WITTENSTEIN

WITTENSTEIN high **integrity** systems

Creating a safer, greener, more secure future

- SAFE**RTOS**®
- OPEN**RTOS**®
- 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. SAFE**RTOS**® has a similar functional model to FreeRTOS, whereas OPEN**RTOS**® 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.

Andrew Longhurst
Managing Director

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

With three decades of expertise in real time embedded systems, Steve excels in hardware and software. His industry experience in Automotive, Defence, Aerospace, Telecoms, and Medical sectors offers invaluable insights into challenges faced by engineering teams across diverse industries.

Stephanie Bean
Marketing Leader

Stephanie Bean is a dynamic Marketing Leader committed to fostering strategic partnerships within the industry. With a focus on elevating the WITTENSTEIN high integrity systems brand and online footprint, Stephanie champions progressive marketing strategies to drive impactful results.

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.

Neil Johnson
Finance and Operations Manager

Bringing a wealth of experience to the table as a qualified accountant, with a keen eye for detail and a strategic mindset. Dedicated to data-driven decision making and commitment to excellence, Neil plays a pivotal role in shaping our company's growth and sustainability.

Simon Hodges
Process and Quality Manager

Unwavering dedication to continuous improvement, innovation and ensuring our products meet the highest quality standards. Simon's expertise is the bedrock of our product and service integrity.

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

The image on the front cover is the WITTENSTEIN Innovation Factory, Germany.

RTOS & Middleware

The Complete, Integrated Solution

Empowering Embedded Excellence
WHIS tailors its RTOS ecosystem to empower software engineers to efficiently develop robust, responsive products. Our products support a wide array of embedded platforms and tool chains, offering solutions for both commercial and safety-critical applications. Flexible licensing terms further enhance the adaptability of our offerings.

Comprehensive Support for Your Journey
Our team of expert engineers provides technical assistance, guidance on safety-critical development, and insights on product certification. Whether you're an individual engineer or a corporation, our extensive product range provides a compelling solution, unifying your RTOS and middleware needs across your entire organization.

Pre-certified to IEC 61508 SIL 3 by TÜV SÜD
SAFE**RTOS**® achieves the highest safety rating possible - SIL 3 - as pre-certified by TÜV SÜD. IEC 61508 is the international standard for electrical, electronic, and programmable electronic safety-related systems. It defines a meticulous process, considering the risks involved, and establishes four Safety Integrity Levels (SILs). SIL 3 addresses the highest risks, incorporating specific end product risks. Our adherence to this standard facilitates effective communication across the supply chain, ensuring a common understanding of system parameters and terminology.

The FreeRTOS kernel is a market leader, which is downloaded every 170 seconds

We rebuilt for the safety sector, adding support for multiple certification standards to create SAFE**RTOS**®

We offer commercial licensing and professional support to create OPEN**RTOS**®

We provide a leading RTOS ecosystem that's achieved global recognition

Partners

email: sales@highintegritysystems.com
web: www.highintegritysystems.com

SAFERTOS®

For Systems that Require Safety Certification

SAFE**RTOS**® 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, SAFE**RTOS**® has been independently certified by TÜV SÜD to IEC 61508-3 SIL3 and ISO 26262-6 ASIL D.

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
SAFE**RTOS**® 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 SAFE**RTOS**®.

A Smooth Certification Path
Using our extensive safety critical design experience we have made certifying SAFE**RTOS**® 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 SAFE**RTOS**® 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 SAFE**RTOS**® on your target hardware, and provides a solid, dependable platform for your development.

MMU/MPU Support as Standard
SAFE**RTOS**® supports the definition and manipulation of MPU regions on a per task basis. This feature provides the tools allowing developers to add a degree of spatial separation between tasks, which used effectively, can help prevent tasks directly making unintentional or accidental access to incorrect memory regions.

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 SAFE**RTOS**® with the latest compiler version, ensuring you can use SAFE**RTOS**® with the very latest tools.

SAFE**RTOS**® **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 26262-6 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.

Multicore

SAFE**RTOS**® empowers engineers working with multicore devices to swiftly and efficiently create integrated safety-critical designs using an Asymmetric Multi-Processing (AMP) architecture, while also seamlessly incorporating stream buffers for enhanced data communication and synchronization.

