WITTENSTEIN high integrity systems

A Safety Company Specialising in RTOS and Middleware

SAFERTOS  OPENRTOS  FreeRTOS Services
Committed to Safety

Safety Critical RTOS Experts

WITTENSTEIN high integrity systems: experts in embedded RTOS and Middleware technology with a specialisation in safety certified software. Supplying advanced RTOS and Middleware components across a broad range of market sectors and applications, from basic embedded designs, up to complex safety systems demanding the highest levels of certification.

A Safety Systems Company
WITTENSTEIN high integrity systems (WHIS) is part of the WITTENSTEIN Group, a global technology company established in 1948 with a presence in over 45 countries.

WHIS is the Group’s centre of excellence for high integrity and safety critical embedded systems design. WHIS is first and foremost a safety systems company, a key differentiation in the real-time operating systems market, as WHIS has direct experience developing safety critical products.

The WHIS functional safety management structure, and high integrity development life cycles, ensure that WHIS safety products deliver consistently high levels of performance and dependability.

Our Relationship with Amazon FreeRTOS
WHIS leverage RTOS technology from FreeRTOS, the market leading embedded RTOS. SAFERRTOS has a similar functional model to FreeRTOS, whereas OPENRTOS is FreeRTOS, with a commercial license that includes professional support and middleware integration.

Richard Barry created FreeRTOS in 2003 whilst working as Innovation Manager at WHIS. In 2017, Amazon Web Services (AWS) announced it had taken over stewardship of FreeRTOS, with Richard also moving to AWS. Simultaneously, WHIS and AWS announced they had formed a Strategic Business Alliance, enabling WHIS to continue to supply commercial and safety critical alternatives to FreeRTOS.

Partners

Salomea Paprotny
Sales Leader
A highly experienced, global sales executive, and a passionate believer in excellent customer relationship management, responsiveness and attentive customer service. An advocate for seeing the world from the customer’s perspective and finding solutions that meet their needs.

Andrew Longhurst
Business Leader
A WITTENSTEIN Pioneer, with an extensive background in electrical, electronic, software engineering and business development. Andrew has an in-depth understanding of the challenges facing embedded engineers within the safety critical sector.

Steve Ridley
Head of Engineering
A highly knowledgeable and talented engineer with more than 20 years’ experience designing real time embedded software for use in safety critical applications across aerospace, automotive, industrial and telecoms industries.

WITTENSTEIN high integrity systems
Americas: +1 408 625 4712
ROTW: +44 1275 395 600
We provide a leading RTOS ecosystem that’s achieved global recognition.

**RTOS & Middleware**

The Complete, Integrated Solution

**RTOS, Middleware, Tools and Services**
The WHIS RTOS ecosystem has been tailored to enable embedded software engineers to develop robust and responsive products, efficiently and on-time.

**Extensive Architecture and Tool Chain Support**
WHIS products support an extensive range of embedded platforms and tool chains, providing solutions for commercial and safety critical applications, backed up by flexible licensing terms.

**Knowledgeable, Comprehensive Support**
Customers are supported from project conception and throughout the lifetime of their product. The WHIS team of expert engineers provide technical support, as well as advice on how to use our components within a safety critical development, and guidance on product certification.

**From Single Products to Corporate Solutions**
The extensive and feature rich WHIS product range offers a compelling solution for engineers seeking software components for their next project, and for corporations seeking a single supplier for their RTOS and middleware needs throughout their entire organization.

**Continual Innovation**
SAFERTOS® was the first RTOS to be certified to IEC 61508 by TÜV SÜD, as well as the first pre-certified RTOS to be ROM’ed within a mainstream microprocessor. WHIS continues to lead the way with its family of real time operating systems solutions that have revolutionised the RTOS market.

The FreeRTOS kernel is a market leader, with over 100,000 downloads per year.

We rebuilt for the safety sector, adding support for multiple certification standards to create SAFERTOS®.

We offer commercial licensing and professional support to create OPENRTOS®.

We provide a leading RTOS ecosystem that’s achieved global recognition.
SAFERTOS® is a pre-emptive, pre-certified real time operating system that delivers unprecedented levels of determinism and robustness to embedded systems. Based on the FreeRTOS functional model, but specifically re-designed for the safety market by our own team of safety experts, SAFERTOS has been independently certified by TÜV SÜD to IEC 61508 SIL3 and ISO 26262 ASIL D.

