SYSGO
EMBEDDING INNOVATIONS

PikeOS
EN 50128 Certification Kit

The Certified Safe and Secure
Hard Real-Time Hypervisor

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD

CERTIFICATE

No. Z10 13 10 79750 003

Holder of Certificate: SYSGO AG
Am Pfaffenstein 14
55270 Klein-Winternheim
GERMANY

Factory(ies): 79750

Certification Mark:

Product: Software, Operating Systems
Real Time Operating Systems

Model(s): PikeOS 3.4

Parameters: The operating system is qualified up to SIL 4 according to EN 50128.

The assessment report SK85271G of TÜV SÜD Rail GmbH and the Safety Case 00101-0105 of SYSGO AG are mandatory parts of this certificate.

Tested according to: EN 50128:2011 (SIL 4)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: SK85271G

Date, 2013-10-21

(Günter Greil)

365301

Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstrasse 65 · 80339 München · Germany

TÜV®

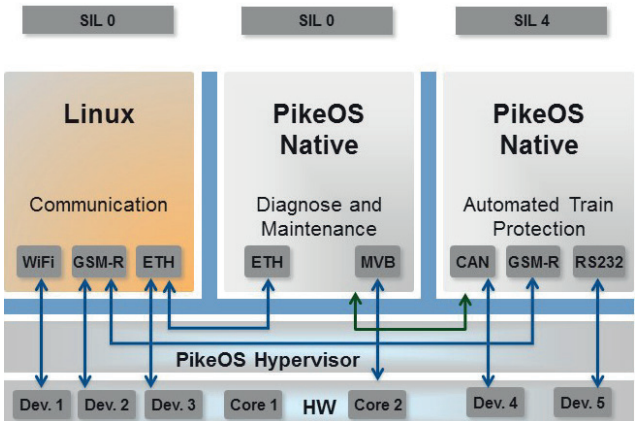
A1 / 03.08

PikeOS is the ideal platform for safe transportation applications requiring EN50128 certification. Projects benefit from the fact, that PikeOS has achieved an EN50128 SIL4 certification on a multicore platform.

Introduction

PikeOS combines a real-time safety operating system and a virtualization platform for embedded systems in one architecture. The safety concept of the PikeOS Real-Time Hypervisor is based on safe and secure separation of mixed critical applications.

The PikeOS Certification Kit (CertKit) provides all necessary artifact to prove the compliance of PikeOS to all objectives of the EN50128 safety standard. By using the PikeOS CertKit, SYSGO customers can focus on the certification of their application(s).



A PikeOS Board Support Package (BSP) implements software support for the customers hardware and will require its own certification artifacts. SYSGO has the in-house expertise and tools to develop and certify PikeOS BSPs for custom BSPs. If SYSGO customers want to develop their own BSP, the PikeOS/BSP Validation Kit provides the tooling to re-run a subset of the PikeOS test-suites together with the customers BSP to validate the correct coexistence of both components.

PikeOS Certification Kit (CertKit) contents

The CertKit offering includes the following documents:

- The Certificate for the specified PikeOS version for the applicable hardware architecture(e.g. TUEV certification report)
- The Safety Case for the generic PikeOS components and for the custom Board Support Package. The Safety Case describes the processes performed and the documentation generated by SYSGO during the software lifecycle
- Validation Report, showing completeness of the development, verification and validation activities
- The Safety Manual for PikeOS and an add. Safety Manual for the specific processor architecture. The Safety Manual describes the safety requirements and the usage domain restrictions for using PikeOS to build a safe system.
- Certification Kit User Manual which describes the usage and installation of PikeOS in an certifiable environment
- The Interface Specifications required for application development, BSP development and module configuration

PikeOS/BSP Validation Kit

The integration of a custom BSP with PikeOS requires a re-run of a sub-set of the PikeOS test suites. If SYSGO customers develop their own BSP, SYSGO provides a self-contained (i.e. independent from customer infrastructure) subset of the PikeOS Test Suites as part of a PikeOS/BSP Validation Kit. The content is project specific and will include a customized version of:

- The SYSGO Test Framework (TFW)
- Test-Suite for Timing Analysis and Worst Case Execution Time(WCET) Analysis
- Test-Suite for PikeOS validation
- The Test Framework (TFW) is a stand-alone software package, which provides a framework to execute test cases on the customer target hardware. After finishing all tests, special tools provided by the Test Framework create a test case result document.

SYSGO EN50128 Certification Process

PikeOS has been developed using software development, verification & validation processes and procedures beside quality management and safety-related processes and procedures mandated in the EN50128. These processes include requirements traceability, design control and intensive testing, verification and validation. The resulting documentation and records (certification artifacts) form the basis of the PikeOS EN50128 CertKit for railway applications.

