Co-Modeling and Co-Synthesis of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms

Jean-Pierre Talpin
Inst National Recherche Inform Autom

03/20/2017
Final Report

DISTRIBUTION A: Distribution approved for public release.

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ IOE
Arlington, Virginia 22203
Air Force Materiel Command
Co-Modeling and Co-Synthesis of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms

This is the final report on the findings of the USAF/OSR grant to support collaboration between INRIA (FR), University of Kaiserslautern (DE) and Virginia Tech (VA, USA) on research entitled 'Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms. In this project, we consider and integrate two different model-based design flows that are based on synchronous languages: The first design flow starts with a polychronous model that is in some sense a process network whose nodes are triggered whenever input values are available. To ensure that such systems are deterministic and can run with bounded memory, clock consistency constraints have to be checked that are defined for the input and output streams of each node. Even if this has been successfully solved in the past individually for pure synchronous programs, and pure polychronous programs, one has to additionally determine a clock consistent schedule for the final code generation. In this proposal, we will develop new methods to ensure clock consistency in that we will reduce the problem to the constructiveness of (poly)synchronous programs. This will not only lead to new procedures to check clock consistency, but due to the constructive reasoning, we also derive schedules for code generation, and we can implement simulators for polychronous models.
Final report of the USAF/OSR project entitled
“Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms”

Jean-Pierre Talpin
TEA Lab
INRIA Rennes-Bretagne-Atlantique
Campus de Beaulieu
F-35042 Rennes, France

Klaus Schneider and Jens Brandt
Embedded Systems Group
Technical University of Kaiserslautern
Kaiserslautern, Germany

Sandeep Shukla
FERMAT Lab
Electrical and Computer Engineering Department
Virginia Tech
900 North Glebe Road,
Arlington, VA 22203

March 2017
NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them. This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil). AFRL-RI-RS-TR-2009-259 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

Signatures

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.
### 4. TITLE AND SUBTITLE

Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms

### 6. AUTHOR(S)

Talpin, Jean-Pierre & Schneider, Klaus & Brandt, Jens & Shukla, Sandeep K. & Kumar, Preeti & Anderson, Matthew

### 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

INRIA INSTITUT DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE DOM VOLUCEAU BP 105 ROCQUENCOURT F-78150 FRANCE

### 8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

### 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

EUROPEAN OFFICE OF AEROSPACE RESEARCH AND DEVELOPMENT 86 BLENHEIM CRESCENT, RUISLIP, MIDDLESEX HA4 7HB UNITED KINGDOM

### 10. SPONSOR/MONITOR'S ACRONYM(S)

EUROPEAN OFFICE OF AEROSPACE RESEARCH AND DEVELOPMENT

### 12. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

### 14. ABSTRACT

This is the first annual report on the findings of the USAF/OSR grant to support collaboration between INRIA (FR), University of Kaiserslautern (DE) and Virginia Tech (VA, USA) on research entitled "Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms". In this project, we consider and integrate two different model-based design flows that are based on synchronous languages: The first design flow starts with a polychronous model that is in some sense a process network whose nodes are triggered whenever input values are available. To ensure that such systems are deterministic and can run with bounded memory, clock consistency constraints have to be checked that are defined for the input and output streams of each node. Even if this has been successfully solved in the past individually for pure synchronous programs, and pure polychronous programs, one has to additionally determine a clock consistent schedule for the final code generation. In this proposal, we will develop new methods to ensure clock consistency in that we will reduce the problem to the constructiveness of (poly)synchronous programs. This will not only lead to new procedures to check clock consistency, but due to the constructive reasoning, we also derive schedules for code generation, and we can implement simulators for polychronous models.

