Title: Modeling and Checking Real-Time System Designs.

Author: Víctor Adrián Braberman.

Director: Ph.D. Miguel Felder.

Institution: Departamento de Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina.

Dissertation date: 11th September 2000.

Abstract: Real-time systems are found in an increasing variety of application fields. Usually, they are embedded systems controlling devices that may risk lives or damage properties: they are safety critical systems. Hard Real-Time requirements (late means wrong) make the development of such kind of systems a formidable and daunting task. The need to predict temporal behavior of critical real-time systems has encouraged the development of an useful collection of models, results and tools for analyzing schedulability of applications. However, there is no general analytical support for verifying other kind of high level timing requirements on complex software architectures. On the other hand, the verification of specifications and designs of real-time systems has been considered an interesting application field for automatic analysis techniques such as model-checking. Unfortunately, there is a natural trade-off between sophistication of supported features and the practicality of formal analysis.

To cope with the challenges of formal analysis real-time system designs we focus on three aspects that, we believe, are fundamental to get practical tools: model-generation, model-reduction and model-checking. Then, firstly, we develop an automatic approach to model and verify designs of real-time systems for complex timing requirements based on scheduling theory and timed automata theory (a well-known and studied formalism to model and verify timed systems). That is, to enhance practicality of formal analysis, we focus our analysis on designs adhering to Fixed-Priority scheduling. In essence, we exploit known scheduling theory to automatically derive simple and compositional formal models. To the best of our knowledge, this is the first proposal to integrate scheduling theory into the framework of automatic formal verification. To model such systems, we present I/O Timed Components, a notion and discipline to build non-blocking live timed systems. I/O Timed Components, which are build on top of Timed Automata, provide other important methodological advantages like influence detection or compositional reasoning.

Secondly, we provide a battery of automatic and rather generic abstraction techniques that, given a requirement to be analyzed, reduces the model while preserving the relevant behaviors to check it. Thus, we do not feed the verification tools with the whole model as

previous formal approaches. To provide arguments about the correctness of those abstractions, we present a notion of Continuous Observational Bismulation that is weaker than strong timed bisimulation yet preserving many well-known logics for timed systems like TCTL.

Finally, since we choose timed automata as formal kernel, we adapt and apply their deeply studied and developed analysis theory, as well as their practical tools. Moreover, we also describe from scratch an algorithm to model-check duration properties, a feature that is not addressed by available tools.