Effects of Arbitrary Hardware Faults on Multicore Scheduling in Safety-critical Applications

Evaluation by enhanced Markov models and discrete event simulation

Stefan Krämer

University of West Bohemia, Faculty of Applied Sciences
Univerzitní 8, 306 14 Plzen, Czech Republic
OTH Regensburg, Faculty of Electronics and Information Technology
Seybothstr. 2, D-93053 Regensburg, Germany
stefan.kraemer@hs-regensburg.de

Abstract

We present a discrete event simulation-based approach for reliability analysis in combination with schedulability analysis of safety-critical multicore real-time embedded systems. In such a safety-critical system the software execution does not only have to be hardened against sporadic hardware faults, e.g., by means of coded processing or symmetric redundancy, but also the real-time requirements still have to be met in the presence of such faults to guarantee a safe operation of the system. To verify the simulation environment, basic task sets that already include these safety mechanisms are evaluated by an enhanced Markov model. This Markov model is enriched by determination of timing characteristics, such as deadlines. It is shown that the behavior – regarding real-time and safety metrics – of this theoretical model can be transferred into an abstract system timing model which then can be analyzed by a discrete event simulation approach. Therefore it is possible to evaluate the influence regarding the real-time characteristics of a given sporadic fault with a certain fault rate by means of a discrete event simulation. By discrete event simulation the scope of analyzing a system can be extended compared to the Markov model. Now it is possible not only to evaluate single safety and timing metrics for a simplified functionality of the system, but also to evaluate the whole system. Currently there is no analytical approach available to proof the feasibility of global dynamic scheduling on a multicore system. The complete system model – including the mention safety mechanism and their impact on the scheduling itself – should be described. This model also includes the hardware faults that affect the system and is realized by simulated fault injection. In this work we present an approach to evaluate reliability metrics, real-time behavior and schedulability of multicores applications in a holistic

view. Furthermore it is shown that the need arises to implement new safety-aware multicore scheduling algorithms.

Keywords: Markov model; Stochastic simulation; reliability analysis; real-time operating system; multicore scheduling; discrete event simulation; fault injection