PikeOS
ISO 26262 Compliance Sheet

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, which is the fundamental basis for IMA architectures.

The PikeOS Certification Kit (CertKit) provides all necessary artefacts to prove the compliance of PikeOS to all software-relevant objectives of the ISO 26262 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.

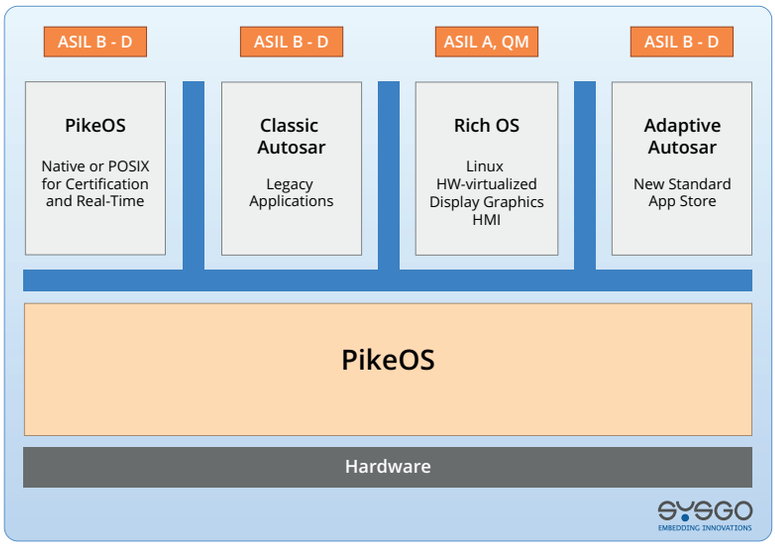


Fig 1: Architecture of PikeOS, mixing different ASIL Level applications and combining AUTOSAR Classic & Adaptive

PikeOS is the ideal platform for Safety certifiable Automotive applications requiring ISO 26262 certification. Projects benefit from the fact that PikeOS shows compliance to ISO 26262 up to ASIL D and has achieved IEC 61508, EN 50128 and DO-178B/C certifications in multiple equipment up to the highest Safety levels.

PIKEOS CERTIFICATION KIT (CERTKIT)

SYSGO's PikeOS CertKit offering includes the following documents:

- Certification Kit user manual which describes the usage and installation of PikeOS in a certifiable environment Safety case for PikeOS describes the processes performed and the documentation generated during the software life cycle. The Safety case includes a compliance matrix to show compliance to relevant ISO 26262 objectives
- Validation report for PikeOS, showing completeness of the development, verification and validation processes
- Safety & Security manual for PikeOS and an additional Safety & Security manual for the specific processor architecture. The Safety & Security manual describes the Safety and Security requirements and the usage domain restrictions for using PikeOS to build a safe and secure system
- A set of PikeOS life cycle data including PikeOS High-Level Requirements (HLRQ) and the PikeOS Interface specifications required for application development, BSP development and module configuration
- Tool Qualification Validation Report includes descriptions and references to the tool qualification approach for PikeOS including operational requirements and user guidance.
- If needed, an official certificate for a specified PikeOS version for an applicable hardware architecture can be foreseen. Typically SYSGO is working together with TÜV SÜD as a notified body.

