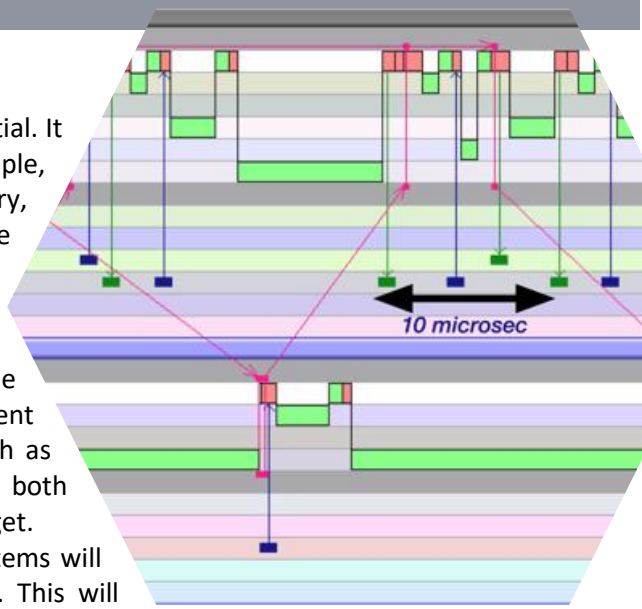
Partitioning space and time for safe and secure cyber physical systems

Challenge & Solutions



Ensuring public safety in the automotive and other critical domains is essential. It requires achieving perfect real-time performance. But that is far from simple, especially with the proliferation of cyber physical systems in machinery, equipment and other hardware. Current techniques involving space-and-time partitioning during the execution of system software are not well suited for embedded systems. Drawbacks include relatively high overhead in data memory and code, serious impacted hard real-time performance and partitions that can be relatively large. In that case, one error can bring the whole application down even if the error is recoverable. Developing an efficient time-partitioning solution for safe and secure cyber physical systems, such as embedded control equipment in transport systems, requires addressing both safety constraints and scheduling efficiency of processing on a multicore target.
In addition, the need to validate the "trustworthiness" of CPS and IoT systems will require more and more certification by neutral, independent authorities. This will require certifiable and rigorous engineering processes and the use of qualified tools and software. The NoFiST project (Novel Fine Grain Space and Time Partitioning for a Mixed Criticality Platform) validated and refined 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.

EuroCPS Support

Thales' multicore platform for mixed criticality applications was key to demonstrating this innovative approach for Altreonic's VirtuosoNext RTOS. In addition to providing the platform, Thales Research & Technology served as coaching partner, ensuring support on the platform, the requirements and the use case. This includes support on the configuration files used in the targeted critical domain. TRT also helped identify potential users of the VirtuosoNext technology.

Digital Skills

Altreonic: VirtuosoNext Designer, the industry's first fault-tolerant fine-grain space-and-time portioning real-time operating system (RTOS).

Thales Research & Technology: Target platform, a multicore processing machine, and the application examples and specific requirements to consider for safety-critical domains, including space-and-time partitioning.

Company

Altreonic is an innovative SME focusing on the embedded market with a unified methodology for developing trustworthy solutions. **VirtuosoNext** RTOS is one of its key products. (BE) www.altreonic.com

5 employees

Since 2008

Partners:
Thales - TRT

Impact / What's next

An initial partnership is underway between Altreonic and a provider of an industrial and certifiable Autopilot/Flight Control System. The company also is applying its solution internally to develop a lightweight electric vehicle with fault-tolerant architecture to support autonomous steer-by-computer driving. The company's business plan targets a market for autonomous shuttles for moving goods (logistics) and people. In both cases, the small code size and the capability to recover from runtime faults without rebooting provide a higher level of safety support without the cost of a complete hardware-redundant architecture.