# Post-doctoral position at IRIT/LAAS-CNRS, Toulouse, France

**Title:**
Formal specification and verification of reconfigurable distributed communicating and mobile cooperative systems.

**Context:**
This study is conducted in the framework of the ROSACE project ("RObots et Systèmes Autoadaptatifs Communicants Embarqués" / "Robots and Embedded Self-adaptive Communicating Systems") funded by the French Network for Advanced Research dedicated to Science and Technology for Aerospace Systems. The project is jointly conducted by IRIT, LAAS and ONERA. The project focuses on a multi-robots platform composed of uninhabited aerial/ground vehicles. This platform will be provided and maintained by LAAS-CNRS and ONERA as an experimental system that will be used to implement, illustrate and validate the outputs of the project.
**Subject:**

**Description of ROSACE/theme1 :**

An obstacle to a wider deployment of robotic platforms is the lack of confidence in their dependability. On one hand, such systems are made of smart components whose self-adaptive behaviours may be hardly predictable, even in nominal conditions. On the other hand, when they operate in an autonomous context, they shall rely on highly dependability skills in order to escape from most hazardous situations without human help.
A way to overcome these difficulties is first to identify accurately the role played by smart components in the system architecture. Then, according to the criticalities of these roles, one shall verify progressively the components more or less thoroughly. Thus one research activity of the project will aim at studying how rigorously can be assessed robotic platforms.
Such platforms shall usually meet same requirements than traditional embedded systems i.e. they shall provide the expected services, within a bounded response time, while preserving a reasonable level of risk. Each class of requirements entails specific analyses. The project proposes to start from up to date researches for each class and extend techniques only if necessary to deal with self adaptation. Moreover, to master the complexity, the assessment is usually organized in progressive steps. First steps deal with understanding the system mission and the performance requested. From the assessment perspective, this step is the starting point that justifies all the initial requirements. Then a system technical specification is defined. It proposes preliminary system architecture and it allocates roles to system components. From the assessment perspective, it shall be compliant with all the needs identified previously. At this level, a special attention shall be paid to the properties highly dependant from the system structure like the dependability, communication or cooperation capacities. Next step tackles the detailed specification and development of the main components. At this level difficulties are related to the identification and proof of the boundaries of the self adaptive components. These boundaries will result from the component role but also from implementation constraints. Finally last steps are dedicated to the validation of the integration of the components inside the platform. The challenge is here to identify the minimal amount of complementary checks.

Thus, this activity will deliver a roadmap that will identify some perimeters of use of robotics platforms and that will recommend for each perimeter a set of relevant assessment methods and tools.

**Description of the work :**

We consider the context of mobile entities cooperating in the context of a critical operation for crisis management. In such a context, we have to deal with heterogeneous and varying communications resources. Adapting the communication acts on the different communication layers (transport and middleware). It deals with the priorities of actors (possibly identified by their roles) and the

priorities of the exchanged data. Adaptation aims to handle changes in constraints at the level of communication and processing resources

The targeted QoS properties to be guaranteed or preserved include:
- The availability of communication resources for a permanent logical connectivity.

In this case, we have to prove that if the physical disconnection does not last more than a given time duration then the buffering capacity is sufficient to make the disconnection transparent to the supported activities and associated applications.

- Preserving the quality of communications (performance and consistency with activity requirements).

In nominal communication phases, we have to prove that the role repartition is consistent wrt attributed communication priorities: for example we have to guarantee that a given critical role (e.g. the activity coordinator or supervisor has the lead over the available resources)

Possible tasks for the post-doc candidate are:

1. to start with a case-study already investigated with graphs to see which problems one can solve by making the transformation from Ontology to formal language for the proof of properties,
2. to study the use of Bi-graphs for the formalization
3. to formalize consistency properties :
    - of system structure: to ensure that a given property is always satisfied by the current configuration: e.g. propagation of information, respect of the priorities of communication
    - of reconfiguration rules: we prove that they preserve the generic properties of interest.
4. Formalization within a logical framework either functional (Isabelle, Coq) or set theory- based (B, Z, TLA) and, if necessary, to consider real-time aspects through model-checking (FIACRE, UPPAAL, TINA)

**Requirements:** PhD in a related field among the following:
- Communicating system architecture (middleware and network)
- Reconfiguration models and techniques
- Formal methods

**Starting date**: September 2010
**Duration**: 1 year
**Applicants should send**:
- a resume/bio
- pointers to their most important publications and/or their PhD (only French or English documents)
- recommendation letter(s)

**Contact people**:
Khalil DRIRA (khalil.drira@laas.fr) Phone: +33 5 61 33 63 22
Mamoun FILALI (filali@irit.fr) Phone: +33 5 61 55 69 26
**Laboratories**
LAAS-CNRS,
7 avenue du Colonel Roche - 31077 Toulouse Cedex 04, France
IRIT, UPS
118, route de Narbonne 31062 Toulouse Cedex 09, France