INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

# *Team tick*

# *Theory and Practice of Synchronous Reactive Systems*

*Sophia Antipolis*

THEME 1C

# Table of contents

# 1. Team

TICK *is a temporary follow-up project of the former* MEIJE*. We are currently proposing a new project named* AOSTE*, jointly with the* SPORTS *team of the university of Nice/Sophia-Antipolis, and the* OSTRE *team from INRIA Rocquencourt.*

**Head of project-team**
Robert de Simone [Senior Researcher, Inria]

**Administrative assistant**
Sophie Honnorat [TR, part-time]

**Ph. D. student**
Fabrice Peix [MENESR scholarship, third year]
Olivier Tardieu [Ingénieur du Corps des Mines, second year]
Eric Vecchié [PACA regional scholarship, third year]

**Temporary Engineer**
Gérald Vormbrock [IE, funded on ARTIST IST NoE (6 months)]

**External collaborator**
Charles André [professor, UNSA]

# 2. Overall Objectives

**Key words:** *synchronous hypothesis*, *synchronous reactive formalisms*, *embedded systems*, *Systems-on-Chip*, *formal semantics*, *high-level modeling*, *automatic verification*, *program analysis*, *code synthesis*, *compilation techniques*, *architectural models*, *code distribution*, *UML behavioral diagrams*.

Research in TICK focuses on the design of real-time embedded systems, using *synchronous reactive formalisms* [1][7]. Here, "design" refers altogether to modeling, analysis & verification, and compilation activities. The synchronous reactive hypothesis allows us to benefit from clean mathematical foundations, and well-defined interpretation and execution models, on which to base these steps. We use as favorite specification formalisms the ESTEREL [4][3][5] and SYNCCHARTS [6] languages, that were invented and developed for over a decade in and around our team and the I3S SPORTS team at the university of Nice/Sophia-Antipolis. We developed innovative techniques for representation, static and dynamic model-checking analysis, optimization and efficient compilation on such systems. These research themes led over years to many contractual collaborations with companies such as Dassault Aviation, Thales, Texas Instruments, France Telecom R&D to mention several. Our results found their way to transfer with the creation of the Esterel Technologies spin-off company. We are currently working on several extensions of our methods [10][9][13], and their contribution to semantically-based UML diagrammatic notations for Real-Time Embedded systems [8], and the distributed implementation of synchronous applications on architecture models (as proposed in SynDEx and the AAA methodology by the OSTRE INRIA team.

# 3. Scientific Foundations

## 3.1. Theory of Synchronous Programming; Applications in compilation and analysis

**Participants:** Robert de Simone, Fabrice Peix, Olivier Tardieu, Eric Vecchié, Dumitru Potop [postdoctorate fellowship, Irisa S4 team].

The synchronous reactive hypothesis builds the foundations on which are laid out most of our activities in modeling, design, analysis and implementation of real-time embedded critical systems. Existence of reference

mathematical models (with sound operational semantics) is a prime justification for the introduction of our techniques, coupled with matching efficient algorithms, also conceived in the team.

Over the years the study of reactive synchronous formalisms, and mostly of the Esterel and SyncCharts specification and programming languages, has led to research topics on efficient methods involved in the design of embedded systems based on such type of representation. The main "classical" research directions are:

semantic foundations Typically here we try to provide sound structural operational semantics, or model translation to provide a behavioral interpretation to all the specification primitives in our formalisms. We study correctness issues such as constructive causality, process reincarnation and the likes. We also study the connection to prevalent modeling formalisms, such as (synchronous) block-diagrams or schematic-level hardware circuit dscriptions.

efficient compilation The existence of reference models can then be taken as a yardstick to evaluate the design of efficient implementation techniques, based on odel representations. Compositionality issues are in order here.

optimization and automatic verification High-level translations usually end up with code that is not optimal. Here we study the various methods for code optimization, borrowed from different horizons to match the relevant domains. Circuit and bollean optimizations are primarily used currently. The semantic interpretation also allows powerful automatic verification (model-checking) techniques, based on operational structures. We have built a particular competency on finite-state model-checking over the years with our checkers AUTO/GRAPH, then XEVE.