### 15. SUBJECT TERMS

Software Engineering, Software Producibility, Component-based software design, behavioral types, behavioral type inference, Polychronous model of computation, Prime Implicates, Boolean Abstraction, real-time embedded software, software synthesis, correct by construction software design, model-driven software design, high-assurance software

### 19a. NAME OF RESPONSIBLE PERSON

WENDY HARRISON

### 19b. TELEPHONE NUMBER (include area code)

+44(0)18956161

---

**Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.**

**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

**1. REPORT DATE (DD-MM-YYYY)**

10-04-2014

**2. REPORT TYPE**

FINAL REPORT

**3. DATES COVERED (From - To)**

April 12, 2013 – April 10, 2014

**5a. CONTRACT NUMBER**

N/A

**5b. GRANT NUMBER**

FA8655-13-1-3049

**5c. PROGRAM ELEMENT NUMBER**

N/A

**5d. PROJECT NUMBER**

N/A

**5e. TASK NUMBER**

N/A

**5f. WORK UNIT NUMBER**

N/A

**13. SUPPLEMENTARY NOTES**

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

**16. SECURITY CLASSIFICATION OF:**

| a. REPORT | U |
| b. ABSTRACT | U |
| c. THIS PAGE | U |

**17. LIMITATION OF ABSTRACT**

U

**18. NUMBER OF PAGES**

U

**19a. NAME OF RESPONSIBLE PERSON**

WENDY HARRISON

**19b. TELEPHONE NUMBER (include area code)**

+44(0)18956161
Contents

FOREWORD................................................................................................................................................................. 5
PREFACE ........................................................................................................................................................................... 6
SCIENTIFIC RESULTS HIGHLIGHTS OF THE PROJECT.................................................................................................. 7
VISITS AND EXCHANGES SUPPORTED BY THE PROJECT .............................................................................................. 7
COURSES AND DISSEMINATION SUPPORTED BY THE PROJECT ..................................................................................... 7
COMPLEMENTARY FUNDING OBTAINED FROM THE PROJECT SUPPORT........................................................................... 7
JOINT PUBLICATIONS SUPPORTED BY THE PROJECT.................................................................................................. 9
Foreword

Multicore processors have become standard for desktop computers since 2005, and are now also frequently used for the implementation of embedded systems. In the near future, many embedded applications including safety critical ones as used in avionics, automotive, mission control systems will run on multicore processors. For this reason, programming multicore processors should have already become a routine engineering practice. However, anybody who experienced programming of multicore processors will acknowledge the difficulty of implementing concurrent software under the currently dominating thread-based programming models: Synchronisation, deadlocks, race conditions, weak memory models, and lack of determinism of usual multithreaded software are extremely difficult to tackle. Ensuring determinism and correctness with respect to required specifications are however mandatory for safety-critical systems. For this reason, retrofitting sequential von Neumann-style programming models to multi-threaded programming is not the right way to go for programming such systems. An interesting solution to this problem is offered by model-based design methods where one can automatically generate multithreaded code from an abstract and simplified, yet formal model, using a provably ‘correct-by-construction’ automatic synthesis. Using the popular synchronous programming paradigms as formal models, one can reach such objectives. This way, one can formally verify the synchronous models of the systems, and once these are proved correct, code can be automatically generated for a multicore processor.
**Preface**

In this proposal, we consider and integrate two different model-based design flows that are based on synchronous languages: The first design flow starts with a polychronous model that is in some sense a process network whose nodes are triggered whenever input values are available. To ensure that such systems are deterministic and can run with bounded memory, clock consistency constraints have to be checked that are defined for the input and output streams of each node. One has to additionally determine a clock consistent schedule for the final code generation. In this proposal, we will develop new methods to ensure clock consistency in that we will reduce the problem to the constructiveness of (poly)synchronous programs. This will not only lead to new procedures to check clock consistency, but due to the constructive reasoning, we also derive schedules for code generation, and we can implement simulators for polychronous models.

The second design flow starts with a fully synchronous model whose reactions are triggered by a single clock. In this project, we will first develop methods to decompose such a synchronous system into components that communicate via elastic buffers instead of the otherwise used immediate broadcast communication. Then, we continue by further desynchronizing these systems in that no longer all the values are communicated between the components, but components can still locally decide when sufficiently many input values are available. Hence, a polychronous system is obtained, and we will ensure that the constructiveness of the original synchronous system is preserved during these design steps. We will additionally make sure that given temporal properties are preserved during this design flow, and we forbid decompositions that would violate these specifications.

