The Road to Safety

WITTENSTEIN high integrity systems

12/18/2024 |

What is SAFE**RTOS**®?

From WITTENSTEIN high integrity systems (WHIS)

SAFE**RTOS**® is a pre-emptive, pre-certified Real Time Operating System which is based on the FreeRTOS functional model; however it was specifically re-designed for the safety market by the WHIS team of safety experts.

SAFE**RTOS**® has been independently certified by TÜV SÜD to IEC 61508-3 SIL3 and ISO26262-6 ASIL D and is used worldwide in safety critical applications supporting a range of international safety design standards.

Industrial – IEC 61508 -1,-3,-4

Medical – FDA 510(k), IEC 62304

Automotive – ISO 26262 -2,-6,-8

Aerospace – DO178C

WITTENSTEIN high integrity systems

Who are WHIS?

A **safety systems** company, providing safety critical software all over the world from their base in Bristol, United Kingdom.

WHIS are a part of the larger WITTENSTEIN group, founded in 1949, a global corporation with a turnover of over 500 million USD that specialise in mechatronic systems.

WHIS has 25 years of experience in safety critical systems for Automotive, Aerospace, Medical, Rail and Industrial systems which sets them apart.

WHIS customers have a 100% success rate certifying SAFE**RTOS**® within their applications.

Starting with FreeRTOS

WHIS relationship with FreeRTOS

Free to Safe journey

FreeRTOS was created by Richard Barry during his time with the company, as the WHIS innovation manager in 2003 right up until 2016 when AWS took over stewardship.

WHIS now holds a strategic business alliance with AWS.

This alliance allows for the popular upgrade path, from development with FreeRTOS to final product with safety critical requirements using SAFE**RTOS**®, to be well supported.

Many WHIS customers adopt this route and find it simple and time efficient to upgrade.

FreeRTOS upgrade Resources

Migrate from FreeRTOS to SAFE**RTOS**

In less than three days

As FreeRTOS and SAFE**RTOS**® share a functional model the upgrade path is vastly simplified.

WHIS have a range of free resources to help you with this, from a written manual to a follow along video demo as well as a range of white papers for wider reading.

- Video Demo
- Technical Upgrade Manual
- White Paper

Develop using the open-source code until there is a need for a safety critical RTOS

Migrate from freeRTOS to SAFE**RTOS**® using our free resources.


SAFERTOS APPLICATION NOTE: #34-172-AN-001

UPGRADING FROM FreeRTOS TO SAFERTOS

Click to view

SAFE**RTOS**® conversion complete in less than 3 days.

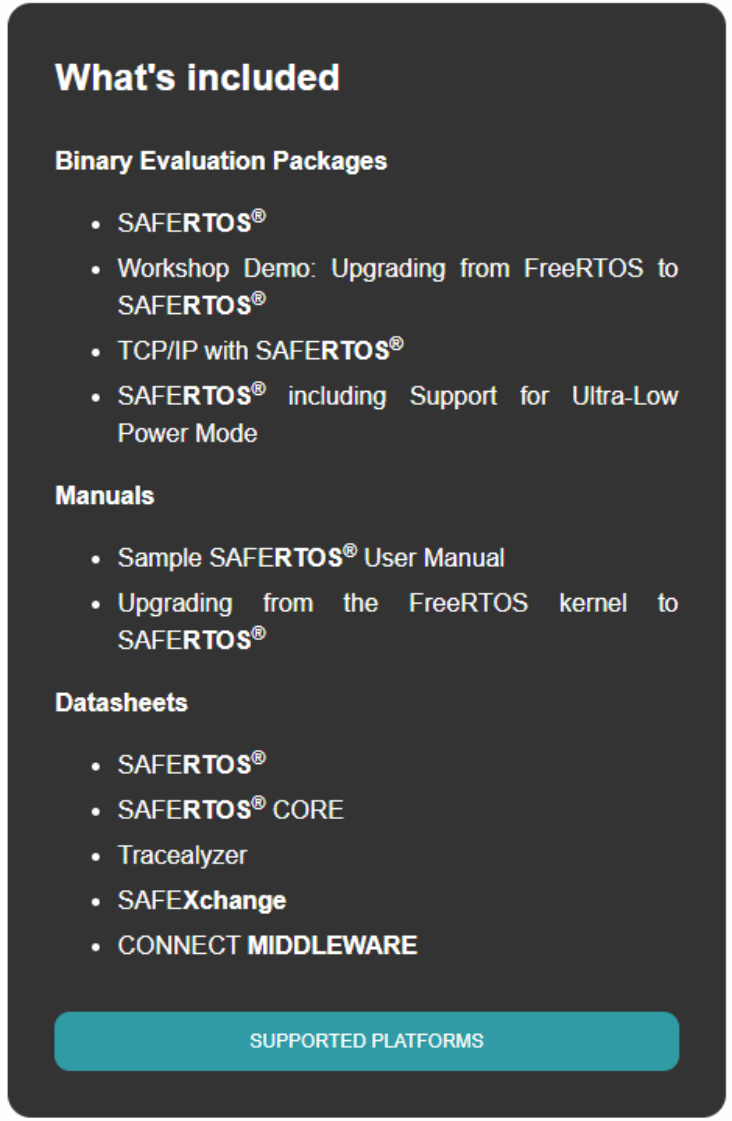
SAFE**RTOS**® Binary Evaluation Packages

Try out SAFE**RTOS**® today

- WHIS provide binary evaluation packages of SAFE**RTOS**® on their website, free to download and use for a wide range of supported platforms.
- This full featured, hands-on experience, allows engineers to become accustomed to using SAFE**RTOS** and even test out the conversion path for themselves.

If you require a demo not listed on the WHIS website please contact the team.

- SAFE**RTOS**® **full source code** 30 day evaluation packages are available on request subject to availability.



