Department of Electrical Engineering, Electronics, Computers, and Systems
PhD Programme in Process Control, Industrial Electronics and Electric Engineering

PhD Thesis:

Bringing Automated Formal Verification to PLC Program Development

A Thesis submitted by Borja Fernández Adiego for the degree of Doctor of Philosophy in the University of Oviedo.

Supervised by:
Dr. Víctor Manuel González Suárez
Dr. Enrique Blanco Viñuela
A mis abuelos Alberto y Fernando.

“Yes, there are two paths you can go by,
but in the long run, there’s still time
to change the road you’re on.”
Led Zeppelin, Stairway to Heaven (1971)
Summary

Automation is the field of engineering that deals with the development of control systems for operating systems such as industrial processes, railways, machinery or aircraft without human intervention. In most of the cases, a failure in these control systems can cause a disaster in terms of economic losses, environmental damages or human losses.

For that reason, providing safe, reliable and robust control systems is a first priority goal for control engineers. Ideally, control engineers should be able to guarantee that both software and hardware fulfill the design requirements. This is an enormous challenge in which industry and academia have been working and making progresses in the last decades.

This thesis focuses on one particular type of control systems that operates industrial processes, the PLC (Programmable Logic Controller) - based control systems. Moreover it targets one of the main challenges for these systems, guaranteeing that PLC programs are compliant with their specifications.

Traditionally in industry, PLC programs are checked using testing techniques. Testing consists in checking the requirements on the real system. Although these testing techniques have achieved good results in different kind of systems, they have some well-known drawbacks such as the difficulty to check safety and liveness properties (e.g. ensuring a forbidden output value combination should never occur).

This thesis proposes an alternative for checking PLC programs. A methodology based on formal verification techniques, which can complement the testing techniques to guarantee that a PLC program is compliant with the specifications.

Formal verification is a technique meant to prove the correctness of a system by using formal methods. One of the most popular formal verification techniques is model checking, which consists in checking a
formalized requirement in a formal model of the system. Comparing model checking with testing, model checking explores all the possible combinations of the state space in the formal model to guarantee that the formal requirement is satisfied.

Formal verification and in particular model checking appears to be a very appropriate technique for this goal. However, the industrial automation community has not adopted yet this approach to verify PLC code, even if some standards, like the IEC 61508 [2010], highly recommend the use of formal methods for Safety Instrumented Systems. This is due to following challenges for control engineers: (1) the difficulty of building formal models representing real-life PLC programs, (2) the difficulty of using specification formalisms to express the requirements and finally, (3) when creating formal models out of real-life software, the number of combinations can be huge and model checking tools may not be able to handle the state space, thus cannot evaluate the given requirement.

This research deals with these three main challenges and tries to fill the gap between the industrial automation and the formal verification communities.

The thesis proposes a general methodology for applying automated formal verification to PLC programs and any complexity related to formal methods is hidden from control engineers.

In this methodology, formal models are built automatically out of the PLC programs. The model transformations are divided in two parts: PLC programs, from the IEC 61131 [2013] standard, are translated to an Intermediate Model (IM), which is the central piece of this methodology. The IM is then transformed to the input modeling languages of different verification tools (e.g. nuXmv, UPPAAL or BIP). This modeling strategy simplifies the model transformations and makes the integration of new verification tools easier.

Regarding the requirements formalization, this methodology provides a solution that allows control engineers to express the requirements in a simple and natural language based on patterns with well-defined semantics. Then, these requirements are translated to temporal logic formalisms as they are the most common formalisms used by the verification tools.

Regarding the state space explosion problem, this methodology provides a set of reduction and abstraction techniques that are applied
to the IM. These techniques are a fundamental part of the methodology, as they make the verification of real-life PLC programs, which usually have huge state spaces, possible.

The methodology has been applied to real-life PLC programs developed at CERN. These experimental results have demonstrated the usability of this methodology by control engineers with no experience in formal methods.
Resumen

Automatización industrial es el campo de la ingeniería que se dedica al desarrollo de sistemas de control para operar sistemas como procesos industriales, trenes, maquinaria o aviones sin intervención humana. En la mayoría de los casos, un fallo en estos sistemas de control puede provocar un desastre en términos de pérdidas económicas, daños medioambientales o pérdidas humanas.

Por esa razón, proporcionar sistemas de control seguros, fiables y robustos es un objetivo de primera prioridad para los ingenieros de control. Idealmente, ingenieros de control deberían de ser capaces de garantizar que tanto el hardware como el software satisfacen los requisitos del diseño. Esto es un gran reto en el cual industria y academia han estado trabajando y haciendo progresos en las últimas décadas.

Esta tesis se centra en un tipo particular de sistemas de control que opera procesos industriales, los sistemas de control basados en PLCs (Programmable Logic Controller) y tiene como meta uno de los principales retos para estos sistemas, garantizar los programas del PLC respetan las especificaciones de diseño.

Tradicionalmente en industria, los programas de PLCs son comprobados utilizando técnicas de testeo. Testear un sistema consiste en comprobar los requisitos del diseño en el sistema real. Aunque estas técnicas han logrado buenos resultados en diferentes tipos de sistemas, tiene algunas limitaciones bien conocidas, como son la dificultad de testear propiedades de seguridad o “liveness” (por ejemplo asegurar que un valor prohibido de una variable de salida nunca ocurra en el sistema).

Esta tesis propone una alternativa para chequear programas de los PLCs. Una metodología basada en técnicas de verificación formal, las cuales pueden complementar las técnicas de testeo para garantizar que el programa del PLC respeta sus especificaciones.
Verificación formal es una técnica que tiene por objetivo probar que un sistema está correctamente diseñado o implementado utilizando métodos formales. Una de las técnicas de verificación formal más populares es “model checking”, la cual consiste en comprobar que un requisito formalizado es respetado en un modelo formal del sistema real. Comparando model checking con las técnicas de testeo, model checking explora todas las posibles combinaciones en el modelo formal para garantizar que el modelo respeta el requisito formalizado.

Técnicas de verificación formal y en particular model checking, parecen ser técnicas muy apropiadas para el objetivo de esta tesis. Sin embargo, la comunidad de automatización industrial no ha adoptado aún estas técnicas para verificar el código de los PLCs, incluso si estándares como el IEC 61508 (2010) recomiendan el uso de métodos formales para sistemas de seguridad. Esto es debido a tres factores fundamentales: (1) la dificultad de construir los modelos formales que representan programas de PLC, (2) la dificultad de usar los formalismos para especificar los requisitos del sistema y finalmente, (3) cuando se crea un modelo formal de un software real, el número de combinaciones posibles a explorar puede ser enorme y las herramientas que implementan model checking pueden no ser capaces de explorar el espacio de estados, por lo tanto no pueden evaluar los requisitos dados.

Este trabajo de investigación se centra en estos tres aspectos e intenta cubrir la grieta que existe en las comunidades científicas de automatización industrial y verificación formal.

La tesis propone una metodología para aplicar automáticamente (sin intervención humana) técnicas de verificación formal a programas PLC y toda complejidad relacionada con métodos formales está oculta para los ingenieros de control.

En esta metodología, modelos formales son generados a partir de los programas PLC. La transformación de modelos está dividida en dos partes: los programas PLC, definidos en el estándar IEC 61131 (2013), son traducidos a un modelo intermedio, referenciado como IM en todo el documento por sus siglas en Inglés (Intermediate model). Este modelo intermedio es la pieza central de esta metodología. Más tarde, el IM es transformado en los modelos necesarios para las diferentes herramientas de verificación (por ejemplo, nuXmv, UPPAAL o BIP). Esta estrategia de modelado simplifica las transformaciones entre mo-
delos y hace mucho más sencilla la integración de nuevas herramientas de verificación.

En cuanto la formalización de los requisitos que el programa debe cumplir, esta metodología proporciona una solución que permite a los ingenieros de control expresar los requisitos con un lenguaje natural y sencillo basado en el uso de patrones con una semántica bien definida. Más tarde, estos requisitos son traducidos a lógica temporal, ya es que el formalismo más utilizado por las herramientas de verificación formal.

En cuanto al problema de la explosión del espacio de estados, esta metodología proporciona un conjunto de técnicas de reducción y de abstracción de modelos, las cuales son aplicadas al IM. Estas técnicas son una pieza fundamental de la metodología, ya que hace posible la verificación formal de programas PLC que controlan sistemas industriales reales, los cuales normalmente tiene un espacio de estados enorme.

La metodología ha sido empleada en programas PLC reales desarrollados en el CERN. Los resultados experimentales han demostrado la utilidad de esta metodología, usada por ingenieros de control sin experiencia en métodos formales.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>v</td>
</tr>
<tr>
<td><strong>Resumen</strong></td>
<td>ix</td>
</tr>
<tr>
<td><strong>Acknowledgements</strong></td>
<td>xvii</td>
</tr>
<tr>
<td><strong>1 Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1 Context</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Motivation and objectives</td>
<td>5</td>
</tr>
<tr>
<td>1.3 Contributions of this thesis</td>
<td>6</td>
</tr>
<tr>
<td>1.4 Publications linked to this thesis</td>
<td>8</td>
</tr>
<tr>
<td>1.5 Document structure</td>
<td>10</td>
</tr>
<tr>
<td><strong>2 Background and related work</strong></td>
<td>13</td>
</tr>
<tr>
<td>2.1 Introduction</td>
<td>13</td>
</tr>
<tr>
<td>2.2 PLC-based control systems</td>
<td>14</td>
</tr>
<tr>
<td>2.2.1 Control system classification</td>
<td>16</td>
</tr>
<tr>
<td>2.2.2 Standards</td>
<td>17</td>
</tr>
<tr>
<td>2.2.3 Frameworks</td>
<td>19</td>
</tr>
<tr>
<td>2.2.4 PLC hardware</td>
<td>23</td>
</tr>
<tr>
<td>2.2.5 PLC software</td>
<td>25</td>
</tr>
<tr>
<td>2.3 Formal methods and formal verification</td>
<td>32</td>
</tr>
<tr>
<td>2.3.1 Formal methods</td>
<td>32</td>
</tr>
<tr>
<td>2.3.2 Formal verification</td>
<td>35</td>
</tr>
<tr>
<td>2.3.3 Model checking</td>
<td>37</td>
</tr>
<tr>
<td>2.3.4 Verification tools</td>
<td>44</td>
</tr>
<tr>
<td>2.4 Related work</td>
<td>45</td>
</tr>
<tr>
<td>2.4.1 Testing-based techniques</td>
<td>46</td>
</tr>
<tr>
<td>2.4.2 Formal verification based techniques</td>
<td>47</td>
</tr>
</tbody>
</table>
2.5 Summary of the chapter ........................................... 56

3 Approach ...................................................................... 59
  3.1 Introduction ................................................................ 59
  3.2 General overview of the approach .............................. 62
  3.3 Intermediate model .................................................. 70
    3.3.1 Intermediate model syntax .................................. 70
    3.3.2 Intermediate model semantics ............................... 71
  3.4 Formal specifications ................................................ 73
    3.4.1 Patterns .......................................................... 75
  3.5 PLC hardware modeling ............................................ 79
    3.5.1 PLC inputs ...................................................... 80
    3.5.2 Safety and standard PLCS .................................. 82
    3.5.3 Interrupts and restarts in PLCS ......................... 82
  3.6 PLC code – IM transformation ................................... 83
    3.6.1 General PLC – IM transformation ......................... 84
    3.6.2 ST – IM transformation ..................................... 89
    3.6.3 SFC – IM transformation ..................................... 93
  3.7 Reduction techniques ............................................... 94
    3.7.1 Cone of influence ............................................. 98
    3.7.2 Rule-based reductions ...................................... 104
    3.7.3 Mode selection ............................................... 107
    3.7.4 Iterative variable abstraction ............................... 108
  3.8 IM – verification tools transformation ......................... 130
    3.8.1 IM–nuXmv transformation ................................ 130
    3.8.2 IM–UPPAAL transformation .............................. 137
    3.8.3 IM–BIP transformation ...................................... 148
  3.9 Modeling timing aspects of PLCS .............................. 160
    3.9.1 Realistic approach ........................................... 161
    3.9.2 Abstract approach ........................................... 169
    3.9.3 Refinement between the two approaches ............... 172
  3.10 Process modeling .................................................. 174
  3.11 Verification and counterexample analysis ................... 177
    3.11.1 Counterexample analysis .................................. 178
  3.12 Methodology CASE tool ......................................... 181
  3.13 Summary of the chapter ........................................... 182
## 4 Case studies and measurements

4.1 Introduction ............................................. 185
4.2 UNICOS framework ................................. 186
4.3 UNICOS baseline object case study ............ 191
  4.3.1 Object description and specification .......... 191
  4.3.2 Experimental results regarding model generation 192
  4.3.3 Experimental results regarding verification of complex properties .................. 199
  4.3.4 Experimental results regarding verification of time properties ................. 201
  4.3.5 Counterexample analysis ......................... 205
4.4 Full UNICOS application case study .......... 208
  4.4.1 Process description and specification .......... 208
  4.4.2 Experimental results regarding verification of safety properties ............ 209
4.5 Summary of the chapter ............................. 217

## 5 Evaluation and analysis

5.1 Introduction ............................................. 219
5.2 Evaluation of requirements formalization ....... 220
5.3 Evaluation of PLC hardware and process modeling ... 222
5.4 Evaluation of the PLC program – IM transformation 224
  5.4.1 Evaluation of the time-related transformation rules .......................... 226
5.5 Evaluation of the reduction techniques .......... 227
  5.5.1 Property preserving reduction techniques .... 228
  5.5.2 State space ........................................... 228
  5.5.3 Verification run-time ............................... 229
  5.5.4 Variable abstraction ............................... 231
5.6 Evaluation of the IM – verification tools transformation 233
5.7 Evaluation of the verification results .......... 234
5.8 Correctness of our approach ........................ 235
5.9 Summary of the chapter ............................. 236

## 6 Conclusions and future work

6.1 Discussion .............................................. 239
6.2 Contributions ......................................... 241
  6.2.1 Methodology ......................................... 241
Contents

6.2.2 IM syntax and semantics ........................................... 241
6.2.3 PLC code - IM transformation rules ......................... 242
6.2.4 IM- input verification tools transformation rules .......... 242
6.2.5 Reduction techniques .............................................. 242
6.2.6 Modeling the timing aspects of PLCs ......................... 243
6.2.7 PLC behavior analysis ............................................. 243
6.2.8 Applicability on CERN control systems ...................... 244
6.3 Future work ............................................................. 245

7 Conclusiones y trabajo futuro ........................................ 249
  7.1 Discusión ............................................................... 249
  7.2 Contribuciones ....................................................... 251
    7.2.1 Metodología ..................................................... 251
    7.2.2 Sintaxis y semántica del IM ................................ 252
    7.2.3 Reglas de transformación código PLC - IM ............... 252
    7.2.4 Reglas de transformación IM- modelo para las herramientas de verificación ............................................. 252
    7.2.5 Técnicas de reducción ......................................... 253
    7.2.6 Modelado de los aspectos temporales de los PLCs ....... 253
    7.2.7 Análisis del funcionamiento de un PLC .................... 254
    7.2.8 Aplicación en sistemas de control desarrollados en el CERN ................................................................. 254
  7.3 Trabajo futuro ........................................................ 256

A PLC programs .................................................................. 259
B nuXmv models ................................................................ 277
List of Acronyms .................................................................. 325
List de Figures .................................................................... 329
List of Tables ..................................................................... 333
List of Listings .................................................................... 335
Bibliography ...................................................................... 337
Acknowledgements

This part of the thesis is certainly the most important one for me, as it allows me to thank and express my appreciation to some of the people who have helped me during the years of my PhD candidature.

I would like to start with my supervisors Enrique Blanco Vinuela and Víctor Manuel González Suárez, who gave me the opportunity to work with them during all these years. I am extremely grateful for their wise advices on the scientific and technological aspects of this research.

To all my colleagues from the EN-ICE group at CERN and specially to Philippe Gayet, who gave me the opportunity to be part of this group.

To my colleague Daniel Darvas, who worked with me in this project for the past one and a half years, for his high quality work and the constructive discussions. I am very pleased that Daniel will continue and complement this research during his PhD candidature.

To my colleague Jean-Charles Tournier for his support on the initial idea of this thesis and for the interesting brainstorming and discussions during the last three years.

To my colleague Luis Gómez Palacín, for his help and good advices during the last two years at CERN.

To my colleague Iván Prieto Barreiro, from whom I have learned a lot about different programming languages and with whom I had the pleasure to work closely during my first two years at CERN.

To all my colleagues from the PLC section at CERN, from whom I have learned a lot during all these years and for the great moments I have shared with them in coffee breaks, dinners, etc.

To Efthymia Laderi from CERN and Gemma Hernández Redondo from the Oviedo University for their patience and help on adminis-
trative matters.
To all the members of the RiSD laboratory directed by Prof. Joseph Sifakis at the EPFL University in Lausanne (Switzerland), especially to Simon Bliudze from whom I have learned a lot about formal methods and formal verification.
To András Vörös and Tamás Bartha from the BUTE University in Budapest (Hungary), for the interesting discussions about formal verification applied to safety critical systems.
To Jan Olaf from the RMIT University in Melbourne (Australia), for the interesting discussions about formal semantics and formal verification applied to PLC programs.

Thanks to these five years at CERN, I have met a lot of people from all over the world who are today an important part of my life. Some of these people are Borja, Guillermo, Piotr, David, Pablo, Miguel, Marc, Edu, Cris, Alberto and my friends from the basketball team.
I cannot forget my friends Kostis and Benja with whom I have shared so many great trips and moments.
Me gustaría agradecer a mi profesor y amigo Pepe, por sus consejos para mis estudios universitarios y mi carrera profesional.
A toda mi familia, por su apoyo, cariño y toda la confianza que siempre depositaron en mí. Desde los más jóvenes, Jimena, Jorge, María, Pablo y Alberto, pasando por mi hermano Adrián, hasta mis abuelos Cuca, Fernando, Mari y Alberto y mi bisabuela Abi.
A mis amigos y compañeros de universidad, entre ellos Samu, Edu, Ablanedo y Manu, con los que he compartido grandes momentos.
A mis amigos de La Bañeza, David, Edu, Javi, Ruben, Saúl e Iván, por todos los momentos compartidos, por las risas juntos y porque cualquier problema o mal rato se olvida cuando paso tiempo con ellos.
A Jenny, por su cariño y paciencia conmigo, por todo su apoyo y ayuda en momentos que no fueron muy fáciles para mí.
A mis padres, a los cuales les debo todo. Cualquier persona que les hubiera tenido como padres hubiera conseguido lo mismo o mucho más de lo que yo he conseguido. Mi mayor motivación en mi carrera profesional es hacerles sentir orgullosos, para agredecerles todo su cariño y apoyo incondicional.
Chapter 1

Introduction

In the nineteenth century, the industrial revolution provoked very significant economic and social changes in the human society. From this event until now, the development of new machines and technologies have had an enormous impact on our lives. Industrial automation was created to free humans from tedious monitoring tasks in industrial processes. Since 1910, when Henry Ford automated his automobile assembly plant, industrial automation has been evolving and becoming an essential element in the development of any industry. The transformation of automation technologies, from the first electro-pneumatic devices to the complex programmable controllers existing today, shows the evolution of this industry, led by a high demand of complex and flexible control devices from other industries.

New progresses in control theory and in control technologies, such as distributed systems, have transformed industrial automation into a relevant area of research with an countless number of practical applications in any aspect of our lives.

“Overall, with more than two centuries’ development and evolution, industrial control and automation technologies have so advanced that they benefit us in all aspects of our life and in all kinds of production systems; they are closely integrated with computer hardware and software, network devices and communication technologies; they are faithfully based on modern results in the mathematical and physical sciences.” (Zhang (2010)).

Nowadays, one of the main needs in industrial automation is the ability to design safe, reliable and robust control systems which are
compliant with their specifications. Model-based design and verification of controllers (hardware and software) are some of the research trends in automation nowadays. Software failures in control systems can provoke enormous damages to human beings, to the environment and cause an enormous economic breakdown. One of many unfortunate examples is the software error which provoked the accident of Ariane 5 space rocket from the European Space Agency. The Ariane 5 software was previously tested.

The formal verification community provides solutions to guarantee that a system is compliant with the system specifications, using strong mathematical bases.

This thesis fills the gap between these two communities, industrial automation and formal verification, to make progress in the development of safer, more reliable and more robust control systems, by guaranteeing that the control software is compliant with the specifications. This thesis focuses on PLC (Programmable Logic Controller) – based control systems, as PLCs are the most common control devices used in industry.

It is important to mention that in the automation industry the so-called “Safety Instrumented Systems” (SIS), defined by the IEC 61511 (2003), are systems designed to protect people, environment and industrial installations. With the evolution of technologies these systems are mostly based on programmable controllers, such as PLCs. This thesis concentrates on the software of PLC control systems independently of its purpose. Obviously guaranteeing that the PLC program of a SIS is compliant with the specification is essential and highly recommended by the standards (for example, the IEC 61508 (2010) standard) but this is also desirable in any PLC control system that monitors and regulates an industrial installation. This is because a software bug can provoke significant damages or the cost of fixing this bug is bigger than the cost of using formal methods. Moreover, nowadays industry demands high availability of industrial control systems to maximize the uptime of the controlled process, even if a bug in the code would not provoke a damage to the installation, it could stop the installation which would cause economic losses.

This chapter is divided in the following sections:

1. Section 1.1 presents the general context of this thesis.
1.1. Context

This PhD has been developed under the doctoral student program at CERN (European Organization for Nuclear Research) in collaboration with the University of Oviedo (Spain).

CERN is the biggest particle physics laboratory in the world, located at the border between France and Switzerland. CERN has four main goals:

1. Push forward the frontiers of knowledge in particle physics.
2. Develop new technologies for accelerators and detectors. Many of these technique can also be applied to other industries. The transfer of knowledge and technology is also an important goal of CERN.
3. Train the scientists and the engineers of tomorrow.
4. Unite people from different countries and cultures.

CERN has a particle accelerator complex to perform the experiments and some of these particle accelerator are: PS (Proton Synchrotron), SPS (Super Proton Synchrotron), LINACs (LINear ACcelerators) and LHC (Large Hadron Collider) (See Fig. 1.1). The LHC is the biggest particle accelerator in the world with 27 km of circumference. The goal of this machine is to recreate the conditions that existed immediately after the big bang. To do that, the LHC accelerates two high-energy particle beams (e.g. protons) at close to the speed of light and makes them collide. These collisions that happen at a very high energy level (14 TeV), provide a very valuable insight of the particles by observing their outcome: energies, trajectories and eventually, the creation of
new particles. Some of them are well-known by the physicists but some others are just part of theories and their existence has never been proved. The LHC aims at proving or disproving these theories, which should help in the understanding of the universe. To detect these new particles the LHC has four main particle detectors (ATLAS, CMS, ALICE and LHCb).

![CERN accelerator complex diagram](http://en.wikipedia.org/wiki/CERN)

To produce these high energy collisions, it requires some auxiliary industrial processes (e.g. cryogenics and vacuum systems) to provide the optimized conditions for the particle accelerators and detectors. Moreover, these industrial processes have to be operated automatically, therefore industrial control systems are needed. This research was done at CERN in the ICE (Industrial Controls & Engineering) group inside the EN (Engineering) department, which develops solutions and provides support in the domain of large and medium scale industrial control systems as well as the accelerator systems.

At the Oviedo University, the thesis is supported by the ISA (System Engineering and Automation) area inside the DIEECS (Electric, Electronics, Computers and Systems Engineering) department. ISA focuses its research on the different areas of the automation field.
1.2 Motivation and objectives

Nowadays any industrial installation has to be controlled and operated automatically, looking for these three main objectives:

1. Increasing the quality and efficiency of the process.

2. Enforcing the safety by reducing human interaction with the industrial process.

3. Reducing the costs by optimizing the energy consumption of the installation.

It is obvious that having a control system that contains flaws may cause damages and economic losses to the installation itself, but it also can affect the environment and people. Having a safe, robust and bug-free control system is a common “desire” of designers and developers involved in the project. However, producing a control system that is fully compliant with the project specifications is a very challenging task. The automation industry lacks of modern software engineering best practices to guarantee it and this research is focused on this topic.

Some standards address this problem, specially standards focused on functional safety, like the IEC 61508 (2010). This standard proposes some guidelines for the development of safety systems and their verification (more details about the standard can be found in Chapter 2).

Certainly, the most challenging task is to guarantee that the control system software is compliant with the specification. In industry, many techniques have been applied to achieve this goal, like manual and automated testing or applying simulation. However these techniques have several drawbacks, like the difficulty of checking liveness properties (e.g. “after a manual request from the operator, the valve $v$ will eventually be closed”) or the difficulty of checking all the possible combinations of the state space in a safety property (e.g. “if valve $v$ is closed, then valve $w$ can never be closed at the same time”).

The IEC 61508 standard recommends the use of formal methods to guarantee that the software is compliant with the specifications, specially for systems with a high Safety Integrity Level (SIL), see

\footnote{SIL is an integrity characteristic to measure the risk-reduction provided by a safety function in a safety instrumented system.}
Table 1.1: This table appears in “Part 3: Software requirements (Table A.2, page 37)” of the IEC 61508 (2010) standard.

Table 1.1: Software design and development: software architecture design (see Table 7.4.3 from the IEC 61508 (2010) standard)

<table>
<thead>
<tr>
<th>Technique/Measure</th>
<th>Ref</th>
<th>SIL1</th>
<th>SIL2</th>
<th>SIL3</th>
<th>SIL4</th>
</tr>
</thead>
<tbody>
<tr>
<td>7b Semi-formal methods</td>
<td>Table</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td></td>
<td>B.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7c Formal methods</td>
<td>C.2.4</td>
<td>–</td>
<td>R</td>
<td>R</td>
<td>HR</td>
</tr>
<tr>
<td>8 Computer-aided specification tools</td>
<td>B.2.4</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
</tbody>
</table>

NR: Not Recommended.
R: Recommended.
HR: Highly Recommended.

Programmable Logic Controllers are the most widely used control devices in industry for automation purposes. At CERN, many industrial installation such as the LHC cryogenic system, cooling & ventilation systems, LHC vacuum systems, etc. are controlled by PLCs (e.g. Willeman et al. (2011)). These systems are developed using the so-called UNICOS framework described in Blanco Viñuela et al. (2011).

The fundamental goal of this thesis is to provide a methodology which guaranties that any PLC program is compliant with the project specifications. This methodology is based on applying automated formal verification to PLC programs, hiding the complexity from the control engineers.

1.3 Contributions of this thesis

To the best of the author’s knowledge, this thesis presents several contributions on the field of formal verification of PLC programs, as follows:

1. The internal behavior (informal semantics) of a PLC is described in this thesis. This description is focused on Siemens PLCs as it
1.3. Contributions of this thesis

is one of the two PLC suppliers at CERN. This analysis, which is presented in Chapter 2, is essential to justify the decisions and the modeling strategy.

2. This thesis presents a general methodology for applying automated formal verification to PLC programs. The methodology is based on an Intermediate Model (IM) and PLC programs written in any PLC language from the IEC 61131 (2013) standard can be expressed in this IM. This IM can be transformed to the input modeling languages of many verification tools. In Chapter 3, the methodology is presented in Section 3.2.

3. The syntax and formal semantics of the IM are described. In Chapter 3, the IM is presented in Section 3.3.

4. As the ST and SFC languages are the most relevant languages in CERN PLC control systems, the formal transformation rules from ST and SFC to the IM are described. The rules are presented in Chapter 3, Section 3.6.

5. The methodology is supported by a CASE tool, which is able to generate formal models from ST and SFC PLC programming languages passing through the IM. Currently the tool generates models for the following verification tools: nuXmv [Cavada et al. (2014)], UPPAAL [Amnell et al. (2001)] and BIP [Basu et al. (2011)]. The rules are presented in Chapter 3, Section 3.8.

6. The generated models of real-life PLC programs have usually a huge state space, which cannot be verified by any of the verification tools. Reduction and abstraction techniques are applied to the intermediate model making verification of these programs feasible (including novel and existing algorithms adapted to this methodology, achieving better results than existing solutions).

7. Modeling time and real time systems increases the complexity of the model and the state space. The strategy of modeling the timing aspects of PLC programs is presented. These particular rules are presented in Chapter 3, Section 3.9.
8. The methodology has been applied to real-life systems at CERN, showing the feasibility and applicability of the methodology. The experimental results are presented in Chapter 4.

1.4 Publications linked to this thesis

The following articles were published during the development of this thesis:


4. Fernández Adiego, B., Darvas, D., Tournier, J.-C., Blanco Viñuela, E., and González Suárez, V. M. (2014c). Bringing automated model checking to PLC program development – A CERN case study. In *Proc. of the 12th IFAC–IEEE International Workshop on Discrete Event Systems*. This paper presents a case study of applying the proposed methodology to a PLC control system developed at CERN.


Before focusing my research on the formal verification of PLC programs, I studied the most relevant control system frameworks which have been applied mainly in scientific installations. In addition, the real-life PLC programs, presented in experimental results of this thesis, have been developed at CERN using the UNICOS framework. Three papers, in which I have participated, have been published about the UNICOS framework:


1.5 Document structure

This thesis is organized as follows:

Chapter 1: this first chapter describes the context of this thesis, presents the motivation and objectives and gives a general overview of the contributions. It also lists the publications produced out of this research.

Chapter 2: this chapter gives an overview of the two different “worlds” linked to this research, industrial automation and formal verification. Initially, it introduces the chapter explaining the link between both fields. Then, it describes the main features related to PLC-based control systems needed to explain the proposed modeling strategy. Lately, an overview of main concepts of formal verification is introduced. Finally, the related work of formal verification applied to PLC-based control systems is presented.

Chapter 3: this chapter presents the core of this thesis. The proposed methodology is introduced and lately the details of the different steps of the methodology are presented: formalization of requirements, system modeling, reduction techniques, verification strategy and analysis of verification results.

Chapter 4: this chapter presents the experimental results obtained by applying the methodology on real-life CERN control systems. These systems are developed using the UNICOS framework. This framework is introduced in this chapter and the two selected systems are presented.

Chapter 5: this chapter presents an evaluation and analysis of the obtained results.
Chapter 6: this chapter concludes the thesis, summarizing the contributions and results and presenting the future work of this research.

Appendix A: this appendix presents one of the real-life PLC programs, which have been verified applying the proposed methodology.

Appendix B: this appendix presents some of the generated nuXmv models out of the real-life PLC programs.

Lists The thesis finishes with the list of acronyms, figures, tables and bibliography.
Chapter 2

Background and related work

2.1 Introduction

This chapter gives an overview of the relevant concepts of the two fields of study involved in this research: industrial automation and formal verification. The automation concepts are either fundamental to understand the proposed methodology for applying formal verification to PLC programs (e.g. description of hardware and software in PLCs) or relevant in the design of reliable control systems (e.g. standards or frameworks).

Automation, in general, is the use of control systems for operating different equipments such as processes in factories, aircraft, machinery, etc. by reducing human intervention. Many different devices are used as control systems depending on the equipment to be controlled (e.g. digital or analog devices) and the needs of control (e.g. speed, PID regulation). Some of the most common devices are: FPGAs (Field-Programmable Gate Array), industrial PCs and PLCs. PLC is the most popular control device for industrial processes such as cooling and ventilation, oil or chemical processes. PLCs are appropriate devices for processes with both digital and analog instrumentation (e.g. digital and analog valves, temperature sensors, digital pumps, etc.) and with strong requirements in reliability under harsh environment. Section 2.2 describes the main characteristics and concepts of PLC-based control systems that have been taken into account in this
research.

Formal verification is a technique meant to prove the correctness of a system by using formal methods of mathematics. Formal verification and formal methods are also introduced in this chapter. In the last two decades, these techniques have been applied successfully in many different industries such as aircraft, space shuttle, and railway systems. The related work section presents a brief overview of the applicability of these techniques in other areas. However, despite PLCs are the most common control device for safety and for standard control systems, formal verification is not really applied in this industry yet. Section 2.4 presents a detailed overview of the different techniques designed to check PLC programs and the differences with this thesis approach.

2.2 PLC-based control systems

The first PLC was born in 1968, when GM Hydramatic asked for an alternative to replace all the hard-wired relay systems by a programmable alternative. The company Bedford Associates came with the winning proposal and the first PLC was created. This first prototype was called 084. Bedford Associates started a new company dedicated to develop, manufacture, sell, and service this new product: Modicon, which is currently property of Schneider Electrics (Schneider Electrics automation website (2014)). One of the person who worked on that project was Dick Morley, who is considered to be the “father” of the PLC.

The PLC is the most widely-used programmable electronic device designed for controlling industrial processes. Even if other kind of controllers, such as industrial PCs, are more powerful, sophisticated and offer more alternatives in terms of programming capacities, PLCs remain the most popular control device due to its reliability and robustness in industrial environments.

A PLC mainly consists of a processing unit and peripheries to connect with sensors and actuators of the process or with other electronic devices.

This thesis is based on Siemens PLCs (Siemens automation website (2014)), as they are widely used at CERN. Although some minor differences exist with the models produced by other manufacturers,
they all have a common PLC architecture described in the [IEC 61131 (2013)] standard.

Industrial control systems are traditionally divided in three main layers:

1. Supervision: this layer provides the interface with the process operator. The tool is usually called SCADA (Supervisory Control and Data Acquisition). It is in charge of showing the process variables to the operator, storing their values in databases and giving access to the operator to send manual orders to the control layer.

2. Control: this layer is composed of the control devices (e.g. PLCs) which contain the logic to automatize the process.

3. Field: this layer is in contact with the process to be controlled. It is composed of sensors, which take the information from the process, and actuators, which execute the orders given by the control layer.

Note that modern control systems include more parts (layers or sub-layers) to this traditional architecture. For example MES (Manufacturing Execution System) or ERP (Enterprise Resource Planning). Fig. 2.1 shows a common representation of the control system layers.

![Figure 2.1: Control system layers](image-url)
2.2.1 Control system classification

Independently of the use of PLCs or other control device, industrial control systems can have many different classifications based on the characteristics of the control layer: type of control applied to the process, controllers architecture, its purpose, etc.

Regarding the control applied to the process, an industrial control system can be classified as:

- Open-loop control system: it is a control system that only uses the current state of the input values and the program of the controller. It does not use feedback to guarantee if the output has the intended value due to the input request.

- Closed-loop control system: it is a control system that uses the current state of the input values, the program of the controller and some information from the output of the system that is returned back to the input and computed by the control program.

Regarding the controllers architecture, an industrial control system can be classified as:

- Centralized control system: it is a control system managed by a single controller, which contains the whole control logic.

- Distributed control system (DCS): it is a control system which is managed by more than one controller. In these systems the logic is split into different controllers. The controllers use field buses for the communication between them. The IEC 61499 (2013) standard proposes a methodology to design distributed systems based on function blocks (this concept is introduced in Section 2.2.5).

Please note that very often in industry the term DCS may refer to a distributed system in terms of the supervision layer, where different servers store the information from the industrial process in a database (usually a distributed database). Both architectures can be combined in the same control system.

Both centralized and distributed control systems can have a decentralized periphery, which uses field buses to communicate with the
2.2. PLC-based control systems

controllers. Some of the most common field buses are Modbus (Modbus website (2014)), Profibus and Profinet (Profibus - Profinet website (2014)).

Regarding the purpose, an industrial control system can be classified as:

− Standard control system: it is a control system dedicated to control and monitor the industrial process.

− Safety control system: it is a control system dedicated to protect people, environment and installations. They are defined by the IEC 61508 (2010) standard as SISs and their goal is to provide Functional Safety, which increases the reliability of the global system.

2.2.2 Standards

When developing industrial control systems, the developer should follow a set of rules to guarantee certain common requirements, such as safety, maintainability or quality of control code. These rules, presented as guidelines, are given by the standards. There are several international organizations in charge of producing standards. The two more relevant organizations for the standardization in the automation discipline are:

− IEC (International Electrotechnical Commission): it is the world’s leading organization that prepares and publishes international standards for all electrical, electronic and related technologies (International Electrotechnical Commission website (2014)).

− ISA (International Society of Automation): is a leading, global, nonprofit organization that prepares and publishes international standards for automation (International Society of Automation website (2014)).

Other organizations, like ISO (International Organization for Standardization website (2014)) or CENELEC (European Committee for Electrotechnical Standardization website (2014)) in Europe, are also relevant in the automation community.

Below a summary of the most relevant standards in the development or industrial control systems is presented:
Chapter 2. Background and related work

1. **IEC 61131 (2013)** standard: it is a general standard for programmable controllers. It is divided into eight parts and it describes the main features of programmable controllers, such as equipment requirements, programming languages, guidelines for the application and implementations of these languages, etc. It is important to emphasize that PLC programming languages from different vendors have been developed or adapted, following the recommendations of this standard, although there are some minor differences between them. Five languages are defined by this standard, three graphical languages and two textual languages: Ladder diagram (LD), Function block diagram (FBD), Sequential function chart (SFC), Structured text (ST) and Instruction list (IL).

2. **IEC 61499 (2013)** standard: this standard extends the concept of function block (FB) defined in the IEC 61131 standard. The extension has the goal of improving this concept using object-oriented features. It also describes a methodology to design the control software based on these FBs. Fig. 2.2 shows the representation of the proposed FB by this standard. This FB is composed of the ECC (Execution Control Chart) and the control algorithms. The execution of these algorithms is triggered by the ECC, which is an event-driven state machine similar to the well-known Harel Statecharts.

3. **ISA 88 (2010)** standard: this standard focuses on the batch process control. It provides a methodology to design control systems for this particular case of processes, with the goal of optimizing the production in a flexible way. It is divided into four parts and it describes the applied models and terminology, the data structures, gives some recipe models and provides examples of use.

4. **IEC 61512 (2009)** standard: as the previous standard, it focuses on the batch process control. It is an extended version of the ISA 88. It proposes the creation of a hierarchy of modules to model and control the batch processes.

5. **IEC 61508 (2010)** standard: it is the standard focused on the Functional Safety of Electrical/Electronic/Programmable Elec-
tronic Safety-related Systems (E/E/PE, or E/E/PES). The goal of this standard is to become the reference standard in terms of functional safety to all kind of industries. It provides guidelines for all the needed steps for the development of a SIS. These steps correspond to the so-called Safety Life Cycle, from risk analysis to the decommissioning of the SIS.

6. IEC 61511 (2003) standard: it is a standard about Functional Safety as well, but focused on the industrial process. It provides the definition of safety concepts such as SIS (Safety Instrumented System), SIF (Safety Instrumented Function) and SIL (Safety Integrity Level). SIL is used to categorize the level of safety of a system and it ranges from 1 (for the lowest safety level in this category) to 4 (for the highest safety level in this category).


Figure 2.2: IEC 61499 FB representation

2.2.3 Frameworks

On the top of the standards, several companies and organizations have developed some “frameworks”, with the goal of homogenizing and standardizing the control systems even more. Many control system frameworks can be found in the literature, mostly the ones developed
by research organizations (e.g. CERN, ESRF, etc.) and universities as private companies usually do not publish this knowledge. These frameworks standardize many different aspects of the control systems such as communication protocols, data storage, control code, SCADA visualization, etc. Some of the advantages for using these frameworks are:

- It reduces the development time, as they usually provide some tools dedicated to solve repetitive tasks, for example code generation tools.
- It improves and simplifies the maintenance of the control systems due to the standardization.
- It reduces the chances of having software errors when the framework provides a solution to standardize the control code, due to the reusability of software blocks (e.g. FBs).

As this thesis has been developed at CERN, some of the most relevant control system frameworks applied to big scientific installations are presented in this section. These frameworks are: EPICS, TANGO, FESA and UNICOS.

### 2.2.3.1 EPICS

EPICS (Experimental Physics and Industrial Controls) is a control system framework co-developed by the “Accelerator technology” control group at Los Alamos (Accelerator and Operations Technology website (2014)) and by the “Advanced Photon Source” control group at the Argonne National Laboratory (Advanced Photon Source website (2014)) in USA. This framework was born to provide a solution for control and supervision in big scientific installations, as the control needs of these installation were not available in industry. EPICS provides a standard solution for the communication between the control and supervision layers in distributed systems. Fig. 2.3 shows the EPICS architecture, which is based on a Client - Server model. The communication is based on the “Channel Access” protocol. The first documentation about its architecture can be found in Dalesio et al. (1991). It also provides a set of tools for the control systems developers. They are called the EPICS subsystems (alarm manager, display
2.2. PLC-based control systems

and the OPI (Operator Interface) consists in workstations where the EPICS subsystems are executed. The IOC (Input-Output Controllers) supports real time databases. The hardware is based on VME/VXI systems using VxWorks or RTEMS operating systems.

![EPICS architecture](image1)

In addition EPICS uses a distributed database providing local control for each IOC. It provides data acquisition, data conversion, alarm detection and control closed loops. It provides a timing system for the events synchronization along the network. As it is shown in Fig. 2.4, different control devices can be connected to the IOCs, e.g. PLCs, FPGAs, etc.

![EPICS control system example](image2)

EPICS is used in more than 100 different projects all over the world, mainly in big scientific installations (e.g. DESY website)
Chapter 2. Background and related work

More information about EPICS can be found on the EPICS website (2014).

2.2.3.2 TANGO

TANGO is the European alternative to EPICS. It was developed initially by the control group of ESRF (ESRF website (2014)), and currently more research centers collaborate on the development (e.g. ALBA website (2014)). Nowadays these institutes constitute the TANGO consortium (TANGO website (2014)), which provides a standard solution for the communication between the different elements of the system as it is shown in Fig. 2.5. It was designed for distributed control systems and it uses the object oriented paradigm based on CORBA (CORBA website (2014)). It provides a set of tools for the development of “device servers”. These elements provide access to all the elements of the control system. Thanks to the consortium, it is possible to develop “device servers” and “clients” in different languages, like C++, Java or Python. In addition, TANGO provides several APIs (Application Programming Interface) for the development of these elements. Hardware can range from simple digital input/outputs up to sophisticated detector systems or entire plant control systems. More information about TANGO can be found in Chaize et al. (1999).

![TANGO architecture](Figure 2.5: TANGO architecture)
2.2.3.3 FESA

FESA (Front-End Software Architecture) is an object oriented framework, developed at CERN by the BE/CO group. It generates automatically code for the control layer, which is based on industrial PCs called FECs (Front End Computers). It provides a set of tools for design, development and test of real time software. At the SCADA level, Java applications have been developed to monitor the information from the FECs. At the control level, the so-called FESA classes represent real devices from the instrumentation of the control system. It also provides a Timing system for the synchronization along the network. The LHC control system at CERN is mainly based on FESA. Other scientific institutes started to use FESA, for example, GSI ([GSI website (2014)]). More information about FESA can be found in Peryt and Martín Marquez (2009).

2.2.3.4 UNICOS

UNICOS (UNified Industrial COntrol System) is a industrial control framework developed at CERN by the EN/ICE group ([CERN EN/ICE group website (2014)]). This framework provides a methodology and a set of tools to develop industrial control systems. The experiments presented in Chapter 4 use PLC programs from the UNICOS library and PLC programs developed using this framework. Therefore, this framework is described in detail in Section 4.2.

Control system frameworks are important in this research as they contribute to produce more reliable control systems. However, none of the described frameworks include the use of formal methods in their development process yet. More general information about control system frameworks can be found in Lopez (2006).

2.2.4 PLC hardware

This section describes the main characteristics of the PLC hardware. The concepts presented in this section are fundamental to understand the modeling strategy of the PLC execution platform.
2.2.4.1 Execution schema

The main particularity of the PLC is its execution scheme, the so-called scan cycle. It consists of three main steps:

1. Reading the inputs from periphery to the Input Image Memory (IIM).
2. Executing the user program that reads and modifies the Output Image Memory (OIM) contents.
3. Writing the values to the output periphery.

The PLC reads the information coming from the process (sensors and actuators) and stores it either in the IIM or the OIM. The IIM values are frozen during the execution of the user program.

The execution of the scan cycle can be interrupted if an event (e.g., timer, hardware event, hardware error) triggers the execution of an interrupt handler. The interrupts are preemptive and they are assigned to priority classes in compilation time that will determine their priority.

2.2.4.2 PLC memory

The “data memory” of a PLC is divided into different areas depending on its purpose. The memory can be divided into two main parts (Siemens (1998a); Siemens AG (2010)).

1. One part of the memory is globally accessible and allocated statically. This part stores the image of the input and output values, and the internal computation results.
2. The rest of the memory is only accessible locally and is allocated dynamically. The so-called L Stack is in this part and it stores the temporary data of functions, separately for each priority class.

2.2.4.3 PLC interrupts and restarts

PLC interrupts are described by the IEC 61131 standard. In Siemens PLCs, interrupts trigger the call of Organization Blocks (OBs), which
are the interfaces between the operating system and the PLC program. They have different priorities and therefore a higher priority OB can interrupt any lower priority OB. Restarts are a special case of interrupts and they trigger a specific OB as well.

There are different kind of interrupts in Siemens PLCs, some of the main examples are:

- Time-of-day interrupts (OB10..17). These interrupts are triggered at a specific time on each day or month.
- Cyclic interrupts (OB30..38). These interrupts are triggered cyclically with a defined cyclic time.
- Hardware interrupts (OB40..47). These interrupts are triggered by hardware events (e.g. errors, diagnostics, etc.).
- Startup (OB100..102). These interrupts are triggered when a PLC restart occurs.

2.2.5 PLC software

The third part of the IEC 61131 (2013) standard describes the different software resources, which are necessary to build the user program in PLCs. However, there are some minor differences between the implementations provided by the PLC vendors. The following paragraphs describes the PLC resources given by Siemens PLCs.

2.2.5.1 PLC blocks

In Siemens PLCs, several kinds of program blocks are defined for various purposes Siemens AG (2010).

- A function (FC) is a piece of executable code with input, output and temporary variables. The variables are stored on the L Stack and they are deleted after the execution of the function.

- An organization block (OB) is a special function that can be only called by the system. These are the entry points of the user code. The main program and the interrupt handlers are implemented as OBs.
A data block (DB) is a collection of static variables that can be accessed globally in the program. These variables are stored permanently. The data block does not contain any executable code.

A function block (FB) is a piece of executable code with input, output, static and temporary variables. Static variables are stored in instance data blocks and these variables can be accessed globally, even before or after the execution of the FB. The temporary variables are stored on the L Stack, similarly to the FC’s variables.

2.2.5.2 Programming

There are five PLC languages defined by the IEC 61131 (2013) standard: ST, SFC, Ladder, FBD and IL. The PLC programmer can choose one or several of these languages, depending on the characteristics of the application, to build the PLC code.

ST is the most used PLC programming language at CERN. However SFC and IL are also used:

- ST is a textual high-level language that is syntactically similar to Pascal.
- The SFC language is a graphical programming language based on steps and transitions. It is useful when a part of the PLC program can be conveniently represented as a finite-state machine (FSM).
- The IL language is a low level language that is syntactically similar to assembly.
- The FBD language is a graphical language based on logic gates.
- The Ladder language is a graphical language based on electric circuit diagrams of relay logic hardware.

All these languages are compiled to a common byte code called MC7 and this is the code transferred to the PLC. The MC7 instructions are assumed to be atomic and they cannot be interrupted. A
2.2. PLC-based control systems

A single ST or SFC statement can correspond to several MC7 instructions.

Listing 2.1 shows an example ST code. This example code defines a function block (FB100) with three variables \((a, b, c)\). There is an instance data block (DB1) defined for FB100. In the organization block OB1, the FB100 is called using the instance data block DB1 with input parameter \(a=false\). Then the \(c\) variable of this instance is assigned to the output Q1.0.

```plaintext
FUNCTION_BLOCK FB100
VAR_INPUT
    a : BOOL;
END_VAR
VAR_TEMP
    b : BOOL;
END_VAR
VAR
    c : BOOL;
END_VAR
BEGIN
    b := NOT a;
    c := b;
END_FUNCTION_BLOCK
DATA_BLOCK DB1 FB100
BEGIN
END_DATA_BLOCK
ORGANIZATION_BLOCK OB1
VAR_TEMP
    info : ARRAY[0..19] OF BYTE; // reserved
END_VAR
BEGIN
    FB100.DB1(a := FALSE);
    Q1.0 := DB1.c;
END_ORGANIZATION_BLOCK
```

Listing 2.1: Example of ST code

Listing 2.2 shows an example SFC code. It defines a FSM with three states (Stop, Fill, Run) with three possible transitions. The conditions of the transitions are Boolean input variables (StopCond, FillCond, RunCond) and their value is assigned outside of the FSM-representing function block. The graphical representations can be seen in Fig. 2.6 and Fig. 2.7 (this last representation corresponds with screenshot of the SIMATIC tool of Siemens).

```plaintext
FUNCTION_BLOCK FB101
VAR_INPUT
```

Listing 2.2: Example of SFC code
### Listing 2.2: Example of the textual representation of SFC code

```plaintext
Var
  FillCond : BOOL := FALSE;
  RunCond : BOOL := FALSE;
  StopCond : BOOL := FALSE;
END_VAR

INITIAL_STEP Stop: END_STEP
STEP Fill: END_STEP
STEP Run: END_STEP

TRANSITION S_F
  FROM Stop TO Fill CONDITION := FillCond
END_TRANSITION

TRANSITION F_R
  FROM Fill TO Run CONDITION := RunCond
END_TRANSITION

TRANSITION R_S
  FROM Run TO Stop CONDITION := StopCond
END_TRANSITION
END_FUNCTION_BLOCK
```

### Figure 2.6: Example SFC

![Example SFC Diagram](image)

#### 2.2.5.3 Timing behavior of PLCs

PLC control systems can perform timing operations and these operations are very common when controlling industrial processes. Un-
2.2. PLC-based control systems

Understanding the behavior of these operations is essential to justify the proposed modeling strategy.

In standard PLCs, the cycle time is not fixed, but there is an upper limit surveyed by a *watchdog* module. If the PLC cycle time gets longer than this upper limit, e.g. due to an infinite loop in the PLC program, the PLC executes a special part of the program responsible for handling timing errors. By contrast, safety PLCs have a fixed cycle time in order to avoid dangerous situations.

Timing operations, such as timers defined by [IEC 61131](https://www.iec.ch) (2013), can be considered as function blocks that delay a signal or produce a pulse.

Different types of timers can be found in PLCs. The most common timers are TON (Timer On-delay), TOFF (Timer Off-delay) and TP (Pulse Timer) timers. Fig. 2.8 shows the three timer diagrams. All three timers have the same input and output variables. Two input variables: IN and PT. IN is a Boolean input signal and PT is the delay time. And two output variables: Q and ET. Q is the Boolean output variable and ET is the elapsed time.

Figure 2.7: Example SFC (Screenshot from SIMATIC tool by Siemens)
TON: in this timer, the value of $Q$ will be true after the predefined delay ($PT$) when $IN$ performs a rising edge, and it will be false if $IN$ is false. The value of $ET$ is increased until $PT$, starting when a rising edge occurred on $IN$.

TOFF: in this case, the value of $Q$ will be true if $IN$ is true and it will be false after the predefined delay ($PT$) when $IN$ performs a falling edge. The value of $ET$ is increased until $PT$, starting when a falling edge occurred on $IN$.

TP: in this case, the value of $Q$ will be true if $IN$ is true and it will be false after the predefined delay ($PT$), independently of the value of $IN$. The value of $ET$ is increased until $PT$, starting when a rising edge occurred on $IN$.

PLC timers use a specific data type for timing operations called $TIME$. The IEC 61131 (2013) standard defines this data type as a finite variable and states the following:

“The range of values and precision of representation in these data types is implementation-dependent.”

Representing time by a finite variable leads to a non-monotonic time representation as the variable can overflow (c.f. the upper part of §2.9). For example, in Siemens S7 PLCs, the $TIME$ data type is defined as a signed 32-bit integer with a resolution of 1 ms (see Siemens (1998b)), having an upper limit of approximately +24 days and a lower limit of −24 days. However, in Schneider and Beckhoff PLCs, the $TIME$ data type is an unsigned 32-bit integer with a resolution of 1 ms. In this thesis, the signed time interpretation as defined in Siemens PLCs is considered.

The following section presents some fundamental concepts about formal methods and formal verification.
2.2. PLC-based control systems

![Timer Diagrams](image)

(a) TON time diagram

(b) TOFF time diagram

(c) TP time diagram

Figure 2.8: Timer diagrams
Chapter 2. Background and related work

2.3 Formal methods and formal verification

The selected strategy to guarantee that PLC programs are compliant with the specification implies to apply formal verification to these programs. This requires the knowledge and understanding of formal methods and formal verification. This section presents a small review of these two fields of research related to this project.

2.3.1 Formal methods

The term “formal methods” has been defined by many authors. According to NASA (1977), formal methods can be defined as follows:

“The term Formal Methods refers to the use of techniques from logic and discrete mathematics in the specification, design and construction of computer systems and software. The word formal derives from formal logic and means pertaining to the structural relationship (i.e., form) between elements. Formal logic refers to methods of reasoning that are valid by virtue of their form and independent of their content.”

In the last decades, formal methods have proved its importance in the design and implementation of complex and critical systems. The main goal of formal methods is to minimize human interpretation in
the different steps of critical system development, by providing lan-
guages with well-defined semantics.

“That is, reduce the acceptability of an argument to a calculation
that can, in principle, be checked mechanically thereby replacing
the inherent subjectivity of the review process with a repeatable
exercise.” (from NASA (1977)).

Formal methods can be applied in different levels of the develop-
ment process of a system. For example, they can be used to produce
unambiguous system requirements or to facilitate communication be-
tween different steps of the development (i.e. design, implementation
and review process). They can be classified by the level of formaliza-
tion or by the scope of use. Each level of formalization corresponds
to a particular scope of formal methods use, as it is represented in
Table 2.1 from NASA (1977).

Table 2.1: The Range of Formal Methods Options Summarized in
Terms of (a) Levels of Formalization and (b) Scope of Formal Methods
Use.

<table>
<thead>
<tr>
<th>Levels of Formalization</th>
<th>Scope of FM Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Mathematical concepts and notation, informal analysis (if any), no mechanization</td>
<td>Life cycle phases: all/selected</td>
</tr>
<tr>
<td>2. Formalized specification languages, some mechanized support</td>
<td>System components: all/selected</td>
</tr>
<tr>
<td>3. Formal specification languages, comprehensive environment, including automated proof checker/theorem prover</td>
<td>System functionality: full/selected</td>
</tr>
</tbody>
</table>

Therefore formal methods can be applied in different steps of a
system development. Here we enumerate some of the most common
ones:

- Specification and modeling: the use of an unambiguous language
describing a system.
Chapter 2. Background and related work

− Execution/Simulation: formal models are created to simulate them and analyze the behavior of the real system.

− Formal verification: formalized properties are checked against a formal model.

− Refinement: code refinement is the process of proving that two pieces of code behave identically, where one version is more abstract. It can be achieved by using formal methods.

− Test generation: formal models can be used to automatically generate relevant test cases for the real system.

The benefits of using formal methods in the development of critical systems can be summarized in two essential aspects:

1. Discipline: formal methods provide rigor to the design and development processes. A formal proof of correctness can be achieved by using formal methods.

2. Precision: natural languages are ambiguous and open to interpretations. Formal methods provide specification languages with formal semantics that can be used to describe a system or functional requirement with precision.

However, in some industries like industrial automation, formal methods are not widely used. These are the main reasons:

1. Cost: using formal methods is more expensive than traditional alternatives in engineering. The initial cost of using formal methods in the design and development of a system is much higher than other approaches.

2. Limits of computational models: formal models of real-life systems can be too large to be handled by a simulator or model checker.

3. Usability: using formal methods implies a learning process of the formalism and how to use it. This is sometimes a barrier in industry which makes engineers to look for other alternatives.
Traditionally, formal methods are considered highly abstract, extremely rigorous, and very expensive techniques, ignoring some of the theoretical advances that provide solutions for these drawbacks in the last years. However, many success stories can be referenced to prove the applicability and benefits of these techniques in industry.

Under the umbrella of formal methods, a huge range of techniques and languages can be included, for example: Boolean algebra, finite automata, Petri Nets, temporal logic, etc. Some of these concepts are briefly described in the following paragraphs. When using formal methods for verification purposes, a fact has to be taken into consideration: the more expressive the formalism, the less the proof (that a property holds) is amenable to be automatized.


2.3.2 Formal verification

The term verification refers the act of checking requirements on a system as it is shown in Fig. 2.10. In this figure, the requirement specification represents “what the engineer wants” and the implementation “what the engineer gets”. The transformation from the specification (the idea) into the implementation (the real systems) is done by the design process. The verification process consists in checking that the real system “behaves” as it is described in the specifications. The term verification includes both testing (the specifications are checked on the real system) and formal verification.

Formal verification is the act of checking the correctness of a system with respect to a formal property or specification by using formal methods. Formal verification techniques explore all the possible combinations of the state space to prove that the formal requirement is satisfied.

There are two main families of formal verification techniques:

1. Axiomatic verification.
2. Algorithmic verification.
**Axiomatic verification:** it consists in a semiautomatic verification technique based on reasoning about the functional correctness of a structured sequential program, by tracing its state changes from an initial condition $P$ to a final condition $R$ according to a set of self-evident rules (i.e., axioms).

Theorem provers (tools which apply axiomatic verification) are driven by skilled researchers or engineers, and the full automation of the verification process using these techniques is very challenging and in some cases cannot be achieved.

Formally it can be defined as: $\{P\} S \{R\}$, where $P$ is the precondition, $R$ the postcondition and $S$ is the program. The correctness of $S$ is achieved when $P$ holds before the execution of $S$, $S$ terminates and $R$ will hold afterward.

**Algorithmic verification:** it consists in the use of semi-algorithms to check that a global model, which represents the system, meets the given formal requirements. Techniques like model checking or static analysis are included in this category. The main benefit of these techniques is that they are oriented to be fully automatized, avoiding human interaction. The most well-known drawback of these techniques is the state explosion problem of real-life models, but it can be overcome by using appropriate abstraction techniques.

In industry, algorithmic verification is the most popular formal verification technique because it can be automatized. For that reason,
algorithmic verification is the selected verification technique in this thesis. In particular, model checking has been applied to verify PLC programs. The following sections give an overview of this technique.

2.3.3 Model checking

Model checking is an algorithmic verification, which was first described by Edmund Clarke and Allen Emerson in Clarke and Emerson (1982), and also in parallel by Joseph Sifakis in Queille and Sifakis (1982). Due to their contributions in this area of research, they received the Turing award in 2007.

Model checking is an automatic verification technique for finite state systems. Given a global model of the system and a formal property (requirement), the model checking algorithm checks exhaustively that the model meets the property. Three steps are required to perform model checking:

1. Requirement formalization.
2. System modeling.
3. Model checking algorithms execution (model checker).

2.3.3.1 Requirements formalization

Requirements engineering is one of the major research challenges nowadays. The goal of producing a complete and unambiguous specification of a system by engineers is still an utopia in many industries. Requirements engineering can be defined as follows (from Laplante (2013)):

“Requirement engineering is the branch of engineering concerned with the real-world goals for, functions of, and constraints on, systems. It is also concerned with the relationship of these factors to precise specifications of system behavior and to their evolution over time and across families of related systems.”

In order to produce precise and unambiguous requirements, the use of formal methods is required. In model checking techniques, temporal logic is the most common formalism to express the requirements or
properties. Temporal Logic, in general, can be defined as follows (from Bérard et al. (2001)):

“Temporal logic is a form of logic specifically tailored for statements and reasoning which involve the notion of order in time.”

With temporal logic, engineers and researchers can specify ongoing behaviors, rather than input/output relations. There are multiple temporal logic formalisms. The two more extended formalisms are: LTL (Linear Temporal Logic) and CTL (Computation Tree Logic). Other temporal logic formalism are: PLTL (Propositional Linear Temporal Logic) or ACTL (subset of CTL only using the path quantifier $A$).

**LTL:** properties can be expressed as an infinite sequence of states where each state has a unique successor. LTL can use the following temporal operators: $G$ (always), $F$ (future), $X$ (next), $U$ (until). Fig. 2.11 represents the meaning of these LTL operators. The violet shading represents the state space where the atomic proposition $p$ holds.

**CTL:** properties can be expressed as a combinations of path quantifiers and linear-time operators. The possible path quantifiers are: $A$ (for every path) and $E$ (there exists a path). The liner-time operators are: $Xp$ ($p$ holds true next time), $Fp$ ($p$ holds true sometime in the future), $Gp$ ($p$ holds true globally in the future) and $pUq$ ($p$ holds true until $q$ holds true), where $p$ and $q$ are atomic propositions. Fig. 2.12 represents the meaning of these CTL properties. The violet shading represents the state space where $p$ holds.

Some of the properties that can be expressed using CTL and LTL are:

- Reachability Properties: it states that a particular situation can be reached. CTL is more suitable than LTL for expressing reachability properties (i.e. $EFp$).

- Safety Properties: it expresses that, under certain conditions, an specific event should never occurs. Both CTL and LTL can easily express safety properties (i.e. $AG\neg p$ for CTL and $G\neg p$ for LTL).
2.3. Formal methods and formal verification

Liveness Properties: it states that, under certain conditions, some event will ultimately occur. The $F$ operator is the most appropriate for this kind of properties ($AG(p \rightarrow AFq)$ for CTL and $G(p \rightarrow Fq)$ for LTL).

Deadlock-freeness: it states that the system can never be in a situation in which it cannot progress. CTL is more suitable than LTL for expressing reachability properties (i.e. $AGEXtrue$).

More information about the applicability of temporal logic can be found in Bérard et al. (2001).

2.3.3.2 System Modeling

Once the properties to be verified are identified and formally described, the construction of the formal model is the second step. As the formal model consists of an abstraction of the real system, it is important to express those properties that are relevant for verification.
Figure 2.12:CTL operators representation
The first model checking algorithms use an explicit representation of the Kripke structure. Kripke structure consists in a simple abstract machine (a mathematical object) to model a computing machine. It is a graph whose nodes represent the reachable states of the system and whose edges represent state transitions. A labeling function maps each node to a set of properties that hold in the corresponding state. This can be formally defined as follows (from Clarke et al. (1999)):

**Definition 1 (Kripke structure)** Let $AP$ be a set of atomic propositions. A Kripke structure is a 4-tuple $M = (S, S_0, R, L)$, where $S$ is a finite set of states, $S_0 \subseteq S$ is a finite set of initial states, $R \subseteq S \times S$ is the transition relation that must be total, that is, for every state $s \in S$ such that $R(s, s')$ and $L : S \to 2^{AP}$ is a function that labels each state with the set of atomic propositions true in that state.

