PikeOS
EN 50128 Certification Kit

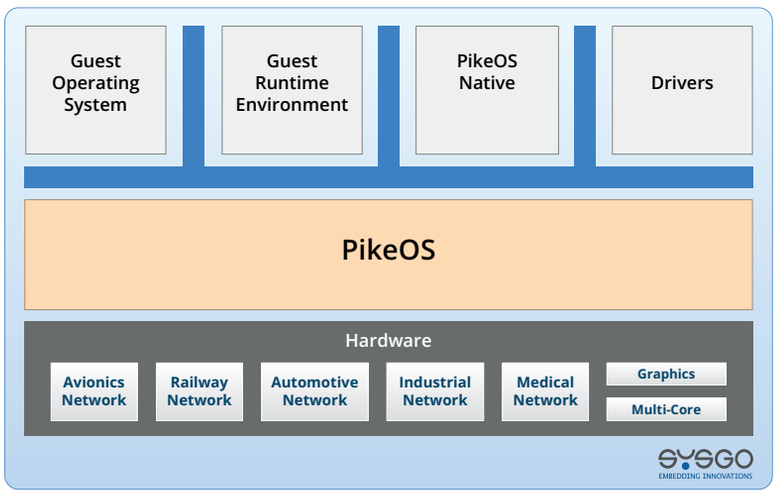
Reduce Certification Costs and Time-to-Market by using pre-certified Software Components

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 artefacts to prove the compliance of PikeOS to all objectives of the EN 50128 Safety standard. By using the PikeOS CertKit, SYSGO customers can focus on the certification of their application(s).

The PikeOS Board Support Package (BSP) implements software support for the customer's hardware and will require its own certification artefacts. SYSGO has the in-house expertise and tools to develop and certify PikeOS BSPs for custom hardware. 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, in order to validate the correct coexistence of both components.



PIKEOS CERTIFICATION KIT (CERTKIT)

PikeOS is the ideal platform for certifiable Safety Railway & Transportation applications requiring EN 50128 certification. Projects benefit from the fact, that PikeOS has achieved an EN 50128 SIL4 certification on a multicore platform.

In order to comply with the applicable parts of the EN 50128, SYSGO generates all artefacts, which are required for the certification of PikeOS running on custom hardware. The following list is a high level summary of the certification artefacts generated by SYSGO and mandated by the EN 50128:

- Certificate for the specified PikeOS version for the applicable hardware architecture (e.g. TÜV certification report)
- 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 completenefss of the development, verification and validation activities
- Safety manual for PikeOS and an additional 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
- Interface specifications required for application development, BSP development and module configuration

The Master Document List (MDL) for the overall certification process references detailed documentation, which SYSGO is able to present to the certification authorities (e.g. EASA, FAA) in order to obtain the PikeOS certification. If requested, this documentation is available for reviews and audits by SYSGO customers or the certification authorities.

PIKEOS/BSP VALIDATION KIT

The integration of a custom BSP 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:

- 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 EN 50128 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 EN 50128. These processes include requirements traceability, design control and intensive testing, verification and validation. The resulting documentation and records (certification artefacts) form the basis of the PikeOS EN 50128 CertKit for Railway & Transport 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 EN 50128 SIL 4.

Additionally to the compliance to EN 50128, SYSGO provides more 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 EN 50126 and EN 50129 requirements. The following list is a high level summary of the certification artefacts generated by SYSGO and required for the EN 50128 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)
- Tool qualification reports for the tools used within the PikeOS development which need qualification
- Stack analysis, WCET/timing analysis and partitioning analysis reports for PikeOS
- Software deployment documentation
- Software assessment documentation (e.g. TÜV certification report)

PIKEOS SOURCE CODE INSPECTION

Source code inspection is typically required for a certification in regards to EN 50128. Source code is not automatically included in the PikeOS CertKit, but always available additionally. Depending on the customers' requirements, the 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.

SYSGO CERTIFICATION SERVICES

The certification kit is complemented with a certification services package. The main objective of this 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 is typically managed by the customer. Nevertheless, SYSGO has established a good partnership to the certification authorities (e.g. EASA) due to successful projects in the past. Therefore, the attendance of SYSGO to audits and meetings with authorities is usual. SYSGO is open to provide detailed information about the developed products upon request.

SYSGO CERTIFICATION SUPPORT AND MAINTENANCE

To comply with the EN 50128 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:

- Defining the documentation needed for problem reporting and/or corrective actions, with the aim of giving feedback to the responsible management
- Defining analysis of the information collected in the problem reports to identify its causes
- Defining 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. The support contracts include SYSGO's commitment to maintain:

- The certified PikeOS version as well as corresponding certifications artefacts 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. EN 50128, EN 61508 and DO-178B). Certification artefacts are available for the following PikeOS components:

- **PikeOS Native GuestOS** provides a direct API for PikeOS.
- **PikeOS POSIX GuestOS** provides a PSE51 and PSE52 conformant API for PikeOS.
- **ARINC 653 GuestOS** for PikeOS is a complete and fully compliant implementation of the ARINC 653 P1-3 specification and parts of ARINC 653 P2-2.
- **Certifiable File System (CFS)** add-on provides a compact and robust file system running on top of a POSIX GuestOS or PikeOS Native GuestOS. CFS guarantees data integrity under any conditions, such as power failures.
- **Certifiable IP Stack (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 Republic
Phone +420 222 138 111
sales-cz@sysgo.com

www.sysgo.com