POSIX 1003.1 Subset For FACE™ Safety Extended and Safety Base Profile Conformance

The Open Group Future Airborne Capability Environment (FACE) Consortium has developed a reference architecture and standard for real-time embedded avionics systems. The FACE™ Technical Standard defines required capabilities for real-time operating systems (RTOS), I/O services, transport services, and a shared data model to facilitate information exchange between portable components. RTOS requirements specified by the FACE Operating System Segment (OSS) are based on ARINC 653 and POSIX 1003.1b subset tailored to address the needs of avionics systems.

DDC-I's Deos was the first RTOS to receive the Conformance Certificate for the FACE Technical Standard, Edition 3.1. The certification covers the Safety Extended and Safety Base Profiles for the Operating System Segment (OSS).

To offer the POSIX interfaces for FACE Conformance, DDC-I para-virtualized RTEMS (an open source POSIX RTOS). RTEMS was originally released in 1990 as a deterministic real-time environment and is employed in military, space, and some industrial applications. The integrated platform combines the strengths and pedigree of both ARINC 653 and POSIX RTOSs, providing the industry standard interfaces and feature set required for conformance with the FACE Technical Standard Safety Extended/Safety Base and Security and Operating System Profiles, all in a time and space partitioned, hard-real-time, multicore execution model.

RTEMS on Deos delivers efficient execution within a Deos partition, which provides the required operating system services to RTEMS. This allows RTEMS to execute in user space with its normal critical sections, proper memory layout, and only interfaces with the Deos kernel for timing and I/O. POSIX applications on RTEMS therefore will be partitioned and will be provided the I/O services needed by the Deos kernel . This cooperative capability allows Deos to schedule ARINC-653 applications, POSIX applications in RTEMS partitions, and native Deos threads scheduled according to the rate monotonic algorithm (RMA) all on the same system. Figure 1 depicts this partitioning and the placement of the user-kernel boundary in the combined system.

Key Features Overview

- Support for ARM, PowerPC and x86 Processors
- Offers application portability from Linux and other POSIX-based operating systems
- FACE Conformance Delivers Maximum Application Portability
- Targets Safety Extended and Safety Base Profiles
- Contains Both POSIX 1003.1 & ARINC 653 API's
- POSIX API's Delivered by RTEMS Virtualized in a Deos Partition
  - RTEMS – Mature, Stable RTOS Supporting POSIX since 1990
  - Employed on numerous safety/mission critical military and space applications
  - Priority pre-emptive RTOS
- Development environment integrated seamlessly with Deos tool chain
  - Compiler/linker/debugger all provided and integrated with DDC-I Open Arbor Eclipse framework
  - Deos profiling tools exhibit POSIX application resource and timing usage