Nowadays in practice, there are many different formalisms used by model checkers, for example: automata, timed automata, Petri net, etc. More details about different modeling formalism used by model checkers can be found in Bérard et al. (2001).

### 2.3.3.3 Formal definition of model checking

Once the requirements are formalized and the formal model of the system is built, the model checking algorithm can be applied. A general model checking definition can be expressed as follows (from Clarke (2008)):

**Definition 2 (Model checking problem)** Let $M$ be a Kripke structure (i.e., state-transition graph). Let $f$ be a formula of temporal logic (i.e., the specification or property to be checked). Find all states $s$ of $M$ such that $M, s \models f$.

This is a so-called global model checking approach.

### 2.3.3.4 Model checking approaches

Formal models representing real-life systems usually have a huge state space. The state space exploration performed by model checking algorithms may find the limits. For that reason, researchers have been working in improving the model checking algorithms and providing
some alternatives, in the last decades. The first proposed algorithms for model checking were called *explicit model checking*, as they store and handle the states individually. In the following paragraphs, two of the most popular model checking approaches are briefly introduced: *symbolic model checking* and *bounded model checking*.

**Symbolic model checking:** Instead of enumerating reachable states one at a time, in 1987 Ken McMillan implemented a version of theCTL model checking algorithm using a symbolic representation of the state space based on BDDs (Binary Decision Diagrams). More information about symbolic model checking can be found in McMillan (1993).

BDDs are data structures where the state space can be encoded. This symbolic representation allowed to verify much larger systems (formal model of $10^{20}$ states and beyond, see Bruch et al. (1992)).

After the first definition of symbolic model checking, many new algorithms have been proposed. Some of them are based on decision diagrams, for example using MDD (Multivalued Decision Diagrams). In addition, other kind of symbolic model checking is based in SMT (Satisfiability Modulo Theories) solvers, consisting in SAT-based algorithms.

**Bounded model checking:** Traditional model checking algorithms consists in the exploration of the full state space. Sometimes this is not needed, or not even possible due to the huge size of some models. Bounded model checking allows to check properties on a part of the state space.

This technique is appropriate for reachability properties (i.e. $EFp$ in CTL). If the evaluation of the property or formula $p$ is false, no answer can be provided, the algorithm will explore a bigger part of the state space until the evaluation is true or the full state space is explored. It is also good for safety (invariant) properties. If a counterexample is found in a part of the state space is a valid counterexample for the whole model (and the model checking can be finished). Some of the advances in this technique can be found in Biere et al. (2003) and Vörös et al. (2011).

Many other techniques meant to optimize the verification process
2.3. Formal methods and formal verification

can be mentioned here. For example, statistical model checking (Legay et al. (2010)), compositional verification (Besalem et al. (2010)), etc. They all propose alternatives and improvements to deal with the state space explosion problem.

In addition to the different model checking algorithms, reduction and abstraction techniques can be applied to the formal models to face the problem of the state space explosion (e.g. cone of influence or predicate abstraction). A review of these techniques for model checking can be found in Radek (2006).

2.3.3.5 Advantages and disadvantages of model checking

Model checking techniques can be found in many different industries, however still some myths about formal methods in general provoke that engineers look for other alternatives (Hall (1990) and Bowen and Hinchey (1995)).

Summarizing the main advantages of applying model checking techniques are:

− It is an automatic verification method.

− Model checking explores all the possible combinations of the state space model to guarantee that a property holds.

− When a property does not hold on the model, a counterexample is produced by the model checker, which contains relevant information to identify the source of the problem.

− Comparing with testing techniques, model checking can check safety or liveness properties, e.g. ensuring that a forbidden output value combination should never occur. This is one of the main limitations of testing.

The main disadvantages of formal verification techniques are:

1. State space explosion.

2. Complexity of building formal models.

3. Difficulty of using property specification formalism like temporal logic.
2.3.4 Verification tools

All the concepts and algorithms mentioned before are implemented in verification tools, which allow engineers to automatize the verification process or guide them at least. Some of the most popular verification tools are:


- **UPPAAL**: it supports timed automata based models and a subset of CTL for property specification. Internally models are represented as CDDs (Clock Difference Diagrams). More information in [UPPAAL website](https://www.uppaal.com) (2014) and [Amnell et al. (2001)](https://www.uppaal.com).

- **BIP**: BIP is a component-based framework for rigorous system design aiming at correctness-by-construction for essential properties of the designed system. A BIP model consists of three layers: Behavior, Interaction and Priority. The BIP framework provides C code generation from BIP models and its verification tool, called DFinder, is specialized in deadlock detection. More information in [BIP website](https://www.bipsite.org) (2014) and [Basu et al. (2011)](https://www.bipsite.org).

- **SPIN**: it performs symbolic model checking on LTL formulas. The modeling language is called PROMELA and it supports embedded C code as part of model specification. More information in [SPIN website](https://spin.sourceforge.net) (2014).

- **KRONOS**: it performs symbolic model checking on TCTL (extension of the temporal logic CTL that allows quantitative temporal reasoning over dense time). Its modeling language is based on timed automaton. More information in [KRONOS website](https://kronos.sourceforge.net) (2014).

- **COQ**: it is a theorem prover which implements a program specification and mathematical higher-level language called “Gallina”. More information in [Coq website](https://coq.inria.fr) (2014).
2.4. Related work

This section presents the related work to formal verification of PLC control systems. As it was mentioned in Chapter 1 the goal of this thesis is to provide a general solution to guarantee that PLC programs are compliant with the specifications, independently of the purpose of the PLC-based control systems.

In addition to safety standards like IEC 61508 (2010) for Safety Instrumented Systems, where guaranteeing the correctness of the control code is a critical task, the automation industry has adopted some solutions trying to minimize the number of errors in PLC programs.

Siemens is one of the most important companies in the development of Safety Instrumented Systems based on PLCs. This company provides the Safety Matrix and the Distributed Safety products, which are software packages integrated in the SIMATIC and TIA portal programming environments for PLCs.

There is an assumption that states that the logic of a Safety Instrumented System program is much simpler than a standard PLC program. The Safety matrix package provides a tool and a methodology that reduces the configuration, testing and maintenance time by merging the traditionally separate steps of creating a cause and effect matrix diagram, and configuring the safety system. It provides a cause and effect matrix diagram where the PLC programmer can describe the safety functions and the PLC code is automatically generated from this matrix. Only very simple Safety PLC programs can be created. The “philosophy” here is to reduce the number of potential error in the code by restricting the PLC program variability to the maximum.

A similar approach is provided by the Distributed safety package, where a library of software blocks (usually FBs), approved by the TÜV (the certification provider TÜV Rheinland website (2014)), which can be used by the programmer to build the safety PLC programs. The goal is to reduce the amount of code produced directly by the PLC
programmer and allow him to reuse these objects.

In addition to these packages, the Siemens programming environment of SIMATIC and TIA portal for safety programs is restricted compared with standard PLC programs which follow the IEC 61131 (2013) standard. For example, only Ladder and FBD languages are allowed, the data types are also restricted (e.g. the data type REAL is not allowed), etc.

All these restrictions in the development of PLC programs from the PLC vendors do not exclude the need of applying testing or other mechanism to check the code against the specifications.

The use of frameworks like UNICOS and the standardization or code generation of safety critical software is essential to reduce the number of potential bugs in the PLC (e.g. Coupat et al. (2014)).

In addition to that, many other tools and methodologies can be applied in the design of safety systems. These tools are usually not specific for PLCs (e.g. LDRA, Exidia, ISOGRAF, RAM commander, etc.). These tools contribute indirectly to guarantee the safety in industrial control systems.

The two main “families” or techniques to check control software against the specifications are testing and formal verification. This section presents the related work divided into these two groups. Then, more details about algorithmic formal verification related work is presented as this is the solution adopted in this thesis.

2.4.1 Testing-based techniques

Testing is a verification technique that implies the check of certain properties or test cases in the real system. In the automation industry, manual and automated testing are the most popular verification techniques. Following the industrial automation standard: ISA 62381 (2010), process control applications testing is done in two main stages: Factory Acceptance Test (FAT) and Site Acceptance Test (SAT). FAT is conducted to check if the requirements of a specification are met. SAT checks if the system meets the requirements and these tests are performed in the real plant.

In academia, some authors propose solutions for checking PLC programs based on testing techniques. For example, in Kramer (2001), a testing approach based on simulation is proposed. In Jee et al.
the authors propose a control and data flow testing coverage criteria to the flow graph in order to generate test cases. The same authors in Jee et al. (2010) provide a test coverage criteria for FBD programs.

Testing activities are very useful and needed techniques in the verification of industrial control systems. However they have some limitations, testing is unable to check effectively safety and liveness properties. This is main reason for us, to adopt a formal verification approach in the verification of PLC programs.

It is important to remark that, testing and formal verification techniques complement each other and for specific parts of a system testing can be more effective than formal verification.

Our paper Fernández Adiego et al. (2013a), briefly describes some of the applied testing techniques for PLC programs at CERN and how they can complement the formal verification approach presented in this thesis.

2.4.2 Formal verification based techniques

The following sections present the related work to this project. Before focusing on related work to formal verification of PLC programs, a brief overview of formal methods applied in different industries is presented here. The goal is to show how extended are formal methods in industries with critical systems.

2.4.2.1 Formal verification in industry

The use of formal methods and formal verification in different industries with critical systems began more than 20 years ago and has many success stories. Nowadays more and more industries integrate formal methods in the design, development and verification of their systems. When talking about the formal verification technique employed, the big majority applied algorithmic verification techniques (e.g. model checking or static analysis).

In some industries with safety critical systems, the use of formal methods has become a common practice. Some of these industries are: aircraft, space, robotic systems, transportation, etc. Here some examples are presented:
Verification and validation of a NASA flight software: static analysis, runtime analysis and model checking were compared to traditional testing with respect to their ability to find seeded errors in a prototype of the Mars Rover controller (Brat et al. (2004)).

Air traffic control systems: formal methods were applied to the CCF (Central Control Facility) display information system at the London Air Traffic Control Centre (Hall and Isaac (1992)).

Train and subway industries: in the subway of Paris, the B method was employed in the specification of new subway line (Behm et al. (1999)). Model checking was applied to the European train control system (Faber and Meyer (2006)). SAT-based model checking has been applied to an interlock railway system (James and Roggenbach (2010)).

There are many examples in the automation industry but mainly restricted to the robotic field. One example can be found in Abdellatif et al. (2012).

In nuclear plants, some examples of using formal methods are: Fukumoto et al. (1998), IAEA (1999), Yoo et al. (2005).

Finally, one of the most advanced industries in the use of formal verification and formal methods is the aircraft industry. An example of the verification of the flight control system can be found in Meenakshi et al. (2007).

All these examples and many more prove the applicability of formal methods in real-life systems. Although different industries have different challenges to solve, these examples inspired this research project of providing a solution for the industrial automation systems.

The application of formal methods for PLCs has been studied in previous works for many years. In Frey and Litz (2000), one of the first studies about the applicability of formal methods and formal verification strategies to PLC programs is presented. The rest of the Section is divided into two parts, corresponding with the two groups of formal verification strategies: axiomatic formal verification and algorithmic formal verification applied to PLC programs.
2.4. Related work

2.4.2.2 Axiomatic formal verification applied to PLC programs

Not many studies or developments are found in the literature when looking for axiomatic verification applied to PLC programs. The reason, as it was mentioned earlier in this chapter (Section 2.3), is that axiomatic verification is difficult to automatize and its success highly depends on the engineer skills.

Some examples of axiomatic verification applied to PLC programs are presented in the following paragraphs.

In Blech and Ould Biha (2011), a proposal of formal semantics of two of the PLC languages (IL and SFC) is presented for verification purposes using the Coq theorem prover.

The paper Xiaoa et al. (2012) presents a modeling strategy of data types, statements and the denotational semantics of PLC program with the “Gallina” language. In addition, the Coq theorem prover is used to prove the correctness of the programs. A similar approach can be found in Chen et al. (2010).

In Mader et al. (2001), the paper reports on the systematic design and validation of a PLC control program for the batch plant. The formal proof of correctness was obtained using the PVS theorem prover and the SPIN model checker. Both strategies are presented and the limitations are discussed.

In Völker and Krämer (1999), the authors suggest to complement testing techniques with compositional theorem proving for FB-based industrial control systems.

In Sadolewski (2011), the Coq theorem prover is applied to PLC programs. The property specification expressiveness is reduced to simple safety assertions.

These approaches cannot be applied to our systems and needs, as one of the main requirements of this project was to hide any complexity related to formal methods to the control engineers. In addition, none of these approaches deals with PLC programs with a significant size, therefore they are not applicable to CERN control systems.
2.4.2.3 Algorithmic formal verification applied to PLC based programs

Model checking is the most popular algorithmic formal verification technique suggested by the literature for PLC programs. However static analysis solutions for PLC programs have been also proposed by some authors. Static analysis and model checking techniques can complement each other.

For example, the Arcade.PLC tool (ARCADE.PLC website (2014); Biallas et al. (2014); Stattelmann et al. (2014)) from the RWTH Aachen University and the PLC Checker tools (PLC Checker website (2014)) from the Itris Automation Square company provide static analysis solutions for PLC programs.

The following paragraphs present an exhaustive analysis of related publications where model checking was the adopted verification technique for PLC programs. The analysis presents the main differences with the adopted approach of this thesis, regarding the following aspects: the PLC languages, the requirement specification, the modeling and verification constrains, the abstraction and reduction techniques and the modeling strategy of the timing aspects in PLC programs.

Many studies and proposals can be found in the literature of applying model checking to PLCs programs: Bartha et al. (2012); Bauer et al. (2004); Biallas et al. (2010); Blech et al. (2011); Campos et al. (2008); Canet et al. (2000a); Flake et al. (2004); Gourcuff et al. (2008); Huuch (2003); Lange et al. (2013); Mader and Wupper (1999); Mokadem et al. (2010); Pavlović and Ehrlich (2010); Perin and Faure (2013); Sarmento et al. (2008); Smet et al. (2000); Soliman and Frey (2011); Soliman et al. (2012); Sülflew and Drechsler (2008); Yoo et al. (2008).

However, none of the described methods can be applied directly to the control systems developed at CERN, for the reasons discussed hereafter.

Regarding the PLC languages: in the literature, most of the the modeling strategies target a single PLC language.

Formal verification has been mainly applied to IL (e.g. Canet et al. (2000a); Mader and Wupper (1999)) and SFC (e.g. Bauer et al. (2004); Sarmento et al. (2008)).
2.4. Related work

A few works target the verification of FBD programs (e.g. Bartha et al. (2012)) and Ladder (e.g. Bender et al. (2008)). Some work targets specifically the verification of ST programs (e.g. Gourcuff et al. (2006, 2008)). Finally a very few approaches can handle multiple PLC languages (e.g. Biallas et al. (2010); Gourcuff et al. (2008); Sadolewski (2011)).

The approach proposed in this document differs from previous works as the modeling strategy has been designed to provide a general methodology where any PLC language can be included. For that, an automata based formalism has been adopted as an intermediate step between the PLC code and modeling languages of the verification tools. This formalism is appropriate to model all the features of any PLC language.

In addition, the automatic translation from the PLC languages into the modeling language of the verification tools is split into two parts, making the methodology more flexible as adding a new language does not imply a completely new modeling approach.

Regarding the requirement specification: very few authors targeted the problem of requirement specification in the application of formal verification of PLC programs, even if this issue is one of the main obstacles of these approaches to be deployed in industry.

Authors like, Campos et al. (2008) and Campos and Machado (2013) propose an approach to hide the complexity of using complex specification formalism like temporal logic. This approach is based on patterns that can be easily used by the engineers and they are automatically translated to temporal logic formulas.

The solution provided in this thesis is also based on patterns. A set of patterns with a well-defined semantics is provided to engineers. Once the requirement is created with these patterns, the corresponding temporal logic formula is generated automatically. The main difference with the previous approaches is the set of patterns. Previous works did not cover all the specification needs we had for our systems. Our patterns are based on the experience of the control engineers at CERN.

These approaches based on patterns are useful to find bugs in the PLC programs, although it does not guarantee to provide a complete and coherent formal specification.
Other authors propose solutions based on UML techniques (e.g. Flake et al. (2004); Remenska et al. (2014)) to help engineers to build the temporal logic formulas. Although there are not specific for PLC control systems, the ideas can be adapted to this field.

An overview of the different approaches in requirements engineering can be found in Laplante (2013).

Regarding the modeling and verification constraints: In certain cases, the modeling and verification strategies are applicable to a reduced set of PLC programs due to some restrictions.

Some authors apply formal verification, but only for small examples, without discussing the reduction of the models that is unavoidable for verifying industrial-sized programs. For example, Bartha et al. (2012); Canet et al. (2000a); Mokadem et al. (2010); Pavlović and Ehrich (2010); Perin and Faure (2013); Sarmento et al. (2008); Soliman and Frey (2011); Soliman et al. (2012); Sülfow and Drechsler (2008). Only a few authors deal with this important issue (e.g. Biallas et al. (2010); Gourcuff et al. (2008); Lange et al. (2013)).

Some of the studies only target the modeling of PLCs without providing a verification solution. For example, Blech et al. (2011); Mader and Wupper (1999).

Many papers do not address the automatic generation of the model from the PLC program, or just explain the high-level principles. For example, Bartha et al. (2012); Bauer et al. (2004); Biallas et al. (2010); Canet et al. (2000a); Mokadem et al. (2010); Pavlović and Ehrich (2010); Perin and Faure (2013); Sarmento et al. (2008); Smet et al. (2000); Soliman and Frey (2011); Yoo et al. (2008).

In some cases, the modeling strategies restrict the expressiveness of the property specifications. In Sadolewski (2011), the proposed approach restricts the requirements to assertions that provide smaller expressiveness than LTL or CTL (in this work, axiomatic formal verification was applied). In other cases, the abstraction techniques imply constraints in the expressiveness of properties (e.g. Biallas et al. (2010); Lange et al. (2013)).

In addition, most of the approaches are attached to a specific verification tool. In the literature, the most popular verification tools for PLC programs are NuSMV and UPPAAL.

Table 2.2 summarizes some of the constraints of the previous work.
## 2.4. Related work

<table>
<thead>
<tr>
<th>Reference</th>
<th>Input lang.</th>
<th>Verifier</th>
<th>Req. language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bauer et al. (2004)</td>
<td>SFC</td>
<td>Cadence SMV</td>
<td>CTL</td>
</tr>
<tr>
<td>Sarmento et al. (2008)</td>
<td>SFC</td>
<td>UPPAAL</td>
<td>CTL subset</td>
</tr>
<tr>
<td>Bauer et al. (2004)</td>
<td>timed SFC</td>
<td>UPPAAL</td>
<td>CTL subset</td>
</tr>
<tr>
<td>Blech et al. (2011)</td>
<td>SFC, FBD</td>
<td>BIP</td>
<td>—</td>
</tr>
<tr>
<td>Bartha et al. (2012)</td>
<td>FBD</td>
<td>PetriDotNet</td>
<td>CTL</td>
</tr>
<tr>
<td>Canet et al. (2000b)</td>
<td>IL</td>
<td>Cadence SMV</td>
<td>LTL</td>
</tr>
<tr>
<td>Mader and Wupper (1999)</td>
<td>IL</td>
<td>UPPAAL</td>
<td>CTL subset</td>
</tr>
<tr>
<td>Gourcuff et al. (2006)</td>
<td>ST</td>
<td>NuSMV</td>
<td>—</td>
</tr>
</tbody>
</table>

1 Only Boolean variables are permitted.
2 The following limitations apply: only Boolean variables, no iteration statements. The method can be applied for LD and IL too, but it is not presented in Gourcuff et al. (2006).
The main differences of this thesis with previous works, are the following ones:

- We propose a fully automated methodology from the property specification to the counterexample analysis.

- We do not target a single verification tool, which allow us to select the appropriate tool for different verification cases.

- We verify “complex” properties expressed with temporal logic and we provide two kind of reduction technique for our models: property preserving reduction techniques and the variable abstraction technique. The first group does not bring any constraint to the expressiveness of the property specification but the second group is restricted to safety properties. The second group is only applied when the property preserving techniques are not powerful enough for a specific property and PLC program.

Regarding the abstraction and reduction techniques: As it was mentioned before, only a few authors targeted the issue of reduction techniques for PLC program verification.

In Gourcuff et al. (2008), the authors address the problem of state explosion of formal models derived from IL (Instruction List) PLC programs by using an algorithm based on data and interpretation abstraction. Their algorithm has some limitations, e.g. only Boolean variables can be used.

The paper Biallas et al. (2010) applies CEGAR (counterexample-guided abstraction refinement, proposed in Clarke et al. (2000)) to models of PLC programs written in IL, but they do not present large case studies that would show the scalability of the methods. The limitations of the approach are the same as for other CEGAR approaches: it can handle only ACTL properties.

In Biallas et al. (2013), the authors apply predicate abstraction to PLC programs. As well as the previous paper, the author focus on safety properties.

In Lange et al. (2013), bounded model checking is applied to PLC programs. The authors introduce powerful reduction methods applied to IL code. Reduction techniques such as constant folding, slicing, and forward expression propagation are employed to optimize the models.
for bounded model checking. This approach restricts the requirement language to simple safety properties.

Table 2.3 summarizes the related work of abstraction and reduction techniques applied to formal models from PLC programs.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Abstraction techniques</th>
<th>PLC language</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gourcuff et al. (2008)</td>
<td>data and interpretation abstraction</td>
<td>IL</td>
<td>only Boolean var.</td>
</tr>
<tr>
<td>Lange et al. (2013)</td>
<td>constant folding, slicing, and forward expression propagation</td>
<td>IL</td>
<td>only Safety properties</td>
</tr>
<tr>
<td>Biallas et al. (2010)</td>
<td>CEGAR</td>
<td>IL</td>
<td>only Safety properties</td>
</tr>
<tr>
<td>Biallas et al. (2013)</td>
<td>Predicate abstraction</td>
<td>ST</td>
<td>only Safety properties</td>
</tr>
</tbody>
</table>

These papers provide very interesting ideas and contributions to improve the performance of PLC programs verification. Our approach differs with these works in the following aspects:

- Our reductions are independent of the verification tools as they are applied in a higher level of our methodology, the IM.

- In addition, as mentioned before, we provide two kind of reduction techniques for our models: property preserving reduction techniques and the variable abstraction technique. The first group does not bring any constraint to the expressiveness of the property specification but the second group is restricted to safety properties.

Regarding the modeling strategy for the timing aspects of PLC programs: finally, most of the described works do not model
time in PLCs. Only a few works have been found targeting time and timers in PLCs, i.e. Mader and Wupper (1999); Mokadem et al. (2010); Perin and Faure (2013); Wang et al. (2013).

Indeed, Mader and Wupper (1999) or Perin and Faure (2013) propose an approach for modeling PLC timers using timed automaton models, but they do not present verification results. As time is considered as a linear and monotonic function, the generated models would have a huge state space, making verification not feasible if this approach would be applied to large systems, as the systems developed at CERN.

Similarly, Mokadem et al. (2010) presents a case study where a global model for a timed multitask PLC program is created for verification purposes. This approach is similar to the one proposed by Mader and Wupper (1999) but verification is performed with UPPAAL using clocks and therefore with monotonic time representation.

In Wang et al. (2013), several aspects of PLC control systems including timers are modeled, using the component-based BIP framework. In this case, they assume fixed PLC cycle length which is a big constraint, and timer models are not precise enough compare to real PLC timers. In addition, verification results are not presented.

Table 2.4 summarizes the related work of modeling strategies for the timing aspects of PLC programs.

This thesis proposes two different approaches to model time and timers in PLCs:

- The first one includes a realistic approach in which time is modeled as a finite variable as it is implemented in PLCs.

- The alternative is a very abstract model of timer where time is not modeled in order to deal with the state space explosion problem.

All the details are presented in Section 3.9.

2.5 Summary of the chapter

This chapter presented the theoretical background and the related work needed to understand the contributions of this thesis. From the automation community, the main concepts of PLC-based control
systems are described, including classification, standards and basic concepts about the hardware and software of these systems. From the formal methods community, some definitions of formal methods and formal verification are included. The focus of this section is on the model checking technique. Finally, the related work of this thesis is presented, including a discussion of the most relevant contributions on this topic of research. The main differences of previous works with this thesis are also described.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Formalism</th>
<th>Verification tool</th>
<th>Time model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perin and Faure (2013)</td>
<td>Timed automaton</td>
<td>–</td>
<td>monotonic representation</td>
</tr>
<tr>
<td>Mokadem et al. (2010)</td>
<td>Timed automaton</td>
<td>UPPAAL</td>
<td>monotonic representation</td>
</tr>
<tr>
<td>Wang et al. (2013)</td>
<td>BIP language</td>
<td>–</td>
<td>monotonic representation</td>
</tr>
</tbody>
</table>
Chapter 3

Approach

3.1 Introduction

This chapter presents the proposed approach and main contribution of this thesis. It consists in a methodology that allows to apply automated formal verification to PLC programs. The two main goals of this research are:

1. Finding bugs in the PLC code, increasing the quality of the software.

2. Hiding the complexity of applying formal methods, from control engineers and designers.

Nowadays, development of PLC programs in industry is a very traditional procedure in most of the cases as it is represented in Fig. 3.1. An informal specification is the starting point, where the control engineer and the process engineer describe the required logic to control the process in a natural language. Then the PLC programmer (often the same person as the control engineer) implements the PLC code according to the specifications. In the best case, the PLC programmer uses some standards in the development process (e.g. IEC 61499 (2013)) or frameworks (e.g. UNICOS framework from Blanco Viñuela et al. (2011) for CERN control systems). Finally manual testing is performed on the PLC before the commissioning of the system. For safety systems the procedure is more strict, as all the steps defined in the so-called “Safety Life Cycle” have to be performed. The “Safety Life Cycle” is defined in IEC 61508 (2010).
Chapter 3: Approach

The methodology proposed here is meant to be integrated in this traditional development process or in any variant of this schema. It has the goal of not modifying the PLC program development process of any company or developer. Therefore existing PLC programs can also be verified.

This methodology creates automatically formal models out of PLC programs and is meant to be general and able to transform the languages defined in IEC 61131 (2013) standard into different modeling languages used by formal verification tools. This transformation is based on an Intermediate Model (IM), which is the central point of the methodology.

The content of this chapter is divided according to the different steps of the methodology.

- Section 3.2 presents a general overview of the approach.
- Section 3.3 describes the syntax and semantics of the IM.
- Section 3.4 presents the procedure for formalizing the informal
requirements from developers and designers.

- Section 3.5 presents the “execution platform” knowledge included in the formal models, extracted from the PLC hardware.

- Section 3.6 presents the transformation rules from the PLC programs into the IM. Currently the methodology includes ST and SFC languages.

- Section 3.7 presents the reduction techniques on the formal models that make possible formal verification.

- Section 3.8 presents the transformation rules from the IM into the modeling languages used by the formal verification tools. Currently the methodology includes nuXmv, UPPAAL and BIP modeling languages.

Two extra sections have been created to describe in detail two particular subjects in the modeling strategy:

- Section 3.9 presents the transformation rules related to time and timers. Due to the complexity of these transformation rules, they are presented as an independent section.

- Section 3.10 presents the adopted solution for including process information in the formal models.

The chapter concludes with the last step of the methodology and a brief overview of the implementation of the methodology in a CASE (Computer-Aided Software Engineering) tool.

- Section 3.11 presents the final step of the methodology, how the verification procedure is applied and how the information extracted from the verification tools is used to help the PLC programmers to find the source of the problem.

- Section 3.12 describes the basis of the CASE tool, which implements the methodology.
3.2 General overview of the approach

The methodology presented in this chapter allows control engineers and designers to apply formal verification to PLC programs without any expertise in the field of formal methods or formal verification. The methodology is designed to be general so any PLC language can be included in it. Moreover, its design allows to extend the methodology with several formal verification tools. To achieve that, it relies on an intermediate model (IM) which is the central piece of the methodology. This IM is an automata-based formalism extended with data (the formal definition of the IM syntax and semantics are defined in Section 3.3). PLC code is automatically translated to the IM, including the PLC execution platform knowledge. In a second step, the IM is translated to several input models for different verification tools. It also provides a solution for formalization of the requirement specification. The methodology is represented in Fig. 3.2.

Figure 3.2: Methodology overview

The figure is divided in four blocks, suggesting the reader the different steps of the methodology.

- The first block is called “PLC world”. It shows the source of information needed to build the formal models and the formal requirements. In this block, the PLC programs, the informal requirements and the execution platform knowledge are included.
3.2. General overview of the approach

− The second block is called “Internal model”. It is composed of the IM, the formalized requirements to be verified and the reduction techniques to simplify the model.

− The third block is called “External models”. In this block, the IM is translated into the input modeling language of the selected verification tools.

− The fourth and final block is called “Analysis”. It is where the verification is performed and the verification results are analyzed and presented to the PLC developers in order to find the source of the problem if any.

From the user point of view, i.e. the control system developer and designer, they only need to feed the methodology with the requirements to be fulfilled and the PLC programs. As a result, an analysis report is obtained, extracting the information from the verification results given by the verification tools. This report tells the user if the models meet the requirements, and if not, it provides useful information to find the source of the problem. All the intermediate transformations are hidden and fully automatized by the CASE tool.

The internal steps of the methodology are the following:

1. **Formalization of the requirements**: usually the requirement specifications are expressed in a non-formal language by the control system developers and designers. Temporal logic formalisms are the most popular formalism used by verification tools for property specification. However, they are complex and control systems developers and designers are not familiar with them. Section 3.4 describes this first step, hiding the complexity of using temporal logic for the requirement specification.

2. **PLC code – IM transformation**: This step consists in the transformation of the PLC code into the IM. The PLC code is parsed, building an Abstract Syntax Tree (AST), which represents the abstract syntax of the PLC code. This AST is then transformed to a Control Flow Graph (CFG) which represents the semantics of the code as an automata-based IM. The transformation process uses the abstract model of the PLC hardware to be able to represent the PLC scan cycle. The transformation rules from
the PLC code into the IM are presented in Section 3.6. The execution platform information used to build the abstract model of the PLC hardware is presented in Section 3.5.

3. Reduction and abstraction techniques applied to the IM: when modeling real-life PLC programs, the state space of the generated model is huge and in most cases formal verification cannot be applied. Section 3.7 presents the reduction techniques proposed in this methodology to make formal verification possible.

4. Transformation IM– modeling languages of the verification tools: once the IM is reduced, it is translated into the input modeling language of specific verification tools. Section 3.8 shows the IM translation into the selected verification tools. Currently NuSMV/nuXmv (from this point referenced as nuXmv), UPPAAAL and BIP are included.

5. Verification and analysis of the results: when the verification tool finds discrepancies between the formal model and the formal specification, a counterexample is produced. This information is analyzed, reduced and presented in a report to the developers and designers, providing useful information in order to find the source of the problem. Section 3.11 presents this analysis of the information provided by the verification tools.

A CASE tool based on EMF (Eclipse Modeling Framework) that supports this methodology has been developed. It provides a graphical interface for the PLC program developer.

This brief description of the methodology may have risen some obvious questions to the reader. This section is dedicated to answer them in order to introduce and justify our decisions.

Why model checking? Among different formal verification techniques, model checking was the most appropriate for our purposes. The main reasons are: it is possible to automatize and it is possible to hide the complexity from PLC developers as it was mentioned before. About the specific model checking technique, the methodology is meant to be general and open to any tool with different model checking techniques. For example, symbolic model checking is applied as
nuXmv is integrated and by using BIP framework, compositional verification \cite{bensalem2011} and statistical model checking \cite{basu2012} can be applied.

**Why the models are created out of the PLC code?** When the methodology design started, two possibilities were considered: (1) The first one was to build the models from a high-level specification, then verify these models and finally generate the PLC code (See Fig. 3.3(a)). This is the so-called “correctness by construction” approach, and many authors and even companies promote this approach (e.g. the SCADE tool-set from Esterel technologies\footnote{http://www.esterel-technologies.com/products/scade-suite/} or the BIP framework from the Verimag laboratory\footnote{http://www-verimag.imag.fr/Rigorous-Design-of-Component-Based.html}). This approach has multiple and obvious benefits in the design of safety critical systems. For example, at the specification level, many constrains can be introduced and the variability is reduced, therefore the space state of the models is smaller. It is actually the ideal approach for any software design. But it also implies to impose the developers and designers to use a specific formalism for specification, however, there is not a standard nor a single solution adopted so far by the automation community. This approach would imply to change the development process of PLC programs and verification of existing PLC control systems would not be possible. (2) The second possibility considered, which was the selected approach, was to build the models out of the PLC code (See Fig. 3.3(b)). This approach has two main drawbacks: the complexity of the transformation rules from the PLC code into the formal models and the state space size of the generated models, as the PLC developer can write PLC programs without any constraint (just the ones imposed by the PLC language). However, we have strong arguments for using the second approach. As it was mention before, nowadays there is no unified formalism to specify industrial control systems, including of course PLC control systems. Requirements for software engineering is a topic addressed by some authors (e.g. Laplante \cite{laplante2013}), even some general standards give some guidelines about software specification (e.g. \textbf{IEEE 830} \cite{IEEE830}) but in industry, almost every company that develops control systems has a different way to specify. However, the PLC languages are unified by the \textbf{IEC 61131} \cite{IEC61131} standard, there are only small differences in
the languages implemented by the different PLC vendors, and every PLC developer uses them. In addition, a requirement for this project was to provide a solution for verifying and finding bugs in existing systems. These systems have been developed using completely different specification techniques. The methodology is meant to be general and it can be used by any PLC developer. Similar approaches were adopted also for many different authors (See Section 2.4).

In addition, as it was mentioned before, this approach is meant to be integrated in the existing, traditional process of PLC programs development. Fig. 3.4 shows the proposed methodology integrated in the PLC program development process. In the left part of the figure, the “traditional” PLC program development is shown. The PLC code is produced from an informal specification. In the best cases, the developer uses some standards (e.g. IEC 61499 [2013]) or frameworks (e.g. UNICOS framework Blanco Vinuela et al. [2011] for CERN control
3.2. General overview of the approach

systems) and testing is performed before or during the commissioning phase of the project. The new methodology creates formal models out of the PLC code and the formal specification is created by using patterns. A model checker is used to check the requirements on the model and when a bug is found, the counterexample can be used to generate a “Verification report” with the useful information to help the developers to find the source of the problem. Moreover, a “PLC demonstrator” can be a automatically generated and integrated in the PLC program for proving that the bug found by the model checker exists in the real system.

![Diagram](image-url)

Figure 3.4: Integration of the proposed methodology in the PLC program development process.
**Why introducing an intermediate model?** There are multiple reasons to include an intermediate step in our approach, including:

- It implies the transformation from PLC code into the input languages of the verification tools. The transformation rules are split into two parts: “AST to CFG” (Abstract Syntax Tree to Control Flow Graph) transformation from the PLC code into the IM and “CFG to CFG” (Control Flow Graph to Control Flow Graph) transformation from the IM into the different model checker inputs. The “CFG to CFG” transformations are much simpler than the first ones, it consists in transforming the IM in another formalism with a different syntax. By decoupling the transformations in two different steps it allows to clearly separate the two roles of the transformation by making them independent one from another (separation of concerns design approach).

- This approach allows us to easily add new model checkers, if their input languages are close to an automata-based formalism.

- Abstraction techniques can be applied to the IM, therefore the performance of the verification can be increased for all the model checkers included in the tool chain.

**Why automata-based intermediate model?** Automata-based formalism is a simple formalism but strong enough to model all the features of a PLC control system. In addition, many verification tools use modeling languages close to this idea, e.g. nuXmv (Cavada et al. (2014)), UPPAAL (Ammell et al. (2001)) and the BIP framework (Basu et al. (2011)). Therefore the transformation rules between the IM and the input of nuXmv, UPPAAL, DFinder (from the BIP framework) or any other similar model checkers are simple to implement and the methodology, as well as the tool, can be easily extended.

**Why not timed automata as intermediate model?** When modeling PLC programs, one of the main problems we had to face is how to model the timing aspects of these systems, i.e. modeling time and timers. As a first thought, we considered to use timed automata for this purpose, using for example the UPPAAL formalism. However PLC timers use a specific data type defined by the IEC 61131 (2013)
standard called \textit{TIME}. This data type is a finite variable and its representation is a non-monotonic time representation as the variable can overflow. Each PLC brand has its own definition of the \textit{TIME} data type. For example, Simenex S7 PLCs represent \textit{TIME} as a signed 32-bit integer with a precision of 1 ms. Modeling time with clocks, for example using the UPPAAL formalism, will imply a monotonic representation of the \textit{TIME} data type, which it was not desirable for our approach. For that reason, we decided to use an automata-based formalism which is closer to more verification tools formalism and the \textit{TIME} data is modeled as a finite variable. All the details about modeling timing aspects of PLCs are described in Section 3.9.

\textbf{Why more than one verification tool is needed?} The existing verification tools provide different advantages and disadvantages in terms of performance, simulation facilities and properties specification. The formal verification community is advancing fast and new algorithms are providing better verification performance. Our goal is not to develop a new verification tool, therefore we wanted to compare them according to this three features and provide the PLC developers the best alternative for our models. For instance, up to now, nuXmv provides better results in terms of verification performance for our current models. nuXmv also supports the full LTL and CTL for the specification properties but it lacks good simulation facilities; UPPAAL provides very good simulation facilities but it only supports a subset of CTL; BIP provides a language for modeling component-based systems, code generation and simulation facilities. From BIP, model-based automated testing can be applied, some results applied to PLC control systems can be found in Fernández Adiego et al. (2013b) and its verification tool for compositional verification (called DFinder) only supports deadlock and safety properties. The formal verification community is continuously proposing new and improved verification algorithms and tools, which can be easily included in the proposed methodology. This strategy makes the methodology independent of a single verification tool.

\textbf{How to avoid state space explosion in large PLC program models?} Automata-based models of PLC programs, as any software model for verification purposes, usually face the problem of huge state
Chapter 3. Approach

space. Therefore abstraction and reduction techniques are needed to be able to apply formal verification to PLC programs. In this methodology these techniques are applied to the IM and all the specific model formats can benefit from these techniques. Section 3.7 presents the proposed reduction and abstraction techniques.

3.3 Intermediate model

This section presents the definition of syntax and semantics of the IM.

3.3.1 Intermediate model syntax

The IM is based on an automata network model, consisting of synchronized automata.

Definition 3 (Network of automata) A network of automata is a tuple \( N = (A, I) \), where \( A \) is a finite set of automata, \( I \) is a finite set of synchronizations.

Definition 4 (Interactive automaton) An automaton is a structure \( a = (L, T, l_0, V_a, Val_0) \in A \), where \( L = \{l_0, l_1, \ldots\} \) is a finite set of locations, \( T \) is a finite set of guarded transitions, \( l_0 \in L \) is the initial location of the automaton, \( V_a = \{v_1, \ldots, v_m\} \) is a finite set of variables, and \( Val_0 = (Val_{l_0, 0}, \ldots, Val_{l_m, 0}) \) is the initial value of the variables.

Let \( \hat{V} \) be the set of all variables in the network of automata \( N \), i.e. \( \hat{V} = \bigcup_{a \in A} V_a. (\forall a, b \in A : V_a \cap V_b = \emptyset) \)

Definition 5 (State) A state of an interactive automaton is a pair \( LV_a = (l, Val) \), where \( l \in L \) is the current location and \( Val \) is the vector of current values of each variable \( v \in V \) (in a fixed order).

Definition 6 (Interactive transition) A transition is a tuple \( t = (l, g, amt, i, l') \), where \( l \in L \) is the source location, \( g \) is a logical expression on variables of \( \hat{V} \) that is the guard, \( amt \) is the memory change (variable assignment), \( i \in I \cup \{NONE\} \) is a synchronization attached to the transition, and \( l' \in L \) is the target location.

Definition 7 (Synchronization) A synchronization is a pair \( i = (t, t') \), where \( t \in T \) and \( t' \in T' \) are two synchronized transitions in different automata. The variable assignments attached to the transitions \( t \) and \( t' \) should not use the same variables.
3.3. Intermediate model

Fig. 3.5 shows an example of the IM built from PLC code. In this example, the reader can observe all the elements, which have just been defined in this section. Please note that initial and final locations (i.e. $l_0$ and $l_n$) are represented as init and end respectively on the figures to make them more clear. The green box represents a part the user PLC program logic. The red box represents a function call to the function $FC1$ (represented by the automaton $FC1$). All the details about the transformation from the PLC program into the IM will be explained in the following Sections.

$$xa := \overline{(ia > 0)}$$
$$xb := \overline{(ib > 0)}$$
$$c := c + 1$$
$$ya := \overline{FC1}$$

Figure 3.5: Example of IM

3.3.2 Intermediate model semantics

The behavior of this automata-based formalism can be easily explained informally as follows: when an automaton is in location $l$ and a transition $t$ goes from $l$ to $l'$, it is enabled if its guard $g$ is satisfied and it has no synchronizations ($i = NONE$). If this transition $t$ occurs (fires), the location of the automaton will be $l'$ and the variable assignments defined for $t$ will be executed. The transitions joined by a synchronization can only fire together and only if both are enabled (synchronous composition).

In the next paragraphs, the previous informally introduced semantics is presented in a formal way. For that purpose, the product-
automaton of our IM (with regards to the synchronizations) is represented as a state transition system (STS).

**Definition 8 (State transition system)** A (finite) state transition system is a \((S_{STS}, s_0, \mathcal{N})\) tuple, where \(S_{STS}\) is a finite set of states, \(s_0 \subseteq S_{STS}\) is a set of initial states, \(\mathcal{N} \subseteq S_{STS} \times S_{STS}\) is a relation over \(S_{STS}\) which describes the possible state changes i.e. transitions. In the following, a transition from state \(s\) to \(s'\) will be marked as \(s \rightarrow s'\) to improve readability.

**Definition 9 (Semantics of interactive automata network)** Let \(N = (A, I)\) be an interactive automata network (where \(A = \{a_1, \ldots, a_n\}\)). The semantics of this automata network can be defined as a state transition system \((S_{STS}, s_0, \mathcal{N})\), where \(S_{STS}\) is the set of states \(LV_{a_1} \times \cdots \times LV_{a_n}\), and \(s_0 = (l_{0,1}, Val_{0,1}, \ldots, l_{0,n}, Val_{0,n})\) is the initial state. The set of transitions \(\mathcal{N} \subseteq S_{STS} \times S_{STS}\) is constructed in the following way:

- For every transition \(t = (l, g, amt, int, l') \in T\) in an automaton \(a_i\), where \(int = \text{NONE}\) (defined as \(i\) in the IM syntax), for every \((Val, Val^*) \in \text{amt}\): if \(g(Val) = \text{true}\), then add:

  \[
  (lv_1, \ldots, lv_{i-1}, (l, Val), lv_{i+1}, \ldots, lv_n) \rightarrow \\
  (lv_1, \ldots, lv_{i-1}, (l', Val^*), lv_{i+1}, \ldots, lv_n)
  \]

  \((\forall lv_j \in LV_{A_j}, \text{ where } j \neq i)\).

- For every transition \(t = (l, g, amt, int, k) \in T\) in automaton \(a_i\), where \(int = (t, t')\) (defined as \(i\) in the IM syntax) and \(t' = (l', g', amat', int, k')\) in automaton \(a_j\), for every \((Val, Val^*) \in \text{amt}\), for every \((Val', Val'^*) \in \text{amt}'\), for every \((Val^*, Val^{**}) \in \text{iamt}\), and for every \((Val'^*, Val^{**'}) \in \text{iamt}\): if \(g(Val) = \text{true}\) and \(g'(Val') = \text{true}\), then add:

  \[
  (lv_1, \ldots, lv_{i-1}, (l, Val), \ldots, (l', Val'), lv_{j+1}, \ldots) \rightarrow \\
  (lv_1, \ldots, lv_{i-1}, (k, Val^{**}), \ldots, (k', Val^{**'}), lv_{j+1}, \ldots)
  \]

  \((\forall lv_x \in LV_{A_x}, \text{ where } x \neq i \text{ and } x \neq j)\).
3.4. Formal specifications

An example of this approach to describe the automata semantics as STS is shown in Fig. 3.6. In this example an automata network, which contains two automata is represented by a STS. The automaton A contains one variable $a$, three states, three transitions and one interaction $i$ with the automaton B. The automaton B contains one variable $b$, one state, one transition and one interaction $i$ with the automaton A. The corresponding STS contains six states in which the location of each automaton and the values of the variables $a$ and $b$ are located. For example the first state of the STS is $(\text{init}, \text{false}, p_0, \text{false})$.

Figure 3.6: Example of representing an interactive automata network as a STS

3.4 Formal specifications

The first step of the methodology is to formalize the control system specifications. Specification is usually carried out by two actors in collaboration: the process engineer, who has the knowledge about the industrial process to be controlled, and the control engineer, who can design the control strategy to fulfill the requirements established by the process engineer. Traditionally in any field of engineering, specification is a major problem. Requirements specification are usually incomplete, ambiguous and even contradictory. Finding a solution to this problem is very challenging, as an expressive formal specification
Chapter 3. Approach

A language is needed and it has to be easy to understand and natural for process and control engineers.

In industrial control systems development, this problem remains unsolved. In addition, control and process engineers are not familiar with complex formal specification languages used by the verification tools, e.g. LTL or CTL. Previous works have presented some solutions for the formalization of requirements in automation, e.g. [Campos et al. (2008)]. However, nowadays there is not a unified standard for control system specification.

In this methodology, we provide a similar approach than the one provided in [Campos et al. (2008)] for the formalization of the requirements specification, which is based on patterns. Patterns are simple templates with well-defined semantics, where the control and process engineer can easily write the specifications using a simple and natural language. Then these pseudo-formalized requirements can be automatically translated to the specification formalism used by the verification tools (typically temporal logic). Obviously, this solution does not solve the specification challenge for industrial control systems, but it provides a simple solution to formalize the requirements so the methodology can be applied. Comparing the patterns included in this methodology with those presented in [Campos et al. (2008)], more complex patterns were needed. Discussions with our PLC program developers at CERN allowed us to provide the list of patterns that cover all the current needs for verification of their PLC programs. Completeness is guaranteed this way.

According to our experience, control and process engineers usually provide ambiguous requirements, even for simple examples. For example:

“If \( A \) is true, then \( B \) has to be true.”

This requirement is obviously ambiguous. It is needed to specify in which moment of the PLC execution this property has to hold. In most of the cases, PLC developers want to verify that a property holds at the end of the PLC cycle. This is the critical moment as the output variables are assigned to the real peripheries at this point. Assuming this, the unambiguous requirement is:

“If \( A \) is true at the end of the PLC cycle, then \( B \) is always true at the end of the same PLC cycle.”
This requirement is formal enough to be expressed as a CTL formula. One possible formalization is the following:

\[ AG( (EoC \land A) \to B ) \]

In these formalizations, \( EoC \) means “end of PLC cycle” and is true only at the end of PLC cycles. Another typical example of an ambiguous requirement:

“If there is a rising edge on \( A \) and \( B \) is true, then \( C \) is true.”

This pattern is ambiguous, as there are multiple possible interpretations of “there is a rising edge”. This has to be reformalized in order to have an unambiguous meaning:

“If in Cycle \( N \): \( A \) is false and \( B \) is true, and in Cycle \( N + 1 \): \( A \) is true and \( B \) is true, then \( C \) is always true (in Cycle \( N + 1 \)).”

As in previous example, this requirement is formal enough to be expressed as an LTL formula. One possible formalization is the following:

\[ G( (EoC \land \neg A \land B \land X(\neg EoC \lor (EoC \land A \land B))) \to X(\neg EoC \lor (EoC \land C)) ) \]

In the formal models produced by this methodology, \( EoC \) is a symbol that represents the end of the PLC cycle. The details about this mechanism will be described in Section \[3.5\].

3.4.1 Patterns

The list of patterns that have been currently implemented in the methodology, can be classified in four families: Patterns for safety properties involving one PLC cycle, Patterns for safety properties involving several PLC cycles, Patterns for liveness properties and Patterns for time-related properties. Here both LTL and CTL are used for formalization.
3.4.1.1 Patterns for safety properties involving one PLC cycle

**Pattern TL1 (General truth under condition)** If \[\text{[2]}\] is true (at the end of the PLC cycle), \[\text{[1]}\] is always true (at the end of the PLC cycle).

or

\[\text{[1]}\] is always true (at the end of the PLC cycle), if \[\text{[2]}\] is true (at the end of the PLC cycle).

The corresponding temporal logic formula is:

\[\text{AG}\left(\left(\text{EoC} \land [2]\right) \rightarrow [1]\right)\]

**Pattern TL2 (Impossibility under condition)** If \[\text{[2]}\] is true (at the end of the PLC cycle), \[\text{[1]}\] is impossible (at the end of the PLC cycle).

or

\[\text{[1]}\] is impossible (at the end of the PLC cycle), if \[\text{[2]}\] is true (at the end of the PLC cycle).

The corresponding temporal logic formula is:

\[\text{AG}\left(\left(\text{EoC} \land [2]\right) \rightarrow \neg [1]\right)\]

**Pattern TL3 (General truth)** \[\text{[1]}\] is always true (at the end of every PLC cycle).

The corresponding temporal logic formula is:

\[\text{AG}\left(\text{EoC} \rightarrow [1]\right)\]

**Pattern TL4 (State change during a cycle)** If \[\text{[2]}\] is true (at the beginning of the PLC cycle), \[\text{[1]}\] is always true (at the end of the same PLC cycle).

The corresponding temporal logic formula is:

\[\text{AG}\left(\left(\text{SoC} \land [2]\right) \rightarrow \text{A}\left(\neg \text{EoC} \cup [1]\right)\right)\]

where \text{SoC} means “Start of PLC cycle” and is true only at the begging of PLC cycles.
3.4. Formal specifications

3.4.1.2 Patterns for safety properties involving several PLC cycles

**Pattern TL5 (General truth on rising edge)** If _______ [1] has a rising edge (at the end of the PLC cycle), _______ [2] is always true (at the end of the PLC cycle).

A rising edge on [1] means that [1] is false at the end of cycle N and true at the end of cycle N+1. The corresponding temporal logic formula is:

\[
G\left((\neg EoC \land \neg [1] \land X (\neg EoC U (EoC \land [1])))\right) \\
\rightarrow X(\neg EoC U (EoC \land [2]))
\]

**Pattern TL6 (General truth on rising edge under condition)** If _______ [1] has a rising edge and _______ [3] is true (at the end of the PLC cycle), then _______ [2] is always true (at the end of the PLC cycle).

The corresponding temporal logic formula is:

\[
G\left((EoC \land \neg [1] \land X (\neg EoC U (EoC \land [1] \land [3])))\right) \\
\rightarrow X(\neg EoC U (EoC \land [2]))
\]

**Pattern TL7 (State change between cycles)** If _______ [1] is true at the end of cycle N and _______ [2] is true at the end of cycle N+1, then _______ [3] is always true at the end of cycle N+1.

The corresponding temporal logic formula is:

\[
G\left((EoC \land [1] \land X (\neg EoC U (EoC \land [2])))\right) \\
\rightarrow X(\neg EoC U (EoC \land [3]))
\]

**Pattern TL8 (State change between cycles (emulating sequence))** If _______ [1] is true at the end of cycle N, then _______ [2] is true at the end of cycle N, and also if _______ [3] is true at the end of cycle N+1, then _______ [4] is always true at the end of cycle N+1.

The corresponding temporal logic formula is:

\[
G\left((EoC \land [1] \land X (\neg EoC U (EoC \land [3])))\right) \\
\rightarrow [2] \land X(\neg EoC U (EoC \land [4]))
\]
3.4.1.3 Patterns for liveness properties

**Pattern TL9 (Liveness)** If _______ [1] is true (at the end of the PLC cycle), then _______ [2] will definitely be true sometime (at the end of a PLC cycle).

The corresponding temporal logic formula is:

\[ \text{AG} \left( \text{EoC} \land [1] \rightarrow \text{AF} \left( \text{EoC} \land [2] \right) \right) \]

3.4.1.4 Patterns for time-related properties

When verifying time-related properties with explicit time in it, a “monitor” or observer automata is added to the model, as CTL and LTL do not provide the required expressiveness. In this case, a monitor consists in an automaton added to the global model of the PLC program with the same behavior as a TON timer but independent of the rest of the program logic. With this monitor the formal property is simplified to a safety as it is shown in the Pattern TL10. The output of this monitor is compared to the variable or group of variables which is part of the property to be verified (referenced as [3] in the pattern) and affected by the timer and by the program logic. All the details about time and timers modeling and verification of time-related properties can be found in Section 3.9.

**Pattern TL10 (TON-like property)** If there is a rising edge on _______ [1] and it remains true then after ___ [2] seconds, _______ [3] will be true (at the end of the PLC cycle).

TON monitor on [1] with PT=[2] and the corresponding temporal logic formula is:

\[ \text{AG} \left( \text{EoC} \land \text{MonitorQ} \rightarrow [3] \right) \]

**Pattern TL11 ((11) TP-like property)** If there is a rising edge on _______ [1], then for the next ___ [2] seconds, _______ [3] will be true (at the end of the PLC cycles).

TP monitor on [1] with PT=[2] and the corresponding temporal logic formula is:

\[ \text{AG} \left( \text{EoC} \land \text{MonitorQ} \rightarrow [3] \right) \]
3.5 PLC hardware modeling

In order to apply formal verification to PLC software, the PLC execution platform has to be modeled. In Fig. 3.2, the first block of the methodology called “PLC world” contains the “PLC knowledge” needed to build the IM. A simple modeling approach is proposed in this methodology for the PLC hardware.

**Assumption 1.** Currently, only centralized PLC control systems consisting in one single PLC are considered. Modeling distributed systems will require to find an appropriate level of abstraction to minimize the state explosion problem.

A simple model is proposed, consisting in modeling the scan cycle: input reading, execution of the logic, and writing the variables in the outputs. This knowledge provides the skeleton of the complete model.

**Assumption 2.** Other hardware devices, such as input and output cards, communication interfaces, field buses or any kind of communication with the SCADA, are not modeled. This implies that failures coming from the PLC hardware will not be detected by using this approach (however it is not the goal of the methodology).

The PLC hardware information, which gives the skeleton of the models, is shown in the example of Fig. 3.7. This example shows the four main characteristics introduced in the models from the PLC hardware:

- The cyclic execution of the IM, representing the *PLC scan cycle*.

- The initialization of the variables of the IM in the first location of the model (*init*). In this location, the example shows a special case of input variables: the *parameters*. Parameters are input variables that are constant during the execution, as they are hard-coded into the PLC application.

- In the first transition of the model, from *init* to *l₁*, random values are assigned to all the *input variables* of the system, representing the first step of the scan cycle: reading the input values from the periphery and writing this values in the Input Image Memory.

- The rest of the model represents the execution of PLC code and the final location of the model *end* (i.e. *EoC*). This final location represents the moment when the values are written from the
Output Image Memory to the output periphery. This location will be used in the properties to be verified as it was described in Section 3.4.

It is obvious that identifying automatically the input variables from the system is critical for the methodology. Even if it may look a simple task it is quite complex. When a real-life PLC program is modeled, different kind of input can be found. The next paragraph describes the different kind of inputs, how to identify them and how they are modeled in this methodology.

3.5.1 PLC inputs

In a centralized or decentralized control system (i.e. one single PLC), four kind of inputs can be found:

1. The input variables connected to the process through a local input card: these variables are mapped in the IIM and can be easily identified. For example in Siemens PLCs, the I0.0 is a variable from the IIM connected to a digital sensor. Its value can be modified at the beginning of every PLC cycle.
2. The input variables connected to the process through a decentralized periphery: when using field buses like Profibus or Profinet the values of these inputs can be mapped in the IIM, but sometimes they are mapped in different variables: for example in Siemens PLCs they can be mapped in a DataBlock (DB) variable or in a Memory (M) variable. In this case, its value can also be modified at the beginning of every PLC cycle.

3. The input variables coming from the SCADA: these variables are the orders coming from the operator of the system. These orders are not mapped in the IIM, for example in Siemens PLCs they can be mapped in a DataBlock (DB) variable. Their value can be modified at any moment in every PLC cycle, but it depends on the implementation of the communication protocol between the PLC and the SCADA.

4. Parameters: they can be considered as a special case of input variables. A parameter has a constant initial value and this value does not change in the whole execution of the PLC program.

The main problem now is how to identify these four input variables and how to model them. In general, any input variable coming from the SCADA or from the process can be identified as no value is assigned to these variables in the PLC program. Parameters are assigned once with a constant value and never modified again. However, based on our experience, it may happen that in real-life PLC programs other variables, not only input variables are never assigned. So if this happens, the generated models will be obviously wrong. For that reason, before identifying the input variables of the system, we recommend to perform a static analysis and ensure that this situation will not happen.

As it was mentioned before, any input variable coming from the process is modeled assigning them a random value in the first transition of the IM. In the case of input variables coming from the SCADA, these values can be modified in the PLC program at any time of the PLC program execution, as it depends on the communication protocol between the SCADA and PLC. As we do not consider concurrency problems, any input variable coming from the SCADA is modeled assigning them a random value in the first transition of the IM as well.
Parameters are initialized in the initial location of the model and its value remains constant along the execution of the model.

### 3.5.2 Safety and standard PLCs

For the methodology, the difference in terms of modeling strategy between safety and standard PLCs has been analyzed. If time-related properties are not required, there is no difference from the modeling point of view. But if required, a small difference in the model is produced. Modeling the timing aspects of PLCs is described in the Section 3.9. In a safety PLC, the PLC cycle time is fixed and constant due to the safety constrains, however in a standard PLC it is variable. As it is described in Section 3.9, when a time related property is required, a 16-bits variable modeling time is created. This variable will be incremented with the PLC cycle time at the end of the PLC cycle. Therefore, models from Safety PLCs will increment this variable with a constant value of time and standard PLCs will increment the time variable with a random value between some bounds.

### 3.5.3 Interrupts and restarts in PLCs

As it was described in Section 2.2, PLC programs are composed of the main program and it may contain interrupts and restarts (which are a particular case of interrupts), for example, OB35 in Siemens PLCs. These interrupts can occur at any time. The main program is interrupted and the routine associated to the interrupt is executed. When the execution of this routine finishes, the main program continues the execution from the same point where it was interrupted. This behavior of the PLC scheduler is not modeled in the methodology, therefore currently concurrency problems cannot be detected. For that reason, concurrency problems should be checked before, by applying static analysis techniques and checking that the main program, the interrupts and restarts routines do not modify the same variables of the PLC programs.

Once the program does not contain these kind of problems, model checking can be applied. The PLC program, the interrupts and restarts routines are then modeled. The following modeling strategy is applied:
3.6. PLC code – IM transformation

1. For each interrupt or restart routine, an automaton will be created.

2. The model of the PLC scheduler consists in the main program being executed at every cycle. At the end of the main program automaton, two extra transitions and one location are created per interrupt or restart routine. These transitions contain a synchronization $i$, to synchronize the main program automaton with the interrupt or restart automaton.

3. These interactive transitions are non-deterministically executed, simulating a random execution of the PLC interrupt.

Fig. 3.8 shows a model example of a Siemens PLC program. The original PLC program is composed of the main program (OB1) and a cyclic interrupt (OB35). The corresponding model contains two automata, modeling the behavior of both routines. In addition, two interactive transitions are added in order to synchronize OB1 with OB35. But these transitions will be executed depending on a random value assigned to the variable $ic$.

3.6 PLC code – IM transformation

Once the specification is formalized and the skeleton of the models is defined, the PLC code is automatically translated to the IM. This section describes the most relevant transformation rules from PLC code to the IM. As it was mentioned in Section 2.2, five languages are defined by the IEC 61131-3 standard. Here the transformation from ST and SFC languages are presented, as they are the two most relevant and used PLC languages at CERN. These transformation rules can be extended for the rest of PLC languages defined by the standard. It has to be noticed that although not all of the PLC vendors follow the IEC 61131-3 standard 100%, sometimes there are only a few syntactic differences, it does not imply any difference for the modeling strategy. Along this Section, when examples of PLC code are shown to illustrate the transformation rules, they correspond to Siemens PLC code as it is the main brand used at CERN. The section is divided in the following subsections:
Chapter 3. Approach

Figure 3.8: Example of IM with one PLC interrupt

- General transformation rules from PLC code into IM (Section 3.6.1).
- Transformation rules from ST code into IM (Section 3.6.2).
- Transformation rules from SFC code into IM (Section 3.6.3).

Before the rules, the data type mapping between the PLC code and the different modeling languages has to be introduced. Table 3.1 presents the mapping between the most common data types used in PLC, the data types used in IM and the data types used in the verification tools (nuXmv, UPPAAL and BIP).

3.6.1 General PLC – IM transformation

The transformation rules are presented hierarchically from high level to low level rules. Actually the first rule, which is included here, is the link with PLC hardware modeling strategy.
### Table 3.1: Data type mapping

<table>
<thead>
<tr>
<th>PLC</th>
<th>IM</th>
<th>nuXmv</th>
<th>BIP2</th>
<th>UPPAAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>bool</td>
<td>Boolean</td>
<td>Boolean</td>
<td>char</td>
<td>bool</td>
</tr>
<tr>
<td>int</td>
<td>signed Integer (16 bit)</td>
<td>signed word[16]</td>
<td>int</td>
<td>int</td>
</tr>
<tr>
<td>uint</td>
<td>unsigned Integer (16 bit)</td>
<td>unsigned word[16]</td>
<td>int</td>
<td>int[0,65535]</td>
</tr>
<tr>
<td>dint</td>
<td>signed Integer (32 bit)</td>
<td>signed word[32]</td>
<td>int</td>
<td>int(^1)</td>
</tr>
<tr>
<td>udint</td>
<td>unsigned Integer (32 bit)</td>
<td>unsigned word[32]</td>
<td>int</td>
<td>int</td>
</tr>
<tr>
<td>real</td>
<td>signed Real (32 bit)</td>
<td>signed word[32]</td>
<td>int</td>
<td>int</td>
</tr>
<tr>
<td>char</td>
<td>unsigned Char (8 bit)</td>
<td>unsigned word[8]</td>
<td>char</td>
<td>int[0,255]</td>
</tr>
<tr>
<td>time</td>
<td>signed Time (32 bit)</td>
<td>signed word[32]</td>
<td>int</td>
<td>int</td>
</tr>
<tr>
<td>date</td>
<td>signed Date (16 bit)</td>
<td>signed word[16]</td>
<td>int</td>
<td>int</td>
</tr>
<tr>
<td>byte</td>
<td>8 x Boolean</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>word</td>
<td>16 x Boolean</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dword</td>
<td>32 x Boolean</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) The int in UPPAAL is 16 bit long, thus some information is missing for this particular mapping. (The default range of int in UPPAAL is int[-32768, 32767]).
Chapter 3. Approach

Rule PLC1 (Multiple concurrent code blocks) As it was mentioned in Section 3.5, PLC programs are composed of the main program (i.e. OB1 in Siemens PLCs), which is executed cyclically, and the interrupt handlers.