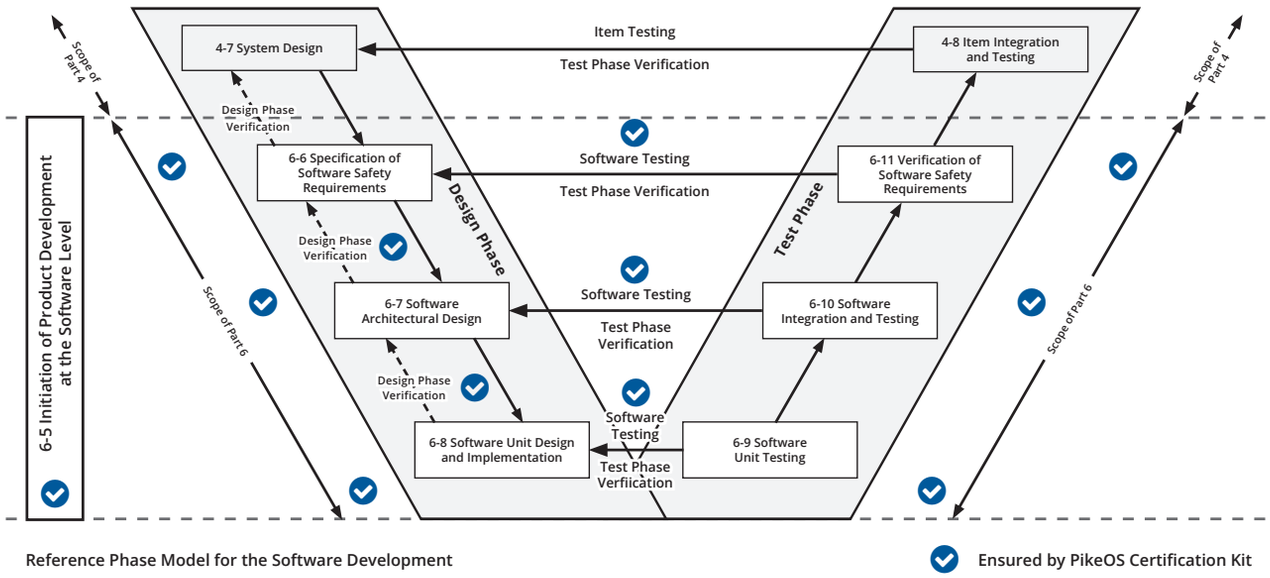
SYSGO ISO 26262 CERTIFICATION PROCESS

PikeOS has been developed using software development, verification & validation processes and procedures beside quality management and Safety & Security-related processes and procedures mandated in the ISO 26262. 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 ISO 26262 CertKit for automotive applications.

PikeOS is designed as an Safety Element out of Context (SEooC) as defined in ISO 26262 Part 10 §9. PikeOS can be used as a generic software component for a variety of nstallations purely by the provision of application-specific configuration data and algorithms. PikeOS is usable in systems with Safety integrity requirements up to ISO 26262 ASIL D.

Additionally to the compliance to ISO 26262, SYSGO provides further 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 ISO 26262 but also enable the compliance to other industry standards like IEC 61508, EN 50128 and DO-178C.

In order to comply with the applicable parts of the ISO 26262, 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 required for the ISO 26262 certification of PikeOS:

- PikeOS planning documentation
- Software development standards
- Software high-level requirements documentation
- Software architecture and low-level design documentation
- Implementation documentation
- Software testing and additional verification & validation documentation (including SW structural coverage reports as mandated by the applicable ASIL level (e.g. MC/DC coverage for ASIL D).
- Software Integration documentation
- Software deployment documentation like a Safety case which includes a compliance list to ISO 26262 and a Safety & Security manual which includes procedures for the integrator and application developer on how to use PikeOS in a safe and secure way.
- Tool qualification validation report for the tools used within the PikeOS development which need qualification including operational requirements and user guidance.
- Analysis documentation like stack analysis, WCET/timing analysis and partitioning analysis reports
- Software certificate and assessment documentation (e.g. TÜV certification report if needed)

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 SOURCE CODE INSPECTION

Source code inspection is typically not required for a certification in regards to ISO 26262. Source Code is not automatically included in the PikeOS CertKit, but always available additionally. 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.

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. TÜV) to manage certification procedures. 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

The PikeOS CertKit support contract enables SYSGO customers to have an effective implementation of this regulatory. For devices launched to the field a customer-specific long-term based device cycle maintenance contract keeps this implementation of the regulatory available and includes 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)

Additionally SYSGO's implemented Safety & Security board analyses any product issue reported by SYSGO support organization in relevance to contracted Safety and/or Security certification projects. Results of the Safety & Security board are communicated to SYSGO customers under a valid certification support or life cycle maintenance contract by Safety & Security bulletins on a quarterly base.

CERTIFIED PIKEOS ADD-ONS/OPTIONAL COMPONENTS

PikeOS and its middleware components were certified according to various industry standards (e.g. DO-178B, EN 50128 and EN 61508). 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.

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 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