while newer topics involve:

static analysis The translation and expansion of Esterel programs to lower-evel operational models involve a number of specific transformation/compilation phases. So far the design of the compiler itself was not relying on any formal or informal techniques, and its asserted relation with the official semantics was only stated as a matter of correct reimplementation of intricate functions. Our use of static analysis technqiues, directly extracted from correct semantic rules, can be seen as an attempt to extract a compiler specification before-hand on many aspects, thereby leveraging the concerns for code corectness and code validation.

distributed implementation So far the main implementations of Esterel remain sequential. While respecting the synchronous hypothesis, we are willing the face the issue of code distribution in an embedded setting, with an architectural model providing target description.

## 3.2. High-level modeling of Synchronous systems (and beyond)

**Participants:** Robert de Simone, Charles André.

Currently, the synchronous assumptions are contradictory to many of UML ones. We want to endow some of UML diagrammatical notations, found useful for modeling practice, in a synchronous setting.

SyncCharts were a first attempt at describing formal models of synchronous formalisms using UMl-like diagrammatic notations (in this case state diagrams, actually introduced later than SyncCharts). We want to extend this move to other parts of the UML unified notations (as already well started by Charles André and its team). But, importantly, while doing so we want to promote and stay faithful to our semantic standards. In fact we believe that synchronous systems (and variants) are very important in modeling *different domains* than those classicallly tacked by UML (asynchronous threads and CORBA middleware) concerning concurency. Instead we aim at representatioon of real-time embedded systems and controlers, where simultaneous behaviours and instantaneous propagation are the rule at modeling level.

# 4. Application Domains

## 4.1. Real-Time Embedded Systems

**Key words:** *embedded systems*, *automotive*, *aircraft*, *mobile telephone*, *electronic appliances*, *safety-critical*, *design-flow*, *systems-on-chip*.

The main application doamin for our techniques resides in real-time embedded applications such as found in modern transportation vehicles (cars, planes), in the convergence of telephones, PDAs and other small electronic appliances allying fancy modal interfaces and intensive data computations for multimedia signal processing.

We are currently formalizing more extensive collaborations with industrial parners of these fields, such as Thales, Texas Instruments, ST MicroElectronics or Nokia. With the forthcoming advent of AOSTE we should also extend collaborations towards transportation industry companies (as present in the OSTRE team).

# 5. Software

## 5.1. Modules for analysis and compilation of Esterel programs

**Participants:** Robert de Simone [correspondant], Fabrice Peix, Dumitru Potop [post-doc Irisa], Olivier Tardieu, Eric Vecchié.

**Key words:** *Esterel*, *reactive synchronous formalisms*, *compilation*, *static analysis*, *verification*, *model-checking*, *distributed code generation*.

The official distribution of ESTEREL is now handled by Esterel Technologies. We still use the former academic version to support new tool developpement for additional modules implementing new techniques and research ideas in various directions. A distinct prototype compiler is also developed, based on static analysis formulations of several important specific compilation phases, and their direct reflection into CaML code.

Recent developments and software initiatives led in our team around Esterel or SyncCharts comprise:

an efficient software code compiler, written by Dumitru Potop, from an imtermediate representation format named GRC. This compiler only execute as far as possible code which is usefully activated in a simulation scheme. Results can on some examples be a hundred times faster than the regular compiler, based on the execution of the circuit translation.

a Syntax-driven model checker, written by Eric Vecchié during its PhD thesis. See section 6.1 for technical motivations. The BDD symbolic implemnetation gives promising results on the preliminary case studies conducted.

a translator to SynDEx format, written by Fabrice Peix in the course of its PhD thesis. The main concern here is to provide the translation in such a way that the embedded mapping of SynDEx towards architectural descriptions can benefit at the most of potential concurrency and independence relations. More powerful directives (such as informations on exclusive behaviors that could be mapped on teh same resource) should also be provided. This may lead in places to an actual extension of the SynDEx interface, as well as of its internal algorithms. See more practical details in section 6.2.

a new Esterel compiler based on static analysis correctness features, written by Olivier Tardieu from his PhD results. Despite advertising sound and precise behavioral semantics for programs, the mainline ESTEREL compiler does not rely truly on any formal method for its implementation, and the relations between the compilation theory and this compiler are only some of trust and confidence to the implementers. While studying the formalization of some, if not most, compliation issues tied to Esterel as static analysis ones, we were able to lay the ground for a potential validation of the relevant compiler phases (instantaneous loop detection, reincarnated code problems,...), at least by a formalisation from which the implementation is far more directly obtained. See 6.3 for details.

