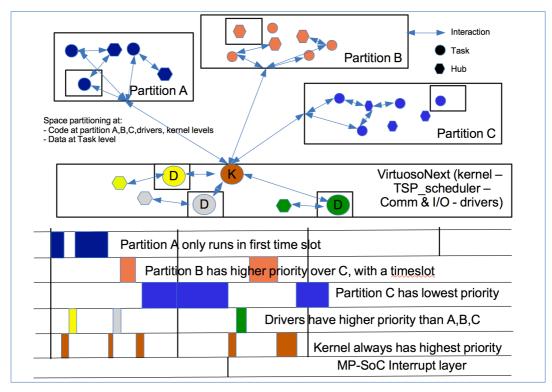# NoFist, Novel Fine Grain Space and Time partitioning for a Mixed Criticality Platform

The NoFist project aims at validating and refining a novel approach to Space and Time Partitioning that is specifically adapted to the needs of mixed criticality real-time embedded systems, in particular when executing on advanced and heterogeneous many/multi-core SoC target systems. Contrary to existing approaches, no dynamic code is used but a static memory image. No hypervisor layer and timeslicing is used but a formally developed and verified RTOS kernel (VirtuosoNext™) with a much smaller code size. Together with a driver layer, it isolates the application layer from hardware faults as a trusted layer. Tasks can be individually isolated or as an application group from each other by using the hardware support (MMU or MPU). The benefits of the approach are lower memory requirements and the capability to still meet hard real-time constraints as achievable with a non-partitioning RTOS.

VirtuosoNext comes with a visual modelling environment allowing programming a heterogeneous target system in a transparent way. Priorities are global, but time properties can be used as additional restrictions on the space partitioning support. VirtuosoNext also provides support for fault tolerance allowing to continue operation in the presence of faults, to recover or to gracefully restart. The transparent support for distributed and heterogeneous target systems, also facilitates implementing redundancy (e.g. TMR schemas) as well as diversity.

Schematic overview of VirtuosoNext managing 3 partitioned applications

The approach will be validated by implementing an adapted VirtuosoNext on the multi/manycore platform selected by Thales TRT for mixed criticality applications in the avionics domain. The requirements will be analysed, test suites developed, benchmarks developed and documented as a dependency tree project in GoedelWorks. The results will be disseminated in workshops and papers. The results are applicable across many other safety and security critical domains such as automotive, railway, medical and mission critical infrastructure systems.

Contact

Altreonic NV

Email: eric.verhulst@altreonic.com

Internet: http://www.altreonic.com/