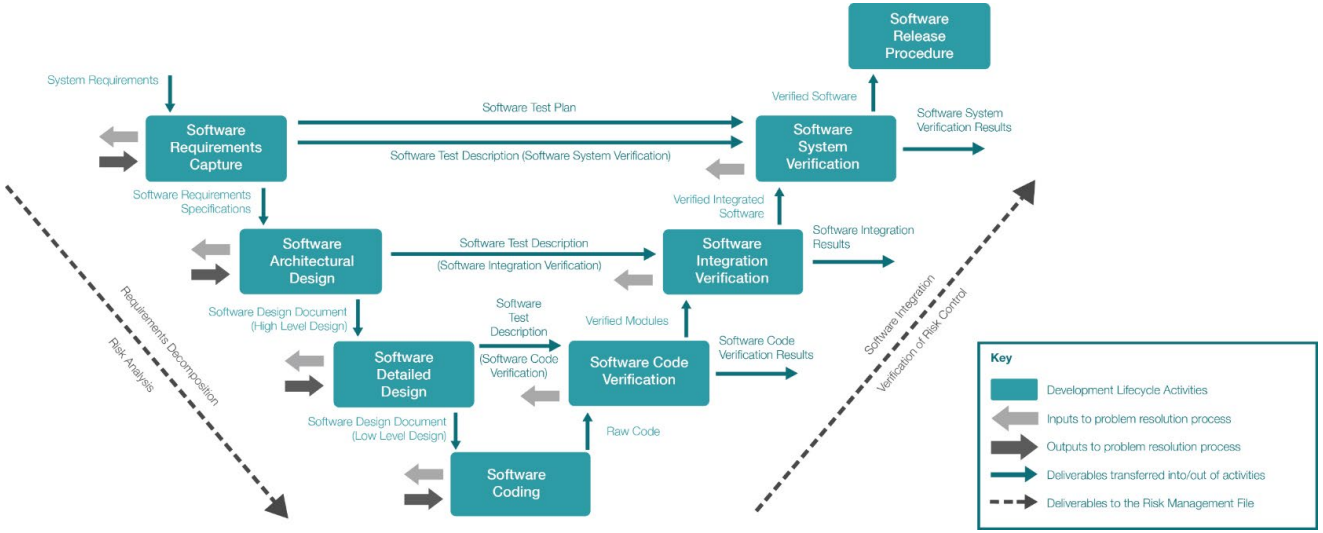
SAFE**RTOS**®

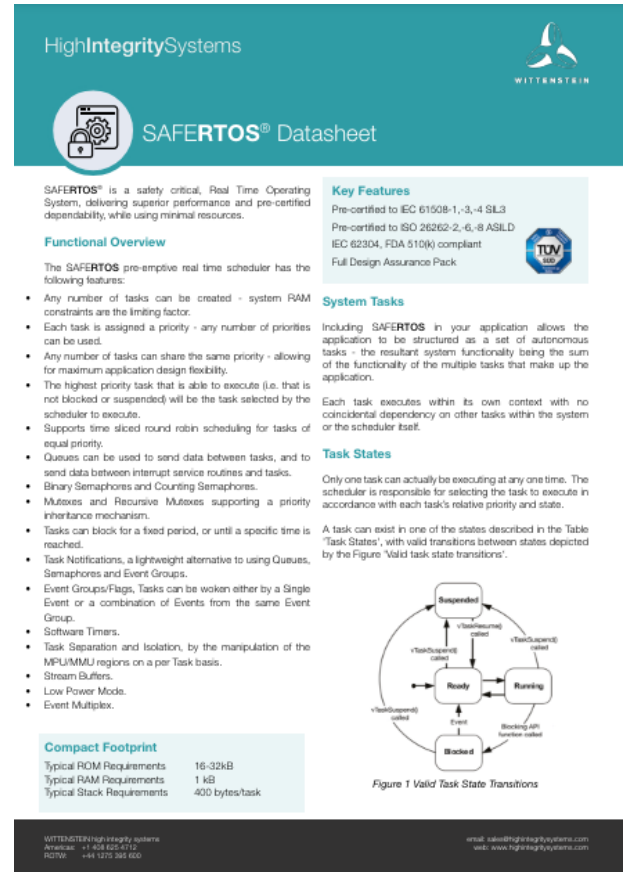
How we created SAFE**RTOS**®

The safety critical RTOS

WHIS engineers took the FreeRTOS functional model, exposed it to a full HAZOP, identified all areas of weakness within the functional model and API, and took the functional and safety requirements through an IEC 61508 SIL 3 development life cycle, the **highest possible for a software only component**.

As a result, SAFE**RTOS**® is a highly trusted RTOS used in safety critical applications ranging from **heart pumps** to integrated **cockpit systems**.




HighIntegritySystems

SAFE**RTOS**® Datasheet

SAFE**RTOS**® is a safety critical, Real Time Operating System, delivering superior performance and pre-certified dependability, while using minimal resources.

Functional Overview

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

- 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 interrupt service routines and tasks.
- Binary Semaphores and Counting Semaphores.
- Mutexes and Recursive Mutexes supporting a priority inheritance mechanism.
- Tasks can block for a fixed period, or until a specific time is reached.
- Task Notifications, a lightweight alternative to using Queues, Semaphores and Event Groups.
- Event Groups/Flags, Tasks can be woken either by a Single Event or a combination of Events from the same Event Group.
- Software Timers.
- Task Separation and Isolation, by the manipulation of the MPU/MMU regions on a per Task basis.
- Stream Buffers.
- Low Power Mode.
- Event Multiplex.

Compact Footprint

Typical ROM Requirements	16-32kB
Typical RAM Requirements	1 kB
Typical Stack Requirements	400 bytes/task

Key Features

Pre-certified to IEC 61508-1,-3,-4 SIL3

Pre-certified to ISO 26262-2,-6,-8 ASILD

IEC 62304, FDA 510(k) compliant

Full Design Assurance Pack

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 in the Table 'Task States', with valid transitions between states depicted by the Figure 'Valid task state transitions'.

Figure 1 Valid Task State Transitions

Click to view

Why use SAFE**RTOS**

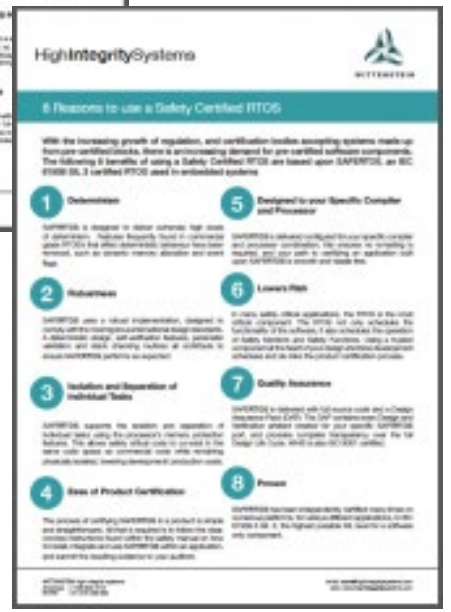
The safety critical RTOS

SAFE**RTOS**® is customized for your processor/compiler and includes full source code and a Design Assurance Pack (DAP).

The DAP offers transparency throughout the design lifecycle, ensuring high quality and:

- No need for retesting on target hardware
- Easy installation and integration
- Reduced development costs and faster time to market
- Smooth certification process

Click to view reasons to use an RTOS

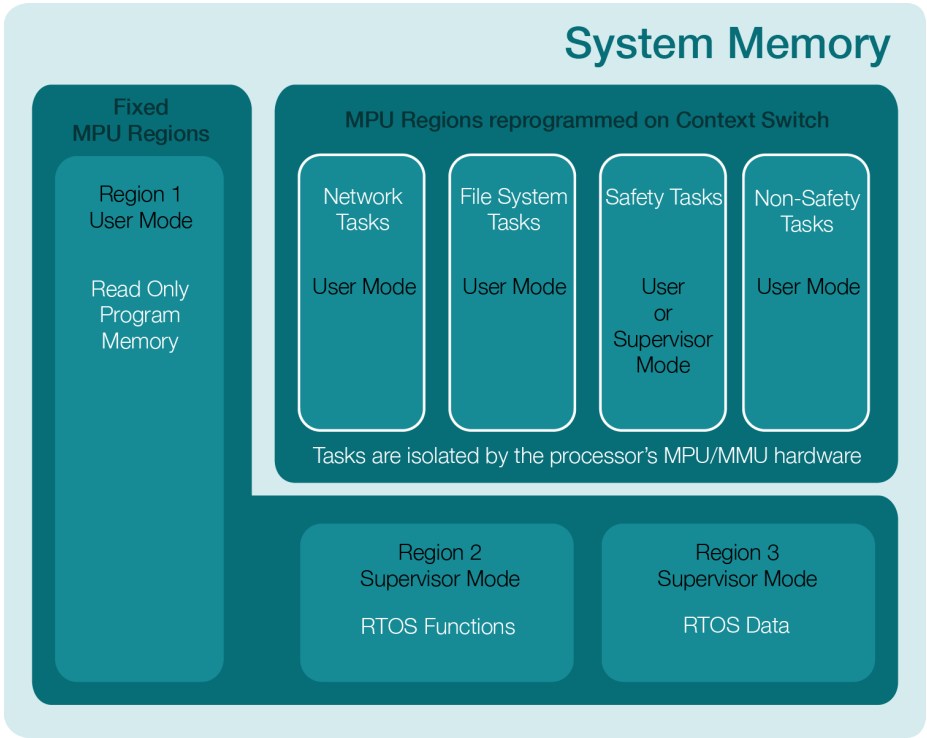


Click to view Pre-certified RTOS reasons

WHIS Licencing

Included with your licence purchase

- Full SAFE**RTOS**® source code
- SW Test harness
- Design Assurance Pack – contains the SAFE**RTOS**® certification evidence and full life-cycle information generated during development of your specific SAFE**RTOS**® variant.
- Memory Protection Unit support as standard – enables the development of spatial separation between Tasks
- Demonstrable deliverable on your selected processor / compiler combination



