. The purpose of the report is to give the reader an insight into the state-of-the-art of formal methods. The reader is assumed to have some knowledge about software development, but not on formal methods. The background for the railway authorities’ interest in formal methods is the fact that during the next decade a total renewal of the Danish signalling infrastructure is going to take place. Central parts of the new systems will be software components that must fulfill strong safety requirements: in order to get the software certified at the highest Safety Integrity Levels of the European CENELEC standards for railway applications, the software providers are expected to use formal methods.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Software Engineering
Authors: Haxthausen, A. E. (Intern)
Number of pages: 32
Publication date: 2010

Publication information
Place of publication: Kgs. Lyngby, Denmark
Original language: English
Main Research Area: Technical/natural sciences
Formal methods
Electronic versions:
FormalMethodsNoteTS.pdf

Bibliographical note
This report is a delivery to The Danish Government’s railway authority, Trafikstyrelsen, as a part of the Public Sector Consultancy service offered by the Technical University of Denmark.

Relations
Modelling and Verification of Relay Interlocking Systems
This paper describes how relay interlocking systems as used by the Danish railways can be formally modelled and verified. Such systems are documented by circuit diagrams describing their static layout. It is explained how to derive a state transition system model for the dynamic behaviour of a relay system from such diagrams. Safety properties are identified and formalised as LTL formulae. Model checking is finally used to verify that a model satisfies the safety properties. The method is tested for an existing station in Denmark.

Towards a Framework for Modelling and Verification of Relay Interlocking Systems
This paper describes a framework currently under development for modelling, simulation, and verification of relay interlocking systems as used by the Danish railways. The framework is centred around a domain-specific language (DSL) for describing such systems, and provides (1) a graphical editor for creating DSL descriptions, (2) a validator for checking that DSL descriptions are statically well-formed, (3) a graphical simulator for simulating the dynamic behaviour of relay interlocking systems, and (4) verification support for deriving and verifying safety properties of relay interlocking systems. The paper also touches upon how such a framework can be developed using the RAISE Formal Method.
A Domain-specific Framework for Automated Construction and Verification of Railway Control Systems

The development of modern railway and tramway control systems represents a considerable challenge to both systems and software engineers: The goal to increase the traffic throughput while at the same time increasing the availability and reliability of railway operations leads to a demand for more elaborate safety mechanisms in order to keep the risk at the same low level that has been established for European railways until today. The challenge is further increased by the demand for shorter time-to-market periods and higher competition among suppliers of the railway domain; both factors resulting in a demand for a higher degree of automation for the development verification, validation and test phases of projects, without impairing the thoroughness of safety-related quality measures and certification activities. Motivated by these considerations, this presentation describes an approach for automated construction and verification of railway control systems.

Developing a Domain Model for Relay Circuits

In this paper we stepwise develop a domain model for relay circuits as used in railway control systems. First we provide an abstract, property-oriented model of networks consisting of components that can be glued together with connectors. This model is strongly inspired by a network model for railways made by Bjørner et.al., however our model is more general: the components can be of any kind and can later be refined to e.g. railway components or circuit components. Then we show how the abstract network model can be refined into an explicit model for relay circuits. The circuit model describes the statics as well as the dynamics of relay circuits, i.e. how a relay circuit can be composed legally from electrical components as well as how the components may change state over time. Finally the circuit model is transformed into an executable model, and we show how a concrete circuit can be defined, checked to be legal, and the reaction to an input can be simulated.
CASL, the Common Algebraic Specification Language

CASL is an expressive specification language that has been designed to supersede many existing algebraic specification languages and provide a standard. CASL consists of several layers, including basic (unstructured) specifications, structured specifications and architectural specifications; the latter are used to prescribe the modular structure of implementations. We describe a simplified version of the CASL syntax, semantics and proof calculus for each of these three layers and state the corresponding soundness and completeness theorems. The layers are orthogonal in the sense that the semantics of a given layer uses that of the previous layer as a "black box", and similarly for the proof calculi. In particular, this means that CASL can easily be adapted to other logical systems. We conclude with a detailed example specification of a warehouse, which serves to illustrate the application of both CASL and the proof calculi for the various layers.

General information
State: Published
Organisations: Software Engineering, Department of Informatics and Mathematical Modeling, Universität Bremen, University of Edinburgh, Warsawa University
Authors: Mossakowski, T. (Ekstern), Haxthausen, A. E. (Intern), Sannella, D. (Ekstern), Tarlecki, A. (Ekstern)
Publication date: 2008

Host publication information
Title of host publication: Logics of Specification Languages
Publisher: Springer
Editors: Bjørner, D., Henson, M. C.
ISBN (Print): 978-3-540-74106-0

Series: Monographs in Theoretical Computer Science. An EATCS Series
Number: XXII
Main Research Area: Technical/natural sciences

CASL
Links:
Source: orbit
Source-ID: 207245
Publication: Research - peer-review › Book chapter – Annual report year: 2008

Specification, proof, and model checking of the Mondex electronic purse using RAISE

This paper describes how the communication protocol of Mondex electronic purses can be specified and verified against desired security properties. The specification is developed by stepwise refinement using the RAISE formal specification language, RSL, and the proofs are made by translation to PVS and SAL. The work is part of a year-long project contributing to the international grand challenge in verified software engineering.

General information
State: Published
The Logic of the RAISE Specification Language
This chapter describes the logic of the RAISE Specification Language, RSL. It explains the particular logic chosen for RAISE, and motivates this choice as suitable for a wide spectrum language to be used for designs as well as initial specifications, and supporting imperative and concurrent specifications as well as applicative sequential ones. It also describes the logical definition of RSL, its axiomatic semantics, as well as the proof system for carrying out proofs. Finally, a case study illustrates specification and verification methods in RAISE.

General information
State: Published
Organisations: Software Engineering, Department of Informatics and Mathematical Modeling, United Nations University International Institute for Software Technology
Authors: George, C. (Ekstern), Haxthausen, A. E. (Intern)
Publication date: 2008

Host publication information
Title of host publication: Logics of Specification Languages
Publisher: Springer
Editors: Bjoerner, D., Henson, M. C.
ISBN (Print): 978-3-540-74106-0

Series: Monographs in Theoretical Computer Science. An EATCS Series
Number: XXII
Main Research Area: Technical/natural sciences
RAISE
Source: orbit
Source-ID: 207252
Publication: Research - peer-review › Book chapter – Annual report year: 2008

A Domain-oriented, Model-based Approach for Construction and Verification of Railway Control Systems

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Universität Bremen
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Pages: 320-348
Publication date: 2007

Host publication information
Title of host publication: Formal Methods and Hybrid Real-Time Systems: Essays in Honour of Dines Bjørner and Zhou Chaochen on Occasion of their 70th Birthdays
Publisher: Springer
Editors: Jones, C. B., Liu, Z., Woodcock, J.
ISBN (Print): 978-3-540-75220-2

