Activity Report 2017

Team KAIROS

Logical Time for Formal Embedded System Design

Inria teams are typically groups of researchers working on the definition of a common project, and objectives, with the goal to arrive at the creation of a project-team. Such project-teams may include other partners (universities or research institutions).

Table of contents

Team KAIROS

Creation of the Team: 2017 January 01

Keywords:

Computer Science and Digital Science:
        A1.1.1. - Multicore, Manycore
        A1.1.2. - Hardware accelerators (GPGPU, FPGA, etc.)
        A1.2.5. - Internet of things
        A1.2.7. - Cyber-physical systems
        A1.5.2. - Communicating systems
        A2.2. - Compilation
        A2.3. - Embedded and cyber-physical systems
        A2.4. - Verification, reliability, certification
        A2.5.1. - Software Architecture & Design

Other Research Topics and Application Domains:
        B5.1. - Factory of the future
        B5.4. - Microelectronics
        B6.1. - Software industry
        B6.4. - Internet of things
        B6.6. - Embedded systems
        B6.7. - Computer Industry (harware, equipments...)
        B7.2. - Smart travel
        B8.1. - Smart building/home
        B8.2. - Connected city
        B9.4.1. - Computer science

1. Personnel

Research Scientists
    Robert de Simone [Team leader, Inria, Senior Researcher, HDR]
    Eric Madelaine [Inria, Researcher, HDR]

Faculty Members
    Julien Deantoni [Univ de Nice - Sophia Antipolis, Associate Professor]
    Frederic Mallet [Univ de Nice - Sophia Antipolis, Professor, HDR]
    Marie Agnes Peraldi Frati [Univ de Nice - Sophia Antipolis, Associate Professor]
    Sid Touati [Univ de Nice - Sophia Antipolis, Professor, HDR]

PhD Students
    Hui Zhao [Inria and Labex UCN@sophia]
    Emilien Kofman [Inria, until Feb 2017]

Technical staff
    Luc Hogie [CNRS, part-time]
    Ales Mishchenko [Inria, PIA Clarity project, until Aug 2017]
    Amin Oueslati [Inria, PIA Clarity project]

Interns

Giovanni Liboni [Inria, until May 2017]
Arsak Megkrampian [Inria, from Mar 2017 until Aug 2017]
Xudong Qin [Inria, until Feb 2017]

Administrative Assistants

Patricia Lachaume [Inria]
Christine Riehl [Inria, until Feb 2017]

Visiting Scientists

Dongdong An [PhD at East China Normal University]
Marwa Hami [Visiting PhD, ENISO Sousse, from Oct 2017]
Zauwali Sabitu Paki [Univ de Nice - Sophia Antipolis, from Nov 2017]
Reinhard Von Hanxleden [UCA Visiting Professor from Kiel Univ., from Jul 2017 until Sep 2017]

2. Overall Objectives

2.1. Overall Objectives

The Kairos proposal ambitions to deal with the Design of Cyber-Physical Systems (CPS), at various stages, using Model-Based techniques and Formal Methods. Design here stands for co-modeling, co-simulation, formal verification and analysis activities, with connections both ways from models to code (synthesis→, and ←──instrumentation for optimization). Formal analysis, in turn, concerns both functional and extra-functional correctness properties. Our goal is to link these design stages together, both vertically along the development cycle, and horizontally by considering the interactions between cyber/digital and physical models. These physical aspects comprise both physical environments and physical execution platform representations, which may become rather heterogeneous as in the cases of the Internet of Things and computing at the edges of the gateways. The global resulting methodology can be tagged as Model-Based, Platform-Based CPS Design (fig.1).

CPS design must take into account all 3 aspects of application requirements, execution platform guarantees and contextual physical environment to establish both functional and temporal correctness. The general objective of the Kairos proposal is thus to contribute in the definition of a corresponding design methodology, based on formal Models of Computation for joint modeling of cyber and physical aspects, and using the important central concept of Logical Time for expressing the requirements and guarantees that define CPS constraints.