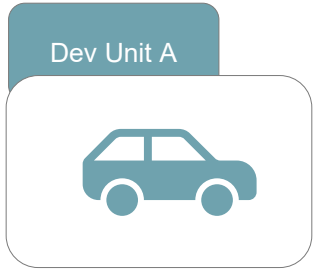
SAFE**RTOS**® and its DAP significantly shorten product development times, reduce risk, and save cost in your overall project and final system certification.

WHIS licensing model

Perpetual, full production license with no royalties, no run-time fees and no production limit

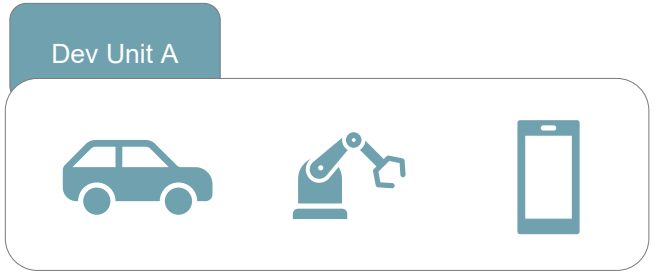
Product License

Unlimited concurrent developers from a single Development Unit, the use of the Software for one specified processor and compiler combination, for use within **one End Product and variants of the same End Product**.



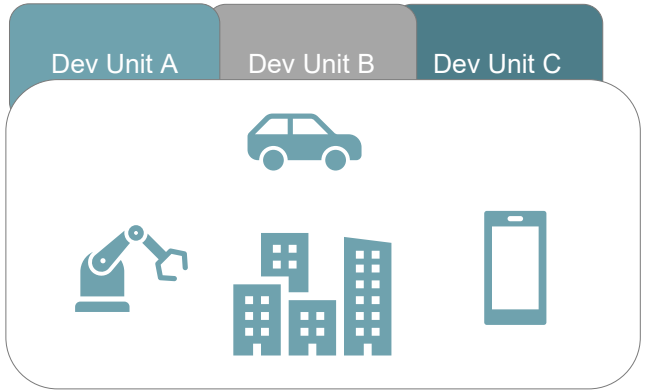
Multi Product License

Unlimited concurrent developers from a single Development Unit, the use of the software for one specified processor and compiler combination, for use within **any End Product**.



Corporate License

Unlimited concurrent developers **across the corporation**, the use of the software for one specified processor and compiler combination, for **use within any Product.**



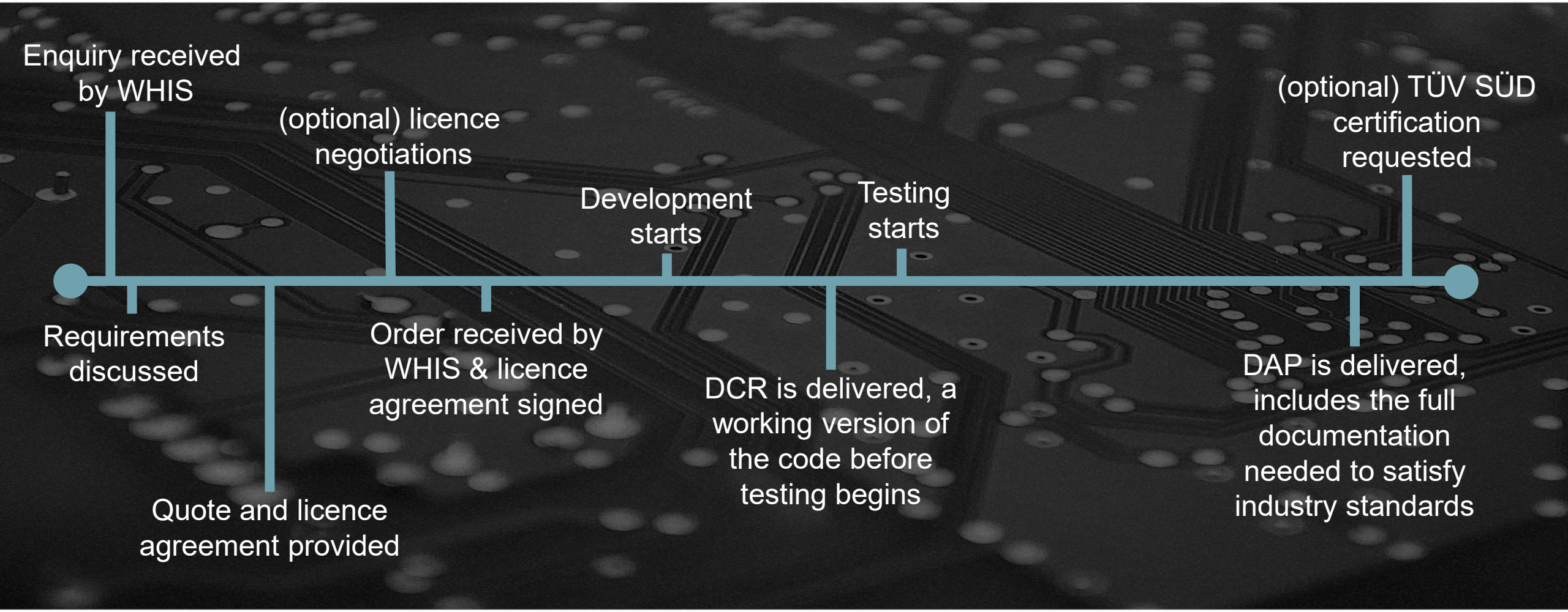
Tools/compilers

- SAFE**RTOS**® is not limited by compiler, you are able to select the best solution for your project
- With a wide range of partnerships, SAFE**RTOS**® is well supported across the industry
- SAFE**RTOS**® is able to support **both** certified and non-certified compilers
- WHIS verify the output of the compiler during testing, so we do not require the compiler to be certified
- Any other tools (debuggers, test suites, etc.) are not included in the RTOS purchase and are not limited by SAFE**RTOS**®. Most tools are SAFE**RTOS**® aware.