Series: Lecture Notes in Computer Science
Number: 4700
Main Research Area: Technical/natural sciences
Conference: Festschrift Symposium dedicated to the 70th birthdays of Dines Bjørner and Zhou Chaochen, Macau, 01/01/2007
domain engineering, formal methods, verification, domain-specific languages, railway control systems, code generation
Source: orbit
Source-ID: 207240
Publication: Research - peer-review › Article in proceedings – Annual report year: 2007

Object Code Verification for Safety-Critical Railway Control Systems

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Peleska, J. (Ekstern), Haxthausen, A. E. (Intern), Schnieder, E. (ed.) (Ekstern), Tarnai, G. (ed.) (Ekstern)
Pages: 184-199
Publication date: 2007
Specification, Proof, and Model-checking of the Mondex Electronic Purse using RAISE

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: George, C. (Ekstern), Haxthausen, A. E. (Intern)
Publication date: 2007

Publication information
Publisher: UNU-IIST
Original language: English
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 200915
Publication: Research - peer-review › Report – Annual report year: 2007

Specification and Proof of the Mondex Electronic Purse

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: George, C. (Ekstern), Haxthausen, A. E. (Intern)
Publication date: 2006

Host publication information
Title of host publication: Proceedings of Automated Formal Methods 2006 (AFM 2006), Seattle, USA
Main Research Area: Technical/natural sciences
Conference: Unknown, 01/01/2006
Source: orbit
Source-ID: 193068
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Specification and Proof of the Mondex Electronic Purse

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern), George, C. (Ekstern), Schutz, M. (Ekstern)
Publication date: 2006

Host publication information
Publisher: UNU-IIST
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 193069
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Designing a Flexible Kernel Providing VDM++ Support for Eclipse

General information
Proof support for RAISE - by a Reuse Approach Based on Institutions

Formal methods are mathematically based methods for developing software. Such methods usually involve that software and requirements are specified in a formal specification language, after which it is verified that the software meets the requirements. RAISE is a formal method with the associated specification language RSL and a proof system. Computer-based proof tools are available for RAISE, but a higher degree of automation is desired. Isabelle/HOL is a proof assistant for higher-order logic (HOL). It is an instantiation of the generic proof assistant Isabelle which offers a suitable degree of automation and flexibility. In order to use the Isabelle/HOL proof assistant for the RAISE method, translation from RSL to HOL is considered. The translation is based on institutions which formalize the informal notion of "a logical system". Institutions and morphisms between institutions are presented together with specifications over institutions and model-theoretic semantics of specifications. The concept of "light institution comorphisms" is introduced as a modification of well-known institution comorphisms, and it is proved that a light institution comorphism enables sound reuse of proof assistants when it has certain properties. Moreover, the concept of looser semantics of specifications is introduced as a model-theoretic description of the semantics of RSL specifications, and an equivalence result is proved. An institution for an applicative, deterministic subset of RSL, referred to as "mRSL", is defined. Then, a well-known institution for HOL is presented, and Isabelle/HOL is briefly described. An institution comorphism from the mRSL institution to the HOL institution is defined, providing a translation from mRSL to Isabelle/HOL, and it is proved that the light institution comorphism has the properties that enable sound reuse of the Isabelle/HOL proof assistant. The use of the translation is described in connection with three examples: logical circuits, a generalized railway crossing, and an encoding of Duration Calculus in RSL. In Danish: Formelle metoder er matematisk baserede metoder til udvikling af programvel. Sådanne metoder involverer som regel, at software og krav beskrives i et formalt specifikationssprog, hvorefter det verificeres, at programmet opfylder de ønskede krav. RAISE er en formel metode med det tilhørende specifikationsprog og et bevisssystem. Der findes datamatbaserede bevisværktøjer til RAISE, men en højere grad af automation er ønskværdig. Isabelle/HOL er en bevisfører for højereordens logik (HOL). Bevisføreren er en instantiering af den generiske bevisfører Isabelle, der tilbyder en passende grad af automation og fleksibilitet. Med henblik på at benytte bevisføreren Isabelle/HOL i forbindelse med RAISE metoden, betragtes oversættelse fra RSL til HOL. Oversættelsen baseres på institutioner, der formaliserer det uformelle begreb "logisk system ". Institutioner og morfier mellem institutioner gennemgås sammen med specifikationer over institutioner og modelteoretisk semantik af specifikationer. Begrebet "iet institutionscomorf" introduseres som en modifikation af velkendte institutionscomorfer, og det bevises, at en let institutionscomorfi muligvis sund genbrug af bevisførere, når den har visse egenskaber. Derudover introduceres begrebet løse semantik af specifikationer som en modelteoretisk beskrivelse af semantikken af RSL- specifikationer, og et ekvivalensresultat bevises. Der defineres en institution for en applikativ, deterministisk delmængde af RSL, der benævnes "mRSL". Herefter
præsenteres en velkendt institution for HOL, og Isabelle/HOL gennemgås kort. Der defineres en let institutionscomorfi fra mRSL- institutionen til HOL-institutionen, hvorved der fås en oversættelse fra mRSL til Isabelle/HOL, og det bevises, at den definerede lette institutionscomorfi har de egenskaber, der muliggør sund genbrug af bevisføreren Isabelle/HOL. Brugen af den definerede oversættelse beskrives i forbindelse med tre eksempler: logiske kredsløb, en jernbaneoverskæring og en indkodning af varighedsøklylen i RSL.

**General information**
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Lindegaard, M. P. (Intern), Hansen, M. R. (Intern), Haxthausen, A. E. (Intern)
Publication date: May 2004

**Publication information**
Original language: English
Main Research Area: Technical/natural sciences
Electronic versions:
imm3148.ps
Links:
Source: orbit
Source-ID: 154831
Publication: Research › Ph.D. thesis – Annual report year: 2004

**Automated Verification for Train Control Systems**

**General information**
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Peleska, J. (Ekstern), Grosse, D. (Ekstern), Haxthausen, A. E. (Intern), Drechsler, R. (Ekstern)
Publication date: 2004

**Host publication information**
Title of host publication: Proceedings of Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT 2004), Braunschweig
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 154659
Publication: Research - peer-review › Article in proceedings – Annual report year: 2004

**CASL Semantics**

**General information**
State: Published
Organisations: Software Engineering, Department of Informatics and Mathematical Modeling
Publication date: 2004

**Host publication information**
Volume: Lecture Notes in Computer Science, Vol. 2960
Main Research Area: Technical/natural sciences
Links:
http://www.informatik.uni-bremen.de/~till/papers/cai.ps
Source: orbit
Source-ID: 154722
Publication: Research - peer-review › Book chapter – Annual report year: 2004
UML-ising formal techniques

