Contents

1. Introduction

REAL-TIME systems are usually characterized by timely computations, which are bounded by *Deadline*, besides correct results of the computations [3]. They are applied in many *safety-critical embedded* systems, which are specialized computer systems designed for safety-critical applications, e.g., the braking system inside the electical/electronic system of vehicles. The braking system applies proportional force on the wheel to the pedal press, consequently, the vehicle must slow down (or halt) before the deadline otherwise accident can occur. Therefore, safety-critical real-time systems should be analyzed rigorously for functional and timing correctness, which is also specified in the functional safety standards such as the ISO 26262 "Road vehicles-Functional safety" [10]. Further, the standard suggests the use *formal methods*, which are mathematical techniques and tools that enable unambiguous specification, modeling and rigorous analysis [22].

In distributed computing [], the safety-critical software is mapped on multiple hardware systems to capitalize on the computational power provided by the distributed architecture, e.g., the braking software can be executed on multiple electronic control units (ECU). Since the distributed software is normally exposed to a greater degree of permanent and transient faults, reliability of the safety-critical software should be maximized to improve dependability of the system which requires additional critical systems resource such as power and energy besides computational resources. However, the embedded hardware is usually resource constrained, therefore, the software should be efficiently mapped to the hardware to conserve critical system resources, thereby accommodate current and future growth of the software functionality.

In this thesis, we apply formal methods to improve the requirements specifications of safety-critical systems, and to analyze the functional and timing behavior of the safety-critical software against the specifications. The safety-critical specifications should be unambiguous, comprehensible, etc [1]. In fact, according to the ISO 26262 standards, semi-formal or formal languages are recommended to specify safety-critical requirements. However, natural language is the de facto method to specify embedded systems requirements in industry because it is intuitive and expressive, though inherently ambiguous [1]. In the context of natural language, template-based specification and controlled natural language are the two most commonly used semi-formal and formal specification methods. The

template-based specification methods, e.g., requirements boilerplates [9], property-specification systems [5], etc., lack meta-model to effectively create templates, and is usually cumbersome to select the templates. The controlled natural languages, e.g., Attempto [8][7], etc., renders the syntax and semantics of the natural language and have formal semantics, however lacks support for embedded systems, hence are less effective. In this thesis, we propose a constrained natural language which is domain-specific and uses the notion of boilerplates to facilitate reuse. The specifications have semantics in Boolean logic and description logic to enable rigorous analysis via Boolean satisfiability [18] and ontology [**?**], respectively.

The specifications are employed in subsequent system development including software design to verify the latter for correct functionality. The software design is usually modeled, simulated and analyzed before implementation. In this regard, Simulink is one of the most widely used development environment for multi-domain, multi-rate, discrete and continuous safety-critical systems in industry [11]. For this main reason, there is increasing interest in formal analysis of Simulink models [19]. Simulink Design Verifier[1], which is based on the Prover[2] model checker, is the de facto tool in the Simulink environment to formally verify Simulink design models. However, it has limited functionality, e.g., it supports only discrete models, has issues with scalability due to state-space explosition, and lacks verification of timed properties [14]. In contrast, we propose a scalable, timed analysis via a statistical model checking [13], which uses traces of executions and statistical analysis techniques, e.g., monte-carlo simulation, etc., first by transformating Simulink models into a network of stochastic time using design patterns of time automata [**?**].

The software design is mapped to hardware, which should take into consideration effectiveness and efficiency. The software should be effectively mapped to the execution platform, that is satisfying the timing and reliability requirements of the distributed safety-critical software. We consider the software is scheduled using a fixed-priority preemptive policy and posses end-to-end timing requirments, and we consider fault tolerance as a means to maximize reliability by employs redundant functionality mapped on different computing units.. Furthermore, the allocation should be efficient so that the power consumption is minimized to ensure extensibility, and increasing complexity of the software, which is evident for instance in the automotive electrical/electronic systems where hundreds of software functions are executed. We propose *exact* and *heuristic* methods, which deliver optimal and near-optimal solutions, respectively, to map the distributed safety-critical software to a network of computing units. Specifically, we propose a formulation of the software allocation as an integer-linear programming (ILP) [16]., subsequently solved via branch and bound, and a hybrid-particle

[1] Simulink Design Verifier - https://se.mathworks.com/products/sldesignverifier.html
[2] Prover - https://www.prover.com/software-solutions-rail-control/formal-verification/

optimization [20], which is meta-heuristic algorithm, to solve large problems [**?**].

1.1 Research Contributions Overview

In this subsection, we give overview of the thesis contributions, and later in Section x, the contributions are further discussed in detail.

