Reliability-Aware Embedded Systems Design Suite

Cristiana Bolchini, Antonio Miele
Dip. Elettronica e Informazione - Politecnico di Milano
P.zza L. da Vinci, 32 - 20133 Milano - Italy
{bolchini|miele}@elet.polimi.it

Nowadays, the necessity of ensuring system reliability has considerably increased with respect to the past due to the recent advances in the integrated circuit manufacturing process, because aggressive technological scaling, noise margin reduction, etc. are leading to the realization of devices with higher performance but higher susceptibility to faults, and specifically *soft errors*. This situation raises an important concern not only in the traditional application scenarios of mission- and safety-critical environments, where misbehaviors may be threatening for the people or the environment (e.g., automotive cruise control units or medical testing systems), but also in common application environments, due to pervasiveness of embedded systems in today's life (e.g., personal mobile devices, mobile phones or household appliances). As a consequence, dependability assumes today the role of a main driver in embedded system design, at the same level of classical parameters (e.g., performance and power).

Reliability-oriented techniques for digital systems have been thoroughly studied in the literature, offering a wide range of strategies devoted to introduce fault detection/tolerance/recovery properties. These strategies may be applied at different levels of abstraction and granularity; moreover, they introduce several overheads on the system implementation (area, performance). Furthermore, since modern system architectures are complex, composed by several heterogeneous components (such as microprocessors, reconfigurable modules, etc.), the straightforward application of a single, pre-defined hardening technique often does not produce an optimal solution. On the other hand, the large number of available techniques and the possibility to apply each technique at different levels of abstraction generate a huge space of alternative reliable implementations, characterized by different costs performance and reliability properties. As a consequence, there is a quest for new, flexible approaches able to exploit these degrees of freedom and providing the designer with the possibility to explore the design space composed by all the reliable implementations of the considered system, comparing the different solutions in terms of costs and benefits with respect to a set of metrics, including both classical and reliability-oriented ones.

In this demo we present a design suite that enhances the classical design flow for embedded systems by introducing reliability-awareness. The rationale of the proposed tools is to meet reliability requirements by applying reliability-oriented techniques while exploring different possible hardened system implementation characterized by a suitable trade-off between costs and benefits. As shown in Figure 1, besides the system specification, the target architecture and the design metrics, each tool requires also an additional set of inputs including the characterization of the system in terms of fault management requirements and the repository of the available hardening techniques. The methodological approach is based on the integration of the system hardening and reliable implementation tasks within the same design space exploration framework that selects the candidate hardening techniques satisfying the specified fault management requirements and optimizing the hardening process to minimize the overhead on the final system implementation. The proposed suite consists of design tools working at the system and device levels, as detailed below.

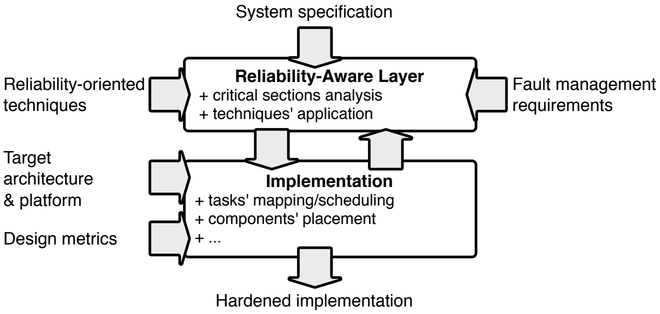
System specification
Reliability-Aware Layer
+ critical sections analysis
+ techniques' application
Reliability-oriented techniques
Fault management requirements
Target architecture & platform
Design metrics
Implementation
+ tasks' mapping/scheduling
+ components' placement
+ ...
Hardened implementation

Figure 1. Reliability-aware design framework.

Reliability-aware system-level synthesis. The standard system-level synthesis on heterogeneous multiprocessor systems is devoted to identification of a mapping and scheduling solution of the various tasks of an application on the architecture's processing units. The reliability-aware framework is intended as an extension of this flow to introduce a step devoted to the introduction of application-level and architecture level fault management mechanisms able to handle faults in the critical sections of the application. The objective function of the optimization process is the system performance.

Reliability-aware FPGA system design. A novel design step has been defined for hardening the hardware accelerators by exploiting hardening strategies based on classical fault detection/mitigation techniques and FPGA reconfiguration features for error recovery. This step has been integrated within the classical implementation flow for FPGA reconfigurable systems; in particular the floorplanning activity has been enhanced to deal with reliability-related issues. The objective functions of the optimization process are system area and recovery time.