This invited paper presents a number of correlated specifications of example railway system problems. They use a variety of partially or fully integrated formal specification. The paper thus represents a mere repository of what we consider interesting case studies. The existence of the Unified Modeling Language [10,67,36,20] has caused, for one reason or another, the research community to try formalise one or another facet of UML. In this paper we report on another way to achieve what UML attempts to achieve: Broadness of application, convenience of notation, and multiplicity of views. Whether these different UML views are unified, integrated, correlated or merely co-located is for others to dispute. We also seek to support multiple views, but are also in no doubt that there must be sound, well defined relations between such views. We thus report on ways and means of integrating formal techniques such as RAISE (RSL) [58,59], Petri Nets [56,62,37,61,411, Message and Live Sequence Charts [42,43,44,64,13], Statecharts [23,24,26,27], RAISE with Timing (TRSL) [18,45,461, and TRSL with Duration Calculus (79,30]. In this way one achieves a firm foundation for combined uses of these formal development techniques, one that can be believably deployed for as wide a spectrum, or even a wider spectrum of software (and hardware) development, as, respectively than UML.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Bjørner, D. (Intern), George, C. W. (Ekstern), Haxthausen, A. E. (Intern), Madsen, C. (Ekstern), Holmslykke, S. (Ekstern), Penicka, M. (Intern)
Publication date: 2004

Host publication information
Title of host publication: Integration of software specification techniques for applications in engineering
Place of publication: Berlin
Publisher: Springer-verlag Berlin
ISBN (Print): 3-540-23135-8
Series: Lecture Notes in Computer Science
Number: 3147
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 197273
Publication: Research - peer-review › Book chapter – Annual report year: 2004

"UML-ising" Formal Techniques

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Bjørner, D. (Intern), George, C. W. (Ekstern), Haxthausen, A. E. (Intern), Madsen, C. K. (Ekstern), Holmslykke, S. (Ekstern), Penicka, M. (Ekstern)
Publication date: 2004

Host publication information
Title of host publication: Proceedings of INT2004 - Integration of Software Specification Techniques for Applications in Engineering
Volume: Lecture Notes in Computer Science
Publisher: Springer
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 154597
Generation of Executable Railway Control Components from Domain-Specific Descriptions

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Publication date: 2003

Host publication information
Publisher: L'Harmattan Hongrie
ISBN (Print): 96-39-45745-0
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 58528
Publication: Research - peer-review › Article in proceedings – Annual report year: 2003

The Logic of the RAISE Specification Language

This paper describes the logic of the RAISE Specification Language, RSL. It explains the particular logic chosen for RAISE, and motivates this choice as suitable for a wide spectrum language to be used for designs as well as initial specifications, and supporting imperative and concurrent specifications as well as applicative sequential ones. It also describes the logical definition of RSL, its axiomatic semantics, as well as the proof system for carrying out proofs.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: George, C. (Ekstern), Haxthausen, A. E. (Intern)
Pages: 323-350
Publication date: 2003
Main Research Area: Technical/natural sciences

Publication information
Journal: Computing and Informatics
Volume: 22
Issue number: 3-4
ISSN (Print): 1335-9150
Ratings:
BFI (2018): BFI-level 1
BFI (2017): BFI-level 1
A Domain Specific Language for Railway Control Systems

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Publication date: 2002

Host publication information
Title of host publication: Proceedings of the Sixth Biennial World Conference on Integrated Design and Process Technology (IDPT2002)
Main Research Area: Technical/natural sciences

Links:
Source: orbit
Source-ID: 58178
Publication: Research - peer-review › Article in proceedings – Annual report year: 2002
Formal development and verification of a distributed railway control system
The authors introduce the concept for a distributed railway control system and present the specification and verification of the main algorithm used for safe distributed control. Our design and verification approach is based on the RAISE method, starting with highly abstract algebraic specifications which are transformed into directly implementable distributed control processes by applying a series of refinement and verification steps. Concrete safety requirements are derived from an abstract version that can be easily validated with respect to soundness and completeness. Complexity is further reduced by separating the system model into a domain model and a controller model. The domain model describes the physical system in absence of control and the controller model introduces the safety-related control mechanisms as a separate entity monitoring observables of the physical system to decide whether it is safe for a train to move or for a point to be switched.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Pages: 687-701
Publication date: 2000
Main Research Area: Technical/natural sciences

Publication information
Journal: IEEE Transaction on Software Engineering
Volume: 26
Issue number: 8
ISSN (Print): 0098-5589
Ratings:
BFI (2018): BFI-level 2
BFI (2017): BFI-level 2
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 2
Scopus rating (2016): SJR 0.934 SNIP 3.678 CiteScore 5.51
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 1.112 SNIP 4.207 CiteScore 4.97
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 1.167 SNIP 3.955 CiteScore 4.62
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 1.248 SNIP 4.803 CiteScore 5.29
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 1.568 SNIP 4.918 CiteScore 5.32
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 1.524 SNIP 4.761 CiteScore 5.11
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 1.671 SNIP 5.175
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 2.008 SNIP 5.241
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 1.745 SNIP 5.969
Scopus rating (2007): SJR 1.942 SNIP 5.279
Scopus rating (2006): SJR 1.649 SNIP 5.424
Scopus rating (2005): SJR 1.918 SNIP 4.707
Scopus rating (2004): SJR 1.677 SNIP 3.772
Scopus rating (2003): SJR 1.811 SNIP 3.348
Scopus rating (2002): SJR 1.917 SNIP 2.978
Scopus rating (2001): SJR 1.619 SNIP 3.366
Formal Methods for the Specification and Verification of Distributed Railway Control Systems: From Algebraic Specifications to Distributed Hybrid Real-Time Systems

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Pages: 263-271
Publication date: 2000

Host publication information
Title of host publication: Forms '99 Formale Techniken für die Eisenbahnsicherung
Publisher: VDI-Verlag
Main Research Area: Technical/natural sciences
Conference: Forms '99 Formale Techniken für die Eisenbahnsicherung, 01/01/2000
Source: orbit
Source-ID: 176407
Publication: Research - peer-review › Journal article – Annual report year: 2000

Duration Calculus (DC) is an interval-based real-time logic, which can be used in capturing and eliciting users' real-time requirements. The Timed RAISE Specification Language (TRSL) is an extension of the RAISE Specification Language with real-time features. This paper links DC and TRSL together in a method for real-time developments. An operational semantics with behavior is specified for TRSL. It is defined what its means for a TRSL process to satisfy a DC requirement, and a method for verifying whether the satisfaction relation holds or not is provided. Our contribution also demonstrates a general approach for linking state-based real-time logics together with event-based, timed process algebra languages.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern), Yong, X. (Ekstern)
Pages: 25-44
Publication date: 2000

Host publication information
Title of host publication: IFM'2000 2nd Int. Conf. on Integrated Formal Methods, no. 1945
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Conference: IFM'2000 2nd Int. Conf. on Integrated Formal Methods, 01/01/2000
Source: orbit
Source-ID: 176484
Publication: Research - peer-review › Article in proceedings – Annual report year: 2000

Modelling Railway Interlocking Systems
In this report we present a model of interlocking systems, and describe how the model may be validated by simulation. Station topologies are modelled by graphs in which the nodes denote track segments, and the edges denote connectivity.
for train traffic. Points and signals are modelled by annotations on the edges, thereby restricting the driving possibilities. We define the safe station states as predicates on the graph, and present a first step towards an implementation of these predicates.

