Paper ID: 24254
student

SPACE SYSTEMS SYMPOSIUM (D1)
Poster Session (P)

Author: Mr. Jacopo Panerati
Ecole Polytechnique de Montreal, Canada, jacopo.panerati@polymtl.ca

Prof. Giovanni Beltrame
Ecole Polytechnique de Montreal, Canada, giovanni.beltrame@polymtl.ca

FAULT-TOLERANT SOFT REAL-TIME COMPUTING SYSTEMS BASED ON DYNAMIC BAYESIAN REASONING

Abstract

In space, there is no atmosphere to protect from ionizing or particle radiation. Without an atmosphere, and hence convection, efficient thermal management becomes a critical issue. In such conditions, current CMOS technology-based electronics are subject to transients faults, generalized performance reduction, accelerated wear, and, ultimately, unrecoverable system failure.

In computing systems for space applications, the traditional approaches adopted to guarantee reliability and extended lifetime are based on redundancy. Noteworthy examples are slack allocation, i.e. the allocation of excess resources, and triple-modular redundancy (TMR), i.e. the replication and majority aggregation of potentially faulty functionalities. However, these solutions are expensive in terms of resources and require a careful trade-off, because they increase complexity and area of the system, exposing it to a higher risk of overheating and radiation effects.

We propose a methodology that exploits a rigorous statistical framework to make the best use of the available resources by taking autonomous decisions in unforeseeable situations. Our methodology leverages dynamic Bayesian reasoning to cope with the uncertainty that might arise from different sources, such as, a defective implementation, noisy sensors, temperature spikes, and/or the unpredictability of fault manifestations. Using an array of sensors, we enable self-awareness in order to maximize the expected utility (i.e. a combination of lifetime, throughput, and deadlines met) achievable by the system.

Therefore, our methodology provides computing systems with the ability to detect and overcome faults, manage system temperature, and, at the same time, meet performance and real-time requirements. All of this is achieved with no additional area costs and minimal computational overhead. In our vision, this methodology allows for the creation of a new generation of computing systems able to autonomously perform their tasks for longer periods of time, fostering simpler and cheaper space exploration.

We tested the effectiveness of our approach in a multi-resource computing model, performing fault-injection through statistical processes with real-life parameters. In our preliminary results, we show that a probabilistic reasoning framework based on dynamic hidden Markov models (D-HMMs) always manages to find a better lifetime-availability balance than traditional static hidden Markov models (HMMs) and rule-based systems.