VERIFICATION AND VALIDATION OF LOGIC CONTROL SAFETY APPLICATIONS

VERIFIKATION UND VALIDIERUNG VON STEUERUNGSSOFTWARE FÜR SICHERHEITSANWENDUNGEN

Dissertation

zur Erlangung des Grades

der Doktorin der Ingenieurwissenschaften

der Naturwissenschaftlich-Technischen Fakultät II

- Physik und Mechatronik -

der Universität des Saarlands

von

Doaa Soliman

Saarbrücken

2012

Tag des Kolloquiums:	06.12.2012
Dekan:	Univ.-Prof. Dr. rer. Nat. Helmut Seidel
Mitglieder des Prüfungsausschusses:	Prof. Dr.-Ing. Michael Vielhaber
	Prof. Dr.-Ing. Georg Frey
	Prof. Dr.-Ing. Holger Voos
Akademischer Mitarbeiter:	Dr.-Ing. Tilman Sauerwald

Berichte aus der Automatisierungstechnik

Doaa Soliman

Verification and Validation of Logic Control Safety Applications

Verifikation und Validierung von Steuerungssoftware für Sicherheitsanwendungen

Shaker Verlag
Aachen 2013

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.: Saarbrücken, Univ., Diss., 2012

Printed in Germany.

ISBN 978-3-8440-1757-1
ISSN 0945-4659

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

ACKNOWLEDGEMENTS

I am heartily thankful to my supervisor, Georg Frey, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

I would also like to thank Professor Kleanthis Thramboulidis for the continuous support throughout my PhD study and research, for motivation, and immense knowledge.

Lastly, I offer my regards and blessings to my colleagues and all of those who supported me in any respect during the completion of this thesis.

Doaa Soliman

Contents

ABSTRACT

Functional Safety according to the safety standard IEC 61508 is a major concern in the design of automation systems today. Many of those systems are realised using Programmable Logic Controllers (PLCs) executing software applications programmed according to the programing standard IEC 61131-3. PLCopen as an IEC 61131 user organisation specified a Function Block (FB) library to be used in safety-related applications. However, safety applications built up from safety FBs are still needed to be verified against the given safety specification.

In the presented work, a methodology of verifying and validating PLC safety applications built up from PLCopen safety FBs is introduced. To allow formal analytical approaches, the application is translated into a system of timed automata models. This formal model is used in the UPPAAL model checker tool for formal verification and simulative validation.

To ease the application of the presented methodology, the transformation process of PLCopen safety applications to UPPAAL timed automata is automated. A library of timed automata models in UPPAAL, corresponding to the safety FB library in PLCopen, is defined, verified and validated. The transformation of a safety application that uses these automata as building blocks for the formal model is introduced. For this transformation a software tool is developed.

To demonstrate the applicability of our methodology, it is applied to a laboratory system as part of an upgrading process of a legacy system to conform to safety standards.

KURZFASSUNG

Funktionale Sicherheit nach IEC 61508 umzusetzen ist heutzutage eine der größten Herausforderungen im Design von Automatisierungssystemen. Viele dieser Systeme werden mittels einer Speicherprogrammierbaren Steuerung (SPS) realisiert, welche nach IEC 61131-3 erstellte Steuerungssoftware ausführt. PLCopen, eine Nutzerorganisation mit Fokus auf IEC 61131, spezifizierte in diesem Kontext eine Bibliothek von Funktionsblöcken (FB) zur Verwendung in sicherheitsrelevanten Anwendungen. Dennoch müssen mithilfe dieser Bibliothek erstellte Sicherheitsanwendungen hinsichtlich gegebener Sicherheits-Spezifikationen überprüft werden.

Diese Arbeit präsentiert eine Methodik zur Verifikation und Validierung von SPS-Sicherheitsanwendungen, welche aus Funktionsblöcken der PLCopen-Bibliothek erstellt werden. Um formale Analyseansätze verwenden zu können, wird die Sicherheitsanwendung zunächst in ein System aus Modellen zeitbehafteter Automaten überführt. Das entstandene formale Modell kann durch den UPPAAL-Modelchecker formal verifiziert und simulativ validiert werden.

Zur einfacheren Anwendbarkeit der vorgestellten Methodik wird die Überführung der PLCopen-Sicherheitsanwendung in zeitbehaftete Automaten nach UPPAAL automatisiert. Hierzu wird eine Modellbibliothek zeitbehafteter Automaten in UPPAAL definiert und verifiziert, die mit der PLCopen-FB-Bibliothek korrespondiert. Die Überführung in das formale Modell nutzt jene Automaten als Blöcke, zur Automatisierung wird ein Software-Tool entwickelt.

Um die Anwendbarkeit der Methodik zu demonstrieren, wird ihr Einsatz bei der sicherheitstechnischen Modernisierung einer Laboranlage beschrieben.