Some Approaches for Integration of Specification Techniques
It is often useful to apply several specification techniques within the same software development project. This raises the question how specification techniques can be integrated. In this presentation we give three different examples of how this can be done. In the first example, we summarise how the wide-spectrum approach has been used in the RAISE Specification Language (RSL) to integrate algebraic and model-oriented, applicative and imperative, and sequential and concurrent specification...

Subsorted Partial Higher-order Logic as an extension of CASL
CASL is a specification language combining first-order logic, partiality and subsorting. However, in many applications, first-order logic does not suffice. Consider e.g. the specification of functional programs, which often gain their conciseness through the use of higher-order functions, or the specification of predicate transformers, which is inherently higher-order. This work generalizes the CASL logic to also include higher-order functions and predicates. The combination of subsorting, partiality, higher-order functions and predicate logic is new to our knowledge. The logic is presented in a modular step-by-step reduction: the logic is defined in terms of a generalized subsorted partial logic which in turn is defined in terms of many-sorted partial first-order logic. We believe that it is crucial to follow this modular style for two main reasons. One reason is reduction of complexity. We use a two step reduction involving three logics in our presentation, adding new features step by step. Thus each step (and its interaction with the previous steps) can be understood separately. This is important since there is quite a number of different non-trivial interactions. The other reason is compatibility of sublanguages and extensions. First of all, (first-order) CASL should be faithfully embeddable into its higher-order extension. Secondly, it should be possible easily to restrict higher-order CASL to various sublanguages, as it has been done for first-order CASL. A new notion of homomorphism is introduced to meet the need to get a faithful embedding of first-order CASL into higher-order CASL. Finally, it is discussed how a proof calculus for the proposed logic can be developed.
Towards Domain-Specific Formal Specification Languages for Railway Control Systems

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Peleska, J. (Ekstern), Baer, A. (Ekstern), Haxthausen, A. E. (Intern), Schnieder, E. (ed.) (Ekstern), Becker, U. (ed.) (Ekstern)
Pages: 147-152
Publication date: 2000

Host publication information
Title of host publication: WADT'99
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Conference: WADT'99, 01/01/1999
Source: orbit
Source-ID: 176505
Publication: Research - peer-review › Article in proceedings – Annual report year: 2000

CASL - The CoFI Algebraic Specification Language - Semantics.

General information
State: Published
Organisations: Department of Information Technology
Authors: Haxthausen, A. (Intern)
Publication date: 1999

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Links:
http://www.brics.dk/Projects/CoFI/Notes/S-9
Source: orbit
Source-ID: 175043
Publication: Research - peer-review › Report – Annual report year: 1999

Formal Development and Verification of a Distributed Railway Control System
In this article we introduce the concept for a distributed railway control system and present the specification and verification of the main algorithm used for safe distributed control. Our design and verification approach is based on the RAISE method, starting with highly abstract algebraic specifications which are transformed into directly implementable distributed control processes by applying a series of refinement and verification steps. Concrete safety requirements are derived from an abstract version that can be easily validated with respect to soundness and completeness. Complexity is further reduced by separating the system model into a domain model describing the physical system in absence of control and a controller model introducing the safety-related control mechanisms as a separate entity monitoring observables of the physical system to decide whether it is safe for a train to move or for a point to be switched.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, University of Bremen
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Publication date: 1999
A RAISE Specification Framework and Justification assistant for the Duration Calculus

RAISE is a product consisting of a development method, an associated formal specification language (RSL) and a collection of computer-based tools. RAISE has turned out to be useful in the development of many kinds of software systems. However, RSL has no “real-time” features, and hence, it is difficult to specify real-time applications using RSL. The Duration Calculus (DC) is a formalism which can be used for that. However, DC is “just” a logic, and for practical purposes it would be nice to have a richer language providing modules, facilities for declaring symbols to be used in DC.
The goal of our work is two-fold: (1) to extend RSL with real-time features, and (2) to provide a specification language and tools support (e.g. a syntax and type checker, a justification assistant, etc.) for DC. A first step towards this goal, could be to combine DC and RSL achieving the power of both. So far, we have encoded DC in RSL and set up a proof assistant tool to verify (encoded) DC formulas using the RAISE Justification tools. This paper first introduces a RAISE specification framework for DC, and then explains how the justification assistant is set up.
the physical system to decide whether it is safe for a train to move or for a point to be switched.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, University of Bremen
Authors: Haxthausen, A. E. (Intern), Peleska, J. (Ekstern)
Publication date: 1998

Host publication information
Title of host publication: Proceedings of First FMERail Workshop
Place of publication: Breukelen
Publisher: Origin
Main Research Area: Technical/natural sciences
Conference: First FMERail Workshop, Breukelen, 01/01/1998
Source: orbit
Source-ID: 169877
Publication: Research - peer-review › Article in proceedings – Annual report year: 1998

Subsorted Partial Higher-order Logic as an Extension of CASL

General information
State: Published
Organisations: Department of Information Technology, University of Bremen
Authors: Mossakowski, T. (Ekstern), Haxthausen, A. (Intern), Krieg-Bruckner, B. (Ekstern)
Publication date: 1998

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Links:
http://www.brics.dk/Projects/CoFI/Notes/L-10/index.html
Source: orbit
Source-ID: 169878
Publication: Research - peer-review › Report – Annual report year: 1998

CASL - The CoFI Algebraic Specification Language (Tentative Design, version 0.95) -- Language Summary with annotations concerning questions and doubts

General information
State: Published
Organisations: Department of Information Technology
Authors: Haxthausen, A. (Intern)
Publication date: 1997

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 167716
Publication: Research - peer-review › Report – Annual report year: 1997

CASL - The CoFI Algebraic Specification Language (Tentative Design, version 0.95) - Language Summary, with annotations concerning the semantics of constructs.

General information
State: Published
Organisations: Department of Information Technology
Authors: Haxthausen, A. (Intern)
Publication date: 1997

Publication information
CASL - The CoFI Algebraic Specification Language (version 0.97) - Semantics

General information
State: Published
Organisations: Department of Information Technology
Authors: Haxthausen, A. (Intern)
Publication date: 1997

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 167717
Publication: Research - peer-review › Report – Annual report year: 1997

CASL- The Common Algebraic Specification Language- Summary

General information
State: Published
Organisations: Department of Information Technology
Authors: Haxthausen, A. (Intern)
Publication date: 1997

Publication information
Original language: English
Main Research Area: Technical/natural sciences

Bibliographical note
0.98
Source: orbit
Source-ID: 167721
Publication: Research - peer-review › Report – Annual report year: 1997

LYCOS: The Lyngby Co-Synthesis System

General information
State: Published
Organisations: Department of Information Technology
Authors: Madsen, J. (Intern), Grode, J. N. R. (Intern), Knudsen, P. V. (Intern), Petersen, M. E. (Intern), Haxthausen, A. (Intern)
Pages: 195-236
Publication date: 1997
Main Research Area: Technical/natural sciences

Publication information
Journal: Design Automation for Embedded Systems
Volume: 2
Issue number: 2
Original language: English
Source: orbit
Source-ID: 166194
Publication: Research - peer-review › Journal article – Annual report year: 1997
Order-sorted Algebraic Specifications with Higher-order

