Exploitation of Non-intrusive Monitoring in Real-Time Embedded System Systems*

Ricardo C. Pinto and José Rufino

LaSIGE - Faculty of Sciences - University of Lisboa
ricardo.pinto@ciencias.ulisboa.pt, ruf@di.fc.ul.pt

Abstract. Software execution monitoring in embedded systems can be performed with different purposes, ranging from system characterization to run-time verification (RV). Traditional RV techniques require the intrumentation of the code for monitoring, which brings an overhead to the execution of the system - both in performance and timeliness. In real-time systems this overhead is exarcebated by the need of new worst-case execution time estimation and schedulability analysis.
In this paper we show how non-intrusive monitoring mechanisms can be exploited to support Run-time Verification (RV) in real-time embedded systems, thus allowing run-time verification without the need for code instrumentation and therefore negating the penalties incurred by instrumentation.

Keywords: Run-time Verification; Real-time Embedded Systems; Non-intrusive Monitoring

1 Introduction

Ever increasing deployments of applications based on cyber-physical systems have pushed the topic of system monitoring and Run-time Verification (RV) for embedded systems into the agendas of both academia and industry. Such systems have a strong (feedback) connection to their surroundings - e.g. autonomous vehicles - and failure of such a system may translate into catastrophic consequences. Therefore, guaranteeing correctness of the behaviour at all times is essential.

The basis of RV consists in monitoring the state of a system. Such state can be described through: values of variables; execution of functions and procedures; input/output activities, materialized by the reading/writing of specific memory addresses, or ports. The result of the monitoring activities is then verified against a specification, in order to assess the adherence of the system's behaviour to the specification - in short, system correctness.

* This work was partially supported by the EC, through project IST-FP7-STREP-288195 (KARYON) and by FCT, through project PTDC/EEI-SCR/3200/2012 (READAPT), through LaSIGE Strategic Project PEst-OE/EEI/UI0408/2014, and Individual Doctoral Grant SFRH/BD/72005/2010.