PikeOS is designed as a generic software component (defined in EN 50128:2011 chapter 7) so that it can be used for a variety of installations purely by the provision of application-specific configuration data and algorithms. PikeOS is usable in systems with safety integrity requirements up to EN50128 SIL 4.

Additionally to the compliance to EN50128, SYSGO provides additional documentation for PikeOS (e.g. Safety Plan, Safety Case) to support the integration of PikeOS into the customer specific hardware certification strategy. These documents are compliant to EN50126 and EN50129 requirements.

The following list is a high level summary of the certification artifacts generated by SYSGO and required for the EN50128 certification of PikeOS:

- Planning documentation
- SW Development Standards
- Software Requirements documentation
- Architecture and Design documentation

- Component Design, Module Design, Implementation and Testing documentation
- Software Integration documentation
- Overall Software Testing and final validation documentation (including SW Structural Coverage Reports (e.g. MC/DC coverage).
- The Tool qualification reports for the tools used within the PikeOS development which need qualification
- The Stack Analysis, WCET/Timing Analysis and Partitioning Analysis reports for PikeOS
- Software Deployment documentation
- Software Assessment documentation (e.g. TUEV certification report)

The Master Document List (MDL) for the overall certification process references detailed documentation, which SYSGO is able to present to the certification authority or notified bodies in order to obtain the PikeOS certification. The PikeOS CertKit includes a subset of this documentation, but if required, the complete documentation is available for reviews and audits by SYSGO customers.

PikeOS Source Code Inspection

Source code inspection is typically not required for a certification in regards to EN50128. Therefore source code is not automatically included in the PikeOS CertKit, but always available separately. Depending on the customers' requirements, PikeOS source code can be licensed as read-only, build and read/write license. If requested, a source code inspection can be agreed for reviews and audits by SYSGO customers or the certification authority / notified bodies.

SYSGO Certification Services

The PikeOS CertKit is complemented with a certification services package. The main objective of this certification service is to establish communication and understanding between SYSGO, the customer and the certification authorities regarding the certification aspects throughout the software life cycle and to assist the customer in the certification process.

The coordination with the certification authorities / notified bodies is typically managed by the customer. SYSGO has a direct interface to notified bodies (e.g. TUEV) to manage certification procedures. SYSGO may be required to attend to the reviews and meetings on the customer's application with the certification authorities and provide detailed information about the developed products upon request.

SYSGO Certification Support and Maintenance

In compliance with the EN50128 safety standard, SYSGO and the customer have to establish, document and maintain procedures for problem reporting and corrective actions. These procedures especially cover the following aspects:

- Define the documentation needed for problem reporting and/or corrective actions, with the aim of giving feedback to the responsible management
- Define analysis of the information collected in the problem reports to identify its causes
- Define the practices to be followed for reporting, tracking and resolving problems identified both during the development phase and during software maintenance

The PikeOS CertKit support contract enables SYSGO customers to have an effective implementation of this regulatory. A valid support contract includes SYSGO's commitment to maintain:

- The certified PikeOS version as well as corresponding certifications artifacts purchased by the customer
- The certification knowledge of the related certification standard and of the particular version of PikeOS used by the customer
- All tools used for the certification of the PikeOS version (i.e. development and test tools)

The SYSGO Safety Board analyses and communicates safety-related problem reports within Safety Bulletins regularly to SYSGO customers under a valid support and maintenance contract. Safety Bulletins are generated on a quarterly basis for all certification related projects.

Certified PikeOS Add-Ons / Optional Components

- PikeOS and its middleware components were certified according to various industry standards (e.g. EN50128, EN61508 and DO-178B). Certification artifacts are available for the following PikeOS components:

PikeOS Native Personality:

- The PikeOS Native personality provides a direct API for PikeOS.

PikeOS POSIX Personality:

- The PikeOS POSIX personality provides a PSE51 and PSE52 conformant API for PikeOS.

Certifiable File System (CFS):

- The CFS add-on provides a compact and robust file system running on top of a POSIX Personality or PikeOS Native Personality.CFS guarantees data integrity under any conditions, such as power failures.

Certifiable IP Stack (CIP):

- The CIP add-on provides a UDP/IP stack implemented for POSIX and PikeOS Native API.

SYSGO Headquarters
Phone +49 6136 9948 500
sales-de@sysgo.com

SYSGO France
Phone +33 1 30 09 12 70
sales-fr@sysgo.com

SYSGO Czech
Phone +420 222 138 111
sales-cz@sysgo.com

SYSGO EMBEDDING INNOVATIONS