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

Enhanced Security

For Safety-Critical Devices

Cyber security is increasingly a fundamental requirement for almost every embedded software component, but especially the RTOS. The RTOS not only protects itself, but it can also help mitigate cyber security risks within other elements of the software architecture.

An enhanced security RTOS should be able to:

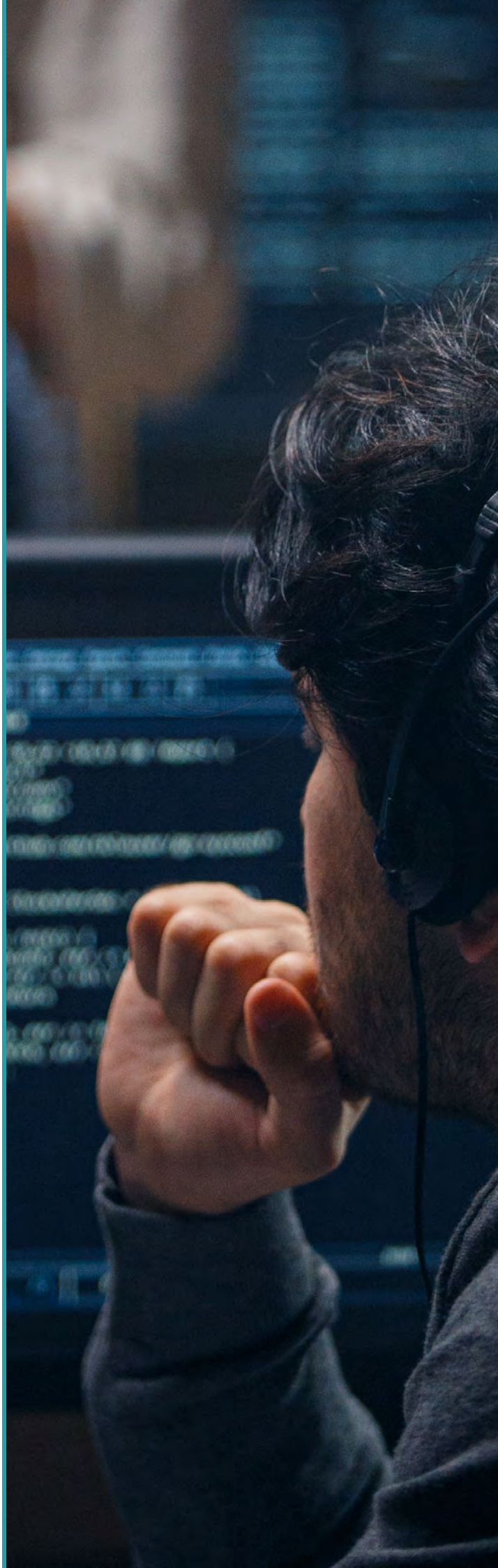
- Detect and report the presence of a cyber security threat;
- Protect sensitive system information;
- Stop the cyber security threat from developing into a system wide attack;
- Allow developers to claim a degree of cyber security compliance.

It's quite common for software architectures to be constructed from a mixture of bespoke software and third party software. Integrating third-party components from unknown sources, like open-source libraries, inherently injects cyber security risks. These external elements may harbor hidden backdoors or vulnerabilities, jeopardizing your system's security. Selecting an RTOS with an enhanced security capability can help mitigate this threat, as the RTOS should be able to detect when a bad actor has compromised a Task and should restrict and prevent the cyber security threat from obtaining sensitive system data or taking control of other elements of the system.

SAFE**RTOS**® can be purchased with an Enhanced Security Module (ESM), which has been designed to comply with ISO 21434 the Automotive Cyber Security standard. The intention of the ESM is to detect the presence of a cyber security threat and then to significantly contain and restrict it to just the compromised Task.