Logical Multiform Time. It may be useful to provide an introduction and motivation for the notion of Logical Multiform Time (and Logical Clocks), as they play a central role in our approach to Design. We call Logical Clock any repetitive sequence of occurrences of an event (disregarding possible values carried by the event). It can be regularly linked to physical time (periodic), but not necessarily so: fancy processors may change speeds, simulation engine change time-integration steps, or much more generally one may react with event-driven triggers of complex logical nature (do this after 3-times that unless this...). It is our belief that user specifications are generally expressed using such notions, with only partial timing correlations between distinct logical clocks, so that the process of realization (or "model-based compilation") consists for part in establishing (by analysis or abstract simulation) the possible tighter relations between those clocks (unifying them from a partial order of local total orders to a global total order). We have defined in the past a small language of primitives expressing recognized constraints structuring the relations between distinct logical clocks. This language (named CCSL for Clock Constraint Specification Language), borrows from notions of Synchronous Reactive Languages, Real-Time Scheduling Theory, and Concurrent Models of Computations and Communication (MoCCs) in Concurrency Theory altogether. Corresponding extensions of Timed Models originally based on single (discrete or continuous) time can also be considered. Logical Time is used in our approach to express relation constraints between heterogeneous models, of cyber or physical origin, and to support analysis and co-simulation. Addressing cyber-physical systems demands to revisit logical time to deal with the multi-physical and sometimes uncertain environments.
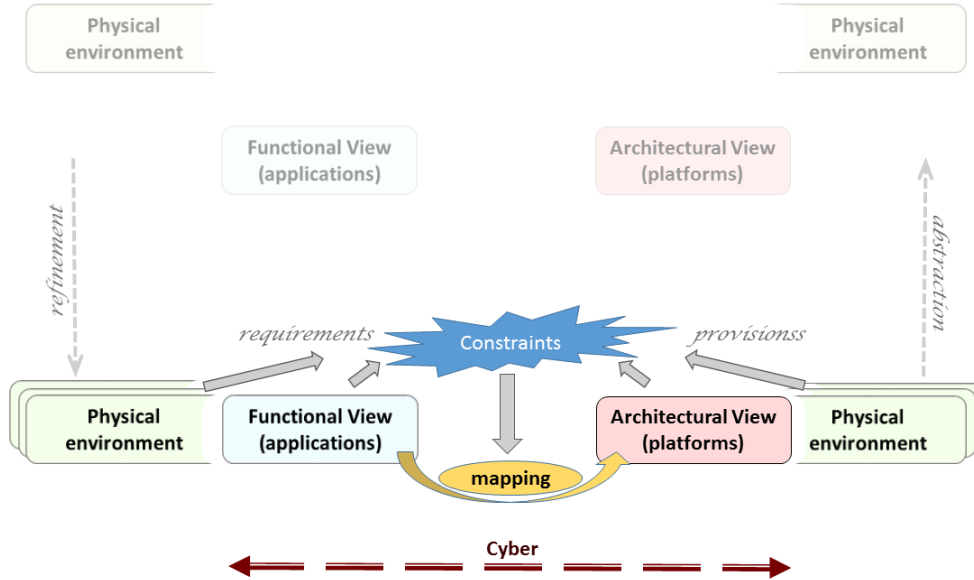
Figure 1. Cyber-Physical generic architectural features

In the following sections we describe in turn the research agenda of Kairos on co-modeling, co-simulation, co-analysis and verification, and relation from models to code, respectively.

3. Research Program

3.1. Cyber-Physical co-modeling

Cyber-Physical System modeling requires joint representation of digital/cyber controllers and natural physics environments. Heterogeneous modeling must then be articulated to support accurate (co-)simulation, (co-)analysis, and (co-)verification. The picture above sketches the overall design framework. It comprises functional requirements, to be met provided surrounding platform guarantees, in a contract approach. All relevant aspects are modeled with proper DSLs, so that constraints can be gathered globally, then analyzed to build a mapping proposal with both a structural aspect (functions allocated to platform resources), but also a behavioral ones, scheduling activities. Mapping may be computed automatically or not, provably correct or not, obtained by static analytic methods or abstract execution. Physical phenomena (in a very broad acceptance of the term) are usually modeled using continuous-time models and differential equations. Then the "proper" discretization opportunities for numerical simulation form a large spectrum of mathematical engineering practices. This is not at all the domain of expertise of Kairos members, but it should not be a limitation as long as one can assume a number of properties from the discretized version. On the other hand, we do have a strong expertise on modeling of both embedded processing architectures and embedded software (= the kind of usually concurrent, sometimes distributed software that reacts to and control the physical environment). This is important as, unlike in the "physical" areas where modeling is common-place, modeling of software and programs is far from mainstream in the Software Engineering community. These domains are also an area of computer science where modeling, and even formal modeling, of the real objects that are originally

of discrete/cyber nature, takes some importance with formal Models of Computation and Communications. It seems therefore quite natural to combine physical and cyber modeling in a more global design approach (even multi-physic domains and systems of systems possibly, but always with software-intensive aspects involved). ur objective is certainly not to become experts in physical modeling and/or simulation process, but to retain from it only the essential and important aspects to include them into System-Level Engineering design, based on Model-Driven approaches allowing formal analysis.

This sets an original research agenda: Model-Based System Engineering environments exist, at various stages of maturity and specificity, in the academic and industrial worlds. Formal Methods and verification/certification techniques also exist, but generally in a pointwise fashion. Our approach aims at raising the level of formality describing relevant features of existing individual models, so that formal methods can have a greater general impact on usual, "industrial-level", modeling practices. Meanwhile, the relevance of formal methods is enhanced as it now covers various aspects in a uniform setting (timeliness, energy budget, dependability, safety/security).

New research directions should focus on the introduction of uncertainty (stochastic models) in our particular framework, on relations between (logical) real-time and security, on the concern with discovery and mobility inherent to Connected Objects and Internet of Things. While sketched below, these issues are developed in the long version of the Kairos proposal.

3.2. Cyber-Physical co-simulation

The FMI standard (Functional Mock-Up interface) has been proposed for "purely physical" co-simulation, and then adopted in frameworks such as Matlab/Simulink and Ansys, to mention two famous model editors. Conversely, the SystemC extension language of C/C++ is also a popular standard for hardware and System-on-Chip (SoC) simulation. A closer inspection shows that our kind of targeted "reactive" software applications share some of the features in that spectrum. But none of these formalisms and standards actually aims or pretends to describes in any formal way the functional and temporal constraints that are to bind several simulation models together.

3.3. Formal analysis and verification

Because the nature of our constraints is specific, we want to adjust verification methods to the goals and expressiveness of our modeling approach. Quantitative (interval) timing conditions on physical models combined with (discrete) cyber modes suggest the use of SMT (Satisfiability Modulo Theories) automatic solvers, but the natural expressiveness requested (as for instance in our CCSL constructs) shows this is not always feasible. Either interactive proofs, or suboptimal solutions (essentially resulting of abstract run-time simulations) should be considered. Complementarily to these approaches, we are experimenting with new variants of symbolic behavioural semantics, allowing to construct finite representations of the behaviour of CPS systems with explicit handling of data, time, or other non-functional aspects.