- **Formal Analysis of natural language requirements:** we propose a fairly expressive, flexible yet structured and domain-specific constrained natural language, called *ReSA* [15][17]. The language has semantics in Boolean and description logic to support for shallow and rigorous analysis, respectively. The Boolean specifications are checked for consistency using the satisfiability-modulo theory via the Z3 SMT solver. Whereas, the description logic is used to encode the specification as ontology, where we check consistency of the specifications at the lexical level using Reasoner (Inference engine) such Hermit. The ReSA tool, which consists of an editor and implements consistency-checking functionality, is integrated seamlessly into EATOP, which is an open source EAST-ADL IDE, to complement the requirements modeling.

- **Scalable analysis of Simulink models:** we propose a pattern-based, execution-order preserving automatic transformation of atomic and composite Simulink blocks into stochastic timed automata that can be formally analyzed using UPPAAL Statistical Model Checker [2]. Our method is scalable, and has been validated on industrial use cases [6]. The statistical model checker analyzes a state-transition system by conducting statistical analysis on the collected traces of the system executions, effectively mitigating the state-space explosion of (exact) model checking [13].

- **Efficient Power consumption ILP and metaheuristics:** we propose an integer-linear programming (ILP) model to the allocation of distributed software on the network of heterogeneous computing units, which have different processor speed, failure rate and power consumption specifications. The ILP implemented in JAVA using the ILOG CPLEX interface, and subsequently solved the CPLEX solver.

- **Validation on industrial use cases:** Our contributions such as its the ReSA language as well as the proposed formal analysis of Simulink model is validated on industrial use cases, which are provided

Our solutions are evaluated on industrial automotive use cases and on a realistic benchmark. The formal analysis of the natural language requirements

specifications in ReSA and the formal analysis of Simulink models are evaluated on the adjustable speed-limiter (ASL) and brake-by-wire (BBW) systems provided by Volvo Group Trucks Technology (VGTT). ASL is a speed-limitation automotive function which controls the vehicle speed of Volvo trucks from speeding up, and is useful in roads where speed-limitation signs are in place. The ASL use case consists of around 300 requirements, which are specified in natural language, architectural models in EAST-ADL and Simulink models. The integrated software allocation is evaluated on the engine management system benchmark provided by Bosch [] provided for AUTOSAR applications. The benchmark consists of statistics of the schedulable objects, such as mean values, shares of timing specifications and activation mechanisms of the schedulable objects in the system.

1.2 Thesis Outline Overview

The thesis is divided into two parts. The first part is a summary of our research. It is organized as follows: in Chapter 2, we give the background information on description logic, Boolean satisfiability problem, Simulink, stochastic timed automata, and meta-heuristic optimization. In Chapter 3, we explain the research problem and outline the research goals. The thesis contributions are discussed in Chapter 4, followed by the related work in Chapter 5. In Chapter 3, we describe the research method applied to conduct the research. Finally, in Chapter 7, we conclude the thesis and outline possible directions for future work.

2. Preliminary

3. Problem Formulation

The automotive electrical/electronic system executes complex safety-critical software, e.g., x-by-wire software, engine control, traction control, etc. Over the last decades, the complexity of the safety-critical software has been on the rise which is evident on the modern cars, which implement many and complex automotive functions, and also on the emergence of the electrical and autonomous vehicles. Thus, the thesis is motivated by the need for advanced (or rigorous) methods to the requirements specification, modeling and analysis of the complex safety-critical automotive software, and their seamless integration into the existing methods and tools of the automotive systems development at VGTT and Scania. Furthermore, the thesis is motivated by the need for efficient safety-critical software allocation in the distributed computing, to enable the current and future growth of the software functionality.

Thus, the *overall goal* of the thesis is to:

> *provide assurance and extensibility of safety-critical system design, at the various levels of abstraction, via formal analysis and optimization techniques*

The overall goal is refined via *research goals*, which state the needs or concerns that the thesis should address and are formulated as follows:

3.1 Research Goals

Safety-critical automotive systems are developed according to the ISO 26262 standard, including the development processes and methods. The standard highly recommends the use of semi-formal languages to specify safety-critical requirements to improve quality of the specifications, e.g., by reducing ambiguity and improving comprehensibility. In the context of textual representations, the semi-formal specification methods are constrained natural languages, such as templates (or requirements boilerplates), controlled natural languages, e.g., Attempto, PING, etc.

The template-based methods inherently lack meta-model (or grammar), therefore is difficult to add new templates effectively, moreover, template selection is usually cumbersome. The existing controlled natural languages lack effective support of specifying embedded systems requirements.