## 5.2. Modules for analysis and compilation of SyncCharts specifications

**Participants:** Charles André [correspondant], Gérald Vormbrock.

SYNCCHARTS are a graphical formalism close to textual ESTEREL, developed in the I3S SPORTS team by Charles André and his collegues. Under funding by the 5th PCRD NoE ARTIST (a joint INRIA participation handled at IRISA by A. Benveniste), we started a new modular version of the execution engine, flexible so as to experiment with various issues in visual and semantic expressivity.

# 6. New Results

## 6.1. Syntax-driven model checking

**Participants:** Robert de Simone, Eric Vecchié.

This work deals with efficient automatic verification, based on BDD symbolic techniques, here applied to structured Esterel programs [13].

We considered the issue of exploiting the structural form of ESTEREL programs to partition the algorithmic Reachable State Space fix-point construction used in model-checking techniques. The basic idea sounds utterly simple, as seen on the case of sequential composition: in $P;Q$, first compute entirely the states reached in $P$, and then only carry on to $Q$, each time using only the relevant transition relation part. Difficulties appear in our decomposition approach when scheduling the different transition parts in presence of parallelism and local signal exchanges. Program blocks (or "Macro-states") put in parallel can be synchronized in various ways, due to dynamic behaviors, and considering all possibilities may lead to an excessive division complexity. The goal was here to find a satisfactory trade-off between compositional and global approaches.

## 6.2. Distributed embedding of Esterel programs

**Participants:** Robert de Simone, Fabrice Peix.

This work deals with the issue of distributed implementation of control-dominated synchronous programs, and tries to set up a formal correpondance between Esterel and SynDEx at the proper level of abstraction.

SYNDEX currently allows to distribute Synchronous data flow programs over a hardware architecture, with the optimization objectives both in space and time consumed. As control flow takes a prevalent place in ESTEREL, a large behavior part remains inactive at each reaction. Our objective was to connect ESTEREL with **SynDEx** while introducing and exploiting the high level information given by the control constructs of the language. The information of exclusion between parts of program, extracted from **Esterel**, can be used to improve the placement of the program over the hardware architecture. For this purpose we study relation between control flow and data flow models, and more precisely how to interconnect these two approaches in one unified model. This model must integrate the data path linking variables of the program through compute operator networks (as in block diagrams), while the program drives such computation blocks and their connections to insure the correct flow principle (each data used must be produced, and vice-versa). This work was realized in connection with the INRIA OSTRE team.

## 6.3. Static Analysis of Synchronous Languages

**Participants:** Robert de Simone, Olivier Tardieu.

This work deals with the formal specification of an Esterel compiler itself, and compiler correctness.

Compilers for synchronous languages not only benefit from static analysis techniques in optimization passes, but they heavily rely on them just to achieve correct compilation.

We formalize two key analyses involved in the compilation of the synchronous language ESTEREL, respectively concerned with instantaneous loops [9] and schizophrenia [11]. Instantaneous loops lead to diverging behaviors and must be rejected. Schizophrenic programs – programs having instantly reentered statements – have to be identified as they require special care from the compiler.

In addition, we consider the introduction of a new "jump" primitive in ESTEREL [12]. We use it for encoding state machines in the language, and to define a program transformation that efficiently rewrites schizophrenic programs into non-schizophrenic equivalent programs.

### 6.4. Integration of Data and Control flows in Synchronous models

**Participants:** Robert de Simone, Charles André.

This works with the independent description, and later integration of data paths and control flows in high-level, UML-inspired modeling of synchronous applications.

