HighIntegritySystems

WITTENSTEIN

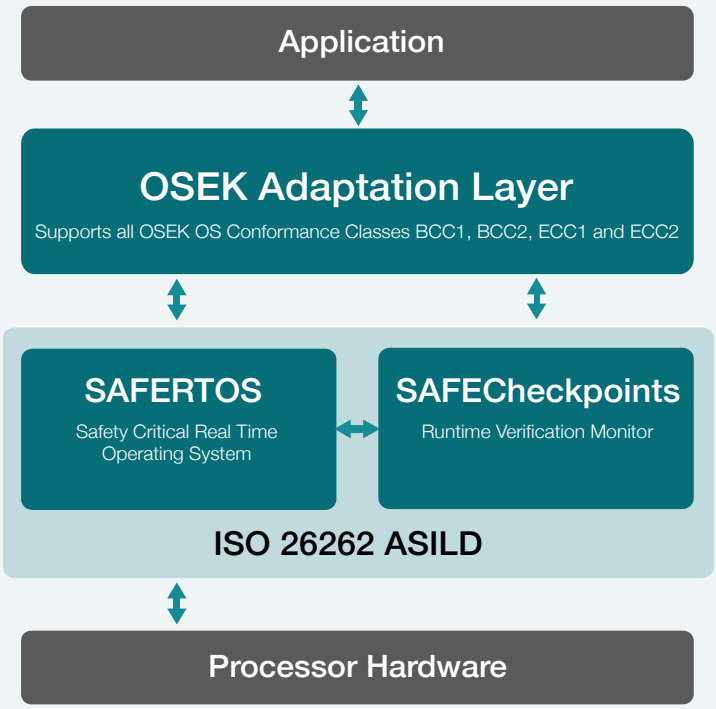
SAFERTOS® for Automotive

Introduction

WITTENSTEIN high integrity systems (WHIS) has long recognised that there is an increasing need for safe, secure, embedded solutions that provide responsive, feature rich functionality within a networked environment. In response we have created a complete RTOS package for the Automotive sector:

- **SAFERTOS®** – pre-certified to ISO 26262 ASIL D. A high performance, small footprint RTOS
- **SAFECheckpoints** – fulfils the requirement of ISO 26262 ASIL C&D software designs to have a runtime monitor
- **OSEK OS Adaptation Layer** – creating a 'drop-in' OSEK OS RTOS package frequently used in Automotive Designs

This package is modular, meaning you can select just SAFE**RTOS**, SAFE**RTOS** with either SAFE**Checkpoints** or the OSEK OS adaptation layer, or all three, knowing that each component is developed to the highest standards.



SAFERTOS

SAFE**RTOS** is available pre-certified to ISO 26262 ASIL D by TÜV SÜD.

The ISO 26262 standard is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/ Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive, electronic, and electrical safety-related systems.

ASIL D is the highest possible safety rating under this standard, and is achieved by performing a risk analysis of a potential hazard that examines the severity, exposure and controllability of the vehicle operating scenario. As the final application where SAFE**RTOS** will be used is not known, SAFE**RTOS** has been certified as a "Safety Element out of Context" (SEooC). When designing SAFE**RTOS**, our engineers have made assumptions about the safety goals and ASIL level required. These safety goals are described within the SAFE**RTOS** Safety Manual along with the installation and integration instructions. Developers using SAFE**RTOS** need to confirm that the safety goals defined by SAFE**RTOS** meet the requirements of their project.

OSEK OS Adaptation Layer (Optional)

OSEK is an open standard, published by a consortium founded by the automobile industry. OSEK was designed to provide a standard software architecture for the various Electronic Control Units (ECUs) in a vehicle.

SAFE**RTOS** can be supplied with an optional OSEK OS adaptation layer, supporting OSEK OS Conformance Classes BCC1, BCC2, ECC1 and ECC2. This allows SAFE**RTOS** to be used as a drop-in component within OSEK OS compliant systems, which are frequently used within automotive systems.