WHIS Purchase Process

Certification Path with SAFE**RTOS**®

The usual steps in the process, timeframes vary depending on project requirements

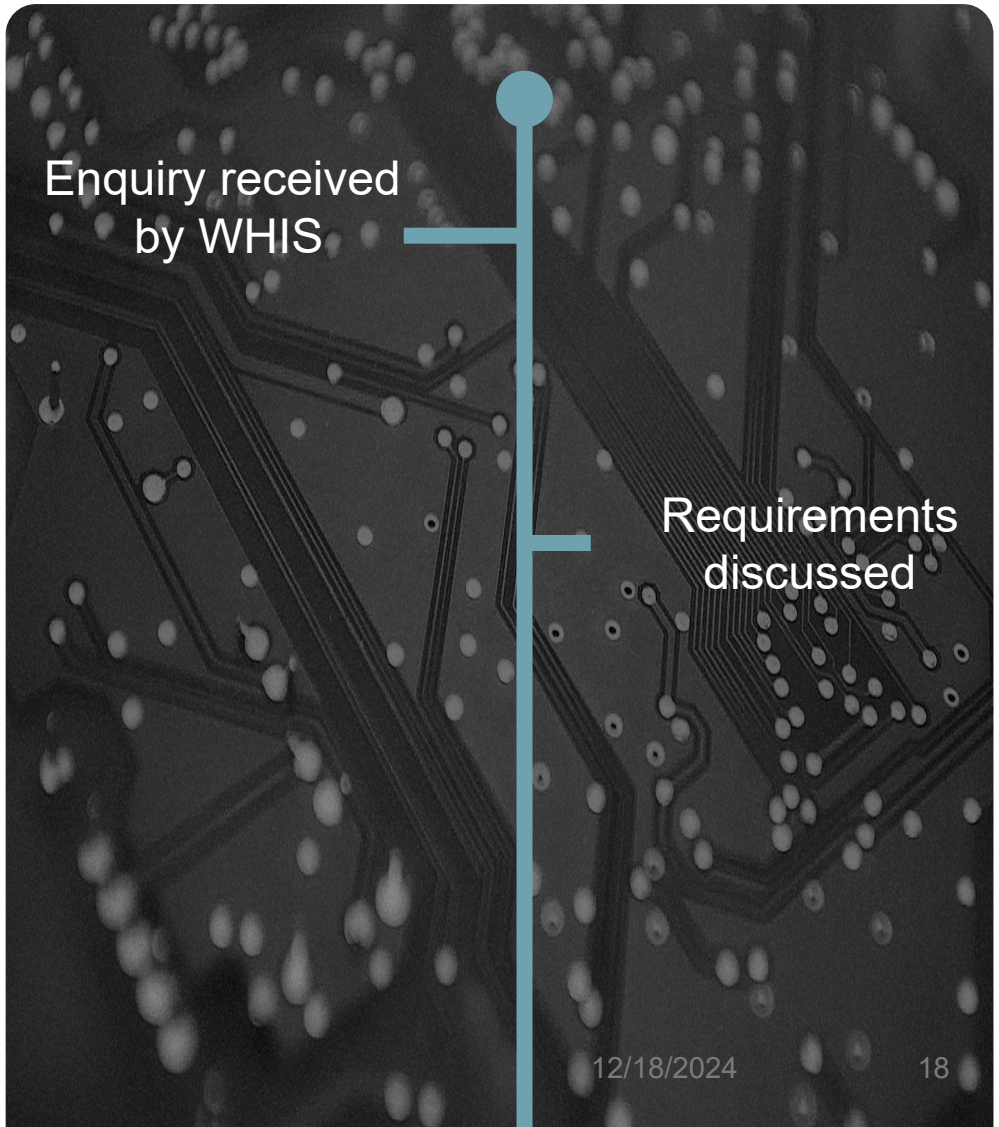


Enquiry & requirements

To ensure that the process is as smooth as possible, and to determine suitability of our product, WHIS will ask the following questions at this stage:

- Which processor and compiler have you selected?
- What kind of product are you planning to develop?
- Which license model is suitable for you?
- When are you planning to start development?
- Does your project need to be certified? If so, to which standard? (eg: ISO 26262 ASIL D)

This helps WHIS engineers and product managers to determine the scope of the work and best advise on how long the process may take. The more information provided at this stage, the better this can be estimated this for you.



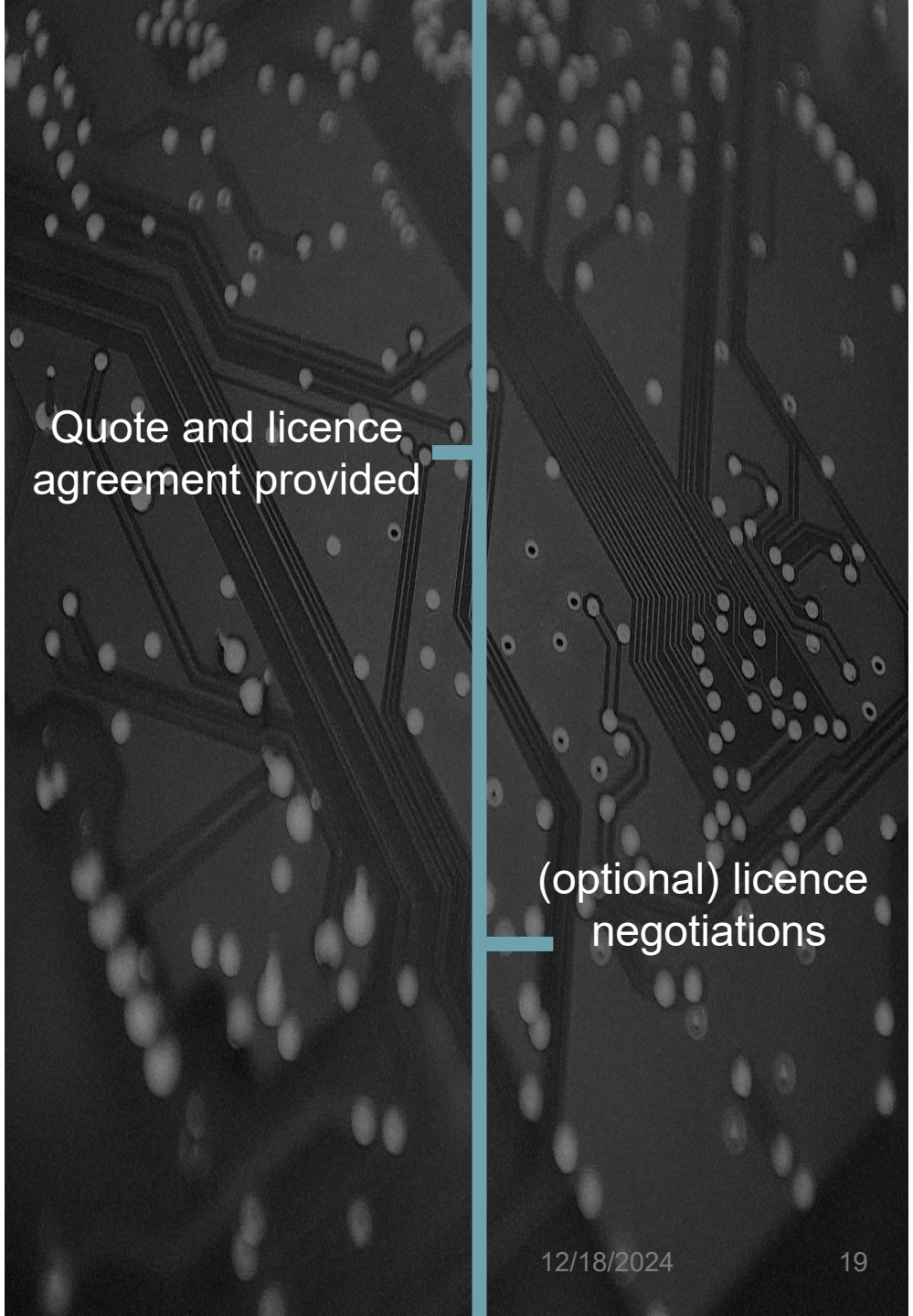
Quote & Licence

Once WHIS understands the project they can provide, in parallel, license agreements and quotations.

