



SYSGO & PikeOS

Security Certification Kit

SYSGO’s PikeOS Security Certification Kit helps customers prepare their certification in projects aiming Common Criteria for examination and evaluation of IT security (EAL) from the Federal Office for Information Security (BSI) or the Airbus SAR SAL up to the highest levels.

PIKEOS AND SECURITY

The Certification Kit covers a strong separation in time and space of user applications in different Security criticalities. This separation is established by PikeOS and does not allow interferences (e.g. grabbing RAM or CPU time) or any communications unless they are explicitly allowed by configuration, i.e. a very strong white list Security policy. PikeOS has been developed using software development, verification & validation processes and procedures beside quality management and Safety & Security-related processes and procedures for different industry standards.

USE CASES

One of the most important documents when starting a certification project is the Security manual that is delivered with the Certification Kit. It can also be ordered upfront to a certification project in order to start planning and gathering information. To comply with different Security standards the supplier and/or developer has to establish, document and maintain procedures for problem reporting and corrective actions. These procedures especially cover the following aspects:

BOARD SUPPORT PACKAGE

The PikeOS Board Support Package (BSP) implements software support for the customer’s hardware and will require its own certification artifacts. SYSGO has the in-house expertise and tools to develop and certify PikeOS BSPs for custom hardware.

BENEFITS

- Reduction of certification costs
- Integration of certified and non-certified applications
- Keep the system expandable for new Security features while maintaining the certification level
- Support and input to work with certification agencies
- Provides compliance to export regulations
- Trustworthy and approved in avionics projects

- 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

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.

FEATURES

For different architectures, such as x86 64-bit, ARMv8, or PowerPC, the product is aligned to fulfill basic customer requirements and artefacts needed for their certification projects, such as:

- PikeOS Security Target
- Security Management and Development Plan (SMDP) (incl. Secure Development and Delivery), SW Development, SW Verification, SW Quality Assurance and SW Configuration Management Plan
- SW Requirements-, Design- and Coding Standard
- PikeOS Master Document List (MDL), Software Configuration Index Document (SCI), SW Aspects of Certification (SAS), PikeOS Security Target (Testing) or Stack Analysis
- Different items, such as High Level Requirement (HLRQ) or Design Documents or description of interfaces, verification and validation documents for Security
- PikeOS tool validation report
- PikeOS Security manual

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.

HIGHEST QUALITY & COMMON CRITERIA CERTIFICATION

As our products are used in the most critical environments and applications, SYSGO has strict in-house quality requirements in product development. Our company processes are certified according to ISO 9001:2015, and in

CERTIFICATION DOCUMENTATION

- **Avionics & Defense:** DO-178C Certification Kit
- **Railway & Transportation:** EN 5128 / EN 50657 Certification Kit
- **Automotive:** ISO 26262 Compliance Sheet

→ www.sysgo.com/certkits

The content of the Certification Kits varies, depending on assurance level, industry and addressed standard. For more details on the content of a Certification Kit, please contact us:

→ sales@sysgo.com

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.

2016 we achieved the certification against ISO/IEC 27001:2013. Since 2019 the PikeOS hypervisor is also certified according to Common Criteria EAL3+. Read more → www.sysgo.com/common-criteria

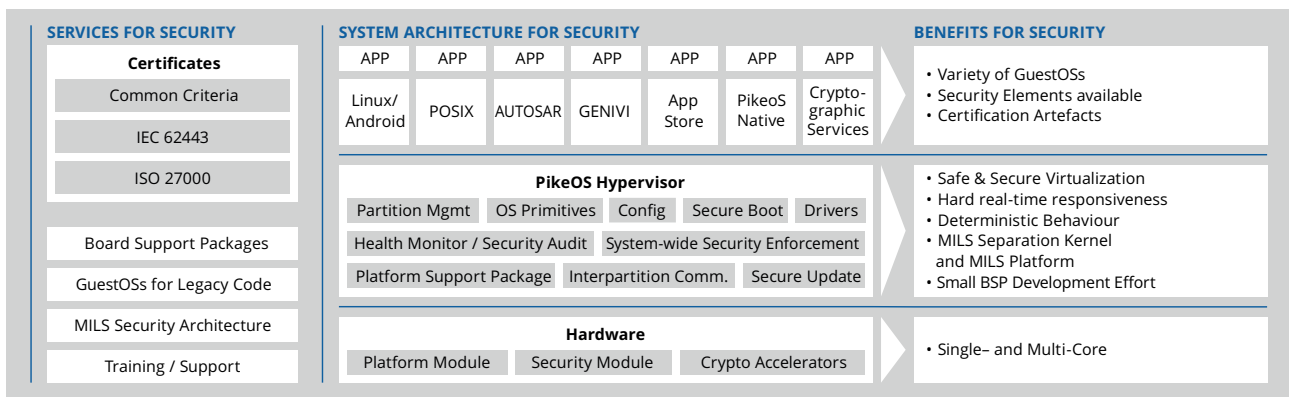


Figure 1: Scheme of a Security System with PikeOS Architecture

Founded in 1991, SYSGO became a trusted advisor for Embedded Operating Systems and is the European leader in hypervisor-based OS technology offering worldwide product life cycle support. We are well positioned to meet customer needs in all industries and offer tailor-made solutions with highest expectations in Safety & Security. More information at www.sysgo.com/security