SAFERTOS key features include:

- Intrinsic self-verification routines
- MMU/MPU support as standard
- Migration path from FreeRTOS
- Pre-certified to IEC 61508-3 SIL 3 by TÜV SÜD
- Pre-certified to ISO 26262 ASIL D by TÜV SÜD
- MISRA C compliant
- Contains no open source code
- Comprehensive MC/DC verification coverage
- Supports wide range of microprocessors
- Supports all popular development tools
- Full source code and Design Assurance Pack
- Ultra-Low Power Mode

Built Specifically for the Safety Market
Designing a safety critical RTOS is about more than just applying process. Risk management is required across the complete development life cycle to identify a full set of safety requirements. These safety requirements have a major impact on the implementation of the RTOS, resulting in a trusted product containing intrinsic self-verification routines and other features essential for use in a safety critical application.

The Design Assurance Pack
SAFERTOS is tailored to your specific processor/compiler combination, and delivered with evidence supporting certification for your industry in the form of a Design Assurance Pack (DAP). The DAP gives you complete transparency over the full Design Life Cycle, and illustrates the exceptional high quality of SAFERTOS.

A Smooth Certification Path
Using our extensive safety critical design experience we have made certifying SAFERTOS integrated within a product an easy and hassle-free process.

Contained within the DAP is the all-important Safety Manual. The Safety Manual explains exactly how to install and integrate SAFERTOS into your development environment. Following the concise instructions will also generate the evidence required by your auditors to confirm the process has been followed correctly. This removes the need to re-test SAFERTOS on your target hardware, and provides a solid, dependable platform for your development.

MMU/MPU Support as Standard
SAFERTOS is supplied with Memory Management Unit (MMU) and Memory Protection Unit (MPU) support as standard. With care this allows both safety critical and non-safety critical code to be present within the same linear address space, whilst remaining isolated from each other, greatly reducing development time and cost.

Full Life Cycle Support
Our own team of software and safety experts are on hand to help. With extensive knowledge and direct experience of safety certified software, we can help resolve your technical, safety and certification issues.

As part of our standard support and maintenance agreement, we will, on request revalidate your version of SAFERTOS with the latest compiler version, ensuring you can use SAFERTOS with the very latest tools.
SAFERTOS® CORE

For Systems that Need to Consider Safety

SAFERTOS CORE provides the complete functionality and API of SAFERTOS. It’s designed to support embedded systems that need to consider safety, but don’t require safety certification.

Full SAFERTOS Functionality and API
SAFERTOS CORE is the RTOS for embedded systems where safety needs to be considered, or designed-in for future consideration. It is ideal for projects where full safety certification/documentation is not required, or at least not required at the start of a long safety development life cycle. SAFERTOS CORE provides the complete functionality and API of SAFERTOS.

SAFERTOS CORE is ideal for companies who are developing products that:

- Need to consider safety but don’t require full certification
- May require certification in the future, and need to future proof their designs;
- Require a robust, highly deterministic RTOS, incorporating key safety features;
- Are at the start of a lengthy development cycle where certification evidence/documentation will not be required until the final stages.

SAFERTOS or SAFERTOS CORE?
SAFERTOS is designed for systems that require safety certification.

SAFERTOS CORE uses the actual core SAFERTOS source code, common across safety certified variants of SAFERTOS, however it is ported for use upon your specific processor/compiler combination using commercial grade processes.

Whereas SAFERTOS is supplied with a Design Assurance Pack (Industrial), or a Design History File (Medical) supporting safety certification, SAFERTOS CORE is supplied as source code accompanied by a comprehensive User’s Manual.

SAFERTOS CORE is available fully integrated with our advanced, feature rich Middleware and Safety Components, delivered as one seamless build of code.