Assumption 3. Interrupting blocks and the interrupted blocks should use disjoint set of variables. This is a reasonable assumption, since it can be validated by existing static analysis techniques.

According to our experience, different OBs usually use different variables. Furthermore, high level of concurrency is rare in PLC programs.

Having this assumption, instead of modeling the interrupts in a preemptive manner, we model them with non-preemptive semantics: the model of the PLC scheduler consists in the main program being executed at every cycle, whereas one or several interrupts can be executed non-deterministically at the end of the PLC cycle. An example of this rule was presented in Fig. 3.8.

Rule PLC2 (FC) This rule translates functions into IM. An OB can be considered as a special FC that is invoked by the operating system, thus this rule also applies to OBs.

Assumption 4. Recursion is not allowed, i.e. no FC or FB can directly or indirectly generate a call to itself. This assumption is consistent with the IEC 61131 (2013) standard. However, Siemens PLCs allows the use of recursion with some restrictions even if it is not recommended. Recursion can be statically detected by building the call graph of a program and checking whether it contains cycles. Thus we can assume that variables of a function are stored at most once on each L Stack stack.

For each function \( Func \), we create an automaton \( A_{Func} \). The locations, transitions and initial location of this automaton are generated using the rules presented below. For each variable defined in \( Func \) we create a corresponding variable in \( A_{Func} \). If the return type of the function is different from void, a special output variable called \( RET\_VAL \) is also added to the automaton. \( A_{Func} \) contains at least the initial location \( init \), the final location \( end \) and the transition \( t_{end} \) from \( end \) to \( init \).

Fig. 3.9 shows an example of the transformation of a FC into the IM. This rule is general for any PLC language.
Rule PLC3 (FB instance) This rule translates FB instances into IM. Assumption 4 also applies here.

For each instance inst of each function block FBlock, we create an automaton $A_{FBlock, inst}$. The locations, transitions and initial location of this automaton are generated using the rules presented below. For each variable in FBlock we create a corresponding variable in all the corresponding $A_{FBlock, inst}$ automata. Each automaton contains at least the initial location init, the final location end and the transition $t_{end}$ from end to init.

Fig. 3.10 shows an example of the transformation of a FB instance into the IM. This rule is general for any PLC language.
Rule PLC4 (Variables) This rule maps program variables to variables in the IM model.

Assumption 5. All variables, except system inputs, that do not have uniquely defined initial values on the PLC platform (e.g. temporary variables, output variables of FCs) are written before they are read. This means that we do not have to model such variables as non-deterministic variables in the IM model, which allows us to limit the state space growth of the generated model.

For each variable \( v \) in the program block, there is exactly one corresponding variable \( F_V(v) \) in the corresponding automaton. If the variable represents a system input (i.e. variables representing signals coming from the field), it is assigned non-deterministically at the beginning of each PLC cycle. How to identify input variables is explained in the Section 3.5.

Rule PLC5 (FC or FB call) This rule translates FC or FB calls into the IM.

Assumption 6. All the input variables are assigned in the caller, and all the output variables are assigned in the callee in order to avoid the accessing of uninitialized variables that could contain unpredictable values. This means that we do not have to model them as non-deterministic variables and the state space will not be incremented drastically.

For every function (block) call \( ([r :=] Func(p_1 := Expr_1, p_2 := Expr_2, \ldots )) \) in a code block represented by automaton \( A_{\text{caller}} \), we add the following elements. (\( Func \) can be a function or an instance of a function block, represented by automaton \( A_{\text{callee}} \). If \( Func \) is a function block or a void function, the “\( r := \)” part is omitted.)

- A new location \( l_{\text{wait}} \) is added to \( A_{\text{caller}} \). It represents the state when the caller block is waiting for the end of the function call. (For every function call, we add a separate \( l_{\text{wait}} \) location.)

- A transition \( t_1 \) is added to \( A_{\text{caller}} \), which has no guard and goes from the corresponding location marked as \( F_S(stmt) \) to \( l_{\text{wait}} \). It assigns the function call parameters to the corresponding variables in \( A_{\text{callee}} \). (It assigns \( Expr_1 \) to \( F_V(p_1) \), etc.)

- A transition \( t_2 \) is added to \( A_{\text{caller}} \), which has no guard and goes from \( l_{\text{wait}} \) to the location end of the corresponding automaton


3.6. PLC code – IM transformation

$F_S(n(stmt))$. It assigns $RET\_VAL$ of the callee to the corresponding variable (variable $F_V(r)$) in $A_{\text{caller}}$, if $RET\_VAL$ exists. It also assigns the corresponding values to the output variables.

- A synchronization $i_1$ is added to the automata network, connecting transition $t_1$ with the first transition of $A_{\text{callee}}$.

- A synchronization $i_2$ is added to the automata network, connecting the $end \rightarrow init$ transition of $A_{\text{callee}}$ with transition $t_2$.

Fig. 3.11 shows an example of the transformation of a FB instance into the IM. This rule is general for any PLC language.

---

**Figure 3.11: FC call – IM transformation**

**Rule PLC6 (Building blocks)** PLC code often uses functions or function blocks provided by the system. The source code of these blocks is not available, it has to be created manually. One widely used group of these system blocks are timers. Modeling the timing aspects of timers is a challenging task and it highly increases the state space of the models. Section 3.9 describes the details of corresponding models for the different PLC timers.

3.6.2 ST – IM transformation

This section is dedicated to the specific transformation rules from the ST language into the IM.

**Rule ST1 (ST statement)** A statement is the smallest standalone element of an ST program. It can contain other components (e.g.
expressions). There are different kinds of statements like conditional branches, loops, variable assignments. In this section we define the representation of a single code block consisting of these statements in our IM.

For each statement \( stmt \), let \( n(stmt) \) be the next statement after \( stmt \). As we model cyclic PLC programs, the last statement in the ST code is followed by the first one. Furthermore, for a statement list \( sl \) let \( first(sl) \) be the first statement of the list. The Assumption 3 is also applied here. For each ST statement \( stmt \) in the program block, there is at least one corresponding location marked as \( F_S(stmt) \) in automaton \( A \).

**Rule ST2 (Variable assignment)** This rule translates ST variable assignments into the IM.

**Assumption 7.** For each “variable access” the variable to be accessed can be determined in transformation time. This means that pointers are not supported. However, we support various single and compound variables (arrays and user defined structures). Typically, this is not a restriction as the usage of pointers is not recommended in PLC programs.

For each variable assignment \( stmt = \langle v_i := Expr \rangle \), we add a transition to automaton \( A \) which goes from \( F_S(stmt) \) to \( F_S(n(stmt)) \) which has no guard and no synchronization, and it assigns \( Expr \) to the variable \( F_V(v_i) \) and does not modify the other variables. (Formally: \( t = (F_S(stmt), \text{TRUE}, \langle F_V(v_i) := Expr \rangle, \text{NONE}, F_S(n(stmt))) \).)

Listing 3.1 shows an example of ST code with a simple variable assignment and Fig. 3.12 shows the corresponding automaton fragment.

```plaintext
FUNCTION FC150
  VAR_INPUT
  ...
  END_VAR
  VAR
    v1 : BOOL;
  END_VAR
  BEGIN
    v1 := Expr;
  END_FUNCTION_BLOCK
```

Listing 3.1: Variable assignment in ST code

![Automaton fragment](image)
Rule ST3 (Conditional statement) For each conditional statement \( stmt = \langle \text{IF } c \text{ THEN } sl_1 \text{ ELSE } sl_2 \text{ END_IF} \rangle \), we add two transitions \((t_1 \text{ and } t_2)\) to automaton \( A \):

- The transition \( t_1 \) goes from \( F_S(stmt) \) to \( F_S(first(sl_1)) \), it has no assignments and no synchronizations, and it has a guard \( c \). (Formally: \( t_1 = (F_S(stmt), c, a_{\text{identity}}, \text{NONE}, F_S(first(sl_1))) \))

- The transition \( t_2 \) goes from \( F_S(stmt) \) to \( F_S(first(sl_2)) \), it has no assignments and no synchronizations, and it has a guard \( \text{NOT } c \). (Formally: \( t_2 = (F_S(stmt), \text{NOT } c, a_{\text{identity}}, \text{NONE}, F_S(first(sl_2))) \))

Listing 3.2 shows an example of ST code with a simple conditional statement and Fig. 3.13 shows the corresponding automaton fragment. The statement lists \( sl_1 \) and \( sl_2 \) are modeled according to the rule 1.

```st
FUNCTION FB_A
  VAR_TEMP
  c : BOOL;
  END_VAR
  BEGIN
  IF c THEN
    sl1;
  ELSE
    sl2;
  END_IF;
END_FUNCTION
```

Listing 3.2: Conditional statement in ST code

![Figure 3.13: Corresponding automaton fragment for for conditional statement](image)

Listing 3.3 shows a small example of Siemens ST program, composed of the main program (OB1), a function block (FB_B) and an instance of this function block. The corresponding IM is shown in Fig. 3.14.

```st
ORGANIZATION_BLOCK OB1
  VAR_TEMP
  a2 : BOOL;
  a3 : BOOL;
  END_VAR
  BEGIN
```

![image]
IF a2 THEN
  FB_B.DB1(b1:=NOT a2);
END_IF;
a2 := NOT I0.0;
a3 := DB1.b2;
END_FUNCTION_BLOCK

FUNCTION_BLOCK FB_B
  VAR_INPUT
    b1 : BOOL;
  END_VAR
  VAR_OUTPUT
    b2 : BOOL;
  END_VAR
  BEGIN
    b2 := NOT b1;
  END_FUNCTION_BLOCK

DATA_BLOCK DB1 FB_B
  BEGIN
  END_DATA_BLOCK

Listing 3.3: Example of ST code

Figure 3.14: Example of transformation from a FC call into the IM
3.6.3 SFC – IM transformation

This section is dedicated to a high-level overview of the specific SFC–IM transformation rules.

Assumption 8. There is no parallel branch in the FSM, thus at most one step can be active at the same time. Also steps do not contain any actions. This allows to simplify the discussion.

Each call of a FB implemented in SFC will initiate one transition in the FSM (or zero, if there is no allowed transitions) under our assumptions, multiple transitions cannot be fired by one call.

Rule SFC1 (SFC block) This rule adds to the IM the needed extra information for SFC blocks.

Each automaton $A$ representing an SFC is extended with a transition $t = (l_1, g, amt_{\text{id}}, NONE, end)$, where $g$ is true iff no other $l_1 \rightarrow end$ transitions are enabled. The transition does not change the values of the variables. It represents that if no SFC transitions are allowed, the current state of the FSM will not be modified.

Rule SFC2 (SFC steps) For each step “STEP stepName: END_STEP” we create a Boolean variable $stepName.x$ in $A$. These variables represent the current state of the FSM.

Rule SFC3 (SFC initial step) For the initial step “INITIAL_STEP initStepName: END_STEP” besides of creating a Boolean variable $initStepName.x$ in $A$, we add also a location $l_1$ and a transition $t_1$ from $init$ to $l_1$ without any condition.

We also add a new transition $t = (l_1, g, amt, NONE, end)$. The guard $g$ is $stepName_1 = false \land stepName_2 = false \land \ldots$. The assignment is $amt = \langle initStepName.x := true \rangle$. It means if no steps are active, then the initial step should be active.

Rule SFC4 (SFC transitions)

Assumption 9. Based on our experiments with the SFC editor of Siemens we assume that transitions are defined in ascending order of priority.

For each transition “TRANSITION tName FROM step1 TO step2 CONDITION := C END_TRANSITION” we create a transition $t = (l_1, g, amt, NONE, end)$ in $A$. The guard $g$ of $t$ is a Boolean expression that is only true if (1) $C$ is true, (2) $step1.x$ is true, (3) all the guards
of automaton transitions representing higher priority SFC transitions are false. The assignment is \( amt = (\text{step1}.x := \text{false}; \text{step2}.x := \text{true}) \).

An example automaton representing the SFC shown in Listing 3.4. Its graphical form (Screenshot from SIMATIC tool by Siemens) in Fig. 3.15. Finally, Fig. 3.16 shows the corresponding IM for this example.

```plaintext
FUNCTION_BLOCK FB101
  VAR_INPUT
    FillCond : BOOL := FALSE;
    RunCond : BOOL := FALSE;
    StopCond : BOOL := FALSE;
  END_VAR

  INITIAL_STEP Stop: END_STEP
  STEP Fill: END_STEP
  STEP Run: END_STEP

  TRANSITION S_F
    FROM Stop TO Fill CONDITION := FillCond
  END_TRANSITION

  TRANSITION F_R
    FROM Fill TO Run CONDITION := RunCond
  END_TRANSITION

  TRANSITION R_S
    FROM Run TO Stop CONDITION := StopCond
  END_TRANSITION
END_FUNCTION_BLOCK
```

Listing 3.4: Example of the textual representation of SFC code

### 3.7 Reduction techniques

Once the IM is built and the requirements are formalized, the next step of the methodology is to apply automatic reduction and abstraction techniques to reduce the state space of the IM. For industrial size PLC programs, this step is extremely important as formal verification will not be possible without these reduction techniques.

Some verification tools provide some automatic reduction and abstraction techniques. If these tools are integrated in the methodology,
3.7. Reduction techniques

Figure 3.15: Example SFC (Screenshot from SIMATIC tool by Siemens)

Figure 3.16: IM representation of the SFC example
the methodology will benefit from the reduction techniques. Some authors have proposed reduction techniques applied to a specific input model of a verification tool. In some cases, these reductions cannot be applied to other formalism, because these reduction use the specificities of the modeling language (e.g. Gourcuff et al. (2008) with NuSMV models built from PLC programs).

In this methodology, these reductions are applied to the IM as it is meant to be independent from the verification tools and all the verification tools that are integrated in the methodology can benefit from these techniques. Most of these reduction techniques are general for any CFG, not just for the CFGs of PLC programs. Both alternatives (apply reduction to the IM or the input models of the verification tools) are valid in our approach as it can be seen in Fig. 3.17.

As it was mentioned in Section 3.4, the requirements to be verified are often complex, containing multiple temporal logic operators and involving a large number of variables, which limits the set of possible reduction techniques.

In this methodology, the reduction and abstraction techniques that have been implemented can be classified in two groups:

1. Property preserving reduction techniques: These algorithms aim at preserving only those behaviors of the system that are relevant from the specification point of view. By using property preserving techniques, the meaning of the model is not modified with regard to our assumptions, thus these reductions do not induce any false results that would make the verification much more difficult.

2. Non-preserving abstractions, where the resulting model “loose” some information regarding the original model.

The correctness of the transformation when applying the techniques from the first group is easier to prove, as the reduced model and the original are equivalent for a specific property. However, in some particular cases non-preserving abstractions are applied in this methodology, for example, Section 3.9 presents the modeling strategy for timers. In this case, non-preserving abstractions were applied.

Before describing the reduction techniques, it has to be noticed that in a PLC, the requirements usually are checked only at the beginning and at the end of the PLC cycles, but not in the intermediate
3.7. Reduction techniques

states, as the transient values are not written to the physical outputs of the PLC. As a consequence, the order of the variable assignments is not important, as long as the result at the end of the PLC cycle will be the same. Thus, we know that the requirements are only to be checked at specific locations of the CFG. As it was mentioned in Section 3.6.2, concurrency problems are not considered (assumption 3 described in the previous section).

Figure 3.17: Reduction techniques applied to the IM and to the verification tool models

This section presents the four reduction and abstraction techniques implemented in this methodology. The first three techniques are property preserving reduction techniques and the last one is not:

- First, a new heuristic cone of influence reduction algorithm adapted for models representing CFGs is presented in Section 3.7.1.
- Secondly, a heuristic rule-based reduction techniques to support the cone of influence algorithm is presented in Section 3.7.2.
- Then, a mode selection method which allows the developer to fine-tune the verification by setting the operational mode to be verified in Section 3.7.3.
Finally, a method called *variable abstraction* is described in Section 3.7.4. This method allows to verify large PLC programs, when the previous reduction are insufficient but only verification of safety properties is possible.

The first three reduction techniques have been published in our paper Darvas et al. (2014).

### 3.7.1 Cone of influence

*Cone of influence* (COI), described in Clarke et al. (1999), is one of the most powerful property preserving reduction techniques. It consists in identifying which part of the model is relevant for the evaluation of the given requirement. The unnecessary parts of the model can be removed without affecting the result.

#### 3.7.1.1 Motivation for applying COI at the IM level

Some model checkers, such as NuSMV has a built-in COI implementation that can reduce the verification time drastically. Some experiments applied with our models with the NuSMV model checker, show a bad verification performance even when the COI algorithm could theoretically reduce the model size to trivial. By analyzing the NuSMV’s COI implementation, we found out that this reduction technique could be much more powerful if it was applied to IM directly, where the structure of the CFG is known, before it is transformed to a general state-transition system. In addition, the rest of the verification tools can benefit from this reduction technique if it is applied to the IM.

In higher level models there is usually more knowledge about the modeled system, therefore the reductions are generally more efficient if they are applied to a higher abstraction level. In this case, the COI algorithm can benefit from the structure information present in the intermediate model, but missing from the generated NuSMV model. Therefore, a new heuristic cone of influence algorithm has been developed, which outperforms the COI method built in NuSMV for our models and highly improves the verification performance of our models. To explain the idea behind our approach, first an overview of the COI implementation of NuSMV is given. Then, the new heuristic is introduced and compared with the NuSMV’s COI.
3.7. Reduction techniques

\[
\begin{aligned}
&\text{IF } l_a > 0 \text{ THEN} \\
&\quad x_a := \text{TRUE;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{ELSE} \\
&\quad x_a := \text{FALSE;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{IF } l_b > 0 \text{ THEN} \\
&\quad x_b := \text{TRUE;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{ELSE} \\
&\quad x_b := \text{FALSE;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{END IF;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{END IF;}
\end{aligned}
\]

\[
\begin{aligned}
&c := c + 1
\end{aligned}
\]

\[
\begin{aligned}
&\text{xa} := F \\
&\text{xb} := F
\end{aligned}
\]

\[
\begin{aligned}
&\text{xb} := T
\end{aligned}
\]

\[
\begin{aligned}
&\text{xa} := T
\end{aligned}
\]

\[
\begin{aligned}
&\text{xa} := T
\end{aligned}
\]

\[
\begin{aligned}
&ib > 0
\end{aligned}
\]

\[
\begin{aligned}
&ib > 0
\end{aligned}
\]

\[
\begin{aligned}
&\text{c} := c + 1
\end{aligned}
\]

\[
\begin{aligned}
&\text{init (loc) := initial;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{next (loc) := case}
\end{aligned}
\]

\[
\begin{aligned}
&\text{loc = end : initial;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{loc = initial : l1;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{loc = l1 & ((lA > 0) & lB = 0) : l2;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{loc = l1 & ((lA > 0) & lB = 1) : l3;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{loc = l2 : end;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{TRUE : loc;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{esac;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{next (XA) := case}
\end{aligned}
\]

\[
\begin{aligned}
&\text{loc = l1 & ((lA > 0) & lB = 0) : TRUE;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{loc = l1 & ((lA > 0) & lB = 1) : FALSE;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{TRUE : XA;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{esac;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{false;}
\end{aligned}
\]

\[
\begin{aligned}
&\text{...}
\end{aligned}
\]

Figure 3.18: Example for control flow graph representation of an ST code in NuSMV

The input language of NuSMV represents a Mealy machine, whose states comprise the set of possible valuations of every defined state variable [Cavada et al. 2014, 2011]. In order to create a NuSMV model corresponding to a control flow graph, a natural way of modeling is to express every variable with a dedicated state variable, and to represent the current location in the CFG with an additional state variable (called \( \text{loc} \) in the methodology). This variable \( \text{loc} \) encodes the structure of the CFG along with the guard expressions on its transitions. All the details about the transformation from IM to nuXmv models are described in Section 3.8. The example on Fig. 3.18 shows an extract from a simple ST code, the corresponding CFG and its NuSMV representation.

The COI algorithm of NuSMV has no public documentation. However, as this tool is released under the LGPL license, it is possible to analyze its source code.

At the creation of the NuSMV’s internal COI model, the dependencies of each variable are computed (function \texttt{coiInit}). A variable \( v \) depends on every variable \( v' \) used for the computation of \( v \) (e.g. if the next state of \( v \) is defined with a case block in the NuSMV model, all the variables and values will be in the set of dependencies.) Then, a transitive closure is computed for all the variables occurring in the
formula to be evaluated. If a variable $x$ is necessary for some reason, all the variables presented in the assignment block of $x$ will be necessary too. Therefore, it is trivial that according to the NuSMV implementation, the variable $loc$ is necessary for a variable $v$, if it is assigned at least once in the CFG, because this assignment is guarded by a location of the CFG. As $loc$ is necessary, all the variables in its next-state relation definition will be necessary too, which means all variables taking place in guards are necessary. Thus, none of the variables used in guards can be eliminated by the COI of NuSMV.

3.7.1.2 COI algorithm for the IM

It has been observed that it would be possible to reduce the models by removing conditional branches that do not affect the variables in the requirement. In the example shown in Fig. 3.18, none of the conditional branches is necessary if only variable $c$ is used in the requirement, therefore the variables $ia$ and $ib$ could be eliminated as well.

Guards can affect the control flow, therefore it is not possible to eliminate all the guards. Here the heuristic is proposed, which provides good results when applying it to the IM. The idea is that there are states (locations) in the CFG that are “unconditional”, i.e. all possible executions go through them.

This COI variant consists of three steps (formally: see Algorithm 1):

1. Identification of unconditional states.
2. Identification of variables influencing the evaluation of the given requirement.
3. Elimination of non-necessary variables.

In the following part of this section, these three steps are introduced.

Identification of Unconditional States. The first step of our COI reduction is to identify the set $L$ of unconditional states. To ensure the correctness of the algorithm, it is necessary that $L$ does not include conditional states.

To identify the unconditional states, we defined a measure for the states. A trace is a list of states $(init, l_1, l_2, \ldots, l_n, end)$, where $init$
3.7. Reduction techniques

Algorithm 1: ConeOfInfluence

input: $\mathcal{M}$: network of automata, $Q$: requirement
output: true, iff COI modified the model

$\mathcal{L} \leftarrow \text{UnconditionalStates}(\mathcal{M})$;
$D \leftarrow \text{NecessaryVariables}(\mathcal{M}, \mathcal{L}, Q)$;
Removal of all variables in $V \setminus D$, with their guards and assignments;
return $V \setminus D \neq \emptyset$;

is the initial state of the automaton, $\text{end}$ is the end state of the automaton, and there is a transition between each $(l_i, l_{i+1})$ state pairs. Let $F(l)$ be the fraction of possible traces going through a state $l$. It is known that all the traces go trough the initial state $\text{init}$, therefore $F(\text{init}) = 1$. For the rest of the states, $F$ can be calculated based on the incoming transitions.

Let $I_T(l) \in 2^T$ depict the set of incoming transitions to state $l$, and mark the set of outgoing transitions from state $l$ as $O_T(l) \in 2^T$. Let $I_L(t) \in L$ be the source state of transition $t$. With this notation, the formal definition of $F(l)$ is the following:

$$F(l) := \begin{cases} 1 & \text{if } l = \text{init}, \\ \sum_{t \in I_T(l)} \frac{F(I_L(t))}{|O_T(I_L(t))|} & \text{otherwise.} \end{cases} \quad (3.1)$$

After calculating $F$ for each state, it is easy to compute the set of unconditional states: $\mathcal{L} = \{l \in L : F(l) = 1\}$.

Notice, that the intermediate model can contain loops (beside the main loop representing the PLC cycle) due to loops in the input model. In this case, we handle all states in the loop as conditional states (without computing $F$ for them).

Identification of Necessary Variables. The goal of the second step is to collect automatically all the variables necessary to evaluate the given requirement (see Algorithm 2). Let $D$ be the set of necessary variables. It is trivial that every variable in the requirement should be

---

\(^3\)Here we do not consider cycles inside the CFG beside of the cycle corresponding to the main cycle.
in $D$. After that, for each variable assignments that modify a variable in $D$, the variables in the assignment will also be added to the set $D$. Furthermore, the guard dependencies should also be added to $D$, i.e. all the variables that can affect the execution of the analyzed variable assignment. If the set of $D$ grew, all the assignments should be checked again.

In the following, we define a function $A_T: T \rightarrow 2^V$, which gives all the variables that can affect the execution of variable assignments on transition $t$.

First, a supporting function $A_L: L \rightarrow 2^V$ is defined which gives all the variables necessary to determine if state $l$ will be active or not during an execution. This function can benefit from the previously explored unconditional states $L$, as it is known that no variable is necessary to decide if they can be activated during an execution. Thus, for every state $l \in L$, the function $A_L(l)$ is the following:

$$A_L(l) := \begin{cases} \emptyset & \text{if } l \in \mathcal{L} \\ \bigcup_{t \in I_L(l)} A_T(t) & \text{if } l \notin \mathcal{L}. \end{cases} \quad (3.2)$$

It means that for the unconditional states, the set of affecting variables is empty, as a consequence of their definition. If a state is not unconditional, the set of variables affecting that this state is active or not is the set of variables affecting the firing of all its incoming transitions.

For every transition $t \in T$, the function $A_T(t)$ is the following:

$$A_T(t) := A_L(I_L(t)) \cup \bigcup_{t' \in O_T(I_L(t))} \{ \text{variables in guard of } t' \}. \quad (3.3)$$

It means that the firing of transition $t$ is affected by the variables that influences its source state ($I_L(t)$) and by the variables in the guard of $t$. Furthermore, it is also influenced by the variables used in the guard of transitions that can be in conflict with $t$, i.e. the guard variables of $t' \in O_T(I_L(t))$.

**Elimination of Non-necessary Variables.** In the second step, the set $D$ of necessary variables is determined. In the last step, all the variables not in $D$ should be deleted. Also, to ensure the syntactical
Algorithm 2: NecessaryVariables

\textbf{input}: \(\mathcal{M}\): network of automata, \(\mathcal{L}\): set of unconditional states, 
\(Q\): requirement 

\textbf{output}: \(D\): set of necessary variables 

\[D \leftarrow \{\text{variables in } Q\};\]

\textbf{repeat}

\textbf{foreach} variable assignment \(\langle v := \text{Expr} \rangle\) on transition \(t\) \textbf{do}

\textbf{if} \(v \in D\) \textbf{then}

\textit{// adding assignment and guard dependencies}

\[D \leftarrow D \cup \{\text{variables in } \text{Expr}\} \cup \mathcal{A}_T(t);\]

\textbf{until} \(D\) is not changed;

\textbf{return} \(D\);

\[
\text{correctness, all the guards and variable assignments containing variables } v \notin D \text{ should be deleted. They do not affect the evaluation of the requirement, otherwise they should be in set } D.\\
\]

\textbf{Difference between our COI and the COI of NuSMV.} The main difference between our COI and the COI implementation of NuSMV is in the handling of conditional branches. If there is a conditional branch in the CFG, but the variables in the requirement are not affected by this choice, there is no need for the variables in its guard. This difference can be observed in Fig. 3.19, which shows the CFG introduced in Fig. 3.18 after applying the different COIs, and assuming that only variable \(c\) is used in the requirement (e.g. \(\text{EF}c < 0\)). The COI of NuSMV can identify that the variables \(xa\) and \(xb\) are not used to compute \(c\), therefore they will be removed. But the variables \(ia\) and \(ib\) are used in guards, thus they are kept (see Fig. 3.19(a)).

Our COI algorithm can detect that because \(xa\) and \(xb\) are deleted, the \(ia\) and \(ib\) variables can be deleted too, because those guards do not affect \(c\), i.e. no matter which computation path is executed between locations \(l_1\) and \(l_3\), the assignment of variable \(c\) will be the same (see Fig. 3.19(b)). The resulting IM after applying our COI algorithm is shown in Fig. 3.19(c).
Chapter 3. Approach

3.7.2 Rule-based reductions

The COI applied to the IM only eliminates variables, the connected variable assignments and guards, without modifying the structure of the CFG. Therefore, the resulting model of the COI often contains empty transitions, unnecessary states, etc. For these situations, rule-based reductions have been implemented that make the model smaller and easier to verify.

This kind of CFG reductions are not new, they are used for example in numerous compilers to simplify the machine code and to improve the performance. More details can be found in Cooper and Torczon (2012).

The rule-based reductions applied to the IM can be classified as follows:

- **Model simplifications.** The aim of these reductions is to simplify the intermediate model without reducing its potential state space (thus without eliminating states or variables). This group includes elimination of unnecessary variable assignments or transitions, and simplification of logical expressions. These reductions do not reduce the model themselves, we created them...
to support the other reduction techniques. For example, if the model contains an empty conditional branch (due to for example another reduction), it can be removed without changing the meaning of the model. This rule is illustrated in Fig. 3.20(a).

- **Model reductions.** These methods can reduce the potential state space by eliminating states and variables. This group includes heuristics to merge transitions or states, to eliminate variables that have always the same constant value, etc. For example, if a transition has no guard, no synchronization, and no variable assignment (which can be a side effect of the COI reduction), then the two states on the end of the transition can be merged and the transition can be deleted. This rule is illustrated in Fig. 3.20(b).

- **Domain-specific reductions.** These reductions are benefited by the PLC domain knowledge using the assumption introduced at the beginning of Section 3.7, that variables are only checked at the end of the PLC cycle. Two main domain-specific reductions are developed:

  - **Transition merging.** Two consecutive transitions can be merged if they represent a sequence in the CFG and their variable assignments are not in conflict, i.e. their order does not affect each other’s value. Formally, \( v_a := E_a \) and \( v_b := E_b \) are not in conflict if \( v_a \notin \text{Vars}(E_b) \), \( v_b \notin \text{Vars}(E_a) \), and \( v_a \neq v_b \), where \( \text{Vars}(E) \) means all variables used in expression \( E \). This can easily be extended to two set of variable assignments, thus it can be reapplied to merged transitions. Fig. 3.20(c) illustrates this reduction rule.

  - **Variable merging.** Two variables can be merged if they always have the same value at the end of the PLC cycles. While creating two variables for the same purpose can be considered as a bad programming practice, it is a common pattern in the source code of our systems. This feature is used to improve code readability by assigning a meaningful name to a bit of an input array (for example `PFailSafePosition` instead of `ParReg01[8]`).
It has to be noted that not all the previously mentioned reduction techniques are property preserving in themselves. For instance, if two variables \( v \) and \( w \) are merged, thus \( w \) will be deleted, the properties containing \( w \) are not possible to evaluate. For this reason, we generate a mapping throughout the reductions that contains all the variable substitutions. Based on this mapping, the necessary aliases can be generated for the NuSMV model. For example, an alias \( w \) can be added to the model having always the same value as \( v \), as it is known that they always contain the same value at the end of the PLC cycles. Aliases do not modify the size of the state space or the complexity of the model checking.

As discussed at the beginning of Section 3.7.2, the COI algorithm can enable the rule-based reductions. Therefore, after applying the COI algorithm, all the reduction techniques introduced in this section will be applied, which can enable other reductions or other possible variable removal for the COI algorithm. Therefore we implemented the reductions in an iterative manner. First, the COI is executed. Then, all the possible reductions are applied. If the COI or one of the rule-based reductions was able to reduce the model, all the reductions are executed again. This iterative workflow is described formally in

Figure 3.20: Example reduction rules from Darvas et al. (2014)
3.7. Reduction techniques

Algorithm 3. (The function $\text{Reduce}(r, M)$ applies reduction $r$ on the model $M$ and returns true, iff the reduction modified the model.)

A simple example is shown here illustrating our reduction workflow. If our COI is applied to the Fig. 3.18 CFG example, then Fig. 3.19(c) CFG will be obtained. If the reductions presented on Fig. 3.20(a) and Fig. 3.20(b) are applied on it, the result will be the simple Fig. 3.21 CFG.

**Algorithm 3: Reductions**

```plaintext
input : $M$: model, $Q$: requirement
bool changed;
repeat
    changed ← $\text{ConeOfInfluence}(M, Q)$;
    foreach $r \in \{\text{rule-based reductions}\}$ do
        changed ← $\text{Reduce}(r, M) \lor changed$;
    until changed = false;
```

![Figure 3.21: Example CFG after our COI and the reductions from Darvas et al. (2014)](image)

3.7.3 Mode selection

Good practices and standards in PLC program development (e.g. [IEC 61499 (2013)]) suggest to have a library of Function Blocks, which are the basic building modules of the control systems. These modules can be reused in different PLC programs. For example, at CERN, the UNICOS framework provides a library of objects where the elements from the instrumentation can be represented. In the PLC code, these objects are Function Blocks and they are generic so can be adapted for the specific uses by setting some parameters. Parameters are input variables that are constant during the execution, as they are hard-coded into the PLC application.

A significant part of our real requirements have assumptions on the parameters, like:

“if parameter $p_1$ is true, then it is always true that ...”
For these requirements, general models can be used and the parameter configuration can be included in the temporal logic formula, or by adding invariants to the model. However, better performance can be achieved if the configuration is encoded in the model itself by replacing the parameter with its constant value. This way, the developers can select the operational mode of the object on which the verification should be performed, i.e. they can fine-tune the verification to their needs. This method is applied only once, before all the other reductions.

The advantages of this method are the following:

- There is no need to create a variable for the fixed parameter as it is substituted with a constant.

- The rule-based reductions can simplify the expressions. For example, if there is a guard \([p_1 \land p_2 \land p_3]\) in the CFG and \(p_1\) is fixed to false, the guard will be always false and can be replaced by a constant false.

- The simplification of the expressions can help the cone of influence reduction to remove the unnecessary variables, e.g. if \(p_2\) and \(p_3\) are only used in the guard \([p_1 \land p_2 \land p_3]\), and \(p_1\) is fixed to false, the variables \(p_2\) and \(p_3\) can be removed. Using the COI in NuSMV or if the fixed parameter is expressed through invariants, this reduction cannot be done.

Now the complete reduction workflow can be summarized. After the transformation of the source code into the intermediate model, the given parameters are fixed to the required values. Then the cone of influence reduction and the rule-based reductions are performed iteratively (as seen in Fig. 3.22). It is important to note, that since every reduction rule deletes something from the model upon firing, they cannot “reduce” the model infinite times, thus the iteration cycle will stop in finite time.

### 3.7.4 Iterative variable abstraction

The effectiveness of the previous reduction techniques highly depends on the property specification. In some cases, these reductions can be very effective but in some others they are not sufficient for the
3.7. Reduction techniques

verification tools, for example when the reduced model contains still a lot of variables or the data types of these variables are not just Boolean. In these cases, the state space of the reduced model is still too large to be verified by any tool, for example in most of the verification cases of complete UNICOS PLC programs (Chapter 4 presents one of these programs).

For that reason, a new method called variable abstraction is included in the methodology. Using this technique, abstract models are created by replacing some of the variables by non-deterministic values, transforming these variables in “input variables”, which were described in Section 3.5. As these new input variables do not depend on any other variables, the COI algorithm will be able to eliminate more variables from the model automatically.

The resulting model, after this abstraction, is an over-approximation of the original model, which contains less variables than the original model and it represents a bigger range of possible behaviors of a system. This means that the abstract model has some states (combination of variable values) that do not belong to the original model and therefore to the real PLC program.

Before describing the method, a few basic concepts are discussed. This technique is currently limited to the following safety properties: $\text{AG}(\alpha \rightarrow \beta)$. This is because the requirements for the verification of complete UNICOS PLC program are currently safety properties. By restricting the possibilities in the property specification, a more aggressive abstraction technique can be applied and we increase the chances of getting a verification result from the model checker. This is the reason of including this restriction.

In this technique, abstract models are created using the variable dependency graph of the original model (which corresponds with the PLC program).

Consider an abstract model $AM'_n$ and a safety property $p$ ($\text{AG}(\alpha \rightarrow \beta)$). When applying model checking, if $p$ holds on $AM'_n$, it implies that
Chapter 3. Approach

$p$ also holds in the original model $OM'$ as a bigger range of possible behaviors is explored. If $p$ does not hold on $AM'_n$, a counterexample $c$ is generated. To determine if $p$ holds on $OM'$, it is needed to analyze if $c$ is a real or a spurious counterexample. If it is a spurious counterexample, $AM'_n$ needs to be refined.

Fig. 3.23 represents this idea. The violet shading represents all the possible models where $p$ holds. In other words, it represent all the possible behaviors where the property $p$ is respected. Note that $AM'_n$ is an over-approximation of $OM'$. $AM'_n$ has a state space size smaller than $OM'$ (as it contains less variables) but it represents a bigger range of possible behaviors.

In Fig. 3.23(a) $p$ holds in $AM'_n$ and therefore it holds in $OM'$. In Fig. 3.23(b) and Fig. 3.23(c) $p$ does not hold in $AM'_n$ and it is not possible to determine if $p$ holds on $OM'$ without analyzing the counterexample.

Figure 3.23: Verification cases for $AG(\alpha \rightarrow \beta)$ in abstract models

In order to determine if this counterexample is real or spurious,
one possibility is to transform this counterexample in a reachability property \((\text{EF}(\gamma \& \theta))\). Regarding the verification of a reachability property \(r\) in an abstract model \(AM''_n\), the logic is different. If \(r\) does not hold in \(AM''_n\), then \(r\) does not hold in the original model \((OM'')\). But if \(r\) holds on \(AM''_n\), we cannot determine if \(r\) holds on \(OM''\) or not.

Fig. 3.24 describes this idea. In this case, the black dot represent the state where the property \(r\) holds.

In Fig. 3.24(a) \(r\) does not hold on \(AM''_n\) and therefore it does not hold in \(OM''\). In Fig. 3.24(b) and Fig. 3.24(c), \(r\) holds in \(AM''_n\) and it is not possible to determine if \(r\) holds on \(OM''\).

Figure 3.24: Verification cases for \(\text{EF}(\gamma \& \theta)\) in abstract models

These concepts are applied in the variable abstraction technique.

The variable dependency graph is provided by the COI algorithm (defined in 3.7.1) and it gives all the necessary variables \(D\) for a given requirement. Fig. 3.25 shows an example of the variable dependency graph in a model from a real-life PLC program. The gray variables are part of the requirement, the red edges represent assignment depen-
dependencies and the blue edges represent conditional dependencies. Two different variables connected by an edge are in a distance equals to 1. The concept of distance between variables is used to build the abstract models.

3.7.4.1 General description of the variable abstraction technique

This technique is represented in Fig. 3.26 and as well as the previous reduction techniques, it is applied to the IM.

The basic idea of the algorithm is the following: The safety property \( p \) is verified in an abstract model \( (AM'_n) \), where \( n \) corresponds to the number of iterations of the algorithm. If \( p \) holds on \( AM'_n \), the algorithm is over and we can conclude that \( p \) holds on the original model \( (OM') \). If \( p \) does not hold on \( AM'_n \), a counterexample \( (c) \) is provided by the model checker but we need to determine if \( c \) is a spurious counterexample due to the abstraction or it is real. To do so, two steps are performed: first a new safety property \( (q) \) is checked on \( AM'_n \) with the goal of obtaining more information about the state space of \( AM'_n \) where \( p \) holds. Then, if no extra information is provided, \( c \) is transformed into a reachability property \( (r) \) to prove or discard that \( c \) is real. If \( c \) is real, it means that \( p \) does not hold on \( OM' \). If \( c \) is spurious, an invariant is added to \( AM'_n \) or a new abstraction of \( AM'_n \) (a more refined model) is created if the number of potential invariants \( (m) \) is not worthwhile to be analyzed. Then the process is repeated.

The algorithm can be divided then in five steps (see Fig. 3.27), regarding the five decision points of the flow diagram (the initial one is not considered, as it is the input to this algorithm: a time out is obtained when verifying \( p \) on the original model \( OM' \)):

1. Checking the original safety property \( (p) \) on an abstract model \( (AM'_n) \).
2. Checking the safety property \( (q) \) on the same abstract model \( (AM'_n) \).
3. Checking the reachability property \( (r) \) on the original model \( (OM'') \).
3.7. Reduction techniques

Figure 3.25: Variable dependency graph example
4. Checking the reachability property \((r)\) on an abstract model \((AM''_n)\).

5. Extracting an invariant from the counterexample obtained in step 2 if \(m\) is \(\leq 10\).

The following paragraphs describe the details of the five steps of this technique.

### 3.7.4.2 Checking the original safety property \((p)\) on an abstract model \((AM'_n)\)

The algorithm starts by checking the safety property \(p\) (i.e. \(AG(\alpha \rightarrow \beta)\)) on the original model \(OM'\). \(OM'\) is the result of applying the property preserving reductions (described earlier in this section) to the generated model from the PLC code. In addition, two parameters (\(\delta'\) and \(\delta''\)) are initialized to 0.

- \(\delta'\) represents the distance between variables in the variable dependency graph for \(OM'\). \(\delta''\) represents the distance between variables in the variable dependency graph for \(OM''\).

- \(OM'\) is the resulting model of applying the property preserving reduction techniques for the original safety property \(p\). \(OM''\) is the resulting model of applying the property preserving reduction techniques for the reachability property \(r\).

- Abstract models \((AM'_n\) and \(AM''_n)\) are created automatically using \(\delta'\) and \(\delta''\) respectively.

- \(TO\) (Time Out) is a parameter set at the beginning of this technique, which represents the maximum amount of time given to the model checker to provide an answer (true or false) for the verification.

In the first iteration, if the model checker cannot provide an answer when verifying \(p\) on \(OM'\) and the \(TO\) is reached, an abstract model is automatically generated using \(\delta' = 1\), i.e. \(AM'_1\). Then the model checker verifies if \(p\) holds on \(AM'_1\). Three possible answer can be provided by the model checker:

1. **True**: \(p\) holds on \(AM'_n\), therefore the algorithm is over and we can conclude that \(p\) holds on \(OM'\) (as it was described in Fig. 3.23).

2. **TO**: the algorithm is over and we cannot prove whether \(p\) holds or not on \(OM'\) (this situation should never happen on the first
3.7. Reduction techniques

iterations of the algorithm, e.g. $AM_1'$ and $AM_2'$, as they usually have a much small state space size when compared to $OM'$). This is the limitation of the methodology, it is not possible to determine if the generated counterexamples from previous abstractions ($AM_{n-1}$, $AM_{n-2}$, ... $AM_1$) were real or spurious.

3. **False:** $p$ does not hold on $AM_n'$, and the algorithm moves to the step 2 in order to prove that the provided counterexample ($c$) is real or spurious (as it was described in Fig. 3.23).

The abstract models are built applying the following logic: Having $OM'$ and $p$ $(AG(\alpha \rightarrow \beta))$, a set of variables from $OM'$ are converted to “input variables”. The idea here is that all variables with a distance $(d)$ equals to $\delta'$ from the variable $\beta$ are transformed to “input variables”. $\alpha$ is also transformed to an “input variable”, if the distance of $\alpha$ with respect of $\beta$ is $d \geq \delta'$.

The initial value of $\delta'$ is 0 and incremented to 1 in the first iteration ($n = 1$). This means that in the first iteration the resulting abstract model ($AM_1'$) is the most abstract model possible. In the following iterations, depending on the decisions of the steps 3 and 5, $\delta'$ is increased ($\delta' := \delta' + 1$) or is not modified.

The algorithm 4 summarizes the proposed heuristic.

---

**Algorithm 4: ModelAbstraction**

**input** : $D_g'$; dependency graph of the $OM'$, $p$: requirement, $\delta'$: distance

**output**: $AM_n'$: abstract model

$V \leftarrow AbstractedVariables$;

Identify the variables to be abstracted $V$: $d = \delta'$ from $\beta$. $\alpha$ is also included in $V$ (if $\alpha$ is a distance $d \geq \delta'$);

Removal of all the assignments of the abstracted variables $V$;

Replace all the abstracted variables $V$, by non-deterministic values;

**return** $AM_n'$;
3.7.4.3 Checking the safety property \(q\) on the same abstract model \((AM'_n)\)

This step is included in the algorithm to extract more information about the verification of \(p\) on \(AM'_n\) before analyzing the counterexample \(c\). The idea is to check the property \(q\): \(\text{AG}(\alpha \rightarrow \neg \beta)\), on the same abstract model \((AM'_n)\) as \(p\). \(q\) only differs from \(p\) on the negation of \(\beta\).

Verifying the property \(q\) on \(AM'_n\) has a similar complexity as verifying \(p\) on \(AM'_n\), because the model is the same and the property has the same temporal operator (AG) and the same variables. Therefore a \(TO\) should never happen in this step if it did not happen with \(p\) in the previous step. However this possibility is also considered on the algorithm. Therefore three possible answers can be provided by the model checker:

1. \(True\): \(q\) holds on \(AM'_n\) and the algorithm is over. We can conclude that \(p\) does not hold on \(OM'\) and the provided counterexample in the previous step \((c)\) is real.

2. \(False\): \(q\) does not hold on \(AM'_n\) and the algorithm moves to the step 3 in order to prove that the provided counterexample \((c)\) is real or spurious by transforming \(c\) in a reachability problem.

3. \(TO\): no further information is provided and the algorithms moves to the step 3 in order to prove that the provided counterexample \((c)\) is real or spurious by transforming \(c\) in a reachability problem.

Fig. 3.28 describes graphically the different verification cases that may occur in this step. Again, the violet shading represents all the possible models or state spaces where the properties \(q\) or \(p\) hold.

In 3.28(a) \(q\) holds in \(AM'_n\) and therefore \(p\) does not hold on \(AM'_n\) and we can conclude that \(p\) does not hold on \(OM'\). The counterexample \(c\), provided in step 1, is real.

In 3.28(b), 3.28(c) and 3.28(d) \(q\) does not hold in \(AM'_n\) and it is not possible to determine if \(p\) holds on \(AM'_n\) and \(OM'\) without analyzing the counterexample.
3.7. Reduction techniques

(a) $\text{AG}(\alpha \rightarrow \neg \beta)$ is true in $\text{AM}_n'$, therefore $\text{AG}(\alpha \rightarrow \beta)$ is false in $\text{AM}_n'$ and $\text{OM}'$

(b) $\text{AG}(\alpha \rightarrow \neg \beta)$ is false in $\text{AM}_n'$ and $\text{AG}(\alpha \rightarrow \beta)$ is true in $\text{AM}_n'$ and $\text{OM}'$

(c) $\text{AG}(\alpha \rightarrow \neg \beta)$ is false in $\text{AM}_n'$ and $\text{AG}(\alpha \rightarrow \beta)$ is false in $\text{AM}_n'$ and $\text{OM}'$

(d) $\text{AG}(\alpha \rightarrow \neg \beta)$ is false in $\text{AM}_n'$ and $\text{AG}(\alpha \rightarrow \beta)$ is false in $\text{AM}_n'$ but true in $\text{OM}'$

Figure 3.28: Relationship between the verification cases for $\text{AG}(\alpha \rightarrow \neg \beta)$ and $\text{AG}(\alpha \rightarrow \beta)$ in abstract models
3.7.4.4 Checking the reachability property \((r)\) on the original model \((OM'')\)

The third step of the algorithm consists in extracting a reachability property \(r\) from the counterexample \(c\). In addition, using the property preserving reduction techniques with this property, a new “original model” \(OM''\) is generated. Note that \(OM''\) and \(OM'\) may be different as the properties \(p\) and \(r\) contain different variables and therefore the reduction techniques, such as, COI will eliminate different variables from the model.

Initially \(r\) is verified on \(OM''\) and three possible answers can be provided by the model checker:

1. **True**: \(r\) holds on \(OM''\), which means that \(c\) is real and therefore \(p\) does not hold on \(OM'\).
2. **False**: \(r\) does not hold on \(OM''\), which means that \(c\) is spurious and the algorithm moves to the step 5.
3. **TO**: an answer cannot be provided and the algorithm moves to the step 4.

It has to be noticed that the counterexample \(c\) can be complex (it contains the variable values in any location of the IM). However, as it was mentioned in Section 3.5 in PLC programs the relevant values are at the end of the PLC cycle. This assumption reduces the counterexample, as we need the value of the variables at the location end of the IM.

For the reachability property, it is only needed the “input variables”, as they are the ones that add more possible behaviors to the AM. For example, if a generated counterexample contains the “input variables” \(\gamma\) and \(\zeta\), only these variables are part of the reachability property, i.e. \(\text{EF}(\gamma \& \zeta)\).

In addition, even more complex counterexamples can be produced: counterexamples containing variable values from different PLC cycles. In this situation, several reachability property can be extracted. For example, if the counterexample has three cycles, three reachability properties checking the values of the variables at the end of each PLC cycle and two reachability properties checking the transitions between
the cycles could be extracted. If only one of the properties are not satisfied, this means the counterexample is spurious.

Potentially in step 5 of the algorithm, spurious counterexample can be added as invariants to $AM'_n$ and the process is repeated. However, to the best of the author’s knowledge, most of the model checkers only allow to add invariants without temporal operators (e.g. NuSMV), therefore the two reachability properties checking the transitions between the cycles cannot be extracted.

The strategy in this situation is that only one reachability property $r$ is extracted, corresponding to the values of the transformed “input variables” at the end of the first PLC cycle. If when verifying $r$ on $OM''$ the result is false and in step 5 an invariant is added, in the next iterations of the algorithm new counterexamples will be generated and the same strategy is applied.

3.7.4.5 Checking the reachability property ($r$) on an abstract model ($AM''_n$)

When a $TO$ is reached in the previous step, the property $r$ is verified in an abstract model $AM''_n$. The strategy of producing abstract models here is the same as in the step 1 (algorithm 4), but now the inputs are $D''_g$ (dependency graph of the $OM''$), $r$ and $\delta''$ and the output $AM''_n$.

In the first iteration, $AM''_1$ is automatically generated using a $\delta'' = 1$. Three possible answers can be provided by the model checker:

1. **False**: $r$ does not hold on $AM''_n$ and therefore it does not hold on $OM''$ (as it was described in Fig. 3.24), which means that $c$ is spurious and the algorithm moves to the step 5.

2. **True**: $r$ holds on $AM''_n$ but we cannot determine if it holds on $OM''$ (as it was described in Fig. 3.24). In this case, a new abstract model $AM''_n$ is created by incrementing $\delta''$ ($\delta'' = \delta'' + 1$), and the process is repeated.

3. **TO**: an answer cannot be provided and the algorithm moves to the step 1 and a new iteration of the algorithm is executed with a new abstract model $AM'_n$ ($\delta' := \delta' + 1$).
3.7.4.6 Extracting an invariant from the counterexample obtained in step 2 if \( m \) is \( \leq 10 \)

When the previous steps have determined that the counterexample \( c \) is spurious, this step takes the decision of adding a new invariant to the same abstract model \( AM'_n \) or moving to a new abstraction \( AM'_{n+1} \) by incrementing \( \delta' \).

The strategy in this step is based on the relationship between the abstract models and the maximum number of possible invariants for all the abstract models \( (AM'_1, AM'_2, ..., AM'_n) \), where \( AM'_n \) correspond to the original model \( OM' \).

Fig. 3.29 shows four examples corresponding with three different PLC programs of the relationships between the abstract models and the maximum number of invariants to be extracted if variable abstraction is applied. In all of the PLC programs we have verified, we found the same pattern as it can be observed in this figure. In most of them, for \( \delta' \leq 2 \), the number of invariants is reasonable to be extracted but from \( \delta' > 2 \) is more optimal to move to a new abstract model as it contains more information and the computational problem is likely smaller.

The mapping between the abstract models and the maximum number of possible invariants is automatically generated when the variable dependency graph is created. Therefore, the strategy is the following: for each \( AM'_n \) with a maximum number of possible invariants \( m \leq 10 \) (in our experiments it usually corresponds with \( \delta' \leq 2 \)) and the reachability property verification result is false, an invariant is added to the same \( AM'_n \). If \( m > 10 \), then no invariant is added and the algorithm moves to a new iteration with a new \( AM'_{n+1} \) by incrementing \( \delta' \) \( (\delta' := \delta' + 1) \).

For example, if the reachability property is \( EF(\gamma \& \zeta) \), the extracted invariant is the following:

\[
\text{INVAR: } \neg(\gamma \& \zeta)
\]

3.7.4.7 Example of applicability

To help the understanding of this method, the following paragraphs present the verification a very simple PLC program using this technique (obviously the model of this PLC program does not need ab-
3.7. Reduction techniques

Figure 3.29: Relationship between the abstract models and the maximum number of possible invariants for the variable abstraction technique
straction to be verified, but it is useful to understand the different steps of this technique). The PLC code of this example is shown in Listing 3.5. It consists of a simple function with six Boolean variables and it uses two input variables from the IIM. The requirement to be checked is the following:

“If \( b \) is true at the end of the PLC cycle, then \( a \) is always true at the end of the same PLC cycle.”

The formalized requirement \( p \) using the patterns is:

\[
AG((EoC \land b) \rightarrow a)
\]

\( EoC \) is the variable which is TRUE when the active location of the IM is \textit{end} and FALSE when is any other location.

```plaintext
FUNCTION Test1
VAR
  a : BOOL;
  b : BOOL;
  w : BOOL;
  x : BOOL;
  y : BOOL;
  z : BOOL;
END_VAR
BEGIN
  z := I0.0 AND I0.1;
  b := z;
  w := I0.1 AND NOT I0.0;
  y := z AND NOT w;
  x := b AND I0.0;
  a := x AND y;
END_FUNCTION
```

Listing 3.5: Example of ST code

The corresponding IM for this PLC program is represented in Fig. 3.30.

**Step 1:** the variable dependency graph for this PLC program is represented in Fig. 3.31
3.7. Reduction techniques

![Diagram of IM with variables and equations]

**Figure 3.30:** Example of IM

![Diagram of variable dependency graph]

**Figure 3.31:** Variable dependency graph of the original model corresponding to the PLC program example
Following this algorithm, the resulting variable dependency graph for the proposed PLC program example is represented in Fig. 3.32.

In the first iteration $AM'_1$ is generated using $\delta := 1$. The variables $x$ and $y$ are at distance 1 from $a$, and therefore they are converted to input variables. The variable $b$ is not at distance 1 from $b$, therefore it is also converted to an input variable.

![Variable dependency graph of the abstract model corresponding to the PLC program example](image)

Figure 3.32: Variable dependency graph of the abstract model corresponding to the PLC program example

Due to this abstraction based on the variable dependency graph, the IM of the new $AM$ is presented in Fig. 3.33. It can be observed that the variables $w$, $z$, $I0.0$ and $I0.1$ are eliminated and the variables converted to input variables are $y$ and $z$ and $a$.

The verification result for $p$ is false, and the generated counterexample $c$ is shown in Table 3.2.

<table>
<thead>
<tr>
<th>Variable</th>
<th>End of Cycle1</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>FALSE</td>
</tr>
<tr>
<td>b</td>
<td>TRUE</td>
</tr>
<tr>
<td>x</td>
<td>FALSE</td>
</tr>
<tr>
<td>y</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

| Step 2: the safety property $q$ is the following: |
3.7. Reduction techniques

Figure 3.33: Abstraction strategy applied to the example
AG\left(\left(EoC \land b\right) \rightarrow \neg a\right)

EoC is the variable which is TRUE when the location of the IM is end and FALSE when is a any other location.

In this case, the verification result is false again and we cannot determine yet if c is real or spurious. Therefore the algorithm moves to the step 3.

**Step 3:** the reachability property r generated from c is:

\[ EF\left(EoC \land b \land \neg x \land \neg y\right) \]

When verifying r in the new OM", the result is false, which means that c is spurious and the algorithm moves to the step 5.

**Step 5:** as the number of potential invariants for AM'_1 is 8, an invariant is added to the same abstract model (AM'_1). The extracted invariant is the following:

\[ \text{INVAR: } \neg(b \land \neg x \land \neg y) \]

**Step 1:** p is verified again on AM'_1 but containing the new invariant. The verification result is false and the new counterexample c is shown in Table 3.3.

<table>
<thead>
<tr>
<th>Variable</th>
<th>End of Cycle1</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>FALSE</td>
</tr>
<tr>
<td>b</td>
<td>TRUE</td>
</tr>
<tr>
<td>x</td>
<td>TRUE</td>
</tr>
<tr>
<td>y</td>
<td>FALSE</td>
</tr>
</tbody>
</table>
3.7. Reduction techniques

Step 2: the safety property \( q \) is verified again on \( AM'_1 + \) invariant. In this case, the verification result is false again and we cannot determine yet if \( c \) is real or spurious. Therefore the algorithm moves to the step 3.

Step 3: the reachability property \( r \) generated from \( c \) is:

\[
\text{EF} \left( EoC \land b \land x \land \neg y \right)
\]

When verifying \( r \) in the new \( OM'' \), the result is false, which means that \( c \) is spurious and the algorithm moves to the step 5.

Step 5: as the number of potential invariants for \( AM'_1 \) is 8, a second invariant is added to the same abstract model (\( AM'_1 \)). The extracted invariant is the following:

\[
\text{INVAR}: \neg (b \land x \land \neg y)
\]

Step 1: \( p \) is verified again on \( AM'_1 \) but also containing the second invariant. The verification result is false and the new counterexample \( c \) is shown in Table 3.4.

<table>
<thead>
<tr>
<th>Variable</th>
<th>End of Cycle1</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>FALSE</td>
</tr>
<tr>
<td>b</td>
<td>TRUE</td>
</tr>
<tr>
<td>x</td>
<td>FALSE</td>
</tr>
<tr>
<td>y</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

Step 2: the safety property \( q \) is verified again on \( AM'_1 + 2 \) invariants. In this case, the verification result is false again and we cannot determine yet if \( c \) is real or spurious. Therefore the algorithm moves to the step 3.
Step 3: the reachability property $r$ generated from $c$ is:

$$\text{EF}(EoC \land b \land \neg x \land y)$$

When verifying $r$ in the new $OM''$, the result is false, which means that $c$ is spurious and the algorithm moves to the step 5.

Step 5: as the number of potential invariants for $AM'_1$ is 8, a third invariant is added to the same abstract model ($AM'_1$). The extracted invariant is the following:

$$\text{INVAR}: \neg(b \land \neg x \land y)$$

Step 1: $p$ is verified again on $AM'_1$ but also containing the third invariant. The verification result is true, the algorithm is over and we can conclude that $p$ holds on $OM'$.

### 3.8 IM– verification tools transformation

This section describes the transformation from the IM to the modeling languages used as inputs by the verification tools. Currently, three tools have been integrated in the methodology: nuXmv, UPPAAL and BIP. This section is divided in 3 parts explaining the rules for each tool:

- Transformation rules from IM code to nuXmv.
- Transformation rules from IM code to UPPAAL.
- Transformation rules from IM code to BIP.

#### 3.8.1 IM–nuXmv transformation

The following paragraphs contain a brief introduction of the nuXmv modeling language and the transformation rules to produce nuXmv code from the IM.
3.8. IM– verification tools transformation

3.8.1.1 nuXmv models

NuSMV is a symbolic model checker developed by FBK-IRST, Carnegie Mellon University, University of Genova and University of Trento. In 2014, a new version of this verification tool called nuXmv has been released.

The input language of nuXmv describes the input model as a Finite State Machine (FSM) that range from completely synchronous to completely asynchronous. It uses BDD-based and SAT-based techniques as model checking techniques. It provides some heuristics to handle the state explosion problem and for the analysis of specification it supports CTL and LTL formalisms.

The definition of a model consists of variable declarations and the transition rules between states. It provides the following set of finite data types: boolean, scalars and fixed arrays. Static data types can also be constructed. There are two possible definition syntaxes for the transition rules: with the TRANS keyword, (from_state; to_state) pairs can be declared, with the ASSIGN keyword, the next states of each variable can be declared. If no next state is defined for a variable, then it will non-deterministically get a value from its range.

Consider a small example of a FMS with two states: ready and busy. When the FSM is in ready and there is a request, it will move to busy. If there is not request, it stays in ready. If the FSM is in the state busy, it can move to ready or stay in busy non-deterministically.

Fig. 3.34 shows the graphical representation of the FSM and Listing 3.6 shows the corresponding nuXmv code. In NuSMV, The FSM is represented by a MODULE. two variables are defined: request and state. request is a boolean variable and state can have to values: ready and busy. In the ASSIGN section, the value in the state is set. As the next value of the request variable is not defined, it will have a non-deterministic value for each state.

4http://nusmv.fbk.eu/
Figure 3.34: Graphical representation as a FSM

Listing 3.6: NuSMV code example

All the details about the modeling language of nuXmv can be found in Cavada et al. (2011). Note that there exists small differences between the NuSMV and nuXmv input language, for example two new data types are introduced: real and integer. However, our models remains the same for both model checkers.

3.8.1.2 Rules

These are the most relevant IM–nuXmv transformation rules, implemented in the methodology:

Rule nuXmv1 For the automata network \( N \), a new module main is created. This will contain all the automaton instances. It contains also a variable interaction, whose domain is the set of possible synchronizations in the automata network \( I = \{i_1, i_2, \ldots \} \) and the value NONE. This variable and the main module are passed as parameters to every module instance to be able to access them. The corresponding nuXmv code fragment can be seen on Listing 3.7

Listing 3.7: Representation of automata network \( a \) in nuXmv
3.8. IM– verification tools transformation

Rule nuXmv2 For every automaton $a$, a new module $a$ is created in the nuXmv model with one single instance $inst_a$. This module will contain a variable $loc$ which stores the current location of the automaton. The domain of this variable is the set of possible locations in automaton $a$ (i.e., $L = \{l_0, l_1, \ldots \}$). The default value of the variable $loc$ will be the initial location $l_0$. The corresponding nuXmv code fragment can be seen on Listing 3.8.

```plaintext
MODULE a(main, interaction)
VAR
   loc : {l0, l1, l2, ...};
...
ASSIGN
   init(loc) := l0;
...
MODULE main
VAR
   inst_a : a(self, interaction);
```

Listing 3.8: Representation of automaton $a$ in nuXmv

Rule nuXmv3 For every variable $v$ in automaton $a$, a new variable $v$ is created in the nuXmv model $a$. Each variable will have a next-value assignment statement in the assignment block of the module (See Listing 3.9). If a variable is not modified by an assignment explicitly, it will keep its value.

```plaintext
next(v) := case
   ...
   TRUE : v;
esac;
```

Listing 3.9: Next-value assignment statement

Rule nuXmv4 For every transition $t = (l_1, g, amt, i, l_2)$ in automaton $a$, a new assignment rule is added for the corresponding $loc$ variable. It will express that if the current location is $l_1$, the next location will be $l_2$, if guard $g$ is true and interaction $i$ is enabled. If there is no interaction or guard connected to transition $t$, the corresponding condition can be omitted. This transformation can be seen on Fig. 3.35 and Listing 3.10.
If the transition $t$ contains variable assignment $v := \text{Expr}$ for variable $v$, the next-value assignment corresponding to $v$ is extended too, as it can be seen on Fig. 3.36 and Listing 3.11.

