Mixed-Criticality and Fault-Tolerance in Real-time Systems

Federico Reghenzani[1] and William Fornaciari[1]
Dipartimento di Elettronica, Informazione e Bioingegneria – Politecnico di Milano

Computer architectures evolved considerably in the last years, introducing several advanced features to overcome the single-core performance barrier. This incremental complexity makes their use in critical embedded systems difficult due to the strict design requirements. At the same time, these new architectures would make the consolidation of several applications in one single computing platform possible. Such applications may have different criticality requirements, creating in this way a so-called mixed-criticality system. This approach is very attractive for many domains, especially for aerospace, because the reduction of the on-board weight and development cost is a key goal to achieve.

Moving to more recent computing technologies and consolidating applications with different criticality on the same platform is, however, very challenging. In addition to hard real-time requirements, mission-/safety-critical systems must comply with failure requirements. However, hardware components are not only increasing in complexity, but also becoming smaller and smaller, thus increasing the fault probability, especially the occurrence of transient faults. On the other hand, the necessity to reduce the development and production costs, size, power, energy, and weight poses many challenges and pushes for software solutions that do not require hardware replication and permit the use of Commercial Off-The-Shelf building blocks even for critical applications.

Software fault-tolerant mechanisms are well-known and already available in scientific literature and industrial solutions. However, their effect on real-time scheduling has not been properly studied. The coexistence of different criticality applications makes not only the real-time scheduling challenging, but creates new unexplored research questions related to the fault-tolerance.

Recently, a research project has been approved for co-sponsorship by the European Space Agency, and it aims to: (1) identify the current limits and misconceptions on the implementation of mixed-critical approaches to real systems; (2) investigate the effect of fault-tolerant mechanisms when applied to real-time scheduling and develop new techniques for a joint failure-scheduling analysis; (3) stimulate the beginning of a standardization process that will allow the use of novel architectures and mixed-criticality approaches in the next generation of spacecraft computers.

[1] <name>.<surname>@polimi.it