# UCN@Sophia Ph.D. Proposal: Multi-Level Design for Cyber Physical Systems

Frédéric Mallet, Ludovic Apvrille
Frederic.Mallet@unice.fr
ludovic.apvrille@telecom-paristech.fr

September 9, 2015

## About our proposal

- **Financing request**: We ask for **only one year and a half of financing (1/2 Ph.D**)
- The other part of the Ph.D. financing comes from the PIAVE LEOC project Clarity that started in September 2014 (`http://www.clarity-se.org/`)
- Scientific axis: "Calcul distribué et ubiquitaire", i.e., "Inventer de nouveaux modèles, méthodes et techniques pour la création d'applications distribuées fiables et efficaces."
- Thesis directors and co-director: Frédéric Mallet (Université Nice Sophia Antipolis) and Ludovic Apvrille (LTCI)
- The Ph.D. student will be localized at INRIA, AOSTE team.

## Context and problematic

The advent of 5G networks will certainly foster the deployment of Internet of Things and smart objects. Among them, complex sensors, actuators and their software/hardware support will form networks of Cyber-Physical Systems (CPS). CPS are highly complex systems made of heterogeneous subsystems that combine both discrete and continuous aspects. They may also be safety-critical and widely distributed [8]. Also, their design commonly address a wide variety of domain (*e.g.*, discrete control, physics modeling, sensor networking, security) and usually there is not a single central model but rather a collection of models, possibly in different languages adapted to the domain of the model. The different languages used in each domain are heterogeneous both in terms of their syntax and their behavioral semantics. However, the models developed with these different languages must be coordinated to understand the system behavior [4], so as to better design them. By "better", we mean safer, more secure, and more efficient.

There is a large diversity of tools and frameworks, supporting individual languages, to work in each individual domain. This coordination usually relies on two different kinds of relations, one (vertical) of functional refinement, and another one (horizontal) of interaction between the different models. Engineering models like UML, or its extensions to system modeling SysML and to real time embedded modeling MARTE, can be seen as de-facto standards for the early development stages. However they poorly address the coordination problem, because of two reasons:

1. **Refinement**. The gap between UML/SysML and well-established lower level model implementations (*e.g.* Scade models) is tremendous [6] due to a huge difference between these two abstraction levels and a lack of precise semantics of UML/SysML models.

2. **Interaction**. The semantic gap between the different domain involved in the development of CPS cannot be clearly specified in the same formalism, thus making it it is difficult to understand the impacts of the interactions between the different parts/domains of the systems (*e.g.*, how much the addition of an encryption algorithm impacts the timing behavior of the system). This is mainly due to both a lack of a native notion of viewpoint (as defined in the ISO standard 42010) and to a lack of a clear behavioral semantics for the different involved languages.

The Clarity project promotes the use of a system engineering language (named Capella[1]) to syntactically deal with the coordination between different languages in the two directions previously identified (*i.e.*, refinement and interaction). The language supports the notion of viewpoints, in which a language used for a specific viewpoint can be tailored to a specific domain (DSL). In this context, making explicit the behavioral semantics of such languages is a first (but insufficient) step toward understanding their coordination [5, 14].

## Contribution and expected outcomes

The thesis will study how to tackle and unify the need for vertical and horizontal coordination in the design of CPS. This framework should make comprehensive:

1. The semantic relations that exist between models at different stages of the development process, and in particular, between a system-level functional model and its concrete implementation in another language

2. The semantic relation that exists between different views of the system (*e.g.*, between the real time behavior, the privacy requirements and the energy consumption)

Also, these semantic relationships should be amenable to automatic reasoning (*i.e.*, simulation, analysis, cost propagation). **The expected output is the definition of new models, along with an adequate modeling framework and analysis tools for the design of smart objects with physical components (CPS)**, that can assist designers in the diversity of views and domains that are required, with a strong emphasis on the consistency between these views.

To reach the proposed objective, we expect to define a link between the different models (*i.e*, views) at the same and at different refinement levels, both ways. More precisely, at a given specification level, we intend to define an explicit way to abstract, formally, the functional and non-functional

[1] `https://www.polarsys.org/capella/`

properties of both the models and their interactions. We want to use this abstraction as a way to check the correct interaction between models from different domains but also to check the correct refinement of models along the development process. We want to leverage analysis/verification results on individual models to feed and refine their specification at a upper level or their interaction with other models. This will result into a possibly iterative process between the different models, either at different abstraction levels or from different domains, with a successive enrichment of both the properties of the component and of their interactions.

The co-modeling environment we intend to settle shall help to combine as much as possible the existing formalisms and tools used by the different stakeholders. In addition to the syntactic capabilities provided by system engineering environment like Capella, the proposed co-modeling environment must handle behavioral properties of the different heterogeneous models. Adding a management of the behavioral properties from different models opens the road to many expected benefits among which:

1. The possibility to automate/assist the generation of a correct by construction master algorithm for co-simulation (for instance by relying on existing interaction standards like the Functional Mockup Interface [9]).

2. The possibility to automate/assist the generation of observers or test cases to verify that the models satisfies the properties of a more abstract specification.