**Rule nuXmv5** For each synchronization $i_1$ connecting transition $t_1$ which goes from location $l_1$ to $l_2$ in automaton $a$, and transition $t_2$ which goes from location $l_1$ to $l_2$ in automaton $b$, an invariant is added to the model, as it can be seen on Fig. 3.37 and Listing 3.12.

Listing 3.10: Corresponding nuXmv code

```plaintext
next(loc) := case
  ... 
  loc = l1 & g & interaction = i1 : l2;
  ... 
esac;
```

Listing 3.11: Corresponding nuXmv code

```plaintext
next(v) := case
  ... 
  loc = l1 & g & interaction = i1 :
    Expr;
  ...
  TRUE : v;
esac;
```

Listing 3.12: Corresponding nuXmv code

```plaintext
INVAR (interaction = i1 <->
  (inst_a.loc = l1 &
   inst_b.loc = l1 & g1 &
   g2));
```

Listing 3.13 shows an example of a small ST code, the corresponding IM is shown in Fig. 3.38 and the nuXmv code in Listing 3.14.
3.8. IM– verification tools transformation

ST code contains a single function block which implements a counter without any function calls. The corresponding IM has a single automaton with no interactions. The nuXmv model generated from IM contains two modules: the module *main* for the network, and the module *counter* for the single automaton.

```
FUNCTION_BLOCK counter
  VAR_INPUT
    enabled : BOOL;
    reset : BOOL;
  END_VAR
  VAR_OUTPUT
    cntr : INT := 0;
  END_VAR
  BEGIN
    IF enabled THEN
      cntr := cntr+1;
    END_IF;
    IF reset THEN
      cntr := 0;
    END_IF;
  END_FUNCTION_BLOCK
```

Listing 3.13: PLC ST code

```
MODULE COUNTER(interaction, main)
VAR
  loc : {10, end, 11, 12, 13, 14};
  ENABLED : boolean;
  RESET : boolean;
  CNTR : signed word[16];
ASSIGN
  init(loc) := 10;
  next(loc) := case
    loc = end : 10;
    loc = 10 : 11;
    loc = 11 & (ENABLED) : 12;
    loc = 11 & (!(ENABLED)) : 13;
    loc = 12 : 13;
    loc = 13 & (RESET) : 14;
    loc = 13 & (!(RESET)) : end;
    loc = 14 : end;
    TRUE: loc;
    esac;
next(ENABLED) := case
  loc = 10 : {TRUE, FALSE};
  TRUE : ENABLED;
  esac;
next(RESET) := case
  loc = 10 : {TRUE, FALSE};
  TRUE : RESET;
  esac;
init(CNTR) := 0sd16_0;
```

Figure 3.38: Corresponding IM
Another example of nuXmv Code, which is generated automatically from PLC code that contains two blocks is shown in Listing 3.15. The original PLC code contains the main program (OB1) and an instance of FB.

Listing 3.14: nuXmv code

```plaintext
MODULE main
VAR
interaction : {NONE};
inst_counter : COUNTER(interaction, self);

MODULE module_MAINBLOCK(interaction, main)
VAR
loc : {l0, end, 11, 12, 13, 14, 12_ret};
A1 : boolean;
A2 : boolean;
A3 : boolean;
ASSIGN
init(loc) := l0;
next(loc) := case
  loc = end : l0;
  loc = 10 : 11;
  loc = 11 & (A2) : 12;
  loc = 11 & (!A2) : 13;
  loc = 12 & ((interaction = interactionFB_B1)) : 12_ret;
  loc = 12_ret & ((interaction = interactionFB_B_ret2)) : 13;
  loc = 13 : 14;
  loc = 14 : end;
  TRUE: loc;
esac;
next(A1) := case
  loc = l0 : {TRUE, FALSE};
  TRUE : A1;
esac;
init(A2) := FALSE;
next(A2) := case
  loc = 13 : !(A2);
  TRUE : A2;
esac;
init(A3) := FALSE;
next(A3) := case
  loc = 14 : DB1.B2;
  TRUE : A3;
esac;

MODULE module_DB1(interaction, main)
VAR
loc : {10, end, 11};
B1 : boolean;
B2 : boolean;
```

Listing 3.15: PLC code
3.8. IM– verification tools transformation

### 3.8.2 IM–UPPAAL transformation

The following paragraphs contain a brief introduction of the UPPAAL modeling language and the transformation rules to produce UPPAAL code from the IM.

#### 3.8.2.1 UPPAAL models

UPPAAL is a toolbox for verification of real-time systems developed by Uppsala University and Aalborg University. It provides an integrated
tool environment for modeling, validation and verification of real-time systems modeled as networks of timed automata, extended with data types.

The input language of UPPAAL is based on the theory of timed automata, including extra features like bounded integer variables and urgency. The internal representation of the models is based on CDDs (Clock Difference Diagrams). For the property specification it supports the TCTL (timed computation tree logic) formalism.

A timed automaton is a FSM extended with clock variables. All the clocks progress synchronously. In UPPAAL, a system is modeled as a network of several such timed automata in parallel.

Consider a similar small example, as the one presented for nuXmv, consisting in a FMS with two states: ready and busy. When the FSM is in ready and there is a request, it will move to busy. If there is not request, it stays in ready. If the FSM is in the state busy, it will remain there for five units of time (representing seconds) and then it will move to ready.

Fig. 3.39 shows the graphical representation of the FSM and the Listing 3.16 its representation in UPPAAL. In UPPAAL, the FSM is represented by a template inside the network of automata (nta). In the declaration section, two elements are defined: a Boolean variable request and a clock $x$.

![Figure 3.39: Screenshot of the UPPAAL model](image-url)
3.8. IM– verification tools transformation

Listing 3.16: UPPAAL code example

All details about UPPAAL can be found in Amnell et al. (2001) and Behrmann et al. (2004).

3.8.2.2 Rules

These are the most relevant IM– UPPAAL transformation rules, implemented in the methodology:

**Rule UPPAAL1** For the *automata network N*, a new network of timed automata (*nta*) is created. This *nta* is composed of the following sections: the *template* section, which contains the automaton definitions; the *declaration* section, which contains all the variables of the model (accessible from any part of the model) and the channels (*chan*) for the synchronizations; finally the section *system*, which contains the instances of all the templates. An example of an UPPAAL code fragment can be seen on Listing 3.17.
Rule UPPAAL2 For every automaton $a$, a template $a$ is created in the UPPAAL model with one single instance $\text{inst}_a$ in the system section. For each location in automaton $a$ (i.e., $L = \{l_0, l_1, \ldots \}$), a location element is created in this template. The default location will be the initial location $l_0$. An example of an UPPAAL code fragment can be seen on Listing 3.18.

Listing 3.18: Representation of automaton $a$ in UPPAAL
3.8. IM– verification tools transformation

**Rule UPPAAL3** For every variable $v$ in automaton $a$, a new variable $v$ is created in the UPPAAL model in the *declaration* section as this variable can be accessed globally at the IM model. An example of an UPPAAL code fragment can be seen on Listing 3.19.

```
<declaration>
  bool v;
</declaration>
```

Listing 3.19: Variables of automaton $a$ in UPPAAL

**Rule UPPAAL4** For every transition $t = (l_1, g, amt, i, l_2)$ in automaton $a$, a new transition element is added to the corresponding *template*. This transition is composed of the following elements: *source*, representing the initial location of the transition; *target*, representing the final location of the transition; *label kind=“guard”*, representing the guard $g$ if exists; *label kind=“assignment”*, representing the assignment $amt$ if exists; *label kind=“synchronization”*, representing the synchronization $i$ if exists. Fig. 3.40 shows a basic transition in IM, and Listing 3.20 shows its representation in UPPAAL. The variable assignment is shown in Fig. 3.41 and the corresponding UPPAAL code in Listing 3.21.

```
<transition>
  <source ref="l1"/>
  <target ref="l2"/>
  <label kind="guard">g</label>
  <label kind="synchronization">i1</label>
</transition>
```

Figure 3.40: Automaton fragment for a transition

Listing 3.20: Corresponding UPPAAL code
Rule UPPAAL5 For each synchronization $i_1$ connecting transition $t_1$ which goes from location $l_1$ to $l_2$ in automaton $a$ and transition $t_2$ which goes from location $l_1$ to $l_2$ in automaton $b$, a label kind="synchronization" is added. The symbol ! and ? indicate which transition is the caller transition and which is the callee respectively. The corresponding IM is shown on Fig. 3.42 and the UPPAAL code in Listing 3.42.

Figure 3.41: Automaton fragment for a variable assignment

Listing 3.21: Corresponding UPPAAL code

```xml
<transition>
    <source ref="l1"/>
    <target ref="l2"/>
    <label kind="guard">g</label>
    <label kind="synchronization">i1!</label>
    <label kind="assignment">v:=Expr</label>
</transition>
```
Listing 3.22: Corresponding UPPAAL code

Listing 3.23 shows an example of a small ST code and Fig. 3.43 its corresponding IM. The corresponding UPPAAL code is shown in Listing 3.24. The ST code contains a single function block that implements a counter without any function calls. The corresponding IM have a single automaton with no interactions. The UPPAAL model generated from IM contains two modules: the module main for the network, and the module counter for the single automaton.
FUNCTION_BLOCK counter
VAR_INPUT
  enabled : BOOL;
  reset : BOOL;
END_VAR
VAR_OUTPUT
  cntr : INT := 0;
END_VAR
BEGIN
  IF enabled THEN
    cntr := cntr+1;
  END_IF;
  IF reset THEN
    cntr := 0;
  END_IF;
END_FUNCTION_BLOCK

Listing 3.23: PLC ST code
### Listing 3.24: Corresponding UPPAAL model

Another example of UPPAAL code, generated automatically from PLC code with two blocks is shown in Listing 3.25. The original PLC code contains the main program (OB1) and an instance of FB.
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE nta PUBLIC '-//Uppaal Team //DTD Flat System 1.1//EN' 'http://www.it.uu.se/research/group/darts/uppaal/flat-1_1.dtd'>
<nta>
<declaration>
chan interactionFB_B1;
chan interactionFB_B_ret2;
// Global variables
// Local variables
// For automaton mainBlock
bool mainBlock_A1;
bool mainBlock_A2 = FALSE;
bool mainBlock_A3 = FALSE;
// For automaton DB1
bool DB1_B1 = FALSE;
bool DB1_B2 = FALSE;
</declaration>
<template>
<name>TEMPLATE_mainBlock</name>
<location id="MAINBLOCK_init"><name>initial</name></location>
<location id="MAINBLOCK_end"><name>end</name></location>
<location id="MAINBLOCK_l1"><name>l1</name></location>
<location id="MAINBLOCK_l2"><name>l2</name></location>
<location id="MAINBLOCK_l3"><name>l3</name></location>
<location id="MAINBLOCK_l4"><name>l4</name></location>
<location id="MAINBLOCK_l2_ret"><name>l2_ret</name></location>
<init ref="MAINBLOCK_init" />
<transition>
<source ref="MAINBLOCK_end"/>
<label kind="assignment">
mainBlock_A1 = random_1
</label>
</transition>
<transition>
<source ref="MAINBLOCK_l1"/>
<label kind="guard">mainBlock_A2</label>
</transition>
<transition>
<source ref="MAINBLOCK_l1"/>
<label kind="guard">!(mainBlock_A2)</label>
</transition>
<transition>
<source ref="MAINBLOCK_l2"/>
<label kind="assignment">
DB1_B1 = !(mainBlock_A2)
</label>
</transition>
</template>

Listing 3.25: Synchronization of two automaton in UPPAAL
3.8.3 IM–BIP transformation

The following paragraphs contain a brief introduction of the BIP modeling language and the transformation rules to produce BIP code from the IM.

3.8.3.1 BIP models

BIP is a component-based framework for rigorous system design aiming at correctness-by-construction for essential properties of the designed system. To this end, the implementation of the system is obtained by automatic code generation preceded, where necessary, by a series of transformations from a high-level model formally analyzed to validate the required properties.

A BIP model consists of the following three layers:

1. The *Behavior* of the atomic components, modeled by LTS (Labeled Transition Systems) extended with data. Each transition is labeled by a port name. Furthermore transitions can be guarded by boolean conditions and trigger updates of the local data.

2. The *Interaction model* is a set of interactions, i.e. sets of ports, which defines allowed synchronizations between ports of different atomic components.

3. The *Priority model* is a strict partial order on interactions, which allows to restrict non-determinism when multiple allowed interactions are possible simultaneously.

Figure 3.44 shows a system composed of two atomic components and a binary connector, which imposes a strong synchronization between their respective transitions *begin* and *work*. Thus, the left component can only “begin work” when the right component is in the *On* mode. The three transitions *end*, *on* and *off* can only happen individually, i.e. without any synchronization. Furthermore, the priority *on* < *end* imposes that, when both transitions are possible (in the state *(Work, Off)*) the transition *end* will be chosen (if the system has received an instruction to switch off while working, the *on* instructions
should be suppressed until the current job is done). Detailed presentation of the BIP model and semantics can be found in Bludze and Sifakis (2007).

### 3.8.3.2 Rules

Before starting with the definition of the transformation rules from IM to BIP, it is necessary to mention an important difference. BIP language does not support global variables. Therefore this requires a modeling strategy for the situation when one automaton is accessing (reading or writing) variables from a different automaton or global variables at the IM level. These are the most relevant IM– BIP transformation rules, implemented in the methodology:

**Rule BIP1** For the *automata network* $N$, a new package $PLCProgram$ is created. This will contain all the automaton definitions (atomic component or *atom*). The package contains the definition of the needed *ports* and *connectors*. Table 3.1 shows the data type mapping between the IM and BIP. This mapping imposes the definition of the required ports and connectors. The following port types are created: (1) the *voidPort* port type is used by the connector for the synchronization between *atoms* and for triggering the transitions of the automaton. Basically *voidPort* is used for every transition that does not contain any assignment *amt* with variables from a different automaton or global variables (data transfer); (2) the *intDataPort* and *charDataPort* ports are used when an assignment in the automaton $a$ contains variables from a different automaton or global variable (see rules BIP3 and BIP6), according with the corresponding data type (see Table 3.1).

The following connector types are created: (1) the *SynchroAtoms*
connector is used for the synchronization between atoms and it uses the *voidPort*; (2) the *Singleton* connector is used for triggering single transitions with no synchronization and it also uses the *voidPort*; (3) the *IntDataTransferAtoms* and the *CharDataTransferAtoms* are used when an assignment in the automaton \( a \) contains variables from a different automaton or global variable (see rules BIP3 and BIP6), according with the corresponding data type (see Table 3.1). They use the *intDataPort* and *charDataPort* port types.

As global variables are not supported in BIP but they are at the IM, two special atoms called *intGlobalVariable* and *charGlobalVariable* are created. They contain one single place \( INIT \) and two ports: \( p1 \) for reading the value of the variable and \( p2 \) for writing this value. In addition a *compound* will be created containing all the atom and connector instances. The corresponding BIP code fragment can be seen on Fig. 3.26.

```plaintext
package PLCProgram

port type voidPort()
port type intDataPort(int data)
port type charDataPort(char data)

atom type intGlobalVariable()
data int Value
export port intDataPort p1(Value)
export port intDataPort p2(Value)
place 10
initial to 10
on p1 from 10 to 10 do{}
on p2 from 10 to 10 do{}
end

atom type charGlobalVariable()
data int Value
export port charDataPort p1(Value)
export port charDataPort p2(Value)
place 10
initial to 10
on p1 from 10 to 10 do{}
on p2 from 10 to 10 do{}
end

connector type SynchroAtoms(voidPort a, voidPort b)
define a b
```
The code snippet and the explanation are as follows:

```plaintext
3.8. IM– verification tools transformation

Listing 3.26: Representation of automata network in BIP

Rule BIP2 For every automaton $a$, a new atom $a$ is created in the BIP model with one single instance or component inst$a$. The number of places is the set of possible locations in the automaton $a$ (i.e., $L = \{l_0, l_1, \ldots\}$). However if a transition $t$ in the automaton contains a variable assignment $amt$ that contains variables from a different automaton, extra places, ports and connectors have to be created (See rule BIP6). The default place will be the initial location $l_0$. An example of the the corresponding BIP code fragment can be seen on Listing 3.27.

Listing 3.27: Corresponding BIP code fragment

```
Chapter 3. Approach

```c
export port VoidPort p3()
export port intDataPort t1(B1)
export port intDataPort t2(B2)

/* STATES */
place 10, 11, 12, 13, 14

/* INITIAL STATE*/
initial to 10 do {
    /* VARIABLE INITIALIZATIONS */
    B1 = 0;    // Default value
    B2 = 0;    // Default value
}

/* TRANSITIONS */
on p2 from 10 to 11
on t1 from 11 to 12
on p3 from 12 to 13 do {B2 = !((B1 == 1));}
on t2 from 13 to 14
on p1 from 14 to 10
end

component a inst_a(param1)
```

Listing 3.27: Representation of automaton a in BIP

**Rule BIP3** For every variable $v$ in an automaton $a$, a local variable $v$ is created in the BIP atom $a$. If a variable $v_1$ is used in the automaton $a$ but it belongs to another automaton, an extra variable $v_1$ is created in the atom $a$. In addition, for every variable $v_1$ from an automaton $a$ that is accessed (read or written) by any other automaton (global variable), a new instance of the atom `intGlobalVariable` or `charGlobalVariable` is created, depending on the data type of $v$ (the mapping between PLC data types and BIP data types was shown in Table 3.1). For every input variable, a random value will be assigned to the variable. This can be done using C language as BIP framework supports it. If the BIP language is used for this purpose, abstractions and restrictions on the assignments have to be applied as currently BIP does not support random values. A example is shown in Listing 3.28. In the atom $a$ the variables $B1$ and $B2$ are coming from a different atom. In addition, $B1Var$ and $B2Var$ (instances of `intGlobalVariable`) are created representing global variables, and the variable
$A1$ represents an input variable in the atom $a$, therefore it is initialized to random at the beginning of the PLC cycle.

```plaintext
... 

/* DEFINITION OF THE AUTOMATON */
atom type a()

/* Input VARIABLES */
data int A1

/* VARIABLES From different atom*/
data int B2

/* PORTS */
export port VoidPort p1()
export port VoidPort p2()
export port VoidPort p3()
export port intDataPort t1(B1)
export port intDataPort t2(B2)

/* STATES */
place 10, 11, 12, 13, 14

/* INITIAL STATE*/
initial to 10

/* TRANSITIONS */
on p1 from 10 to 11 do {
   A1 = (rand() % 2);
}
on t1 from 11 to 12

on p3 from 12 to 13 do {
   B2 = !A1 & B1;
}
on t2 from 13 to 14
```

Rule BIP4 For every transition $t = (l_1, g, amt, i, l_2)$ in automaton $a$, a new voidPort port and a transition labeled by a port name is added to the atom $a$. It will express that if the current location is $l_1$, the next location will be $l_2$, if guard $g$ is true and synchronization $i1$ is enabled. If there is no synchronization or guard connected to transition $t$, the corresponding condition can be omitted. If $t$ does not contain a synchronization $i1$ a Singleton connector instance is created. If $t$ contains a synchronization $i1$ a SynchroAtoms connector instance is created. If the transition $t$ contains a variable assignment $amt$ containing variables from a different automaton, extra transitions have to be created (See rule BIP6). Fig. 3.45 shows a basic transition in IM and the corresponding BIP code in Listing 3.29. The variable assignment is shown in Fig. 3.46 and the corresponding BIP code on Listing 3.30.

```
  on t2 from 14 to 10
  end
...
component intGlobalVariable B1Var()
component intGlobalVariable B2Var()
```

Listing 3.28: Representation of automaton $a$ in BIP

```
  export port VoidPort p1()
...
  on p1
    from 11 to 12 provided (g == 1)
  ...
  connector VoidPortConnector i1(a.p1, b.p1)
```

Listing 3.29: Corresponding BIP code
3.8. IM– verification tools transformation

Rule BIP5 For each synchronization $i_1$ connecting a transition $t_1$ which goes from location $l_1$ to $l_2$ in automaton $a$ and a transition $t_2$ which goes from location $l_1$ to $l_2$ in automaton $b$, a $SynchroAtoms$ connector instance has to be created. The corresponding IM is shown Fig. 3.47 and the corresponding BIP code fragment can be seen on Fig. 3.31.

Rule BIP6 For each $amt$ in $t$ that contains variables from different automaton, extra places, transition and ports are created. For each $Boolean$ or $Unsigned Char$ variable from different automaton or global variable from an $amt$ in a transition $t$, an instance of $charDataPort$ port type is created. For the rest of variables from a different automaton or global variable from an $amt$ in a transition $t$, an instance of $intDataPort$ port type is created. If a $Boolean$ or $Unsigned Char$ variable from a different automaton or global variable is read a transition labeled by a $charDataPort$ and an extra place are created just before of the assignment. If a $Boolean$ or $Unsigned Char$ variable from a
different automaton or global variable is written, a transition labeled
by a `charDataPort` and an extra place are created just after the
assignment. If a non `Boolean` or `Unsigned Char` variable from a different
automaton or global variable is read, a transition labeled by a `intData-
Port` and an extra place are created just before the assignment. If
a non `Boolean` or `Unsigned Char` variable from a different automaton
or global variable is written, a transition labeled by a `intDataPort`
and an extra place are created just after the assignment. An example
of a BIP code fragment containing variable assignments is shown on
Listing 3.34.

Listing 3.32 shows an example of a small ST code and Fig. 3.32 its
(corresponding IM. The corresponding BIP code is shown in 3.33. The
ST code contains a single function block implementing a counter with-
out any function calls. The corresponding IM has a single automaton
with no interactions. The BIP model generated from IM contains two
modules: the module `main` for the network and the module `counter`
for the single automaton.

```cpp
#include "stdio.h"
package PLCProgram
/* PORT TYPE DEFINITION */
port type VoidPort()
atom type counter()
/* VARIABLES */
data int enabled
data int reset
data int cntr
```

<table>
<thead>
<tr>
<th>FUNCTION_BLOCK counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>VAR_INPUT</td>
</tr>
<tr>
<td>enabled : BOOL;</td>
</tr>
<tr>
<td>reset : BOOL;</td>
</tr>
<tr>
<td>END_VAR</td>
</tr>
<tr>
<td>VAR_OUTPUT</td>
</tr>
<tr>
<td>cntr : INT := 0;</td>
</tr>
<tr>
<td>END_VAR</td>
</tr>
<tr>
<td>BEGIN</td>
</tr>
<tr>
<td>IF enabled THEN</td>
</tr>
<tr>
<td>cntr := cntr+1;</td>
</tr>
<tr>
<td>END_IF;</td>
</tr>
<tr>
<td>IF reset THEN</td>
</tr>
<tr>
<td>cntr := 0;</td>
</tr>
<tr>
<td>END_IF;</td>
</tr>
<tr>
<td>END_FUNCTION_BLOCK</td>
</tr>
</tbody>
</table>

Listing 3.32: PLC ST code

Figure 3.48: Corresponding IM
Another example of BIP Code, generated automatically from PLC code with two blocks is shown in Listing 3.34. The original PLC code contains the main program (OB1) and an instance of FB.
package PLCProgram

/* PORT TYPE DEFINITION */
port type VoidPort()
port type intDataPort(int data)

atom type intGlobalVariable()
data int Value
export port intDataPort r(Value)
export port intDataPort w(Value)
place l0
initial to l0
on r from l0 to l0 do{}
on w from l0 to l0 do{}
end

/* AUTOMATA*/
/* DEFINITION OF THE AUTOMATON */
atom type MAINBLOCK_MAINBLOCK()

/* VARIABLES */
data int A1
data int A2
data int A3

/* VARIABLES From different atom*/
data int B1
data int B2

/* PORTS */
export port VoidPort p1()
export port VoidPort p2()
export port VoidPort p3()
export port VoidPort p4()
export port VoidPort p5()
export port VoidPort p6()
export port VoidPort p7()
export port VoidPort p8()
export port intDataPort t1(B1)
export port intDataPort t2(B2)

/* STATES */
place INITIAL, END, 11, 12, 13, 14, 15, 16, 17

/* INITIAL STATE*/
initial to INITIAL do {
/* VARIABLE INITIALIZATIONS */
A2 = 0; // Default value
A3 = 0; // Default value
}

/* TRANSITIONS */
on p1 from INITIAL to 11 do {
    A1 = (rand() % 2);
}
on p2 from 11 to 12 provided (A2 == 1)

on p3 from 11 to 15 provided (!(A2 == 1))

on p4 from 12 to 13 do {
  B1 = !((A2 == 1));}

on t1 from 13 to 14

on p5 from 14 to 15

on p6 from 15 to 16 do {
  A2 = !A2;}

on t2 from 16 to 17

on p7 from 16 to END do {
  A3 = B2;}

on p8 from END to INITIAL

end

/* DEFINITION OF THE AUTOMATON */
atom type DB1_FB1()

/* VARIABLES */
data int B1
data int B2

/* PORTS */
export port VoidPort p9()
export port VoidPort p10()
export port VoidPort p11()
export port intDataPort t3(B1)
export port intDataPort t4(B2)

/* STATES */
place INITIAL, END, l1, l2, l3

/* INITIAL STATE*/
initial to INITIAL do {
/* VARIABLE INITIALIZATIONS */
  B1 = 0; // Default value
  B2 = 0; // Default value
}

/* TRANSITIONS */
on p10 from INITIAL to l1

on t3 from l1 to 12

on p11 from l2 to l1 do {
  B2 = !((B1 == 1));}

on t4 from l1 to END
Listing 3.34: BIP example

3.9 Modeling timing aspects of PLCs

This section presents how the timing aspects of PLCs are integrated in the proposed methodology. The modeling strategy for timers and time in PLCs has been published in [Fernández Adiego et al., 2014a].
Timing operations are widely used in PLC control systems. This section is focused on the modeling strategy for the three most commonly used timers in PLC programs: TON, TOFF, and TP timers.

A subset of the PLC timers were presented in detail in Section 2.2.4. Fig. 3.49 summarizes their behaviors to help understanding the proposed modeling strategies.

In this methodology, a PLC timer is represented by a separated automaton synchronized with the main program. Moreover, modeling PLC timers also implies to model the `TIME` data type. However, as it was mentioned previously, timed models usually contain a huge state space, which cannot be handled by model checkers. Based on this observation, two different approaches are proposed for the methodology:

1. The first is a realistic timer representation, which is close to the reality, enabling precise modeling and verification.

2. The second approach proposes an abstract time representation, which is less accurate, but drastically reduces the state space of the model.

Both approaches are described hereafter focusing on the time and timer representation (for TON, TOFF, and TP timers) and the property specification. In addition, the proof that the abstract approach simulates the realistic one is presented, thus guaranteeing that any property verified on the abstract approach also holds in the realistic one, even if it is much simpler.

### 3.9.1 Realistic approach

This first approach presents a realistic model of the PLC timers and the time handling. This approach allows to specify properties with explicit time in it. Having this realistic representation of the timer implies that `time` needs also to be modeled realistically.

#### 3.9.1.1 Time representation

Three main characteristics are considered to model time for this approach:
Figure 3.49: Timer diagrams
1. **Time is modeled as a finite variable**: it represents with high fidelity the *TIME* data type in a PLC. However, instead of having a signed 32-bits integer variable (like in Siemens PLCs), a 16-bits variable is used to represent this data type. This range reduction is possible as the behavior of a PLC is cyclic and the cycle time, the delays of the timers, and the delays in the requirements are much smaller than the range of this 16 bit variable. The accuracy of this variable is 1 ms, as it is in real PLCs. Because of this time representation, overflow of time has to be considered when the timer is modeled, and also when the requirement to be checked is expressed (e.g. the current time can be smaller for a later event, see Fig. 3.50).

2. **Time is incremented by adding the cycle time**: In this representation, time is not incremented by individual units of time. It is instead incremented by the duration of the last PLC cycle at the end of it. This assumption obviously simplifies the global model and there is not any loss of accuracy when comparing with the real implementation in a PLC, considering that the timers are called at most once in each PLC cycle, which holds for our real cases.

3. **Cycle time is chosen non-deterministically**: in order to represent standard PLC with a varying cycle time, a random value is generated at the end of each cycle to represent this. The selected random values are between 5 ms and 100 ms, which is a valid assumption based on the PLC systems at CERN.

### 3.9.1.2 TON timer representation

Given this finite time representation, the behavior of the TON timer is represented in ST code as it is shown in Listing 3.35. In this code, the input variables are *IN* and *PT*, and the output variables are *Q* and *ET*. The variable *ctime* represents the current time and it is modeled as previously explained. In addition, two variables are added: *running* and *start*, where *running* is a Boolean variable representing when the timer is working after a rising edge on *IN* and *start* contains the value of *ctime* when *IN* has a rising edge.
Figure 3.50: Consequences of finite time representation

Listing 3.35: ST code of TON

```plaintext
FUNCTION_BLOCK TON
VAR_INPUT
  PT : TIME;
  IN : BOOL;
END_VAR
VAR_OUTPUT
  Q : BOOL := FALSE;
  ET : TIME;  // elapsed time
END_VAR
VAR
  running : BOOL;
  start : TIME;
END_VAR
BEGIN
  IF IN = FALSE THEN
    Q := FALSE;
    ET := 0;
    running := FALSE;  // t1
  ELSEIF running = FALSE THEN
    start := CTIME;
    running := TRUE;   // t2
  ELSIF CTIME - (start + PT) >= 0 THEN
    Q := TRUE;
    ET := PT;          // t3
  ELSE
    IF NOT Q THEN
      ET := CTIME - start;
      END_IF;           // t4
  END_IF;
END_FUNCTION_BLOCK
```
3.9. Modeling timing aspects of PLCs

By applying the extended methodology, the corresponding automaton of the TON ST code was produced. The equivalent state machine is shown in Fig. 3.51 (Note that the assignments of ET are omitted from the state machine to simplify the figure.) This state machine contains three states corresponding to the three original states of the TON: NR (not running; running=false, Q=false), R (running; running=true, Q=false) and TO (timeout; running=true, Q=true). The transitions in the state machine (labeled as $t_1, t_2, t_3, t_4$) correspond to the conditional statements in the ST code.

\[
\begin{align*}
\mathcal{P} &\equiv (CTIME - (start + PT) \geq 0) \\
\end{align*}
\]

Figure 3.51: State machine of the realistic TON representation

At most one transition can happen in this state machine for every call of the timer. Therefore, the timer cannot go from state NR to state TO with one function call, which is valid if we assume that delays are always greater than zero ($PT > 0$). According to the specification of the Siemens TON implementation (Siemens (1998b)), the parameter $PT$ should be positive.

The potential state space (PSS) size of this timer representation is $3.38 \cdot 10^{16}$ and its reachable state space (RSS) is $5.91 \cdot 10^{15}$ without counting the variable ctime (as it is a global variable used by all the timers).

3.9.1.3 TOFF timer representation

The same strategy is applied to the TOFF timer. The corresponding ST code is shown in Listing 3.35. The input and output variables are
the same than for the TON. In this case, \textit{running} is a Boolean variable representing when the timer is working after a falling edge on \textit{IN} and \textit{start} contains the value of \textit{ctime} when \textit{IN} has a falling edge.

\begin{lstlisting}[language=ST]
FUNCTION_BLOCK TOFF
  VAR_INPUT
  PT : TIME;
  IN : BOOL;
  END_VAR
  VAR_OUTPUT
  Q : BOOL := FALSE;
  ET : TIME; // elapsed time
  END_VAR
  VAR
  running : BOOL;
  start : TIME;
  END_VAR
  BEGIN
    IF IN = TRUE THEN
      Q := TRUE;
      ET := 0;
      running := FALSE; // t1
    ELSIF running = FALSE THEN
      start := CTIME;
      running := TRUE; // t2
    ELSIF CTIME - (start + PT) >= 0 THEN
      Q := FALSE;
      ET := PT; // t3
    ELSE
      IF Q THEN
        ET := CTIME - start;
      END_IF; // t4
    END_IF;
  END_FUNCTION_BLOCK
\end{lstlisting}

Listing 3.36: ST code of TOFF

As well as for the TON, by applying the extended methodology, the corresponding automaton of the TOFF ST code was produced and the equivalent state machine is shown in Fig. 3.52. This state machine contains the same states and transitions as the previous timer.

3.9.1.4 TP timer representation

The same strategy is applied to the TP timer. The corresponding ST code is shown in Listing 3.37. The input and output variables are the
3.9. Modeling timing aspects of PLCs

\[ P \equiv (\text{CTIME} - (\text{start} + \text{PT}) \geq 0) \]

Figure 3.52: State machine of the realistic TOFF representation

```
FUNCTION_BLOCK TP
VAR_INPUT
  PT : TIME;
  IN : BOOL;
END_VAR
VAR_OUTPUT
  Q : BOOL := FALSE;
  ET : TIME;
END_VAR
VAR
  running : BOOL;
  start : TIME;
END_VAR
BEGIN
  IF Q = FALSE AND running = FALSE THEN
    IF IN THEN
      start := CT;
      running := TRUE;
      Q := TRUE; // t1
    END_IF;
  ELSIF Q = TRUE AND running = TRUE THEN
    IF IN AND (CTIME - (start + PT) >= 0) THEN
      running := TRUE;
      Q := FALSE; // t2
    ELSIF NOT IN AND (CTIME - (start + PT) >= 0) THEN
```
running := FALSE;
Q := FALSE;       // t3
END_IF;
ELSIF Q = FALSE AND running = FALSE THEN
  IF NOT IN THEN
    running := FALSE;
    Q := FALSE;       // t4
  END_IF;
END_IF;
END_FUNCTION_BLOCK

Listing 3.37: ST code of TP

As well as for the previous timers, by applying the extended methodology, the corresponding automaton of the TP ST code was produced and the equivalent state machine is shown in Fig. 3.53. This state machine contains the same states and transitions as the previous timers.

\[ \neg in \land P \]

\[ in \land P \]

\[ \neg P \]

\[ [\neg in] \]

\[ [in] \]

\[ [\neg in \land P] \]

\[ [in \land P] \]

\[ [\neg in] \]

\[ t_1 \]

\[ t_2 \]

\[ t_3 \]

\[ t_4 \]

\[ NR \]

\[ R \]

\[ TO \]

\( P \equiv (CTIME - (start + PT) \geq 0) \)

Figure 3.53: State machine of the realistic TP representation

3.9.1.5 Property specification

Using the methodology and the developed tool, input models for nuXmv are automatically generated. The experimental results presented here are produced using this model checker. The goal is to verify properties with explicit time in them, like:
“if $C_1$ is true, after $t_m$ time $C_2$ will be true, if $C_1$ remained true.”

Where $C_1$ and $C_2$ are Boolean expressions, $C_1$ contains input variables and parameters and $C_2$ contains output variables.

CTL and LTL do not provide this expressiveness, for this reason a monitor or observer automata is added to the model. The goal of the monitor is to check $C_1$, and if it is true for at least $t_m$ time, the monitor output value $Mout$ is set to true.

By using such monitor, the requirement is simplified as:

“If $Mout$ is true, then $C_2$ should be true.”

This requirement can be formalized easily in CTL:

$$\text{AG}(Mout \rightarrow C_2)$$

An example for this monitor usage can be seen in Fig. 3.54. As the computed values are assigned to the real outputs of the PLC only at the end of the PLC cycle, the requirements should be checked only at this point. The general CTL expression extended with it is the following:

$$\text{AG}(EoC \land (Mout \rightarrow C_2))$$

Where $EoC$ is true, iff the execution is at the end of a PLC scan cycle.

The behavior of this monitor is similar to the TON timer, but it is independent of the rest of the program logic, therefore $Mout$ will be true after $t_m$ time, if $C_1$ is true and it can be used to verify if outn holds the property. Notice that it is not enough to save a “timestamp” $t_{C_1}$ when $C_1$ is true, and formalize the requirement as $\text{AG}((ctime \geq t_{C_1} + t_m) \rightarrow C_2)$, because the $ctime$ variable is a finite integer, thus it can overflow, as it is illustrated by Fig. 3.50.

This technique for specification can be used with any timer models. Chapter 4 will provide some experimental results regarding this modeling approach.

### 3.9.2 Abstract approach

The models created by applying the realistic approach have a big state space even if only one TON is modeled. If this approach is applied
Chapter 3. Approach

Figure 3.54: Verification configuration for OnOff model extended with monitor

to large models, probably verification would not be even possible. For that reason, a second approach is proposed, which is based on a data abstraction of the first approach.

3.9.2.1 Time representation

In this case, time is not represented explicitly in the model, the variable \( ctime \) representing the current time is not maintained. Therefore properties with explicit time cannot be validated.

3.9.2.2 TON timer representation

This timer representation approach consists in a non-deterministic model produced as an abstraction of the realistic approach. The corresponding state machine is presented in Figure 3.55.

Similarly to the realistic model, this model has three possible internal state: \( NR \) (not running), \( R \) (running) and \( TO \) (timed out). If the input \( IN \) is true, the TON will start to run (goes to state \( R \)). After that, the TON can stay in the state \( R \) or go to \( TO \) non-deterministically, which means, we do not know when the timer will stop. However, by adding a fairness constraint to the model, it is ensured that the timer cannot stay in state \( R \) for infinite time. Only one transition can be fired in one PLC cycle, i.e., the timer cannot go from
3.9. Modeling timing aspects of PLCs

state \( NR \) to state \( TO \) with one call. This corresponds to the previously introduced \( PT > 0 \) constraint. Figure 3.56 shows the timing diagram of the abstract approach compared with the realistic one. The size of the PSS and RSS for this model is 6 comprising the Boolean input variable, reducing significantly the size of the realistic approach but introducing some limitations of the property specification.

This representation can result false positives, meaning that verification tools can give spurious counterexample that cannot occur in reality. However false negatives can never occur, therefore if a property holds in the abstract model, it holds in the real system.

3.9.2.3 TOFF timer representation

Following the same strategy, the TOFF abstract model is represented in Fig. 3.57.

3.9.2.4 TP timer representation

Following the same strategy, the TP abstract model is represented in Fig. 3.58.
3.9.2.5 Property specification

Obviously, this abstract model implies certain limitations in the specification properties. Explicit delay times cannot be expressed in the requirement, but safety or liveness properties can be expressed, for example:

“if $a$ is sometime true and remains true forever, eventually $b$ will be true”.

Where $a$ and $b$ are variables affected by timers in the PLC program.

Chapter 4 will provide some experimental results using these models.

3.9.3 Refinement between the two approaches

We can verify that the realistic approach indeed refines the abstract approach. Using this proof, we are able to guarantee that requirements verified on the abstract model – where verification is easier – also hold on the realistic model – where automatic verification would be harder and more time consuming. However, the false result on the abstract model does not imply false result on the realistic model. Using more abstract models for verification purposes and lifting results to realistic models is a well known technique ([Clarke et al. (1999); Loiseaux et al. (1995)]) and we apply it to the PLC domain. Specifically to PLC timer...
models where we perform a proof in a similar fashion as the refinement proofs described in Blech and Grégoire (2011).

For example, for the TON model, the proof is done by first establishing a simulation relation $S$ between realistic (Fig. 3.51) and abstract automaton (Fig. 3.55) that relates the states of the different automata with each other such that only the following holds:

\[
S(NR_{\text{realistic}}, NR_{\text{abstract}}) \\
S(R_{\text{realistic}}, R_{\text{abstract}}) \\
S(TO_{\text{realistic}}, TO_{\text{abstract}})
\]

Furthermore, the simulation relation ensures that $Q$ has the same value in all states. In order to finish the proof, we show that:

- The initial states are in the simulation relation: $NR_{\text{realistic}}$ and $NR_{\text{abstract}}$ are in the simulation relation and the value of $Q$ is the same, false.

- Each pair of realistic and abstract model state transitions with a corresponding condition – regarding the value of $in$ – from possible states in the simulation relation $S$ lead to a pair of states for which $S$ holds again. Most cases are trivial except: the transition of the $[in]$-guarded transition in the abstract model in the $(TO_{\text{realistic}}, TO_{\text{abstract}})$ state pair has two corresponding
transitions in the realistic model since we do not regard the value of $P$ in the abstract model.

Due to the fairness constraint in the abstract model, its state cannot be $R_{abstract}$ for infinite time. However, this is also true for the corresponding $NR_{realistic}$ state of the realistic model if it is called sufficiently often\footnote{It is not defined in the standard or in the manual, but our implementation works properly, if the elapsed time between two calls is less than the maximal value of the TIME data type, which is about 30 s represented on 16 bits or 24 days represented on 32 bits. Usually, the timers are called in every PLC cycle, thus this is not a limitation. This is also needed for the timers to work properly.}, because the delay time $PT$ is finite.

Based on the definition of the simulation relation, safety properties making use of the atomic elements – like conditions on the used variables $Q$ and $in$ – that are preserved in $S$ are also preserved between abstract and realistic model. However, the abstract model can impose false positives, i.e. the given abstract counterexamples can never occur in the in the real system.

### 3.10 Process modeling

The previous sections were dedicated to describe the rules for building the formal models. However there is a missing part of the system, that was not considered: the controlled process. Process information
is important but building the process model is a very challenging and
time consuming task (as extracting the information from the process
is done manually). In addition, building a complete model of the
controlled process increases significantly the state space of models.

Other authors (e.g. Machado (2006), Machado et al. (2003a),
Machado et al. (2003b), Machado and Eurico (2013)) studied the use
of process information to verify PLC programs. Their results show
that some properties can only be verified using the process information
and if this information is not included, false positives are produced,
i.e. the verification tool will report a bug that can never occur in the
real system.

Considering the following PLC code 3.38. It shows an example
where the process information is necessary.

```
FUNCTION_BLOCK Valve
VAR_INPUT
  AuOnR: BOOL := FALSE;
  AuOffR: BOOL := FALSE;
  HFOn: BOOL := FALSE;
  HFOff: BOOL := FALSE;
END_VAR
VAR_OUTPUT
  Status : BOOL;
  Open: BOOL;
  Close: BOOL;
END_VAR
BEGIN
  IF AuOnR AND NOT AuOffR THEN
    Open := TRUE;
  END_IF;
  IF AuOffR AND NOT AuOnR THEN
    Close := TRUE;
  END_IF;
  IF Open AND HFOn AND NOT HFOff THEN
    Status := TRUE;
  ELSIF Close AND HFOff AND NOT HFON THEN
    Status := FALSE;
  END_IF;
END_FUNCTION_BLOCK
```

Listing 3.38: ST code example

This PLC program consists in a single FB representing the behavior
of a digital valve. It has 4 inputs and 3 outputs variables.
Chapter 3. Approach

- $AuOnR$ is an input variable that represents an order to open the valve.
- $AuOffR$ is a input variable that represents an order to close the valve.
- $HFOn$ is a input variable that represents the feedback from the valve, indicating that the valve is open.
- $HFOff$ is a input variable that represents the feedback from the valve, indicating that the valve is close.
- $Status$ is a output variable that represents the status of this digital valve (information sent to the SCADA).
- $Open$ is a output variable that represents the order to open the digital valve (information sent to the process).
- $Close$ is a output variable that represents the order to close the digital valve (information sent to the process).

In this case, the requirement is the following:

“If $Open$ is TRUE and $HFOn$ is TRUE, $Status$ will be true at the end of the PLC cycle.”

The corresponding CTL formula is:

$$\text{AG} \left( (EoC \land Open \land HFOn) \rightarrow Status \right)$$

In this trivial example is obvious that the verification result by using nuXmv is FALSE, due to $HFOff$. The relevant information extracted from the counterexample is presented in Table 3.5.

However, if the hardware of the valve is correct, the input variables $HFOn$ and $HFOff$ can never be equal to true at the same time, as it means that the valve is open and close at the same moment. This information can be added to the methodology as an invariant:

$$\text{INVAR: } \neg (HFOn \land HFOff)$$

After adding the invariant, model checking is applied again and the result of the verification is TRUE. It shows that without some information from the controlled process, some properties cannot be proved.
3.11 Verification and counterexample analysis

Table 3.5: Variables values from the counterexample at the end of the PLC cycle

<table>
<thead>
<tr>
<th>Variable</th>
<th>End of Cycle1</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuOffR</td>
<td>FALSE</td>
</tr>
<tr>
<td>AuOnR</td>
<td>TRUE</td>
</tr>
<tr>
<td>HFOff</td>
<td>TRUE</td>
</tr>
<tr>
<td>HFOn</td>
<td>TRUE</td>
</tr>
<tr>
<td>Close</td>
<td>FALSE</td>
</tr>
<tr>
<td>Open</td>
<td>TRUE</td>
</tr>
<tr>
<td>Status</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

that they are TRUE so false positives are produced (the model checker gives as a result a spurious counterexample for the property). However, it also implies that by adding wrong invariants, we can hide bugs in the PLC program and produce false negatives in the verification, which is much more dangerous.

In general in this methodology, the formal model of the controlled process is not included, due to the complexity of building these models and because it can potentially increment the state space of the models. However, invariants with the process information can be manually added to the methodology when needed.

3.11 Verification and counterexample analysis

Once the input models for the verification tools are automatically generated and reduced, formal verification can be applied and the analysis of the results can be performed. This step of the methodology has been published in Fernández Adiego et al. (2014c).
3.11.1 Counterexample analysis

The counterexample produced by the model checkers when a property is not satisfied, provides the relevant information to identify the source of the problem in the PLC program.

The model checker generates detailed counterexamples, containing the value of each variable after each transition in the model (corresponding to the execution of an instruction in the PLC code). However, these counterexamples are usually too long. In some of our experiments, the counterexample produced by nuXmv contains around 37 500 lines. This information is too detailed for human analysis. However, it can be automatically reduced, as it is enough to know the value of the input and output variables at the end of each PLC cycle, thus the variable valuations of the intermediate states can be removed. By removing the unnecessary states and the temporary variables, the counterexample for the same requirement can be reduced to approximately 100 lines. This information can be given to the PLC program developer for human analysis.

The counterexample can also be used to demonstrate the problem in a real environment. Using the nuXmv’s counterexample, a demonstrator PLC code can be easily generated by adding a module that simulates the variables from the counterexample and checks the expected result. By doing so, it can be proved that the counterexample is not caused by a mistake during the model generation or due to bad reductions.

Listing 3.39 shows an extract from the generated counterexample of a real PLC program and Listing 3.40 the corresponding part of the PLC demonstrator source code.

Furthermore, the PLC demonstrator can help us to reduce the counterexample. Usually, most of the input variables do not have any effect on the evaluated requirement. Those variables can be fixed to constant values thus helping to focus on the input value changes that causes the violation of the requirement.
In the current example, by using the counterexample and the reduced PLC demonstrator, we were able to identify the source of the problem. It turned out that from *Forced* mode the logic cannot switch to *Auto* mode. It can only be done by the operator. The corresponding part of the implementation can be seen in Fig. 3.41. The code shows the transition from *Forced* mode to *Auto* mode, which does not take into account the *AuAuMoR* input. This behavior is correct and intentional, in this case the source of the problem is not the PLC code, the specification contains a mistake.

```
IF (MMoSt_aux AND (E_MAuMoR OR E_AuAuMoR)) OR
  (FoMoSt_aux AND E_MAuMoR) OR
  (SoftLDSt_aux AND E_MAuMoR) OR
  (MMoSt_aux AND AuIhMMo) OR
  (FoMoSt_aux AND AuIhFoMo) OR
NOT (AuMoSt_aux OR MMoSt_aux OR
  FoMoSt_aux OR SoftLDSt_aux) THEN
  (* Setting mode to Auto *)
  AuMoSt_aux := TRUE;
  MMoSt_aux := FALSE;
  FoMoSt_aux := FALSE;
  SoftLDSt_aux := FALSE;
END_IF;
```

In the source code, the variables starting with “E_” indicate the rising edges of the corresponding inputs. AuMoSt_aux is true if the current mode is Auto. The meaning of variables MMoSt_aux, FoMoSt_aux, and SoftLDSt_aux are similar, for the other modes.
requirement

In the bottom part of Fig. 3.59, it can be observed that the PLC demonstrator generation is integrated in the methodology.

![Diagram](image)

**Figure 3.59:** Integration of the proposed methodology on the PLC program development process.

Many safety and liveness requirements have been verified using this methodology and the number of discrepancies between the specification and PLC program were significant even if testing was previously applied. In all these cases, three possible situations were identified as the source of the problem: a bug in the implementation, a mistake in the specification or an incomplete specification.
3.12 Methodology CASE tool

This methodology has been implemented in a CASE tool using EMF (Eclipse Modeling Framework described in Steinberg et al. (2009)) and Xtext technologies (Eysholdt and Behrens (2010)). The grammar of the PLC languages is implemented as a Xtext grammar. The IM is implemented as an EMF metamodel as it can be seen in Fig. 3.60. The transformation rules from the PLC languages to the IM, the reduction techniques and the transformation rules from IM to nuXmv, UPPAAL and BIP have been implemented using Xtend (Xtend website (2014)) and Java. The Xtext framework provides a parser, an over linker, an interpreter, an editor, and many other features to help the developer (Xtext website (2014)).

Figure 3.60: EMF implementation

The tool provides a graphical interface, where the user can create a verification project. The user has to provide the PLC code and the properties to verify, and the tool returns the verification result (TRUE
and FALSE) and a report with all the details of the counterexample analysis. Figures 3.61, 3.62, 3.63 and 3.64 show some screenshots of the tool.

Figure 3.61: CASE tool editor for the PLC code

Figure 3.62: CASE tool property description

3.13 Summary of the chapter

This chapter presented the contribution of this thesis: a general approach to apply formal verification to PLC programs. Each step of
3.13. Summary of the chapter

the methodology has been described in a separate section as well as the syntax and semantics of the IM. These methodology hides any complexity related to formal methods from control engineers. For that purpose, the methodology provides a solution for the following challenges:

1. Requirements specification.
2. PLC hardware modeling.
3. PLC code – formal models transformation.
4. Time and timers modeling.

5. Process modeling.

6. Counterexample analysis.

In addition, a brief discussion about the CASE tool that supports this methodology is presented.
Chapter 4

Case studies and measurements

4.1 Introduction

This chapter presents the experimental results of applying the proposed methodology to real-life PLC programs. The selected systems have been developed and deployed at CERN using the UNICOS framework and Siemens S7 PLCs. The verification results presented in this chapter, are obtained using nuXmv as it is currently the verification tool which give us better results from the verification point of view. The measurements were performed on a PC with Intel® Core™ i5-3230M 2.60 GHz CPU, 8 GB RAM, on Windows 7 x64.

This chapter is divided in 3 main parts:

1. Section 4.2 introduces the UNICOS framework describing the control system architecture obtained when applying it.

2. Section 4.3 describes the experimental results of applying the methodology to a PLC program corresponding to one single UNICOS object. This PLC code consists of one main FB and some additional FCs and timers.

3. Finally, Section 4.4 presents the experimental results of a complete PLC program of the LHC cryogenics control system. This PLC program contains hundreds of FBs, FCs and DBs.
4.2 UNICOS framework

UNICOS is an object-based control system framework developed at CERN and based on the IEC 61512 (2009) standard. This framework provides a methodology, a library of objects and a set of code generation tools to produce control programs.

UNICOS was born more than a decade ago to provide a solution for the LHC cryogenics control system. The first reference about a control system developed with UNICOS can be found in Casas-Cubillos et al. (2002) and the first reference about the framework itself in Gayet and Barillère (2005). Since that first development, the framework has been enriched, becoming a more general and flexible framework. The last updates can be found in Blanco Vinuela et al. (2011).

When developing a control system using the UNICOS framework, control and process engineers design and describe the control strategy in a high level specification and the automatic generation tools produce the control code for the control layer and the configuration of the supervision layer. In addition, the necessary code for the communication between these layers is also automatically generated.

The framework produces control programs for different control devices, i.e. PLCs or industrial PCs. Regarding the type of process and the control devices used, UNICOS can be divided in different packages as it is shown in Fig. 4.1.

![Figure 4.1: Different UNICOS packages](image)

Here we focus on the CPC (Continuous Process Control) package, which produces control systems based on PLCs at the control
layer (currently Siemens and Schneider PLCs) and on the WinCC OA SCADA (from Siemens) at the supervision layer. This package produces mainly control systems for continuous processes. The common architecture of the control systems developed with UNICOS CPC is shown in Fig. 4.2. Details about the PLC code generated by the UNICOS CPC package are presented in the following paragraphs.

Figure 4.2: UNICOS CPC control system architecture

By using the UNICOS CPC package, the control engineer designs a model of the process units (e.g., sensors, actuators, subsystems, etc.). On this model, every element from the process instrumentation is represented by the UNICOS CPC objects (also called UNICOS CPC baseline objects). These objects are based on the UNICOS metamodel described in Copy et al. (2011) and classified in families. There are 4 UNICOS CPC object families:

1. **I/O object family**: they represent the inputs and output signals connecting the PLC inputs and outputs with sensors and actuators. For example, a temperature sensor (which is connected to the digital input card of the PLC) is represented by a “Digital-Input” object.

2. **Field object family**: they represent instrumentation equipment such as valves, pumps, motors, heaters, etc. Usually these devices are connected to the real PLC inputs and outputs through
several input or output objects (e.g. a digital valve may receive one signal to open the valve, one signal to close it and it may send two feedback signals to the PLC indicating if the valve is open or close). For example, a digital pump is represented by a “OnOff” object.

3. **Control object family:** they represent a group of instrumentation equipments or a subsystem operated independently from the rest of the process. The corresponding object in this case is called “ProcessControl” object. This object behaves as a master, sending orders to the *Field objects* that are part of the corresponding subsystem. This family also includes the objects that represent the PID controllers, the alarms and interlocks of the system.

4. **Interface object family:** they represent information communicated between the SCADA and the control layer. Typically parameters or status are part of this family. One example is the “AnalogParameter” object, which represents the analog parameters sent from the SCADA to the control layer (e.g. thresholds).

In the CPC package, each UNICOS CPC object has its corresponding PLC code, containing the behavior of the object. This PLC code consists in one FB (sometimes including some additional FCs).

The PLC code of a complete control system, developed with UNICOS CPC, consists in a common software architecture where the object instances are interconnected and the specific logic to control the process according with the high level specification is included.

Fig. 4.3 shows an example of this mapping between the process instrumentation and the UNICOS objects. In this high level model, each element on the process side (sensors, actuators, signals, subsystems, alarms, etc.) correspond to one UNICOS object and they are interconnected.

The PLC code is automatically generated from this high level model, according with a set of rules included in the generation tool (See Fernández Adiego et al. (2011)). The code contains the instance of the UNICOS CPC objects, the interconnection between them and functions containing the specific logic of the application (according with the specification).
4.2. **UNICOS framework**

Fig. 4.3 shows the static representation of the PLC code architecture for Siemens S7 PLCs. It shows the main program (i.e OB1), a cyclic interrupt (i.e. OB35), an event interrupt (i.e. OB82) and a restart subroutine (i.e. OB100). All the baseline object FBs (the ones starting by “CPC_FB_”, e.g. \texttt{CPC_FB_DI}) are called from the main program as well as the specific logic of the control system. The PLC languages used in UNICOS CPC for Siemens PLCs are SCL (Structured Control Language) and Graph, which is similar to GRAFCET (Graphe Fonctionnel de Croissant Étape Transition). They are the Siemens implementation of ST and SFC from the \texttt{IEC 61131} (2013) standard.

This framework has been used in many industrial installations, for example, the LHC cryogenics, cooling, HVAC (Heating, Ventilating, and Air Conditioning) and the LHC vacuum systems. It has become a standard in the control system development at CERN.

The following paragraphs present the verification case studies of UNICOS PLC programs.
Figure 4.4: UNICOS PLC code architecture
4.3 UNICOS baseline object case study

The proposed methodology has been applied to verify the UNICOS CPC objects. The size and complexity in terms of coding logic of these objects varies from the simplest objects, such as the DigitalInput and the DigitalParameter objects to the most complex, such as the Controller.

The selected object to present the experimental results in this chapter is the so-called OnOff object. The OnOff object size and complexity are representative of the UNICOS CPC objects and many requirements (complex safety properties, liveness properties are time-related properties) were provided by the UNICOS developers. In most of the cases, verification of these properties was possible by applying the property preserving reduction techniques proposed in this thesis.

This section presents a detailed description of the experimental results and it is divided in the following subsections:

- Description and some metrics about the OnOff PLC implementation (Section 4.3.1).
- Experimental results regarding model generation (Section 4.3.2).
- Experimental results regarding verification of complex properties (Section 4.3.3).
- Experimental results regarding verification of time properties (Section 4.3.4).
- Example of a counterexample analysis (Section 4.3.5).

Part of these experimental results were published in Fernández Adiego et al. (2014c).

4.3.1 Object description and specification

This object represents a physical equipment driven by digital signals, e.g. an on-off valve, heater or motor. The corresponding PLC code, used for the experimental results, consists on one FB and some additional FCs written in SCL. Some key metrics about this object are shown in Table 4.1. The complete OnOff PLC code can be found in the Appendix A.1.
Chapter 4 Case studies and measurements

Table 4.1: Case Study metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>OnOff PLC code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lines of code</td>
<td>≈ 820</td>
</tr>
<tr>
<td>Program blocks</td>
<td>1 main FB, 2 timers and 3 FCs</td>
</tr>
<tr>
<td>Statements</td>
<td>418</td>
</tr>
<tr>
<td>Function calls</td>
<td>21</td>
</tr>
<tr>
<td>Input variables</td>
<td>29 (20 BOOL, 3 WORD, 2 ARRAY of 16 BOOL and 4 TIME)</td>
</tr>
<tr>
<td>Output variables</td>
<td>31 (27 BOOL, 2 WORD and 2 ARRAY of 16 BOOL)</td>
</tr>
<tr>
<td>Internal variables</td>
<td>82 (73 BOOL, 1 TIME, 2 TP timer instances, 1 TON timer instance, 1 REAL and 4 INT)</td>
</tr>
<tr>
<td>PLC data types</td>
<td>BOOL, INT, REAL, WORD, TIME, STRUCT and ARRAY</td>
</tr>
<tr>
<td>Timers</td>
<td>3 instances</td>
</tr>
</tbody>
</table>

Fig. 4.5 shows the OnOff signal interface. More details about the OnOff object and about UNICOS in general can be found in the UNICOS documentation website ([UNICOS CPC Team (2013)]).

4.3.2 Experimental results regarding model generation

As it was described in the methodology, the first step is the formalization of the requirements. This first step has an important impact on the generation of the models, as the performance of reduction techniques such as COI highly depends on the property requirements. About fifty requirements have been verified on the OnOff object, finding many discrepancies between the specification and the PLC program. As well as for the OnOff object, the methodology has also been successfully applied to rest of the UNICOS CPC baseline objects.

In this section, two verification cases are presented to illustrate how this methodology is applied to the OnOff object. Both requirements are connected to the so-called Mode manager.

The Mode manager specification describes the different operating modes in which the OnOff can be operated. This object can operate in one of the following five modes:
4.3. **UNICOS baseline object case study**

Figure 4.5: OnOff signals interface
Chapter 4. Case studies and measurements

- **Auto**: the object is driven by the control logic of a higher object of the hierarchy (e.g. a PCO (Process Control Object) from the control object family).

- **Manual**: the object is driven by the operator from the supervision and it can change to Auto mode with a control logic request.

- **Forced**: the object is driven by the operator from the supervision but it can only change to Auto mode with an operator request.

- **Software Local Drive**: the object is driven locally by a local software such as a local touch panel.

- **Hardware Local Drive**: the object is driven locally by the process field.

The transitions between the operating modes are performed by “mode requests”, coming from the implemented logic, the operator or a local device. To perform an operation mode change, a rising edge is necessary on the corresponding mode request input. For example, one of these inputs is **AuAuMoR**, which stands for “Auto mode request initiated by the logic”. Similarly, there is a **MAuMoR** input which stands for “Auto mode request initiated by the operator”. Fig. 4.6 shows the state machine that specifies the behavior of the mode manager for the three main modes. In the figure, “RE(x)” stands for rising edge on input $x$.

The PLC code corresponding to the mode manager is 4.1. However, it is affected by more variables from the rest of the PLC program.

```
(* MODE MANAGER *)
IF NOT (HLD AND PHLD) THEN

(* Forced Mode *)
IF (AuMoSt_aux OR MMoSt_aux OR SoftLDSt_aux) AND
   E_MFoMoR AND NOT(AuIhFoMo) THEN
   AuMoSt_aux := FALSE;
   MMoSt_aux := FALSE;
   FoMoSt_aux := TRUE;
   SoftLDSt_aux := FALSE;
END_IF;

(* Manual Mode *)
IF (AuMoSt_aux OR FoMoSt_aux OR SoftLDSt_aux) AND
   E_MMMoR AND NOT(AuIhMMo) THEN
   AuMoSt_aux := FALSE;
```

Figure 4.6: State machine of the OnOff mode manager from the UNICOS specifications

```
17       MMoSt_aux := TRUE;
18       FoMoSt_aux := FALSE;
19       SoftLDSt_aux := FALSE;
20       END_IF;
21
22       (* Auto Mode *)
23       IF (MMoSt_aux AND (E_MAuMoR OR E_AuAuMoR)) OR (FoMoSt_aux AND E_MAuMoR)
24           OR (SoftLDSt_aux AND E_MAuMoR) OR (MMoSt_aux AND AuIhMMo) OR 
25           (FoMoSt_aux AND AuIhFoMo) OR (SoftLDSt_aux AND AuIhFoMo) OR NOT( 
26           AuMoSt_aux OR MMoSt_aux OR FoMoSt_aux OR SoftLDSt_aux) THEN
27           AuMoSt_aux := TRUE;
28           MMoSt_aux := FALSE;
29           FoMoSt_aux := FALSE;
30           SoftLDSt_aux := FALSE;
31           END_IF;
32
33       (* Software Local Mode *)
34       IF (AuMoSt_aux OR MMoSt_aux) AND E_MSoftLDR AND NOT AuIhFoMo THEN
35           AuMoSt_aux := FALSE;
36           MMoSt_aux := FALSE;
37           FoMoSt_aux := FALSE;
38           SoftLDSt_aux := TRUE;
39           END_IF;
40
41       (* Status setting *)
42       LDSt := FALSE;
43       AuMoSt := AuMoSt_aux;
44       MMoSt := MMoSt_aux;
45       FoMoSt := FoMoSt_aux;
46       SoftLDSt := SoftLDSt_aux;
47       ELSE
48       AuMoSt := FALSE;
49       MMoSt := FALSE;
50       FoMoSt := FALSE;
```
4.3.2.1 First requirement

The first requirement, that is derived from the specification of the object, is shown in Fig. 4.6, is the following:

“If there is a rising edge on the AuAuMoR (Auto mode request initiated by the logic) input, the mode will be changed to Auto.”