3.4. Relation to Code and Optimization

While models considered in Kairos can also be considered as executable specifications (through abstract simulation schemes), they can also lead to code synthesis and deployment. Conversely, code execution of smaller, elementary software components can lead to performance estimation enriching the models before global mapping optimization. CPS introduce new challenging problems for code performance stability. Indeed, two additional factors for performance variability appear, which were not present in classical embedded systems: 1) variable and continuous data input from the physical world and 2) variable underlying hardware platform. For the first factor, CPS software must be analysed in conjunction with its data input coming from the physics, so the variability of the performance may come from the various data. For the second factor, the underlying hardware of the CPS may change during the time (new computing actors appear or disappear, some actors can be reconfigured during execution). The new challenge is to understand how these factors influence performance variability exactly, and how to provide solutions to reduce it or to model it. The modeling of performance variability becomes a new input.

4. Application Domains

4.1. Model-Based Embedded System Design

Kairos general area of activity is embedded systems, as found in transportation (automotive, avionics), connected objects (smartphones,...) satellites, smart AE... More specifically we are focused on the design methods and tools to model and deploy such systems, where software is tightly coupled to its physical environment and its heterogenous running platform. Inversely we are not focused in designing new nature of cyber-physical models, but rather to study tools that help collaborative design between engineers of these distinct fields.

5. New Software and Platforms

5.1. Vercors Component Editor (VCE)

VERification of models for distributed communicating COmponants, with safety and Security

FUNCTIONAL DESCRIPTION: The Vercors tools include front-ends for specifying the architecture and behaviour of components in the form of UML diagrams. We translate these high-level specifications, into behavioural models in various formats, and we also transform these models using abstractions. In a final step, abstract models are translated into the input format for various verification toolsets. Currently we mainly use the various analysis modules of the CADP toolset.

RELEASE FUNCTIONAL DESCRIPTION: It includes integrated graphical editors for GCM component architecture descriptions, UML classes, interfaces, and state-machines. The user diagrams can be checked using the recently published validation rules from, then the corresponding GCM components can be executed using an automatic generation of the application ADL, and skeletons of Java files.

- Participants: Antonio Cansado, Bartlomiej Szejna, Eric Madelaine, Ludovic Henrio, Marcela Rivera, Nassim Jibai, Oleksandra Kulankhina and Siqi Li
- Contact: Eric Madelaine
- URL: http://www-sop.inria.fr/oasis/index.php?page=vercors

5.2. TimeSquare

KEYWORDS: Profil MARTE - Embedded systems - UML - IDM
SCIENTIFIC DESCRIPTION: TimeSquare offers six main functionalities:

* graphical and/or textual interactive specification of logical clocks and relative constraints between them,

* definition and handling of user-defined clock constraint libraries,

* automated simulation of concurrent behavior traces respecting such constraints, using a Boolean solver for consistent trace extraction,

* call-back mechanisms for the traceability of results (animation of models, display and interaction with waveform representations, generation of sequence diagrams...).

* compilation to pure java code to enable embedding in non eclipse applications or to be integrated as a time and concurrency solver within an existing tool.

* a generation of the whole state space of a specification (if finite of course) in order to enable model checking of temporal properties on it

FUNCTIONAL DESCRIPTION: TimeSquare is a software environment for the modeling and analysis of timing constraints in embedded systems. It relies specifically on the Time Model of the Marte UML profile, and more accurately on the associated Clock Constraint Specification Language (CCSL) for the expression of timing constraints.

- Participants: Benoît Ferrero, Charles André, Frédéric Mallet, Julien Deantoni and Nicolas Chleq
- Contact: Julien Deantoni
- URL: http://timesquare.inria.fr

5.3. GEMOC Studio

KEYWORDS: DSL - Language workbench - Model debugging
SCIENTIFIC DESCRIPTION: The language workbench put together the following tools seamlessly integrated to the Eclipse Modeling Framework (EMF):

- Melange, a tool-supported meta-language to modularly define executable modeling languages with execution functions and data, and to extend (EMF-based) existing modeling languages. - MoCCML, a tool-supported meta-language dedicated to the specification of a Model of Concurrency and Communication (MoCC) and its mapping to a specific abstract syntax and associated execution functions of a modeling language. - GEL, a tool-supported meta-language dedicated to the specification of the protocol between the execution functions and the MoCC to support the feedback of the data as well as the callback of other expected execution functions. - BCOoL, a tool-supported meta-language dedicated to the specification of language coordination patterns to automatically coordinates the execution of, possibly heterogeneous, models. - Sirius Animator, an extension to the model editor designer Sirius to create graphical animators for executable modeling languages.
FUNCTIONAL DESCRIPTION: The GEMOC Studio is an eclipse package that contains components supporting the GEMOC methodology for building and composing executable Domain-Specific Modeling Languages (DSMLs). It includes the two workbenches: The GEMOC Language Workbench: intended to be used by language designers (aka domain experts), it allows to build and compose new executable DSMLs. The GEMOC Modeling Workbench: intended to be used by domain designersto create, execute and coordinate models conforming to executable DSMLs. The different concerns of a DSML, as defined with the tools of the language workbench, are automatically deployed into the modeling workbench. They parametrize a generic execution framework that provide various generic services such as graphical animation, debugging tools, trace and event managers, timeline, etc.