<table>
<thead>
<tr>
<th>Features</th>
<th>SAFERTOS</th>
<th>SAFERTOS CORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAFERTOS functionality and API</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Core SAFERTOS source code</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Standard port layer</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Safety qualified port layer</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>DAP and Safety Manual (core and port layer)</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Available pre-certified (IEC 61508 SIL 3)</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>RTOS technical support</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RTOS Safety/ Certification support</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Safety Plugins available</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Middleware available</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Training available</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
RTOS for Industrial

Pre-Certified to IEC 61508 SIL 3 by TÜV SÜD

SAFERTOS provides Industrial developers with a responsive, deterministic embedded Real Time Operating System (RTOS) with a Design Assurance Pack that provides an easy route to achieving certification of SAFERTOS once integrated into an Industrial Safety Product.

Common Applications Using SAFERTOS:
- Sensors
- Industrial automation
- Drilling equipment
- Oil and gas valves
- Power generation applications
- Actuation systems
- Industrial control systems
- Radiation monitoring equipment
- Battery charging devices
Pre-certified to IEC 61508 SIL 3 by TÜV SÜD
SAFE RTOS is pre-certified to IEC 61508-3 SIL 3 by TÜV SÜD. SIL 3 is the highest possible safety rating a software only component can achieve.

IEC 61508 is the international standard for electrical, electronic and programmable electronic safety related systems. It sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL). Four SILs are defined according to the risks involved in the system application. SIL 4 is used to protect against the highest risks, and takes into account specific end product risks. The standard specifies a process that can be followed by all links in the supply chain so that information about the system can be communicated using common terminology and system parameters.

RTOS for Rail
Supporting EN 50128 Certification

The majority of SAFE RTOS rail developers, whether it be for track side or on carriage applications, purchase the standard Industrial DAP supporting certification to IEC 61508 SIL3. For those companies that need to demonstrate compliance to the European Rail Standard EN 50128, WHIS can provide the additional information required integrated into the DAP.

Typical SAFE RTOS rail applications include signalling, control systems, door management and communication systems.
RTOS for Medical

Supports IEC 62304 & FDA 510(k)

Our software is used in a wide variety of medical devices, from infusion pumps to defibrillators to prosthetics. Our experience allows us to offer solutions that accelerate the development of medical devices based on SAFERTOS and its Design History File, supporting FDA 510(k) class III medical device submissions and IEC 62304 class C certifications.

Common Medical Devices Using SAFERTOS:
- Infusion pumps
- Dialysis machines
- Insulin pumps
- Prostheses
- Hemostasis analyser system
- Liver perfusion machines
- Ventricular Assist Devices
- Endoscopes
- Cardio-vascular/hypertension monitors
- Defibrillators
- Self-monitoring blood glucose and dosing devices

Reduced Certification Time & Costs for Medical Submissions
SAFERTOS supports FDA 510(k) class III device submissions and IEC 62304 class C certifications.

The SAFERTOS Safety Manual clearly details how to install and integrate SAFERTOS into a medical device development environment. Following the concise instructions contained within the Safety Manual preserves the verification and validation already performed, and removes the need for expensive and prolonged retesting on the target hardware.

- FDA 510(k) class III medical device submissions
- IEC 62304 class C certification
- Independently assessed by TÜV SÜD to IEC 62304 Class C
- Extensively used in Medical Device developments
SAFE RTOS provides developers with a responsive, robust, and deterministic embedded RTOS, containing features supporting the development of safety critical devices, coupled with an Aerospace Design Assurance Pack that provides an easy route to achieving certification of SAFE RTOS once integrated within an aerospace product.

- **DO178C**
- Deterministic, responsive embedded RTOS
- Reduces certification time and costs
- Reduces product development risks

**21 CFR 820 Medical Design History File**

The SAFERTOS Design History File complies with the requirements of 21 CFR 820. The Design History File contains the documentation and testing evidence, which supports SAFERTOS inclusion in a Major Level Of Concern submission, according to the guidelines contained in the Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices.

The Design History File contains every planning, design and verification document generated during the development of the SAFERTOS variant for a specific processor/compiler combination.

**ISO 14971 Risk Management for Medical Devices**

The SAFERTOS high integrity design life cycle implements a risk management system that, where applicable, complies with ISO 14971:2009 "Application of risk management to medical devices".

This provides reassurance that SAFERTOS has been designed to meet the safety requirements for use within a medical device. It also allows for the easy integration of the Design History File into a medical device development environment.

