PikeOS DO-178C Certification Kit

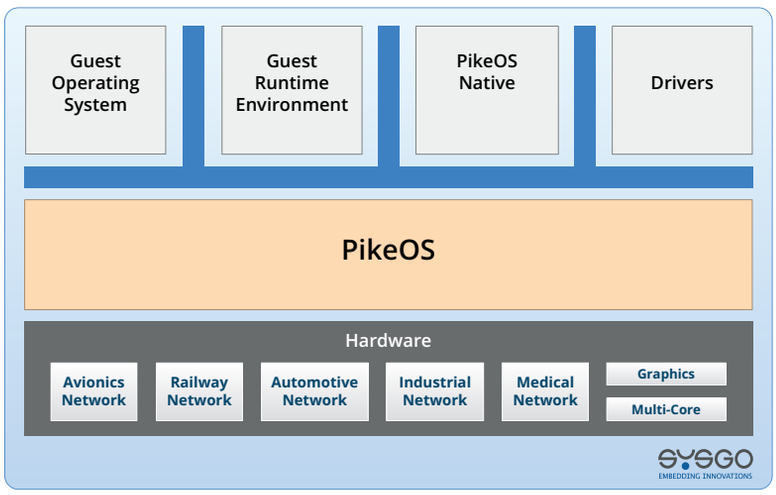
Reduce Certification Costs and Time-to-Market by using pre-certified Software Components

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, 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 objectives of the DO-178C 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 Safety certifiable Avionics & Defense applications requiring DO-178 certification up to DAL A (Design Assurance Level). Projects benefit from the fact that PikeOS has achieved DO-178 certification on civil and military aircraft systems.

In order to comply with the applicable parts of the DO-178C, 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 DO-178C:

- Planning documentation (PSAC, SDP, SVP, SQAP, SCMP)
- Software Standards (SRS, SDS, SCS)
- Software High Level Requirements documentation
- Interface Documentation for all PikeOS components
- Design Documentation (Architecture and Low Level Requirements) including component and module design
- Implementation and verification documentation
- Software Integration documentation
- Software verification and testing documentation (SVCP, SVR)
- Stack analysis, timing analysis and partitioning analysis reports for PikeOS
- Structural coverage documentation
  - Statement coverage (SW level A, B, C)
  - Decision coverage (SW level A, B)
  - MC/DC coverage
  - Source-Code-to-Object-Code coverage (SW level A)
- Traceability documentation
- Safety manual for PikeOS (generic and processor architecture specific)
- Tool qualification reports for the tools used within the PikeOS development which need qualification based on requirements of DO-178C and DO-330
- Software Delivery documentation (SCI, MDL)
- SW Accomplishment Summary (SAS) for the generic PikeOS components. The SAS gives a compliance statement to the processes performed by SYSGO during the software lifecycle.

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 DO-178C CERTIFICATION PROCESS

The SYSGO Certification Kit includes all mandatory evidence and artefacts to comply with the international software standard DO-178C for Aerospace & Avionics software applications, which ensure that any certification audit can be fulfilled by showing compliance to all objectives of this standard.

PikeOS is designed as a Commercial-Off-The-Shelf (COTS) software component (as defined in DO-178C chapter 2.5.3) so that it can be used for a variety of installations purely by the provision of application-specific configuration data and algorithms. It is usable in systems with Safety integrity requirements up to DO-178C SW Level A and is developed using software processes in compliance with this standard.

Additionally to the compliance to DO-178C, SYSGO provides more documentation to support the integration of PikeOS into the customer specific hardware certification strategy. E.g. a Safety manual for PikeOS (generic and processor architecture specific) will be provided to establish Safety requirements for integrators and application developers how to use PikeOS to build a safe system.

PIKEOS SOURCE CODE INSPECTION

Source code inspection is typically required for a certification in the Aerospace & Avionics industry. 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. 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 DO-178C 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. DO-178C, 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.

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