The SAFE**RTOS**® Enhanced Security Module has four main elements:

- A security hardened spatial separation mechanism that improves the spatial separation between individual Tasks and the RTOS. This ensures Tasks only have access to memory regions they have been configured for and cannot access information from other memory regions. This limits the scope of the attack to a smaller memory region.
- The RTOS implements a configurable Access Control Policy (ACP) for its API, allowing restrictions on each individual Task's access. This ACP prevents compromised tasks from creating new tasks, changing privilege levels, or interfering with the scheduler, stopping the security threat developing into a system wide attack.
- The RTOS implements an Object Access Control Policy (OACP) for objects like queues and semaphores, allowing per-task access configuration and reduction. This restricts the amount of information each Task has access to, therefore making it more difficult for a cyber security threat to obtain critical data items.
- A penetration detection mechanism that informs the application when a potential attack is happening. Attacks can happen over a period of time, and the RTOS should be able to detect when a bad actor is probing the system to find system vulnerabilities.



Automotive

Pre-certified to ISO 26262-6 ASIL D by TÜV SÜD

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:

- SAFE**RTOS**® – pre-certified to ISO 26262 ASIL D. A high performance, small footprint RTOS;
- SAFE**Checkpoints** – 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 SAFE**RTOS**®, SAFE**RTOS**® with either SAFE**Checkpoints** or the OSEK OS adaptation layer, or all three, knowing that each component is made to the highest quality.

Pre-certified to ISO 26262-6 ASIL D by TÜV SÜD
SAFE**RTOS**® is pre-certified to ISO 26262 ASIL D by TÜV SÜD.

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. 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.

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**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 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**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.

SAFE**RTOS**® **is Used in Many Automotive Applications:**

- Zone controller safety islands;
- Battery management systems;
- Digital cockpits;
- Engine control units;
- Radar/vision systems;
- Cameras and sensors;
- Network hubs;
- Advance driver assist systems;
- Autonomous drive systems.

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

Aerospace

In Compliance with DO 178C Design Assurance Level A

SAFE**RTOS**® provides aerospace developers with a responsive, robust and deterministic embedded RTOS, supported by clear and concise certification planning documentation, and comprehensive design and verification evidence.

- Deterministic embedded RTOS;
- Clear and concise certification planning documentation;
- Comprehensive design and verification evidence;
- Delivered as source code and binary library.

The SAFE**RTOS**® aerospace development life cycle fully complies with the requirements of DO 178C up to Design Assurance Level (DAL) A and supports the standard aerospace audit cycle. The licensee has the option to lead and/or participate within these audits.

Clear and concise certification planning documentation
At the start of the development we will supply a set of standard certification planning documentation along with a bespoke 'Plan for Software Aspects of Certification' (PSAC). We will work with your Designated Engineering Representatives (DER) to amend and finalize the plans which will be authorized during the Stage Of Involvement (SOI) 1 audit.

- Plan for Software Aspects of Certification;
- Software Development Plan;
- Software Configuration Management Plan;
- Software Quality Assurance Plan;
- Software Verification Plan.

Comprehensive design and verification evidence
The design documentation and source code will be developed in accordance with the WHIS Requirements, Design and Coding standards. At around 50% through the design process a SOI 2 audit will be held to confirm conformance with the certification plans.

Full verification will be performed on the target hardware. Verification test cases are written against the high and low level requirements, with MC/DC testing used to measure test coverage. When 100% MC/DC coverage has been achieved by verifying the requirements, the binary library will have been fully verified.

A SOI 3 audit is normally held when 75% of the verification effort has been achieved.

Certification completion
The SOI 4 audit will complete the certification effort allowing the customer to immediately use the evidence. SOI 4 will ensure that all the documentation is in place, and that the final certification artefacts are ready to be delivered.

- Software Life Cycle Environment Configuration Index;
- Software Configuration Index;
- Software Accomplishment Summary (SAS).

Delivered as source code and binary library
The final delivery will include the fully verified binary library, but also the full source code allowing developers to gain an in-depth knowledge of the operation and features of SAFE**RTOS**®, and aid debugging of complex issues.

Full Quality Records
The SAFE**RTOS**® development life cycle is fully transparent, supported with detailed quality records and evidence required for successful completion of audits. These items include peer review data, problem reports, database contents, and associated records for both SQA and CM. We also supports on-site audits.

