Runtime Verification of Railway Applications with Extended Live Sequence Charts

D I S S E R T A T I O N

zur Erlangung des akademischen Grades
doctor rerum naturalium
(Dr. rer. nat.)
im Fach Informatik

eingereicht an der
Mathematisch-Naturwissenschaftlichen Fakultät
Humboldt-Universität zu Berlin von

Herr M.Eng. Ming Chai
geb. am 21.02.1986 in Hebei

Präsident der der Humboldt-Universität zu Berlin:
Prof. Dr. Jan-Hendrik Olbertz

Dekan der Mathematisch-Naturwissenschaftlichen Fakultät:
Prof. Dr. Elmar Kulke

Gutachter:
1. Prof. Dr. Hogler Schlingloff
2. Prof. Dr. Joachim Fischer
3. Prof. Dr. Martin Leucker

Tag der mündlichen Prüfung: December 21, 2015

Berichte aus der Informatik

Ming Chai

Runtime Verification of Railway Applications with Extended Live Sequence Charts

Shaker Verlag
Aachen 2016

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Berlin, Humboldt-Univ., Diss., 2015

Printed in Germany.

ISBN 978-3-8440-4333-4
ISSN 0945-0807

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

Abstract

Even with most advanced quality assurance techniques, the correctness of complex railway software is hard to be guaranteed. To solve this problem, this thesis uses runtime verification to provide on-going protection during the operational phase. Runtime verification is performed by checking whether an execution of a running computational system satisfies a given monitoring property.

A problem with most runtime verification systems is that the formalisms are often complicated. This thesis proposes extensions of live sequence charts (LSCs) which avoid this problem. It extends the standard LSCs as proposed by Damm and Harel by introducing the notion of "necessary pre-charts", and by adding concatenation and iteration of charts. With the language of extended LSCs (eLSCs), necessary and sufficient conditions of certain statements can be intuitively specified. Moreover, similar as for message sequence charts, sequencing and iteration allow to express multiple scenarios. To express data-relevant properties, the language of parametrized eLSCs (PeLSCs) is defined by introducing condition and assignment structures. Monitors are generated through translating eLSCs and PeLSCs into linear temporal logic formulae and hybrid logic formulae, respectively. This thesis determines that the complexities of the word problem for the languages are both linear with respect to the lengths of input traces.

In practice, an observed execution of a system may contain uncertainties. According to the impact on a monitoring result, this thesis divides various sources of uncertainties into incompleteness and inaccuracy. This thesis proves that a five-valued logic is sufficient to express both of the two dimensions of uncertainties in a monitoring result. The semantics for eLSCs and PeLSCs are extended on basis of the five-valued logic. An efficient formula rewriting algorithm is developed, which allows to record only the last part of the observations necessary to perform the checking.

The proposed monitoring approach is used to test a concrete example of the RBC/RBC handover process from the European Train Control System (ETCS) standard. With the language of eLSCs and PeLSCs, it expresses the properties of three functionalities of the process, including the management of communication, the safe functional module of the euroradio and the RBC/RBC handing over. The feasibility of the approach is shown by evaluating it on several benchmarks.

Zusammenfassung

Wegen der Komplexität heutiger Zugsicherungssysteme ist es schwierig, ihre Fehlerfreiheit während des Betriebs zu garantieren. Um dieses Problem zu lösen, wird in der vorliegenden Arbeit untersucht, wie Zugsicherungssysteme mit Hilfe von Laufzeitverifikation abgesichert werden können. Dabei wird geprüft, ob die Aktionen des laufenden Rechensystems im Betrieb eine vorgegebene Eigenschaft erfüllen. Bei der Überprüfung des Systems weisen die meisten Laufzeitverifikationssysteme das Problem auf, dass der Formalismus übermäßig komplex ist. Zur Vermeidung dieses Problems werden in der vorliegenden Arbeit Erweiterungen zu den „live sequence charts“ (LSCs) von Damm und Harel vorgeschlagen. Diese Erweiterungen sind gegeben durch Einführung von „notwendigen Vordiagrammen“ sowie die Konkatenation und Iteration von Diagrammen. Hinreichende und notwendige Bedingungen der Beobachtungseigenschaften können durch diese erweiterten LSC (eLSC) visuell dargestellt werden. Außerdem ermöglichen es eLSCs, die Konkatenation und Iteration von Multi-Szenarien zu formulieren, wie es auch bei herkömmlichen *message sequence charts* (MSCs) der Fall ist. Um datenrelevante Eigenschaften auszudrücken, wird eine Sprache der parametrisierten eLSCs (PeLSC) durch die Einführung von Bedingungs- und Zuweisungsstrukturen definiert. Monitore werden durch die Übersetzung von eLSCs und PeLSCs in Formeln der linearen temporalen Logik (LTL) bzw. hybriden Logik (HL) konstruiert. In dieser Arbeit wird bewiesen, dass die Komplexität des Wortproblems von erweiterten LSCs in Bezug auf die Länge der Zeichenkette linear ist, weshalb ein „online monitoring“ zur Laufzeit möglich ist.

In der Praxis kann die beobachtete Ausführung eines Systems Unsicherheiten enthalten. Abhängig von den Auswirkungen solcher Unsicherheiten auf das Beobachtungsergebnis werden in dieser Arbeit die Ursachen der Unsicherheiten in „Unvollständigkeit“ und „Ungenauigkeit“ kategorisiert. In dieser Arbeit wird der Beweis erbracht, dass eine fünfwertige Logik ausreicht, um die beiden Unsicherheiten im Beobachtungsergebnis auszudrücken. Die Semantik der eLSCs und PeLSCs wird auf Basis der fünfwertigen Logik erweitert. Es wird ein effizienter Algorithmus zur Anpassung der Formeln entwickelt. Dabei wird nur der Teil der Ausführung gespeichert, der für die Verifikation benötigt wird.

Zum Beweis der Effektivität der Formalismen wird die oben genannte Beobachtungsmethode in einer praktischen Fallstudie angewendet, dem RBC/RBC-Übergabeprozess des *European Train Control Systems* (ETCS). Mittels eLSC und PeLSC werden drei Funktionseigenschaften des Prozesses beschrieben. Diese Funktionen enthalten das Kommunikationsmanagement, das Sicherheitsmodul des Euroradios und den RBC/RBC-Übergabeprozess. Die Anwendbarkeit der Methode wird durch verschiedene Benchmarks überprüft.

Acknowledgement

FIRST AND FOREMOST, I want to express my gratitude to my advisor Professor Holger Schlingloff, who takes me on in his highly energetic research group. Over the last four years, I and my ideas have greatly benefited from working with him. I thank him for the systematic guidance and great effort he put into training me in academic.

I acknowledge my gratitude to Professor Tao Tang for bring me into scientific research field. He is my academic role model over the past few years. During the last four years, Stephan Merz and Markus Roggenbach give me a lot of help on my research, and on many other aspects. I would like to sincerely thank them.

Moreover, I am grateful for many stimulating and discussion on the topics of this thesis with Hartmut Lackner, Mario Friske, Stephan Weißleder, Jaroslav Svacina, Lin Zhao and Jintao Liu. Their broad experience and technical insights have directly or indirectly shaped many different aspects of this thesis.

I am thankful to the China Scholarship Council, who provides me finical support during my stay in Berlin in these four years. My very sincere thanks Birgit Heene for her parent-like support, from which I had benefited even before I came to Berlin.

Last, but not least, I would like to dedicate this thesis to my family and my wife Zhuo Huang, for their love, patience, and understanding. Without their unconditional support, I could not have done the thesis.

Contents