WHIS advise that this is the best route to receiving a purchase order in a timely manner for a smooth project start.

The following information is required:

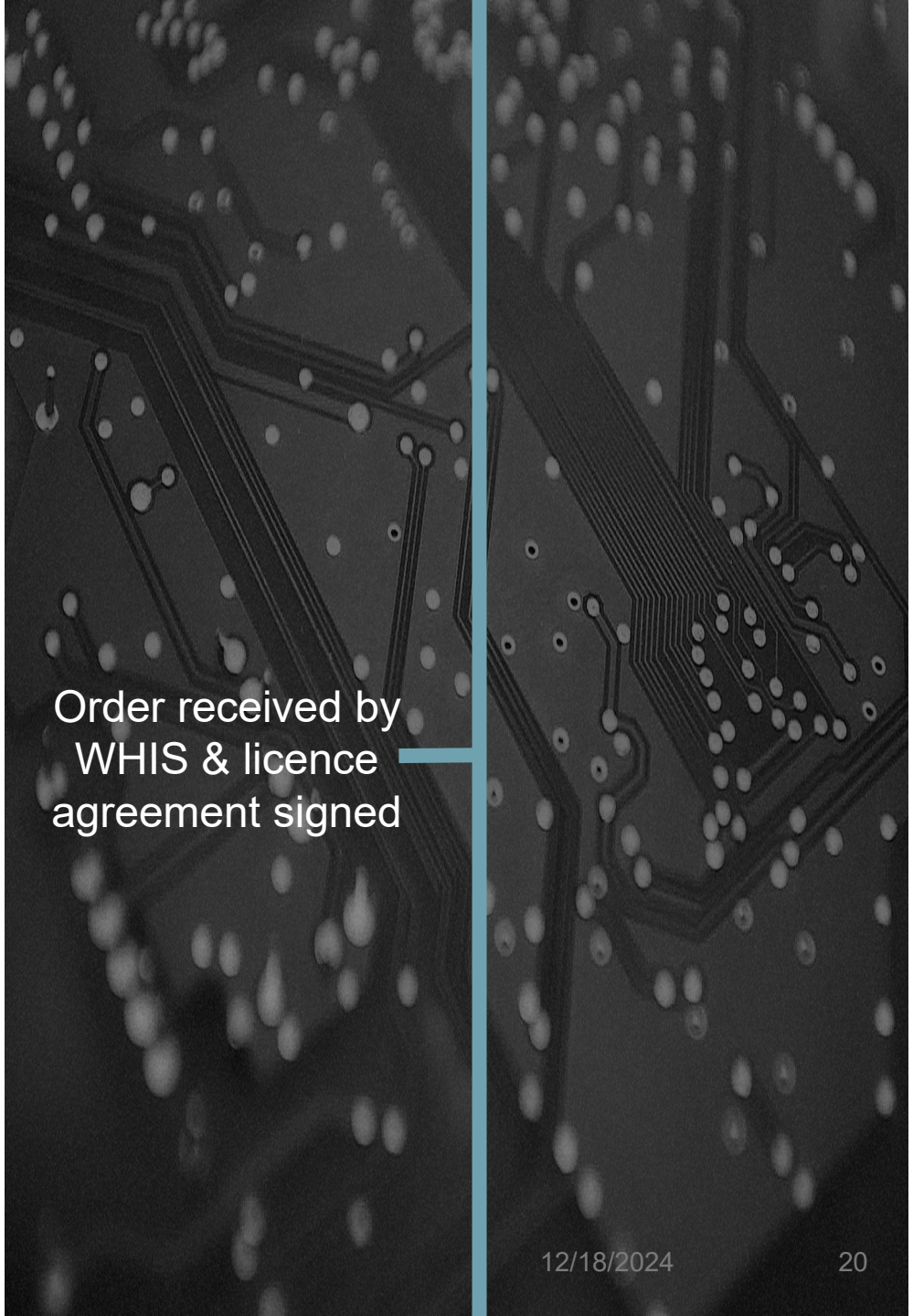
- SAFE**RTOS**® Design Assurance Pack type, depending on documentation needed for certification.
- The product name
- Your finalised Processor and Compiler combination



Quote & Licence

WHIS can only process an order once the PO and signed licence Agreement are received.

Once everything is in place, the WHIS project management team will then schedule your project.



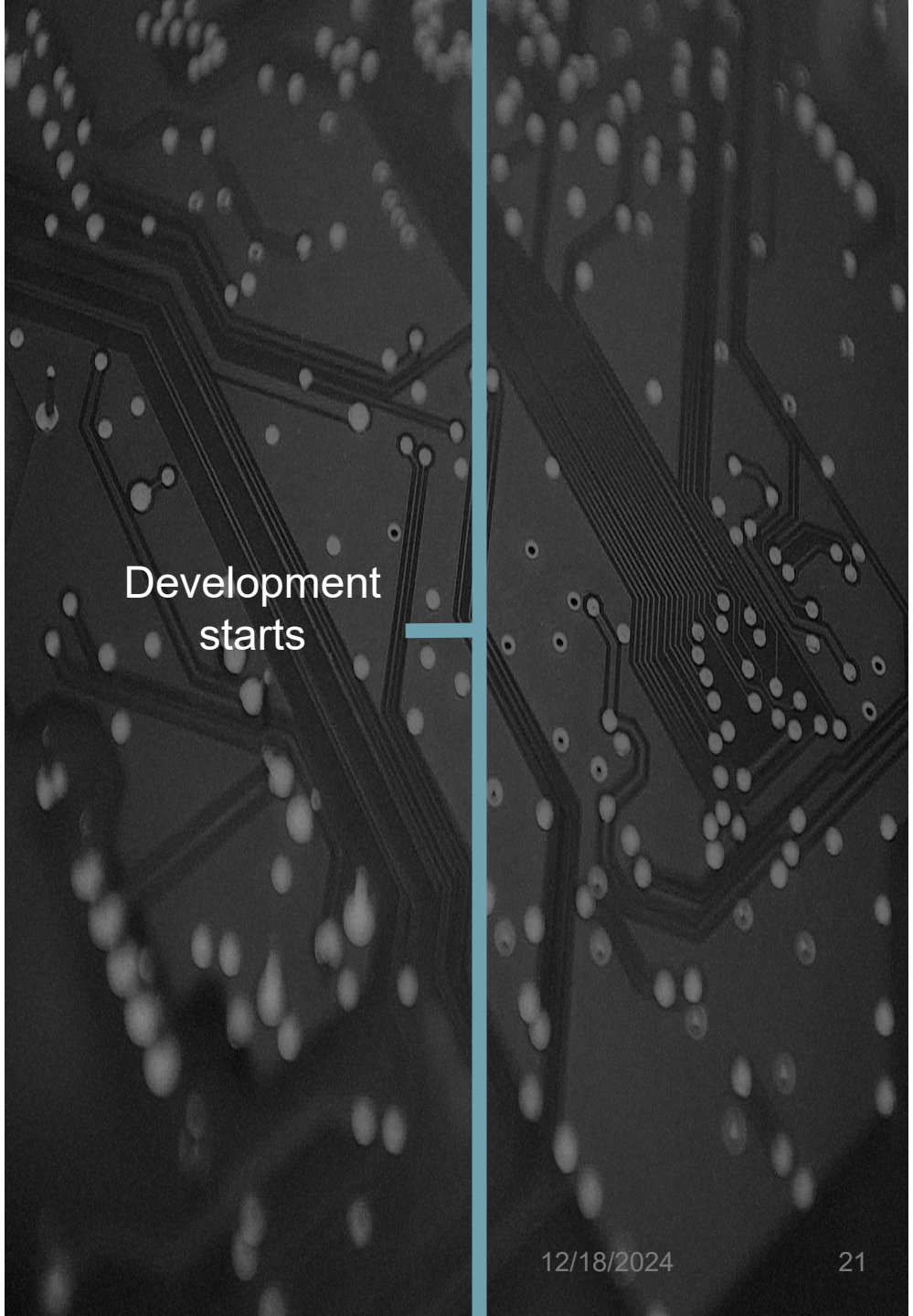
Development Starts

WHIS deliver SAFE**RTOS**® in two distinct deliveries. The first is known as the Development Code Release (DCR). This delivery is the first part of your bespoke product, and will be customised based on information you provide.