This requirement is ambiguous, thus some refinement is needed in order to be able to be formalized and verified:

“If the current mode is Auto, Manual or Forced mode and there is a rising edge on the AuAuMoR (Auto mode request initiated by the logic) input, but there are no other mode change requests, the mode will be Auto at the end of the cycle.”

The corresponding pattern for this requirement is the pattern TL7, defined in Section 3.4:

If \[1\] is true at the end of cycle N and \[2\] is true at the end of cycle N+1, then \[3\] is always true at the end of cycle N+1.

and this is the corresponding LTL formula:

\[
G\left( (EoC \land [1] \land X (\neg EoC \lor (EoC \land [2]))) \rightarrow X (\neg EoC \lor (EoC \land [3]))) \right)
\]

with the corresponding PLC variables:

[1]: not AuAuMoR and (AuMoSt or MMoSt or FoMoSt)
[2]: AuAuMoR and (not MAuMoR and not MMMoR and not HLD and not MSoftLDR and not MFoMoR)
[3]: AuAuMoR
Where $EoC$ means “end of PLC cycle” and is true only at the end of PLC cycles.

The resulting LTL formula is the following:

$$
G \left( (EoC \land \neg AuAuMoR \land (AuMoSt \lor MMoSt \lor FoMoSt) \land (\neg MAuMoR \land \neg MMMoR \land \neg HLD \land MSoftLDR \land \neg MFoMoR) ) \land X (\neg EoC \lor (EoC \land AuAuMoR \land (AuMoSt \lor MMoSt \lor FoMoSt) \land (\neg MAuMoR \land \neg MMMoR \land \neg HLD \land MSoftLDR \land \neg MFoMoR) ) \right) \to X (\neg EoC \lor (EoC \land AuMoSt) )
$$

Note that in the PLC code $MAuMoR$ corresponds to $\text{ManReg01}[8]$, $MMMoR$ corresponds to $\text{ManReg01}[9]$, $MSoftLDR$ corresponds to $\text{ManReg01}[10]$ and $MFoMoR$ corresponds to $\text{ManReg01}[11]$. $\text{ManReg01}$ is an input variable which contains the manual requests from the SCADA operator.

Once the requirement is formalized, the formal models are produced. Table 4.2 shows some key metrics regarding the size of the models and the generation times for the case study. Three different models are compared here:

- $M_1$: a “non-reduced model” without any model reductions.

- $M_2$: a “reduced model”, which is still general (not property specific) as COI has not been applied.

- $M_3$: a model tailored to the current example requirement, which is only suitable for the evaluation of a reduced set of requirements (requirements which contain the same variables). COI has been applied.

By using property preserving reduction techniques, the size of the PSS size of the $\text{OnOff}$ object can be reduced from $1.61 \cdot 10^{218}$ to $3.65 \cdot 10^{10}$, without affecting the verification result.

The run time of the model generation including the ST code parsing, the reductions, and the generation of the nuXmv inputs does not
take more than 10–15 seconds, which is orders of magnitude lower than the achieved reduction in the verification time.

The verification results for this requirement are presented in Section 4.3.3.

### 4.3.2.2 Second requirement

The second experimental result corresponds with the following requirement:

“If the object is controlled locally (is in the so-called Hardware Local mode) and there is no interlock, nor explicit output change request valid in this mode, the output keeps its value”

The requirement is formalized using the pattern TL7 (the same as the previous requirement), and it uses the following values:

If \[1\] is true at the end of cycle N and \[2\] is true at the end of cycle N+1, then \[3\] is always true at the end of cycle N+1.

with the corresponding PLC variables:

[1]: not OutOnOV and not TStopI and not FuStopI and not StartI
[2]: HLD and not HOnR and not HOffR and not TStopI and not FuStopI and not StartI
[3]: not OutOnOV
4.3. **UNICOS baseline object case study**

### Table 4.3: Model generation metrics

<table>
<thead>
<tr>
<th>IM metrics</th>
<th>Models</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No red.</td>
</tr>
<tr>
<td></td>
<td>$(M_1)$</td>
</tr>
<tr>
<td>Variables</td>
<td>259</td>
</tr>
<tr>
<td>Automata</td>
<td>9</td>
</tr>
<tr>
<td>locations</td>
<td>460</td>
</tr>
<tr>
<td>PSS</td>
<td>$1.61 \cdot 10^{218}$</td>
</tr>
<tr>
<td>Generation time</td>
<td>0.2 s</td>
</tr>
</tbody>
</table>

The corresponding LTL formula is the following:

$$G \left( (EoC \land \neg OutOnOV \land \neg TStopI \land \neg FuStopI \land \neg StartI \land HLD \land X(\neg EoC U (EoC \land HLD \land \neg HOnR \land \neg HOffR \land \neg TStopI \land \neg FuStopI \land \neg StartI) ) \rightarrow X(\neg EoC U (EoC \land \neg OutOnOV) ) \right)$$

Table 4.3 shows the metrics for this second requirement. Before the reductions, the PSS size of this baseline object is $1.6 \cdot 10^{218}$. After the general and requirement-dependent reductions, the PSS contains $4.3 \cdot 10^{26}$ states of which $4.9 \cdot 10^{14}$ are reachable. The generation of the model including all the reductions takes 0.6 s.

#### 4.3.3 Experimental results regarding verification of complex properties

When talking about complex properties, we reference properties that need several temporal operators to be formalized, for example, the formulas presented in the previous subsection. These requirements represent sequences of values from different PLC cycles and this was one of the main goals when designing this methodology. The two requirements presented before were verified using the nuXmv model checker, integrated in the methodology.

nuXmv, as well as NuSMV, provides various parameters to fine-tune the verification hence the run time highly depends on the used parameters. Without any given parameters, nuXmv will explore the
full state space before the evaluation of the requirement. However, if this is not necessary for the verification, it can be disabled by the -df parameter. The -dcx parameter disables the generation of the counterexample that makes the verification time smaller, but we cannot profit from the information given by the counterexample. The -dynamic parameter enables the dynamic reordering of the variables, which can drastically reduce the memory consumption of the tool.

Table 4.4 shows verification time results for the first requirement on the OnOff object. As it is shown in the table, the verification of the non-reduced model ($M_1$) was not successful. The requirement can be checked on the general reduced model, taking 160 s with counterexample generation. However, much smaller verification times can be achieved by using the reduced model specific to the given requirement ($M_3$). In this case, the verification and the counterexample generation took less than 1 second together. (The symbol “—” indicates an execution longer than 24 hours). This table shows the difference of verification performance when using the different nuXmv parameters.

For the introduced example requirement, the result of the model checker is false, thus the requirement is not satisfied.

### Table 4.4: Verification run time for the first requirement from Fernández Adiego et al. (2014c)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Non-reduced model ($M_1$)</th>
<th>Reduced model ($M_2$)</th>
<th>Specific model ($M_3$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>no parameters</td>
<td>—</td>
<td>—</td>
<td>8.398 s</td>
</tr>
<tr>
<td>-dynamic</td>
<td>—</td>
<td>≈ 7 h</td>
<td>1.334 s</td>
</tr>
<tr>
<td>-dynamic -df</td>
<td>—</td>
<td>160.8 s</td>
<td>0.547 s</td>
</tr>
<tr>
<td>-dynamic -df -dcx</td>
<td>—</td>
<td>3.787 s</td>
<td>0.141 s</td>
</tr>
</tbody>
</table>

For the second requirement, as it is shown in Table 4.5, the evaluation of the requirement takes 6.1 s using nuXmv without counterexample generation, which showed that the requirement is not satisfied. If the counterexample is generated too, the run time is 19.4 s.

In general, for the baseline objects the property preserving reduction techniques (COI, the general rule-based reductions and mode selection) were enough to verify these objects. For this case study, the variable abstraction technique was not applied. In Section 4.4, the variable abstraction technique has been applied to verify safety prop-
### 4.3. UNICOS baseline object case study

#### Table 4.5: Verification run time for the second requirement

<table>
<thead>
<tr>
<th>Metric</th>
<th>Non-reduced model ($M_1$)</th>
<th>Reduced model ($M_2$)</th>
<th>Specific model ($M_2$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification</td>
<td>—</td>
<td>—</td>
<td>19.4 s</td>
</tr>
<tr>
<td>(-dynamic -df -dcx)</td>
<td></td>
<td></td>
<td>(6.1 s without c.ex.)</td>
</tr>
</tbody>
</table>

As it was mentioned before, more than fifty different requirements, stated by the UNICOS developers, have been verified on the *OnOff* baseline object. These experiments identified several faults in this well-tested base object used all over the CERN control systems.

### 4.3.4 Experimental results regarding verification of time properties

Verification of time related requirements on the *OnOff* are presented in this section. These results can be found in the publication [Fernández Adiego et al. (2014a)](#). As it was described on Section 3.9, two different approaches for modeling the timing aspects of PLCs are included in the methodology. If the requirement contains explicit time in it, the realistic approach is applied. If it does not, the abstract approach is applied. Experiments with both approaches are presented.

#### 4.3.4.1 Realistic Approach

Having the following requirement:

“If there is a rising edge on $C_1$, after $t_m$ units of time $C_2$ will be true, if $C_1$ remained true”.

where, $C_1$, $t_m$ and $C_2$ corresponds with the signals shown in Fig. 4.7, the selected pattern is the TL10 (*TON-like property*), where $C_1$ and $C_2$ corresponds to the following signals of the *OnOff* object:

$C_1 = \text{HFOff and HFOn and not(Re\_OutOvSt\_aux) and not(Fe\_OutOvSt\_aux)}$;
\[ C_2 = \text{PosW}; \]

\( t_m \) is the monitor delay time. 3 different experiments are performed for this requirement: 10 s, 9 s and 1 s.

In addition, the following parameters (mode selection) are set:

\[ \text{PPulse} = \text{FALSE}; \]
\[ \text{POutOff} = \text{FALSE}; \]
\[ \text{PHLD} = \text{FALSE}; \]
\[ \text{PHFOff} = \text{TRUE}; \]
\[ \text{PHFOn} = \text{TRUE}; \]
\[ \text{PFsPosOn} = \text{TRUE}; \]
\[ \text{PWDt} = 10 \text{ s}; \]

Figure 4.7: Verification configuration for OnOff model extended with monitor

Table 4.6 presents different state spaces depending on which abstraction and reduction techniques are applied.

To be able to verify this property, the original model was shrunk from a PSS of \(1.6 \cdot 10^{218}\) states to a PSS of \(1.1 \cdot 10^{36}\) as can be seen in Table 4.6. In order to do so, reductions, fixed parameters (focusing on a specific scenario), and the COI technique (which eliminated 2 timers out of 3) have been applied. As it was mentioned before, time values were modeled as 16-bits variables instead of 32-bits.
Table 4.6: State space of the OnOff model with realistic timer representation from Fernández Adiego et al. (2014a)

<table>
<thead>
<tr>
<th>Time</th>
<th>Monitor</th>
<th>Reductions</th>
<th>PSS</th>
<th>#Vars</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 bit</td>
<td>–</td>
<td>none</td>
<td>$1.6 \cdot 10^{218}$</td>
<td>255</td>
</tr>
<tr>
<td>16 bit</td>
<td>–</td>
<td>none</td>
<td>$2.5 \cdot 10^{160}$</td>
<td>255</td>
</tr>
<tr>
<td>16 bit</td>
<td>–</td>
<td>general</td>
<td>$1.6 \cdot 10^{134}$</td>
<td>185</td>
</tr>
<tr>
<td>16 bit</td>
<td>+</td>
<td>general</td>
<td>$8.5 \cdot 10^{139}$</td>
<td>189</td>
</tr>
<tr>
<td>16 bit</td>
<td>+</td>
<td>general, COI</td>
<td>$1.1 \cdot 10^{85}$</td>
<td>143</td>
</tr>
<tr>
<td>16 bit</td>
<td>+</td>
<td>gen., fix params, COI</td>
<td>$1.1 \cdot 10^{36}$</td>
<td>86</td>
</tr>
</tbody>
</table>

Table 4.7 presents verification results for the OnOff model after applying all the previously mentioned reduction techniques. The requirement has been checked with three different configurations in terms of timer delay ($t_p$) and monitor delay ($t_m$). The first uses $t_p = t_m = 10$ s values, which means the parameter $t_p$ of OnOff and the delay parameter $t_m$ of the monitor were both 10 s. In this case, the result is true, which is given by nuXmv in 11.4 s. The other two configurations use monitor delay times smaller than the parameter $t_p$, therefore the output is expected too early, thus the result should be false. As it can be seen in Table 4.7, in both cases the verification time was around 5 to 20 s, but the generation of the counterexample (C.ex. gen. time) took significantly more time. In the case when we used $t_m = 9$ s, the counterexample was longer (3,876 steps), and its generation time was around 15 times bigger than when we used $t_m = 1$ s. Notice that these verification results can have a timing error not bigger than the maximal cycle time, 100 ms in this case, because the current time is incremented in quanta.

4.3.4.2 Abstract Approach

This approach has also been applied to the OnOff object from the UNICOS library. Three experiments are presented in this section to evaluate the abstract approach.

For Experiment 1 (see Table 4.9), the same reduction techniques and the same fixed parameters as for the realistic approach have been used. The PSS of the OnOff model became $5.5 \cdot 10^{24}$ (instead of
Table 4.7: Verification time on OnOff model with realistic time representation from Fernández Adiego et al. (2014a)

<table>
<thead>
<tr>
<th>Timer delay ($t_p$)</th>
<th>Monitor delay ($t_m$)</th>
<th>Result</th>
<th>Run time</th>
<th>gen. time</th>
<th>C.ex. length</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 s</td>
<td>10 s</td>
<td>true</td>
<td>11.4 s</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>10 s</td>
<td>9 s</td>
<td>false</td>
<td>19.5 s</td>
<td>2513.2 s</td>
<td>3876</td>
</tr>
<tr>
<td>2 s</td>
<td>1 s</td>
<td>false</td>
<td>5.2 s</td>
<td>123.0 s</td>
<td>510</td>
</tr>
</tbody>
</table>

1.1·10^{36}). Representing the requirement checked on the realistic model is not possible in this approach as the time is not counted explicitly. Instead, we can check the following liveness property (pattern TL):

“if $C_1$ is sometime true and remains true forever, eventually $C_2$ will be true”.

The equivalent LTL property is:

$$F\left( G(EoC \rightarrow C_1) \rightarrow F(C_2) \right)$$

In this case, no monitor is needed and $C_1$ and $C_2$ corresponds to the same signals as for the realistic approach:

$$C_1 = \text{HFOff and HFOn and not(Re_{OutOvSt\_aux}) and not(Fe_{OutOvSt\_aux})};$$
$$C_2 = \text{PosW};$$

Two other experiments on the model with abstract time representation are presented (Exp. 2, 3). In these cases, no parameters were fixed and all the three timers had effect on the requirement. The requirement 2 was a simple safety requirement in CTL ($AG(C_3 \rightarrow C_4)$), while requirement 3 was a bit more complex: $AG(C_5 \rightarrow AF(C_6))$.

The experiments (c.f. Table 4.9) show that these requirements can be checked using the abstract time representation, even without fixing any parameters. With the realistic time representation, the state space would be too large to be verified using nuXmv.

Table 4.8 presents different state spaces depending on which reductions techniques are applied and what requirement was verified. Table 4.9 shows the measured run times.
4.3. UNICOS baseline object case study

Table 4.8: State space of the OnOff model with abstract time representation from Fernández Adiego et al. (2014a)

<table>
<thead>
<tr>
<th>Reductions</th>
<th>PSS</th>
<th>#Vars</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>$1.1 \cdot 10^{131}$</td>
<td>243</td>
</tr>
<tr>
<td>general</td>
<td>$4.7 \cdot 10^{112}$</td>
<td>164</td>
</tr>
<tr>
<td>general, COI, fix params (Exp. 1)</td>
<td>$5.5 \cdot 10^{24}$</td>
<td>77</td>
</tr>
<tr>
<td>general, COI (Exp. 2, 3)</td>
<td>$1.1 \cdot 10^{40}$</td>
<td>126</td>
</tr>
</tbody>
</table>

Table 4.9: Verification time on OnOff model with abstract time representation from Fernández Adiego et al. (2014a)

<table>
<thead>
<tr>
<th>Exp.</th>
<th>#Timers</th>
<th>Result</th>
<th>Run time</th>
<th>C.ex.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>1</td>
<td>true</td>
<td>6.1 s</td>
<td>—</td>
</tr>
<tr>
<td>(2)</td>
<td>3</td>
<td>false</td>
<td>294.2 s</td>
<td>18.6 s</td>
</tr>
<tr>
<td>(3)</td>
<td>3</td>
<td>false</td>
<td>4201.9 s</td>
<td>12020.9 s</td>
</tr>
</tbody>
</table>

4.3.5 Counterexample analysis

An example of last step of the methodology is presented here, the counterexample analysis. The selected counterexample corresponds to the verification case presented previously (See Section 4.3.3). This experiment was also published in Fernández Adiego et al. (2014c). The requirement for the verification case is the following:

$$G \bigg( (EoC \land (\neg AuAuMoR \land (AuMoSt \lor MMoSt \lor FoMoSt)) \land (\neg MAuMoR \land \neg MMMoR \land \neg HLD \land \neg MSoftLDR \land \neg MFoMoR)) \bigg)$$

The generated counterexample by nuXmv contains the value of each variable after each transition in the model (corresponding to the execution of one instruction in the PLC code). This detailed counterexample contains about 5000 lines for the specific model ($M_3$) and...
37,500 lines for the generic model ($M_2$). These are too detailed for human analysis. However, they can be reduced, as it is enough to know the value of the input and output variables at the end of each PLC cycle, thus the variable valuations of the intermediate states can be discarded. By removing the unnecessary states and the temporary variables, the counterexample of the current requirement can be reduced to approximately 100 lines.

The counterexample can also be used to demonstrate the problem in a real environment. Using the nuXmv’s counterexample, a demonstrator PLC code can be easily generated by adding a module simulating the variables from the counterexample and checking the expected result. By doing so, it can be demonstrated that the counterexample is not caused by a mistake during the model generation or due to bad reductions. In this case study, the counterexample given by nuXmv was confirmed in a real PLC, showing that the model and the real system are equivalent for this specific requirement.

Listing 4.2 and Listing 4.3 show an extract from the generated counterexample and the corresponding part of the PLC demonstrator source code.

Furthermore, the PLC demonstrator can help the engineer to reduce the counterexample. Usually, most of the input variables do not have any effect on the evaluated requirement. Those variables can be fixed to constant values that can help focusing on the input value changes that causes the violation of the requirement.

```
1-> State: 1.17 <->
2inst.HLD = FALSE
3inst.ManReg01[8] = TRUE
4inst.ManReg01[9] = FALSE
5inst.ManReg01[10] = FALSE
7inst.AuAuMoR = FALSE
8inst.AUIhMMo = FALSE
9inst.AUIhFoMo = FALSE
10...
```

Listing 4.2: Extract from the counterexample

```
1onoff1.HLD := FALSE;
2onoff1.ManReg01 :=
32#0000000000000001;
4onoff1.AuAuMoR := FALSE;
5onoff1.AuIhMMo := FALSE;
6onoff1.AuIhFoMo := FALSE;
7...
8CPC_FB_ONOFF.onoff1();
9// Check:
10b := onoff1.AuMoSt;
```

Listing 4.3: Extract from the PLC demonstrator

In the current case, by using the counterexample and the reduced PLC demonstrator we were able to identify the source of the problem.
It turned out that from \textit{Forced mode} the logic cannot switch to \textit{Auto mode}, it can only be done by the operator. The corresponding part of the implementation can be seen in Listing 4.4\footnote{In the source code, the variables starting with “E\_” indicate the rising edges of the corresponding inputs. \texttt{AuMoSt\textsubscript{aux}} is true if the current mode is Auto. The meaning of variables \texttt{MMoSt\textsubscript{aux}}, \texttt{FoMoSt\textsubscript{aux}}, and \texttt{SoftLDSt\textsubscript{aux}} are similar, with the other modes.}. The highlighted part shows the code implementing the transition from Forced mode to Auto mode, which does not take into account the \texttt{AuAuMoR} input. This behavior is correct and intentional, in this case the specification contained a mistake.

```plaintext
IF (MMoSt\textsubscript{aux} AND (E\_MaMoR OR E\_AuAuMoR)) OR
   (FoMoSt\textsubscript{aux} AND E\_MaMoR) OR
   (SoftLDSt\textsubscript{aux} AND E\_MaMoR) OR
   (MMoSt\textsubscript{aux} AND AuIhMMo) OR
   (FoMoSt\textsubscript{aux} AND AuIhFoMo) OR
   NOT (AuMoSt\textsubscript{aux} OR MMoSt\textsubscript{aux} OR
         FoMoSt\textsubscript{aux} OR SoftLDSt\textsubscript{aux}) THEN
   (* Setting mode to Auto *)
   AuMoSt\textsubscript{aux} := TRUE;
   MMoSt\textsubscript{aux} := FALSE;
   FoMoSt\textsubscript{aux} := FALSE;
   SoftLDSt\textsubscript{aux} := FALSE;
END_IF;
```

Listing 4.4: Extract of the source code causing the violation of the requirement
4.4 Full UNICOS application case study

This section presents the experimental results obtained on one of LHC cryogenics control system. The goal of this section is to complement the experimental results presented in Section 4.3 for large PLC programs where the property preserving reduction techniques included in the methodology are not enough to verify the program. In this section, the variable abstraction technique is applied to verify the PLC program. The section is divided in two main parts:

- Description of the QSDN control system (Section 4.4.1).
- Experimental results of safety properties (Section 4.4.2).

4.4.1 Process description and specification

The so-called QSDN application has been selected as a case study of a complete PLC program. This application controls a subsystem of the LHC cryogenics process.

Fig. 4.8 represents the QSDN subsystem consisting in two nitrogen storage vessels. These vessels provide liquid nitrogen to the cryogenic plants via two digital valves (xPV409). In addition, each vessel is filled from a nitrogen truck and the internal pressure of vessels is regulated by an electrical heater (xEH400). Each vessel has also a gas outlet (xPV408) to provide warm gaseous nitrogen.

The size of QSDN PLC program is rather representative for medium UNICOS control systems. It contains 110 functions and function blocks, and consists of approximately 17,500 lines of code. Before reductions, these results in a huge generated model: the IM contains 302 automata, and the PSS size is $10^{31985}$ (see $M_1$ in Table 4.10).

When verifying full UNICOS control systems, we assume that the base objects from the UNICOS library are already verified, i.e. their specification is satisfied. Therefore the goal is to check the application-specific logic of the PLC program. This program is implemented using ST and SFC languages (SCL and Graph for Siemens PLCs). This logic is described in the UNICOS Functional Analysis, which is a semi-formal textual specification. We extracted the requirements from this

QSDN is a codename for Cryogenics Surface Liquid Nitrogen Storage System.
specification regarding to specific logic. The extracted requirements are safety properties to check the specific logic of this PLC program.

### 4.4.2 Experimental results regarding verification of safety properties

This section presents the experimental results of three safety requirements, extracted from the Functional Analysis of the QSDN control system. These requirements are typically similar to the following structure:

"if $\alpha$ is TRUE, then $\beta$ is TRUE"

The corresponding CTL formula for this example is:

$$\text{AG}(\alpha \rightarrow \beta)$$

Where the Greek letters mark Boolean expressions of variables. The property preserving reduction techniques (i.e. COI, general rule-based reduction and mode selection) remove all the unnecessary variables regarding the given property and the automata network is simplified. The requirements presented in this section correspond to the
so-called “dependent logic” of one of the actuators of the QSDN system: the QSDN_4_1PV408, which corresponds to a on-off valve (modeled by an OnOff object for the UNICOS model).

Listing 4.5 shows the relevant part of the QSDN PLC code related to the three requirements. However, this piece of code is not enough to prove that the requirements hold or not on this QSDN PLC program, so information from the rest of the program is also needed.

```
(* Position Management*)
QSDN_4_1PV408.AuOnR :=
QSDN_4_DN1CT_SEQ_DB.ValvesOn.x OR
QSDN_4_DN1CT_SEQ_DB.Run.x OR
QSDN_4_DN1CT_SEQ_DB.OkSignalOff.x ;
QSDN_4_1PV408.AuOffR := NOT QSDN_4_1PV408.AuOnR;
```

Listing 4.5: Excerpt of QSDN code relevant to the case study

### 4.4.2.1 First requirement

The first requirement to be checked is the following:

“If QSDN_4_DN1CT_SEQ_DB.Stop.x is true (at the end of a scan cycle), QSDN_4_1PV408.AuOffR should be true also.”

The corresponding patterns is TL1 and the corresponding temporal logic formula \( p \) is:

\[
AG\left((EoC \land QSDN_4_DN1CT_SEQ_DB.Stop.x) \rightarrow QSDN_4_1PV408.AuOffR\right)
\]

Table 4.10 presents relevant metrics about the generated model. The original state space is huge and the original model obviously cannot be verified (see \( M_1 \)). After the COI reduction 3757 variables are kept in the reduced model (see model \( M_2 \) with a PSS size of \( 10^{5048} \) states). Formal verification is still not possible. Therefore the variable abstraction technique has to be applied.

Fig. 4.9 shows the variable dependency graph for the given requirement with the distance between variables. The gray variables are part of the requirement (i.e. QSDN_4_1PV408.AuOffR and QSDN_4_DN1CT_SEQ_DB.Stop.x). The red edges represent assignment
dependencies (e.g. $a := b$ will imply a “$b \rightarrow a$” red edge). The blue edges represent conditional dependencies (e.g. $IF a \ THEN b := c$ will imply a “$b \rightarrow a$” blue edge).

Table 4.10: Metrics of the models of QSDN

<table>
<thead>
<tr>
<th>Metric</th>
<th>Non-reduced model ($M_1$)</th>
<th>Reduced model ($M_2$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSS</td>
<td>$10^{31985}$</td>
<td>$10^{5048}$</td>
</tr>
<tr>
<td>Variables</td>
<td>31,402</td>
<td>3757</td>
</tr>
<tr>
<td>Generation</td>
<td>4.2 s</td>
<td>15.3 s</td>
</tr>
</tbody>
</table>

Fig. 4.10 shows the relationship between the abstract models and the maximum number of reachability properties to be checked if variable abstraction is applied (or the maximum number of possible invariants).

Table 4.11 shows the verification results when applying the variable abstraction technique. With this technique described in Section 3.7.4, it is proved that the property is TRUE. The experiment is performed with a TO of 30 s. The answer is given by the tool in 45.309 s (which 30 of these seconds corresponds to the TO obtained when checking the reachability on the $OM''$ model).

To verify this requirement, six steps of the variable abstraction technique are needed (according with the steps defined in the subsection 3.7.4):

- **Step 1**: $p$ is verified on the first abstraction $AM'_1$ and the result is FALSE.

- **Step 2**: $q$ is verified on $AM'_1$ and the result is FALSE. $q$ corresponds with the following CTL property:

  $$AG\left((EoC \land QSDN_4\_DN1CT\_SEQ\_DB\_Stop.x) \rightarrow \neg QSDN_4\_1PV408\_AuOffR\right)$$

- **Step 3**: The extracted counterexample $c$ is transformed in a reachability property $r$ and verified on $OM''$. After 30 s a TO
Figure 4.9: Variable dependency graph for the given requirement of QSDN
is reached by nuXmv. \( r \) corresponds with the following CTL property:

\[
\text{EF} \left( EoC \land \text{QSDN} \_4 \_DN1CT \_SEQ \_DB \_Stop \_x \land \text{QSDN} \_4 \_1PV408 \_AuOnR \right)
\]

- **Step 4:** The same reachability property is verified on \( AM''_1 \) (first abstraction) and the result is TRUE. A new iteration is needed.

- **Step 4:** The same reachability property is verified on \( AM''_2 \) (second abstraction) and the result is FALSE. It means the first counterexample is spurious.

- **Step 5:** the number of potential invariants for \( AM'_1 \) is smaller than 10 (see Fig. 4.10), then an invariant is added to \( AM'_1 \).

- **New iteration. Step 1:** \( p \) is verified again on \( AM'_1 \) with the new invariant. The result is TRUE, proving that the property also holds on the original model \( OM' \). This abstract model is shown in the Listing [B.2] in the Appendix [B].
### Table 4.11: Verification time on QSDN model

<table>
<thead>
<tr>
<th>Model</th>
<th>PSS</th>
<th>Model gen.</th>
<th>nuXmv run-time</th>
<th>Ver. result</th>
</tr>
</thead>
<tbody>
<tr>
<td>p on $AM'_1$</td>
<td>$2.4 \cdot 10^4$</td>
<td>7.549 s</td>
<td>0.030 s</td>
<td>FALSE</td>
</tr>
<tr>
<td>q on $AM'_1$</td>
<td>$2.4 \cdot 10^4$</td>
<td>0 s</td>
<td>0.033 s</td>
<td>FALSE</td>
</tr>
<tr>
<td>r on $OM''$</td>
<td>$7.8 \cdot 10^{4872}$</td>
<td>18.301 s</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>r on $AM''_1$</td>
<td>$5.9 \cdot 10^6$</td>
<td>9.147 s</td>
<td>0.049 s</td>
<td>TRUE</td>
</tr>
<tr>
<td>r on $AM''_2$</td>
<td>$4.28 \cdot 10^{30}$</td>
<td>8.220 s</td>
<td>1.340 s</td>
<td>FALSE</td>
</tr>
<tr>
<td>p on $AM'_1$ + invar.</td>
<td>$2.4 \cdot 10^4$</td>
<td>0 s</td>
<td>0.053</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

#### 4.4.2.2 Second requirement

The second requirement extracted from the functional analysis is the following:

“If \( QSDN_4 \_DN1CT\_SEQ\_DB\_Run.x \) is true (at the end of a scan cycle), \( QSDN_4 \_1PV408\_Au0nR \) should be true also.”

The corresponding patterns is 3.4.1.1 and the corresponding temporal logic formula is:

\[
AG\left((EoC \land QSDN_4 \_DN1CT\_SEQ\_DB\_Run.x) \rightarrow QSDN_4 \_1PV408\_Au0nR\right)
\]

The model after the property preserving reduction techniques has a PSS size of $10^{5048}$ as the previous example. The Table 4.12 shows the verification performance for each step when applying this technique.

- **Step 1:** $p$ is verified on the first abstraction $AM'_1$ and the result is TRUE. This abstract model is shown in the Listing B.3 in the Appendix B.

In this case, the answer is given by the tool in 7.544 s as the property holds in first abstraction of this technique.

#### 4.4.2.3 Third requirement

The third requirement extracted from the functional analysis is presented to show how the algorithm can prove that a property does not hold. The requirement is the following:
4.4. Full UNICOS application case study

<table>
<thead>
<tr>
<th>Table 4.12: Verification time on QSDN model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>p on AM₁</td>
</tr>
</tbody>
</table>

“If QSDN.4_DN1CT_SEQ_DB.Run.x is true (at the end of a scan cycle), QSDN.4_1PV408.AuOffR should be true also.”

The corresponding patterns is 3.4.1.1 and the corresponding temporal logic formula is:

\[
AG\left((\text{EoC} \land QSDN.4_DN1CT_SEQ_DB.Run.x) \rightarrow QSDN.4_1PV408.AuOffR\right)
\]

The model after COI has a PSS size of \(10^{5048}\) as well as the previous examples. In this case, this technique can confirm that this property does not hold and a counterexample was provided in 126.573 s. The summary of all the steps performed to evaluate this property is the following:

- **Step 1:** \(p\) is verified on the first abstraction \(AM₁\) and the result is FALSE.

- **Step 2:** \(q\) is verified on \(AM₁\) and the result is FALSE. \(q\) corresponds with the following CTL property:

\[
AG\left((\text{EoC} \land QSDN.4_DN1CT_SEQ_DB.Run.x) \rightarrow \neg QSDN.4_1PV408.AuOffR\right)
\]

- **Step 3:** The extracted counterexample \(c\) is transformed in a reachability property \(r\) and verified on \(OM''\). After 30 s a TO is reached by nuXmv. \(r\) corresponds with the following CTL property:

\[
EF\left(\text{EoC} \land QSDN.4_DN1CT_SEQ_DB.Run.x \land \neg QSDN.4_1PV408.AUOnR\right)
\]
− **Step 4:** The same reachability property is verified on \( AM_1'' \) (first abstraction) and the result is TRUE. A new iteration is needed.

− **Step 4:** The same reachability property is verified on \( AM_2'' \) (second abstraction) and the result is TRUE. A new iteration is needed.

− **Step 4:** The same reachability property is verified on \( AM_3'' \) (third abstraction) and a TO is reached and no result is provided.

− New iteration. **Step 1:** \( p \) is verified on a new abstraction \( AM_2' \). The result is FALSE and a new counterexample \( c \) is produced.

− **Step 2:** \( q \) is verified on \( AM_2' \) and the result is TRUE. These results implies that \( p \) does not hold on \( AM_2' \) and on \( OM' \). The counterexample \( c \) is real. This abstract model is shown in the Listing B.4 in the Appendix B.

The Table 4.13 shows the verification performance for each step when applying this technique.

<table>
<thead>
<tr>
<th>Model</th>
<th>PSS</th>
<th>Model gen.</th>
<th>nuXmv run-time</th>
<th>Ver. result</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p ) on ( AM_1' )</td>
<td>2.4 \cdot 10^1</td>
<td>9.471 s</td>
<td>0.107 s</td>
<td>FALSE</td>
</tr>
<tr>
<td>( q ) on ( AM_1' )</td>
<td>2.4 \cdot 10^1</td>
<td>0 s</td>
<td>0.028 s</td>
<td>FALSE</td>
</tr>
<tr>
<td>( r ) on ( OM'' )</td>
<td>7.8 \cdot 10^{4872}</td>
<td>19.580 s</td>
<td>TO</td>
<td>—</td>
</tr>
<tr>
<td>( r ) on ( AM_1'' )</td>
<td>2.95 \cdot 10^6</td>
<td>9.510 s</td>
<td>0.076 s</td>
<td>TRUE</td>
</tr>
<tr>
<td>( r ) on ( AM_2'' )</td>
<td>1.34 \cdot 10^{29}</td>
<td>8.232 s</td>
<td>1.260 s</td>
<td>TRUE</td>
</tr>
<tr>
<td>( r ) on ( AM_3'' )</td>
<td>5.11 \cdot 10^{80}</td>
<td>10.436 s</td>
<td>TO</td>
<td>—</td>
</tr>
<tr>
<td>( p ) on ( AM_2' )</td>
<td>4.8 \cdot 10^1</td>
<td>7.825 s</td>
<td>0.026 s</td>
<td>FALSE</td>
</tr>
<tr>
<td>( q ) on ( AM_2' )</td>
<td>4.8 \cdot 10^1</td>
<td>0 s</td>
<td>0.022 s</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

As can be seen, our verification method can be used for isolated verification of modules or for verification of complete PLC applications. Approximately 30 different requirement were extracted from the QSDN functional analysis document.
4.5 Summary of the chapter

This chapter presented the experimental results of applying the proposed methodology to two real-life PLC programs developed at CERN using the UNICOS framework.

The first PLC program corresponds with one of the UNICOS CPC baseline objects, the so-called OnOff object. Complex properties, including time properties and sequences were verified on the OnOff program. The proposed property preserving reduction techniques have been applied to be able to verify the object with successful results.

The second PLC program controls a subsystem of the LHC Cryogenics process at CERN. The significant size of this PLC program with 17,500 lines of code and a generated model with a PSS size of $10^{31985}$, makes the verification very challenging. In this case, safety properties were verified on this program and the “variable abstraction” technique was applied.

The experimental results show that the methodology is useful and PLC programs with a huge state space can be verified. Obviously, there are still some limitation and the combination of the property preserving reduction techniques and the variable abstraction may not be enough in some other cases. Providing new abstraction techniques is one of the future works for this project.

In addition, any complexity linked to formal verification or formal methods is hidden from the user of the methodology. The next chapter will give a deep analysis of these results, focusing in each steps of the methodology.
Chapter 5

Evaluation and analysis

This chapter presents an analysis about the different steps of the methodology and about the experimental results obtained when applying the designed methodology to CERN PLC programs.

5.1 Introduction

Different kind of requirements have been verified on UNICOS CPC baseline objects using the proposed methodology of this thesis, including complex properties (with several temporal logic operators), safety and liveness properties and finally “time-related” properties. The number of discrepancies that were found between the specifications and PLC programs was significant, even if these objects have been previously tested.

In addition, the methodology has been applied to complete UNICOS CPC PLC programs. The PLC program used for the experimental results in this thesis contains approximately 17,500 lines of code. In this case, a subset of safety properties (i.e. $\text{AG}(\alpha \rightarrow \beta)$) was verified on this PLC program.

The usability of the methodology was demonstrated, even for large PLC programs. Any complexity related to formal methods was completely hidden from control engineers.

This chapter analyzes all the steps of the methodology regarding three different aspects: completeness, usability and limitations. The content of this chapter is divided in the following sections:
Chapter 5. Evaluation and analysis

- Section 5.2 analyzes the solution for requirement specification provided by the methodology.

- Section 5.3 analyzes the modeling strategy for modeling the PLC platform and the controlled process.

- Section 5.4 analyzes the transformation rules from the PLC code to the IM.

- Section 5.5 analyzes the reduction techniques applied to the IM that make formal verification possible.

- Section 5.6 analyzes the transformation from the IM to the modeling language of the verification tools.

- Section 5.7 analyzes the verification results provided to the user of these methodology.

- Section 5.8 analyzes briefly the correctness of the different model transformations included in the methodology.

5.2 Evaluation of requirements formalization

This methodology gives a solution for the formalization of requirements for control and process engineers. This solution is based on patterns that rely on the experience of the PLC program developers of the EN-ICE group at CERN.\(^1\)

These patterns, written in English, provide a natural language that can be easily used by control and process engineers to express requirements without any need of knowledge about formal methods. The list of patterns presented in Chapter 3 covers the current needs of PLC developers of the EN-ICE group at CERN. It covers a quite large range of properties, as it includes common safety and liveness properties but also properties involving several PLC cycles and also “time properties”. However this list can be extended if a new type of requirement is needed for verification purposes.

\(^1\)EN-ICE web: http://www.cern.ch/enice/
5.2. Evaluation of requirements formalization

These patterns have a well-defined semantics and they can be automatically translated to temporal logic (either CTL or LTL) for formal verification purposes.

In terms of limitations, the expressiveness of the requirements is limited by the expressiveness of the temporal logic formalisms implemented in the verification tools included in our methodology. Currently, nuXmv provides the biggest range of property specification expressiveness as it fully supports CTL and LTL. UPPAAL is restricted to a subset of CTL and BIP to deadlock and safety properties.

Another limitation on the specification phase is provoked by the “variable abstraction” reduction technique, which only allows to verify a subset of safety properties. This technique has a very aggressive abstraction strategy and is focused on one specific type of safety properties. This restriction is a consequence of the verification requirements for full UNICOS PLC programs that are currently safety properties. For that reason, this reduction is only applied when our property preserving reduction techniques are not enough for verification. The variable abstraction technique could be modified to accept ACTL properties instead of the current safety properties (i.e. $\text{AG}(\alpha \rightarrow \beta)$) if the requirement specification expressiveness needs to be extended. However, this would imply to have a less aggressive abstraction strategy and it could imply a worse performance of this technique.

This proposal for requirement specification is useful and it can help control and process engineers to find bugs in their programs. However, this is not the final solution for requirement specification in control software engineering. Using patterns does not guarantee that the PLC program is complete and fully verified. This approach only guarantees that PLC programs are compliant with the list of requirements, which are created using these patterns. A future work in this direction will have the goal of providing a complete, unambiguous and still useful (easy to understand by non-formal methods experts) formal specification for PLC control code.

In conclusion, we can summarize the specification approach of this methodology emphasizing these three aspects:

- Specification by using patterns is complete for the current needs of the UNICOS PLC developers at CERN, comprising safety, liveness and “time-related” properties. More patterns can be added to this list if required.
– The approach is useful as it provides a very simple natural language to specify.

– The expressiveness limitations are given by the verification tools included in the methodology and by the “variable abstraction” reduction technique.

– The current approach is appropriate to find bugs in PLC programs, but it is not the final solution for control software specification.

5.3 Evaluation of PLC hardware and process modeling

Formal verification of PLC programs implies building a global model of the whole system. The whole system is composed, not only by the control software but also the hardware of the control system and the controlled process (e.g. water treatment, petroleum, ventilation systems, etc.) In this case, this global model should include information about the PLC execution platform and about the controlled process.

Regarding the PLC execution platform, this methodology models the scan cycle of a PLC providing the skeleton of the generated models. It also includes a strategy to identify PLC inputs when parsing the PLC program, as it is a challenging task when these inputs are parameters or they come from the supervision or from a decentralized periphery. The methodology can generate models for both safety and standard PLCs and both models only differ when verifying time properties with explicit time in it. Finally, the methodology also models PLC interrupts and restarts but assuming that there are no concurrency problems on the PLC program.

This modeling strategy is a compromise between the two extreme approaches for modeling the PLC execution platform. The first one would be providing a very detailed model for the execution platform where even distributed systems are modeled and concurrency problems can be detected by the verification tools, but producing very heavy models with a huge state space. The second approach would be to provide a very simple model with a small state space, but it would provoke many false positives in the verification. If these models do
not represent properly the real process can cause false negatives as well.

In conclusion, we can summarize the PLC hardware modeling approach of this methodology emphasizing the following aspects:

- The methodology models PLC interrupts and restarts, however concurrency problems should be checked before using a different technique, for example the static analysis of the PLC code.

- It currently targets centralized PLC control systems, but not distributed control systems. Modeling distributed systems obviously implies a higher complexity in terms of concurrency problems and a bigger size of the generated models.

- This modeling approach is completely hidden from the control and process engineers and contains enough information for PLC program verification purposes.

Regarding the controlled process, this methodology allows the control and process engineers to add invariants to the formal models, including information about the process. However, it does not include a complete model of the process because it would break one of the main goals of this project: hiding the complexity related to formal methods. Including a complete model of the controlled process would imply to build it manually, as in industry there is normally no formal specification of the controlled process.

Not adding any invariant to the formal model may produce false positives (spurious counterexamples) in the verification phase. False positives do not break the safety of the system, as the user gets a report of an error in the model which does not exist in the real system. However, adding a wrong invariant can hide a bug that may occur in the real PLC program (false negative), which is a much bigger problem than a false positive. Therefore adding invariants to the models is a critical step of the methodology.

In conclusion, we can summarize the controlled process modeling approach of this methodology emphasizing the following aspects:

- Adding invariants is a very simple and useful mechanism. The user of the methodology can include invariants in the models in
order to verify a property. It reduces the number of false positives and it can improve the verification performance (it depends on the implementation of this mechanism in the model checker) as it reduces the RSS.

- Adding a wrong invariant implies false negatives, which is a much more dangerous situation than false positives for our goal of finding bugs in PLC programs.

- This approach does not include a complete model of the controlled process. This is because it would imply to create the model manually, as typically in industry there is no formal specification of the process. Modeling manually the controlled process is a challenging and time consuming task and it could hide potential bugs in the real code due to models that do not represent properly the real processes.

5.4 Evaluation of the PLC program – IM transformation

In this methodology, the transformation rules from the PLC code to the modeling languages of the verification tools are split in two groups: PLC - IM transformation rules, and IM- modeling languages of the verification tools transformation rules.

The first group includes the transformation rules that allow translating ST and SFC programs into the IM, already presented in Section 3.6. These transformations are rule-based and they include several assumptions that simplify the rules and improve the verification performance. Even with these assumptions, the generated models are reliable and they represent with high fidelity the real PLC program.

For example, the assumption 3.6 which assumes the non concurrency of PLC blocks, includes some limitations from the verification point of view as concurrency problems cannot be detected. Currently, the assumptions included in the methodology are related to PLC interrupts, recursion, variable access, function calls, pointers and no parallel branches in the SFC code.

These transformations have been implemented in our CASE tool. This tool is based on EMF and Xtext and the transformations have
been implemented in Java and Xtend. However the complete ST and SFC grammars are not yet included. Currently, the implemented grammars and set of rules cover a large set of the full grammars and it is enough for parsing and translating the UNICOS CPC programs to the IM. One example of the features that are not included is the pointers (the use of pointers is not recommended, although it is not forbidden). These rules and tool can be extended to support the full grammar of ST and SFC languages.

In addition, other programming languages from the IEC 61131 (2013) standard (e.g. IL) can be added to the methodology. Adding new languages to the methodology may imply new specific assumptions related to the new language. For example we could assume that IL instructions are atomic and they cannot be interrupted, although in reality an IL instruction can be compiled is several machine code instructions, therefore an IL instruction can be interrupted.

In conclusion, we can summarize the PLC code - IM transformation rules of this methodology emphasizing the following aspects:

− The proposed transformation rules are implemented in our CASE tool and allow to translate automatically PLC code to the IM without any interaction of the user.

− Currently the PLC grammars and transformation rules implemented in our tool do not cover 100% of the ST and SFC grammars defined by the IEC 61131 (2013) standard. However, they support all the needed features of the UNICOS CPC PLC programs, which is a large subset of the grammars.

− A set of assumptions is included to simplify the transformation rules and improve the verification performance but obtaining reliable models. This assumptions imply some limitations from the verification point of view.

− Currently the methodology includes the transformation rules for ST and SFC languages. Other languages can be included, e.g. IL language.

Time-related transformation rules are analyzed in detail in the following paragraphs as they are a particular case of the transformation of PLC code to IM.
5.4.1 Evaluation of the time-related transformation rules

This methodology provides two different approaches to model PLC time and timers.

If the property contains explicit time in it, a realistic model of PLC time and timers is provided. An example of this kind properties is:

“If $a$ is true, after 5 seconds $b$ will be true, if $a$ remained true.”

If the property does not contain explicit time in it, an abstract model of PLC time and timers is provided. An example of this kind properties is:

“If $a$ is sometime true and remains true forever, eventually $b$ will be true”.

The first approach represents with high fidelity the timer implementation on a real PLC (e.g. TON, TOFF and TP). This representation also implies to model time. The accuracy of the model is high enough, using as unit of logic time 1 ms for timers (as in a real PLC). In terms of specification, this approach allows to express properties with explicit time by using CTL and a monitor. However the resulting state space size is very large. Even if some abstraction techniques are applied, verification time can become very long and in some cases model checkers may not be able to provide a verification result.

The second approach solves the problem of state space explosion by proposing a simplified model of the first approach. The resulting model has a non-deterministic nature, so the accuracy is reduced and it can produce false positives. In terms of specification, it is not possible to verify properties with explicit time, however it can verify properties that guarantee that the timer gives a response (liveness property).

Table 5.1 summarizes the main differences of both approaches.

The first approach is thus needed when properties with explicit time have to be verified although there is a higher chance of having a state explosion problem. The second approach is suitable for timed properties without explicit time, like certain before/after properties (e.g. “the variable $b$ has to be true at the end of the PLC cycle, after the variable $a$ becomes false”), and for non-timed properties (for example safety or liveness properties), where the variables linked to
Table 5.1: Overview of the timer representation approaches from Fernández Adiego et al. (2014a)

<table>
<thead>
<tr>
<th></th>
<th>Realistic</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of PSS</td>
<td>huge (e.g. $5.91 \cdot 10^{15}$) for the TON model</td>
<td>moderate (e.g. 6 for the TON model)</td>
</tr>
<tr>
<td>Requirement expressivity</td>
<td>rich requirements with explicit time, CTL/LTL + monitors</td>
<td>requirements without explicit time, CTL/LTL is enough</td>
</tr>
<tr>
<td>Constraints</td>
<td>time incremented by PLC cycle time</td>
<td>no explicit time, false positives</td>
</tr>
</tbody>
</table>

the property are affected by a timer in the real system and this timer cannot be eliminated by using reduction techniques, such as cone of influence. Although false positive results can occur using this approach, false negative can never occur.

5.5 Evaluation of the reduction techniques

In this methodology, the reduction techniques are applied to the IM and then all the verification tools can profit from these reductions.

Two groups of reduction techniques are currently included in the methodology: the so-called property preserving reduction techniques and the variable abstraction technique.

The first group includes the following reductions: COI, general rule-based reduction and mode selection. By using these reductions the resulting and original models are equivalent for the given property.

The variable abstraction technique produces abstract models that are an overapproximation of the original one. These models are produced based on the variable dependency graph of the variables included in the property to be verified.

The rest of this section presents some measurements to evaluate these reduction techniques.
5.5.1 Property preserving reduction techniques

As it was mentioned in Section 3.7, the theoretical concepts of some of the reduction techniques included in this group are already implemented in many verification tools. A clear example is COI, which is implemented for example in the nuXmv model checker.

However, these algorithms were not really effective on our models, so this was the motivation for implementing them at the IM level, which contains a higher level of information making our algorithms more effective.

The rest of the reduction techniques included in this group are domain specific and they benefit from the PLC domain knowledge.

The experimental results performed in PLC programs corresponding to the UNICOS CPC baseline objects were very satisfactory, but we experienced some limitations when verifying complete UNICOS CPC programs. Sometimes the number of variables kept on the model by COI was very large and the state space of the reduced model was still too large to perform formal verification.

An analysis of effectiveness of these techniques regarding the state space and the run-time reduction is presented in this section. To do so, some measurements are presented, showing how the different reduction techniques can complement each other. The measurements also compare our results with the nuXmv’s reduction techniques.

The measurements correspond with the experimental results applied to the UNICOS CPC object OnOff, presented in Section 4.3.

5.5.2 State space

In the case study presented in Section 4.3, the generated model of the OnOff object has a PSS of $1.61 \cdot 10^{218}$ states without any reductions. Fig. 5.1 shows measurements about the size of the OnOff model PSS without any reduction, using nuXmv’s COI and our COI. The measurements are split in two groups: in the first group, on the left part of the figure, the rule-based reductions are not applied. In the second group, on the right part of the figure, the rule-based reductions are applied. As it can be seen, nuXmv’s COI can reduce the state space significantly, however our implementation provides much better results. In addition, applying the rule-based reductions improves significantly the performance of the reductions. For example, if the
rule-based reductions are enabled, the size of the PSS is \(1.2 \cdot 10^8\) with nuXmv’s COI, and \(4.3 \cdot 10^{26}\) with our own COI implementation.

We can conclude that applying the COI to higher level models, i.e. the IM, significantly improves the reduction performance. In addition, we can observe that by using the rule-based reductions the effectiveness of both COI algorithms (nuXmv and ours) is much higher. In this experiment, formal verification of the given requirement would not have been possible without the rule-based reductions.

### 5.5.3 Verification run-time

The difference between the COI implementations can also be observed on the run-time of the verification. Two tables are presented to compare the effectiveness of our COI implementation on the IM and nuXmv’s COI. These tables show verification run-time measurements and measurements about the internal BDD data structures of nuXmv that represent the state space. In these cases, four different real-life requirements were evaluated:

- Req. 1 is an LTL expression with form of \(G(\alpha \lor U \beta)\).

- Req. 2 and 3 are CTL safety expressions (\(AG(\alpha)\)).

- Req. 4 is a complex LTL expression (\(G((\alpha \land X(\beta \lor U \gamma)) \rightarrow X(\beta \lor U \delta)))\) describing a real requirement coming from the UNICOS developers (it represents a sequence of variable values from different cycles).
In these requirements, the Greek letters represent Boolean logical expressions containing multiple (usually 1–5) variables.

Table 5.2 shows the measurements for the nuXmv’s COI algorithm and Table 5.3 shows the measurements for our COI algorithm.

Without our rule-based reductions (even if nuXmv’s COI is used), none of the requirements could have been verified in a day, thus these reductions are inevitable. These measurements show that by using our COI implementation, the verification run-time can be reduced by 1–3 orders of magnitude compared to the COI of nuXmv. The same reduction can be observed in the number of allocated BDD nodes (#Node). The reduction in the peak number of live BDD nodes (#PNode) is smaller, but significant. This comparison shows the efficiency of the proposed method.

<table>
<thead>
<tr>
<th>Req.</th>
<th>nuXmv COI</th>
<th>Runtime</th>
<th>#PNode</th>
<th>#Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>—</td>
<td>896 s</td>
<td>8.8·10^5</td>
<td>1.8·10^8</td>
</tr>
<tr>
<td>2</td>
<td>—</td>
<td>1,250 s</td>
<td>9.9·10^5</td>
<td>8.8·10^8</td>
</tr>
<tr>
<td>3</td>
<td>—</td>
<td>19,300 s</td>
<td>3.4·10^6</td>
<td>1.6·10^10</td>
</tr>
<tr>
<td>4</td>
<td>—</td>
<td>649 s</td>
<td>9.0·10^5</td>
<td>5.5·10^8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Req.</th>
<th>nuXmv COI</th>
<th>Runtime</th>
<th>#PNode</th>
<th>#Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>—</td>
<td>2.5 s</td>
<td>2.2·10^5</td>
<td>1.1·10^6</td>
</tr>
<tr>
<td>2</td>
<td>—</td>
<td>19.0 s</td>
<td>4.6·10^5</td>
<td>1.4·10^7</td>
</tr>
<tr>
<td>3</td>
<td>—</td>
<td>1,440 s</td>
<td>1.3·10^6</td>
<td>1.6·10^9</td>
</tr>
<tr>
<td>4</td>
<td>—</td>
<td>2.3 s</td>
<td>2.2·10^5</td>
<td>9.2·10^5</td>
</tr>
</tbody>
</table>
5.5. Evaluation of the reduction techniques

5.5.4 Variable abstraction

The last reduction technique included in the methodology, the variable abstraction technique, was designed to give an answer to verification cases when the property preserving reduction techniques were not enough. In our experiments, this situation appeared when verifying full UNICOS PLC programs, such as the one presented in Section 4.4 with 17,500 lines of code and an IM of PSS size of $10^{31985}$ (without reductions). The UNICOS developers provided a set of requirements for these programs. These requirements were safety properties of the following nature: $\text{AG}(\alpha \rightarrow \beta)$, where the Greek letters represent Boolean logical expressions containing multiple (usually up to 5) variables.

For that reason, this iterative abstraction technique was designed with a very aggressive abstraction strategy tailored just for $\text{AG}(\alpha \rightarrow \beta)$ properties. In addition, the algorithm heuristic is easy to automatize and include in our CASE tool.

This technique produces abstract models based on the variable dependency graph. In the PLC program presented in Section 4.4 after applying the properties preserving reduction techniques for the three different requirements, the resulting models have a PSS size around $10^{5048}$.

For the first experiment, the algorithm demonstrated in 45.309 s (including the model generation, the verification time and a timeout of 30 s) that the property holds in the model after one iteration on the algorithm, where one invariant was extracted.

For the second experiment, the algorithm demonstrated in 7.544 s (including the model generation and the verification time) that the requirement holds in the model in the first abstraction.

For the third experiment, the algorithm demonstrated in 126.573 s (including the model generation, the verification time, the counterexample generation and two timeouts of 30 s) that the requirement does not hold in the model using two iterations.

These experimental results show that this algorithm is useful to verify properties in models with a huge PSS. However, this technique has also some limitations:

- The algorithm is restricted to safety properties like $\text{AG}(\alpha \rightarrow \beta)$. This helps to provide an aggressive abstraction strategy.
Extracting invariants is sometimes hopeless when the number of potential invariants \( (m) \) is very high. For that reason, we included the step 5 in the algorithm, which only extracts invariants if for an abstract model \( AM'_x \) corresponding with a \( \delta' = n \), the value of \( m \leq 10 \) (usually this corresponds with \( \delta' \leq 2 \), see an example of the QSDN PLC program on Fig.5.2).

One of the weakness of this method is the step 3, when verifying the reachability property \( r \) on the original model \( OM'' \). If verifying \( p \) on \( OM' \) ended in a timeout, there are a lot of chances of getting also a timeout in this step because the size of the models \( OM' \) and \( OM'' \) may be similar. Bounded model checking seems to be a good alternative to check \( r \) on \( OM'' \), as bounded model checking allows to check properties on a part of the state space. nuXmv includes bounded model checking algorithms, however, the experiments with our models were not successful and the tool crashes with an error after small bounds and no answer were obtained.

To conclude, we have demonstrated that this technique is useful
5.6. Evaluation of the IM – verification tools transformation

for large PLC programs where our property preserving reduction techniques are not enough. But obviously, we can have models where a timeout is obtained when verifying the safety properties $p$ on an abstract model $AM'_{n}$ in any of the iterations $\delta' = n$ of the algorithm. In this situation, no answer is provided and we cannot prove that the counterexamples obtained in previous iterations ($AM'_{n-1}, AM'_{n-2}, \ldots, AM'_{1}$) are real or spurious.

5.6 Evaluation of the IM – verification tools transformation

The intermediate step (IM) on the transformation process from the PLC programs to the modeling languages of the verification tools gives a lot of flexibility to the methodology and new verification tools can easily be added and compared. Currently nuXmv, UPPAAL and BIP are included, and new tools are being investigated, e.g. mCRL2\(^2\) This tool has been developed at the Department of Mathematics and Computer Science of the Technical University of Eindhoven, in collaboration with other institutes.

The selected automata-based formalism for the IM simplifies the transformations from IM to the modeling languages of the verification tools. The current verification tools that are integrated in the methodology have state-based modeling languages. These formalism are very close to the IM formalism, although special strategies have to be applied for each verification, like for example, the synchronization between two automata or modules in nuXmv or how to model global variables in BIP.

Obviously, it is easier to integrate in the methodology state-based modeling languages but different formalisms can be included, e.g. mCRL2 has an action-based modeling language. In this case, transformation rules are more complicated but once the strategy is defined it can be equally automatized.

\(^2\)http://www.mcrl2.org/
5.7 Evaluation of the verification results

The experimental results confirmed that this methodology can be applied to real PLC programs without any knowledge about formal methods. UNICOS CPC baseline objects were verified and even experiments with complete UNICOS PLC programs were performed. These experiments reported many discrepancies between these PLC programs and the specifications. But some other relevant conclusions can be extracted in terms of verification performance. The methodology is flexible and different verification tools can be added and compared. Regarding the verification performance of nuXmv, UPPAAL and BIP, we can extract the following conclusions:

− nuXmv provides the best performance in terms of verification for our models.

− BIP provides an infrastructure for code generation that can be applied for model-based testing and we did some experiments in this direction (see Fernández Adiego et al. (2013b)). The verification solution is very promising for our models as compositional verification algorithms are included, but the verification tool (DFinder) does not support currently data transfer between atoms, therefore it cannot be applied to our models. Future work on this direction is planned.

− UPPAAL provides the best environment for model simulation. However, when big models are automatically generated by our tool, UPPAAL cannot even load and visualize the model. In terms of verification performance, UPPAAL provides worse results than nuXmv for our models.

For that reason, for verification purposes most of the experiments were performed using nuXmv.

Due to multiple model to model transformations, the question whether the methodology itself contains errors arises. Section 5.8 presents a brief discussion on this topic.

However in this last step of the methodology, it can be demonstrated that a bug found in the model also exists in the real PLC code. When a counterexample is produced it can be used to produce a PLC demonstrator and check if this counterexample produces the
expected error in the real code. By doing this, errors in the model to model transformation can be detected without proving mathematically these transformations, always assuming that the PLC compiler and the verification tools do not contain bugs.

5.8 Correctness of our approach

Proving the correctness of all the model transformations is a challenging itself. This would require to prove all the model to model transformations, i.e. the PLC code - IM transformations, the IM reductions and the IM- input languages of every verification tools. But also the correctness of the verification tool itself and the correctness of the PLC compiler as they are all part of the methodology.

Proving the model transformations is possible and ideally this methodology could be certified, however, the huge effort that this implies was not a real option (not a priority at least) at the current stage of this project. For that reason, we adopted a more practical approach where we can prove that a bug, found by the verification tool on the model, really exists in the real PLC program. The counterexample provided by the verification tool can be used to prove its existence on the real PLC code as described in Section 3.11. However, in the following paragraphs the steps to guarantee mathematically the correctness of this approach are sketched.

Possible sources of errors in our verification methodology may detect false positives, i.e. may report errors that do not exist in the real system. On the other hand, it may not detect all errors (false negatives), i.e. state that a property that is intend to hold for a system is verified although it does not hold in the real system. The latter one is more dangerous since it potentially states the correctness of an erroneous system.

To ensure correctness in our methodology, we have to investigate the following potential sources of errors:

1. **Formalization of properties**: Errors can be made when translating an informal requirement into a logical formula suitable for processing in verification tools.

2. **Implementation of verification tools**: The implementation of the model checker may contain errors.
3. **Transformation of models**: The translation from SFC and ST code into the IM, the IM reductions as well as the translation from the IM into nuXmv, BIP and UPPAAL models may contain errors.

4. **Interpretation of verification tool results**: A counterexample may be interpreted in a wrong way.

The error source (1) is addressed by thoroughly analyzing our stated properties. We cannot guarantee the absence of errors in the used verification tools in error source (2), however, the used model checkers are well established and employed in a variety of projects. Error source (4) can be avoided by formulating the properties in a way that they yield simple yes/no answers as verification results.