Thus, the first research goal is to:

RG 1:	*reduce ambiguity and improve the comprehensibility of natural-language requirements using domain-specific knowledge of embedded systems.*

One of the mechanisms to improve natural language specifications is by constraining the language, including its syntax, semantics and the lexicon [12]. The design of a constrained natural language for the specification of requirements is not trivial. By constraining the language, its expressiveness and intuitiveness can be impaired [1][21], therefore, appropriate trade-offs should be made during the design in order to have a robust and effective specification language.

Besides improving quality of individual requirements, the latter should be analyzed in ensemble in order to detect errors that span multiple specifications, e.g., logical contradictions. However, natural language lacks formal (or precise and unambiguous) semantic, therefore is difficult to rigorously analyze (or reason) natural-language requirements specifications. There are several methods to natural language semantics, of which the use of *logic* is widespread.

Thus, the second research goal is to:

RG 2:	*facilitate formal analysis of the requirements specifications through transformation to Boolean and description logics*

Natural language specifications are constructed from syntactic units, such as words, phrases, clauses, statements, etc. Consequently, rigorous analysis of the specifications involve parsing and interpreting the syntactic units, which is a complex problem in computational linguistics [4]. The depth of the interpretation (or semantics) greatly affects the applicability of the methods, e.g., the propositional logic representation of the specifications is simple and the analysis scales well, however, it is shallow as it abstracts away the details. On the other hand, the first-order-logic representations are more rigor, thus enable thorough analysis but are less tractable. Therefore, appropriate interpretation of the natural language specifications is crucial.

The software designs and software-design units (or behavioral models) should conform to the requirements specifications. We consider the software-design units are modeled in Simulink, which is the most widely used model-based development environment in industry to model and simulate the behavior of multi-domain, discrete, continuous embedded systems. Simulink also enables the generation of code from discrete Simulink models which directly execute on specific platforms, thus is crucial to conduct rigorous analysis of the Simulink models to reduce errors introduced at generated code.

The automotive Simulink models that we encounter at VGTT and Scania are in the scale of thousands blocks and realize complex safety-critical functionality. The de facto Simulink analysis techniques, e.g., by type checking, simulation, and formal verification via the Simulink Design Verifier (SDV[1]) are not sufficient to address the full correctness of safety-critical real-time Simulink models. SDV lacks support for checking temporal correctness as specified in timed properties, e.g., in TCTL, and also lacks support for verifying continuous models and suffers from scalability due to its reliance on the exact model-checking [14]. In contrast to the exact model checking, the statistical model-checking verifies properties over sufficiently collected traces of system simulations via statistical methods. It scales better over the trade-off for exhaustiveness.

Thus, the third research goal of the thesis is to:

RG 3: *enable scalable formal analysis of multi-rate and hybrid Simulink models using statistical model-checking*

Simulink consists of connected and hierarchical Simulink blocks, which encode mathematical functions [11]. For industrial systems, the number of blocks in a Simulink model can be in the order of thousands, and the blocks can be triggered with different sampling frequencies for discrete blocks and without any sampling frequency for continuous blocks. Therefore, typical industrial Simulink models are usually complex and comprise mixed signals, multiple rates, discrete and continues Simulink blocks, making the model checking challenging.

In the distributed computing, the automotive software is allocated on multiple computing units (or ECU) consequently is exposed to higher permanent and transient faults, hence necessitate to maximize the reliability of safety-critical systems. Fault tolerance using redundancy is the most widely approach to improve reliability, e.g., using redundant software functionality on multiple ECU, however, it requires additional power consumption. In this regard, the software-to-hardware allocation plays a crucial role to minimize the power consumption of fault-tolerant distributed safety-critical software while satisfying the timing and reliability constraints of the safety-critical software.

Thus, the fourth research goal is to

RG 4: *minimize the power consumption of distributed safety-critical software while satisfying the timing and reliability constraints during the software-to-hardware allocation*

Software allocation is NP hard, and thus is difficult to find an optimal solution in the general case especially for large and complex software

[1] https://se.mathworks.com/products/sldesignverifier.html

allocation problems. In this thesis, we consider fixed-priority preemptive scheduling policy, which is widely used in industry, and, for less complex problems, exact methods, e.g., using integer-linear programming, etc., works, however, for large and complex problems, the exact methods are limited, in stead, heuristics is usually applied. Considering exact timing and reliability analysis, the software allocation that is effective and efficient is not trivial.

In order to show the validity of our proposed solutions, a working prototype should be developed and should also evaluated on industrial uses cases. The validation should consider scalability and engineer-friendliness of methods and tools besides effectiveness.

Thus, the last research goal is to:

RG 5:	*Provide automated and engineering-friendly support for the requirements specification, software allocation of embedded and formal analysis of Simulink models.*

Seamless integration of our proposed methods and tools into the existing development process require close cooperation between the domain experts and the practitioners. The role of the domain experts should be to simplify usage of the tools, e.g., by rendering their interface to existing once, etc., and the practitioners should cooperate from providing to materials to the validation of the tools, which is not trivial considering the challenge of formal methods, and companies culture for being restrictive.