The DCR is a source code delivery, including:

- The SAFE**RTOS**® User Manual
- SAFE**RTOS**® Kernel
- Demonstration program

These are prepared for the processor and compiler combination of your choice.



Development & DCR package

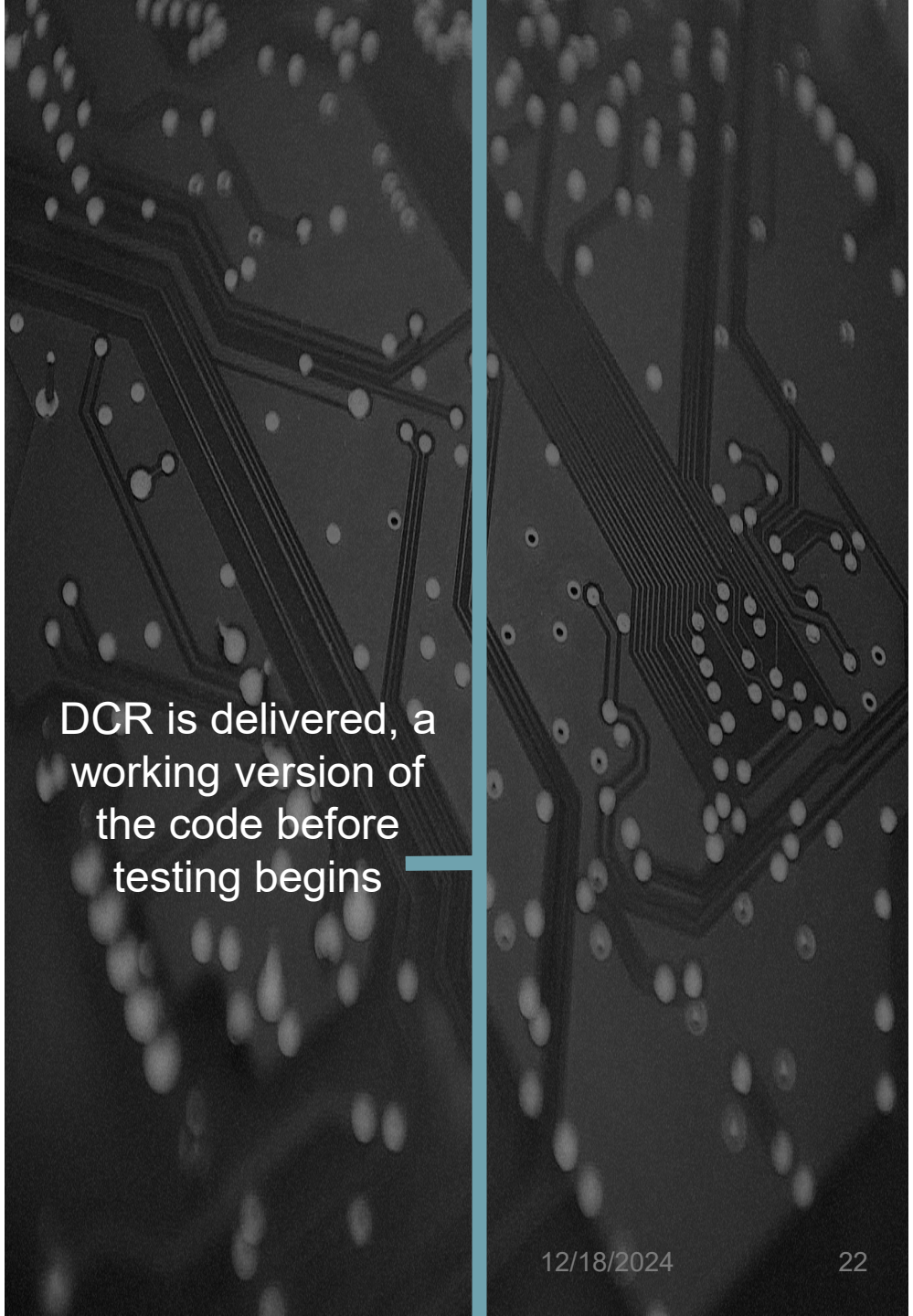
The demo application has two purposes:

- Demonstrating the functionality of the RTOS
- Providing a reference design for a host application.

The DCR code should be treated as **prototype code**. If we find any problems whilst developing and executing the test harness, then we will make the necessary changes and include these in the Design Assurance Pack delivery.

The SAFE**RTOS**® API will not change between the DCR and DAP, so there should be no significant impact on your project.

However, it is important to note that only the SAFE**RTOS**® *code from the final DAP delivery can be used in your final application.*



