Thesis subject: Safety-Bag and safety rules for Systems of Systems

PhD Advisors:

- Schön Walter, Professeur
  Heudiasyc laboratory, UMR CNRS-UTC 7253
  +33 (0)3 44 23 44 83, walter.schon@.utc.fr

- Lussier Benjamin, Enseignant-chercheur contractuel
  Heudiasyc laboratory, UMR CNRS-UTC 7253
  +33 (0)3 44 23 79 82, benjamin.lussier@.utc.fr

Context of the thesis:

The thesis is part of the project activities of the Laboratory of Excellence (LABEX) at the Université de Technologie de Compiègne (UTC) in France on the Control of Technological Systems of Systems (MS2T) (www.utc.fr/labexms2t).

PhD thesis description:

A System of Systems (SoS) is a highly organized meta-system composed of smaller independent systems that cooperate to achieve functions impossible for one of these smaller systems alone. But out of the multiplicity of relatively simple actions of the systems, emergent properties arise in the SOS. These emergent properties can be detrimental to the SoS functions, and even threaten its safety. For example, an heterogeneous geographical repartition of automated transport systems in a multi-modal transport systems can make the SoS more prone to collision between systems. As they only appear during the SoS operations, emergent properties are very hard to predict and thus to address through fault elimination methods during the SoS development. We propose alternatively in this thesis a technique based on fault tolerance to guarantee that no emergent properties will threaten a set of specified safety rules. This technique is based on safety-bags.

A safety-bag is an independent safety component that continuously controls that the system's actions will not threaten its safety rules. This technique has been introduced in the interlocking system ELEKTRA for an automated railway [Klein 1991] and has since been used in other critical applications such as satellites, medical systems or nuclear power plants [Guiochet et al 2008]. The safety-bag seems particularly adapted to SoS and emergent properties, as it supervises the system as a whole, allowing it to determine if the smaller systems actions will threaten the SoS safety on a global state that would be impossible for the smaller systems to perceive.

This thesis proposes to study and develop safety-bags adapted to SoS. Three major aspects need to be addressed:

- How the safety-bag will monitor the state of the SoS? Indeed, the safety-bag needs information on the smaller systems and the SoS environment to assess threats to its safety rules. The safety-bag will use communications and information sent by the smaller systems, but may also need other independent sources.
- What are the safety rules to guarantee? Domain specific safety rules need to be defined and ensured.

- How to react to a threat on a safety rule? Typically, safety bags can either forbid the action that threatens the safety rule, or enforce another action in compensation. For example, if an autonomous system threatens to cross the safety distance with another autonomous system, the safety-bag may either stop the first system, or order the second to move further away, depending of the SoS state.

In all these three points, communication latencies pose a serious problem for the safety-bag.

This thesis subject enters in the Labex scientific field Optimized design of technological SoS, particularly in the third aspect Operational safety of technological SoS. It could be applied to all of the Labex applications, particularly to the multi-modal transport systems and UAV Fleets. Indeed, the targeted applications for validation of this thesis are a fleet of automated vehicles or UAV, and a railway transport system platform.

Requested means:

To support the thesis we request means for three different aspects:

- A master's or engineering degree internship to support the development effort (1600€ to 2400€)
- Participation for one international congress per year (about 4000€ per year totaling to 12000€)
- Miscellaneous expenses: small equipment, summer school, etc. (about 5000€ per year totaling to 15000€).

Connection to other projects (already submitted or financed):

The validation of the thesis work will be connected to other projects depending on the application domain:

- the Robotex equipment project, if the application focuses on a fleet of UAV, autonomous cars or rovers,
- the Perfect and Vegas ANR projects if the application focuses on an automated railway control system.

Candidate's profile:

Master's degree in computer science. Knowledge in dependability and fault tolerance appreciated.

References:

[Klein 1991] P. Klein, *The Safety Bag Expert System in the Electronic Railway Interlocking System ELEKTRA*, Expert Systems with Applications, 3(4), 1991.

[Guiochet et al 2008] J. Guiochet, D. Powell, E. Baudin, J.P. Blanquart, *Online Safety Monitoring Using Safety Modes*, Workshop on Technical Challenges for Dependable Robots in Human Environments, PASADENA, 2008.