



The Flexible Safety RTOS

The Flexible Safety RTOS, called „Cert-Kit“, is a pre-certified real-time kernel for usage in functional safety projects. With a flexible approach in component software design and in certification architecture, you are flexible in many topics where others must regulate the usage more restrictive. This includes:

✓ Flexible Compiler Switches

Adjust compiler switches to your project needs without additional effort or cost.

The pre-certification has been performed with an independent assessor for several cores and all major compilers.

There is no dependency from specific device peripherals to the certified part of the RTOS.

✓ Flexible Device Selection

Change the used microcontroller to a different device with the same core during project without losing the safety capability of the RTOS.

The Flexible Safety RTOS is certified for the main standards in industrial automation, automotive, medical and transportation.

✓ Select Your Certificate

Get the needed certificate for your project. We provide certificates for IEC 61508, ISO 26262, IEC 62304 and EN 50128.

Flexible Safety RTOS

Scope of Delivery

Pre-Certified Source Code

- Real-Time Kernel
- Processor-Core Dependent Port

Manuals

- Safety Manual
- Target Integration Manual
- Reference and User Manuals

Additional Source Code

- Validation Test Software
- Reference Board Support Package

Certificate

Technical Data

Assessment Bodies:

- TÜV Rheinland
- TÜV Süd

<i>Safety Standard</i>	<i>Safety Capability</i>
IEC 61508 2 nd Ed.	SIL 3
ISO 26262	ASIL D
IEC 62304	Class C
EN 50128	SIL 4

Services in Maintenance

- Regular Maintenance-Reports
- Support by Email



Using a Pre-Certified Component

When using a pre-certified component in your safety product development, you get a document from the component vendor, called "Safety-Manual".

This document specifies the rules, which must be adhered to keep the safety capability and the certificate valid. Within your safety-critical product certification, the only action your team must perform is: show that all these rules are observed.

Safety Manual

When comparing pre-certified software components, it is essential to compare the corresponding Safety Manuals.

Board Support Package

The term "Board Support Package" (BSP) is widely used – with a lot of different meanings. In general, the BSP focus the integration of a software component to the specific hardware and/or microcontroller board.

This is a software part, which is by its nature highly dependent on the project requirements. Due to this fact, Embedded Office delivers a BSP with all essential features, needed for a RTOS as a reference implementation.

The Board Support Package in your project must be developed following the same quality rules as you do for the application.

Safety BSP

Embedded Office offers a BSP, which can be adapted and configured to your project's needs. The certification of the resulting BSP is supported by Embedded Office.

If you already have a BSP, or want to use a 3rd party component, this is possible and supported by Embedded Office as well. We assist you to integrate the RTOS in your BSP.

Validation Test Software

We simplify the usage of the Cert-Kit as far as possible. For this reason, the Cert-Kit contains a "Validation Test Software". This software checks the integration of the Cert-Kit to your selected or adapted BSP, running on your custom hardware board and checks by the way some of the rules out of the Safety Manual.

Validation Test Software

You get an automatic test suite, which checks the integrated RTOS on your project hardware with the selected BSP.

Features of the Cert-Kit

The Flexible Safety RTOS is a complete real-time kernel, based on the market leading Micrium μ C/OS. The kernel is extended with some safety functionality, which helps your team designing the application for your safety-critical products.

The kernel API is compatible to the standard kernel version (μ C/OS-II) which allows the move from standard kernel to the Flexible Safety RTOS with minimum effort.

Easy Move to Safety

Separation of one or more tasks in process memory spaces. Full API compatibility to μ C/OS simplifies the step into Safety.

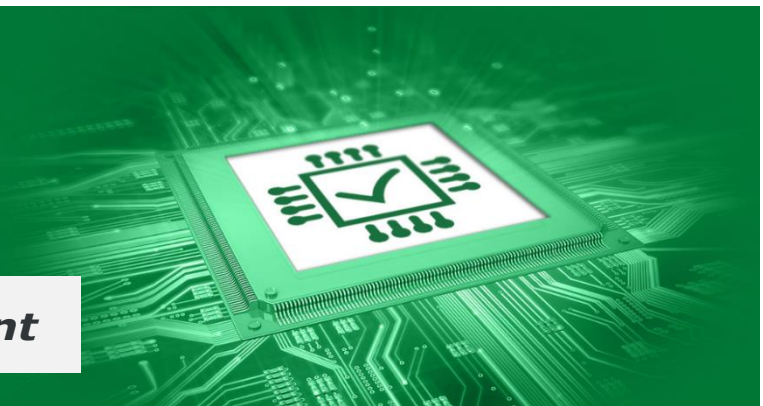
The space protection extension allows the separation of software parts running on a single core. This enables the usage of unchanged 3rd party components within the safety-critical devices.