SYNCCHARTS and ESTEREL are designed at modeling control-dominated systems, just as other synchronous languages such as LUSTRE and SIGNAL aim more towards dat-flow declarative programming and block-diagram modeling. As the traditional compilation of ESTEREL to "circuits" transforms to a large extent control into (Boolean) data flow, a natural question arised about the natural connection between the two styles, and the proper integration to preserve and associate the best of each ? This question was seconded by the commercial acquisition of SCADE by ESTEREL TECHNOLOGIES, stresing the need for an harmonious merge of the formalisms.

We chose to tackle this isue in the context of UML-like high-level modeling. SYNCCHARTS can be seen a formalism strongly related to STATECHARTS and UML State Machines, but with a synchronous semantics that fits in our view much better some application fields (amongst which embedded systems). Similarly, block diagrams can be related to UML activity diagrams, but with a similar (and even greater) semantic distortion. We presented preliminary results in a satelitte workshop of the UML'2003 conference [8].

## 7. Contracts and Grants with Industry

### 7.1. ST MicroElectronics

**Participants:** Robert de Simone.

In the framework of a regional funding program associating the company ST MicroElectronics (located at Le Rousset, near Aix) with academic partners, we are initiating a colaboration with the group of Marc Benveniste, at the ST SmartCard division, on topics of correct-by-construction design of modern Systems-on-Chip using refinement/abstraction techniques. We hope to enlarge the scope of this initial phase in future years.

## 8. Other Grants and Activities

### 8.1. Regional Actions

**Participants:** Robert de Simone.

We are taking an active part in the preparation of the CIM PACA proposal initiative. This project aims, on a regional scale, at bringing together academic and industrial partners active in microelectronic design and related area. The expected added value obtained from promoting collaboration and synergies should help identify PACA as a place of excellence on these topics. Although this project is not officially accepted yet we already invested a significant amount of energy in its definition. Academic participants include all regional Sciences universities, CNRS, ENST/Eurecom, CMP, and INRIA. Industrial partnership lists ST MicroElectronics, Texas Instruents, GemPlus, Atmel, Philips, Infineon, with additional local SMEs and tool providers Synopsys, Cadence, Mentor Graphics.

### 8.2. National Actions

**Participants:** Robert de Simone, Charles André.

In the context of a THALES/CEA/INRIA joint initiative named CARROLL, we contribute to the PROTES project, dedicated to the establishment of a UML profile for Real-Time embedded systems capturing most of the Synchronous Hypothesis requirements. INRIA partners involve the DART, ESPRESSO, OSTRE teams.

## 8.3. European Actions

### *8.3.1. ITEA P2I*

**Participants:** Robert de Simone, Fabrice Peix, Yves Sorel [Ostre team].

We participate to this consortium together with the OSTRE and DART INRIA teams. Other parners are ESTEREL-TECHNOLOGIES, THALES, NOKIA, and the finnish universities of Tampere and Turku. The prospect is to study the immersion of synchronos and intensive data computing in a UML-like framework, with applications to multimedia and mobile telephony. Another. more concrete aspect for us concerns the connection of Esterel to SynDEx.

### *8.3.2. ITEA EAA-EAST*

**Participants:** Charles André, Yves Sorel [Ostre team].

This project (recently closed) gathered most of the european industry car manufacturers, together with prominant suppliers. The objective was to define and develop a common modeling language (in the spirit of UML and ADLs) for automotive applications. Charles André presented our views on synchronous behaviors, and attended several meetings. A continuation project is still pending (on Automotive UML).

### *8.3.3. IST NoE ARTIST*

**Participants:** Robert de Simone, Olivier Tardieu.

This large european consortium gathers a large number of academic partners on the subject of "Real-Time Embedded Systems". Several INRIA teams appear, under the heading of A. Benveniste at IRISA. See ARTIST web page for details. The project is divided in three main Tasks (Hard Real-Time, Components, Scheduling). Its main achievements were to produce perspective roadmaps and training curricula in the three fields.

