

# On-line Verification of Safety Properties in Critical Systems

J. Guiochet                      M. Roy

December 9, 2011

**Keywords:** Safety, Graph Analysis, Runtime Verification, Timed Systems.

Real-time systems for critical industrial systems (e.g., robots in interaction with humans, avionics or automotive systems) require a high level of dependability, while these systems are continuously threatened with many risks coming from the environment, or from internal faults.

A possible way to reduce threats is to equip a system with a monitoring mechanism that supervises the system and checks that safety constraints are always guaranteed. As an example, enforcing timing constraints, or deadlines, must be satisfied even in the presence of failures, possibly inducing a reduction of service.

Preliminary results have been obtained in LAAS-CNRS on this topic. Based on a partial description of the system using so-called “safety modes”, we have developed an algorithm that computes graph that describes, in the case of a violation of any safety mode, a set of possible paths to drive the system back to a predefined safety state. For now, this graph is based on simple heuristics that may be too restrictive.

The objective of this post-doctoral study is to work on the use case of a walking assistance robot to identify interesting safety related graphs and study their characteristics, in order to deduce better heuristics to integrate in the recovery graph computation algorithm. The properties expressed in this graph should include timing constraints. A second task will be to link such graphs with classical timed formalisms such as temporal logics, or timed automata. A third task will be devoted to the implementation issues of such a runtime monitoring system.

The whole study will contribute to a complete methodology for the development of *safety monitors*, from the specification to a realization on a prototype of the laboratory.