Re-Engineering Approach for PLC Programs based on Formal Methods

Re-Engineering-Ansatz für SPS-Programme auf Basis formaler Beschreibungen

vom

Fachbereich Elektro- und Informationstechnik
der Technischen Universität Kaiserslautern
zur Erlangung des akademischen Grades eines

Doktor der Ingenieurwissenschaften (Dr.-Ing.)

genehmigte Dissertation

von

M.Sc. Mohammed Bani Younis

geb. in Dair Abi Said (Jordanien)

D386

Eingereicht am:	29. Mai 2006
Tag der mündlichen Prüfung:	01. September 2006
Dekan des Fachbereichs:	Prof. Dr.-Ing. Wolfgang Kunz

Promotionskommission	
Vorsitzender:	Prof. Dr.-Ing. habil. Lothar Litz
Berichterstattende:	J. Prof. Dr.-Ing. Georg Frey
	Prof. Dr.-Ing. Luca Ferrarini

Berichte aus der Automatisierungstechnik

Mohammed Bani Younis

Re-Engineering Approach for PLC Programs based on Formal Methods

Re-Engineering-Ansatz für SPS-Programme
auf Basis formaler Beschreibungen

D 386 (Diss. Technische Universität Kaiserslautern)

Shaker Verlag
Aachen 2006

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Kaiserslautern, TU, Diss., 2006

ISBN-10: 3-8322-5674-1
ISBN-13: 978-3-8322-5674-6
ISSN 0945-4659

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • E-Mail: info@shaker.de

Acknowledgements

I wish to acknowledge and thank those people who contributed to this thesis:

Much heartiest to my supervisor, Prof. Georg Frey who has provided me with a lot of advice and help throughout the four years of my PhD studies. He has always been there to help and support not only in my work. His support was from the first time I met him with a vague knowledge about the programmable logic controllers up to the submitting of my thesis.

I am grateful to the reviewers of this thesis, Prof. Georg Frey and Prof. Luca Ferrarini for their interest and the time and effort they invested in reviewing this thesis. My overwhelming thanks to the evaluation committee chair Prof. Dr.-Ing. habil Lothar Litz.

I would like to thank my colleagues who have created a very pleasant atmosphere in the Juniorprofessorship Agentbased Automation and stood beside to me till the end of the work. Working at Juniorprofessorship Agentbased Automation in Kaiserslautern is as being part of a team, as well as part of a family. During this period I have gained fruitful memories I will never forget.

A special thank goes to Dr. Bruno Denis from the LURPA in Cachan for the interest in my work and for the long term interesting discussions which have aid me a lot in my work.

Thank you very much my master thesis supervisor Dr. Roland Hecker whom through his support and heedfulness I came to the decision to start my promotion.

Thanks to Tanvir Hussain and Florian Wagner for the support and proof reading of the manuscript. Without their help there could be considerably more errors and flaws in this thesis. Any errors or shortcomings are my responsibility alone.

I am forever indebted to my wife Ghadeer for her understanding, endless patience and encouragement when it most needed. I must thank to my family. I would not be where I am today without them. Thank you Mum, Dad.

Last, but not least, I would like to dedicate this thesis to my Parents, my wife, my son Bassem and my daughter Tuqa, for their love, patience, and understanding—they allowed me to spend most of the time on this thesis. For the past five months, my son kept on reminding me: “Papa, go to Uni. and write your thesis”!

Kaiserslautern, September 2006 Mohammed Bani Younis

Abstract

Today there is a standard for the implementation of programs on Programmable Logic Controllers (PLCs). Furthermore there are methods for the formal development of these programs. The standard allows the interchange of algorithms (e.g. if a new hardware should be used) and the formal methods allow the rigid proof of functionality especially needed in safety critical applications (e.g. using model checking). However, there are a lot of existing PLC programs that have been implemented in proprietary languages before a standard existed and even today formal methods are scarcely used during design. This work outlines a re-engineering approach based on the formalization of PLC programs. The PLC program modules are modeled as Finite State Machines (FSMs). These FSMs are able to communicate with each other to describe the complete dynamic of the PLC system. The resulting formal model can serve as a basis for editing and analyzing the system. The transformation of PLC programs into a vendor independent format and the visualization of its structure is identified as an important intermediate step in this process. It is shown how XML and corresponding technologies can be used for the formalization, visualization, re-implementation, and software measurement of existing PLC programs.

Für die Implementierung von Speicherprogrammierbaren Steuerungen (SPS) existiert heute ein Standard. Darüberhinaus gibt es eine ganze Reihe formaler Entwicklungsmethodiken für SPS-Programme. Während der SPS-Standard den Austausch von Algorithmen ermöglicht (z.B., wenn eine neue Hardware zum Einsatz kommen soll), stellt die Anwendung formaler Methoden die Möglichkeit dar, die Funktionalität der Programme nachzuweisen. Letzteres ist insbesondere für sicherheitskritische Anwendungen unerlässlich. Leider gibt es jedoch eine ganze Reihe bestehender SPS-Programme die implementiert wurden, noch bevor der Standard existierte und selbst heute werden viele Programme noch ohne die Unterstützung formaler Methodiken entworfen. Im Rahmen dieser Arbeit wird ein Re-Engineering Ansatz vorgestellt, welcher auf der Formalisierung von SPS-Programmen beruht. Hierfür werden die SPS-Programmbausteine zunächst auf Basis von Automaten (Finite State Machines, FSM) modelliert. Diese FSMs kommunizieren miteinander um die vollständige Dynamik des SPS-Systems abzubilden. Das so entstehende formale Modell kann als Basis für den weiteren Systembearbeitungs- und -analyseprozess verwendet werden. Die Transformation des SPS-Programms in ein vom Hersteller unabhängiges Format stellt ebenso wie die Visualisierung der Programmstruktur einen wichtigen Schritt des Re-Engineering-Prozesses dar. In der Arbeit wird gezeigt, wie XML und die zugehörigen Technologien für die Formalisierung, Visualisierung, Re-Implementierung und Softwarequalitätsmessung vorhandener SPS-Programme verwendet werden können.

Contents