highintegritysystems

WITTENSTEIN

SAFE**RTOS**® with Enhanced Security Module (ESM)

The SAFE**RTOS**® Enhanced Security Module (ESM) is purpose-built to safeguard embedded applications by creating a robust, secure execution environment. The ESM creates a protective shield around each user-mode Task, isolating and containing threats before they can spread. If a Task is compromised, the ESM ensures the attack is contained, safeguarding the rest of the system.

Designed for automotive-grade security, the ESM is in accordance with ISO 21434, the global standard for road vehicle cybersecurity.

Benefits of the ESM

- Detect threats
- Confine threats
- Protect data

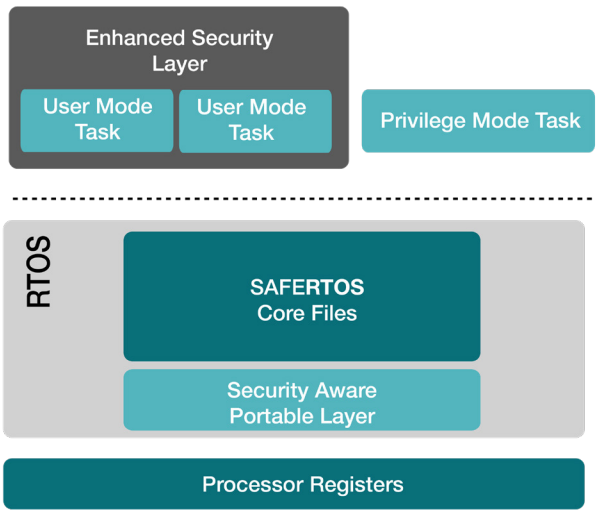

Figure 1 *The Enhanced Security Module,* SAFE**RTOS**® *and the Security Aware Portable Layer*

What sets the ESM apart is its effective containment strategy. Its primary objective is to prevent a compromised user mode Task from accessing information from other Tasks or gaining control of the system. The ESM achieves this by limiting the amount of access each user mode Task has with the rest of the system, using the features listed.

ESM Features

Access Control Policy: The ACP allows the developer to minimize the APIs each Task can access. This can be used to control which SAFE**RTOS**® functions a task can call.

Object Control Policy: The OCP allows the developer to minimize the SAFE**RTOS**® Data objects each Task can access (i.e. Timers, Queues, Mutexes, Semaphores, Event Groups, Event Polls and other Tasks). This prevents the Task from accessing data structures belonging to other Tasks.

Data Obfuscation: Key data structures are now accessed by indirect reference instead a pointer to a memory block. This hides data from a potential back actor.

Memory Isolation: The ESM builds on the SAFE**RTOS**® spatial separation mechanism that allows developers to define MPU/MMU memory regions for each Task. These memory regions limit the amount of memory access each Task has. If a Task accesses a memory region outside of its permitted range an exception is triggered.

Secure Portable layer: When using the ESM, it is necessary to have a security aware portable layer that enforces the kernel/user space partitioning more rigorously.

Task Context Data Isolation: When using the ESM, the actual Task context data is stored in the TCB (Task Control Block) rather than the Task stack. This protects the inactive Tasks from exploitation and data leakage due to access by a different Task.

Penetration detection monitor: When a Task accesses memory, APIs or data objects it does not have permission for an exception is triggered, warning the application that a attack may be underway.

Enhanced Security Module API Functions

The features provided by the ESM do not affect the existing SAFE**RTOS**® API, thereby permitting a simple upgrade path for customers wanting to add this module to an existing project. The ESM requires more attention to the location of statically defined objects and kernel hook functions (most of which should be located with KERNEL_DATA and KERNEL_FUNCTIONS respectively.

WITTENSTEIN high integrity systems
Americas: +1 408 625 4712
ROTW: +44 1275 395 600