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern)
Pages: 157-185
Publication date: 1997
Main Research Area: Technical/natural sciences

Publication information
Journal: Theoretical Computer Science
Volume: 183
Issue number: 2
ISSN (Print): 0304-3975
Ratings:
BFI (2018): BFI-level 2
BFI (2017): BFI-level 2
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 0.97 SJR 0.569 SNIP 1.006
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.623 SNIP 1.212 CiteScore 1
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.708 SNIP 1.228 CiteScore 1.08
Web of Science (2014): Indexed yes
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.739 SNIP 1.38 CiteScore 1.17
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.844 SNIP 1.288 CiteScore 1.16
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.81 SNIP 1.289 CiteScore 1.17
ISI indexed (2011): ISI indexed yes
Web of Science (2011): Indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.91 SNIP 1.329
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.948 SNIP 1.475
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 1.188 SNIP 1.638
Web of Science (2008): Indexed yes
Scopus rating (2007): SJR 0.997 SNIP 1.65
Scopus rating (2006): SJR 0.911 SNIP 1.49
Web of Science (2006): Indexed yes
Scopus rating (2005): SJR 0.821 SNIP 1.486
Web of Science (2005): Indexed yes
Scopus rating (2004): SJR 0.804 SNIP 1.366
Web of Science (2004): Indexed yes
Scopus rating (2003): SJR 0.936 SNIP 1.523
Permissive Subsorted Partial Logic in CASL.
This paper presents a permissive subsorted partial logic used in the CoFI Algebraic Specification Language. In contrast to other order-sorted logics, subsorting is not modeled by set inclusions, but by injective embeddings allowing for more general models in which subtypes can have different data type representations. Furthermore, there are no restrictions like monotonicity, regularity or local filtration on signatures at all. Instead, the use of overloaded functions and predicates in formulae is required to be sufficiently disambiguated, such that all parses have the same semantics. An overload resolution algorithm is sketched.
Developing a Translator from C Programs to Data Flow Graphs Using RAISE

Describes how a translator from a subset of C to data flow graphs has been formally developed using the RAISE (Rigorous Approach to Industrial Software Engineering) method and tools. In contrast to many development examples described in the literature, this development is not a case study, but a real one, and it covers all development phases, including the code-generation phase. The translator is now one of the components of the LYCOS (LYngby CO-Synthesis) system, which is a software/hardware co-synthesis system under development at the Technical University of Denmark. The translator, together with the other components of LYCOS, provides a means for moving parts of C programs to dedicated hardware, thereby obtaining better performance. The translator was refined in steps, starting with an abstract specification and ending with a concrete specification from which C++ code was then automatically generated by the RAISE tools. In addition to illustrating the general methodology of RAISE, the paper also contributes with a specific method for refining set comprehensions.

Overloading, Subtypes and Higher Order Functions
Pushouts of Order-sorted Algebraic Specifications
This paper investigates the existence of pushouts in the category of order-sorted algebraic specifications and specification morphism. As a main result it is shown that the existence can be guarantied by imposing certain conditions on the specification morphisms. This result is important as the pushout construction is one of themost widely used approaches to combine specifications.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern), Nickl, F. (Ekstern)
Pages: 132-147
Publication date: 1996

Host publication information
Title of host publication: Algebraic Methodology and Software Technology
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Conference: AMAST'96, Munich, 01/01/1996
Source: orbit
Source-ID: 164611
Publication: Research - peer-review › Article in proceedings – Annual report year: 1996

Pushouts of Order-sorted Algebraic Specifications (report)

General information
State: Published
Organisations: Department of Information Technology, Ludwig-Maximilians-Universität
Authors: Haxthausen, A. (Intern), Nickl, F. (Ekstern)
Publication date: 1996

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 166261
Publication: Research - peer-review › Report – Annual report year: 1996

Subsorting and Higher-order Functions

General information
State: Published
Organisations: Department of Information Technology, University of Oslo
Authors: Haxthausen, A. (Intern), Dahl, O. (Ekstern)
Publication date: 1996

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 166264
Publication: Research - peer-review › Report – Annual report year: 1996

Subsorting in CASL: CoFI Language Design Study Note

General information
State: Published
Organisations: Department of Information Technology, University of Genoa, University of Bremen, University of Oslo
Order-sorted Algebraic Specifications with Higher-order Functions
This paper gives a proposal for how order-sorted algebraic specification languages can be extended with higher-order functions. The approach taken is a generalisation to the order-sorted case of an approach given by Müller, Tarlecki and Wirsing for the many-sorted case. The main idea in the proposal is to only consider reachable extensional algebras. This leads to a very simple theory, where it is possible to relate the higher-order specifications to first-order specifications.

The RAISE Development Method

A Concurrency Case Study Using RAISE
RAISE: A Product Supporting Industrial Use of Formal Methods

This paper gives an overview of RAISE, a product consisting of a method for developing software, an associated formal specification language and tools supporting the method and the language. The method is based on the notion of stepwise refinement and offers the possibility of formal verification. The specification language incorporates several specification styles in one uniform framework. The product is aimed at industry and is currently being used by several companies.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Haxthausen, A. E. (Intern), Pedersen, J. S. (Ekstern), Prehn, S. (Intern)
Pages: 319-346
Publication date: 1993
Main Research Area: Technical/natural sciences

The RAISE Specification Language

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Group, R. L. (Ekstern), Haxthausen, A. E. (Intern)
Publication date: 1992

Formal, Model-oriented Software Development Methods - From VDM to ProCoS & from RAISE to LaCoS

The first author has been invited to reminisce over almost 20 years of his research into and application of formal methods in software development. The paper deals with model-oriented methods. The title of this paper mentions two methods: VDM (Vienna Development Method) and RAISE (Rigorous Approach to Industrial Software Engineering), the latter derived from the former, and two projects: ProCoS (Provably Correct Systems) and LaCoS (Large-scale Correct Systems). LaCoS is a follow-up on RAISE. ProCoS adheres to the same principles as VDM as VDM and RAISE, but with a twist! The paper will outline the technical/scientific essence of the VDM and RAISE methods, and explain the ProCos and LaCoS project structures. The paper will first outline five central roles of software developers: problem domain specialists, programmers, software engineers, resident computation scientists and managers. We will briefly illustrate examples of specifications in VDM and RAISE. The aim of the paper is to record that formal methods in software development are now well-developed and broadly accepted in Europe.