3. The possibility to automate/assist the generation of observers or test cases to verify that the models correctly implement the interactions specified between models from different domains.

4. While the verification and certification process is well handled for the design of single components, both the integration and the system level design of heterogeneous systems is left with almost no formal verification support. A clear specification of the coordination between the heterogeneous models of the systems is a required step toward the certification of a system development process.

Note that the behavioral properties provided by the models of the co-modeling environment can come from different sources ranging from traditional requirements, formal requirements, tests or from results of functional (*e.g.*,model-checking), or extra-functional (*e.g*,performance or safety) analysis. The main goal of the co-modeling environment is to specify, in a unified framework how these properties can be used to ensure the correctness of vertical and horizontal heterogeneous coordination.

Last, the candidate solutions at both levels should consider engineering aspects (which models are more likely to be extended and enriched, which models are more likely to be integrated into an industrial-size framework/toolkit) and theoretical aspects by reusing theoretical results of existing verification solutions, and use them jointly with existing or emerging engineering solutions.

## Supervision

Due to its link to system engineering, this subject lies at the border of different domains. This is challenging since it requires to communicate frequently with actors from different domains to understand 1) how the coordination between these domains can be specified and 2) how their coordination impacts the heterogeneous models. This is a reason for a co-direction between the AOSTE and the LTCI/LabSoC teams.

AOSTE and LTCI/LabSoC main interest lies in Model Driven Engineering languages, methodologies and tools. However, they have complementary knowledge from different domains. The AOSTE team is a join team between the I3S laboratory and INRIA. They have been involved in definition of the MARTE profile [10], in two projects on multi-view modeling of energy aware system on chips [13, 12], in one project for heterogeneous modeling of software [11] and of course in the Clarity project the subject relates to.

The LTCI/LabSoC team has been involved in the definition of several UML-based profiles, including the UML profile for security [3] [1], and profiles related to the design space exploration of complex embedded systems and Systems-on-Chip [7]. For the latter domain, the LabSoC is currently particularly involved in the definition of model-based engineering frameworks for the design of smart objects, taking into account more particularly the reconfiguration, security and communication waveforms of such objects. The TTool [2] toolkit is developed by the LabSoC in order to support the above-mentioned profiles.

# References

[1] SysML-Sec. `http://sysml-sec.telecom-paristech.fr/`.

[2] TTool. `http://ttool.telecom-paristech.fr/`.

[3] L. Apvrille and Y. Roudier. Sysml-sec: A sysml environment for the design and development of secure embedded systems. In *APCOSEC 2013*, Yokohama, Japan, September 2013.

[4] B. Combemale, J. Deantoni, B. Baudry, R.B. France, J.-M. Jezequel, and J. Gray. Globalizing modeling languages. *Computer*, 47(6):68–71, June 2014.

[5] Benoit Combemale, Julien Deantoni, Matias Vara Larsen, Frédéric Mallet, Olivier Barais, Benoit Baudry, and Robert France. Reifying Concurrency for Executable Metamodeling. In Martin Erwig, Richard F. Paige, and Eric Van Wyk, editors, *SLE - 6th International Conference on Software Language Engineering*, volume 8225 of *Lecture Notes in Computer Science*, pages 365–384, Indianapolis, IN, États-Unis, 2013. Springer. CNRS PICS Project MBSAR (http://gemoc.org/mbsar).

[6] M. Di Natale, F. Chirico, A. Sindico, and A. Sangiovanni-Vincentelli. An MDA Approach for the Generation of Communication Adapters Integrating SW and FW Components from Simulink. In *Model-Driven Engineering Languages and Systems (MODELS)*, pages 353–369, 2014.

[7] Andrea Enrici, Ludovic Apvrille, and Renaud Pacalet. A UML Model-Driven Approach to Efficiently Allocate Complex Communication Schemes. In *17th International Conference on Model Driven Engineering Languages and Systems (MODELS)*, pages 370–385. ACM/IEEE, 2014.

[8] E.A. Lee. Cyber physical systems: Design challenges. In *Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on*, pages 363–369, May 2008.

[9] MODELISAR consortium and Modelica Association Project "FMI". `https://svn.modelica.org/fmi/branches/public/specifications/v2.0/FMI_for_ModelExchange_and_CoSimulation_v2.0.pdf`.

[10] OMG. UML profile for MARTE. *Object Management Group*, v1.1, October 2010.

[11] the GEMOC INS project members. Gemoc. `http://gemoc.org/ins`. ANR-12-INSE-0011).

[12] the HeLP INS project members. Help: High level models for low power systems. `http://www-verimag.imag.fr/PROJECTS/SYNCHRONE/HELP/`. ANR-12-INSE-0011).

[13] the HOPE INS project members. Hope: Hierarchically organized power/energy management. `http://anr-hope.unice.fr/`. ANR-12-INSE-0003).

[14] Matias Ezequiel Vara Larsen, Julien Deantoni, Benoit Combemale, and Frédéric Mallet. A Behavioral Coordination Operator Language (BCOoL). In *ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems (Models)*, September 2015.