- Participants: Didier Vojtisek, Dorian Leroy, Erwan Bousse, Fabien Coulon and Julien Deantoni
- Partners: IRIT - ENSTA - I3S - OBEO - Thales TRT
- Contact: Benoît Combemale
- URL: http://gemoc.org/studio.html

5.4. BCOol

BCOoL
KEYWORDS: DSL - Language workbench - Behavior modeling - Model debugging - Model animation
FUNCTIONAL DESCRIPTION: BCOoL is a tool-supported meta-language dedicated to the specification of language coordination patterns to automatically coordinates the execution of, possibly heterogeneous, models.

- Participants: Julien Deantoni, Matias Vara Larsen, Benoît Combemale and Didier Vojtisek
- Contact: Julien Deantoni
- URL: http://www.gemoc.org

5.5. MoCCML

KEYWORDS: DSL - Language workbench - Modeling workbench - Model debugging - Model animation

FUNCTIONAL DESCRIPTION: The MoCCML / Concurrency provides components and engines supporting concurrency and/or time in execution semantics.

- Participants: Julien Deantoni, Didier Vojtisek, Joël Champeau, Benoît Combemale and Stephen Creff
- Partner: ENSTA
- Contact: Benoît Combemale
- URL: http://www.gemoc.org

6. New Results

6.1. Formal Model-Based, Platform-Based System Engineering for CPS heterogeneous systems

Participants: Julien Deantoni, Robert de Simone, Frédéric Mallet, Marie-Agnès Peraldi-Frati, Ales Mishchenko.

The proper inclusion of our models and techniques into a realistic or proto-industrial design flow is a topic of discussion with partners, which brings back a number of fundamental issues about the nature of modeling itself, specially to allow and promote further analysis. The modeling of execution platforms, which may seem primarily architectural, is itself in fact subject to combined physical model interplay with functionality (as in power consumption and heat dissipation in processors); Internet of Things and industrial embedded systems are new specific focuses for us here. In this context we have been concentrating in the course of the PIA Clarity project (see 7.1) on the CAPELLA system engineering language, and its multi-view aspects; in the new IRT Saint-Exupery ATIPPIC collaboration we intend to focus on a realistic-scale use-case modeled with CAPELLA and proper formal annotations for the design of micro-satellite systems with COTS processor architectures.

6.2. Cyber extensions for the FMI physical API

Participants: Julien Deantoni, Giovanni Liboni, Robert de Simone.

The challenge here is to specify how an appropriate behavioral interface can be specified at the language level so that individual simulators can provide sufficient interface information to allow their correct coordination in terms of correctness and performance. Using our modeling approaches to describe formally the specificities of simulators and scheduling patterns, maybe even targeting synthesis of efficient interactions, is a new research topic [9], conducted in art in the context of the GLOSE project (see 7.1.2) in collaboration with SAFRAN tech.

6.3. Logical Time and Uncertain Physical environments

Participants: Frédéric Mallet, Robert de Simone, Dongdong An.

We developed a specific formalism to express logical time constraints on models. Currently it remains mainly aimed at purely "cyber" models. Combination with continuous physical models, and stochastic uncertainty, will be further studied at the level of constraint expressiveness. The issue of expressing meaningful discrete clocks from stochastic clock schemes, and combining the resulting clocks borne from physics to other clocks borne from sampling oberver environment, is a topic of collaboration with ECNU Shanghai through the PhD long-term visit of AN Dongdong to Sophia, and other discusions as well [3].

6.4. Automatic analysis and verification for specific classes of models

Participants: Robert de Simone, Frédéric Mallet, Emilien Kofman, Julien Deantoni.

This part aims at continuing and extending our work on "mostly-automatic"verification, with SMT solvers and model-checking in place to compute optimal scheduling and allocation, for instance. The new expressiveness of CPS adds new challenges [10]. While the global problem of schedulability for a generic CCSL specification is an open problem. We have identified a particular subclass of scheduling called "periodic scheduling" and establish a sufficient conditions for detecting if there is a valid periodic scheduling for a given CCSL specification. This condition is checked using the MAUDE rewriting system that directly encodes the operational semantics of CCSL [8]. However, the performances highly depend on the "period" of the periodic scheduling.

A more efficient solution based on SMT solver is under investigation and has given first encouraging results. A specific direction is reported in Emilien Kofman PhD thesis [1].

6.5. Behavioral semantics and equivalence notions for Open Systems

Participants: Eric Madelaine, Xudong Qin.

Model-Based Design naturally implies model transformations. To be proven correct, they require equivalence of "Open" terms, in which some individual component models may be omitted. Proper behavioral equivalence in the domain of CPS (which may include variants) is the challenge here. Such models take into account various kind of data parameters, including, but not limited to, time. The middle term goal is to build a formal framework, but also an effective tool set, for the compositional analysis of such programs. Our joint work (between Eric Madelaine and Ludovic Henrio from France, professors Zhang Min, Deng Yuxin and students from ECNU) on symbolic approaches to the composition of concurrent processes has progressed mainly on the pratical side, with an implementation of a prototype algorithm computing the symbolic semantics (called Open Automata) of open systems, and validating the approach for encoding constructs of various formalisms. A paper has been submitted for publication. As a particular set of use-cases, we have started using pNets to encode the behavior of "Architecture Templates" of the BIP language, with the aim of proving generic properties of these constructs, and building full systems by combining such architectures, with proven guarantees.

We have published preliminary work proposing a framework for open systems defining their symbolic semantics and some verification mechanisms (equivalences, model-checking), and we have started developing prototype tools supporting this approach.