General information
State: Published
Projects:

Formal development and verification of railway control systems
Department of Applied Mathematics and Computer Science
Period: 01/11/2012 → 21/01/2016
Number of participants: 6
PhD Student:
Vu, Linh Hong (Intern)
Supervisor:
Peleska, Jan (Ekstern)
Main Supervisor:
Haxthausen, Anne Elisabeth (Intern)
Examiner:
Hansen, Michael Reichhardt (Intern)
Fantechi, Alessandro (Ekstern)
Larsen, Peter Gorm (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU) Samf.
Project: PhD

Modelling and analysis for Cyber-Physical Systems
Department of Applied Mathematics and Computer Science
Period: 01/11/2011 → 30/09/2015
Number of participants: 6
PhD Student:
Dung, Phan Anh (Intern)
Supervisor:
Madsen, Jan (Intern)
Main Supervisor:
Hansen, Michael Reichhardt (Intern)
Examiner:
Haxthausen, Anne Elisabeth (Intern)
Sestoft, Peter (Intern)
Vain, Jüri (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet
Project: PhD

Pattern-oriented Formal Software Development
L'objectif de ce projet est de fournir une méthode pratique pour le développement efficace de logiciel correct. Il est reconnu que ce sont les premières étapes du développement du logiciel qui sont cruciales pour parvenir à la meilleure adéquation entre les besoins exprimés et la réalisation proposée, et pour éliminer au maximum toute source d'erreur. Ceci est particulièrement important pour les applications "critiques", tels que les systèmes de contrôle des trains, où des erreurs peuvent entraîner la perte de vies humaines. L'accent est donc mis tout d'abord sur une expression précise et non ambiguë des besoins dans les spécifications. Différentes approches sont proposées pour aller dans ce sens, avec leurs avantages et inconvénients respectifs. Les spécifications formelles, par leur expression précise, conduisent à se poser des questions qui font progresser dans la compréhension du problème à traiter. Un écueil demeure, c'est celui de la taille et/ou de la complexité, qui rendent malaisée la compréhension synthétique et peuvent égarer dans la démarche. Notre approche est d'utiliser les "patterns" pour aider à maîtriser la complexité des problèmes dans le démarche de spécification. Les "patterns" (traduits par schémas ou patrons) proposent des familles de structures fréquemment rencontrées que l'utilisateur est invité à "essayer" (quitte à les adapter) sur le problème à traiter pour ainsi bénéficier de...

Department of Informatics and Mathematical Modeling

Université Paris 13
Period: 01/04/2005 → 01/04/2010
Number of participants: 1
Project ID: 15407
Project Manager, organisational:
Haxthausen, Anne Elisabeth (Intern)

Financing sources
Source: Sam.arb.aftaler - Udenlandske offentlige og private
Name of research programme: Sam.arb.aftaler - Udenlandske offentlige og private
Amount: 27,248.00 Danish Kroner
Project

Modellering og analyse af globale applikationer

Department of Informatics and Mathematical Modeling
Period: 01/01/2002 → 12/07/2005
Number of participants: 6
Phd Student:
Domain-specific Languages for Railway Control Systems
The purpose of this project is to develop a concept for development of railway control systems. The idea is to provide a generic railway control system, a domain-specific language for specifying application specific parameters and a compiler from domain-specific descriptions into configuration data for the generic control system. A validation, verification and test approach is also to be provided.

Department of Information Technology
Department of Informatics and Mathematical Modeling
University of Bremen
Period: 01/01/2000 → 31/12/2010
Number of participants: 2
Project participant:
Peleska, Jan (Ekstern)
Project Manager, organisational:
Haxthausen, Anne Elisabeth (Intern)

Financing sources
Source: Overhead/overskud
Name of research programme: Overhead/overskud
Amount: 0.00 Danish Kroner
Project

Modelling Railway Interlocking Systems II
The purpose of this project is the model and verify safety properties of computer based railway interlocking systems for lines between stations at the Danish State Railways.
CoFI WG (ESPRIT Working Group no. 29432)
CoFI, the Common Framework Initiative for algebraic specification and development of software, is an open international (but predominantly European) collaboration. CoFI participants have designed CASL, intended as a common language for formal specification of functional requirements and modular software design. The Working Group will coordinate the completion of and disseminate the Common Framework, demonstrate its practical applicability in industrial contexts, and establish the infrastructure needed for future European collaborative research in algebraic techniques.

FMERail (ESPRIT Project EP26538)
This dissemination project aims at promoting the adoption of formal methods in the railway domain. The approach of the project is to arrange a series of workshops to show how different formal method technologies can be applied to railway problems.
Name of research programme: **Overhead/overskud**  
Amount: 201,000.00 Danish Kroner  

**Information project for highschool pupils**  
The goal of this project is to attract more students to the engineering study in informatics. In collaboration with a number of companies, we will inform potential students about how graduated engineers in informatics solve exciting problems using creativity, mathematics, methodology and technology.

Department of Information Technology  
Jacob Frost, Creations  

DDC-I A/S  

PPU Maconomy  

Banestyrelsen A/S  

TERMA Elektronik A/S  

The Vision Factory  
Period: 01/11/1997 → …  
Number of participants: 3  
Project participant:  
Hansen, Bo Stig (Intern)  
Bing, Eva (Intern)  
Project Manager, organisational:  
Haxthausen, Anne Elisabeth (Intern)

**Financing sources**  
Source: Unknown  
Name of research programme: **Ukendt**  
Amount: 205,000.00 Danish Kroner  
Source: Unknown  
Name of research programme: **Ukendt**  
Amount: 10,000.00 Danish Kroner  

**Co-synthesis of RSL Specifications**  
The goal of this project is to integrate the RAISE formal method with the LYCOS software/hardware co-synthesis system obtaining a product which supports formal co-specification and verification as well as co-synthesis of software/hardware systems.

Department of Information Technology  
Period: 01/09/1997 → 31/01/1998  
Number of participants: 1  
Project Manager, organisational:  
Haxthausen, Anne Elisabeth (Intern)

**Dracos**  
In this project we use RAISE to do a formal development and verification of a real distributed railway control system.

Department of Information Technology  

JP Software Consult  
Period: 01/12/1996 → 01/12/1999  
Number of participants: 1  
Project Manager, organisational:  
Haxthausen, Anne Elisabeth (Intern)

**Timed RAISE**  
The goal of this project is to investigate how RAISE can be extended with real-time facilities.
Department of Information Technology
Department of Informatics and Mathematical Modeling
University of Bremen
United Nations University International Institute for Software Technology
Period: 01/08/1996 → 31/12/2000
Number of participants: 2
Project participant:
Peleska, Jan (Ekstern)
Project Manager, organisational:
Haxthausen, Anne Elisabeth (Intern)

Financing sources
Source: Overhead/overskud
Name of research programme: Overhead/overskud
Amount: 0.00 Danish Kroner

CoFI (Common Framework Initiative) is an international project with participants from most major groups working on algebraic specification. The goal of the initiative is to design a common framework for algebraic specification. The rationale behind this is that the lack of such a framework hinders the dissemination and application of research results in algebraic specification. CoFI will provide a family of specification languages, a development method and tool support. The project was partly supported by STVF under the "Codesign" program 1996-1997, and by the ESPRIT CoFI WG 1998-2001.