Managed Memory Protection

The Flexible Safety RTOS removes the burden of memory management from your development team. We keep the usage simple and efficient.



Safety Critical Development



We need to follow a development process to avoid systematic faults and achieve the required quality for safety products. In all phases your project can benefit from the experience of the Embedded Office team.

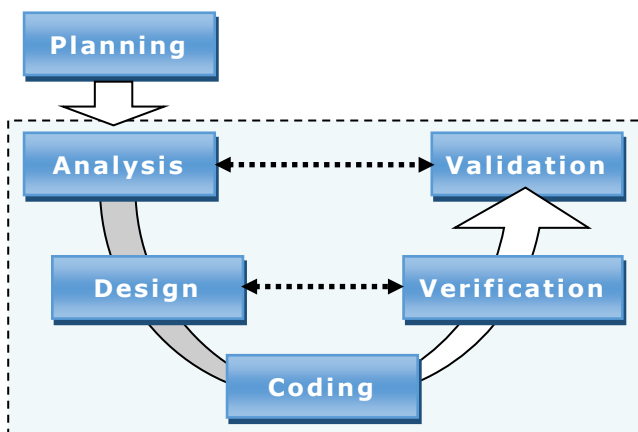
Planning Phase

The planning phase of the safety-critical product belongs to the development process itself.

✓ Safety Mentoring

Embedded Office assist you in defining and establishing a cost efficient and proven development process.

In this phase, the usage of pre-certified components must be considered.



✓ Functional Safety Management

We can take over the functional safety management for your system while you establish your new process.

Analysis Phase

Architectural decisions and calculations of random hardware faults dominate the analysis.

✓ Requirements Engineering

Embedded Office supports your team with functional safety experts in analyzing and writing the specification.

In case your safety product will connect to the cloud, we should analyze the possible attack scenarios in this phase as well.

✓ Security Attack Analysis

With a security team, Embedded Office can help you to identify the potential attack scenarios for your connected device.

Design Phase

While your team is designing your safety product, the experience in designing a system, using a RTOS is essential for a solid and efficient application software.

✓ System Design

Embedded Office offers training and assistance for designing your system with or without a RTOS.

With individual project workshops and optional design reviews we help to reduce the risks of technical issues.



Software Components



Re-Usable Software Components

The design phase decisions are essential for your product Time-to-Market. We don't accept any compromise in features of the used components. For this reason, Embedded Office is working with any software, which matches your project requirements.

We provide high-quality products from market leading partners and use them as a well-known starting point to realize your vision:

✓ Real-Time Operation System

Micrium μ C/OS - with all the bundled components are well known. We use and sell them for more than 12 years.

We work in many customer projects with a lot of different RTOS as well. You can use this knowledge to find the best matching RTOS for your project.

✓ Secure Hypervisor

LynxSecure - provides a high secure environment for running applications in one or more separated security domains.

We see fast rising demands on security requirements since the last 5 years. For your connected project we provide knowledge for scenarios where a hypervisor is a good solution.

✓ CANopen Stack

Flexible and modern design allows your team to integrate this stack fast and efficient.

Coding

In case we can't find a matching component for your requirements, we can change and adapt any existing software to your needs – or write a new one for your product.

✓ Safety Components

Embedded Office offers the pre-certification of reusable customer specific software components.

Verification & Validation

Traceability and Verification activities are mostly based on development tools.

✓ Certified Testing Experts

Strengthen your team with certified test experts from Embedded Office.

After testing many customer projects and the Flexible Safety RTOS, our experts know how to use the testing tools efficiently – or write specialized testing frameworks where the existing tools can't help.

Contact

Embedded Office GmbH & Co. KG
Friedrich-Ebert-Str. 20/1
D-88239 Wangen

Web: www.embedded-office.com
Mail: sales@embedded-office.de
Tel: +49 (0)7522 / 97 00 08-0