Regarding the error source (3), it comprises the model transformations that we developed for this work. We sketch the steps to guarantee correctness using mathematical sound proofs. An example of proof can be found in Fernández Adiego et al. (2014a), which it was conducted for proving the correctness of abstraction rules for timers. The correctness proof requires the establishment of formal semantics for the involved languages, i.e. operational semantics (cf. Plotkin (2004) for the classical structured way) for all languages involved: the model checker languages, the IM and the programming languages defined by the IEC 61131 (2013) standard (cf. Blech and Biha (2011) for IL and FBD). A simulation relation between the original and transformed model can be established. States in one model are related with semantical equivalent states in the transformed model. The simulation relation must preserve the properties that we ultimately want to verify (abstractions can alter the classes of properties that are preserved, cf. Bozga et al. (2008)). The correctness proof comprises the verification of a base case stating that the simulation holds for the initial states of the original and transformed model, and a simulation step, stating that if it holds for two states it will also hold for succeeding states.

### 5.9 Summary of the chapter

This chapter presented an analysis of the different steps of the proposed methodology from the completeness, usability, and limitations
5.9. Summary of the chapter

point of view. The experimental results confirm the usability of the proposed methodology on real life PLC programs In addition, the complexity of applying formal methods is completely hidden from the engineers.

This analysis gives also an idea of the future work to be done, which is presented in detail in Chapter 6.
Chapter 6

Conclusions and future work

This final chapter includes the conclusions of this thesis, presenting the list of contributions, limitations and benefits of this research. In addition, a brief discussion about the future work of this project is presented. This chapter is divided in three sections:

− Section 6.1 presents a discussion about the evolution of the thesis, from the initial requirements until the adopted solution to satisfy them.

− Section 6.2 presents the contributions, the limitations and the benefits of this research.

− Finally, Section 6.3 suggests the future research lines of this project.

6.1 Discussion

This research project was set out to provide a solution to one of the main challenges of PLC program developers and designers in the automation industry, a mechanism to guarantee that the PLC code is compliant with the project specification.

This challenge is particularly important for Safety Instrumented Systems, which are in charge of protecting people, environment and installations, as stated in the IEC 61508 (2010) standard. However this is obviously a desirable feature for any control system.
Nowadays in industry, automated and manual testing of PLC programs are the most popular solutions adopted, but some well-known drawbacks are inherent to these approaches.

This thesis provides a solution for applying automated formal verification to PLC programs. At the beginning of the project, two main goals were set to ensure the applicability of this proposal in real-life PLC programs:

1. Hiding any complexity related to formal verification and formal methods from the automation engineers.

2. Being able to verify new and existing PLC programs. This requires that the proposed solution should not modify the development process of any PLC program.

Satisfying these requirements implied to adopt the solution presented in this PhD thesis: a general automated methodology for formal verification of PLC programs. The term “general” stands for a flexible methodology, in which different verification tools can be added to the methodology. The term “automated” indicates that all the internal steps do not require any human intervention.

Formal models for different verification tools are created automatically out of the PLC code. The methodology is based on an intermediate step, the so-called intermediate model (IM), used as a pivot between all the PLC and formal modeling languages included in the methodology. This approach potentially covers all PLC languages. The current implementation supports ST and SFC and the support for IL is under development.

All the steps of the methodology were presented in Chapter 3: requirements formalization, automatic translation of PLC programs to the IM, reduction of the IM, translation of the IM to the modeling languages of the verification tools and finally the counterexample analysis.

The experimental results presented in Chapter 4 show the applicability of this approach in real-life PLC programs. Many discrepancies between the specification and the PLC programs were found during these experiments, even if these programs were previously tested with other techniques.

The practical and theoretical contributions of this methodology are discussed in the following section.
6.2 Contributions

This PhD thesis is not certainly the first attempt to apply formal verification to PLC programs. Section 2.4 showed the related work to this field. However, none of the approaches satisfied completely our initial requirements, or strong limitations were necessary to apply their solutions. The theoretical and practical contributions of this thesis were enumerated in Section 1.3. Here, more details about these contributions are presented according to the experimental results.

6.2.1 Methodology

The first contribution is the adopted methodology itself. The transformation from different PLC languages to different modeling languages of the verification tools, passing through this intermediate step, already exists in other fields of application but is an innovative approach on the industrial automation community, in particular for the PLC environment. Regarding the requirement formalizations, an approach based on patterns can be found before this document as presented in Section 2.4, but in this case, new patterns are provided in this research to cope with the real-life needs from the PLC program developers at CERN. The counterexample analysis and the automatically generated report, which is provided to the engineer when a bug is found, is a practical contribution which is very helpful for control engineers. The model checker usually provides a huge amount of information when a bug is found in a real-life PLC program, but only the relevant information is extracted and provided to the engineer in order to find the source of the problem.

6.2.2 IM syntax and semantics

The definition of the syntax and semantics of the IM is the second contribution. The goal was to provide a simple formalism where all the features of PLC programs can be modeled with this formalism. After the experimental results, no limitations due to the IM expressiveness were found. The adopted assumptions to translate the PLC code into the IM were taken to simplify the transformation rules and to reduce the state space but obtaining meaningful models. In addition, the IM
Chapter 6. Conclusions and future work

formalism is close to the formalisms adopted by several verification tools, simplifying the transformation and therefore facilitating to add new verification tools in order to check their verification performance and simulation facilities for our models.

6.2.3 PLC code - IM transformation rules

The third contribution is the set of transformation rules from ST and SFC languages to the IM. Although the full grammars are not supported yet, the most relevant transformations are presented which fully cover the needs for the transformation of UNICOS CPC PLC programs.

6.2.4 IM- input verification tools transformation rules

Currently three verification tools are supported and compared in the methodology. The transformation from IM to the nuXmv, UPPAAL and BIP are the fourth contribution. The analysis of these three tools, done in Chapter 5, shows that in terms of verification performance, nuXmv provides the best results of the three tools for our models.

6.2.5 Reduction techniques

The reduction and abstraction techniques proposed in this thesis are a fundamental part of the methodology as they allow to apply formal verification to real-life PLC programs. They are the fifth contribution of this thesis. Two groups of reduction techniques are proposed, the property preserving reduction techniques and the variable abstraction technique:

1. For the first group, some of the applied theoretical concepts were previously defined, like Cone of Influence (COI). However, by using the PLC knowledge and applying the reductions to the IM level, a better verification performance than other implementations was achieved. This thesis compares our property preserving reduction techniques with the COI algorithm implemented in nuXmv.
2. The variable abstraction technique is a novel technique which allowed us to verify safety properties, like $\text{AG}(\alpha \rightarrow \beta)$, on the PLC programs where the first group of reductions was not effective by its own. It has some similarities with the CEGAR technique but it differs in the following aspects: the heuristics of this technique are easier to automatize in our methodology, the abstract models are automatically created using the variable dependency graph of the variables included in the requirement and as we target $\text{AG}(\alpha \rightarrow \beta)$ properties, a more aggressive abstraction strategy can be applied.

6.2.6 Modeling the timing aspects of PLCs

The transformation of the timing aspects of PLC programs are part of the set of rules to translate the PLC programs to the IM. This is a very special and challenging aspect for which this thesis gives a solution. This is the sixth contribution of this thesis. Actually two different solutions are proposed depending on the nature of the requirement to be verified. In the first option, time is modeled as a 16-bits variable. Besides, PLC timers (i.e. TON, TOFF and TP) are modeled with a realistic approach, very close to the reality which allows to verify requirements with explicit time in it. The second option does not model time and an abstract model of the timers is provided instead. This approach allows only to check “before/after” timed properties, but the verification performance is significantly better than the previous approach as the state space is much smaller.

6.2.7 PLC behavior analysis

The last contribution of this thesis is the analysis of the internal behavior of PLCs, focusing in Siemens PLCs. This is not a theoretical contribution of this thesis, however this analysis was a fundamental step in the design of the modeling strategy and also in the definition of the semantics of the IM. One example of a large impact on the modeling strategy was the analysis of the timing aspects of PLCs programs, i.e. the $\text{TIME}$ data type and PLC timers. When defining the syntax and semantics of the IM, one option was to provide a timed automata-based formalism, similar to the UPPAAL modeling
language (described in Amnell et al. (2001)), in order to be able to model these timing aspects as some other authors did before. However, after analyzing the internal PLC behavior, the adopted strategy was to use an automata-based formalism. This is a simpler formalism than timed automata and the timing aspects of PLCs can be properly modeled using this modeling strategy (as described in Section 3.9).

6.2.8 Applicability on CERN control systems

In addition to the contributions, this thesis presents the experiments performed on real-life PLC programs. These systems, which were developed at CERN, have significantly large PLC programs and bugs were found on these systems. To the best of the author’s knowledge, none of the previous works presented experimental results with PLC programs of similar size using a completely automated procedure.

The current limitations of this methodology were presented in Chapter 5. Some features, like the support of the full grammar of ST and SFC, impose currently some small restrictions in the methodology. However, this kind of issues are not theoretical limitations and can be solved with a relatively small effort, comparing with the following limitations.

The three main limitations of this methodology are: the state space explosion of the models (common problem in the formal verification domain), the verification of concurrency problems in PLCs and the requirements specification.

The state space explosion problem is still the main limitation in this methodology, as it is for any model checking application. In this approach, when property preserving reductions and the variable abstraction technique do not provide an answer, the limits of this approach are met. Although the experiments show good results in real-life PLC programs, there is obviously room for improvement and extensions in the reduction techniques.

This approach assumes that no concurrency problems can occur in PLC programs. However, concurrency problems may happen in reality, so this approach suggests to check this kind of problems before applying formal verification of the programs. The reason of this assumption is to simplify the transformation rules and improve the
6.3. Future work

The future research work is related to overcome the main drawbacks described before. There are three main research topics among others:

1. Abstraction techniques.
2. Requirement specification.
3. Applying different formal verification algorithms to our models.

The first field is the reduction and abstraction techniques applied to the methodology. New and improved reduction and abstraction techniques (e.g. predicate abstraction) would be necessary to verify any PLC program as an ultimate goal.
Chapter 6  Conclusions and future work

The second field of research is the design of a specification mechanism for control systems. This mechanism has to provide a formal, unambiguous and easy-to-understand language. Nowadays, it does not exist a unified mechanism or language for requirement specification in control systems as there are unified programming languages. In a near future, unified “formal or pseudo-formal” specification mechanisms should be highly recommended by any of the automation standards in order to develop more robust and safe control systems. Having a complete and unambiguous specification will open the door to the “correctness by construction” approach in industrial automation and it could complement the current approach proposed in this thesis, where formal verification can be applied at different levels of the control system development process: at the specification and control code levels, which would reduce the potential bugs of the systems to the minimum.

Finally, a nice feature of this methodology is that different formal verification techniques can be included and their results can be compared. From this point of view, it would be very interesting to check the benefits of the SAT-based techniques on our models. We started to investigate these techniques and the development and results are an ongoing work. Bounded model checking could also improve the verification performance in some cases for our models. In particular, in the variable abstraction technique, one of the current “bottleneck” of this technique is the verification of reachability properties on very large models, bounded model checking is suitable for the reachability analysis. In addition, compositional formal verification seems to be a very promising verification strategy for our models, specially when verifying full UNICOS PLC programs. This research could open the door to the verification of distributed control systems. The BIP framework provides a solution for compositional verification, although the verification tool does not support yet data transfer between components.

As a final conclusion, I consider that the original requirements defined at the beginning of this project were met during this research. The relevance of the practical and theoretical contributions is demonstrated in the experimental results of real-life PLC programs at CERN. The automation and formal methods communities are getting closer
6.3. Future work

thanks to the contributions from this thesis and from other researchers. However, there is still a long way to have formal verification applied extensively in the automation industry. This thesis has triggered new research topics that hopefully will remove the gap once and for all between these two scientific worlds.
Capítulo 7

Conclusiones y trabajo futuro

Este capítulo final incluye las conclusiones de esta tesis, presentando la lista de contribuciones, limitaciones y beneficios de esta investigación. Además, una breve discusión sobre el futuro de este proyecto es presentado. Este capítulo está dividido en tres secciones:

− La Sección 7.1 presenta una discusión sobre la evolución de la tesis, desde los objetivos iniciales hasta la solución adoptada para lograr dichos objetivos.

− La Sección 7.2 presenta las contribuciones, las limitaciones y los beneficios de esta investigación.

− Finalmente, la Sección 7.3 sugiere las futuras líneas de investigación para este proyecto.

7.1 Discusión

Este proyecto de investigación fue diseñado para proporcionar una solución a uno de los principales retos de los diseñadores y desarrolladores de programas PLC en la industria de automatización, un mecanismo para garantizar que el código PLC respete las especificaciones de diseño.

Este reto es particularmente importante para los sistemas de seguridad, encargados de la protección de personas, medioambiente e
instalaciones, tal y como es indicado en el estándar [IEC 61508 (2010)]. Sin embargo, esto es un elemento deseado para cualquier sistema de control.

Hoy en día en industria, testeo automático y manual de los programas PLC son las soluciones adoptadas más populares, pero tienen limitaciones bien conocidas.

Esta tesis propone una solución para el empleo de verificación formal de forma automática en programas PLC. Al principio de este proyecto, dos objetivos principales fueron establecidos para garantizar que esta estrategia sea útil para la verificación de programas PLC reales:

1. Ocultar cualquier dificultad relacionada con tareas de verificación formal a los ingenierios de automatización.

2. Ser capaces de verificar nuevos programas PLC o programas ya existentes. Esto requiere que la metodología propuesta no debería modificar ningún proceso de desarrollo de programas PLC.

Lograr esos objetivos supuso adoptar la solución presentada en esta tesis: una metodología genérica y automatizada para aplicar verificación formal de programas PLC. El término “general” hace referencia a una metodología flexible, en la cual diferentes herramientas de verificación pueden ser incluidas en la metodología. El término “automatizada” indica que las etapas internas no necesitan de intervención humana.

Los modelos formales para diferentes herramientas de verificación son creados de manera automática a partir del código PLC. La metodología esta basada en una etapa intermedia, el llamado modelo intermedio (IM por sus siglas en inglés: Intermediate Model) usado como eje central entre todos los lenguages PLC y de las herramientas de verificación incluidas en la metodología. Esta estrategia puede ser aplicada potencialmente a todos los programas PLC. El estado actual de la metodología incluye los lenguages ST y SFC, el lenguage IL está bajo desarrollo.

Todas las etapas de la metodología son presentadas en el Capítulo formalización de los requerimientos, traducción automática de los programas PLC al IM, reducción del IM, traducción del IM a los lenguages de las herramientas de verificación y finalmente el análisis del contraejemplo.
7.2 Contribuciones

Los resultados experimentales presentados en el capítulo muestran que esta solución es válida para programas PLC reales. Muchas discrepancias entre las especificaciones y los programas PLC fueron encontradas durante estos experimentos, incluso si estos programas fueron testeados con otras técnicas.

Las contribuciones prácticas y teóricas de esta metodología son analizadas en la próxima sección.

7.2 Contribuciones

Esta tesis doctoral no es el primer intento de aplicar verificación formal con programas PLC. La Sección analiza el estado del arte en este campo de investigación. Sin embargo, ninguna de esas propuestas cumplía completamente con los requisitos iniciales de este proyecto, o imponían limitaciones muy grandes en su aplicación. Las contribuciones teóricas y prácticas de esta tesis fueron enumeradas en la Sección. En esta sección, más detalles sobre dichas contribuciones son presentados en base a los resultados experimentales obtenidos.

7.2.1 Metodología

La primera contribución es la propia metodología. La transformación de diferentes lenguajes PLC a diferentes lenguajes de modelado de las herramientas de verificación, pasando por este paso intermedio, ya existe en otros campos de aplicación pero es un enfoque innovador en la comunidad de automación industrial, particularmente en el campo de PLCs. En cuanto a la formalización de los requerimientos, un enfoque basado en patrones puede ser encontrado antes de este documento tal y como es presentado en la Sección pero en este caso nuevos patrones son incluidos en esta investigación para enfrentarse a las necesidades de los sistemas reales desarrollados por los ingenieros de control del CERN. El análisis de los contraejemplos y los informes generados, los cuales se proporcionan al ingeniero cuando un error es encontrado, es una contribución práctica la cual es muy útil para los ingenieros de control. Las herramientas de verificación (model checkers) normalmente proporcionan una gran cantidad de información cuando un error es encontrado en programas de PLC reales, pero solamente
la información relevante es extraída y proporcionada al ingeniero para que pueda encontrar el origen del problema.

7.2.2 Sintaxis y semántica del IM

La definición de la sintaxis y de la semántica del IM es la segunda contribución. El objetivo fue proporcionar un formalismo simple donde todos los aspectos de los programas PLC puedan ser modelados. Después de los resultados experimentales, no se encontraron limitaciones debidas a la expresividad del IM. Las suposiciones adoptadas para traducir el código PLC al IM ayudan a simplificar las reglas de transformación y a reducir el espacio de estados pero consiguiendo modelos adecuados al sistema real. Además, el formalismo del IM es cercano a los formalismos adoptados por varias herramientas de verificación, lo cual simplifica la transformación y por lo tanto facilita la posibilidad de añadir nuevas herramientas de verificación para comprobar cuáles son sus rendimientos y posibilidades de simulación para nuestros modelos.

7.2.3 Reglas de transformación código PLC - IM

La tercera contribución es el conjunto de reglas de transformación de los lenguajes ST y SFC al IM. Aunque las gramáticas completas no han sido incluidas aún, las transformaciones más relevantes son presentadas. Estas reglas de transformación cubren todas las necesidades para transformar programas UNICOS CPC desarrollados en el CERN.

7.2.4 Reglas de transformación IM- modelo para las herramientas de verificación

Actualmente tres herramientas de verificación son incluidas y comparadas en la metodología. La transformación del IM a los lenguajes de modelado de nuXmv, UPPAAL y BIP es la cuarta contribución. El análisis de estas tres herramientas, presentado en el Capítulo 5, muestra que en términos de rendimiento de los algoritmos de verificación, nuXmv proporciona los mejores resultados de las tres herramientas para nuestros modelos.
7.2.5 Técnicas de reducción

Las técnicas de reducción y abstracción propuestas en esta tesis son una parte fundamental de la metodología ya que permiten aplicar verificación formal a programas PLC reales. Estas técnicas son la quinta contribución de esta tesis. Dos grupos de técnicas de reducción son propuestos, las técnicas de reducción que preservan las propiedades y la técnica de abstracción de variables:

1. Para el primer grupo, algunos de los conceptos teóricos de estas técnicas fueron previamente definidos por otros autores, como por ejemplo “Cone of Influence” (COI). Sin embargo, al utilizar el conocimiento del funcionamiento de los PLCs y aplicando estas técnicas en el IM, un mejor rendimiento en términos de verificación fue logrado para nuestros modelos. Esta tesis compara nuestras técnicas de reducción que preservan las propiedades con el algoritmo implementado en nuXmv.

2. La técnica de abstracción de variables es una técnica innovadora la cual permite verificar propiedades de seguridad, como $\text{AG}(\alpha \rightarrow \beta)$, en aquellos programas PLC donde el primer grupo de reducciones no es lo suficientemente efectivo. Tiene ciertas similitudes con la técnica CEGAR pero difiere en los siguientes aspectos: la heurística de esta técnica es más sencilla para ser automatizada en nuestra metodología, los modelos abstractos son creados automáticamente usando el árbol de variables dependientes de las variables incluidas en la propiedad a verificar y como el objetivo es verificar propiedades como $\text{AG}(\alpha \rightarrow \beta)$, una estrategia de abstracción más agresiva puede ser aplicada.

7.2.6 Modelado de los aspectos temporales de los PLCs

La transformación de los aspectos temporales de los programas PLC forman parte del conjunto de reglas para traducir los programas PLC al IM. Esta tesis proporciona una solución para este caso muy particular y complicado de la transformación de programas PLC al IM. Esta es la sexta contribución de esta tesis. Actualmente dos soluciones diferentes son propuestas dependiendo de la naturaleza de la propiedad
que se va a verificar. En la primera opción, el tiempo es modelado como una variable de 16 bits. Además, los temporizadores TON, TOFF y TP son modelados con un enfoque realista muy cercano a la realidad, que permite verificar propiedades que incluyen tiempo explícitamente. La segunda opción por el contrario no modela el tiempo y un modelo abstracto es creado para representar los temporizadores. Este enfoque permite verificar solamente propiedades temporales del tipo “antes/-después”, pero el rendimiento es significativamente mejor que en el enfoque anterior ya que el espacio de estados es mucho menor.

### 7.2.7 Análisis del funcionamiento de un PLC

La última contribución de la tesis es el análisis del funcionamiento interno de un PLC, en particular de Siemens PLCs. No se trata en este caso de una contribución teórica de esta tesis, sin embargo este análisis fue una etapa fundamental en el diseño de la estrategia de modelado y también en la definición de la semántica del IM.

Un ejemplo del gran impacto en dicha estrategia fue el análisis de los aspectos temporales en los programas PLC, es decir, del tipo de dato TIME y de los temporizadores. Cuando se definó la sintaxis y la semántica del IM, una opción era proporcionar un formalismo basado en automata temporizado, similar al lenguaje de modelado de UPPAAL (descrito en [Amnell et al. (2001)]), para poder modelar estos aspectos temporales tal y como otros autores lo propusieron previamente. Sin embargo, después de analizar el funcionamiento interno del PLC, la estrategia adoptada fue usar un formalismo simplemente basado en automata. Este formalismo es más sencillo que el formalismo basado en automata temporizado y los aspectos temporales de los PLCs pueden ser modelados adecuadamente usando esta estrategia (tal y como fue descrita en la Sección [3.9]).

### 7.2.8 Aplicación en sistemas de control desarrollados en el CERN

Además de las contribuciones, esta tesis presenta los experimentos realizados en programas PLC reales. Estos sistemas, los cuales han sido desarrollados en el CERN, tienen programas PLC de un tamaño no muy significativo y errores fueron encontrados en dichos sistemas. En
ninguno de los trabajos encontrados que son previos a esta tesis, los experimentos fueron realizados en programas de la entidad de los experimentos presentados en esta tesis de una manera completamente automatizada.

Las actuales limitaciones de esta metodología fueron presentadas en el Capítulo 5. Algunos aspectos, como incluir la gramática completa de los lenguajes ST y SFC, implica actualmente pequeñas restricciones en la metodología. Sin embargo, este tipo de problemas no son limitaciones teóricas y pueden ser resueltas con un esfuerzo relativamente pequeño, comparado con las siguientes limitaciones.

Las tres principales limitaciones de este metodología son: la explosión de estados de los modelos (problema común en la comunidad de verificación formal), la verificación de problemas de concurrencia en los PLCs y la especificación de los requisitos.

El problema de explosión de estados es aún la principal limitación en esta metodología, tal y como ocurre en cualquier aplicación de model checking. En esta metodología, cuando las técnicas de reducción que preservan las propiedades y la técnica de abstracción de variables no proporcionan ninguna respuesta, el usuario de la misma no obtiene ningún resultado. Aunque los experimentos presentan buenos resultados en programas PLC reales, existe obviamente margen para mejoras y extensiones en las técnicas de reducción.

Esta metodología asume que no pueden ocurrir problemas de concurrencia en los programas PLC. Sin embargo, esos problemas pueden ocurrir en la realidad, por lo que la estrategia recomendada sugiere analizar dichos problemas antes de aplicar verificación formal a los programas. La razón de esta suposición es simplificar las reglas de transformación y mejorar el rendimiento del proceso de verificación. Por ejemplo, si un modelo muy fiel a la implementación real del PLC fuese creado (donde una interrupción puede parar el programa principal en cualquier momento para ser ejecutado), el espacio de estados de los modelos sería enorme y por lo tanto no sería posible aplicar verificación formal a dichos modelos.

La solución a este problema no es trivial. En lugar de verificación formal, esta metodología propone actualmente aplicar diferentes técnicas para analizar los problemas de concurrencia, por ejemplo, técnicas de análisis estático. Para chequear este tipo de propiedades usando
verification formal, probably would be necessary to use different verification tools than those included in today’s methodology. Another possible solution could be to produce more abstract PLC models to be able to analyze this type of properties.

The last, but not the least, great limitation of this methodology is the specification of the functional requirements that the program should meet. The current approach provides patterns to formalize the requirements. This is a useful solution to find PLC program errors, but it is not the final solution for requirement specification in engineering. For example, with this solution, it cannot be guaranteed that the requirement specification is complete. The aim of providing a mechanism to produce a complete, unambiguous, and coherent specification for control systems has not been achieved. Furthermore, the fact that control and process engineers are not usually familiar with formal methods makes this task much more complicated.

7.3 Trabajo futuro

The future research work is oriented to improve or resolve the limitations described above. We can talk about three main research fields:

1. Abstraction techniques.

2. Requirement specification.

3. The application of different verification algorithms.

The first research field is the reduction and abstraction techniques that can be applied to this methodology. New and improved reduction and abstraction techniques (e.g., "predicate abstraction") are necessary so that this methodology could verify any PLC program, which is the final objective of this methodology.

The second research field is the design of a specification mechanism for control systems. This mechanism has
que proporcionar un lenguage sin ambigüedades y fácil de utilizar. Hoy en día, no existe un mecanismo o lenguage para la especificación de requisitos en sistemas de control tal y como existen languages de programación estandarizados. En un futuro cercano, mecanismos de especificación formales o pseudo-formales deberían ser altamente recomendados por los estándares de automática para desarrollar sistemas de control más seguros y robustos. Disponer de una especificación completa y sin ambigüedades significaría la posibilidad de emplear el enfoque de “exactitud en la construcción (correctness by construction)” en la automatización industrial. Esto podría complementar el enfoque actual de esta tesis, donde verificación formal puede ser aplicada en los diferentes niveles del proceso de desarrollo de sistemas de control: en la especificación y el código de control, lo cual reduciría el número de errores potenciales al mínimo.

Finalmente, un factor muy interesante de esta metodología es que permite incluir diferentes técnicas de verificación formal en ella y los resultados pueden ser comparados. Desde este punto de vista, sería muy interesante incluir técnicas de verificación basadas en SAT para nuestros modelos. Durante el desarrollo de esta tesis, empezamos a estudiar estas técnicas y es un trabajo de investigación que va en proceso. “Bounded model checking” podría también mejorar el rendimiento de la verificación de nuestro modelos. En concreto, en la técnica de abstracción de variables, uno de los actuales cuellos de botella de esta técnica es la verificación de propiedades de “reachability” en modelos muy grandes, “bounded model checking” es una técnica adecuada para este tipo de análisis. Además, “compositional formal verification” es una estrategia de verificación muy prometedora para nuestros modelos, especialmente para programs UNICOS CPC. Esta investigación podría abrir la puerta a la verificación formal de sistemas de control distribuidos. La infraestructura de BIP proporciona una solución para “compositional formal verification”, aunque actualmente su herramienta de verificación no permite la transferencia de datos entre componentes.

Como conclusión final, considero que la tesis da una respuesta a los requisitos originales definidos al inicio de este proyecto. La relevancia de las contribuciones tanto teóricas como prácticas ha sido demostrada en los resultados experimentales usando programas PLC desarrollados...
en el CERN. Las comunidades de automática y métodos formales están cada vez más cerca gracias a las contribuciones de esta tesis y las contribuciones de otros investigadores en este mismo campo.

Sin embargo, existe aún un largo camino para disponer de verificación formal aplicada ampliamente en esta industria. El desarrollo de esta tesis ha desencadenado nuevas líneas de investigación que contribuirán a que el espacio que separa estos dos mundos sea eliminado de una vez por todas.
Appendix A

PLC programs

The following piece of ST code corresponds to the Siemens implementation of the OnOff UNICOS CPC object.

```plaintext
//UNICOS
// Copyright CERN 2013 all rights reserved
(* ON/OFF OBJECT FUNCTION BLOCK ***********************)
FUNCTION_BLOCK CPC_FB_ONOFF
TITLE = 'CPC_FB_ONOFF'
//
// ONOFF Object
//
VERSION: '6.5'
AUTHOR: 'EN/ICE'
NAME: 'OBJECT'
FAMILY: 'FO'

VAR_INPUT
  HFOn: BOOL;
  HFOff: BOOL;
  HLD: BOOL;
  IOError: BOOL;
  IOSimu: BOOL;
  AlB: BOOL;
  Manreg01: WORD;
  Manreg01b AT Manreg01: ARRAY [0..15] OF BOOL;
  HOnR: BOOL;
  HOffR: BOOL;
  StartI: BOOL;
  TStopI: BOOL;
  FuStopI: BOOL;
  Al: BOOL;
  AuOnR: BOOL;
  AuOffR: BOOL;
  AuAuMoR: BOOL;
  AuIhMMo: BOOL;
  AuIhFoMo: BOOL;
  AuAlAck: BOOL;
  IhAuMRW: BOOL;
```

259
Appendix A. PLC programs

```plaintext
AuRstart: BOOL;
POnOff: CPC_ONOFF_PARAM;
POnOffb AT POnOff: STRUCT
ParRegb: ARRAY [0..15] OF BOOL;
PPulseLeb: TIME;
PWDb: TIME;
END_STRUCT;
END_VAR
VAR_OUTPUT
Stsreg01: WORD;
Stsreg01b AT Stsreg01: ARRAY [0..15] OF BOOL;
Stsreg02: WORD;
Stsreg02b AT Stsreg02: ARRAY [0..15] OF BOOL;
OutOnOV: BOOL;
OutOffOV: BOOL;
OnSt: BOOL;
OffSt: BOOL;
AuMoSt: BOOL;
MMoSt: BOOL;
LDSt: BOOL;
SoftLDSt: BOOL;
FoMoSt: BOOL;
AuOnRSt: BOOL;
AuOffRSt: BOOL;
MOnRSt: BOOL;
MOffRSt: BOOL;
HOnRSt: BOOL;
HOffRSt: BOOL;
IOErrorW: BOOL;
IOSimuW: BOOL;
AuMRW: BOOL;
AlUnAck: BOOL;
PosW: BOOL;
StartISt: BOOL;
TStopISt: BOOL;
FuStopISt: BOOL;
AlSt: BOOL;
AlBW: BOOL;
EnRstartSt: BOOL := TRUE;
RdyStartSt: BOOL;
END_VAR
VAR //Internal Variables
//Variables for Edge detection
E_MAuMoR: BOOL;
E_MMMoR: BOOL;
E_MFoMoR: BOOL;
E_MOnR: BOOL;
E_MOffR: BOOL;
E_MAlAckR: BOOL;
E_StartI: BOOL;
E_TStopI: BOOL;
E_FuStopI: BOOL;
E_A1: BOOL;
E_AuAuMoR: BOOL;
E_AuAlAck: BOOL;
E_MSoftLDR: BOOL;
E_MEnRstartR: BOOL;
```
RE_AlUnAck: BOOL;
FE_AlUnAck: BOOL;
RE_PulseOn: BOOL;
FE_PulseOn: BOOL;
RE_PulseOff: BOOL;
RE_OutOVSt_aux: BOOL;
FE_OutOVSt_aux: BOOL;
FE_InterlockR: BOOL;

//Variables for old values
MAuMoR_old: BOOL;
MMMoR_old: BOOL;
MFoMoR_old: BOOL;
MOnR_old: BOOL;
MOffR_old: BOOL;
MA1AckR_old: BOOL;
AuAuMoR_old: BOOL;
AuAIAck_old: BOOL;
StartI_old: BOOL;
TStopI_old: BOOL;
FuStopI_old: BOOL;
A1_old: BOOL;
A1UnAck_old: BOOL;
MSoftLDR_old: BOOL;
MEnRstartR_old: BOOL;
RE_PulseOn_old: BOOL;
FE_PulseOn_old: BOOL;
RE_PulseOff_old: BOOL;
RE_OutOVSt_aux_old: BOOL;
FE_OutOVSt_aux_old: BOOL;
FE_InterlockR_old: BOOL;

//General internal variables
PFsPosOn: BOOL;
PFsPosOn2: BOOL;
PHFOn: BOOL;
PHFOff: BOOL;
Pulse: BOOL;
PulseCste: BOOL;
PHLD: BOOL;
PHLCDmd: BOOL;
PAnim: BOOL;
POutOff: BOOL;
PEnRestart: BOOL;
PRestartFS: BOOL;
OutOnOVSt: BOOL;
OutOffOVSt: BOOL;
AuMoSt_aux: BOOL;
MMoSt_aux: BOOL;
FoMoSt_aux: BOOL;
SoftLDSt_aux: BOOL;
PulseOn: BOOL;
PulseOff: BOOL;
PosW_aux: BOOL;
OutOVSt_aux: BOOL;
fullNotAcknowledged: BOOL;
PulseOnR: BOOL;
PulseOffR: BOOL;
Appendix A. PLC programs

InterlockR: BOOL;

//Variables for IEC Timers
Time_Warning: TIME;
Timer_PulseOn: TP;
Timer_PulseOff: TP;
Timer_Warning: TON;

//Variables for interlock Status delay handling
PulseWidth: REAL;
FSIinc: INT;
TSIinc: INT;
SIinc: INT;
Alinc: INT;
WTStopISt: BOOL;
WStartISt: BOOL;
WAlSt: BOOL;
WFuStopISt: BOOL;

BEGIN

E_MAuMoR := R_EDGE(new:=ManReg01b[8],old:=MAuMoR_old); (* Manual Auto Mode Request *)
E_MMMoR := R_EDGE(new:=ManReg01b[9],old:=MMMoR_old); (* Manual Manual Mode Request *)
E_MFoMoR := R_EDGE(new:=ManReg01b[10],old:=MFoMoR_old); (* Manual Forced Mode Request *)
E_MSoftLDR := R_EDGE(new:=ManReg01b[11],old:=MSoftLDR_old); (* Manual Software Local Drive Request *)
E_MOnR := R_EDGE(new:=ManReg01b[12],old:=MOnR_old); (* Manual On/Open Request *)
E_MOffR := R_EDGE(new:=ManReg01b[13],old:=MOffR_old); (* Manual Off/close Request *)
E_MEnRstartR := R_EDGE(new:=ManReg01b[1],old:=MEnRstartR_old); (* Manual Restart after full stop Request *)
E_MA1AckR := R_EDGE(new:=ManReg01b[7],old:=MA1AckR_old); (* Manual Alarm Ack. Request *)

PFsPosOn := POnOffb.ParRegb[8]; (* 1st Parameter bit to define Fail safe position behaviour *)
PHFOn := POnOffb.ParRegb[9]; (* Hardware feedback On present *)
PHFOff := POnOffb.ParRegb[10]; (* Hardware feedback Off present *)
Pulse := POnOffb.ParRegb[11]; (* Object is pulsed pulse duration : POnOff.PulseLe *)
PHLD := POnOffb.ParRegb[12]; (* Local Drive mode Allowed *)
PHLDCmd := POnOffb.ParRegb[13]; (* Local Drive Command allowed *)
PAnim := POnOffb.ParRegb[14]; (* Inverted Output *)
POutOff := POnOffb.ParRegb[15];
PEnRstart := POnOffb.ParRegb[0]; (* Enable Restart after Full Stop *)
PRstartFS := POnOffb.ParRegb[1];
Enable Restart when Full Stop still active *)

PFsPosOn2 := P0nOff.b.ParRegb[2];  (* 2nd Parameter bit to define Fail safe position behaviour *)
PPulseCste := P0nOff.b.ParRegb[3];  (* Pulse Constant duration irrespective of the feedback status *)
E_AuAuMoR := R_EDGE(new:=AuAuMoR,old:=AuAuMoR_old);  (* Auto Mode Request *)
E_AuAlAck := R_EDGE(new:=AuAlAck,old:=AuAlAck_old);  (* Auto Alarm Ack. Request *)

E_StartI := R_EDGE(new:=StartI,old:=StartI_old);
E_TStopI := R_EDGE(new:=TStopI,old:=TStopI_old);
E_FuStopI := R_EDGE(new:=FuStopI,old:=FuStopI_old);
E_A1 := R_EDGE(new:=A1,old:=A1_old);

StartISt := StartI;  (* Start Interlock present *)
TStopISt := TStopI;  (* Temporary Stop Interlock present *)
FuStopISt := FuStopI;  (* Full Stop Interlock present *)

(* INTERLOCK & ACKNOWLEDGE *)

IF (E_MA1AckR OR E_AuAlAck) THEN
  fullNotAcknowledged := FALSE;
  AUnack := FALSE;
ELSIF (E_TStopI OR E_StartI OR E_FuStopI OR E_A1) THEN
  AUnack := TRUE;
END_IF;

IF (PEnRstart AND (E_MEnRstartR OR AuRstart) AND NOT FuStopISt) OR ( PEnRstart AND PRstartFS AND (E_MEnRstartR OR AuRstart) ) AND NOT fullNotAcknowledged THEN
  EnRstartSt := TRUE;
END_IF;

IF E_FuStopI THEN
  fullNotAcknowledged := TRUE;
IF PEnRstart THEN
  EnRstartSt := FALSE;
END_IF;
END_IF;
END_IF;
END_IF;
END_IF;

InterlockR := TStopISt OR FuStopISt OR FullNotAcknowledged OR NOT EnRstartSt OR
  (StartISt AND NOT POutOff AND NOT OutOnOV) OR
  (StartISt AND POutOff AND ((PFsPosOn AND OutOVSt_aux) OR ( NOT PFsPosOn AND NOT OutOVSt_aux)));

FE_InterlockR := F_EDGE (new:=InterlockR,old:=FE_InterlockR_old);

(* MODE MANAGER *)

IF NOT (HLD AND PHLD) THEN
  (* Forced Mode *)
IF (AuMoSt_aux OR MMoSt_aux OR SoftLDSt_aux) AND
E_MFoMoR AND NOT(AuFoMo) THEN
    AuMoSt_aux := FALSE;
    MMoSt_aux := FALSE;
    FoMoSt_aux := TRUE;
    SoftLDSt_aux := FALSE;
END_IF;

(* Manual Mode *)
IF (AuMoSt_aux OR FoMoSt_aux OR SoftLDSt_aux) AND
E_MMMoR AND NOT(AuIhMMo) THEN
    AuMoSt_aux := FALSE;
    MMoSt_aux := TRUE;
    FoMoSt_aux := FALSE;
    SoftLDSt_aux := FALSE;
END_IF;

(* Auto Mode *)
IF (MMoSt_aux AND (E_MAuMoR OR E_AuAuMoR)) OR
(FoMoSt_aux AND E_MAuMoR) OR
(SoftLDSt_aux AND E_MAuMoR) OR
(MMoSt_aux AND AuIhMMo) OR
(FoMoSt_aux AND AuIhFoMo) OR
(SoftLDSt_aux AND AuIhFoMo) OR
NOT(AuMoSt_aux OR MMoSt_aux OR FoMoSt_aux OR SoftLDSt_aux) THEN
    AuMoSt_aux := TRUE;
    MMoSt_aux := FALSE;
    FoMoSt_aux := FALSE;
    SoftLDSt_aux := FALSE;
END_IF;

(* Software Local Mode *)
IF (AuMoSt_aux OR MMoSt_aux) AND E_MSoftLDR AND NOT AuIhFoMo THEN
    AuMoSt_aux := FALSE;
    MMoSt_aux := FALSE;
    FoMoSt_aux := FALSE;
    SoftLDSt_aux := TRUE;
END_IF;

(* Status setting *)
LDSt := FALSE;
AuMoSt := AuMoSt_aux;
MMoSt := MMoSt_aux;
FoMoSt := FoMoSt_aux;
SoftLDSt := SoftLDSt_aux;
ELSE
    (* Local Drive Mode *)
    AuMoSt := FALSE;
    MMoSt := FALSE;
    FoMoSt := FALSE;
    LDSt := TRUE;
    SoftLDSt := FALSE;
END_IF;

(* LIMIT MANAGER *)
(* On/Open Evaluation *)

OnSt:=(HFOn AND PHFOn) OR

(*Feedback ON present*)

(NOT PHFOn AND PHFOff AND PAnim AND NOT HFOff) OR

(*Feedback ON not present and PAnim = TRUE*)

(NOT PHFOn AND NOT PHFOff AND OutOVSt_aux);

(* Off/Closed Evaluation *)

OffSt:=(HFOff AND PHFOff) OR

(*Feedback OFF present*)

(NOT PHFOff AND PHFOn AND PAnim AND NOT HFOn) OR

(*Feedback OFF not present and PAnim = TRUE*)

(NOT PHFOn AND NOT PHFOff AND NOT OutOVSt_aux);

(* REQUEST MANAGER *)

(* Auto On/Off Request*)

IF AuOffR THEN

AuOnRSt := FALSE;
ELSIF AuOnR THEN

AuOnRSt := TRUE;
ELSIF fullNotAcknowledged OR FuStopISt OR NOT EnRstartSt THEN

AuOnRSt := PFsPosOn;
END_IF;

AuOffRSt:= NOT AuOnRSt;

(* Manual On/Off Request*)

IF (((E_MOffR AND (MMoSt OR FoMoSt OR SoftLDSt))

OR (AuOffRSt AND AuMoSt)

OR (LDSt AND PHLDCmd AND HOffRSt)

OR (FE_PulseOn AND PPulse AND NOT POutOff) AND EnRstartSt)

OR (E_FuStopI AND NOT PFsPosOn)) THEN

MOnRSt := FALSE;

ELSIF (((E_MOnR AND (MMoSt OR FoMoSt OR SoftLDSt))

OR (AuOnRSt AND AuMoSt)

OR (LDSt AND PHLDCmd AND HOnRSt) AND EnRstartSt)

OR (E_FuStopI AND PFsPosOn)) THEN

MOnRSt := TRUE;
END_IF;

MOffRSt:= NOT MOnRSt;

(* Local Drive Request *)

IF HOffR THEN

HOnRSt := FALSE;
ELSE IF HOnR THEN

HOnRSt := TRUE;
END_IF;

END_IF;

HOffRSt := NOT(HOnRSt);
Appendix A. PLC programs

(* PULSE REQUEST MANAGER*)

IF PPulse THEN
  IF InterlockR THEN
    PulseOnR := (PFsPosOn AND NOT PFsPosOn2) OR (PFsPosOn AND PFsPosOn2);
    PulseOffR := (NOT PFsPosOn AND NOT PFsPosOn2) OR (PFsPosOn AND PFsPosOn2);
  ELSIF FE_InterlockR THEN
    (*Clear PulseOnR/PulseOffR to be sure you get a new pulse after InterlockR*)
    PulseOnR := FALSE;
    PulseOffR := FALSE;
    Timer_PulseOn (IN:=FALSE,PT:=T#0s);
    Timer_PulseOff (IN:=FALSE,PT:=T#0s);
  ELSIF (MOffRSt AND (MMoSt OR FoMoSt OR SoftLDSt)) OR (AuOffRSt AND AuMoSt) OR (HOffR AND LDSt AND PHLDCmd) THEN  //Off Request
    PulseOnR := FALSE;
    PulseOffR := TRUE;
  ELSIF (MOnRSt AND (MMoSt OR FoMoSt OR SoftLDSt)) OR (AuOnRSt AND AuMoSt) OR (HOnR AND LDSt AND PHLDCmd) THEN  //On Request
    PulseOnR := TRUE;
    PulseOffR := FALSE;
  ELSE
    PulseOnR := FALSE;
    PulseOffR := FALSE;
  END_IF;

  //Pulse functions
  Timer_PulseOn (IN:= PulseOnR,PT:=POnOffb.PPulseLeb);
  Timer_PulseOff (IN:= PulseOffR,PT:=POnOffb.PPulseLeb);
  RE_PulseOn := R_EDGE(new:=PulseOn,old:=RE_PulseOn_old);
  FE_PulseOn := F_EDGE(new:=PulseOn,old:=FE_PulseOn_old);
  RE_PulseOff := R_EDGE(new:=PulseOff,old:=RE_PulseOff_old);

  //The pulse functions have to be reset when changing from On to Off
  IF RE_PulseOn THEN
    Timer_PulseOff (IN:=FALSE,PT:=T#0s);
  END_IF;

  IF RE_PulseOff THEN
    Timer_PulseOn (IN:=FALSE,PT:=T#0s);
  END_IF;

  IF PPulseCste THEN  (* Pulse constant duration irrespective of feedback status *)
    PulseOn := Timer_PulseOn.Q AND NOT PulseOffR;
    PulseOff := Timer_PulseOff.Q AND NOT PulseOnR;
  ELSE
    PulseOn := Timer_PulseOn.Q AND NOT PulseOffR AND (NOT PHFOn OR (PHFOn AND NOT HFOff));
    PulseOff := Timer_PulseOff.Q AND NOT PulseOnR AND (NOT PHFOff OR (PHFOff AND NOT HFOff));
  END_IF;
(* Output On Request *)
outOnOVSt := (PPulse AND PulseOn) OR 
(NOT PPulse AND ((MOnRSt AND (MMoSt OR FomSt OR SoftLDSt )) OR 
(AuOnRSt AND AuMoSt) OR 
(HOnRSt AND LDSt AND PHLDcmd)));

(* Output Off Request *)
IF POutOff THEN
  outOffOVSt := (PulseOff AND PPulse) OR 
  (NOT(PPulse) AND ((MOffRSt AND (MMoSt OR FomSt OR SoftLDSt)) OR (AuOffRSt AND AuMoSt) OR (HOffRSt AND LDSt AND PHLDcmd)));
END_IF;

(* Interlocks / FailSafe *)
IF POutOff THEN
  IF InterlockR THEN
    IF PPulse AND NOT PFsPosOn2 THEN
      IF PFsPosOn THEN
        outOnOVSt := PulseOn;
        outOffOVSt := FALSE;
      ELSE
        outOnOVSt := FALSE;
        outOffOVSt := PulseOff;
      END_IF;
    ELSE
      outOnOVSt := (PFsPosOn AND NOT PFsPosOn2) OR (PFsPosOn AND PFsPosOn2);
      outOffOVSt := (NOT PFsPosOn AND NOT PFsPosOn2) OR (PFsPosOn AND PFsPosOn2);
    END_IF;
  ELSE
    IF InterlockR THEN
      outOnOVSt := PFsPosOn;
    END_IF;
  END_IF;
END_IF;

(* Ready to Start Status *)
RdyStartSt := NOT InterlockR;

(* Alarms *)
AlSt := Al;

(* SURVEILLANCE *)

(* I/O Warning *)
IOErrorW := IOError;
IOSimuW := IOSimu;

(* Auto<> Manual Warning *)
AuMRW := (MMoSt OR FomSt OR SoftLDSt) AND 
((AuOnRSt XOR MOnRSt) OR (AuOffRSt XOR MOffRSt)) AND NOT IhAuMRW;
(* OUTPUT_MANAGER AND OUTPUT REGISTER *)

IF NOT POutOff THEN
  IF PFsPosOn THEN
    OutOnOV := NOT OutOnOVSt;
  ELSE
    OutOnOV := OutOnOVSt;
  END_IF;
ELSE
  OutOnOV := OutOnOVSt;
  OutOffOV := OutOffOVSt;
END_IF;

(* Position warning *)

(* Set reset of the OutOnOVSt *)

IF OutOnOVSt OR (PPulse AND PulseOnR) THEN
  OutOVSt_aux := TRUE;
END_IF;

IF (OutOffOVSt AND POutOff) OR (NOT OutOnOVSt AND NOT POutOff) OR (PPulse AND PulseOffR) THEN
  OutOVSt_aux := FALSE;
END_IF;

RE_OutOVSt_aux := R_EDGE(new:=OutOVSt_aux,old:=RE_OutOVSt_aux_old);
FE_OutOVSt_aux := F_EDGE(new:=OutOVSt_aux,old:=FE_OutOVSt_aux_old);

IF ((OutOVSt_aux AND ((PHFOn AND NOT OnSt) OR (PHFOff AND OffSt)))
  OR (NOT OutOVSt_aux AND ((PHFOff AND NOT OffSt) OR (PHFOn AND OnSt)))
  OR (OffSt AND OnSt))
  AND (NOT PPulse OR (POutOff AND PPulse AND NOT OutOnOV AND NOT OutOffOV))
THEN
  PosW_aux:= TRUE;
END_IF;

IF NOT ((OutOVSt_aux AND ((PHFOn AND NOT OnSt) OR (PHFOff AND OffSt)))
  OR (NOT OutOVSt_aux AND ((PHFOff AND NOT OffSt) OR (PHFOn AND OnSt)))
  OR (OffSt AND OnSt))
OR RE_OutOVSt_aux
OR FE_OutOVSt_aux
OR (PPulse AND POutOff AND OutOnOV)
OR (PPulse AND POutOff AND OutOffOV)
THEN
  PosW_aux := FALSE;
END_IF;

Timer_Warning(IN := PosW_aux,
              PT := POnoffb.PWDb);
PosW := Timer_Warning.Q;
Time_Warning := Timer_Warning.ET;

(* Alarm Blocked Warning *)
AlBW := AlB;

(* Maintain Interlock status 1.5s in Stsreg for PVSS *)

PulseWidth := 1500 (* msec*) / DINT_TO_REAL(TIME_TO_DINT(T_CYCLE));

IF FuStopISt OR FSIinc > 0 THEN
  FSIinc := FSIinc + 1;
  WFuStopISt := TRUE;
END_IF;

IF FSIinc > PulseWidth OR (NOT FuStopISt AND FSIinc = 0) THEN
  FSIinc := 0;
  WFuStopISt := FuStopISt;
END_IF;

IF TStopISt OR TSIinc > 0 THEN
  TSIinc := TSIinc + 1;
  WTStopISt := TRUE;
END_IF;

IF TSIinc > PulseWidth OR (NOT TStopISt AND TSIinc = 0) THEN
  TSIinc := 0;
  WTStopISt := TStopISt;
END_IF;

IF StartISt OR SIinc > 0 THEN
  SIinc := SIinc + 1;
  WStartISt := TRUE;
END_IF;

IF SIinc > PulseWidth OR (NOT StartISt AND SIinc = 0) THEN
  SIinc := 0;
  WStartISt := StartISt;
END_IF;

IF AlSt OR Alinc > 0 THEN
  Alinc := Alinc + 1;
  WAlSt := TRUE;
END_IF;

IF Alinc > PulseWidth OR (NOT AlSt AND Alinc = 0) THEN
  Alinc := 0;
  WAlSt := AlSt;
END_IF;

(* STATUS REGISTER *)

Stsreg01b[8] := OnSt;  // StsReg01 Bit 00
Stsreg01b[9] := OffSt;  // StsReg01 Bit 01
Stsreg01b[10] := AuMoSt;  // StsReg01 Bit 02
Stsreg01b[11] := MMoSt;  // StsReg01 Bit 03
Stsreg01b[12] := FoMoSt;  // StsReg01 Bit 04
Stsreg01b[13] := LDSt;  // StsReg01 Bit 05
Stsreg01b[14] := IOErrorW;  // StsReg01 Bit 06
Appendix A. PLC programs

564  Stsreg01b[15] := IOSimuW; //StsReg01 Bit 07
565  stsreg01b[0] := AuMRW; //StsReg01 Bit 08
566  Stsreg01b[1] := PosW; //StsReg01 Bit 09
567  Stsreg01b[2] := WStartISt; //StsReg01 Bit 10
568  Stsreg01b[3] := WTStopISt; //StsReg01 Bit 11
569  Stsreg01b[4] := AlUnAck; //StsReg01 Bit 12
570  Stsreg01b[5] := AuIhFoMo; //StsReg01 Bit 13
571  Stsreg01b[6] := WA1St; //StsReg01 Bit 14
572  Stsreg01b[7] := AuIhMMo; //StsReg01 Bit 15
573
574  Stsreg02b[8] := OutOnOVSt; //StsReg02 Bit 00
575  Stsreg02b[9] := AuOnRSt; //StsReg02 Bit 01
576  Stsreg02b[10] := MOnRSt; //StsReg02 Bit 02
577  Stsreg02b[11] := AuOffRSt; //StsReg02 Bit 03
578  Stsreg02b[12] := MOffRSt; //StsReg02 Bit 04
579  Stsreg02b[13] := HOnRSt; //StsReg02 Bit 05
580  Stsreg02b[14] := HOffRSt; //StsReg02 Bit 06
581  Stsreg02b[15] := 0; //StsReg02 Bit 07
582  stseg02b[0] := 0; //StsReg02 Bit 08
583  Stsreg02b[1] := 0; //StsReg02 Bit 09
584  Stsreg02b[2] := WFuStopISt; //StsReg02 Bit 10
585  Stsreg02b[3] := EnRstartSt; //StsReg02 Bit 11
586  Stsreg02b[4] := SoftLDSt; //StsReg02 Bit 12
588  Stsreg02b[6] := OutOffOVSt; //StsReg02 Bit 14
589  Stsreg02b[7] := 0; //StsReg02 Bit 15
590
591  (* Edges *)
592  DETECT_EDGE(new:=AlUnAck,old:=AlUnAck_old,re:=RE_AlUnAck,fe:=FE_AlUnAck);
593  END_FUNCTION_BLOCK
594
595  // Common functions for UNICOS applications + implementation of platform FBs.
596  // UNICOS Copyright CERN 2013 all rights reserved
597
598  (* DATA STRUCTURES ***********************************************************)
599  TYPE CPC_DB_PA_STATUS
600    TITLE = 'CPC_DB_PA_STATUS' AUTHOR : 'EN/ICE'
601    FAMILY : 'Base'
602    STRUCT
603      ReadBack : REAL; //position of the valve
604      ReadBack_status : BYTE; //status of readback
605      Pos_D : BYTE; //position discrete
606      Pos_D_Status : BYTE; //status of Pos_D
607      CheckBack0 : BYTE; //checkback status 0
608      CheckBack1 : BYTE; //checkback status 1
609      CheckBack2 : BYTE; //checkback status 2
610    END_STRUCT; END_TYPE
611  TYPE CPC_DB_COMM
612    TITLE = 'CPC_DB_COMM'
613    FAMILY : 'Base'
614    STRUCT
615      ReadBack : REAL; //position of the valve
616      ReadBack_status : BYTE; //status of readback
617      Pos_D : BYTE; //position discrete
618      Pos_D_Status : BYTE; //status of Pos_D
619      CheckBack0 : BYTE; //checkback status 0
620      CheckBack1 : BYTE; //checkback status 1
621      CheckBack2 : BYTE; //checkback status 2
622    END_STRUCT; END_TYPE
FAMILY : 'Base'

STRUCT

  status_DB : INT;
  status_DB_old : INT;
  size : INT;

END_STRUCT

END_TYPE

TYPE CPC_ONOFF_PARAM

TITLE = 'CPC_ONOFF_PARAM'
///
/// Parameters of ONOFF
///

AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'

STRUCT

  ParReg : WORD;
  PPulseLe : TIME;
  PWDt : TIME;

END_STRUCT

END_TYPE

TYPE CPC_LOCAL_PARAM

TITLE = 'CPC_LOCAL_PARAM'
///
/// Parameters of LOCAL
///

AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'

STRUCT

  ParReg : WORD;

END_STRUCT

END_TYPE

TYPE CPC_ANALOGALARM_PARAM

TITLE = 'CPC_ANALOGALARM_PARAM'
///
/// Parameters of Analog Alarm
///

AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'

STRUCT

  ParReg : WORD;

END_STRUCT

END_TYPE

TYPE CPC_PCO_PARAM

TITLE = 'CPC_PCO_PARAM'
///
/// Parameters of PCO
///

AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'

STRUCT

  ParReg : WORD;

END_STRUCT

END_TYPE

TYPE CPC_ANALOG_PARAM
TITLE = 'CPC_ANALOG_PARAM'

//
// Parameters of Analog and Anadig Objects
//
AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'

STRUCT
    ParReg : WORD;
PMaxRan : REAL;
PMinRan : REAL;
PMStpInV : REAL;
PMSpDeV : REAL;
PMInSpd : REAL;
PDDeSpd : REAL;
FWdt : TIME;
FWdb : REAL;
END_STRUCT
END_TYPE

TYPE CPC_ANADIG_PWM_PARAM
TITLE = 'PARAM_PWM'

//
// Parameters of the Pulse Wave Modulation of Anadig objects
/

AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'

STRUCT
    PTPeriod : TIME;
    PTMin : TIME;
    PInMax : REAL;
END_STRUCT
END_TYPE

TYPE CPC_PID_LIB_PARAM
TITLE = 'PARAM_PID_LIB'

//
// Parameters of the PID
/

AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'

STRUCT
    Kc : REAL;
    Ti : REAL;
    Td : REAL;
    Tds : REAL;
    SPH : REAL;
    SPL : REAL;
    OutH : REAL;
    OutL : REAL;
    EKc : BOOL;
    ETi : BOOL;
    ETd : BOOL;
    ETds : BOOL;
    ESPh : BOOL;
    ESPL : BOOL;
    EOutH : BOOL;
    EOutL : BOOL;
TYPE CPC_PID_PARAM
TITLE = 'PARAM_PID'
/
// Parameters of controller objects
/
AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'
STRUCT
PMinRan : REAL;
PMaxRan : REAL;
POutMinRan : REAL;
POutMaxRan : REAL;
MVFilterTime : TIME;
PIDCycle : TIME;
ScaMethod : INT;
RA : BOOL;
END_STRUCT
END_TYPE

TYPE CPC_RAMP_PARAM
TITLE = 'PARAM_RAMP'
/
// Ramp parameters for PID
/
AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'
STRUCT
InSpd : REAL;
DeSpd : REAL;
END_STRUCT
END_TYPE

TYPE CPC_IOERROR
TITLE = 'TYPE_ERR'
/
// Used for IOError in AI/DI/AO/DO
/
AUTHOR : 'EN/ICE'
NAME : 'DataType'
FAMILY : 'Base'
STRUCT
ADDR : REAL;  //Channel Address
Err : BOOL;   //Error
END_STRUCT
END_TYPE

(∗ OTHER FUNCTIONS ************************************************************)

(∗ Version DB∗)
DATA_BLOCK CPC_DB_VERSION
TITLE = 'DB_CPC_VERSION' AUTHOR : 'UNICOS'
NAME : 'Version'
FAMILY : 'Version'
STRUCT
Baseline_version : REAL := 6.6;  //Version of the baseline used
END_STRUCT
BEGIN
END_DATA_BLOCK

(*Rising Edge*)
FUNCTION R_EDGE : BOOL
TITLE = 'R_EDGE'
/
// Detect a Rising Edge on a signal
//
AUTHOR : 'EN/ICE'
NAME : 'Function'
FAMILY : 'Base'
VAR_INPUT
new : BOOL;
END_VAR
VAR_IN_OUT
old : BOOL;
END_VAR
BEGIN
IF (new = 1 AND old = 0) THEN //Raising edge detected
R_EDGE := 1;
old := 1;
ELSE R_EDGE := 0;
old := new;
END_IF;
END_FUNCTION

(*Falling Edge*)
FUNCTION F_EDGE : BOOL
TITLE = 'F_EDGE'
/
// Detect a Falling Edge on a signal
//
AUTHOR : 'EN/ICE'
NAME : 'Function'
FAMILY : 'Base'
VAR_INPUT
new : BOOL;
END_VAR
VAR_IN_OUT
old : BOOL;
END_VAR
BEGIN
IF (new = 0 AND old = 1) THEN //Falling edge detected
F_EDGE := 1;
old := 0;
ELSE F_EDGE := 0;
old := new;
END_IF;
END_FUNCTION

(*Rising and Falling Edge*)
FUNCTION DETECT_EDGE : VOID
TITLE = 'DETECT_EDGE'
/
// Detect a Rising and Falling Edge of a signal

BEGIN
IF (new = 0 AND old = 1) THEN //Falling edge detected
F_EDGE := 1;
old := 0;
ELSE F_EDGE := 0;
old := new;
END_IF;
END_FUNCTION

(*Rising and Falling Edge*)
FUNCTION DETECT_EDGE : VOID
TITLE = 'DETECT_EDGE'
/
// Detect a Rising and Falling Edge of a signal
//
AUTHOR: 'EN/ICE'
NAME: 'Function'
FAMILY: 'Base'

VAR_INPUT
new : BOOL;
END_VAR

VAR_IN_OUT
old : BOOL;
END_VAR

VAR_OUTPUT
re : BOOL;
fe : BOOL;
END_VAR

BEGIN
IF new <> old THEN
  IF new = TRUE THEN // Raising edge
    re := TRUE;
    fe := FALSE;
  ELSE // Falling edge
    re := FALSE;
    fe := TRUE;
  END_IF;
  old := new; // shift new to old
ELSE re := FALSE; // reset edge detection
  fe := FALSE;
END_IF;
END_FUNCTION

// TIMERS

// Pulse timer
FUNCTION_BLOCK TP
VAR_INPUT
PT : TIME;
IN : BOOL;
END_VAR
VAR_OUTPUT
Q : BOOL := FALSE;
ET : TIME;
END_VAR
VAR
running : BOOL;
Start : TIME;
END_VAR
BEGIN
IF Q = FALSE AND running = FALSE THEN
  IF IN THEN
    Start := CT;
    running := TRUE;
    Q := TRUE; // t1
  END_IF;
ELSIF Q = TRUE AND running = TRUE THEN
  IF IN AND (CTIME - (start + PT) >= 0) THEN
    running := FALSE;
  END_IF;
END_FUNCTION
running := TRUE;
Q := FALSE; // t2
ELSIF NOT IN AND (CTIME - (start + PT) >= 0) THEN
  running := FALSE;
  Q := FALSE; // t3
END_IF;
ELSIF Q = FALSE AND running = FALSE THEN
  IF NOT IN THEN
    running := FALSE;
    Q := FALSE; // t4
  END_IF;
END_IF;
END_FUNCTION_BLOCK

// On−delay timer
FUNCTION_BLOCK TON
VAR_INPUT
  PT : TIME;
  IN : BOOL;
END_VAR
VAR_OUTPUT
  Q : BOOL := FALSE;
  ET : TIME; // elapsed time
END_VAR
VAR
  running : BOOL;
  start : BOOL;
END_VAR
BEGIN
  IF IN = FALSE THEN
    Q := FALSE;
    ET := 0;
    running := FALSE; // t1
  ELSIF running = FALSE THEN
    start := CTIME;
    running := TRUE; // t2
  ELSIF CTIME - (start + PT) >= 0 THEN
    Q := TRUE;
    ET := PT; // t3
  ELSE
    IF NOT Q THEN
      ET := CTIME - start;
    END_IF; // t4
  END_IF;
END_FUNCTION_BLOCK