SAFECheckpoints Runtime Verification Monitoring (Optional)

There is an expectation within ISO 26262 that runtime verification monitors will be used to detect, indicate and handle systematic faults within software rated ASIL C and D.

SAFE**RTOS** includes a range of built-in error checking routines. Additionally, there is the optional SAFE**Checkpoints** module which provides SAFE**RTOS** with a sophisticated Task Monitoring capability, ensuring the scheduling of Tasks

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

is occurring as intended. The Checkpoints mechanism allows the user to specify timing tolerances for critical sections of code; this can be used to ensure that:

- Periodic Tasks run within tolerances.
- Sections of processing within Tasks complete on time.
- Interrupt Event to handler Task processing completes within allowable tolerances.
- Complex functionality involving multiple Tasks completes within allowable tolerances.

Individual checkpoints can specify their own call back function or the system error hook can be activated.

- Single shot and Periodic checkpoints can be created.
- Periodic checkpoints can operate in fixed or relative timing modes.

Safety & Performance

SAFE**RTOS** provides high performance without compromising safety. SAFE**RTOS** is a highly deterministic micro kernel that has a minimum ROM footprint in the region of 10 K Bytes. SAFE**RTOS** contains no dead or unused code and is statically defined at compile time.

It uses deterministic, pre-emptive, priority-based Task scheduling to ensure the primary safety goal - that the highest priority Task able to execute is the Task currently running. SAFE**RTOS** delivers intrinsic safety checking of key data variables by using inverted mirrored data and enhanced parameter checking.

SAFE**RTOS** contains features that assist designers of safety critical systems. For example, the Task Isolation and Separation feature of SAFE**RTOS** enables developers to co-locate safety critical code with non-safety critical code. This feature uses the processor's Memory Management Unit (MMU) or the Memory Protection Unit (MPU), configuring the permitted memory areas for each new Task, on each context switch. Used effectively this can greatly reduce the amount of safety critical code required within an automotive device

With an imperceptible boot time SAFE**RTOS** is an ideal choice in systems that need to protect users and equipment from hazards quickly after a power on or brown out event.

Supported Processors

SAFE**RTOS** supports all the common architectures used within automotive devices. In particular, we have worked closely with Texas Instruments to create a highly optimized port of SAFE**RTOS** for the Hercules safety controller family, with Infineon for the AURIX TriCore™ family, as well as with many other semiconductor companies.

To see our currently supported platforms please see our website, or contact us for the most up-to-date list.

Security in Your Automotive Application

Whilst security has always been important, it has become even more of a priority over the last few years. We take cyber security very seriously, and can provide a variety of solutions.

One cyber security risk factor to consider is the length of the supply chain. The more companies you have in your software supply chain, the greater the risk. SAFE**RTOS** is developed completely in-house here at WHIS, with every line of code accounted for and verified, providing a very strong justification for using SAFE**RTOS** within security applications.

For additional security, we offer SAFE**CRC Checker**, a safety component from WHIS that can be used in conjunction with SAFE**RTOS**. SAFE**CRC Checker** guards against corruption and malicious attack by confirming the correctness of your program memory.

Automotive Design Assurance Pack

SAFE**RTOS** is supplied as source code and accompanied by a Design Assurance Pack (DAP). The DAP contains all the design and verification artefacts required to support ISO 26262 ASIL D certification. SAFE**RTOS** is delivered tailored to your specific processor/compiler combination, removing the need for retesting on the target hardware, and creating a smooth path to re-certifying SAFE**RTOS** within an application. The DAP ensures:

- No retesting on target hardware is required
- Easy installation and integration into your development environment
- Reduced development costs and improved time to market
- Smooth path to certifying SAFE**RTOS** within an application

WITTENSTEIN high **integrity** systems

Worldwide Sales and Support
Americas: +1 408 625 4712
ROTW: +44 1275 395 600
Email: sales@high**integrity**systems.com
Web: www.high**integrity**systems.com