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

RTOS for Industrial

Pre-Certified to IEC 61508-3 SIL 3 by TÜV SÜD

SAFE**RTOS**® 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 SAFE**RTOS**® once integrated into an Industrial Safety Product.

Common Applications Using SAFE**RTOS**®:

- Sensors;
- Industrial Automation;
- Drilling Equipment;
- Oil and Gas valves;
- Power Generation Applications;
- Actuation Systems;
- Industrial Control Systems;
- Radiation Monitoring Equipment;
- Battery Charging Devices;
- Industrial door controllers;
- Safety PLCs.

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 systems;
- Communication systems;
- Control platform for electrified powertrains;
- Control units;
- Battery units;
- Door control units.

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 SAFE**RTOS**® and its Design History File, supporting FDA 510(k) class III medical device submissions and IEC 62304 class C certifications.

Common Medical Devices Using SAFE**RTOS**®:

- 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;
- Surgical robots;
- Heart pumps.

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

The SAFE**RTOS**® Safety Manual clearly details how to install and integrate SAFE**RTOS**® 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.

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 SAFE**RTOS**® 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 SAFE**RTOS**® variant for a specific processor/compiler combination.

ISO 14971 Risk Management for Medical Devices
The SAFE**RTOS**® 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 SAFE**RTOS**® 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® CORE

For Systems that Need to Consider Safety

SAFE**RTOS**® CORE provides the complete functionality and API of SAFE**RTOS**®. It's designed to support embedded systems that need to consider safety, but don't require safety certification.

Full SAFERTOS® Functionality and API

SAFE**RTOS**® 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. SAFE**RTOS**® CORE provides the complete functionality and API of SAFE**RTOS**®.

SAFE**RTOS**® 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?

SAFE**RTOS**® is designed for systems that require safety certification.

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

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

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

Features	SAFE**RTOS**®	SAFE**RTOS**® CORE
SAFE**RTOS**® functionality and API	√	√
Core SAFE**RTOS**® source code	√	√
Standard port layer	-	√
Safety qualified port layer	√	-
DAP and Safety Manual (core and port layer)	√	-
Available pre-certified (IEC 61508 SIL 3)	√	-
RTOS technical support	√	√
RTOS Safety/ Certification support	√	-
Safety Plugins available	√	√
Middleware available	√	√
Training available	√	√

email: sales@highintegritysystems.com
web: www.highintegritysystems.com

OPENRTOS®

Fast, Lightweight, Intuitive

OPEN**RTOS**® provides a commercial license for the FreeRTOS kernel, the highly successful, small and efficient embedded real time operating system. OPEN**RTOS**® and the FreeRTOS kernel share the same code base, however OPEN**RTOS**® 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 OPEN**RTOS**® by selecting from a wide range of middleware components and Board Support Packages.

OPEN**RTOS**® 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 OPEN**RTOS**® later when a commercial license or support is required. FreeRTOS kernel updates and ports are simultaneously released by WITTENSTEIN high integrity systems as OPEN**RTOS**®.

Professional Service
We take responsibility for ensuring OPEN**RTOS**® works with your chosen processor / compiler combination, verifiy its correct operation, and deliver 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. OPEN**RTOS**® is also supplied with one year's free support, giving you direct access to our team of highly experienced engineers.

Supporting Your Processor
OPEN**RTOS**® supports a wide number of processors, including those that FreeRTOS does not support. Our team of engineers are experienced in porting OPEN**RTOS**® 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 OPEN**RTOS**® for your specific processor.

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 three standard levels of licensing- Product, Multi Product and Corporate, but remain flexible and receptive to the needs of our customers.

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

Quality

Ensuring Excellence

A Safety Systems Company
As a safety systems company, we pride ourselves in our exceptional quality measures. In the dynamic landscape of safety-critical industries, where precision and reliability are paramount, choosing a certified provider is not just a preference; it's a necessity.

ISO 9001
As a leading safety systems company, we understand the significance of delivering products that adhere to the highest quality standards. This is why we proudly hold a ISO 9001 certification. Our commitment to ISO 9001 certification extends beyond product quality. It encompasses the core of our mission: ensuring the highest levels of safety across industries.