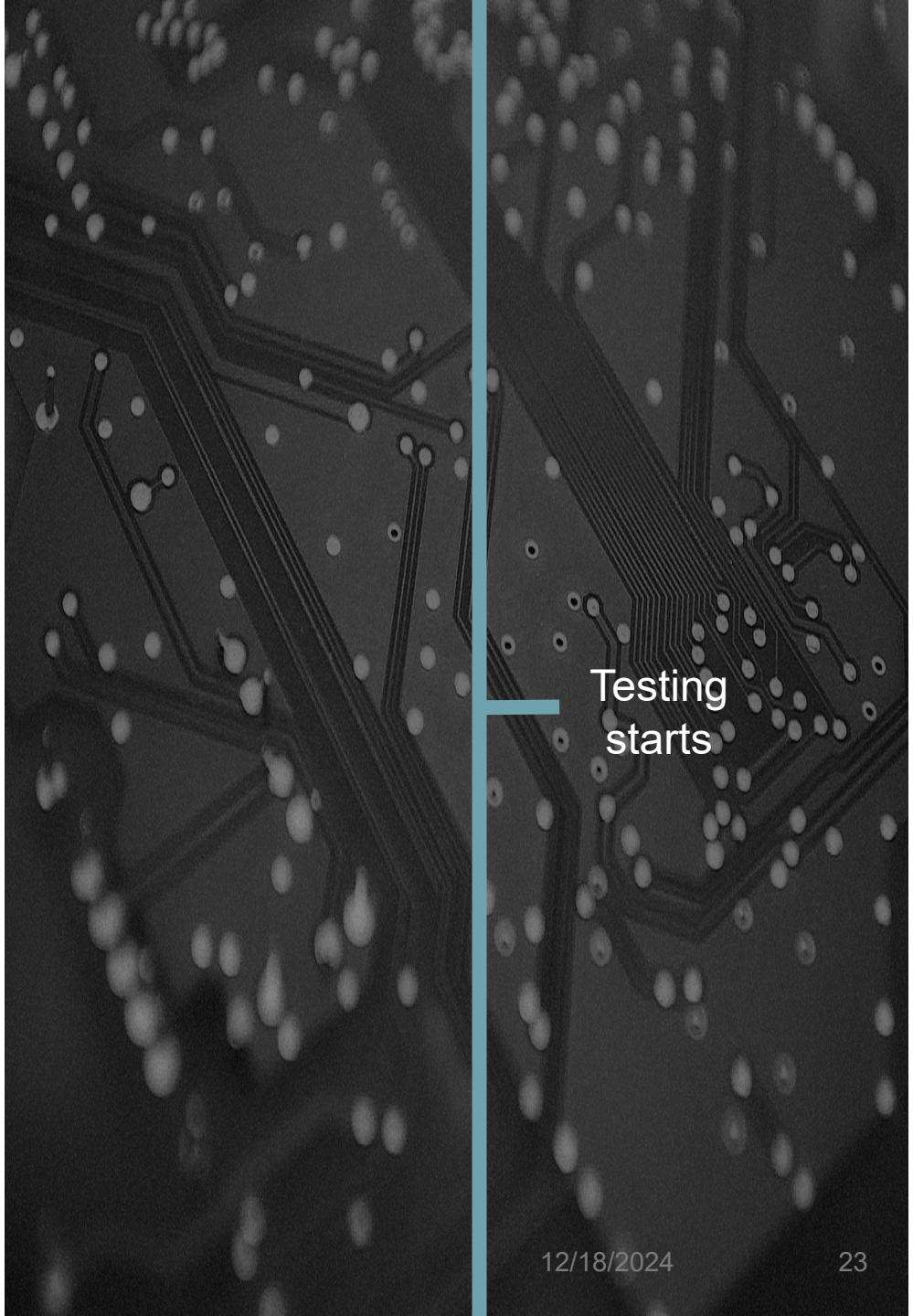
Testing

Once the DCR has been delivered, WHIS are able to commence the validation and verification of your SAFE**RTOS**® product variant.

This is where all the documentation contained in the Design Assurance Pack (DAP) is produced. **The fully validated code included with the DAP Deliverable is the final code release.**

To allow WHIS to carry out the validation correctly the specific device and compiler settings that you are using are needed. WHIS will ask you the following:

- The version of the compiler being used.
- Whether you are using any optimisation or any other settings that would affect the output of the compiler.
- The specific device (full processor designation) we should use to carry out the validation



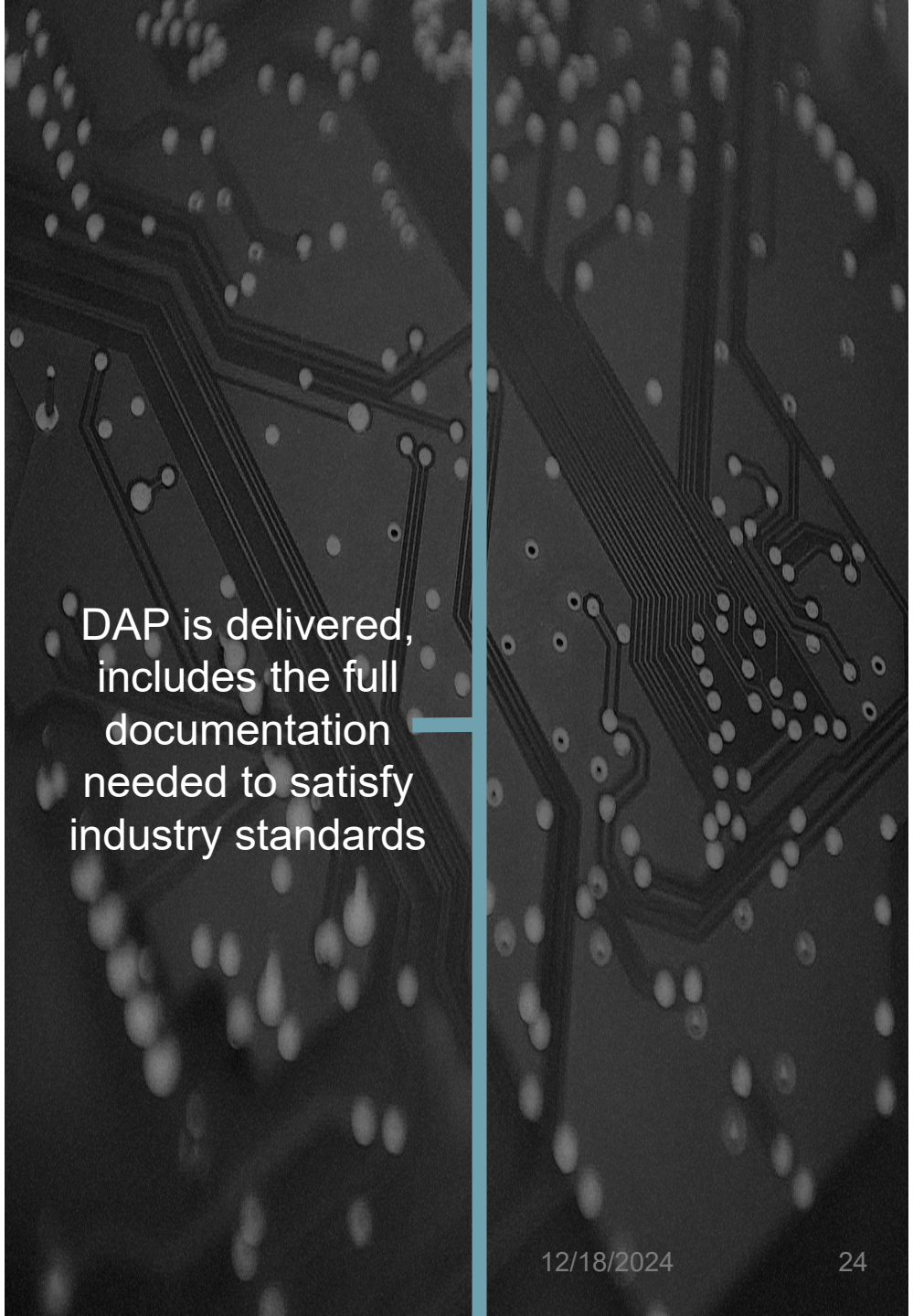
DAP & Certification

Within the DAP/DHF WHIS include all the requirements (Customer, Software, Architectural Design and Detailed Design) that are used when creating a SAFE**RTOS**® product variant.

The Software Test Description documents detail the tests that WHIS perform to verify that all requirements have been satisfied. The test harness is the implementation of those tests and the results of these tests are also included in the DAP (DHF for medical projects).

- There is no need to verify the operation of SAFE**RTOS**® – you just need to prove that you are using SAFE**RTOS**® correctly.
- The DAP/DHF includes a Safety Manual which contains a checklist of items that the application must comply with.
- You need to demonstrate to the certification body that you have considered all the items on this checklist.