4. Contributions

5. Research Method

6. Related Work

7. Conclusions and Future Work

Bibliography

[1] ISO/IEC/IEEE International Standard - Systems and software engineering – Life cycle processes –Requirements engineering. *ISO/IEC/IEEE 29148:2011(E)*, pages 1–94, 12 2011.

[2] Peter Bulychev, Alexandre David, Kim Gulstrand Larsen, Marius Mikučionis, Danny Bøgsted Poulsen, Axel Legay, and Zheng Wang. UPPAAL-SMC: Statistical Model Checking for Priced Timed Automata. *Electronic Proceedings in Theoretical Computer Science*, 2012.

[3] Giorgio C Buttazzo. Hard real-time computing systems: Predictable scheduling algorithms and applications. *Computers & Mathematics with Applications*, 2003.

[4] Alexander Clark, Chris Fox, and Shalom Lappin. *The Handbook of Computational Linguistics and Natural Language Processing*. 2010.

[5] Matthew B. Dwyer, George S. Avrunin, and James C. Corbett. Patterns in property specifications for finite-state verification. In *Proceedings of the 21st international conference on Software engineering - ICSE '99*, 1999.

[6] P. Filipovikj, N. Mahmud, R. Marinescu, C. Seceleanu, O. Ljungkrantz, and H. Lönn. *Simulink to UPPAAL statistical model checker: Analyzing automotive industrial systems*, volume 9995 LNCS. 2016.

[7] Norbert E. Fuchs, Kaarel Kaljurand, and Tobias Kuhn. Attempto Controlled English for Knowledge Representation. pages 104–124. Springer, Berlin, Heidelberg, 2008.

[8] Norbert E Fuchs and Rolf Schwitter. Attempto Controlled English {(ACE)}. *CoRR*, cmp-lg/960, 1996.

[9] Elizabeth Hull, Ken Jackson, and Jeremy Dick. *Requirements Engineering*. Springer London, London, 2011.

[10] ISO26262 ISO. 26262: Road vehicles-Functional safety. Technical report, ISO/TC 22/SC 32 Electrical and electronic components and general system aspects, 2011.

[11] Thomas L. Harman James B. Dabney. *Mastering Simulink*. Pearson, 2003.

[12] Tobias Kuhn. A Survey and Classification of Controlled Natural Languages. *Computational Linguistics*, 40(1):121–170, 3 2014.

[13] Axel Legay, BenoÃ®t Delahaye, and Saddek Bensalem. Statistical Model Checking: An Overview. pages 122–135. Springer, Berlin, Heidelberg, 2010.

[14] Florian Leitner and Stefan Leue. Simulink Design Verifier vs. SPIN a Comparative Case Study. *Proceedings of FMICS*, 2008.

[15] N Mahmud, C Seceleanu, and O Ljungkrantz. ReSA Tool: Structured requirements specification and SAT-based consistency-checking. In *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pages 1737–1746, 9 2016.

[16] Nesredin Mahmud, Guillermo Rodriguez-Navas, Hamid Reza Faragardi, Saad Mubeen, and Cristina Seceleanu. Power-aware Allocation of Fault-tolerant Multi-rate AUTOSAR Applications. In *25th Asia-Pacific Software Engineering Conference*, 12 2018.

[17] Nesredin Mahmud, Cristina Seceleanu, and Oscar Ljungkrantz. ReSA: An ontology-based requirement specification language tailored to automotive systems. In *2015 10th IEEE International Symposium on Industrial Embedded Systems, SIES 2015 - Proceedings*, pages 1–10, 2015.

[18] Sharad Malik and Lintao Zhang. Boolean satisfiability from theoretical hardness to practical success. *Communications of the ACM*, 52(8):76, 2009.

[19] Karthik Manamcheri, Sayan Mitra, Stanley Bak, and Marco Caccamo. A step towards verification and synthesis from simulink/stateflow models. In *Proceedings of the 14th international conference on Hybrid systems: computation and control - HSCC '11*, page 317, New York, New York, USA, 2011. ACM Press.

[20] Seyedali Mirjalili. Particle swarm optimisation. In *Studies in Computational Intelligence*. 2019.

[21] Andriy Myachykov, Christoph Scheepers, Simon Garrod, Dominic Thompson, and Olga Fedorova. Syntactic flexibility and competition in sentence production: The case of English and Russian. *Quarterly Journal of Experimental Psychology*, 2013.

[22] Gerard OâRegan. Concise guide to formal methods, 2017.