Finally, we consider the automated multithreaded code generation for the obtained constructive polychronous models. While clock consistent schedules are already determined by our analyses, further problems have to be solved to generate efficient multithreaded code. We aim at identifying special classes of polychronous systems that simplify the code generation due to the constructive information flow of the clocks. For example, the simplest code generator is obtained for systems where the information flow of clocks follow the computation from input values to output values; (however, this is not possible for all programs). Moreover, we optimize the performance by clustering nodes into single threads, and we consider weak memory models to automatically synchronize threads where necessary taking the clock information into account.

**Acknowledgement**

We acknowledge the support of William McKeever, and Steve Drager from the Air Force Rome Laboratories, Wendy Harrison and James Lawton, from the USAF Office of Scientific Research, for supporting this collaborative research.
Scientific results highlights of the project
The major results of the project over the evaluated period are both scientific and economical. Scientifically, we have jointly published a series of papers [1,2,3] establishing constructive semantic foundations to co-model embedded systems using heterogeneous domain-specific languages: the polychronous data-flow language Signal and the imperative synchronous language. Reference [3], in particular, presents the first constructive semantics of polychronous systems. Based on these findings, we implemented a cross-compiler, Onyx, allowing to bridge two existing synchronous programming environments: Averest (http://www.averest.org) and Polychrony, now an Eclipse-Polarsys project, https://www.polarsys.org/projects/polarsys.pop. Economically, our project and its impact allowed us to reach new contacts with Toyota R&D, Mountain View, which yielded the start of a collaborative project described below. In 2016, Sandeep Shukla left Virginia Tech to join IIT Kanpur in India.

Visits and exchanges supported by the project
The visits and exchanges supported by the project and the co-funded INRIA associate-project POLYCORE over the funded period have been the following:
- Visit of Jean-Pierre Talpin at the Virginia Tech Research Laboratory in Arlington from April 19 to May 3, 2013.
- Visit of Jean-Pierre Talpin at the Virginia Tech Research Laboratory in Arlington from October 18 to 29, 2013.
- Visit of Jean-Pierre Talpin at the Virginia Tech Research Laboratory in Arlington from April 5 to 27, 2014.
- Visit of Jean-Pierre Talpin at the Virginia Tech, Falls Church Campus, from July 28 to September 10, 2014.
- Visit of Jean-Pierre Talpin at the Virginia Tech, Falls Church Campus, from November 4 to November 20, 2014.
- Visit of Jean-Pierre Talpin at the Virginia Tech, Falls Church Campus, from March 17 to April 2, 2015.
- Joint organizational participation to ACM-IEEE MEMOCODE’15 (Austin, Texas) from September 19 to 28, 2015.
- Joint workshop at UC San Diego, California, from November 21 to 27, 2015.

Courses and dissemination supported by the project
In the context of the above visits, Jean-Pierre Talpin was invited to give Master-class lectures at the Virginia Tech campus, Falls Church, on:
- Constructive semantics of synchronous languages, in May 2013.
- An introduction to the UML MARTE and CCSL, in October 2013.

Complementary funding obtained from the project support
In the frame of our ongoing collaboration, and thanks to the project support, we established professional contact with fellow researchers at Toyota R&D, Mountain View in late 2013. We jointly submitted a collaborative project proposal between TR&D, VTRL and INRIA. The topic of the proposal is the model-based formal verification and integration of embedded automotive architectures. The project proposal was just recently accepted and officially starts this month. We will receive funding which, in good synergy with the present project, will allow us to decouple our research and development capability and maximize the impact of our project.
Thanks to the support of the present project, we established professional contact with fellow researchers at Toyota ITC, Mountain View in late 2013. We submitted a joint project proposal to ITC, which was accepted and received an additional funding of approx. 120k$ from April 2014 to April 2015, shared between Virginia Tech and INRIA. The topic of the project is the model-based formal verification and integration of embedded automotive architectures. In the context of that project, we jointly published additional scientific articles [1,2,3], including an invited presentation at ACM DAC’15, the premier system design conference.
Joint publications supported by the project