# 9. Dissemination

## 9.1. Involvements in animation of the scientific community

Charles André was Head of the "Ecole Doctorale STIC" of UNSA (University of Nice/Sophia-Antipolis) until summer 2003. He is a member of the *"Commision de Spécialiste"* (Recrutement jury) in Control theory and Signal Procesing (61th section) at UNSA.

Robert de Simone is a member of the *"Commision de Spécialiste"* (Recrutement jury) in Computer Science (27th section) at UNSA. He is member of the editorial board of the french TSI revue. He is program committee member for the SLAP'03 and MEMOCODE'04 workshops. He was reviewer and examiner of Jean-Pierre Talpin HDR defense.

Al the members of the team attended the yearly SYNCHRON seminar, which gathers french and international researchers active in the field, this year in Luminy near Marseille.

## 9.2. Teaching

Robert de Simone gives a course on "Formal Methods and software Safety/Trustability" in the UNSA Computer Science DEA (Graduate level). He teaches also on similar topics at ISIA (*Institut Superieur d'Informatique et d'Automatique*, a specialized engineer training school run by the Ecole des Mines de Paris). Both courses are about 25 hours.

Under the functions of ATER (*Teaching and Research Technical Assistant*), both Fabrice Peix and Eric Vecchié teach and supervise TD sessions on several topics (computer's architecture, Operating system) at UNSA, for 92 hours yearly each.

Olivier Tardieu teaches an Introductory Course on Algorithms (12 hours), at ISIA.

# 10. Bibliography

## Major publications by the team in recent years

[1] A. BENVENISTE, G. BERRY. *The Synchronous Approach to Reactive and Real-Time Systems.* in « Proceedings of the IEEE », number 9, volume 79, September, 1991, pages 1270-1282.

[2] G. BERRY. *The Foundations of Esterel.* series Foundations of Computing Series, MIT Press, 2000, http://www-sop.inria.fr/esterel.org/Html/Downloads/Doc/StartDocument.htm.

[3] G. BERRY. *The Constructive Semantics of Pure Esterel.* electronic version only, 1999, http://www-sop.inria.fr/esterel.org/Html/Downloads/Doc/StartDocument.htm.

[4] G. BERRY. *The Esterel Language Primer.* version electronique, 1999, http://www-sop.inria.fr/esterel.org/Html/Downloads/Doc/StartDoc

[5] F. BOUSSINOT, R. DE SIMONE. *The Esterel Language.* in « Proceedings of the IEEE », September, 1991.

## Books and Monographs

[6] C. ANDRÉ. *Semantics of SSM (Safe State Machine).* Esterel Technologies, electronic version available at http://www.esterel-technologies.com, April, 2003, http://www.esterel-technologies.com.

## Articles in referred journals and book chapters

[7] A. BENVENISTE, P. CASPI, S. EDWARDS, N. HALBWACHS, P. L. . GUERNIC, R. DE SIMONE. *Synchronous Languages Twelve Years Later.* in « Proceedings of the IEEE », January, 2003.

## Publications in Conferences and Workshops

[8] C. ANDRÉ, R. DE SIMONE. *Towards a Synchronous UML Profile ?.* in « Proceedings of the first Workshop on Specification and Validation of UML models for Real-Time and Embedded Systems (SVERTS'03) », 2003, Electronically available.

[9] R. DE SIMONE, O. TARDIEU. *Instantaneous Termination in Pure Esterel.* in « SAS'03 », series LNCS, 2003.

[10] D. POTOP, R. DE SIMONE. *Optimizations for Faster Execution of Esterel Programs.* in « MEMOCODE'03 », 2003.

[11] O. TARDIEU. *Defining, Diagnosing and Curing Schizophrenia in Esterel.* 2004, Submitted to PLDI'04.

[12] O. TARDIEU. *Goto and Concurrency: Introducing Safe Jumps in Esterel.* 2004, Submitted to ESOP'04.

[13] E. VECCHIÉ, R. DE SIMONE. *Syntax-driven behavior partitioning for model-checking of Esterel programs.* http://www.inrialpes.fr/pop-art/people/girault/Slap04/, Submitted to SLAP'04.