This is joint work with ZHANG Min, from ECNU Shanghai, partially conducted in the framework of the FM4CPS associated-team.

6.6. Formal model of computations, mobility and resource discovery adapted for CPS

Participants: Robert de Simone, Luigi Liquori.

We will adapt formal Models of Computations and formal system like Type Theory to capture properties for distributed, networked and mobile CPS. Discovering and synchronizing, possibly in presence of mobility, are important issues in CPS. We will extend our past distributed resource discovery model with a notion of logical time; the difficulty comes to both discover and synchronize CPSs having different logical times.

6.7. Logical Frameworks with logical time

Participants: Luigi Liquori, Robert de Simone.

Adapting the Logical Framework (LF) based on Type Theory to better understand the analysis and verification of CPS is the challenge here. Previous works on extending Logical Framework with Locked Types and Proof-functional logics could captures the notion synchronizing (via a suitable constraint resolution) two proof systems: the internal and the external one; this type can be viewed as a form of communication between the internal and the external logic. Applications could be feed by suitable outputs of the CPS co-modeling pillar phase like, e.g. CCSL expressions.

6.8. From code to model

Participant: Sid Touati.

This research result is about modeling code performances using gaussian mixtures. Thanks to this performance model, we propose additional precise performance metrics. Our additional statistical metrics for analysing and comparing program performances give the user more precise decision tools to select best code versions, not necessarily based on mean or median numbers. Also, we provide a new metric to estimate performance variability based on Gaussian mixture model. Our statistical methods are implemented with R and distributed as open source code.

This is a collaboration with Julien Worms (LMV, UVSQ), reported in [7].

6.9. From model to code

Participants: Amine Oueslati, Robert de Simone, Arsak Megkrampian.

Synthesizing programs and algorithms in an optimal fashion may call for model transformations, as above, but also on careful tuning at program level, which make take into consideration a number of concrete phenomena absent from abstract models (at the cost of losing exhaustivity). Specific code optimization techniques in a CPS design context is the challenge here. WE are collaborating with Dumitru Potop-Butucaru (formerly from the Aoste team) on the topic, where he develops the LoPhT (Logical to Physical Time) environment dealing with these issues.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. IRT Saint-Exupery ATIPPIC project

Participants: Robert de Simone, Julien Deantoni, Amin Oueslati.

We are collaborating here with Thales Alenia Space and some of their partners, with engineering forces put in secondment to the direct governance of IRT Saint-Exupery, on the topic of introducing COTS processor usage for satellite mission systems, with the corresponding methodological needs (sharing software tasks on a single (multi)processor, with safety-critical constraints against cosmic radiations). We attempt to make this a show-case study for our formal model-based design approach.

7.1.2. GLoSE project of the SAFRAN DESIR research programme

Participants: Robert de Simone, Julien Deantoni, Giovanni Liboni, Frédéric Mallet.

SAFRAN tech set up a collaborative research programme with the major French academic partners in the field of Embedded Systems and Data Analytics, named DESIR. Robert de Simone is Prime Investigator for the Embedded System side. Julien DeAntoni heads a specific research project of this programme, named GloSE (Globalization in Systems Engineering), on co-modeling and co-design to enable co-simulation using enhanced FMU/FMI interfaces. A new PhD thesis should start early next year under a related CIFRE grant, with Giovanni Liboni as PhD candidate (he was with us already as intern last Spring).

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. UCA project Smart IoT for Mobility

Participants: Frédéric Mallet, Julien Deantoni, Robert de Simone, Marie Agnès Peraldi-Frati.

We have started a collaboration with Renault Software Lab and Orange in Sophia Antipolis to apply our system engineering to the field of connected vehicles. The goal is to model formally and with digital models contracts between car manufacturers (like Renault) and service providers that should provide new services for connected vehicles. The contract also involves the communication infrastructure provider (here Orange) that operates the communications. A project funded by Academy RISE of UCA Jedi has started in December 2017 with a Master student starting at the beginning of January 2018. This project is done in collaboration with the LEAT laboratory and the GREDEG Laboratory which provides experts on legal issues for connected objects.

8.2. National Initiatives

8.2.1. FUI CLISTINE

Participants: Robert de Simone, Amin Oueslati, Emilien Kofman.

This project was officially closed this year, but work had finished by the end of last year. The outcomes were somehow weakened by the fact that the original project leader failed to integrate the results of various partners into the promised innovative architecture of network-on-board.

8.2.2. Investissements d'Avenir: PIA Clarity

Participants: Julien Deantoni, Ales Mishchenko, Robert de Simone, Amine Oueslati, Frédéric Mallet, Marie Agnès Peraldi-Frati.

This project is funded by the LEOC Call (*Logiciel Embarqué et Objets Connectés*) of the national support programme *Investissements d'Avenir*. It will end in December 2017. Partners are: Thales (several divisions), Airbus, Areva, Altran, All4Tec, Artal, the Eclipse Fondation, Scilab Enterprises, CESAMES, U. Rennes, and Inria. The purpose of the project is to develop and promote an open-source version of the ARCADIA Melody system design environment from Thales, renamed CAPPELLA for that purpose. In this project we investigated extensions of Capella to enable simulation and analysis of mode automata in the context of model based system engineering.

8.2.3. PEPS CNRS INS³PECT

Participants: Marie Agnès Peraldi-Frati, Julien Deantoni, Frédéric Mallet.