Department of Information Technology
Department of Informatics and Mathematical Modeling
Aarhus University
University of Bremen
Period: 01/11/1995 → 31/12/2003
Number of participants: 38
Project participant:
Mosses, Peter (Ekstern)
Lescanne, Pierre (Ekstern)
Astesiano, Egidio (Ekstern)
Bergstra, Jan (Ekstern)
Bert, Didier (Ekstern)
Bidoit, Michel (Ekstern)
Bettaz, Mohammed (Ekstern)
Broy, Manfred (Ekstern)
Choppy, Christine (Ekstern)
Dahl, Ole-Johan (Ekstern)
Ehrich, Hans-Dieter (Ekstern)
Ehrig, Hartmut (Ekstern)
Fiadeiro, Jose (Ekstern)
Gaudel, Marie-Claude (Ekstern)
Goguen, Joseph A. (Ekstern)
Grosu, Radu (Ekstern)
Heering, Jan (Ekstern)
Kirchner, Helene (Ekstern)
Kreowski, Hans-Joerg (Ekstern)
Krieg-Bruckner, Bernd (Ekstern)
Maibaum, Tom (Ekstern)
Malcolm, Grant (Ekstern)
Meinke, Karl (Ekstern)
Orejas, Fernando (Ekstern)
Module Composition Mechanisms
This work is concerned with mechanisms that can be used to write specifications in a modular way. The pushout approach to modular compositions has been investigated for order-sorted algebraic specifications. The main result is the establishment of a set of conditions which ensure the existence of modular compositions by pushouts. The work has been done in collaboration with Friederike Nickl. The project was partly supported by STVF under the "Codesign" program.

Department of Information Technology
Period: 01/07/1995 → 01/07/1996
Number of participants: 2
Project participant:
Nickl, Friederike (Ekstern)
Project Manager, organisational:
Haxthausen, Anne Elisabeth (Intern)

Subtyping and Higher-order Functions
The goal of this project is to give a proposal for the semantic foundations of algebraic specification languages having subtypes and higher-order functions.

Department of Information Technology
Department of Informatics and Mathematical Modeling
Period: 01/01/1995 → 31/12/1999
Number of participants: 1
Project Manager, organisational:
Haxthausen, Anne Elisabeth (Intern)

Financing sources
Source: Sam.arb.aftaler - Udenlandske offentlige og private
Name of research programme: Sam.arb.aftaler - Udenlandske offentlige og private
Amount: 99,999.00 Danish Kroner

Activities:

Formal Methods for Software Development
Period: 11 Sep 2017 → 14 Sep 2017
Anne Elisabeth Haxthausen (Guest lecturer)
Department of Applied Mathematics and Computer Science
Software Engineering

Description
A PhD course.

Related external organisation

University of Florence
Italy
Activity: Talks and presentations › Guest lectures, external teaching and course activities at other universities

University of Florence
Period: 15 Aug 2017 → 14 Sep 2017
Anne Elisabeth Haxthausen (Visiting researcher)
Department of Applied Mathematics and Computer Science
Software Engineering

Description
Guest professor
Activity: Visiting an external institution › Visiting another research institution

Green Light for Smarter Methods in Railway Safety Verification
Period: 31 May 2017
Anne Elisabeth Haxthausen (Guest lecturer)
Department of Applied Mathematics and Computer Science
Software Engineering

Description
Invited pitch talk

Related event

Transport Summer Summit DTU 2017: Challenges, research and new developments within transportation, mobility and sustainability
31/05/2017 → 31/05/2017
Lyngby, Denmark
Activity: Talks and presentations › Conference presentations

Formel Modellering og Verifikation af Jernbanekontrolsystemer: Et eksempel fra RobustRailS WP 4.1
Period: 3 Feb 2016
Anne Elisabeth Haxthausen (Invited speaker)
Department of Applied Mathematics and Computer Science
Software Engineering

Description
Invited talk at the Inauguration of RailTech DTU, the Centre for Rail Technology

Related external organisation

Unknown external organisation
Activity: Talks and presentations › Conference presentations

Assessment Committee for a post.doc. position (External organisation)
Period: 21 Nov 2012 → 21 Dec 2012
Anne Elisabeth Haxthausen (Participant)
Danish Railway Conference 2012
Period: 9 May 2012
Anne Elisabeth Haxthausen (Participant)
Department of Informatics and Mathematical Modeling
Computer Science and Engineering
Software Engineering
Description
Poster presentation at a DTU stand for the RobustRailS research project.

Danish Railway Conference 2012
Period: 17 Apr 2012
Anne Elisabeth Haxthausen (Participant)
Department of Informatics and Mathematical Modeling
Computer Science and Engineering
Software Engineering
Description
Invited by Banedanmark
An ERTMS conference in Copenhagen

An Introduction to Formal Methods for Software Development
Period: 7 Oct 2011
Anne Elisabeth Haxthausen (Consultant)
Department of Informatics and Mathematical Modeling
Description
Note: This lecture was given as a part of the Public Sector Consultancy service offered by the Technical University of Denmark.

Related external organisation
Banedanmark, Copenhagen
A Model-based Tool Set for Simulation and Verification of Relay Interlocking Systems
Period: 27 Sep 2011
Anne Elisabeth Haxthausen (Speaker)
Department of Informatics and Mathematical Modeling

Related external organisation
The Danish Society of Engineers, IDA
Kalvebod Brygge 31-33, DK-1780, Copenhagen V, Denmark

Towards a Semantics for VDM Core
Period: 20 Jun 2011
Anne Elisabeth Haxthausen (Speaker)
Department of Informatics and Mathematical Modeling

Description
Presentation given at the 9th Overture Workshop, as part of FM 2011.

Related event
Towards a Semantics for VDM Core
20/06/2011 → 20/06/2011
University of Limerick, Ireland

MicroSoft Research Software Summit
Period: 13 Apr 2011 → 15 Apr 2011
Anne Elisabeth Haxthausen (Participant)
Department of Informatics and Mathematical Modeling
Software Engineering

Effective Development and Verification of Railway Control Software
Period: 21 Jan 2011
Anne Elisabeth Haxthausen (Speaker)
Department of Informatics and Mathematical Modeling
Software Engineering

Description
This course module presents a method for effective development of software for a product line of similar railway control systems. The software is constructed in three steps: first a specifications in a domain-specific language is created, then a formal behavioural controller model is automatically created from the specification, and finally the model is compiled into executable object code. Formal verification is performed automatically by tools at three levels: (1) the specification is checked to follow the rules of the domain, (2) the controller model is checked to ensure safety, and (3) the object code is verified to be a correct implementation of the controller model.

Note: This seminar was given as a part of the Public Sector Consultancy service offered by the Technical University of Denmark.
Place: Banedanmark, Copenhagen

Related external organisation
**Unknown external organisation**  
Activity: Talks and presentations › Conference presentations

**Member of the review board for a VIP position at Engineering College of Århus (External organisation)**  
Period: 22 Nov 2010 → 1 Dec 2010  
Anne Elisabeth Haxthausen (Member)  
Department of Informatics and Mathematical Modeling  
Software Engineering

**Related external organisation**

**Member of the review board for a VIP position at Engineering College of Århus**  
Activity: Membership › Membership of committees, commissions, boards, councils, associations, organisations, or similar

**Formal Methods: A Tutorial on Model-oriented Specification**  
Period: 14 Oct 2010  
Anne Elisabeth Haxthausen (Consultant)  
Department of Informatics and Mathematical Modeling  
Software Engineering

**Description**  
Note: This lecture was given as a part of the Public Sector Consultancy service offered by the Technical University of Denmark.