Listing A.1: OnOff PLC program
Appendix B
nuXmv models

The following piece of NuSMV code corresponds to the automatically generated model from the OnOff UNICOS CPC object (without applying any reductions).

```
-- V1.1
-- Generated model from OnOff.scl by bfernand

MODULE module_INSTANCE(interaction, main)

VAR

loc : {initial, end, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 110, 111,
112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124,
125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137,
138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150,
151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163,
164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176,
177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189,
190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 199, 1100, 1101,
1102, 1103, 1104, 1105, 1106, 1107, 1108, 1109, 1110, 1110, 1111,
1112, 1113, 1114, 1115, 1116, 1117, 1118, 1119, 1120, 1121, 1122,
1123, 1124, 1125, 1126, 1127, 1128, 1129, 1130, 1131, 1132, 1133,
1134, 1135, 1136, 1137, 1138, 1139, 1140, 1141, 1142, 1143, 1144,
1145, 1146, 1147, 1148, 1149, 1150, 1151, 1152, 1153, 1154, 1155,
1156, 1157, 1158, 1159, 1160, 1161, 1162, 1163, 1164, 1165,
1166, 1167, 1168, 1169, 1170, 1171, 1172, 1173, 1174, 1175, 1176,
1177, 1178, 1179, 1180, 1181, 1182, 1183, 1184, 1185, 1186, 1187,
1188, 1189, 1190, 1191, 1192, 1193, 1194, 1195, 1196, 1197,
1198, 1199, 1200, 1201, 1202, 1203, 1204, 1205, 1206, 1207, 1208,
1209, 1210, 1211, 1212, 1213, 1214, 1215, 1216, 1217, 1218, 1219,
1220, 1221, 1222, 1223, 1224, 1225, 1226, 1227, 1228, 1229,
1230, 1231, 1232, 1233, 1234, 1235, 1236, 1237, 1238, 1239, 1240,
1241, 1242, 1243, 1244, 1245, 1246, 1247, 1248, 1249, 1250, 1251,
1252, 1253, 1254, 1255, 1256, 1257, 1258, 1259, 1260, 1261,
1262, 1263, 1264, 1265, 1266, 1267, 1268, 1269, 1270, 1271, 1272,
1273, 1274, 1275, 1276, 1277, 1278, 1279, 1280, 1281, 1282, 1283,
1284, 1285, 1286, 1287, 1288, 1289, 1290, 1291, 1292, 1293,
1294, 1295, 1296, 1297, 1298, 1299, 1300, 1301, 1302, 1303, 1304,
1305, 1306, 1307, 1308, 1309, 1310, 1311, 1312, 1313, 1314, 1315,
1316, 1317, 1318, 1319, 1320, 1321, 1322, 1323, 1324, 1325,
```
Appendix B. nuXmv models

1326, 1327, 1328, 1329, 1330, 1331, 1332, 1333, 1334, 1335, 1336, 1337, 1338, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376, 1377, 1378, 1379, 1380, 1381, 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1389, 1390, 1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1440, 1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1127_elsif_1, 1179_elsif_1, 1179_elsif_2, 1184_elsif_1, 1194_elsif_1, 1194_elsif_2, 1194_elsif_3);

7
HFON : boolean;
8
HFOFF : boolean;
9
HLD : boolean;
10
IOERROR : boolean;
11
IOSIMU : boolean;
12
ALB : boolean;
13
MANREG01_0__ : boolean;
14
MANREG01_1__ : boolean;
15
MANREG01_2__ : boolean;
16
MANREG01_3__ : boolean;
17
MANREG01_4__ : boolean;
18
MANREG01_5__ : boolean;
19
MANREG01_6__ : boolean;
20
MANREG01_7__ : boolean;
21
MANREG01_8__ : boolean;
22
MANREG01_9__ : boolean;
23
MANREG01_10__ : boolean;
24
MANREG01_11__ : boolean;
25
MANREG01_12__ : boolean;
26
MANREG01_13__ : boolean;
27
MANREG01_14__ : boolean;
28
MANREG01_15__ : boolean;
29
HONR : boolean;
30
HOFFR : boolean;
31
STARTI : boolean;
32
TSTOPI : boolean;
33
FUSTOPI : boolean;
34
AL : boolean;
35
AUUNR : boolean;
36
AUOFFR : boolean;
37
AUAUMOR : boolean;
38
AUIHMMO : boolean;
39
AUIHFOMO : boolean;
40
AUALACK : boolean;
41
IHAUMRW : boolean;
42
AURSTART : boolean;
43
PONOFF.PARREG_0__ : boolean;
44
PONOFF.PARREG_1__ : boolean;
45
PONOFF.PARREG_2__ : boolean;
46
PONOFF.PARREG_3__ : boolean;
47
PONOFF.PARREG_4__ : boolean;
48
PONOFF.PARREG_5__ : boolean;
49
PONOFF.PARREG_6__ : boolean;
50
PONOFF.PARREG_7__ : boolean;
PONOFF.PARREG_8__ : boolean;
PONOFF.PARREG_9__ : boolean;
PONOFF.PARREG_10__ : boolean;
PONOFF.PARREG_11__ : boolean;
PONOFF.PARREG_12__ : boolean;
PONOFF.PARREG_13__ : boolean;
PONOFF.PARREG_14__ : boolean;
PONOFF.PARREG_15__ : boolean;
PONOFF.PPULSELE : signed word[32];
PONOFF.PWDT : signed word[32];
STSREG01_0__ : boolean;
STSREG01_1__ : boolean;
STSREG01_2__ : boolean;
STSREG01_3__ : boolean;
STSREG01_4__ : boolean;
STSREG01_5__ : boolean;
STSREG01_6__ : boolean;
STSREG01_7__ : boolean;
STSREG01_8__ : boolean;
STSREG01_9__ : boolean;
STSREG01_10__ : boolean;
STSREG01_11__ : boolean;
STSREG01_12__ : boolean;
STSREG01_13__ : boolean;
STSREG01_14__ : boolean;
STSREG01_15__ : boolean;
STSREG02_0__ : boolean;
STSREG02_1__ : boolean;
STSREG02_2__ : boolean;
STSREG02_3__ : boolean;
STSREG02_4__ : boolean;
STSREG02_5__ : boolean;
STSREG02_6__ : boolean;
STSREG02_7__ : boolean;
STSREG02_8__ : boolean;
STSREG02_9__ : boolean;
STSREG02_10__ : boolean;
STSREG02_11__ : boolean;
STSREG02_12__ : boolean;
STSREG02_13__ : boolean;
STSREG02_14__ : boolean;
STSREG02_15__ : boolean;
OUTUNOV : boolean;
OUTUFFOV : boolean;
ONST : boolean;
OFFST : boolean;
AUMOST : boolean;
MMOST : boolean;
LDST : boolean;
SOFTLDST : boolean;
FOMOST : boolean;
AUONRST : boolean;
AUOFFRST : boolean;
MONRST : boolean;
MOFFRST : boolean;
HONRST : boolean;
HOFFRST : boolean;
IOERRORW : boolean;
Appendix B nuXmv models

<table>
<thead>
<tr>
<th>Line</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>109</td>
<td>IOSIMUW : boolean;</td>
</tr>
<tr>
<td>110</td>
<td>AUMRW : boolean;</td>
</tr>
<tr>
<td>111</td>
<td>ALUNACK : boolean;</td>
</tr>
<tr>
<td>112</td>
<td>POSW : boolean;</td>
</tr>
<tr>
<td>113</td>
<td>STARTIST : boolean;</td>
</tr>
<tr>
<td>114</td>
<td>TSTOPIST : boolean;</td>
</tr>
<tr>
<td>115</td>
<td>FUSTOPIST : boolean;</td>
</tr>
<tr>
<td>116</td>
<td>ALST : boolean;</td>
</tr>
<tr>
<td>117</td>
<td>ALBW : boolean;</td>
</tr>
<tr>
<td>118</td>
<td>ENRSTARTST : boolean;</td>
</tr>
<tr>
<td>119</td>
<td>RDYSTARTST : boolean;</td>
</tr>
<tr>
<td>120</td>
<td>E_MAUMOR : boolean;</td>
</tr>
<tr>
<td>121</td>
<td>E_MMMOR : boolean;</td>
</tr>
<tr>
<td>122</td>
<td>E_MFOMOR : boolean;</td>
</tr>
<tr>
<td>123</td>
<td>E_MONR : boolean;</td>
</tr>
<tr>
<td>124</td>
<td>E_MOFFR : boolean;</td>
</tr>
<tr>
<td>125</td>
<td>E_MALACKR : boolean;</td>
</tr>
<tr>
<td>126</td>
<td>E_MSOFTLDR : boolean;</td>
</tr>
<tr>
<td>127</td>
<td>E_MENRSTARTR : boolean;</td>
</tr>
<tr>
<td>128</td>
<td>E_PULSEON : boolean;</td>
</tr>
<tr>
<td>129</td>
<td>E_PULSEOFF : boolean;</td>
</tr>
<tr>
<td>130</td>
<td>E_OUTOVST_AUX : boolean;</td>
</tr>
<tr>
<td>131</td>
<td>E_AL : boolean;</td>
</tr>
<tr>
<td>132</td>
<td>E_AUAUMOR : boolean;</td>
</tr>
<tr>
<td>133</td>
<td>E_AUALACK : boolean;</td>
</tr>
<tr>
<td>134</td>
<td>E_MENRSTARTR : boolean;</td>
</tr>
<tr>
<td>135</td>
<td>RE_ALUNACK : boolean;</td>
</tr>
<tr>
<td>136</td>
<td>RE_PULSEON : boolean;</td>
</tr>
<tr>
<td>137</td>
<td>RE_PULSEOFF : boolean;</td>
</tr>
<tr>
<td>138</td>
<td>RE_OUTOVST_AUX : boolean;</td>
</tr>
<tr>
<td>139</td>
<td>RE_PULSEON : boolean;</td>
</tr>
<tr>
<td>140</td>
<td>RE_PULSEOFF : boolean;</td>
</tr>
<tr>
<td>141</td>
<td>RE_PURGE : boolean;</td>
</tr>
<tr>
<td>142</td>
<td>MAUMOR_OLD : boolean;</td>
</tr>
<tr>
<td>143</td>
<td>MMMOR_OLD : boolean;</td>
</tr>
<tr>
<td>144</td>
<td>MFOMOR_OLD : boolean;</td>
</tr>
<tr>
<td>145</td>
<td>MONR_OLD : boolean;</td>
</tr>
<tr>
<td>146</td>
<td>MOFFR_OLD : boolean;</td>
</tr>
<tr>
<td>147</td>
<td>MALACKR_OLD : boolean;</td>
</tr>
<tr>
<td>148</td>
<td>AUAUMOR_OLD : boolean;</td>
</tr>
<tr>
<td>149</td>
<td>AUALACK_OLD : boolean;</td>
</tr>
<tr>
<td>150</td>
<td>STARTI_OLD : boolean;</td>
</tr>
<tr>
<td>151</td>
<td>TSTOPI_OLD : boolean;</td>
</tr>
<tr>
<td>152</td>
<td>FUSTOPI_OLD : boolean;</td>
</tr>
<tr>
<td>153</td>
<td>AL_OLD : boolean;</td>
</tr>
<tr>
<td>154</td>
<td>ALUNACK_OLD : boolean;</td>
</tr>
<tr>
<td>155</td>
<td>MSOFTLDR_OLD : boolean;</td>
</tr>
<tr>
<td>156</td>
<td>MENRSTARTR_OLD : boolean;</td>
</tr>
<tr>
<td>157</td>
<td>RE_PULSEON_OLD : boolean;</td>
</tr>
<tr>
<td>158</td>
<td>RE_PULSEOFF_OLD : boolean;</td>
</tr>
<tr>
<td>159</td>
<td>RE_PURGE_OLD : boolean;</td>
</tr>
<tr>
<td>160</td>
<td>RE_OUTOVST_AUX_OLD : boolean;</td>
</tr>
<tr>
<td>161</td>
<td>FE_OUTOVST_AUX : boolean;</td>
</tr>
<tr>
<td>162</td>
<td>FE_PULSE : boolean;</td>
</tr>
<tr>
<td>163</td>
<td>FE_PULSE_OLD : boolean;</td>
</tr>
<tr>
<td>164</td>
<td>FE_PULSE : boolean;</td>
</tr>
<tr>
<td>165</td>
<td>PHFON : boolean;</td>
</tr>
<tr>
<td>166</td>
<td>PHFOFF : boolean;</td>
</tr>
</tbody>
</table>
PPULSE : boolean;
PPULSECSTE : boolean;
PHEL : boolean;
PHLDCMD : boolean;
PANIM : boolean;
POUTOFF : boolean;
PENRSTART : boolean;
PRSTARTFS : boolean;
OUTNOVST : boolean;
OUTOFFVST : boolean;
OUTNOVST : boolean;
MMOST_AUX : boolean;
FMOST_AUX : boolean;
SOFTLDST_AUX : boolean;
PULSEON : boolean;
PULSEOFF : boolean;
POSW_AUX : boolean;
OUTOVST_AUX : boolean;
FULLNOTACKNOWLEDGED : boolean;
PULSEONR : boolean;
PULSEOFFR : boolean;
INTERLOCKR : boolean;
TIME_WARNING : signed word[32];
PULSEWIDTH : signed word[32];
FSIINC : signed word[16];
TSIINC : signed word[16];
SIINC : signed word[16];
ALINC : signed word[16];
WTSTOPIST : boolean;
WSTARTIST : boolean;
WALST : boolean;
WFUSTOPIST : boolean;
INLINED_R_EDGE_1__NEW : boolean;
INLINED_R_EDGE_1__OLD : boolean;
INLINED_R_EDGE_2__NEW : boolean;
INLINED_R_EDGE_2__OLD : boolean;
INLINED_R_EDGE_3__NEW : boolean;
INLINED_R_EDGE_3__OLD : boolean;
INLINED_R_EDGE_4__NEW : boolean;
INLINED_R_EDGE_4__OLD : boolean;
INLINED_R_EDGE_5__NEW : boolean;
INLINED_R_EDGE_5__OLD : boolean;
INLINED_R_EDGE_6__NEW : boolean;
INLINED_R_EDGE_6__OLD : boolean;
INLINED_R_EDGE_7__NEW : boolean;
INLINED_R_EDGE_7__OLD : boolean;
INLINED_R_EDGE_8__NEW : boolean;
INLINED_R_EDGE_8__OLD : boolean;
INLINED_R_EDGE_9__NEW : boolean;
INLINED_R_EDGE_9__OLD : boolean;
INLINED_R_EDGE_10__NEW : boolean;
INLINED_R_EDGE_10__OLD : boolean;
INLINED_R_EDGE_11__NEW : boolean;
INLINED_R_EDGE_11__OLD : boolean;
INLINED_R_EDGE_12__NEW : boolean;
INLINED_R_EDGE_12__OLD : boolean;
INLINED_R_EDGE_13__NEW : boolean;
INLINED_R_EDGE_13__OLD : boolean;
INLINED_R_EDGE_14__NEW : boolean;
INLINED_R_EDGE_14__OLD : boolean;
INLINED_F_EDGE_15__NEW : boolean;
INLINED_F_EDGE_15__OLD : boolean;
INLINED_TIMER_PULSEON__PT : signed word[32];
INLINED_TIMER_PULSEON__IN : boolean;
INLINED_TIMER_PULSEON__Q : boolean;
INLINED_TIMER_PULSEON__ET : signed word[32];
INLINED_TIMER_PULSEON__OLD_IN : boolean;
INLINED_TIMER_PULSEON__DUE : signed word[32];

ASSIGN
init(loc) := initial;
next(loc) := case
  loc = end : initial;
  loc = initial : l0;
  loc = l0 : l1;
  loc = l1 : l2;
  loc = l2 & (((INLINED_R_EDGE_1__NEW = TRUE) & (INLINED_R_EDGE_1__OLD = FALSE))) : l3;
  loc = l2 & (!(((INLINED_R_EDGE_1__NEW = TRUE) & (INLINED_R_EDGE_1__OLD = FALSE)))) : l5;
  loc = l3 : l4;
  loc = l4 : l7;
  loc = l5 : l6;
  loc = l6 : l7;
  loc = l7 : l8;
  loc = l8 : l9;
  loc = l9 : l10;
  loc = l10 & (((INLINED_R_EDGE_2__NEW = TRUE) & (INLINED_R_EDGE_2__OLD = FALSE))) : l11;
  loc = l10 & (!(((INLINED_R_EDGE_2__NEW = TRUE) & (INLINED_R_EDGE_2__OLD = FALSE)))) : 111;
loc = 12 & (((INLINED_R_EDGE_1__NEW = TRUE) & (INLINED_R_EDGE_1__OLD = FALSE)));
loc = 12 & (!(((INLINED_R_EDGE_1__NEW = TRUE) & (INLINED_R_EDGE_1__OLD = FALSE))));
loc = 13 : 14;
loc = 14 : 17;
loc = 15 : 16;
loc = 16 : 17;
loc = 17 : 18;
loc = 18 : 19;
loc = 19 : 110;
loc = 110 & (((INLINED_R_EDGE_2__NEW = TRUE) & (INLINED_R_EDGE_2__OLD = FALSE)));
loc = 110 & (!(((INLINED_R_EDGE_2__NEW = TRUE) & (INLINED_R_EDGE_2__OLD = FALSE))));

INLINED_R_EDGE_2__OLD = FALSE)) : l13;
loc = l11 : l12;
loc = l12 : l15;
loc = l13 : l14;
loc = l14 : l15;
loc = l15 : l16;
loc = l16 : l17;
loc = l17 : l18;
loc = l18 & (((INLINED_R_EDGE_3__NEW = TRUE) & (INLINED_R_EDGE_3__OLD = FALSE))) : l19;
loc = l18 & (!(((INLINED_R_EDGE_3__NEW = TRUE) & (INLINED_R_EDGE_3__OLD = FALSE)))) : l21;
loc = l19 : l20;
loc = l20 : l23;
loc = l21 : l22;
loc = l22 : l23;
loc = l23 : l24;
loc = l24 : l25;
loc = l25 : l26;
loc = l26 & (((INLINED_R_EDGE_4__NEW = TRUE) & (INLINED_R_EDGE_4__OLD = FALSE))) : l27;
loc = l26 & (!(((INLINED_R_EDGE_4__NEW = TRUE) & (INLINED_R_EDGE_4__OLD = FALSE)))) : l29;
loc = l27 : l28;
loc = l28 : l31;
loc = l29 : l30;
loc = l30 : l31;
loc = l31 : l32;
loc = l32 : l33;
loc = l33 : l34;
loc = l34 & (((INLINED_R_EDGE_5__NEW = TRUE) & (INLINED_R_EDGE_5__OLD = FALSE))) : l35;
loc = l34 & (!(((INLINED_R_EDGE_5__NEW = TRUE) & (INLINED_R_EDGE_5__OLD = FALSE)))) : l37;
loc = l35 : l36;
loc = l36 : l39;
loc = l37 : l38;
loc = l38 : l39;
loc = l39 : l40;
loc = l40 : l41;
loc = l41 : l42;
loc = l42 & (((INLINED_R_EDGE_7__NEW = TRUE) & (INLINED_R_EDGE_7__OLD = FALSE))) : l43;
loc = l42 & (!(((INLINED_R_EDGE_7__NEW = TRUE) & (INLINED_R_EDGE_7__OLD = FALSE)))) : l45;
loc = l43 : l44;
Appendix B. nuXmv models

loc = l53 : l54;
loc = l54 : l55;
loc = l55 : l56;
loc = l56 : l57;
loc = l57 : l58;
loc = l58 & (((INLINED_R_EDGE_8__NEW = TRUE) & (INLINED_R_EDGE_8__OLD = FALSE))): 159;
loc = l58 & (!((INLINED_R_EDGE_8__NEW = TRUE) & (INLINED_R_EDGE_8__OLD = FALSE))): 161;
loc = l59 : l60;
loc = l60 : l63;
loc = l61 : l62;
loc = l62 : l63;
loc = l63 : l64;
loc = l64 : l65;
loc = l65 : l66;
loc = l66 : l67;
loc = l67 : l68;
loc = l68 : l69;
loc = l69 : l70;
loc = l70 : l71;
loc = l71 : l72;
loc = l72 : l73;
loc = l73 : l74;
loc = l74 : l75;
loc = l75 : l76;
loc = l76 : l77;
loc = l77 : l78;
loc = l78 & (((INLINED_R_EDGE_9__NEW = TRUE) & (INLINED_R_EDGE_9__OLD = FALSE))): 179;
loc = l78 & (!((INLINED_R_EDGE_9__NEW = TRUE) & (INLINED_R_EDGE_9__OLD = FALSE))): 181;
loc = l79 : l80;
loc = l80 : l83;
loc = l81 : l82;
loc = l82 : l83;
loc = l83 : l84;
loc = l84 : l85;
loc = l85 : l86;
loc = l86 & (((INLINED_R_EDGE_10__NEW = TRUE) & (INLINED_R_EDGE_10__OLD = FALSE))): 187;
loc = l86 & (!((INLINED_R_EDGE_10__NEW = TRUE) & (INLINED_R_EDGE_10__OLD = FALSE))): 189;
loc = l87 : l88;
loc = l88 : l91;
loc = l89 : l90;
loc = l90 : l91;
loc = l91 : l92;
loc = l92 : l93;
loc = l93 : l94;
loc = l94 & (((INLINED_R_EDGE_11__NEW = TRUE) & (INLINED_R_EDGE_11__OLD = FALSE))): 195;
loc = l94 & (!((INLINED_R_EDGE_11__NEW = TRUE) & (INLINED_R_EDGE_11__OLD = FALSE))): 197;
loc = l95 : l96;
loc = l96 : l99;
loc = l97 : l98;
loc = l98 : l99;
loc = l99 : l100;
loc = l100 : l101;
loc = l101 : l102;
loc = l102 & (((INLINED_R_EDGE_12__NEW = TRUE) & (INLINED_R_EDGE_12__OLD = FALSE))): l103;
loc = l102 & (!(((INLINED_R_EDGE_12__NEW = TRUE) & (INLINED_R_EDGE_12__OLD = FALSE)))): l105;
loc = l103 : l104;
loc = l104 : l107;
loc = l105 : l106;
loc = l106 : l107;
loc = l107 : l108;
loc = l108 : l109;
loc = l109 : l110;
loc = l110 & (((INLINED_R_EDGE_13__NEW = TRUE) & (INLINED_R_EDGE_13__OLD = FALSE))): l111;
loc = l110 & (!(((INLINED_R_EDGE_13__NEW = TRUE) & (INLINED_R_EDGE_13__OLD = FALSE)))): l113;
loc = l111 : l112;
loc = l112 : l115;
loc = l113 : l114;
loc = l114 : l115;
loc = l115 : l116;
loc = l116 : l117;
loc = l117 : l118;
loc = l118 & (((INLINED_R_EDGE_14__NEW = TRUE) & (INLINED_R_EDGE_14__OLD = FALSE))): l119;
loc = l118 & (!(((INLINED_R_EDGE_14__NEW = TRUE) & (INLINED_R_EDGE_14__OLD = FALSE)))): l121;
loc = l119 : l120;
loc = l120 : l123;
loc = l121 : l122;
loc = l122 : l123;
loc = l123 : l124;
loc = l124 : l125;
loc = l125 : l126;
loc = l126 : l127;
loc = l127 & ((E_MALACKR | E_AUALACK)) : l128;
loc = l127 & (!(E_MALACKR | E_AUALACK)) : l127_elsif_1;
loc = l127_elsif_1 & ((((E_TSTOPI | E_STARTI) | E_FUSTOPI) | E_AL)): l130;
loc = l127_elsif_1 & (!((((E_TSTOPI | E_STARTI) | E_FUSTOPI) | E_AL))): l131;
loc = l128 : l131;
loc = l129 : l131;
loc = l130 : l131;
loc = l131 & ((((PENRSTART & (E_MENRSTARTR | AURSTART)) & !(!FUSTOPIST)): ((PENRSTART & PSTARTFS) & (E_MENRSTARTR | AURSTART)) & !(FULLNOTACKNOWLEDGED))): l132;
loc = l131 & (!((((PENRSTART & (E_MENRSTARTR | AURSTART)) & !(!FUSTOPIST)): ((PENRSTART & PSTARTFS) & (E_MENRSTARTR | AURSTART)) & !(FULLNOTACKNOWLEDGED)))): l133;
loc = l132 : l133;
loc = l133 & (E_FUSTOPI): l134;
loc = l133 & (!(E_FUSTOPI)): l137;
loc = l134 : l135;
loc = l135 & (PENRSTART): l1136;
loc = l135 & (!(PENRSTART)): l1137;
loc = l136 : l137;
loc = l137 : l138;
loc = l138 : l139;
loc = l139 : l140;
loc = l140 & (((INLINE_F_EDGE_15__NEW = FALSE) & (INLINE_F_EDGE_15__OLD = TRUE)) : l141);
loc = l140 & (!((INLINE_F_EDGE_15__NEW = FALSE) & (INLINE_F_EDGE_15__OLD = TRUE))) : l143;
loc = l141 : l142;
loc = l142 : l145;
loc = l143 : l144;
loc = l144 : l145;
loc = l145 : l146;
loc = l146 & (!((HLD & PHLD))) : l147;
loc = l146 & (!(!((HLD & PHLD)))) : l172;
loc = l147 & (((((AUMOST_AUX | MMOST_AUX) | SOFTLDST_AUX) & E_MFOMOR) & !(AUIHFOMO))) : l148;
loc = l147 & (!((((((AUMOST_AUX | MMOST_AUX) | SOFTLDST_AUX) & E_MFOMOR) & !(AUIHFOMO))))) : 1152;
loc = l148 : l149;
loc = l149 : l150;
loc = l150 : l151;
loc = l151 : l152;
loc = l151 & (((((AUMOST_AUX | FOMOST_AUX) | SOFTLDST_AUX) & E_MMMOR) & !(AUIHMMO))) : 1153;
loc = l152 & !((((((MMOST_AUX & (E_MAUMOR | E_AUAUMOR)) | (FOMOST_AUX & E_MAUMOR)) | (SOFTLDST_AUX & E_MAUMOR)) | (MMOST_AUX & AUIHMMO)) | (FOMOST_AUX & AUIHFOMO)) | !((((AUMOST_AUX | MMOST_AUX) | SOFTLDST_AUX)))) : 1158;
loc = l157 & !((((((MMOST_AUX & (E_MAUMOR | E_AUAUMOR)) | (FOMOST_AUX & E_MAUMOR)) | (SOFTLDST_AUX & E_MAUMOR)) | (MMOST_AUX & AUIHMMO)) | (FOMOST_AUX & AUIHFOMO)) | !((((AUMOST_AUX | MMOST_AUX) | SOFTLDST_AUX)))) : 1162;
loc = l158 : l159;
loc = l159 : l160;
loc = l160 : l161;
loc = l161 : l162;
loc = l162 & !(((AUMOST_AUX | MMOST_AUX) & E_MSOFTLDR) & !(AUIHFOMO)) : 1163;
loc = l162 & !(((AUMOST_AUX | MMOST_AUX) & E_MSOFTLDR) & !(AUIHFOMO))) : 1167;
loc = l163 : l164;
loc = l164 : l165;
loc = l165 : l166;
loc = l166 : l167;
loc = l167 : l168;
loc = l168 : l169;
loc = l169 : l170;
loc = l170 : l171;
loc = l171 : l177;
loc = l172 : l173;
loc = l173 : l174;
loc = l174 : l175;
loc = l175 : l176;
loc = l176 : l177;
loc = l177 : l178;
loc = l178 : l179;
loc = l179 & (AUOFFR) : l180;
loc = l179 & (!(!AUOFFR)) : l179_elsif_1;
loc = l179_elsif_1 & (AUONR) : l181;
loc = l179_elsif_1 & (!AUONR) : l179_elsif_2;
loc = l179_elsif_2 & (((FULLNOTACKNOWLEDGED | FUSTOPIST) | !ENRSTARTST)) : l182;
loc = l179_elsif_2 &((FULLNOTACKNOWLEDGED | FUSTOPIST) | !(ENRSTARTST))) : l183;
loc = l180 : l183;
loc = l181 : l183;
loc = l182 : l183;
loc = l183 : l184;
loc = l184 & (((E_MOFFR & ((MMOST | FOMOST) | SOFTLDST)) | (AUOFFRST & AUMOST)) | (LDST & PHLDCMD) & HOFFRST) | (FE_PULSEON & PPULSE) & !(POUTOFF) & ENRSTARTST) | (E_FUSTOPI & !PFSPOSON)) : 1185;
loc = l184 & (((E_MOFFR & ((MMOST | FOMOST) | SOFTLDST)) | (AUOFFRST & AUMOST)) | (LDST & PHLDCMD) & HOFFRST) | (FE_PULSEON & PPULSE) & !(POUTOFF) & ENRSTARTST) | (E_FUSTOPI & !PFSPOSON)) : 1184_elsif_1;
loc = l184_elsif_1 & (((E_MONR & ((MMOST | FOMOST) | SOFTLDST)) | (AUONRST & AUMOST)) | (LDST & PHLDCMD) & HONRST) & ENRSTARTST) | (E_FUSTOPI & PFSPOSON)) : 1186;
loc = l184_elsif_1 & (((E_MONR & ((MMOST | FOMOST) | SOFTLDST)) | (AUONRST & AUMOST)) | (LDST & PHLDCMD) & HONRST) & ENRSTARTST) | (E_FUSTOPI & PFSPOSON)) : 1187;
loc = l185 : l187;
loc = l186 : l187;
loc = l187 : l188;
loc = l188 & (HOFR) : l189;
loc = l188 & (!HOFR) : l190;
loc = l189 : l190;
loc = l190 & (HONR) : l191;
loc = l190 & (!HONR) : l192;
loc = l191 : l192;
loc = l192 : l193;
loc = l193 & (PPULSE) : l194;
loc = l193 & (!PPULSE) : l130;
loc = l194 & (INTERLOCKR) : l195;
loc = l194 & (!INTERLOCKR)) : 1194_elsif_1;
loc = l194_elsif_1 & (FE_INTERLOCKR) : 1197;
loc = l194_elsif_1 & (FE_INTERLOCKR) : 1194_elsif_2;
loc = l194_elsif_2 & (MOFFRST & ((MMOST | FOMOST) | SOFTLDST)) | (AUOFFRST & AUMOST) | (LDST & PHLDCMD) & HOFFRST) : 1223;
loc = l194_elsif_2 & (MOFFRST & ((MMOST | FOMOST) | SOFTLDST)) | (AUOFFRST & AUMOST) | (LDST & PHLDCMD) & HOFFRST) : 1227;
Appendix B. nuXmv models

loc = l195 : l196;
loc = l196 : l229;
loc = l197 : l198;
loc = l198 : l199;
loc = l199 : l200;
loc = l200 : l201;
loc = l201 & (((INLINED_TIMER_PULSEON__IN & !((INLINED_TIMER_PULSEON__OLD_IN)) & !(INLINED_TIMER_PULSEON__Q))) : l202;
loc = l201 & (!(((INLINED_TIMER_PULSEON__IN & !((INLINED_TIMER_PULSEON__OLD_IN)) & !(INLINED_TIMER_PULSEON__Q))) ) : l203;
loc = l202 : l203;
loc = l203 & (main.__GLOBAL_TIME <= INLINED_TIMER_PULSEON__DUE)) : l204;
loc = l203 & (!(main.__GLOBAL_TIME <= INLINED_TIMER_PULSEON__DUE)) : l206;
loc = l204 : l205;
loc = l205 : l210;
loc = l206 : l207;
loc = l207 & (INLINED_TIMER_PULSEON__IN) : l208;
loc = l207 & (!(INLINED_TIMER_PULSEON__IN)) : l209;
loc = l208 : l210;
loc = l209 : l210;
loc = l210 : l211;
loc = l211 : l212;
loc = l212 : l213;
loc = l213 & (((INLINED_TIMER_PULSEOFF__IN & !((INLINED_TIMER_PULSEOFF__OLD_IN)) & !(INLINED_TIMER_PULSEOFF__Q))) : l214;
loc = l213 & (!(((INLINED_TIMER_PULSEOFF__IN & !((INLINED_TIMER_PULSEOFF__OLD_IN)) & !(INLINED_TIMER_PULSEOFF__Q))) ) : l215;
loc = l214 : l215;
loc = l215 & (main.__GLOBAL_TIME <= INLINED_TIMER_PULSEOFF__DUE)) : l216;
loc = l215 & (!(main.__GLOBAL_TIME <= INLINED_TIMER_PULSEOFF__DUE)) : l218;
loc = l216 : l217;
loc = l217 : l222;
loc = l218 : l219;
loc = l219 & (INLINED_TIMER_PULSEOFF__IN) : l220;
loc = l219 & (!(INLINED_TIMER_PULSEOFF__IN)) : l221;
loc = l220 : l222;
loc = l221 : l222;
loc = l222 : l229;
loc = l223 : l224;
loc = l224 : l229;
loc = l225 : l226;
loc = l226 : l229;
loc = l227 : l228;
loc = l228 : l229;
loc = l229 : l230;
loc = l230 : l231;
loc = l231 & (((INLINED_TIMER_PULSEOFF__IN & !((INLINED_TIMER_PULSEOFF__OLD_IN)) & !(INLINED_TIMER_PULSEOFF__Q))) : l232;
loc = l231 & (!(((INLINED_TIMER_PULSEOFF__IN & !((INLINED_TIMER_PULSEOFF__OLD_IN)) & !(INLINED_TIMER_PULSEOFF__Q))) ) : l233;
INLINED_TIMER_PULSEON__OLD_IN)) & !(INLINED_TIMER_PULSEON__Q)))
)
loc = 1232 : 1233;
loc = 1233 & (main.__GLOBAL_TIME <= INLINED_TIMER_PULSEON__DUE)) :
loc = 1233 & !(main.__GLOBAL_TIME <= INLINED_TIMER_PULSEON__DUE)) :
loc = 1234;
loc = 1233 & ((main.__GLOBAL_TIME <= INLINED_TIMER_PULSEON__DUE)) :
loc = 1236;
loc = 1234 : 1235;
loc = 1235 : 1240;
loc = 1236 : 1237;
loc = 1237 & (INLINED_TIMER_PULSEON__IN) : 1238;
loc = 1237 & !(INLINED_TIMER_PULSEON__IN)) : 1239;
loc = 1238 : 1240;
loc = 1239 : 1240;
loc = 1240 : 1241;
loc = 1241 : 1242;
loc = 1242 : 1243;
loc = 1243 : 1244;
loc = 1244 & !(((INLINED_TIMER_PULSEOFF__IN & !(INLINED_TIMER_PULSEOFF__OLD_IN)) & !(INLINED_TIMER_PULSEOFF__Q))) : 1246;
loc = 1244 & !(((INLINED_TIMER_PULSEOFF__IN & !(INLINED_TIMER_PULSEOFF__OLD_IN)) & !(INLINED_TIMER_PULSEOFF__Q))) : 1246;
loc = 1245 : 1246;
loc = 1246 & (main.__GLOBAL_TIME <= INLINED_TIMER_PULSEOFF__DUE)) :
loc = 1247;
loc = 1246 & !(main.__GLOBAL_TIME <= INLINED_TIMER_PULSEOFF__DUE)) :
loc = 1249;
loc = 1247 : 1248;
loc = 1248 : 1253;
loc = 1249 : 1250;
loc = 1250 & (INLINED_TIMER_PULSEOFF__IN) : 1251;
loc = 1250 & !(INLINED_TIMER_PULSEOFF__IN)) : 1252;
loc = 1251 : 1253;
loc = 1252 : 1253;
loc = 1253 : 1254;
loc = 1254 : 1255;
loc = 1255 : 1256;
loc = 1256 : 1257;
loc = 1257 & !(((INLINED_R_EDGE_20__NEW = TRUE) & (INLINED_R_EDGE_20__OLD = FALSE))) : 1258;
loc = 1257 & !(((INLINED_R_EDGE_20__NEW = TRUE) & (INLINED_R_EDGE_20__OLD = FALSE))) : 1258;
loc = 1258 : 1259;
loc = 1259 : 1262;
loc = 1260 : 1261;
loc = 1261 : 1262;
loc = 1262 : 1263;
loc = 1263 : 1264;
loc = 1264 : 1265;
loc = 1265 & !(((INLINED_F_EDGE_21__NEW = FALSE) & (INLINED_F_EDGE_21__OLD = TRUE))) : 1266;
loc = 1265 & !(((INLINED_F_EDGE_21__NEW = FALSE) & (INLINED_F_EDGE_21__OLD = TRUE))) : 1266;
loc = 1266 : 1267;
loc = 1267 : 1270;
loc = 1268 : 1269;
loc = 1269 : 1270;
loc = 1270 : 1271;
loc = 1271 : 1272;
loc = 1272 : 1273;
loc = 1273 & (((INLINED_R_EDGE_22__NEW = TRUE) & (INLINED_R_EDGE_22__OLD = FALSE)) : 1274;
loc = 1273 & !( ((INLINED_R_EDGE_22__NEW = TRUE) & (INLINED_R_EDGE_22__OLD = FALSE)) ) : 1276;
loc = 1274 : 1275;
loc = 1275 : 1278;
loc = 1276 : 1277;
loc = 1277 : 1278;
loc = 1278 : 1279;
loc = 1279 & (RE_PULSEON) : 1280;
loc = 1279 & !(RE_PULSEON)) : 1292;
loc = 1280 : 1281;
loc = 1281 : 1282;
loc = 1282 & (((INLINED_TIMER_PULSEOFF__IN & !(INLINED_TIMER_PULSEOFF__OLD_IN)) & !(INLINED_TIMER_PULSEOFF__Q)) : 1283;
loc = 1282 & !((INLINED_TIMER_PULSEOFF__IN & !(INLINED_TIMER_PULSEOFF__OLD_IN)) & !(INLINED_TIMER_PULSEOFF__Q)) : 1284;
loc = 1283 : 1284;
loc = 1284 & ((main.__GLOBAL_TIME <= INLINED_TIMER_PULSEOFF__DUE)) : 1285;
loc = 1284 & !(main.__GLOBAL_TIME <= INLINED_TIMER_PULSEOFF__DUE)) : 1287;
loc = 1285 : 1286;
loc = 1286 : 1291;
loc = 1287 : 1288;
loc = 1288 & (INLINED_TIMER_PULSEOFF__IN) : 1289;
loc = 1288 & !(INLINED_TIMER_PULSEOFF__IN)) : 1290;
loc = 1289 : 1291;
loc = 1290 : 1291;
loc = 1291 : 1292;
loc = 1292 & (RE_PULSEOFF) : 1293;
loc = 1292 & !(RE_PULSEOFF)) : 1305;
loc = 1293 : 1294;
loc = 1294 : 1295;
loc = 1295 & (((INLINED_TIMER_PULSEON__IN & !(INLINED_TIMER_PULSEON__OLD_IN)) & !(INLINED_TIMER_PULSEON__Q)) : 1296;
loc = 1295 & !((INLINED_TIMER_PULSEON__IN & !(INLINED_TIMER_PULSEON__OLD_IN)) & !(INLINED_TIMER_PULSEON__Q)) : 1297;
loc = 1296 : 1297;
loc = 1297 & ((main.__GLOBAL_TIME <= INLINED_TIMER_PULSEON__DUE)) : 1298;
loc = 1297 & !(main.__GLOBAL_TIME <= INLINED_TIMER_PULSEON__DUE)) : 1300;
loc = 1298 : 1299;
loc = 1299 : 1304;
loc = 1300 : 1301;
loc = 1301 & (INLINED_TIMER_PULSEON__IN) : 1302;
loc = 1301 & !(INLINED_TIMER_PULSEON__IN)) : 1303;
loc = 1302 : 1304;
loc = 1303 : 1304;
loc = l304 : l305;
loc = l305 & (PPULSECSTE) : l306;
loc = l305 & (!$(PPULSECSTE)) : l308;
loc = l306 : l307;
loc = l307 : l310;
loc = l308 : l309;
loc = l309 : l310;
loc = l310 : l311;
loc = l311 & (POUTOFF) : l312;
loc = l311 & (!$(POUTOFF)) : l313;
loc = l312 : l313;
loc = l313 & (POUTOFF) : l314;
loc = l313 & (!$(POUTOFF)) : l315;
loc = l314 : l315;
loc = l314 & (INTERLOCKR) : l315;
loc = l314 & (!$(INTERLOCKR)) : l316;
loc = l315 & (POUTOFF & !(PFSPOSON2)) : l316;
loc = l315 & (!$(POUTOFF & !(PFSPOSON2))) : l317;
loc = l316 & (POUTOFF) : l317;
loc = l316 & (!$(POUTOFF)) : l318;
loc = l317 : l318;
loc = l318 & (PFSPOSON) : l319;
loc = l318 & (!$(PFSPOSON)) : l319;
loc = l320 : l325;
loc = l321 : l325;
loc = l322 : l325;
loc = l323 & (POUTOFF) : l324;
loc = l323 & (!$(POUTOFF)) : l324;
loc = l325 : l326;
loc = l326 : l327;
loc = l326 : l327;
loc = l328 : l329;
loc = l329 : l330;
loc = l330 & (!$(POUTOFF)) : l331;
loc = l330 & (!$(!!(POUTOFF))) : l332;
loc = l331 & (PFSPOSON) : l332;
loc = l331 & (!$(PFSPOSON)) : l333;
loc = l332 : l336;
loc = l333 : l336;
loc = l334 : l336;
loc = l335 : l336;
loc = l336 & (OUTONOVST | (PPULSE & PULSEONR)) : l337;
loc = l336 & (!$((OUTONOVST | (PPULSE & PULSEONR))))) : l338;
loc = l337 : l338;
loc = l338 & (OUTOFFOVST & POUTOFF | (!$(OUTOVST) & !(POUTOFF))) | (PPULSE & PULSEOFFR)) : l339;
loc = l338 & (!$((OUTOFFOVST & POUTOFF) | (!$(OUTOVST) & !(POUTOFF)) | (PPULSE & PULSEOFFR)))) : l340;
loc = l339 : l340;
loc = l340 : l341;
loc = l341 : l342;
loc = l342 & (INLINED_R_EDGE_25__NEW = TRUE) & (INLINED_R_EDGE_25__OLD = FALSE)) : l343;
loc = l342 & (!$((INLINED_R_EDGE_25__NEW = TRUE) & (INLINED_R_EDGE_25__OLD = FALSE)))) : l344;
loc = l343 : l344;
loc = l344 : l347;
loc = l345 : l346;
loc = l378 : l379;
loc = l379 & ((FUSTOPIST | (FSIINC > 0sd16_0))) : l380;
loc = l379 & (!((FUSTOPIST | (FSIINC > 0sd16_0)))) : l382;
loc = l380 : l381;
loc = l381 : l382;
loc = l382 & (((extend(FSIINC, 16) > PULSEWIDTH) | (!FUSTOPIST) & (FSIINC = 0sd16_0))) : l383;
loc = l382 & (!(((extend(FSIINC, 16) > PULSEWIDTH) | (!FUSTOPIST) & (FSIINC = 0sd16_0)))) : l385;
loc = l383 : l384;
loc = l384 : l385;
loc = l385 & ((TSTOPIST | (TSIINC > 0sd16_0))) : l386;
loc = l385 & (!((TSTOPIST | (TSIINC > 0sd16_0)))) : l388;
loc = l386 : l387;
loc = l387 : l388;
loc = l388 & (((extend(TSIINC, 16) > PULSEWIDTH) | (!TSTOPIST) & (TSIINC = 0sd16_0))) : l391;
loc = l388 & (!(((extend(TSIINC, 16) > PULSEWIDTH) | (!TSTOPIST) & (TSIINC = 0sd16_0)))) : l393;
loc = l389 : l390;
loc = l389 : l391;
loc = l391 & ((STARTIST | (SIINC > 0sd16_0))) : l392;
loc = l391 & (!((STARTIST | (SIINC > 0sd16_0)))) : l394;
loc = l392 : l393;
loc = l393 : l394;
loc = l394 & (((extend(SIINC, 16) > PULSEWIDTH) | (!STARTIST) & (SIINC = 0sd16_0))) : l397;
loc = l394 & (!(((extend(SIINC, 16) > PULSEWIDTH) | (!STARTIST) & (SIINC = 0sd16_0)))) : l399;
loc = l395 : l396;
loc = l396 : l397;
loc = l397 & ((ALST | (ALINC > 0sd16_0))) : l398;
loc = l397 & (!((ALST | (ALINC > 0sd16_0)))) : l400;
loc = l398 : l399;
loc = l399 : l400;
loc = l400 & (((extend(ALINC, 16) > PULSEWIDTH) | (!ALST) & (ALINC = 0sd16_0))) : l401;
loc = l400 & (!(((extend(ALINC, 16) > PULSEWIDTH) | (!ALST) & (ALINC = 0sd16_0)))) : l403;
loc = l401 : l402;
loc = l402 : l403;
loc = l403 : l404;
loc = l404 : l405;
loc = l405 : l406;
loc = l406 : l407;
loc = l407 : l408;
loc = l408 : l409;
loc = l409 : l410;
loc = l410 : l411;
loc = l411 : l412;
loc = l412 : l413;
loc = l413 : l414;
loc = l414 : l415;
loc = l415 : l416;
loc = l416 : l417;
loc = l417 : l418;
loc = l418 : l419;
loc = l419 : l420;
loc = l420 : l421;
loc = l421 : l422;
loc = l422 : l423;
loc = l423 : l424;
loc = l424 : l425;
loc = l425 : l426;
loc = l426 : l427;
loc = l427 : l428;
loc = l428 : l429;
loc = l429 : l430;
loc = l430 : l431;
loc = l431 : l432;
loc = l432 : l433;
loc = l433 : l434;
loc = l434 : l435;
loc = l435 : l436;
loc = l436 : l437;
loc = l437 : l438;
loc = l438 : l439;
loc = l439 & ((INLINED_DETECT_EDGE_28__NEW !=
    INLINED_DETECT_EDGE_28__OLD)) : l440;
loc = l439 & (!(((INLINED_DETECT_EDGE_28__NEW !=
    INLINED_DETECT_EDGE_28__OLD))))) : 1446;
loc = l440 & ((INLINED_DETECT_EDGE_28__NEW = TRUE)) : 1441;
loc = l440 & (!(((INLINED_DETECT_EDGE_28__NEW = TRUE))))) : 1443;
loc = l441 : l442;
loc = l442 : l445;
loc = l443 : l444;
loc = l444 : l445;
loc = l445 : l448;
loc = l446 : l447;
loc = l447 : l448;
loc = l448 : l449;
loc = l449 : l450;
loc = l450 : end;
TRUE: loc;
esac;

next(HFON) := case
  loc = initial : {TRUE, FALSE};
  TRUE : HFON;
esac;

next(HFOFF) := case
  loc = initial : {TRUE, FALSE};
  TRUE : HFOFF;
esac;

next(HLD) := case
  loc = initial : {TRUE, FALSE};
  TRUE : HLD;
esac;

next(IOERROR) := case
  loc = initial : {TRUE, FALSE};
  TRUE : IOERROR;
esac;

next(IOSIMU) := case
  loc = initial : {TRUE, FALSE};
  TRUE : IOSIMU;
esac;
next(ALB) := case
  loc = initial : {TRUE, FALSE};
  TRUE : ALB;
esac;
next(MANREG01_0__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_0__;
esac;
next(MANREG01_1__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_1__;
esac;
next(MANREG01_2__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_2__;
esac;
next(MANREG01_3__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_3__;
esac;
next(MANREG01_4__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_4__;
esac;
next(MANREG01_5__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_5__;
esac;
next(MANREG01_6__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_6__;
esac;
next(MANREG01_7__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_7__;
esac;
next(MANREG01_8__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_8__;
esac;
next(MANREG01_9__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_9__;
esac;
next(MANREG01_10__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_10__;
esac;
next(MANREG01_11__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_11__;
esac;
next(MANREG01_12__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : MANREG01_12__;
esac;
next(MANREG01_13__) := case
  loc = initial : {TRUE, FALSE};
TRUE : MANREG01_13__;

esac;
next(MANREG01_14__) := case
loc = initial : {TRUE, FALSE};
TRUE : MANREG01_14__;
esac;
next(MANREG01_15__) := case
loc = initial : {TRUE, FALSE};
TRUE : MANREG01_15__;
esac;
next(HONR) := case
loc = initial : {TRUE, FALSE};
TRUE : HONR;
esac;
next(HOFFR) := case
loc = initial : {TRUE, FALSE};
TRUE : HOFFR;
esac;
next(STARTI) := case
loc = initial : {TRUE, FALSE};
TRUE : STARTI;
esac;
next(TSTOP1) := case
loc = initial : {TRUE, FALSE};
TRUE : TSTOP1;
esac;
next(FUSTOP1) := case
loc = initial : {TRUE, FALSE};
TRUE : FUSTOP1;
esac;
next(AL) := case
loc = initial : {TRUE, FALSE};
TRUE : AL;
esac;
next(AUONR) := case
loc = initial : {TRUE, FALSE};
TRUE : AUONR;
esac;
next(AUOFFR) := case
loc = initial : {TRUE, FALSE};
TRUE : AUOFFR;
esac;
next(AUAUMOR) := case
loc = initial : {TRUE, FALSE};
TRUE : AUAUMOR;
esac;
next(AUIHMMO) := case
loc = initial : {TRUE, FALSE};
TRUE : AUIHMMO;
esac;
next(AUIHFOMO) := case
loc = initial : {TRUE, FALSE};
TRUE : AUIHFOMO;
esac;
next(AUALACK) := case
loc = initial : {TRUE, FALSE};
TRUE : AUALACK;
esac;
next(IHAUMRW) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : IHAUMRW;
esac;
next(AURSTART) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : AURSTART;
esac;
next(PONOFF.PARREG_0__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_0__;
esac;
next(PONOFF.PARREG_1__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_1__;
esac;
next(PONOFF.PARREG_2__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_2__;
esac;
next(PONOFF.PARREG_3__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_3__;
esac;
next(PONOFF.PARREG_4__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_4__;
esac;
next(PONOFF.PARREG_5__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_5__;
esac;
next(PONOFF.PARREG_6__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_6__;
esac;
next(PONOFF.PARREG_7__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_7__;
esac;
next(PONOFF.PARREG_8__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_8__;
esac;
next(PONOFF.PARREG_9__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_9__;
esac;
next(PONOFF.PARREG_10__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_10__;
esac;
next(PONOFF.PARREG_11__) := case
  loc = initial : \{TRUE, FALSE\};
  TRUE : PONOFF.PARREG_11__;
esac;
next(PONOFF.PARREG_12__) := case
  loc = initial : \{TRUE, FALSE\};
TRUE : PONOFF.PARREG_12__; esac;

next(PONOFF.PARREG_13__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : PONOFF.PARREG_13__; esac;

next(PONOFF.PARREG_14__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : PONOFF.PARREG_14__; esac;

next(PONOFF.PARREG_15__) := case
  loc = initial : {TRUE, FALSE};
  TRUE : PONOFF.PARREG_15__; esac;

next(PONOFF.PPULSELE) := case
  loc = initial : main.random_r53;
  TRUE : PONOFF.PPULSELE; esac;

next(PONOFF.PWDT) := case
  loc = initial : main.random_r54;
  TRUE : PONOFF.PWDT; esac;

init(STSREG01_0__) := FALSE;
next(STSREG01_0__) := case
  loc = l411 : AUMRW;
  TRUE : STSREG01_0__; esac;

init(STSREG01_1__) := FALSE;
next(STSREG01_1__) := case
  loc = l412 : POSW;
  TRUE : STSREG01_1__; esac;

init(STSREG01_2__) := FALSE;
next(STSREG01_2__) := case
  loc = l413 : WSTARTIST;
  TRUE : STSREG01_2__; esac;

init(STSREG01_3__) := FALSE;
next(STSREG01_3__) := case
  loc = l414 : WTSTOPIST;
  TRUE : STSREG01_3__; esac;

init(STSREG01_4__) := FALSE;
next(STSREG01_4__) := case
  loc = l415 : ALUNACK;
  TRUE : STSREG01_4__; esac;

init(STSREG01_5__) := FALSE;
next(STSREG01_5__) := case
  loc = l416 : AUIHFOMO;
  TRUE : STSREG01_5__; esac;

init(STSREG01_6__) := FALSE;
next(STSREG01_6__) := case
  loc = l417 : WALST;
  TRUE : STSREG01_6__; esac;

init(STSREG01_7__) := FALSE;
next(STSREG01_7__) := case
  loc = 1418 : AUTHMMD;
  TRUE : STSREG01_7__;
esac;
init(STSREG01_8__) := FALSE;
next(STSREG01_8__) := case
  loc = 1403 : ONST;
  TRUE : STSREG01_8__;
esac;
init(STSREG01_9__) := FALSE;
next(STSREG01_9__) := case
  loc = 1404 : OFFST;
  TRUE : STSREG01_9__;
esac;
init(STSREG01_10__) := FALSE;
next(STSREG01_10__) := case
  loc = 1405 : AUMOST;
  TRUE : STSREG01_10__;
esac;
init(STSREG01_11__) := FALSE;
next(STSREG01_11__) := case
  loc = 1406 : MMOST;
  TRUE : STSREG01_11__;
esac;
init(STSREG01_12__) := FALSE;
next(STSREG01_12__) := case
  loc = 1407 : FOMOST;
  TRUE : STSREG01_12__;
esac;
init(STSREG01_13__) := FALSE;
next(STSREG01_13__) := case
  loc = 1408 : LDST;
  TRUE : STSREG01_13__;
esac;
init(STSREG01_14__) := FALSE;
next(STSREG01_14__) := case
  loc = 1409 : IOERRORW;
  TRUE : STSREG01_14__;
esac;
init(STSREG01_15__) := FALSE;
next(STSREG01_15__) := case
  loc = 1410 : IOSIMUW;
  TRUE : STSREG01_15__;
esac;
init(STSREG02_0__) := FALSE;
next(STSREG02_0__) := case
  loc = 1427 : FALSE;
  TRUE : STSREG02_0__;
esac;
init(STSREG02_1__) := FALSE;
next(STSREG02_1__) := case
  loc = 1428 : FALSE;
  TRUE : STSREG02_1__;
esac;
init(STSREG02_2__) := FALSE;
next(STSREG02_2__) := case
  loc = 1429 : WFUSTOPIST;
  TRUE : STSREG02_2__;
Appendix B nuXmv models

```plaintext
esac;
init(STSREG02_3__) := FALSE;
next(STSREG02_3__) := case
    loc = 1430 : ENRSTARTST;
    TRUE : STSREG02_3__;
esac;
init(STSREG02_4__) := FALSE;
next(STSREG02_4__) := case
    loc = 1431 : SOFTLDST;
    TRUE : STSREG02_4__;
esac;
init(STSREG02_5__) := FALSE;
next(STSREG02_5__) := case
    loc = 1432 : ALBW;
    TRUE : STSREG02_5__;
esac;
init(STSREG02_6__) := FALSE;
next(STSREG02_6__) := case
    loc = 1433 : OUTOFFOVST;
    TRUE : STSREG02_6__;
esac;
init(STSREG02_7__) := FALSE;
next(STSREG02_7__) := case
    loc = 1434 : FALSE;
    TRUE : STSREG02_7__;
esac;
init(STSREG02_8__) := FALSE;
next(STSREG02_8__) := case
    loc = 1419 : OUTONOVST;
    TRUE : STSREG02_8__;
esac;
init(STSREG02_9__) := FALSE;
next(STSREG02_9__) := case
    loc = 1420 : AUONRST;
    TRUE : STSREG02_9__;
esac;
init(STSREG02_10__) := FALSE;
next(STSREG02_10__) := case
    loc = 1421 : MONRST;
    TRUE : STSREG02_10__;
esac;
init(STSREG02_11__) := FALSE;
next(STSREG02_11__) := case
    loc = 1422 : AUOFFRST;
    TRUE : STSREG02_11__;
esac;
init(STSREG02_12__) := FALSE;
next(STSREG02_12__) := case
    loc = 1423 : MOFFRST;
    TRUE : STSREG02_12__;
esac;
init(STSREG02_13__) := FALSE;
next(STSREG02_13__) := case
    loc = 1424 : HONRST;
    TRUE : STSREG02_13__;
esac;
init(STSREG02_14__) := FALSE;
next(STSREG02_14__) := case
```