The project is funded by CNRS-INS2I call PEPS 2017 Connected Objects Algorithms Algorithm, Application and Architecture. It ended in December 2017.
The focus is on System Level engineering for Secured Services for connected Objects. The idea is to have a high level modeling and verification of services that integrate hardware, communication and computing edges, and the software parts. Security is transversal in this value chain and is included as a viewpoint in the design. See https://www.i3s.unice.fr/ins3pect/ for more information.

Academic partners are I3S (Sophia), LIG(Grenoble), LabSTICC (Lorient), LEAT (Sophia). An internal meeting was held in late Spring, while a more open Workshop was held in Sophia in December.

8.3. International Initiatives

8.3.1. Inria International Labs

8.3.1.1. LIAMA project SACCADES

This project was supported by the associated-team FM4CPS 8.3.1.2, with Vania Joloboff from EPI TEA in Inria Rennes as Prime Investigator. The chinese partner was ECNU Shanghai, whose status inside LIAMA was then to be established.

8.3.1.2. FM4CPS

Title: Formal Models and tools for Cyber-Physical Systems

International Partner (Institution - Laboratory - Researcher):

ECNU (China) - Artificial Intelligence Lab - Jifeng He

Start year: 2015

See also: https://project.inria.fr/fm4cps/

Cyber-Physical Systems (CPS) and the connected Internet of Things (IoT) are inherently heterogeneous systems, with ("cyber") computer digital parts interacting with their physical sensible environment, under user requirements for functional and temporal correctness. Thus, design of such systems as a whole requires a diversity of models, and the behavior orchestration between such models must be carefully defined and analyzed.

FM4CPS will address several facets of Formal Model-Driven Engineering for Cyber-Physical Systems and Internet of Things. The design of such large heterogeneous systems calls for hybrid modeling, and the combination of classes of models, most previously well-established in their own restricted area: Formal Models of Computations drawn from Concurrency Theory for the "cyber" discrete processors, timed extension and continuous behaviors for physical environments, requirement models and user constraints extended to non-functional aspects, new challenges for designing and analyzing large and highly dynamic communicating software entities. Orchestration and comparison of models, with their expressive power vs. their decidable aspects, shall be considered with the point of view of hybrid/heterogeneous modeling here. Main aspects are the various timing or quantitative structure extensions relying for instance on a hybrid logical clock model for the orchestration of underlying components.

The associated team aims at various level of research, from formal models, semantics, or complexity, to experimental tools development. This will start for example on one side with building a formal orchestration model for CPSs, based on an hybrid clock model that combine discrete and physical time, synchronous and asynchronous computations or communications. Another goal will be the study of expressiveness and decidability for CPS, based on dedicated sub-families of well-structured push-down systems, addressing both unbounded communication and time-sensitive models.

Beyond their own expertise in this field, the partners will build on the results of previous cooperations in the context of the Liama projects Hades and Tempo, and the associated team DAESD. The current proposal widely broadens the domain of collaboration, and with the inclusion, for the first time, of Jiao Tong University. We expect this is the first step towards the extension of LIAMA in Shanghai with the strengthening of the involvement of E.C.N.U., and the contribution of new top notch universities such as Jiaotong.

8.3.2. Inria International Partners

8.3.2.1. Declared Inria International Partners

A Memorandum of Understanding (MoU) was signed a couple of years ago between Inria and ECNU Shanghai. The same kind was agreement was also concluded between University Côte d'Azur (UCA) and ECNU, covering mostly our colaboration, both on research and on academic student exchange sides.
We have an ongoing contractual collaborative project on our joint activities on co-modeling, named FIDEL, with the Computer Science department from the University of Verona; it is funded on their side by a specific University programme. The collaboration should be strenghtened on our side with the arrival of Giovanni Liboni, formerly student there, as PhD student working with us on a CIFRE grant by SAFRAN on the same topic.

8.3.3. Participation in Other International Programs

We are active members of the International Joint Lab of Trustworthy Software (IJLTS), of which Eric Madelaine is Steering Committee Member. The lab is funded by the Chinese Ministry of Reseach, and headed by ECNU, Shanghai (together with CWI, ENS Rennes, ENS Lyon, as partners amongst others). This Joint Lab forms the counterpart of the FM4CPS associated team and SACCADES LIAMA project, and in particular funded the Chinese partners in joint actions and visits. All this is reported under the FM4CPS Associated-Team section 8.3.1.2.

Marie-Agnes Peraldi Frati is involved in the DNITT (Danang International Institute of Technology) Institute in Vietnam which is co-managed by UCA and University of Danang. She visited the institute 10 days in May 2017 in the context of the IGLOO (Specific Domain Language For Experience Global Orchestration) research project. The research topic is on domain specific scenario language for Home care and eHealth.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Visiting Professors

> Reinhard von Hanxleden
> > Date: July 2017 - Sept. 2017
> > Institution: University of Kiel (Germany)
> Min ZHANG
> > Date: 2017 - 2017
> > East China Normal University (Shanghai, China)
> Jing LIU
> > Date: December 2017 - January 2018
> > East China Normal University (Shanghai, China)

8.4.1.2. Visiting PhD students

> Donddong AN
> > Date: Oct. 2016 - March 2018
> > ECNU Shanghai
> Maroua El Hami
> > Date: Oct. 2017 - July 2018
> > ENISO, Sousse (Tunisia)

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Eric Madelaine was General Chair of the 11th IEEE International conference on Theoretical Aspects of Software Engineering (TASE'2017), which was held in Sophia-Antipolis, september 2017. The whole conference was organized by the services of Inria Sophia Méditerranée Center.
- Marie-Agnès Peraldi-Frati and Frédéric Mallet organized the Workshop InS3Pect System engineering for Secured Services for Connected Objects. The workshop gathered approximately thirty researchers and industrials to explore a transdisciplinary approach for Connected Objects Secured Services modeling and validation https://www.i3s.unice.fr/ins3pect/fr/node/8/.

