

**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

Copyright Shaker Verlag 2013

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

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](http://www.shaker.de) • e-mail: [info@shaker.de](mailto: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 .....	iv
KURZFASSUNG .....	v
1 INTRODUCTION .....	1
1.1 Related Work and Problem Definition .....	1
1.2 Goals and Objectives .....	2
1.2.1 Qualified PLC editor .....	4
1.2.2 Approach to build a SFB TA library .....	5
1.2.3 Approach to transform a safety application to TA models .....	6
1.2.4 Approach for verification and validation .....	6
1.2.5 Transformation tool SA2TA .....	7
1.3 Case Study .....	8
1.4 Organisation .....	9
2 VERIFICATION AND VALIDATION .....	11
2.1 Description of PLCopen Specifications .....	12
2.1.1 Complete description of a SFB: SF_Equivalent .....	12
2.1.2 Complete description of a safety application .....	15
2.2 Constructing the SFB Library in UPPAAL for Verification .....	18
2.2.1 State diagrams .....	18
2.2.2 Timed automata .....	19
2.2.3 Approach to transform a state diagram to timed automaton .....	22
2.2.4 Temporal logic .....	26
2.2.5 Approach for formalisation of SFBs in UPPAAL .....	30
2.3 Verification and Validation of a Safety Application .....	35
2.4 Tasks of the Transformation Tool .....	42
2.5 Summary .....	44
3 CONSTRUCTING SFB LIBRARY IN IL .....	45
3.1 Implementation of SFBs in a PLC Programming Tool .....	45
3.1.1 The approach of converting a state diagram to IL code .....	46
3.2 Implementation of a Safety Application .....	50
3.3 Summary .....	51
4 THE TOOL SA2TA .....	53
4.1 Related Work .....	53
4.2 Semi-automatic V&V Process .....	55

4.3	Meta-models of Source and Target Domains.....	56
4.3.1	PLCopen XML meta-model.....	56
4.3.2	UPPAAL XML meta-model.....	58
4.3.3	General transformation rules based on meta-models.....	59
4.4	Formal Definitions of FBD and UPPAAL Timed Automata System.....	60
4.4.1	Function Block Diagram (FBD).....	60
4.4.2	UPPAAL TA System.....	64
4.4.3	Transformation rules based on formal definitions.....	68
4.5	Case Study.....	71
4.5.1	Constructing the safety application in FBD.....	73
4.5.2	Extracting simulation scenarios.....	75
4.5.3	Transforming the safety application into UPPAAL TA.....	75
4.5.4	Verification process against extracted simulation patterns.....	78
4.5.5	Validation process.....	79
4.6	Summary.....	80
5	METHODOLOGY TO UPGRADE LEGACY SYSTEMS.....	81
5.1	Introduction.....	81
5.2	Integrating Safety Engineering with the Development Process.....	83
5.3	XY Table Laboratory Case Study.....	84
5.4	Proposed Approach.....	85
5.4.1	Preliminary Hazard Analysis.....	86
5.4.2	Design of safety system and solution dependent Hazard Analysis.....	93
5.4.3	Verification of the safety application.....	95
5.4.4	Safety integration.....	96
5.5	Summary.....	98
6	CONCLUSIONS.....	99
	LIST OF FIGURES.....	101
	APPENDIX A.....	103
	APPENDIX B.....	107
	REFERENCES.....	115
	PUBLICATIONS.....	118





## **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 programming 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.