**SAFERTOS in Multicore Medical Devices**

SAFERTOS enables dual and multicore/processor medical device designers to create seamless, mixed safety criticality designs quickly and efficiently. Due to its small size and its safety critical credentials, SAFERTOS is ideally suited for use on the primary core. This allows the system to boot and configure itself securely before enabling other cores that could run non-critical applications such as Linux to implement web servers and WiFi connections.

In a multicore environment, SAFERTOS is typically used on cores implementing safety critical functionality, or on cores providing monitoring/verification of the primary function. Due to its high safety classification, SAFERTOS can safely be used on both primary and monitoring cores, removing the need to use differential software.

**100% MC/DC Test Coverage**

MC/DC is used in avionics software development to ensure adequate testing of the most critical software, which is defined as that software which could provide, or prevent failure of, continued safe flight and landing of an aircraft.

**Tracing into Source Code**

SAFERTOS supports Bidirectional tracing between the aerospace Design Assurance Pack and the SAFERTOS source code to comply with the rigorous requirements of DO178C. This is achieved by tracing to function level code within the DOORS database.

**PSAC support**

WHIS will supply clear and concise information for the inclusion of SAFERTOS into an aerospace project. This information can be included within the RTOS section of your PSAC.
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 an 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 ideal for Automotive designs

This package is modular, meaning you can select just SAFERTOS, SAFERTOS with either SAFECheckpoints or the OSEK OS adaptation layer, or all three, knowing that each component is made to the highest quality.

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 SAFERTOS will be used is not known, SAFERTOS has been certified as a “Safety Element out of Context” (SEooC). When designing SAFERTOS, our engineers have made assumptions about the safety goals and ASIL level required. These safety goals are described within the SAFERTOS Safety Manual along with the installation and integration instructions.
SAFECheckpoints Runtime Verification Monitoring

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

OSEK OS Adaptation Layer

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

Fast, Lightweight, Intuitive

OPENRTOS® provides a commercial license for the FreeRTOS kernel, the highly successful, small, efficient embedded real time operating system. OPENRTOS and the FreeRTOS kernel share the same code base, however OPENRTOS truly transitions developers into the professional world, with commercial licensing, and access to direct support, backed up by tools, training and consultancy services. Developers can extend the functionality of OPENRTOS by selecting from a wide range of middleware components and Board Support Packages.

OPENRTOS supports a large number of microprocessors and FPGA soft cores, can be used in System on Chip devices and even ROM’ed into the memory of microprocessors.

Start Your Development for Free

Our novel approach to licensing means developers can start their development for free using the FreeRTOS kernel and upgrade to OPENRTOS later when a commercial license or support is required. FreeRTOS kernel updates and ports are simultaneously released by WITTENSTEIN high integrity systems as OPENRTOS.

Professional Service

WHIS takes responsibility for ensuring OPENRTOS works with your chosen processor / compiler combination, verifies its correct operation, and delivers a working demonstration project with full source code integrated with any purchased middleware components. This approach has been designed to ensure your developers are working effectively with our products without delay. OPENRTOS is also supplied with one year’s free support, giving you direct access to our team of highly experienced engineers.

Supporting Your Processor

OPENRTOS supports a wide number of processors, including those that FreeRTOS does not support. Our team of engineers are experienced in porting OPENRTOS to a variety of processors, optimizing speed and integration. If your processor is not supported by FreeRTOS, please ask us about creating a new version of OPENRTOS for your specific processor.

Key Features

OPENRTOS key features include:

• Pre-emptive, cooperative, & round robin scheduling options
• Unlimited number of tasks and priority levels
• Queues, semaphores and mutexes
• Event Flags
• Task Notification
• Run time statistics
• Very efficient software timers
• Uses minimum system resources
• Supports wide range of microprocessors
• Supports all popular tool chains
• Very large user base
• Easy to use

Royalty Free, Perpetual Licensing

We aim to provide customers with a license model that best suits their needs, supported by a transparent pricing policy.

Our standard licensing model uses a royalty free, perpetual license with an unlimited number of production units.

We have four standard levels of licensing- Single Product, Product Line, Multi Product and Corporation, but remain flexible and receptive to the needs of our customers.
OPENRTOS IE

Intel Server Platforms

OPENRTOS IE is a powerful, small footprint RTOS and IE Driver solution for the Intel Innovation Engine (IE), located on Intel’s Data Server Platforms. OPENRTOS IE allows system builders to develop novel functionality on Intel server platforms quickly and efficiently, helping to create product differentiation within the server market.