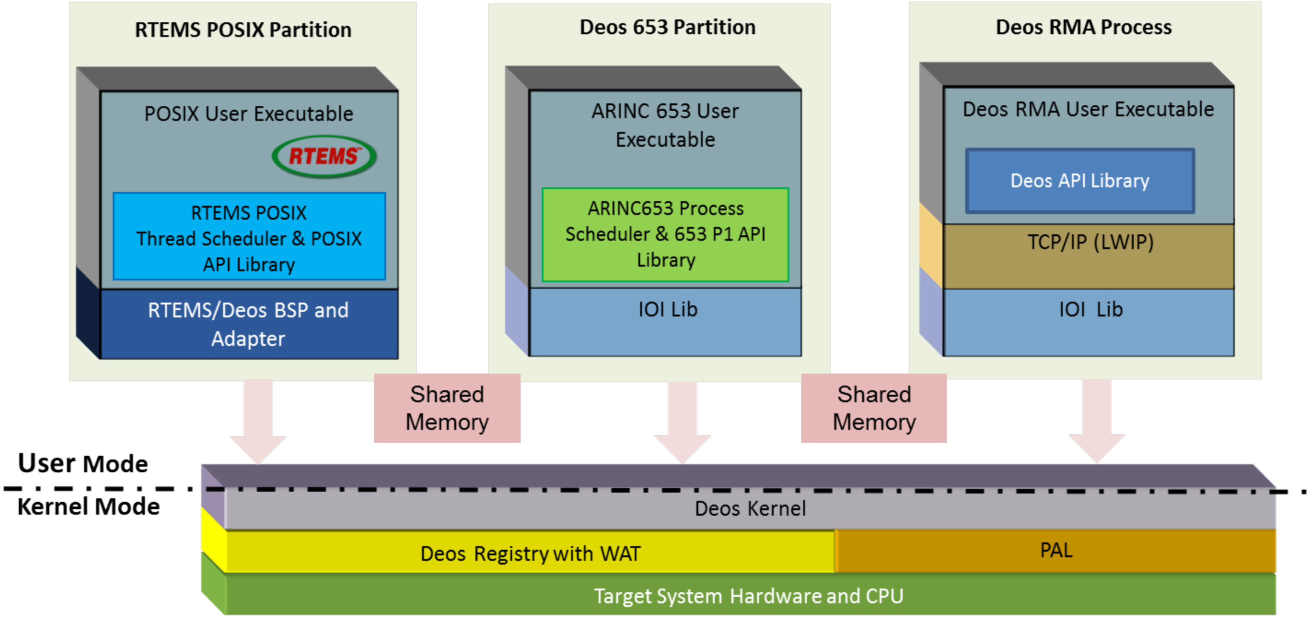

Figure 1: System Architecture across User-Kernel Modes

The Deos/RTEMS approach is applicable to single core and multicore environments. Figure 2 shows how DDC-I's SafeMC™ Technology for safety critical real-time on multicore processors may be configured to schedule ARINC 653 or POSIX applications on multiple cores. Deos allows the scheduling of POSIX tasks in the RTEMS partition concurrently with ARINC-653 processes in 653 partitions. The beauty of this design is that core attributes of both RTOSs are preserved. Deos is unmodified and retains its DO-178 DAL A certifiability. RTEMS remains a POSIX based RTOS with all of its capabilities intact – yet bounded in time and space partitions by Deos for safety critical needs. Additionally, legacy applications from each RTOS can be integrated together in this model, yet operate independently just as they can on separate systems. Extending the use case for this model even further, legacy applications written on bare metal RTEMS can, within limits, also run in a RTEMS partition. This integration allows new and existing applications to coexist within time windows executing RTEMS, ARINC 653 or Deos RMA processes and threads.

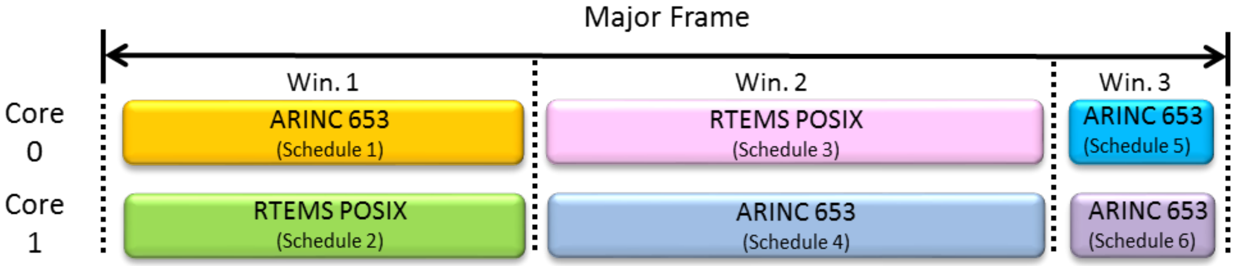

Figure 2: Multicore scheduling of ARINC 653 and POSIX Applications

Summary:

The heart of any safety critical avionics system is the operating system on which it is hosted. FACE Conformant operating systems for the safety & security profiles are expected to provide hard partitioning between software subsystems as well as ARINC 653 API's plus as a subset of POSIX APIs. These profiles, targeted at systems typically expected to undergo a safety certification, require a combination of the features historically found in certified ARINC 653 operating systems such as Deos, as well as the POSIX API's historically found in real-time operating systems like RTEMS. This integration available from DDC-I maximizes standards based applications software portability in a safety critical time and space partitioned hard real time environment.