loc = 1425 : HOFFRST;
   TRUE : STSREG02_14__;
esac;
init(STSREG02_15__) := FALSE;
next(STSREG02_15__) := case
   loc = 1426 : FALSE;
   TRUE : STSREG02_15__;
esac;
init(OUTONOV) := FALSE;
next(OUTONOV) := case
   loc = l332 : !(OUTONOVST);
   loc = l333 : OUTONOVST;
   loc = l334 : OUTONOVST;
   TRUE : OUTONOV;
esac;
init(OUTOFFOV) := FALSE;
next(OUTOFFOV) := case
   loc = l335 : OUTOFFOVST;
   TRUE : OUTOFFOV;
esac;
init(ONST) := FALSE;
next(ONST) := case
   loc = l177 : (((HFON & PHFON) | (((!(PHFON) & PHFOFF) & PANIM) & !HFOFF)) | (((PHFON) & !(PHFOFF)) & OUTOVST_AUX));
   TRUE : ONST;
esac;
init(OFFST) := FALSE;
next(OFFST) := case
   loc = l178 : (((HFOFF & PHFOFF) | (((!(PHFOFF) & PHFON) & PANIM) & !HFON)) | (((PHFON) & !(PHFOFF)) & !(OUTOVST_AUX)));
   TRUE : OFFST;
esac;
init(AUMOST) := FALSE;
next(AUMOST) := case
   loc = l168 : AUMOST_AUX;
   loc = l172 : FALSE;
   TRUE : AUMOST;
esac;
init(MMOST) := FALSE;
next(MMOST) := case
   loc = l169 : MMOST_AUX;
   loc = l173 : FALSE;
   TRUE : MMOST;
esac;
init(LDST) := FALSE;
next(LDST) := case
   loc = l167 : FALSE;
   loc = l175 : TRUE;
   TRUE : LDST;
esac;
init(SOFTLDST) := FALSE;
next(SOFTLDST) := case
   loc = l171 : SOFTLDST_AUX;
   loc = l176 : FALSE;
   TRUE : SOFTLDST;
esac;
init(FOMOST) := FALSE;
next(FOMOST) := case
loc = 1170 : FOMOST_AUX;
loc = 1174 : FALSE;
TRUE : FOMOST;
esac;
init(AUONRST) := FALSE;
next(AUONRST) := case
loc = 1180 : FALSE;
loc = 1181 : TRUE;
loc = 1182 : FOMOST;
TRUE : AUONRST;
esac;
init(AUOFFRST) := FALSE;
next(AUOFFRST) := case
loc = 1183 : !(AUONRST);
TRUE : AUOFFRST;
esac;
init(MONRST) := FALSE;
next(MONRST) := case
loc = 1185 : FALSE;
loc = 1186 : TRUE;
TRUE : MONRST;
esac;
init(MOFFRST) := FALSE;
next(MOFFRST) := case
loc = 1187 : !(MONRST);
TRUE : MOFFRST;
esac;
init(HONRST) := FALSE;
next(HONRST) := case
loc = 1189 : FALSE;
loc = 1191 : TRUE;
TRUE : HONRST;
esac;
init(HOFFRST) := FALSE;
next(HOFFRST) := case
loc = 1192 : !(HONRST);
TRUE : HOFFRST;
esac;
init(IOERRORW) := FALSE;
next(IOERRORW) := case
loc = 1327 : IOERROR;
TRUE : IOERRORW;
esac;
init(IOSIMUW) := FALSE;
next(IOSIMUW) := case
loc = 1328 : IOSIMU;
TRUE : IOSIMUW;
esac;
init(AUMRW) := FALSE;
next(AUMRW) := case
loc = 1329 : (((FOMOST | FOMOST) | SOFTLDST) & ((AUONRST xor MONRST)
| (AUOFFRST xor MOFFRST))) & !(IHAUMRW));
TRUE : AUMRW;
esac;
init(ALUNACK) := FALSE;
next(ALUNACK) := case
loc = 1129 : FALSE;
loc = 1130 : TRUE;
TRUE : ALUNACK;
esac;
init(POSW) := FALSE;
next(POSW) := case
loc = 1375 : INLINED_TIMER_WARNING__Q;
TRUE : POSW;
esac;
init(STARTIST) := FALSE;
next(STARTIST) := case
loc = l124 : STARTI;
TRUE : STARTIST;
esac;
init(TSTOPIST) := FALSE;
next(TSTOPIST) := case
loc = l125 : TSTOPI;
TRUE : TSTOPIST;
esac;
init(ALST) := FALSE;
next(ALST) := case
loc = l326 : AL;
TRUE : ALST;
esac;
init(ALBW) := FALSE;
next(ALBW) := case
loc = l377 : ALB;
TRUE : ALBW;
esac;
init(ENRSTARTST) := TRUE;
next(ENRSTARTST) := case
loc = 1132 : TRUE;
loc = 1136 : FALSE;
TRUE : ENRSTARTST;
esac;
init(RDYSTARTST) := FALSE;
next(RDYSTARTST) := case
loc = 1325 : !(INTERLOCKR);
TRUE : RDYSTARTST;
esac;
init(E_MAUMOR) := FALSE;
next(E_MAUMOR) := case
loc = 13 : TRUE;
loc = 15 : FALSE;
TRUE : E_MAUMOR;
esac;
init(E_MMMOR) := FALSE;
next(E_MMMOR) := case
loc = 111 : TRUE;
loc = 113 : FALSE;
TRUE : E_MMMOR;
esac;
init(E_MFOMOR) := FALSE;
next(E_MFOMOR) := case
loc = 119 : TRUE;
loc = l121 : FALSE;
TRUE : E_MFOMOR;
esac;
init(E_MONR) := FALSE;
next(E_MONR) := case
loc = l135 : TRUE;
loc = l137 : FALSE;
TRUE : E_MONR;
esac;
init(E_MOFFR) := FALSE;
next(E_MOFFR) := case
loc = l143 : TRUE;
loc = l145 : FALSE;
TRUE : E_MOFFR;
esac;
init(E_MALACKR) := FALSE;
next(E_MALACKR) := case
loc = l159 : TRUE;
loc = l161 : FALSE;
TRUE : E_MALACKR;
esac;
init(E_STARTI) := FALSE;
next(E_STARTI) := case
loc = l195 : TRUE;
loc = l197 : FALSE;
TRUE : E_STARTI;
esac;
init(E_TSTOPI) := FALSE;
next(E_TSTOPI) := case
loc = l1103 : TRUE;
loc = l1105 : FALSE;
TRUE : E_TSTOPI;
esac;
init(E_FUSTOPI) := FALSE;
next(E_FUSTOPI) := case
loc = l1111 : TRUE;
loc = l1113 : FALSE;
TRUE : E_FUSTOPI;
esac;
init(E_AL) := FALSE;
next(E_AL) := case
loc = l1119 : TRUE;
loc = l1121 : FALSE;
TRUE : E_AL;
esac;
init(E_AUAUMOR) := FALSE;
next(E_AUAUMOR) := case
loc = l179 : TRUE;
loc = l181 : FALSE;
TRUE : E_AUAUMOR;
esac;
init(E_AUALACK) := FALSE;
next(E_AUALACK) := case
loc = l187 : TRUE;
loc = l189 : FALSE;
TRUE : E_AUALACK;
esac;
init(E_MSOFTLDR) := FALSE;
next(E_MSOFTLDR) := case
    loc = 127 : TRUE;
    loc = 129 : FALSE;
    TRUE : E_MSOFTLDR;
esac;
init(E_MENRSTARTR) := FALSE;
next(E_MENRSTARTR) := case
    loc = 151 : TRUE;
    loc = 153 : FALSE;
    TRUE : E_MENRSTARTR;
esac;
init(RE_ALUNACK) := FALSE;
next(RE_ALUNACK) := case
    loc = 1449 : INLINED_DETECT_EDGE_28__RE;
    TRUE : RE_ALUNACK;
esac;
init(FE_ALUNACK) := FALSE;
next(FE_ALUNACK) := case
    loc = 1258 : TRUE;
    loc = 1260 : FALSE;
    TRUE : FE_ALUNACK;
esac;
init(RE_PULSEON) := FALSE;
next(RE_PULSEON) := case
    loc = 1274 : TRUE;
    loc = 1276 : FALSE;
    TRUE : RE_PULSEON;
esac;
init(RE_OUTOVST_AUX) := FALSE;
next(RE_OUTOVST_AUX) := case
    loc = 1343 : TRUE;
    loc = 1345 : FALSE;
    TRUE : RE_OUTOVST_AUX;
esac;
init(MAUMOR_OLD) := FALSE;
next(MAUMOR_OLD) := case
    loc = 17 : INLINED_R_EDGE_1__OLD;
    TRUE : MAUMOR_OLD;
esac;
init(MMOMOR_OLD) := FALSE;
next(MMOMOR_OLD) := case
    loc = 115 : INLINED_R_EDGE_2__OLD;
    TRUE : MMOMOR_OLD;
esac;
init(MFOMOR_OLD) := FALSE;
next(MFOMOR_OLD) := case
    loc = 123 : INLINED_R_EDGE_3__OLD;
    TRUE : MFOMOR_OLD;
esac;
init(MONR_OLD) := FALSE;
next(MONR_OLD) := case
    loc = 139 : INLINED_R_EDGE_5__OLD;
    TRUE : MONR_OLD;
esac;
init(MOFFR_OLD) := FALSE;
next(MOFFR_OLD) := case
    loc = 147 : INLINED_R_EDGE_6__OLD;
    TRUE : MOFFR_OLD;
esac;
init(MALACKR_OLD) := FALSE;
next(MALACKR_OLD) := case
    loc = 163 : INLINED_R_EDGE_8__OLD;
    TRUE : MALACKR_OLD;
esac;
init(AUAUMOR_OLD) := FALSE;
next(AUAUMOR_OLD) := case
    loc = 183 : INLINED_R_EDGE_9__OLD;
    TRUE : AUAUMOR_OLD;
esac;
init(AUALACK_OLD) := FALSE;
next(AUALACK_OLD) := case
    loc = 191 : INLINED_R_EDGE_10__OLD;
    TRUE : AUALACK_OLD;
esac;
init(STARTI_OLD) := FALSE;
next(STARTI_OLD) := case
    loc = 199 : INLINED_R_EDGE_11__OLD;
    TRUE : STARTI_OLD;
esac;
init(TSTOPI_OLD) := FALSE;
next(TSTOPI_OLD) := case
    loc = 1107 : INLINED_R_EDGE_12__OLD;
    TRUE : TSTOPI_OLD;
esac;
init(FUSTOPI_OLD) := FALSE;
next(FUSTOPI_OLD) := case
    loc = 1115 : INLINED_R_EDGE_13__OLD;
    TRUE : FUSTOPI_OLD;
esac;
init(AL_OLD) := FALSE;
next(AL_OLD) := case
    loc = 1123 : INLINED_R_EDGE_14__OLD;
    TRUE : AL_OLD;
esac;
init(ALUNACK_OLD) := FALSE;
next(ALUNACK_OLD) := case
   loc = 1448 : INLINED_DETECT_EDGE_28__OLD;
   TRUE : ALUNACK_OLD;
esac;
init(MSOFTLDR_OLD) := FALSE;
next(MSOFTLDR_OLD) := case
   loc = 131 : INLINED_R_EDGE_4__OLD;
   TRUE : MSOFTLDR_OLD;
esac;
init(MENRSTARTR_OLD) := FALSE;
next(MENRSTARTR_OLD) := case
   loc = 155 : INLINED_R_EDGE_7__OLD;
   TRUE : MENRSTARTR_OLD;
esac;
init(RE_PULSEON_OLD) := FALSE;
next(RE_PULSEON_OLD) := case
   loc = 1262 : INLINED_R_EDGE_20__OLD;
   TRUE : RE_PULSEON_OLD;
esac;
init(RE_PULSEOFF_OLD) := FALSE;
next(RE_PULSEOFF_OLD) := case
   loc = 1278 : INLINED_R_EDGE_22__OLD;
   TRUE : RE_PULSEOFF_OLD;
esac;
init(RE_OUTOVST_AUX_OLD) := FALSE;
next(RE_OUTOVST_AUX_OLD) := case
   loc = 1347 : INLINED_R_EDGE_25__OLD;
   TRUE : RE_OUTOVST_AUX_OLD;
esac;
init(FE_PULSEON_OLD) := FALSE;
next(FE_PULSEON_OLD) := case
   loc = 1270 : INLINED_F_EDGE_21__OLD;
   TRUE : FE_PULSEON_OLD;
esac;
init(FE_OUTOVST_AUX_OLD) := FALSE;
next(FE_OUTOVST_AUX_OLD) := case
   loc = 1355 : INLINED_F_EDGE_26__OLD;
   TRUE : FE_OUTOVST_AUX_OLD;
esac;
init(FE_INTERLOCKR_OLD) := FALSE;
next(FE_INTERLOCKR_OLD) := case
   loc = 1145 : INLINED_F_EDGE_15__OLD;
   TRUE : FE_INTERLOCKR_OLD;
esac;
init(PFSPOSON) := FALSE;
next(PFSPOSON) := case
   loc = 164 : PONOFF.PARREG_8__;
   TRUE : PFSPOSON;
esac;
init(PFSPOSON2) := FALSE;
next(PFSPOSON2) := case
   loc = 174 : PONOFF.PARREG_2__;
   TRUE : PFSPOSON2;
esac;
init(PHFON) := FALSE;
next(PHFON) := case
loc = 165 : PONGOFF.PARREG_9__; TRUE : PHFON;

init(PHFOFF) := FALSE;
next(PHFOFF) := case
  loc = 166 : PONGOFF.PARREG_10__; TRUE : PHFOFF;
  esac;

init(PPULSE) := FALSE;
next(PPULSE) := case
  loc = 167 : PONGOFF.PARREG_11__; TRUE : PPULSE;
  esac;

init(PPULSECSTE) := FALSE;
next(PPULSECSTE) := case
  loc = 175 : PONGOFF.PARREG_3__; TRUE : PPULSECSTE;
  esac;

init(PHLD) := FALSE;
next(PHLD) := case
  loc = 168 : PONGOFF.PARREG_12__; TRUE : PHLD;
  esac;

init(PHLDCMD) := FALSE;
next(PHLDCMD) := case
  loc = 169 : PONGOFF.PARREG_13__; TRUE : PHLDCMD;
  esac;

init(PANIM) := FALSE;
next(PANIM) := case
  loc = 170 : PONGOFF.PARREG_14__; TRUE : PANIM;
  esac;

init(POUTOFF) := FALSE;
next(POUTOFF) := case
  loc = 171 : PONGOFF.PARREG_15__; TRUE : POUTOFF;
  esac;

init(PENRSTART) := FALSE;
next(PENRSTART) := case
  loc = 172 : PONGOFF.PARREG_0__; TRUE : PENRSTART;
  esac;

init(PRSTARTFS) := FALSE;
next(PRSTARTFS) := case
  loc = 173 : PONGOFF.PARREG_1__; TRUE : PRSTARTFS;
  esac;

init(OUTONOVST) := FALSE;
next(OUTONOVST) := case
  loc = 1310 : ((PPULSE & PULSEON) | !(PPULSE) & (((MONRST & ((MMOST | FOMOST) | SOFTLDST)) | (AUONRST & AUMOST)) | ((MONRST & LDST) & PHLDCMD)));
  loc = 1317 : PULSEON;
  loc = 1319 : FALSE;
  loc = 1321 : ((PFSPOSON & !(PFSPOSON2)) | (PFSPOSON & PFSPOSON2));
  loc = 1324 : PFSPOSON;
  TRUE : OUTONOVST;
esac;

init(OUTOFFOVST) := FALSE;

next(OUTOFFOVST) := case
    loc = 1312 : ((PULSEOFF & PPULSE) | (!PPULSE) & (((MOFFRST & ((MMOST | FOMOST) | SOFTLDS)) | (AUOFFRST & AUMOST)) | ((HOFFRST & LDST) & PHLDMC));
    loc = 1318 : FALSE;
    loc = 1320 : PULSEOFF;
    loc = 1322 : (!PFSPSON & !PFSPSON2) | (PFSPSON & PFSPSON2));

    TRUE : OUTOFFOVST;

esac;

init(AUMOST_AUX) := FALSE;

next(AUMOST_AUX) := case
    loc = 148 : FALSE;
    loc = 153 : FALSE;
    loc = 158 : TRUE;
    loc = 163 : FALSE;
    TRUE : AUMOST_AUX;

esac;

init(MMOST_AUX) := FALSE;

next(MMOST_AUX) := case
    loc = 149 : FALSE;
    loc = 154 : TRUE;
    loc = 159 : FALSE;
    loc = 164 : FALSE;
    TRUE : MMOST_AUX;

esac;

init(FOMOST_AUX) := FALSE;

next(FOMOST_AUX) := case
    loc = 150 : TRUE;
    loc = 155 : FALSE;
    loc = 160 : FALSE;
    loc = 165 : FALSE;
    TRUE : FOMOST_AUX;

esac;

init(SOFTLDST_AUX) := FALSE;

next(SOFTLDST_AUX) := case
    loc = 151 : FALSE;
    loc = 156 : FALSE;
    loc = 161 : FALSE;
    loc = 166 : TRUE;
    TRUE : SOFTLDST_AUX;

esac;

init(PULSEON) := FALSE;

next(PULSEON) := case
    loc = 1306 : ((INLINED_TIMER_PULSEON__Q & !PULSEOFFR));
    loc = 1308 : ((INLINED_TIMER_PULSEON__Q & !PULSEOFFR) & ((PHFON) | (PHFON & !HFOFF)));
    TRUE : PULSEON;

esac;

init(PULSEOFF) := FALSE;

next(PULSEOFF) := case
    loc = 1307 : ((INLINED_TIMER_PULSEOFF__Q & !PULSEONR));
    loc = 1309 : ((INLINED_TIMER_PULSEOFF__Q & !PULSEONR) & ((PHOFF) | (PHOFF & !PHOFF)));
    TRUE : PULSEOFF;

esac;
init(POSW_AUX) := FALSE;
next(POSW_AUX) := case
    loc = 1357 : TRUE;
    loc = 1359 : FALSE;
    TRUE : POSW_AUX;
esac;
init(OUTOVST_AUX) := FALSE;
next(OUTOVST_AUX) := case
    loc = 1337 : TRUE;
    loc = 1339 : FALSE;
    TRUE : OUTOVST_AUX;
esac;
init(FULLNOTACKNOWLEDGED) := FALSE;
next(FULLNOTACKNOWLEDGED) := case
    loc = 1128 : FALSE;
    loc = 1134 : TRUE;
    TRUE : FULLNOTACKNOWLEDGED;
esac;
init(PULSEONR) := FALSE;
next(PULSEONR) := case
    loc = 1195 : ((PFSPOSON & !(PFSPOSON2)) | (PFSPOSON & PFSPOSON2));
    loc = 1197 : FALSE;
    loc = 1223 : FALSE;
    loc = 1225 : TRUE;
    loc = 1227 : FALSE;
    loc = 1241 : INLINED_TIMER_PULSEON__IN;
    TRUE : PULSEONR;
esac;
init(PULSEOFFR) := FALSE;
next(PULSEOFFR) := case
    loc = 1196 : (((PFSPOSON) & !(PFSPOSON2)) | (PFSPOSON & PFSPOSON2))
    ;
    loc = 1198 : FALSE;
    loc = 1224 : TRUE;
    loc = 1226 : FALSE;
    loc = 1228 : FALSE;
    loc = 1254 : INLINED_TIMER_PULSEOFF__IN;
    TRUE : PULSEOFFR;
esac;
init(INTERLOCKR) := FALSE;
next(INTERLOCKR) := case
    loc = 1137 : ((((({TSTOPIST | FUSTOPIST) | FULLNOTACKNOWLEDGED} | !(EHSTARTST)) | ((STARTIST & !(POUTOFF)) & !(OUTONOV))) | ((STARTIST & POUTOFF) & ((PFSPOSON & OUTOVST_AUX) | (!(PFSPOSON) & !(OUTOVST_AUX))))));
    TRUE : INTERLOCKR;
esac;
init(TIME_WARNING) := 0sd32_0;
next(TIME_WARNING) := case
    loc = 1376 : INLINED_TIMER_WARNING__ET;
    TRUE : TIME_WARNING;
esac;
init(PULSEWIDTH) := 0sd32_0;
next(PULSEWIDTH) := case
    loc = 1378 : (0sd32_150000 * 0sd32_100) / (signed(extend(main. 
        T_CYCLE, 16)) * 0sd32_100);
    TRUE : PULSEWIDTH;
esac;
init(FSIINC) := 0sd16_0;
next(FSIINC) := case
  loc = 1380 : (FSIINC + 0sd16_1);
  loc = 1383 : 0sd16_0;
  TRUE : FSIINC;
esac;
init(TSIINC) := 0sd16_0;
next(TSIINC) := case
  loc = 1386 : (TSIINC + 0sd16_1);
  loc = 1389 : 0sd16_0;
  TRUE : TSIINC;
esac;
init(SIINC) := 0sd16_0;
next(SIINC) := case
  loc = 1392 : (SIINC + 0sd16_1);
  loc = 1395 : 0sd16_0;
  TRUE : SIINC;
esac;
init(ALINC) := 0sd16_0;
next(ALINC) := case
  loc = 1398 : (ALINC + 0sd16_1);
  loc = 1401 : 0sd16_0;
  TRUE : ALINC;
esac;
init(WTSTOPIST) := FALSE;
next(WTSTOPIST) := case
  loc = 1387 : TRUE;
  loc = 1390 : WTSTOPIST;
  TRUE : WTSTOPIST;
esac;
init(WSTARTIST) := FALSE;
next(WSTARTIST) := case
  loc = 1393 : TRUE;
  loc = 1396 : STARTIST;
  TRUE : WSTARTIST;
esac;
init(WALST) := FALSE;
next(WALST) := case
  loc = 1399 : TRUE;
  loc = 1402 : ALST;
  TRUE : WALST;
esac;
init(WFUSTOPIST) := FALSE;
next(WFUSTOPIST) := case
  loc = 1381 : TRUE;
  loc = 1384 : FUSTOPIST;
  TRUE : WFUSTOPIST;
esac;
init(INLINED_R_EDGE_1__NEW) := FALSE;
next(INLINED_R_EDGE_1__NEW) := case
  loc = end : FALSE;
  loc = 11 : MANREG01_8___;
  TRUE : INLINED_R_EDGE_1__NEW;
esac;
init(INLINED_R_EDGE_1__OLD) := FALSE;
next(INLINED_R_EDGE_1__OLD) := case
  loc = end : FALSE;
  loc = 10 : MAUMOR_OLD;
loc = 14 : TRUE;
loc = 16 : INLINED_R_EDGE_1__NEW;
TRUE : INLINED_R_EDGE_1__OLD;

esac;
init(INLINED_R_EDGE_2__NEW) := FALSE;
next(INLINED_R_EDGE_2__NEW) := case
loc = end : FALSE;
loc = 19 : MANREG01_9__;
TRUE : INLINED_R_EDGE_2__NEW;
esac;
init(INLINED_R_EDGE_2__OLD) := FALSE;
next(INLINED_R_EDGE_2__OLD) := case
loc = end : FALSE;
loc = 18 : MMOR_OLD;
loc = 112 : TRUE;
loc = 114 : INLINED_R_EDGE_2__NEW;
TRUE : INLINED_R_EDGE_2__OLD;
esac;
init(INLINED_R_EDGE_3__NEW) := FALSE;
next(INLINED_R_EDGE_3__NEW) := case
loc = end : FALSE;
loc = 117 : MANREG01_10__;
TRUE : INLINED_R_EDGE_3__NEW;
esac;
init(INLINED_R_EDGE_3__OLD) := FALSE;
next(INLINED_R_EDGE_3__OLD) := case
loc = end : FALSE;
loc = 116 : MFOMOR_OLD;
loc = 120 : TRUE;
loc = 122 : INLINED_R_EDGE_3__NEW;
TRUE : INLINED_R_EDGE_3__OLD;
esac;
init(INLINED_R_EDGE_4__NEW) := FALSE;
next(INLINED_R_EDGE_4__NEW) := case
loc = end : FALSE;
loc = 125 : MANREG01_11__;
TRUE : INLINED_R_EDGE_4__NEW;
esac;
init(INLINED_R_EDGE_4__OLD) := FALSE;
next(INLINED_R_EDGE_4__OLD) := case
loc = end : FALSE;
loc = 124 : MSOFTLDR_OLD;
loc = 128 : TRUE;
loc = 130 : INLINED_R_EDGE_4__NEW;
TRUE : INLINED_R_EDGE_4__OLD;
esac;
init(INLINED_R_EDGE_5__NEW) := FALSE;
next(INLINED_R_EDGE_5__NEW) := case
loc = end : FALSE;
loc = 133 : MANREG01_12__;
TRUE : INLINED_R_EDGE_5__NEW;
esac;
init(INLINED_R_EDGE_5__OLD) := FALSE;
next(INLINED_R_EDGE_5__OLD) := case
loc = end : FALSE;
loc = 132 : MONA_OLD;
loc = 136 : TRUE;
loc = 138 : INLINED_R_EDGE_5__NEW;
TRUE : INLINED_R_EDGE_5__OLD;

esac;

init(INLINED_R_EDGE_6__NEW) := FALSE;
next(INLINED_R_EDGE_6__NEW) := case
loc = end : FALSE;
loc = 141 : MANREG01_13__;
TRUE : INLINED_R_EDGE_6__NEW;
esac;

init(INLINED_R_EDGE_6__OLD) := FALSE;
next(INLINED_R_EDGE_6__OLD) := case
loc = end : FALSE;
loc = 140 : MOFFR_OLD;
loc = 144 : TRUE;
loc = 146 : INLINED_R_EDGE_6__NEW;
TRUE : INLINED_R_EDGE_6__OLD;
esac;

init(INLINED_R_EDGE_7__NEW) := FALSE;
next(INLINED_R_EDGE_7__NEW) := case
loc = end : FALSE;
loc = 149 : MANREG01_1__;
TRUE : INLINED_R_EDGE_7__NEW;
esac;

init(INLINED_R_EDGE_7__OLD) := FALSE;
next(INLINED_R_EDGE_7__OLD) := case
loc = end : FALSE;
loc = 148 : MERNSTARTR_OLD;
loc = 152 : TRUE;
loc = 154 : INLINED_R_EDGE_7__NEW;
TRUE : INLINED_R_EDGE_7__OLD;
esac;

init(INLINED_R_EDGE_8__NEW) := FALSE;
next(INLINED_R_EDGE_8__NEW) := case
loc = end : FALSE;
loc = 157 : MANREG01_7__;
TRUE : INLINED_R_EDGE_8__NEW;
esac;

init(INLINED_R_EDGE_8__OLD) := FALSE;
next(INLINED_R_EDGE_8__OLD) := case
loc = end : FALSE;
loc = 156 : MALACKR_OLD;
loc = 160 : TRUE;
loc = 162 : INLINED_R_EDGE_8__NEW;
TRUE : INLINED_R_EDGE_8__OLD;
esac;

init(INLINED_R_EDGE_9__NEW) := FALSE;
next(INLINED_R_EDGE_9__NEW) := case
loc = end : FALSE;
loc = 177 : AUAUMOR;
TRUE : INLINED_R_EDGE_9__NEW;
esac;

init(INLINED_R_EDGE_9__OLD) := FALSE;
next(INLINED_R_EDGE_9__OLD) := case
loc = end : FALSE;
loc = 176 : AUAUMOR_OLD;
loc = 180 : TRUE;
loc = 182 : INLINED_R_EDGE_9__NEW;
TRUE : INLINED_R_EDGE_9__OLD;
esac;
appendix b nuXmv models

init(INLINED_R_EDGE_10__NEW) := FALSE;
next(INLINED_R_EDGE_10__NEW) := case
    loc = end : FALSE;
    loc = 185 : AUALACK;
    TRUE : INLINED_R_EDGE_10__NEW;
esac;
init(INLINED_R_EDGE_10__OLD) := FALSE;
next(INLINED_R_EDGE_10__OLD) := case
    loc = end : FALSE;
    loc = 184 : AUALACK_OLD;
    loc = 188 : TRUE;
    loc = 190 : INLINED_R_EDGE_10__NEW;
    TRUE : INLINED_R_EDGE_10__OLD;
esac;
init(INLINED_R_EDGE_11__NEW) := FALSE;
next(INLINED_R_EDGE_11__NEW) := case
    loc = end : FALSE;
    loc = 193 : STARTI;
    TRUE : INLINED_R_EDGE_11__NEW;
esac;
init(INLINED_R_EDGE_11__OLD) := FALSE;
next(INLINED_R_EDGE_11__OLD) := case
    loc = end : FALSE;
    loc = 192 : STARTI_OLD;
    loc = 196 : TRUE;
    loc = 198 : INLINED_R_EDGE_11__NEW;
    TRUE : INLINED_R_EDGE_11__OLD;
esac;
init(INLINED_R_EDGE_12__NEW) := FALSE;
next(INLINED_R_EDGE_12__NEW) := case
    loc = end : FALSE;
    loc = 1101 : TSTOPI;
    TRUE : INLINED_R_EDGE_12__NEW;
esac;
init(INLINED_R_EDGE_12__OLD) := FALSE;
next(INLINED_R_EDGE_12__OLD) := case
    loc = end : FALSE;
    loc = 1100 : TSTOPI_OLD;
    loc = 1104 : TRUE;
    loc = 1106 : INLINED_R_EDGE_12__NEW;
    TRUE : INLINED_R_EDGE_12__OLD;
esac;
init(INLINED_R_EDGE_13__NEW) := FALSE;
next(INLINED_R_EDGE_13__NEW) := case
    loc = end : FALSE;
    loc = 1109 : FUSTOPI;
    TRUE : INLINED_R_EDGE_13__NEW;
esac;
init(INLINED_R_EDGE_13__OLD) := FALSE;
next(INLINED_R_EDGE_13__OLD) := case
    loc = end : FALSE;
    loc = 1108 : FUSTOPI_OLD;
    loc = 1112 : TRUE;
    loc = 1114 : INLINED_R_EDGE_13__NEW;
    TRUE : INLINED_R_EDGE_13__OLD;
esac;
init(INLINED_R_EDGE_14__NEW) := FALSE;
next(INLINED_R_EDGE_14__NEW) := case
loc = end : FALSE;
loc = 1117 : AL;
TRUE : INLINED_R_EDGE_14__NEW;
esac;
init(INLINED_R_EDGE_14__OLD) := FALSE;
next(INLINED_R_EDGE_14__OLD) := case
loc = end : FALSE;
loc = 1116 : AL_OLD;
loc = 1120 : TRUE;
loc = 1122 : INLINED_R EDGE_14__NEW;
TRUE : INLINED_R EDGE_14__OLD;
esac;
init(INLINED_F EDGE_15__NEW) := FALSE;
next(INLINED_F EDGE_15__NEW) := case
loc = end : FALSE;
loc = 1139 : INTERLOCKR;
TRUE : INLINED_F EDGE_15__NEW;
esac;
init(INLINED_F EDGE_15__OLD) := FALSE;
next(INLINED_F EDGE_15__OLD) := case
loc = end : FALSE;
loc = 1138 : FE INTERLOCKR OLD;
loc = 1142 : FALSE;
loc = 1144 : INLINED_F EDGE_15__NEW;
TRUE : INLINED_F EDGE_15__OLD;
esac;
init(INLINED_TIMER_PULSEON__PT) := 0sd32_0;
next(INLINED_TIMER_PULSEON__PT) := case
loc = end : 0sd32_0;
loc = 1199 : 0sd32_0;
loc = 1229 : PONOFF.PPULSELE;
loc = 1293 : 0sd32_0;
TRUE : INLINED_TIMER_PULSEON__PT;
esac;
init(INLINED_TIMER_PULSEON__IN) := FALSE;
next(INLINED_TIMER_PULSEON__IN) := case
loc = end : FALSE;
loc = 1200 : FALSE;
loc = 1230 : PULSEONR;
loc = 1294 : FALSE;
TRUE : INLINED_TIMER_PULSEON__IN;
esac;
init(INLINED_TIMER_PULSEON__Q) := FALSE;
next(INLINED_TIMER_PULSEON__Q) := case
loc = end : FALSE;
loc = 1204 : TRUE;
loc = 1206 : FALSE;
loc = 1234 : TRUE;
loc = 1236 : FALSE;
loc = 1298 : TRUE;
loc = 1300 : FALSE;
TRUE : INLINED_TIMER_PULSEON__Q;
esac;
init(INLINED_TIMER_PULSEON__ET) := 0sd32_0;
next(INLINED_TIMER_PULSEON__ET) := case
loc = end : 0sd32_0;
loc = 1205 : (INLINED_TIMER_PULSEON__PT - (INLINED_TIMER_PULSEON__DUE - main.__GLOBAL_TIME));
loc = l208 : INLINED_TIMER_PULSEON__PT;
loc = l209 : 0sd32_0;
loc = l235 : (INLINED_TIMER_PULSEON__PT - (INLINED_TIMER_PULSEON__DUE - main.__GLOBAL_TIME));
loc = l238 : INLINED_TIMER_PULSEON__PT;
loc = l239 : 0sd32_0;
loc = l299 : (INLINED_TIMER_PULSEON__PT - (INLINED_TIMER_PULSEON__DUE - main.__GLOBAL_TIME));
loc = l302 : INLINED_TIMER_PULSEON__PT;
loc = l303 : 0sd32_0;
TRUE : INLINED_TIMER_PULSEON__ET;
esac;
init(INLINED_TIMER_PULSEON__OLD_IN) := FALSE;
next(INLINED_TIMER_PULSEON__OLD_IN) := case
loc = end : FALSE;
loc = l210 : INLINED_TIMER_PULSEON__IN;
loc = l240 : INLINED_TIMER_PULSEON__IN;
loc = l304 : INLINED_TIMER_PULSEON__IN;
TRUE : INLINED_TIMER_PULSEON__OLD_IN;
esac;
init(INLINED_TIMER_PULSEON__DUE) := 0sd32_0;
next(INLINED_TIMER_PULSEON__DUE) := case
loc = end : 0sd32_0;
loc = l202 : (main.__GLOBAL_TIME + INLINED_TIMER_PULSEON__PT);
loc = l232 : (main.__GLOBAL_TIME + INLINED_TIMER_PULSEON__PT);
loc = l296 : (main.__GLOBAL_TIME + INLINED_TIMER_PULSEON__PT);
TRUE : INLINED_TIMER_PULSEON__DUE;
esac;
init(INLINED_TIMER_PULSEOFF__PT) := 0sd32_0;
next(INLINED_TIMER_PULSEOFF__PT) := case
loc = end : 0sd32_0;
loc = l211 : 0sd32_0;
loc = l242 : PONOFF.PPULSELE;
loc = l280 : 0sd32_0;
TRUE : INLINED_TIMER_PULSEOFF__PT;
esac;
init(INLINED_TIMER_PULSEOFF__IN) := FALSE;
next(INLINED_TIMER_PULSEOFF__IN) := case
loc = end : FALSE;
loc = l212 : FALSE;
loc = l243 : PULSEOFFR;
loc = l281 : FALSE;
TRUE : INLINED_TIMER_PULSEOFF__IN;
esac;
init(INLINED_TIMER_PULSEOFF__Q) := FALSE;
next(INLINED_TIMER_PULSEOFF__Q) := case
loc = end : FALSE;
loc = l216 : TRUE;
loc = l218 : FALSE;
loc = l247 : TRUE;
loc = l249 : FALSE;
loc = l285 : TRUE;
loc = l287 : FALSE;
TRUE : INLINED_TIMER_PULSEOFF__Q;
esac;
init(INLINED_TIMER_PULSEOFF__ET) := 0sd32_0;
next(INLINED_TIMER_PULSEOFF__ET) := case
loc = end : 0sd32_0;
loc = l217 : (INLINED_TIMER_PULSEOFF__PT - (INLINED_TIMER_PULSEOFF__DUE - main.__GLOBAL_TIME));
loc = l220 : INLINED_TIMER_PULSEOFF__PT;
loc = l221 : 0sd32_0;
loc = l248 : (INLINED_TIMER_PULSEOFF__PT - (INLINED_TIMER_PULSEOFF__DUE - main.__GLOBAL_TIME));
loc = l251 : INLINED_TIMER_PULSEOFF__PT;
loc = l252 : 0sd32_0;
loc = l286 : (INLINED_TIMER_PULSEOFF__PT - (INLINED_TIMER_PULSEOFF__DUE - main.__GLOBAL_TIME));
loc = l289 : INLINED_TIMER_PULSEOFF__PT;
loc = l290 : 0sd32_0;
TRUE : INLINED_TIMER_PULSEOFF__ET;

esac;

init(INLINED_TIMER_PULSEOFF__OLD_IN) := FALSE;
next(INLINED_TIMER_PULSEOFF__OLD_IN) := case
loc = end : FALSE;
loc = l222 : INLINED_TIMER_PULSEOFF__IN;
loc = l253 : INLINED_TIMER_PULSEOFF__IN;
loc = l291 : INLINED_TIMER_PULSEOFF__IN;
TRUE : INLINED_TIMER_PULSEOFF__OLD_IN;

esac;

init(INLINED_TIMER_PULSEOFF__DUE) := 0sd32_0;
next(INLINED_TIMER_PULSEOFF__DUE) := case
loc = end : 0sd32_0;
loc = l214 : (main.__GLOBAL_TIME + INLINED_TIMER_PULSEOFF__PT);
loc = l245 : (main.__GLOBAL_TIME + INLINED_TIMER_PULSEOFF__PT);
loc = l283 : (main.__GLOBAL_TIME + INLINED_TIMER_PULSEOFF__PT);
TRUE : INLINED_TIMER_PULSEOFF__DUE;

esac;

init(INLINED_R_EDGE_20__NEW) := FALSE;
next(INLINED_R_EDGE_20__NEW) := case
loc = end : FALSE;
loc = l256 : PULSEON;
TRUE : INLINED_R_EDGE_20__NEW;

esac;

init(INLINED_R_EDGE_20__OLD) := FALSE;
next(INLINED_R_EDGE_20__OLD) := case
loc = end : FALSE;
loc = l255 : RE_PULSEON_OLD;
loc = l259 : TRUE;
loc = l261 : INLINED_R_EDGE_20__NEW;
TRUE : INLINED_R_EDGE_20__OLD;

esac;

init(INLINED_F_EDGE_21__NEW) := FALSE;
next(INLINED_F_EDGE_21__NEW) := case
loc = end : FALSE;
loc = l264 : PULSEON;
TRUE : INLINED_F_EDGE_21__NEW;

esac;

init(INLINED_F_EDGE_21__OLD) := FALSE;
next(INLINED_F_EDGE_21__OLD) := case
loc = end : FALSE;
loc = l263 : FE_PULSEON_OLD;
loc = l267 : FALSE;
loc = l269 : INLINED_F_EDGE_21__NEW;
TRUE : INLINED_F_EDGE_21__OLD;

esac;
init(INLINED_R_EDGE_22__NEW) := FALSE;
next(INLINED_R_EDGE_22__NEW) := case
    loc = end : FALSE;
    loc = 1272 : PULSEOFF;
    TRUE : INLINED_R_EDGE_22__NEW;
esac;
init(INLINED_R_EDGE_22__OLD) := FALSE;
next(INLINED_R_EDGE_22__OLD) := case
    loc = end : FALSE;
    loc = 1271 : RE_PULSEOFF_OLD;
    loc = 1275 : TRUE;
    loc = 1277 : INLINED_R_EDGE_22__NEW;
    TRUE : INLINED_R_EDGE_22__OLD;
esac;
init(INLINED_R_EDGE_25__NEW) := FALSE;
next(INLINED_R_EDGE_25__NEW) := case
    loc = end : FALSE;
    loc = 1341 : OUTOVST_AUX;
    TRUE : INLINED_R_EDGE_25__NEW;
esac;
init(INLINED_R_EDGE_25__OLD) := FALSE;
next(INLINED_R_EDGE_25__OLD) := case
    loc = end : FALSE;
    loc = 1340 : RE_OUTOVST_AUX_OLD;
    loc = 1344 : TRUE;
    loc = 1346 : INLINED_R_EDGE_25__NEW;
    TRUE : INLINED_R_EDGE_25__OLD;
esac;
init(INLINED_TIMER_WARNING__PT) := 0sd32_0;
next(INLINED_TIMER_WARNING__PT) := case
    loc = end : 0sd32_0;
    loc = 1360 : PONOFF.PWDT;
    TRUE : INLINED_TIMER_WARNING__PT;
esac;
init(INLINED_TIMER_WARNING__IN) := FALSE;
next(INLINED_TIMER_WARNING__IN) := case
    loc = end : FALSE;
    loc = 1361 : POSW_AUX;
    TRUE : INLINED_TIMER_WARNING__IN;
esac;
init(INLINED_TIMER_WARNING__Q) := FALSE;
next(INLINED_TIMER_WARNING__Q) := case
    loc = end : FALSE;
    loc = 1363 : FALSE;
loc = l373 : TRUE;
TRUE : INLINED_TIMER_WARNING__Q;
esac;
init(INLINED_TIMER_WARNING__ET) := 0sd32_0;
next(INLINED_TIMER_WARNING__ET) := case
loc = end : 0sd32_0;
loc = l364 : 0sd32_0;
loc = l369 : 0sd32_0;
loc = l372 : (main.__GLOBAL_TIME - INLINED_TIMER_WARNING__START);
loc = l374 : INLINED_TIMER_WARNING__PT;
TRUE : INLINED_TIMER_WARNING__ET;
esac;
init(INLINED_TIMER_WARNING__RUNNING) := FALSE;
next(INLINED_TIMER_WARNING__RUNNING) := case
loc = end : FALSE;
loc = l365 : FALSE;
loc = l368 : TRUE;
TRUE : INLINED_TIMER_WARNING__RUNNING;
esac;
init(INLINED_TIMER_WARNING__START) := 0sd32_0;
next(INLINED_TIMER_WARNING__START) := case
loc = end : 0sd32_0;
loc = l367 : main.__GLOBAL_TIME;
TRUE : INLINED_TIMER_WARNING__START;
esac;
init(INLINED_DETECT_EDGE_28__NEW) := FALSE;
next(INLINED_DETECT_EDGE_28__NEW) := case
loc = end : FALSE;
loc = l438 : ALUNACK;
loc = l437 : ALUNACK_OLD;
loc = l445 : INLINED_DETECT_EDGE_28__NEW;
TRUE : INLINED_DETECT_EDGE_28__NEW;
esac;
init(INLINED_DETECT_EDGE_28__OLD) := FALSE;
next(INLINED_DETECT_EDGE_28__OLD) := case
loc = end : FALSE;
loc = l438 : ALUNACK;
loc = l437 : ALUNACK_OLD;
loc = l445 : INLINED_DETECT_EDGE_28__NEW;
TRUE : INLINED_DETECT_EDGE_28__OLD;
esac;
init(INLINED_DETECT_EDGE_28__RE) := FALSE;
next(INLINED_DETECT_EDGE_28__RE) := case
loc = end : FALSE;
loc = l436 : RE_ALUNACK;
loc = l441 : TRUE;
loc = l443 : FALSE;
loc = l446 : FALSE;
loc = l447 : FALSE;
TRUE : INLINED_DETECT_EDGE_28__RE;
esac;
init(INLINED_DETECT_EDGE_28__FE) := FALSE;
next(INLINED_DETECT_EDGE_28__FE) := case
loc = end : FALSE;
loc = l435 : FE_ALUNACK;
loc = l442 : FALSE;
loc = l444 : TRUE;
loc = l447 : FALSE;
TRUE : INLINED_DETECT_EDGE_28__FE;
esac;
MODULE main
VAR

interaction : \{NONE \};
INSTANCE : module_INSTANCE(interaction, self);
random_random_t_cycle : unsigned word[8];
random_r53 : signed word[32];
random_r54 : signed word[32];
__GLOBAL_TIME : signed word[32];
T_CYCLE : unsigned word[16];
CPC_DB_VERSION.BASELINE_VERSION : signed word[32];

INVAR ( (INSTANCE.loc != initial -> random_r53 = 0sd32_0) & (INSTANCE.loc != initial -> random_r54 = 0sd32_0) ); --

ASSIGN

init(__GLOBAL_TIME) := 0sd32_0;
next(__GLOBAL_TIME) := case
INSTANCE.loc = initial : (__GLOBAL_TIME + signed(extend(T_CYCLE, 16)))
TRUE : __GLOBAL_TIME;
esac;
init(T_CYCLE) := 0ud16_0;
next(T_CYCLE) := case
INSTANCE.loc = end : (((extend(random_random_t_cycle,8))) mod 0ud16_116 + 0ud16_5);
TRUE : T_CYCLE;
esac;
init(CPC_DB_VERSION.BASELINE_VERSION) := 0sd32_660;
next(CPC_DB_VERSION.BASELINE_VERSION) := case
TRUE : CPC_DB_VERSION.BASELINE_VERSION;
esac;

DEFINE

PLC_START := (INSTANCE.loc = l0);
PLC_END := (INSTANCE.loc = end);

Listing B.1: NuSMV model for the OnOff UNICOS object

The following piece of NuSMV code corresponds to the automatically generated abstract model from the QSDN UNICOS CPC program for the first requirement in Section 4.4.2. This abstract model is enough to verify the following safety property $p$:

$$\text{AG} \left( (EoC \land \text{QSDN.4.DN1CT_SEQ_DB.Stop} \cdot \text{x}) \rightarrow \text{QSDN.4.1PV408.AuOffR} \right)$$

-- V1.1
-- Generated model from QSDN.scl by bfernand

MODULE module_INSTANCE(interaction, main)
VAR
loc : {initial, end, l1};

ASSIGN
init(loc) := initial;
next(loc) := case
  loc = end : initial;
  loc = initial : l1;
  loc = l1 : end;
  TRUE: loc;
esac;

MODULE main
VAR
interaction : {NONE };
INSTANCE : module_INSTANCE(interaction, self);
QSDN_4_DN1CT_SEQ_DB.STOP.X# : boolean;
QSDN_4_1PV408.AUONR : boolean;
QSDN_4_1PV408.AUOFFR : boolean;

ASSIGN
init(QSDN_4_DN1CT_SEQ_DB.STOP.X#) := FALSE;
next(QSDN_4_DN1CT_SEQ_DB.STOP.X#) := case
  INSTANCE.loc = initial : {TRUE, FALSE};
  TRUE : QSDN_4_DN1CT_SEQ_DB.STOP.X#;
esac;
init(QSDN_4_1PV408.AUONR) := FALSE;
next(QSDN_4_1PV408.AUONR) := case
  INSTANCE.loc = initial : {TRUE, FALSE};
  TRUE : QSDN_4_1PV408.AUONR;
esac;
init(QSDN_4_1PV408.AUOFFR) := FALSE;
next(QSDN_4_1PV408.AUOFFR) := case
  INSTANCE.loc = l1 : !(QSDN_4_1PV408.AUONR);
  TRUE : QSDN_4_1PV408.AUOFFR;
esac;

DEFINE
PLC_START := (INSTANCE.loc = l1);
PLC_END := (INSTANCE.loc = end);

INVAL
!( (QSDN_4_DN1CT_SEQ_DB.STOP.X# = TRUE ) & (QSDN_4_1PV408.AUONR = TRUE ) );

CTLSPEC AG((PLC_END) -> (QSDN_4_DN1CT_SEQ_DB.STOP.X# -> QSDN_4_1PV408.AUOFFR)) ;

Listing B.2: Abstract model \( AM'_1 \), where \( p \) is verified

The following piece of NuSMV code corresponds to the automatically generated abstract model from the QSDN UNICOS CPC program for the second requirement in Section 4.4.2. This abstract model
is enough to verify the following safety property $p$:

$$
AG \left( (EoC \land QSDN_4_DN1CT_SEQ_DB.Run.x) \rightarrow QSDN_4_1PV408.AuOnR \right)
$$
The following piece of NuSMV code corresponds to the automatically generated abstract model from the QSDN UNICOS CPC program for the third requirement in Section 4.4.2. This abstract model is enough to verify the following safety property $p$:

$$\text{AG}\left((\neg \text{EoC} \land \text{QSDN}_4\text{DN1CT_SEQ_DB.Run.x}) \rightarrow \text{QSDN}_4\text{1PV408.AuOffR}\right)$$
Listing B.4: Abstract model $AM'_2$, where $p$ is verified
List of Acronyms

AM: Abstract Model
API: Application Programming Interface
AST: Abstract Syntax Tree
BE/CO: Beams department / Controls group at CERN
BDD: Binary Decision Diagram
BIP: Behavior, Interaction and Priority
CEGAR: Counterexample guided Abstraction Refinement
CENELEC: European Committee for Electrotechnical Standardization
CERN: International Electrotechnical Commission
CDD: Clock Difference Diagram
CFG: Control Flow Graph
COI: Cone of Influence
CORBA: Common Object Request Broker Architecture
CPC: Continuous Process Control
CTL: Computation Tree Logic
DB: Data Block
DCS: Distributed Control System
DESY: Deutsches Elektronen-Synchrotron
DIEECS: Electric, Electronics, Computers and Systems Engineering
EMF: Eclipse Modeling Framework
EN/ICE: Engineering department / Industrial Controls & Engineering group at CERN
EoC: End of Cycle
EPICS: Experimental Physics and Industrial Controls
ERP: Enterprise Resource Planning
ESRF: European Synchrotron Radiation Facility
FAT: Factory Acceptance Test
FB: Function Block
FBD: Function Block Diagram
FC: Function
FESA: Front-End Software Architecture
FPGA: Field-Programmable Gate Array
FSM: Finite State Machine
GRAFCET: Graphe Fonctionnel de Croissant Étape Transition
HVAC: Heating, Ventilating, and Air Conditioning
IEC: International Electrotechnical Commission
IL: Instruction List
IIM: Input Image Memory
IM: Intermediate Model
IOC: Input-Output Controllers
**ISA:** International Electrotechnical Commission or System Engineering and Automation

**ISO:** International Organization for Standardization

**LEP:** Large Electron-Positron Collider

**LHC:** Large Hadron Collider

**LINAC:** LINear ACcelerators

**LTL:** Linear Temporal Logic

**LTS:** Labelled Transition System

**M:** Memory

**MDD:** Multivalued Decision Diagram

**MES:** Manufacturing Execution System

**NR:** Not Running

**OB:** Organization Block

**OIM:** Output Image Memory

**OM:** Original Model

**OPI:** Operator Interface

**PC:** Personal Computer

**PID:** Proportional Integral Derivative

**PLC:** Programmable Logic Controller

**PLTL:** Propositional Linear Temporal Logic

**PS:** Proton Synchrotron

**PSS:** Potential State Space

**PT:** Predefined delay
List of Acronyms

R: Runnning

RiSD: Rigorous System Design

RMIT: Royal Melbourne Institute of Technology

RSS: Reachable State Space

SAT: Satisfiability or Site Acceptance Test

SCADA: Supervisory Control and Data Acquisition

SCL: Structured Control Language

SFC: Sequential Function Chart

SIF: Safety Instrumented Function

SIL: Safety Integrity Level

SIS: Safety Instrumented System

SMT: Satisfiability Modulo Theories

SPS: Super Proton Synchrotron

ST: Structured Text

STS: State Transition System

TCTL: Timed Computation Tree Logic

TO: Time Out

TON: Timer On-delay

TOFF: Timer Off-delay

TP: Pulse Timer

UNICOS: Unified Industrial Control System
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Control system layers</td>
<td>15</td>
</tr>
<tr>
<td>2.2</td>
<td>IEC 61499 FB representation</td>
<td>19</td>
</tr>
<tr>
<td>2.3</td>
<td>EPICS architecture</td>
<td>21</td>
</tr>
<tr>
<td>2.4</td>
<td>EPICS control system example</td>
<td>21</td>
</tr>
<tr>
<td>2.5</td>
<td>TANGO architecture</td>
<td>22</td>
</tr>
<tr>
<td>2.6</td>
<td>Example SFC</td>
<td>28</td>
</tr>
<tr>
<td>2.7</td>
<td>Example SFC (Screenshot from SIMATIC tool by Siemens)</td>
<td>29</td>
</tr>
<tr>
<td>2.8</td>
<td>Timer diagrams</td>
<td>31</td>
</tr>
<tr>
<td>2.9</td>
<td>Consequences of finite time representation</td>
<td>32</td>
</tr>
<tr>
<td>2.10</td>
<td>Verification schema</td>
<td>36</td>
</tr>
<tr>
<td>2.11</td>
<td>LTL operators representation</td>
<td>39</td>
</tr>
<tr>
<td>2.12</td>
<td>CTL operators representation</td>
<td>40</td>
</tr>
<tr>
<td>3.1</td>
<td>Traditional PLC program development</td>
<td>60</td>
</tr>
<tr>
<td>3.2</td>
<td>Methodology overview</td>
<td>62</td>
</tr>
<tr>
<td>3.3</td>
<td>Two main approaches for the verification and design of PLC programs.</td>
<td>66</td>
</tr>
<tr>
<td>3.4</td>
<td>Integration of the proposed methodology in the PLC program development process.</td>
<td>67</td>
</tr>
<tr>
<td>3.5</td>
<td>Example of IM</td>
<td>71</td>
</tr>
<tr>
<td>3.6</td>
<td>Example of representing an interactive automata network as a STS</td>
<td>73</td>
</tr>
<tr>
<td>3.7</td>
<td>Example of IM</td>
<td>80</td>
</tr>
<tr>
<td>3.8</td>
<td>Example of IM with one PLC interrupt</td>
<td>84</td>
</tr>
<tr>
<td>3.9</td>
<td>FC – IM transformation</td>
<td>87</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>3.10</td>
<td>FB instance – IM transformation</td>
<td>87</td>
</tr>
<tr>
<td>3.11</td>
<td>FC call – IM transformation</td>
<td>89</td>
</tr>
<tr>
<td>3.12</td>
<td>Corresponding automaton fragment for variable assignment</td>
<td>90</td>
</tr>
<tr>
<td>3.13</td>
<td>Corresponding automaton fragment for for conditional statement</td>
<td>91</td>
</tr>
<tr>
<td>3.14</td>
<td>Example of transformation from a FC call into the IM</td>
<td>92</td>
</tr>
<tr>
<td>3.15</td>
<td>Example SFC (Screenshot from SIMATIC tool by Siemens)</td>
<td>95</td>
</tr>
<tr>
<td>3.16</td>
<td>IM representation of the SFC example</td>
<td>95</td>
</tr>
<tr>
<td>3.17</td>
<td>Reduction techniques applied to the IM and to the verification tool models</td>
<td>97</td>
</tr>
<tr>
<td>3.18</td>
<td>Example for control flow graph representation of an ST code in NuSMV</td>
<td>99</td>
</tr>
<tr>
<td>3.19</td>
<td>Example comparing our and the NuSMV’s cone of influence algorithm from [Darvas et al. (2014)]</td>
<td>104</td>
</tr>
<tr>
<td>3.20</td>
<td>Example reduction rules from [Darvas et al. (2014)]</td>
<td>106</td>
</tr>
<tr>
<td>3.21</td>
<td>Example CFG after our COI and the reductions from [Darvas et al. (2014)]</td>
<td>107</td>
</tr>
<tr>
<td>3.22</td>
<td>Overview of the reduction workflow</td>
<td>109</td>
</tr>
<tr>
<td>3.23</td>
<td>Verification cases for AG(α → β) in abstract models</td>
<td>110</td>
</tr>
<tr>
<td>3.24</td>
<td>Verification cases for EF(γ &amp; θ) in abstract models</td>
<td>111</td>
</tr>
<tr>
<td>3.25</td>
<td>Variable dependency graph example</td>
<td>113</td>
</tr>
<tr>
<td>3.28</td>
<td>Relationship between the verification cases for AG(α → ¬β) and AG(α → β) in abstract models</td>
<td>119</td>
</tr>
<tr>
<td>3.29</td>
<td>Relationship between the abstract models and the maximum number of possible invariants for the variable abstraction technique</td>
<td>123</td>
</tr>
<tr>
<td>3.30</td>
<td>Example of IM</td>
<td>125</td>
</tr>
<tr>
<td>3.31</td>
<td>Variable dependency graph of the original model corresponding to the PLC program example</td>
<td>125</td>
</tr>
</tbody>
</table>
List of Figures

3.32 Variable dependency graph of the abstract model corresponding to the PLC program example 126
3.33 Abstraction strategy applied to the example 127
3.34 Graphical representation as a FSM 132
3.35 Automaton fragment for a transition 134
3.36 Automaton fragment for a variable assignment 134
3.37 Automaton fragment for an interaction 134
3.38 Corresponding IM 135
3.39 Screenshot of the UPPAAL model 138
3.40 Automaton fragment for a transition 141
3.41 Automaton fragment for a variable assignment 142
3.42 Automaton fragments for a synchronization 143
3.43 Corresponding IM 144
3.44 BIP model with two components 149
3.45 Automaton fragment for a transition 154
3.46 Automaton fragment for a variable assignment 155
3.47 Automaton fragments for a synchronization 155
3.48 Corresponding IM 156
3.49 Timer diagrams 162
3.50 Consequences of finite time representation 164
3.51 State machine of the realistic TON representation 165
3.52 State machine of the realistic TOFF representation 167
3.53 State machine of the realistic TP representation 168
3.54 Verification configuration for OnOff model extended with monitor 170
3.55 State machine of the abstract TON representation 171
3.56 Timing diagram of TON modeled using different approaches 172
3.57 State machine of the abstract TOFF representation 173
3.58 State machine of the abstract TP representation 174
3.59 Integration of the proposed methodology on the PLC program development process 180
3.60 EMF implementation 181
3.61 CASE tool editor for the PLC code 182
3.62 CASE tool property description 182
3.63 CASE tool property formalization by using patterns 183
3.64 CASE tool verification report 183
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Different UNICOS packages</td>
<td>186</td>
</tr>
<tr>
<td>4.2</td>
<td>UNICOS CPC control system architecture</td>
<td>187</td>
</tr>
<tr>
<td>4.3</td>
<td>Mapping between the process instrumentation and the UNICOS objects example</td>
<td>189</td>
</tr>
<tr>
<td>4.4</td>
<td>UNICOS PLC code architecture</td>
<td>190</td>
</tr>
<tr>
<td>4.5</td>
<td>OnOff signals interface</td>
<td>193</td>
</tr>
<tr>
<td>4.6</td>
<td>State machine of the OnOff mode manager from the UNICOS specifications</td>
<td>195</td>
</tr>
<tr>
<td>4.7</td>
<td>Verification configuration for OnOff model extended with monitor</td>
<td>202</td>
</tr>
<tr>
<td>4.8</td>
<td>QSDN process</td>
<td>209</td>
</tr>
<tr>
<td>4.9</td>
<td>Variable dependency graph for the given requirement of QSDN</td>
<td>212</td>
</tr>
<tr>
<td>4.10</td>
<td>Relationship between the abstract models and the maximum number of reachability properties for the variable abstraction technique $m$</td>
<td>213</td>
</tr>
<tr>
<td>5.1</td>
<td>Measurements comparing the different COI solutions from Darvas et al. (2014)</td>
<td>229</td>
</tr>
<tr>
<td>5.2</td>
<td>Relationship between the abstract models and the maximum number of reachability properties for the variable abstraction technique</td>
<td>232</td>
</tr>
</tbody>
</table>
# List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Software design and development: software architecture design (see Table 7.4.3 from the IEC 61508 (2010) standard)</td>
<td>6</td>
</tr>
<tr>
<td>2.1</td>
<td>The Range of Formal Methods Options Summarized in Terms of (a) Levels of Formalization and (b) Scope of Formal Methods Use</td>
<td>33</td>
</tr>
<tr>
<td>2.2</td>
<td>Related work</td>
<td>53</td>
</tr>
<tr>
<td>2.3</td>
<td>Related work: Abstraction techniques</td>
<td>55</td>
</tr>
<tr>
<td>2.4</td>
<td>Related work: Time modeling strategy</td>
<td>57</td>
</tr>
<tr>
<td>3.1</td>
<td>Data type mapping</td>
<td>85</td>
</tr>
<tr>
<td>3.2</td>
<td>Counterexample for $p$ on $AM'_1$</td>
<td>126</td>
</tr>
<tr>
<td>3.3</td>
<td>Counterexample for $p$ on $AM'_1 + 1$ invariant</td>
<td>128</td>
</tr>
<tr>
<td>3.4</td>
<td>Counterexample for $p$ on $AM'_1 + 2$ invariants</td>
<td>129</td>
</tr>
<tr>
<td>3.5</td>
<td>Variables values from the counterexample at the end of the PLC cycle</td>
<td>177</td>
</tr>
<tr>
<td>4.1</td>
<td>Case Study metrics</td>
<td>192</td>
</tr>
<tr>
<td>4.2</td>
<td>Model generation metrics</td>
<td>198</td>
</tr>
<tr>
<td>4.3</td>
<td>Model generation metrics</td>
<td>199</td>
</tr>
<tr>
<td>4.4</td>
<td>Verification run time for the first requirement from [Fernández Adiego et al. (2014c)]</td>
<td>200</td>
</tr>
<tr>
<td>4.5</td>
<td>Verification run time for the second requirement</td>
<td>201</td>
</tr>
<tr>
<td>4.6</td>
<td>State space of the OnOff model with realistic timer representation from [Fernández Adiego et al. (2014a)]</td>
<td>203</td>
</tr>
<tr>
<td>4.7</td>
<td>Verification time on OnOff model with realistic time representation from [Fernández Adiego et al. (2014a)]</td>
<td>204</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>4.8</td>
<td>State space of the OnOff model with abstract time representation from Fernández Adiego et al. (2014a)</td>
<td>205</td>
</tr>
<tr>
<td>4.9</td>
<td>Verification time on OnOff model with abstract time representation from Fernández Adiego et al. (2014a)</td>
<td>205</td>
</tr>
<tr>
<td>4.10</td>
<td>Metrics of the models of QSDN</td>
<td>211</td>
</tr>
<tr>
<td>4.11</td>
<td>Verification time on QSDN model</td>
<td>214</td>
</tr>
<tr>
<td>4.12</td>
<td>Verification time on QSDN model</td>
<td>215</td>
</tr>
<tr>
<td>4.13</td>
<td>Verification time on QSDN model</td>
<td>216</td>
</tr>
<tr>
<td>5.1</td>
<td>Overview of the timer representation approaches from Darvas et al. (2014a)</td>
<td>227</td>
</tr>
<tr>
<td>5.2</td>
<td>Requirement evaluation measurements with nuXmv COI from Darvas et al. (2014)</td>
<td>230</td>
</tr>
<tr>
<td>5.3</td>
<td>Requirement evaluation measurements with our COI from Darvas et al. (2014)</td>
<td>230</td>
</tr>
</tbody>
</table>
## Listings

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Example of ST code</td>
<td>27</td>
</tr>
<tr>
<td>2.2</td>
<td>Example of the textual representation of SFC code</td>
<td>27</td>
</tr>
<tr>
<td>3.1</td>
<td>Variable assignment in ST code</td>
<td>90</td>
</tr>
<tr>
<td>3.2</td>
<td>Conditional statement in ST code</td>
<td>91</td>
</tr>
<tr>
<td>3.3</td>
<td>Example of ST code</td>
<td>91</td>
</tr>
<tr>
<td>3.4</td>
<td>Example of the textual representation of SFC code</td>
<td>94</td>
</tr>
<tr>
<td>3.5</td>
<td>Example of ST code</td>
<td></td>
</tr>
<tr>
<td>3.6</td>
<td>NuSMV code example</td>
<td>124</td>
</tr>
<tr>
<td>3.7</td>
<td>Representation of automata network in nuXmv</td>
<td>132</td>
</tr>
<tr>
<td>3.8</td>
<td>Representation of automaton a in nuXmv</td>
<td>133</td>
</tr>
<tr>
<td>3.9</td>
<td>Next-value assignment statement</td>
<td>133</td>
</tr>
<tr>
<td>3.10</td>
<td>Corresponding nuXmv code</td>
<td>134</td>
</tr>
<tr>
<td>3.11</td>
<td>Corresponding nuXmv code</td>
<td>134</td>
</tr>
<tr>
<td>3.12</td>
<td>Corresponding nuXmv code</td>
<td>134</td>
</tr>
<tr>
<td>3.13</td>
<td>PLC ST code</td>
<td>135</td>
</tr>
<tr>
<td>3.14</td>
<td>nuXmv code</td>
<td>135</td>
</tr>
<tr>
<td>3.15</td>
<td>nuXmv model example</td>
<td>136</td>
</tr>
<tr>
<td>3.16</td>
<td>UPPAAL code example</td>
<td>139</td>
</tr>
<tr>
<td>3.17</td>
<td>Representation of automata network in UPPAAL</td>
<td>140</td>
</tr>
<tr>
<td>3.18</td>
<td>Representation of automaton a in UPPAAL</td>
<td>140</td>
</tr>
<tr>
<td>3.19</td>
<td>Variables of automaton a in UPPAAL</td>
<td>141</td>
</tr>
<tr>
<td>3.20</td>
<td>Corresponding UPPAAL code</td>
<td>141</td>
</tr>
<tr>
<td>3.21</td>
<td>Corresponding UPPAAL code</td>
<td>142</td>
</tr>
<tr>
<td>3.22</td>
<td>Corresponding UPPAAL code</td>
<td>143</td>
</tr>
<tr>
<td>3.23</td>
<td>PLC ST code</td>
<td>144</td>
</tr>
<tr>
<td>3.24</td>
<td>Corresponding UPPAAL model</td>
<td>144</td>
</tr>
<tr>
<td>3.25</td>
<td>Synchronization of two automaton in UPPAAL</td>
<td>146</td>
</tr>
<tr>
<td>3.26</td>
<td>Representation of automata network in BIP</td>
<td>150</td>
</tr>
<tr>
<td>3.27</td>
<td>Representation of automaton a in BIP</td>
<td>151</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>3.28</td>
<td>Representation of automaton ( \alpha ) in BIP</td>
<td>153</td>
</tr>
<tr>
<td>3.29</td>
<td>Corresponding BIP code</td>
<td>154</td>
</tr>
<tr>
<td>3.30</td>
<td>Corresponding BIP code</td>
<td>155</td>
</tr>
<tr>
<td>3.31</td>
<td>Corresponding BIP code</td>
<td>155</td>
</tr>
<tr>
<td>3.32</td>
<td>PLC ST code</td>
<td>156</td>
</tr>
<tr>
<td>3.33</td>
<td>Corresponding BIP model</td>
<td>156</td>
</tr>
<tr>
<td>3.34</td>
<td>BIP example</td>
<td>158</td>
</tr>
<tr>
<td>3.35</td>
<td>ST code of TON</td>
<td>164</td>
</tr>
<tr>
<td>3.36</td>
<td>ST code of TOFF</td>
<td>166</td>
</tr>
<tr>
<td>3.37</td>
<td>ST code of TP</td>
<td>167</td>
</tr>
<tr>
<td>3.38</td>
<td>ST code example</td>
<td>175</td>
</tr>
<tr>
<td>3.39</td>
<td>Counterexample fragment</td>
<td>179</td>
</tr>
<tr>
<td>3.40</td>
<td>Corresponding ST code demonstrator</td>
<td>179</td>
</tr>
<tr>
<td>3.41</td>
<td>Extract of the source code causing the violation of the requirement</td>
<td>179</td>
</tr>
<tr>
<td>4.1</td>
<td>OnOff mode manager program</td>
<td>194</td>
</tr>
<tr>
<td>4.2</td>
<td>Extract from the counterexample</td>
<td>206</td>
</tr>
<tr>
<td>4.3</td>
<td>Extract from the PLC demonstrator</td>
<td>206</td>
</tr>
<tr>
<td>4.4</td>
<td>Extract of the source code causing the violation of the requirement</td>
<td>207</td>
</tr>
<tr>
<td>4.5</td>
<td>Excerpt of QSDN code relevant to the case study</td>
<td>210</td>
</tr>
<tr>
<td>A.1</td>
<td>OnOff PLC program</td>
<td>259</td>
</tr>
<tr>
<td>B.1</td>
<td>NuSMV model for the OnOff UNICOS object</td>
<td>277</td>
</tr>
<tr>
<td>B.2</td>
<td>Abstract model ( AM_1 ), where ( p ) is verified</td>
<td>320</td>
</tr>
<tr>
<td>B.3</td>
<td>Abstract model ( AM_1' ), where ( p ) is verified</td>
<td>322</td>
</tr>
<tr>
<td>B.4</td>
<td>Abstract model ( AM_2 ), where ( p ) is verified</td>
<td>323</td>
</tr>
</tbody>
</table>
Bibliography


337


Bibliography


Flake, S., Müller, W., Pape, U., and Ruf, J. (2004). Specification and formal verification of temporal properties of production automation systems. In Ehrig, H., Damm, W., Desel, J., Große-Rhode, M., Reif, W., Schnieder, E., and Westkämper, E., editors, Integration of


ISA 62381 (2010). Factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT), automation systems in the process industry.