9.1.1.2. Member of the Organizing Committees

Frederic Mallet was a member of the organizing committee of COMPAS 2017, organized in Antibes from June 27th to 30th 2017 https://compas2017.sciencesconf.org/.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- Robert de Simone: was Program Chair of EMSOFT 2017, part of the federated "superconference" ESWEEK 2017 (Seoul, Korea, October).
- Frédéric Mallet was Program Chair for TASE 2017.
- Eric Madelaine was Steering Committee Chair for the Int. Symposium on Formal Aspects of Component Software (FACS 2017).
- Frederic Mallet was steering committee member of ETR 2017

9.1.2.2. Member of Conference Program Committees

- Robert de Simone: FDL 2017, MEMOCODE 2017.
- Frederic Mallet: DATE 2017, Euromicro DSD 2017, FDL 2017, ModelsWard 2017, DHS 2017, ICTERI 2017.
- Julien Deantoni: Models 2017, DSD 2017, TASE 2017, Momo 2017, GEMOC 2017, EXE 2017, MDEbug 2017.
- Marie-Agnès Peraldi-Frati: national French Conférence en Ingénierie du Logiciel (CIEL).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Eric Madelaine was Guest Editor for the Science of Computer Programming journal, of a special issue on FACS 2016 selected papers.

9.1.4. Invited Talks

Sid Touati gave an Invited Tutorial entitled "Parametric statistics for program performance analysis, comparison and evaluation" at the 2017 International Conference on High Performance Computing and Simulation (HPCS 2017, Genova, Italy).
Eric Madelaine gave an invited seminar at ECNU Shanghai in Nov. 2017.
Frederic Mallet gave an invited talk on the "Model-Based System Engineering for Cyber-Physical Systems" at ECNU in Shanghai and in Suzhou University in December 2017. He also gave an invited talk together with Julien DeAntoni in the GT OVSTR of the Labex Digicosme in Telecom ParisTech in April 2017.
Julien Deantoni was invited speaker on the fourteenth Bellairs CAMPaM workshop on multi-paradigm modeling and simulation, in Barbados (http://msdl.cs.mcgill.ca/conferences/CAMPaM/2017/).

9.1.5. Leadership within the Scientific Community

Robert de Simone is Prime Investigator for the FM4CPS Associated-Team (with ECNU Shanghai); he is also Inria contact coordinator for the DESIR collaborative programme from SAFRAN on embedded system design.
Eric Madelaine is member of the Council Board of the International Joint Lab of Trustworthy Software (IJLTS), from ECNU Shanghai.

9.1.6. Research Administration

Robert de Simone was Deputy Director of the EDSTIC Doctoral School until September 2017.
Frederic Mallet is the deputy director of the I3S Laboratory (UMR 7271 CNRS UNS) and he is in charge of the relationships with LEAT and of the research formations. He is also a member of the Steering Committee of the Poˆle de Compétitivité Solutions Communicantes Sécurisées (SCS) and of its board. He is the head of the first Year of the International Track of the Master on Foundations of Computer Sciences.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: Robert de Simone, Models of Computation for Networks-on-Chips (MoCs for NoCs), 36h, M2 Internationbal, UNS.

Master: Robert de Simone, Functional and Temporal Correctness, 36h, M1 Internationbal, UNS.

Master : Julien Deantoni, Systèmes embarqués et Ambient, 10h, M2, Polytech'Nice, France.

Master : Julien Deantoni, Langage C++, 88h, M1,Polytech'Nice, France.

Master : Julien Deantoni, Finite State Machines, 24h, M1,Polytech'Nice, France.

Master : Julien Deantoni, Internship Management, 20h, M2, Polytech'Nice, France.

Licence : Marie-Agnes Peraldi-Frati, Algorithms and programming 60h,L1, UNS Institute of technology.

Licence : Marie-Agnes Peraldi-Frati, System and Networks administration 80h, L2, UNS Institute of technology .

Licence : Marie-Agnes Peraldi-Frati, Web Programming 50 h, L2, UNS Institute of technology.

Licence: Frédéric Mallet, Conception Orientée Objet, 45h, L3, UNS.

Licence: Frédéric Mallet, Programmation Orientée Objet, 45h, L3, UNS.

Master: Frédéric Mallet, Programmation Avancée et Design Patterns, 45h, M1, UNS.

Master: Frédéric Mallet, Vérification temporelle et fonctionnelle, 24h, M1, UNS.

Master: Frédéric Mallet, Model-Driven Engineering, 24h, M1, UNS.