You are responsible for the verification and validation of your application



TÜV SÜD Certification

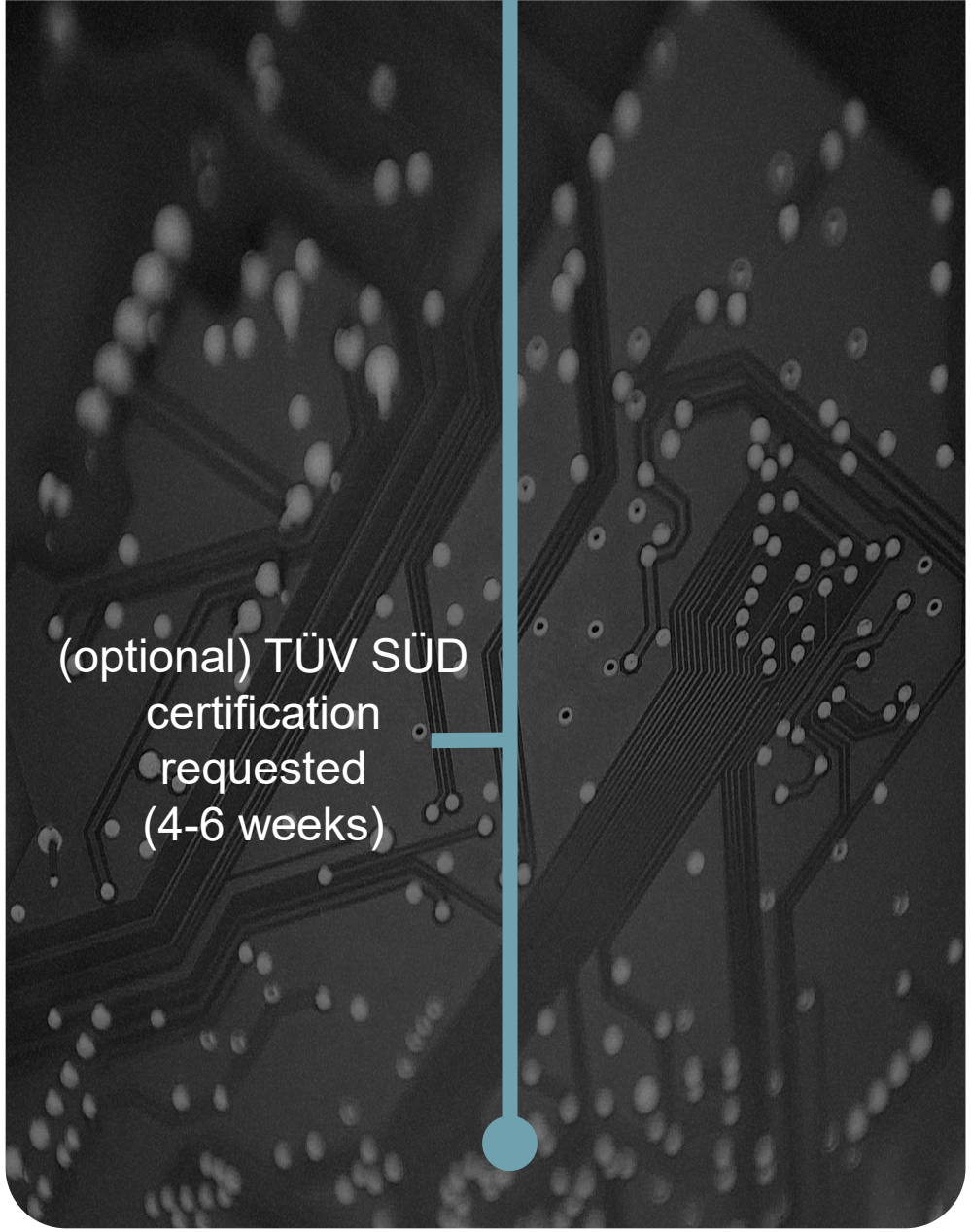
A SAFE**RTOS**® product variant is defined by its full processor designation, the specific compiler version and the compiler configuration settings.

SAFE**RTOS**® is pre-certified.

It was originally certified to IEC 61508 SIL 3 by TÜV SÜD in 2007, and to ISO 26262 ASIL D in 2017.

WHIS submit SAFE**RTOS**® product variants to be independently certified by TÜV SÜD on a regular basis in order to receive continuing confirmation that development life cycles and products remain consistent with the above safety standards.

If you require independent TÜV SÜD certification for your specific SAFE**RTOS**® product variant this can be quoted for on request.



WHIS Support & Maintenance

Support & Maintenance

- Each purchase of SAFE**RTOS**® includes **12 months free** support & maintenance as standard.
- WHIS understand the need for easy access to engineers in that initial year. You will be able to ask questions on a wide range of topics regarding your RTOS purchase from Safety and certification to technical details.
- Support is provided via our online helpdesk.
- You will have access to the engineers that directly worked on your project, allowing for optimal responses to your questions.

HighIntegritySystems

WITTENSTEIN

SAFERTOS® Support and Maintenance

WITTENSTEIN high integrity systems' (WHIS) expert engineers are dedicated to providing high quality support.

Every SAFERTOS® purchase is supplied with 12 months free Support and Maintenance.

With a valid Support and Maintenance agreement, you can rely on WHIS engineers to swiftly address any RTOS-related enquiries and provide guidance whenever it is needed, ensuring a seamless experience throughout.

Support is provided by the WHIS engineering team, usually by engineers that have worked on the development of the software directly. This provides the best possible support, as help is received from those already familiar with the project.

WHIS engineers are passionate about sharing their engineering experiences and take great pride in providing a responsive, friendly and helpful service.

SAFERTOS® Technical Support

SAFERTOS® technical support includes access to the WHIS online support ticket system for up to 5 developers (up to 10 developers for a Corporate License).

- Responsive, online support;
- Direct contact with highly experienced engineers;
- Cost efficient licence upgrades.

Safety Support

For our safety related products, support also covers safety and certification activities. This ensures developers using our products always have access to a WHIS employee who can provide support on all aspects of our products, including Technical, Safety and Certification questions. Upon request, TÜV SÜD certification can be quoted.

License Upgrades

A significant benefit of a Support and Maintenance agreement is the ability to increase the scope of a purchased license while only paying the difference between the current license held and the cost of a wider scope license. For example, upgrading from a Product License to a Multi Product Licence would only cost the delta between the licence prices.

Responsive Support & Maintenance

Initial 12 months free of charge;
Access to experienced engineers;
Discounted license upgrades;
Technical/Safety/Certification support.

This allows you to start small, enjoy the benefits that WHIS offers, and cost efficiently upgrade to a larger scope license when needed. View licenses

SAFERTOS® Re-validation

Re-validation of the purchased software can be requested every year that the Support and Maintenance contract is renewed, from the second year onwards. This includes re-issue of documentation and is accessible under the condition that the processor remains unchanged and the compiler is an updated version of the original.

Errata Notices and Maintenance Releases

Having an active Support and Maintenance agreement provides access to any Errata notices and maintenance releases relating to your licensed software. At the end of a Support and Maintenance period, you will also receive a summary of any Errata notices raised during the time the agreement was active. Errata notices form extensions to the Safety Manual.

License Administration

Change of addresses, contact details and License amendments can all be made without charge.

Support After the Initial 12 Month Period

After the initial 12 months, Support and Maintenance can be purchased in consecutive 12 month blocks. There is no obligation to take out a Support and Maintenance agreement. However, if you wish to continue to benefit from the advantages of the support agreement, please contact a WHIS sales consultant to receive a quotation.

WITTENSTEIN high integrity systems
Americas: +1 408 625 4712
ROTW: +44 1275 395 600
email: sales@highintegritysystems.com
web: www.highintegritysystems.com

Click to view

Contact details

+44 1275 395 600

Brown’s Court, Long Ashton Business Park
Yanley Lane, Long Ashton, Bristol, BS41 9LB, UK

sales@wittenstein.co.uk

www.highintegritysystems.com