**Related external organisation**

**Unknown external organisation**  
Activity: Public and private sector consultancy › Public sector consultancy

**An Introduction to Formal Methods for the Development of Safety-critical Applications**  
Period: 1 Sep 2010  
Anne Elisabeth Haxthausen (Consultant)  
Department of Informatics and Mathematical Modeling  
Software Engineering

**Description**  
Note: This lecture was given as a part of the Public Sector Consultancy service offered by the Technical University of Denmark.

**Related external organisation**

**Trafikstyrelsen (Danish Transport Authority)**  
Activity: Public and private sector consultancy › Public sector consultancy

**An Introduction to Formal Methods for Software Development**  
Period: 25 Jun 2010  
Anne Elisabeth Haxthausen (Consultant)  
Department of Informatics and Mathematical Modeling  
Software Engineering

**Description**  
Note: This lecture was given as a part of the Public Sector Consultancy service offered by the Technical University of Denmark.

**Related external organisation**

**Banedanmark (Rail Net Denmark)**
**Talentudvikling og karriererådgivning**

Period: 17 May 2010 → 7 Dec 2010

Anne Elisabeth Haxthausen (Participant)

Department of Informatics and Mathematical Modeling

Software Engineering

**Description**

Talentudvikling og karriererådgivning

Place: Technical University of Denmark, Lyngby

Degree of recognition: Local

**Related event**

Talentudvikling og karriererådgivning

17/05/2010 → 07/12/2010

Kgs. Lyngby, Denmark

Activity: Attending an event › Participating in or organising workshops, courses, seminars etc.

---

**JAIST Advanced School on Formal Specification and Systems Verification 2010 (JAIST-FSSV2010)**

Period: 1 Mar 2010 → 5 Mar 2010

Anne Elisabeth Haxthausen (Participant)

Department of Informatics and Mathematical Modeling

Software Engineering

**Related event**

JAIST Advanced School on Formal Specification and Systems Verification 2010 (JAIST-FSSV2010)

01/03/2010 → 05/03/2010

Kanazawa, Japan

Activity: Attending an event › Participating in or organising a conference

---

**Member of the review board of a Ph.D. thesis entitled "Domain-specific Modelling of Railway Control Systems with Integrated Verification and Validation", by Kirsten Mewes, Bremen University (External organisation)**

Period: 12 Nov 2009

Anne Elisabeth Haxthausen (External examiner)

Department of Informatics and Mathematical Modeling

Software Engineering

Activity: Examinations and supervision › External examination

---

**Towards a Framework for Modelling and Verification of Relay Interlocking Systems**

Period: 11 Nov 2009

Anne Elisabeth Haxthausen (Speaker)

Department of Informatics and Mathematical Modeling

Software Engineering

**Description**

This talk describes a framework currently under development for modelling, simulation and verification of relay interlocking systems as used by the Danish railways. The framework is centered around a domain-specific language (DSL) for describing such systems, and provides (1) graphical editors for creating DSL descriptions, (2) a validator for checking that DSL descriptions are statically well-formed (follow structural rules of the domain), (3) a graphical simulator for simulating the dynamic behaviour of relay interlocking systems, and (4) generators that from a DSL description can derive a state transition system model for the dynamic behaviour of the described relay interlocking system and its physical environment, as well as safety conditions (a model checker can then be applied to verify that the system satisfies the safe conditions). A description in the language consists of a track layout for the station under control, train route tables, and circuit diagrams describing the static layout of the circuits implementing the relay interlocking system. The talk will finally touch upon how
the framework is formally developed using the RAISE formal method. Note: Invited seminar talk.
Place: Universität Bremen

Related external organisation
Unknown external organisation
Activity: Talks and presentations › Conference presentations

A Domain-specific, Model-based Approach for Construction and Verification of Railway Control Systems
Period: 23 Jan 2009
Anne Elisabeth Haxthausen (Speaker)
Department of Informatics and Mathematical Modeling
Software Engineering

Description
This talk describes a complete model-based development and verification approach for railway control systems. For each control system to be generated, the user makes a description of the application-specific parameters in a domain-specific language. This description is automatically transformed into an executable control system model expressed in SystemC. This model is then compiled into object code. Verification is performed at different levels: (0) The domain-specific description is validated wrt. internal consistency by static analysis. (1) The crucial safety properties are verified for the SystemC model by means of bounded model checking. (2) The object code is verified to be I/O behavioural equivalent to the SystemC model from which it was compiled.
Note: Invited seminar talk
Place: Christian-Albrechts-Universität zu Kiel

Related external organisation
Unknown external organisation
Activity: Talks and presentations › Conference presentations

Press clippings:

Returning to the Rails.: Rail Safety: Back in the Spotlight.
Anne Elisabeth Haxthausen
18/03/2016

Description
Article and interview made by Jean Christophe-Piot.

Subject
Rail safety.
Department of Applied Mathematics and Computer Science, Software Engineering

Media contribution (1)

Returning to the Rails.: Rail Safety: Back in the Spotlight.
18/03/2016
Technologist magazine issue no.9, pages 42-43, July 2016, Print
EuroTech Universities
Printed in July 2016.
http://www.technologist.eu/returning-to-the-rails/
Anne Elisabeth Haxthausen
Department of Applied Mathematics and Computer Science, Software Engineering
Press / Media

Ekspert om tysk togkollision: ”Besynderlig ulykke”
Anne Elisabeth Haxthausen
09/02/2016

Description
Interviewed for an article in the Danish newspaper Politiken concerning a train accident in Germany
Subject
A train accident in Germany
Department of Applied Mathematics and Computer Science, Software Engineering

Media contribution (1)
Ekspert om tysk togkollision: “Besynderlig ulykke”
09/02/2016
Politiken, Print
http://politiken.dk/udland/ECE3058885/ekspert-om-tysk-togkollision-besynderlig-ulykke/
Anne Elisabeth Haxthausen
Department of Applied Mathematics and Computer Science, Software Engineering
Press / Media

Matematik mindsker risiko for togkollision
Anne Elisabeth Haxthausen
01/12/2015
Department of Applied Mathematics and Computer Science, Software Engineering

Media contribution (1)
Matematik mindsker risiko for togkollision
01/12/2015
Dynamo nr. 43, Print
Iben Julie Schmidt
Anne Elisabeth Haxthausen
Department of Applied Mathematics and Computer Science, Software Engineering
Press / Media

Matematisk gennembrud øger tog sikkerheden
Anne Elisabeth Haxthausen
01/09/2015
Department of Applied Mathematics and Computer Science, Software Engineering

Media contribution (1)
Matematisk gennembrud øger tog sikkerheden
01/09/2015
DTU Avisen, Print
Iben Julie Schmidt
Anne Elisabeth Haxthausen
Department of Applied Mathematics and Computer Science, Software Engineering
Press / Media