9.2.2. Supervision

- PhD: Emilien Kofman, *Conception Haut Niveau Low Power d'objets mobiles communicants*, 2017, supervised by Robert de Simone, co-supervised by François Verdier (UMR CNRS/UNS LEAT).
- PhD in progress: Hui (Vincent) Zhao, UNS, started February 2016, supervised by Frédéric Mallet, co-supervised by Ludovic Apvrille (Telecom ParisTech)
- PhD in progress: Dongdong An, ECNU-SEI/China, started November 2016, co-supervised by R. de Simone, supervised by Jing Liu (ECNU).
- PhD in progress: Pierre Leca, CIFRE thesis at Huawey Research Lab (Paris), started 2017, supervised by Gaetan Haines and Ludovic Henrio, co-advisor Eric Madelaine
- PhD in progress: Zhao Yanrui, ECNU-SEI/China, started in January 2017, co-supervised by Yixiang Chen (ECNU) and Frederic Mallet

9.2.3. Juries

Robert de Simone: Examiner (Président) for the PhD of Vincenzo Mastandrea (UCA)

Frédéric Mallet: Examiner (President) for the HDR of Jerome Hugues from ISAE Sup'Aero.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] E. KOFMAN. *Low power application architecture adaptation using SMT solvers*, Université Côte d'Azur, February 2017, https://tel.archives-ouvertes.fr/tel-01534440

Articles in International Peer-Reviewed Journals

[2] R. AMEUR-BOULIFA, L. HENRIO, O. KULANKHINA, E. MADELAINE, A. SAVU. *Behavioural semantics for asynchronous components*, in "Journal of Logical and Algebraic Methods in Programming", 2017, vol. 89, pp. 1 - 40 [*DOI :* 10.1016/J.JLAMP.2017.02.003], https://hal.archives-ouvertes.fr/hal-01526055

[3] Y. BAO, M. CHEN, Q. ZHU, T. WEI, T. ZHOU, F. MALLET. *Quantitative Performance Evaluation of Uncertainty-Aware Hybrid AADL Designs Using Statistical Model Checking*, in "IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems", December 2017, vol. 36, n° 12, pp. 1989 - 2002 [*DOI :* 10.1109/TCAD.2017.2681076], https://hal.inria.fr/hal-01644285

[4] A. KHAN, F. MALLET, M. RASHID. *A framework to specify system requirements using natural interpretation of UML/MARTE diagrams*, in "Software and Systems Modeling", March 2017 [*DOI :* 10.1007/S10270-017-0588-7], https://hal.inria.fr/hal-01670423

[5] V. KHERBACHE, E. MADELAINE, F. HERMENIER. *Scheduling Live Migration of Virtual Machines*, in "IEEE transactions on cloud computing", September 2017, pp. 1-14 [*DOI :* 10.1109/TCC.2017.2754279], https://hal.inria.fr/hal-01644729

[6] F. LEMOINE, T. AUBONNET, L. HENRIO, S. KESSAL, E. MADELAINE, N. SIMONI. *Monitoring as-a-service to drive more efficient future system design*, in "EAI Endorsed Transactions on Cloud Systems", June 2017, vol. 3, n° 9, pp. 1 - 15 [*DOI :* 10.4108/EAI.28-6-2017.152754], https://hal.archives-ouvertes.fr/hal-01582593

[7] J. WORMS, S. TOUATI. *Modelling Program's Performance with Gaussian Mixtures for Parametric Statistics*, in "IEEE Transactions on Multi-Scale Computing Systems", September 2017, 16 p. [*DOI :* 10.1109/TMSCS.2017.2754251], https://hal.inria.fr/hal-01645009

[8] M. ZHANG, F. DAI, F. MALLET. *Periodic scheduling for MARTE/CCSL: Theory and practice*, in "Science of Computer Programming", September 2017 [*DOI :* 10.1016/J.SCICO.2017.08.015], https://hal.inria.fr/hal-01670450

International Conferences with Proceedings

[9] G. LIBONI, J. DEANTONI, A. PORTALURI, D. QUAGLIA, R. DE SIMONE. *Beyond Time-Triggered Co-simulation of Cyber-Physical Systems for Performance and Accuracy Improvements*, in "10th Workshop on Rapid Simulation and Performance Evaluation: Methods and Tools", Manchester, United Kingdom, January 2018, https://hal.inria.fr/hal-01675396

[10] J.-V. MILLO, E. KOFMAN, J. DEANTONI, F. MALLET, A. OUESLATI, R. DE SIMONE. *Explicit Control of Dataflow Graphs with MARTE/CCSL*, in "MODELSWARD 2017 - 5th International Conference on Model-Driven Engineering and Software Development, MODELSWARD 2017", Porto, Portugal, Scitepress, February 2017, pp. 542-549 [*DOI :* 10.5220/0006269505420549], https://hal.inria.fr/hal-01644294

[11] H. ZHAO, L. APVRILLE, F. MALLET. *Multi-View Design for Cyber-Physical Systems*, in "PhD Symposium at 13th International Conference on ICT in Education, Research, and Industrial Applications", Kiev, Ukraine, May 2017, pp. 22-28, https://hal.inria.fr/hal-01669918

Scientific Books (or Scientific Book chapters)

[12] F. MALLET, E. VILLAR, F. HERRERA. *MARTE for CPS and CPSoS: Present and Future, Methodology and Tools*, in "Cyber-Physical System Design from an Architecture Analysis Viewpoint", J.-P. TALPIN (editor), Springer, May 2017, pp. 81-108 [*DOI :* 10.1007/978-981-10-4436-6_4], https://hal.inria.fr/hal-01671190

Books or Proceedings Editing

[13] F. MALLET, Z. GRYGORIY (editors). *PhD Symposium at 13th International Conference on ICT in Education, Research, and Industrial Applications*, May 2017, https://hal.inria.fr/hal-01669920

[14] F. MALLET, M. ZHANG, E. MADELAINE (editors). *Eleventh International Symposium on Theoretical Aspects of Software Engineering*, IEEE, September 2017, https://hal.inria.fr/hal-01670407