ISO 9001, the internationally recognized Quality Management System (QMS) standard, serves as a testament to our unwavering commitment to excellence. This certification is not just a badge; it's a guarantee that our processes, from development to delivery, are meticulously planned, monitored, and improved upon. By adhering to ISO 9001, we ensure that our RTOS solutions consistently meet or exceed customer expectations.

Certification to ISO 9001 brings a systematic approach to quality management, enhancing our ability to identify and mitigate risks effectively.

This proactive stance translates into increased product reliability, reduced errors, and enhanced safety critical factors in industries where real-time responsiveness is non-negotiable. Our commitment to ISO 9001 empowers us to continuously assess and enhance our processes, resulting in heightened efficiency and a more responsive safety critical RTOS tailored to evolving industry needs.

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 SAFE**RTOS**®.

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 SAFE**RTOS**®, our safety engineers will provide an example showing how the SAFE**RTOS**® MPU functionality could be used to isolate middleware code from other safety critical code segments. Used effectively, MPU functionality may allow mixed safety integrity levels of software to coexist within the same build of code, resulting in lower development & production costs.

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.

It's features and RAM footprint are fully scalable, making it equally applicable to smaller, lower throughput microcontrollers as to larger more powerful processors. It is available with a light weight HTTPS web server.

Support, Training & Consultancy

Benefit from our Expertise

Support
Our support team is composed of highly experienced engineers dedicated to assisting you. As part of our support offering, you will have access to the WHIS online support ticket system for a team of up to five developers. This allows client engineers to reach out to the WHIS engineering team with any queries related to 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.

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

Development Tools

In Depth Analysis

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.

- Stateviewer IDE plug-in tool;
- Offered with IAR and Eclipse tools;
- Compatible with OPEN**RTOS**® and SAFE**RTOS**®;
- Freely available for download from the WHIS website.

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.

Working with our Partners

PLS Universal Debug Engine UDE
With Universal Debug Engine (UDE®) PLS offers on top solutions for software development of systems-on-silicon.

- UDE provides debug support for 16-/32- and 64-bit microcontrollers;
- An add-on extends UDE functions for real-time and safety-critical apps;
- Designed for applications under SAFE**RTOS**® operating system.

Lauterbach TRACE32®
TRACE32® from Lauterbach offers a ready-to-run configuration for SAFE**RTOS**®.

- Supports technologies such as JTAG, SWD, NEXUS, or ETM;
- Embedded debuggers, software, and hardware trace are included;
- Logic analyzer systems are supported;
- Compatibility with over 3500 cores and CPUs;
- Encompasses 250 families, including Arm Cortex-A/-M/-R, PowerArchitecture, TriCore, RH850, MIPS, and more.

VectorCAST
VectorCAST is the fully integrated solution for critical application development.

- VectorCAST Test Automation Platform closely integrates with SAFE**RTOS**®;
- Ideal for testing and verifying applications, especially those under IEC 61508, EN 62304, and FDA 510(k) regulatory requirements;
- Supports multiple target environments and architectures;
- Utilizes the latest development methodologies;
- Enables continuous integration with change impact analysis.

email: sales@highintegritysystems.com
web: www.highintegritysystems.com

Free, Fully Functional Binary Demos

Download free SAFE**RTOS**® Demos, along with datasheets, manuals and tutorials.

Visit www.highintegritysystems.com to see what's available.

SAFE**RTOS**® Evaluations

SAFE**RTOS**® evaluation package offers engineers access to full SAFE**RTOS**® source code, an 'out of the box' SAFE**RTOS**® demonstration application and user manual. Contact us today for your evaluation.

WITTENSTEIN

high**integrity**systems

Americas +1 408 625 4712
ROTW +44 1275 395600

Headquarters
WITTENSTEIN high integrity systems
Brown's Court
Long Ashton Business Park
Bristol
BS41 9LB, UK

www.high**integrity**systems.com

LRQA CERTIFIED ISO 9001 — UKAS MANAGEMENT SYSTEMS 0001

WITTENSTEIN high integrity systems use an ISO 9001:2015 Quality Management System, certified by Lloyds Register LRQA UK applicable to:

"Design, development, and support of high integrity software covering medical, aviation automotive and industrial applications."