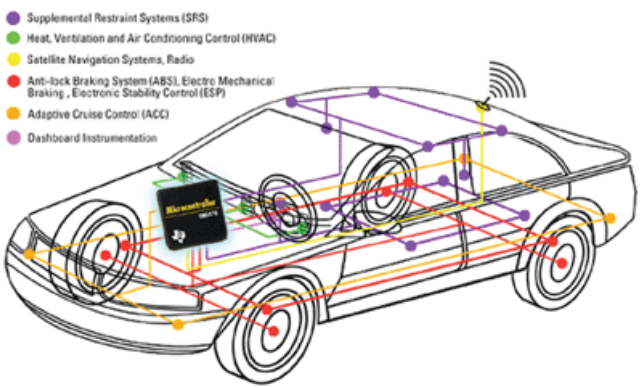
DEPENDABLE SYSTEMS: DESIGN METHODOLOGIES

HW/SW Co-Design of Reliable Embedded Systems

In the past, the capability of a system to cope with the occurrence of faults during its lifetime was deemed a requirement for only a limited number of complex systems, mainly devoted to space applications, or to other critical areas (e.g., nuclear plants). Today, the pervasiveness of embedded systems in our lives (from consumer electronics, to automotive, to domotics) poses an important issue on their dependability, not only to make sure that the product is able to perform its functionality also when fault occurs (or at least let the user know it) but also to grant that, in case of a failure, the system does not cause damages to people or the environment. As a result, design methodologies for the realization of embedded systems able to mitigate the effects of a failure play a fundamental role.



Dependability Analysis

Software-Implemented Hardware Fault Injection (SWIFI) strategies act on the specification of a component functionality to inject faults, and then monitor the effects it produces and how the system reacts in such anomalous situations.

We are currently building an environment to perform dependability analysis by means of :

- Fault Injection into systems implemented on FPGAs.
- SWIFI into SystemC models, simulated with the ReSP platform.

R4R Reconfiguration for Reliability

Using Field Programmable Gate Arrays (FPGAs)? RAM-based FPGAs are particularly sensible to Single Event Upsets faults (SEUs), which manifest themselves as a single (or multiple) bit flip in any one of the memory elements. In an FPGA a bit flip can corrupt a data value or modify the functionality of the device. Dynamic, partial reconfiguration can be exploited to mitigate the effects of these and other failures, to design systems able to self-heal and perform correctly.

We are building a framework for exploring the design space, exploiting reconfiguration coupled with classical and innovative techniques to achieve FPGA-based systems able to cope with failures.