# FEDERAL FINANCIAL REPORT

<table>
<thead>
<tr>
<th>1. Federal Agency and Organizational Element to Which Report is Submitted</th>
<th></th>
<th>Page of 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>EUROPEAN OFFICE OF AEROSPACE RESEARCH AND DEVELOPMENT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNIT 4515 BOX 144PO EA 94241 USA</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Federal Grant or Other Identifying Number Assigned by Federal Agency (To report multiple grants, use FFR Attachment)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FA8655-15-1-3049</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4a. DUNS Number</th>
<th>4b. EIN</th>
<th>5. Recipient Account Number or Identifying Number (To report multiple grants, use FFR Attachment)</th>
</tr>
</thead>
<tbody>
<tr>
<td>381909938</td>
<td>0</td>
<td>FR76 1007 1780 0000 0010 0395 848</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. Report Type</th>
<th>7. Basis of Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarterly</td>
<td>Cash</td>
</tr>
<tr>
<td>Semi-Annual</td>
<td>Accrual</td>
</tr>
<tr>
<td>Annual</td>
<td></td>
</tr>
<tr>
<td>Final</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. Project/Grant Period From: (Month, Day, Year)</th>
<th>To: (Month, Day, Year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/15/2013</td>
<td>11/30/2016</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. Reporting Period End Date (Month, Day, Year)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11/30/2016</td>
<td></td>
</tr>
</tbody>
</table>

## 10. Transactions

<table>
<thead>
<tr>
<th>Lines a-c for single or multiple grant reporting</th>
<th>Cumulative</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Federal Cash (To report multiple grants, also use FFR Attachment):</strong></td>
<td></td>
</tr>
<tr>
<td>a. Cash Receipts</td>
<td>48,039 € (60,000 $)</td>
</tr>
<tr>
<td>b. Cash Disbursements</td>
<td></td>
</tr>
<tr>
<td>c. Cash on Hand (line a minus b)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lines d-o for single grant reporting</th>
<th>Federal Expenditures and Unobligated Balance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>d. Total Federal funds authorized</td>
<td>48,039 €</td>
</tr>
<tr>
<td>e. Federal share of expenditures</td>
<td>37,254 €</td>
</tr>
<tr>
<td>f. Federal share of unliquidated obligations</td>
<td>0</td>
</tr>
<tr>
<td>g. Total Federal share (sum of lines e and f)</td>
<td>37,254 €</td>
</tr>
<tr>
<td>h. Unobligated balance of Federal funds (line d minus g)</td>
<td>10,785 € (11,723 $)</td>
</tr>
</tbody>
</table>

## 11. Remaining recipient share required

<table>
<thead>
<tr>
<th>a. Type</th>
<th>b. Rate</th>
<th>c. Period From</th>
<th>d. Period To</th>
<th>e. Base</th>
<th>f. Amount Charged</th>
<th>g. Federal Share</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## 12. Remarks: Attach any explanations deemed necessary or information required by Federal sponsoring agency in compliance with governing legislation:

## 13. Certification: By signing this report, I certify that it is true, complete, and accurate to the best of my knowledge. I am aware that any false, fictitious, or fraudulent information may subject me to criminal, civil, or administrative penalties. (U.S. Code, Title 18, Section 1001)

<table>
<thead>
<tr>
<th>a. Typed or Printed Name and Title of Authorized Certifying Official</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

La responsable du pôle en INFORMATIQUE ET EN AUTOMATIQUE INRIA Rennes-Bretagne Atlantique

Carole BROISSARD

## 14. Agency use only:

DISTRIBUTION A. Approved for public release: distribution unlimited.