SAFE**RTOS**®

The safety certified real time kernel for the SmartFusion family from Microsemi. Delivering superior performance and pre-certified dependability, whilst utilising minimal resources.

Functional Overview

The SAFE**RTOS** pre-emptive real time scheduler has the following characteristics:

- Any number of tasks can be created - system RAM constraints are the limiting factor.
- Each task is assigned a priority - any number of priorities can be used.
- Any number of tasks can share the same priority - allowing for maximum application design flexibility.
- The highest priority task that is able to execute (i.e. that is not blocked or suspended) will be the task selected by the scheduler to execute.
- Supports time sliced round robin scheduling for tasks of equal priority.
- Queues can be used to send data between tasks, and to send data between tasks and interrupt service routines.
- Binary semaphores and counting semaphores make use of the queue primitive – ensuring code size is kept to a minimum.
- Tasks can block for a fixed period.
- Tasks can block to wait for a specified time.
- Tasks can block with a specified timeout period to wait for events.
- FPU support.
- Definition and manipulation of MPU regions on a per task basis.
- Run time statistics.

Compact Footprint

Typical ROM Requirements	6-15K
Typical RAM Requirements	500 bytes
Typical Stack Requirements	400 bytes/task

Key Features

IEC 61508-3 SIL3 certified.

IEC 62304 Class C compliant.

Supports SmartFusion from Microsemi

Downloadable evaluation demos.

System Tasks

Including SAFE**RTOS** in your application allows the application to be structured as a set of autonomous tasks - the resultant system functionality being the sum of the functionality of the multiple tasks that make up the application.

Each task executes within its own context with no coincidental dependency on other tasks within the system or the scheduler itself.

Task States

Only one task can actually be executing at any one time. The scheduler is responsible for selecting the task to execute in accordance with each task's relative priority and state.

A task can exist in one of the states described by the Table 'Task States', with valid transitions between states depicted by the Figure 'Valid task state transitions'.

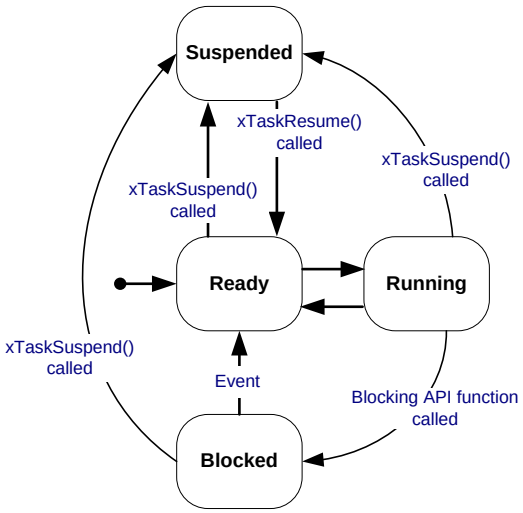

Figure *Valid task state transitions*

SAFE**RTOS** for Microsemi's SmartFusion

Table *Task States*

Task State	Description
Running	The task selected by the scheduler to execute and is currently utilising the processor.
Blocked	A task waiting for an event. It cannot continue until the event occurs. Tasks in the Blocked state always have a timeout period, after which the task will become unblocked.
Suspended	A task will enter the Suspended state when it is the subject of a call to the xTaskSuspend() API function, and remain in the Suspended state until unsuspended by a call to the xTaskResume() API function.
Ready	A task is in the Ready state if it is able to enter the Running state but is not currently the task that is selected to execute.

Scheduling Policy

The scheduler selects as the task to be in the Running state the highest priority task that would otherwise be in the Ready state. In other words, the task chosen to execute is the highest priority task that is able to execute. Tasks in the Blocked or Suspended state are not able to execute.

Different tasks can be assigned the same priority. When this is the case the tasks of equal priority are selected to enter the Running state in turn. Each task will execute for a maximum of one tick period before the scheduler selects another task of equal priority to enter the Running state.

While the scheduler will ensure that tasks of equal priority will be selected to enter the Running state in turn, it is not guaranteed that each such task will get an equal share of processing time.

Development Life Cycle

SAFE**RTOS** was built as a complimentary offering to FreeRTOS™, with common functionality but with a uniquely designed safety critical implementation.

The FreeRTOS functional model was subjected to a full HAZOP, all weakness within the functional model and API where identified and resolved. The resulting requirements set was put through a full IEC 61508 SIL 3 development life cycle, the highest possible for a software only component.

SAFE**RTOS** Configuration

SAFE**RTOS** is licensed as a SAFE**RTOS** variant, where a variant is defined according to the developer's choice of micro-processor and tool chain. A robust RTOS that inherently has less risk - the API and the core SAFE**RTOS** design and code is common between all SAFE**RTOS** variants; the remaining port layer is adapted to support the selected micro-processor. Each SAFE**RTOS** variant is subjected to the full IEC 61508 compliant development life cycle.

Certification

SAFE**RTOS** can be licensed as a pre-certified software component.

SAFE**RTOS** was initially certified by TÜV SÜD in 2007, resulting in the world's first ever pre-certified RTOS.

Design Assurance Pack

The DAP contains every design artefact produced during the full development life cycle, from development and safety life cycle plans, requirements specifications and design documents, to HAZOPS, the source code, all verification and validation documents and relating evidence. We also supply the full test harness, with user and safety manuals.

The SAFE**RTOS** safety manual clearly identifies each and every component included within the SAFE**RTOS** variant, and their relating checksums. The safety manual contains a concise list of instructions clearly identifying the installation and integration process engineers should follow when incorporating SAFE**RTOS** into a development environment.

Evaluation Packages

Full featured SAFE**RTOS** binary demos for Microsemi's range of SmartFusion devices are available for download from our website.

License Model

SAFE**RTOS** is royalty free, with flexible licensing models.

WITTENSTEIN High Integrity Systems
Worldwide Sales and Support
Phone: +44 1275 395 600
Email: Sales@HighIntegritySystems.com
Web: www.HighIntegritySystems.com