Intel Innovation Engine
The Innovation Engine is a small Intel architecture processor and I/O sub-system embedded into Intel’s Server Platforms. The Intel IE enables system builders to create their own unique, differentiating firmware for the server, storage and networking markets. Some possible usages include a lightweight BMC providing basic manageability and reduced overall system cost, or to improve server performance by offloading BIOS and BMC routines to the IE.

The Most Compact Solution
OPENRTOS IE is a fast, lightweight, small footprint Real Time Operating System complete with a comprehensive set of IE device drivers. OPENRTOS is the smallest RTOS option enabled for the Intel IE, with the RTOS requiring less that 10Kbytes and the entire RTOS and IE driver solution less than 100Kbytes, maximizing the amount of memory available for the system builder’s application code.
Safety Plugins

Increasing Integrity

Our safety plugins are designed to bring greater integrity to your safety critical application. All of our safety plugins are delivered as high integrity modules, with both full source code and a Design Assurance Pack built to the same exceptionally high standard as SAFERTOS.

SAFEXchange

Securely share safety critical data between multiple processors and cores across black channel communication buses. Conforms to the principles of IEC 61784-3.

SAFECRC Checker

Guard against corruption and malicious attack by confirming the correctness of your program memory.

SAFECheckpoints

Provides a sophisticated task monitoring capability that allows the user to specify timing tolerances for critical sections of code.

Middleware

Fully Integrated Solutions

WHIS Middleware components are available with all WHIS RTOS products as one highly integrated, fully optimised and verified package, accompanied by a demonstration application, allowing engineers to work effectively from the day they are delivered.

When integrating middleware with SAFERTOS, our safety engineers will use the SAFERTOS MPU functionality to isolate middleware code from other safety critical code segments. This allows mixed safety integrity levels of software to coexist within the same build of code, resulting in lower development & production costs.

Board Support Packages (BSP)

We provide full Board Support Package services, and will design to your specific requirements for use with either OPENRTOS or SAFERTOS.

File Systems

Our storage solution provides a compact, resource efficient and highly reliable embedded FAT16/FAT32 file system, created especially for embedded applications that use portable storage media such as SD/MMC, USB drives and Flash.

TCP/IP

Our networking solution is a scalable, thread safe TCP/IP stack. It provides a familiar, standards based, Berkeley sockets interface, making it as simple to use and as quick to learn as possible. An alternative callback interface is also available for advanced users.

Free Downloadable Demos

Download free, fully functional demos for SAFERTOS, along with datasheets, manuals and tutorials.

Visit www.highintegritysystems.com to see what’s available.
Development Tools

In Depth Analysis

**Tracealyzer**
Tracealyzer is a powerful profiling tool, that visualizes real-time system events, enabling engineers to debug and optimize their applications.

- Over twenty different interlinked views
- Analyse CPU loading profiles
- Understand the interaction of tasks and ISR
- Provides tracing of all kernel events
- Logging of additional user defined events
- Runs on any Windows host
- Smooth magnification and scrolling to change views

**STATEVIEWER**
Stateviewer is a development tool providing enhanced kernel awareness, including the ability to check the stack usage of each task as well as the task’s switching and resource states. The Stateviewer IDE plug-in tool is offered with IAR and Eclipse tools and works with both OPENRTOS and SAFERTOS. It is freely available for download from our website.

Support, Training & Consultancy

**Support**
Only the most experienced engineers are assigned to provide support. This includes access to the WHIS online support ticket system for up to 5 developers. Client engineers can contact the WHIS engineering team if they have any questions regarding licensed components.

**Training Courses**
Utilise the experienced WHIS team of engineers to fully understand the full capability of the purchased RTOS and make greater use of its features. Enjoy enhanced designs and shortened development schedules.

**Consultancy**
The WHIS consultancy services are designed to support customers, providing the knowledge and experience to help optimize the final design, improve the design processes, and smooth the route to certification. Just a few hours of consultancy to review a preliminary design and check the approach being taken is correct has been proven to deliver significant benefits to the outcome of a project.
Design, development, and support of high integrity software covering medical, aviation automotive and industrial applications.