email: sales@high**integrity**systems.com
web: www.high**integrity**systems.com

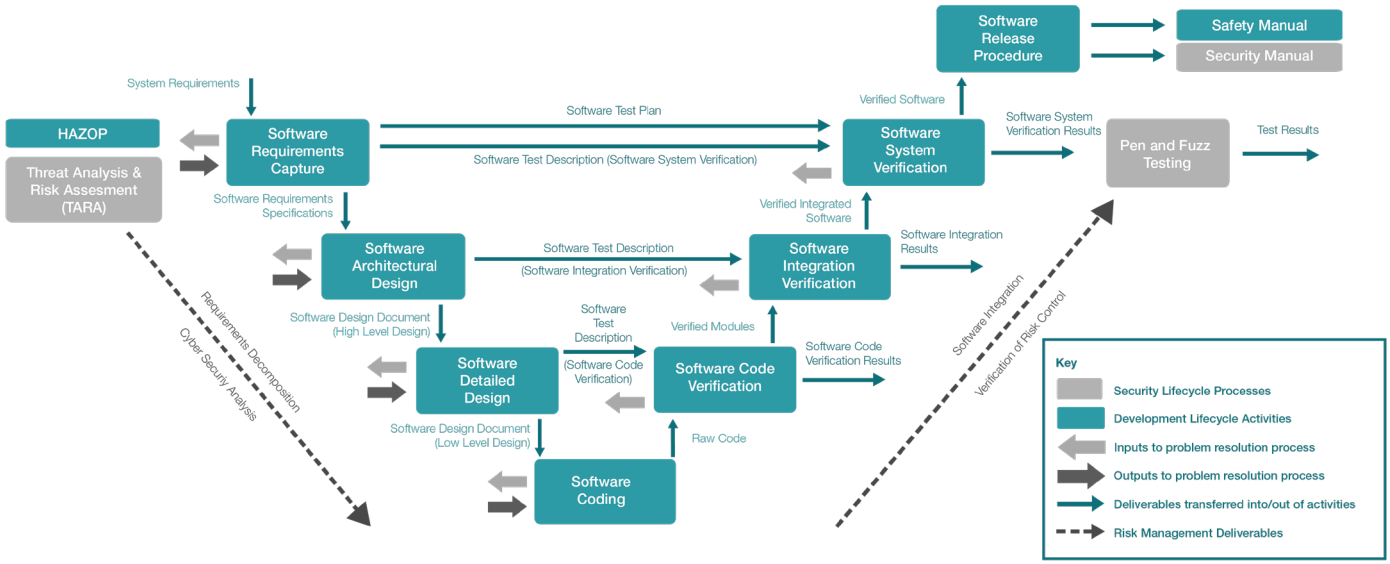

Figure 2 SAFE**RTOS**® *ESM Product Lifecycle*

In addition the following API functions have been added to support the configuration of Task access capabilities during scheduler initialisation.

```
xTaskConfigureACP()

portBaseType xTaskConfigureACP(
        portTaskHandleType xTaskToConfigure,
        portUInt32Type ulTaskPermissionsMask,
        portUInt32Type ulTimerPermissionsMask,
        portUInt32Type ulQueueMutexSemaphorePermissionsMask,
        portUInt32Type ulEventpollEventGroupPermissionsMask
);
```

Configures the security extensions' Access Control Policy (ACP) for the specified Task.

This will only succeed if called when the Scheduler is in the initialization state. On successful completion, the specified Task will only be able to call the API functions determined by the permissions masks: all other API functions will return an error.

```
xTaskConfigureOACP()

portBaseType xTaskConfigureOACP(
        portTaskHandleType xTaskToConfigure,
        void *pvObjectToAllow
);
```

Configures the security extensions' Object Access Control Policy (OACP) for the specified Task.

The OACP allows individual Tasks to be granted permissions to access particular RTOS Objects. This is achieved by calling xTaskConfigureOACP() prior to starting the Scheduler to associate Objects with Tasks. The Task specified by xTaskToConfigure will then be able to call API functions taking pvObjectToAllow as an Object Handle. Multiple calls to xTaskConfigureOACP() may be made with different objects passed in pvObjectToAllow to give the Task permissions to access multiple objects.

Development Process

The ESM uses the same development life cycle as SAFE**RTOS**® but with additional cybersecurity activities. Alongside the standard HAZOP, which is used to identify safety requirements, WHIS now implements a Threat Analysis and Risk Assessment (TARA) and a Cybersecurity Analysis Report (CAR) to identify security requirements.
The cybersecurity requirements are entered into the WHIS requirements management tool along with the existing SAFE**RTOS**® functional and safety requirements. All requirements, safety, functional and security are then developed to the highest possible Safety Integrity Level.
Additional Pen and Fuzz testing are added to the development life cycle along side the traditional functional and safety verification activities.

DAP

SAFE**RTOS**® ESM is supplied as full source code, along with the test harness and a demonstration application that provides examples of how to use the SAFE**RTOS**® API. The DAP contains all the design and verification artefacts generated during the development of SAFE**RTOS**® ESM for the specific processor/complier combination, along with Safety, Security and Users manuals.

Support & Maintenence

Continuous support and maintenance is available on an annual basis, providing access to incident reports and errata notices, product updates and patches.

Evaluations

Please contact our sales team to request source code evaluation packages for SAFE**RTOS**® ESM
Email: sales@highintegritysystems.com

WITTENSTEIN high integrity systems
Americas: +1 408 625 4712
ROTW: +44 1275 395 600

WITTENSTEIN

email: sales@high**integrity**systems.com
web: www.high**integrity**systems.com