SYSGO
EMBEDDING INNOVATIONS

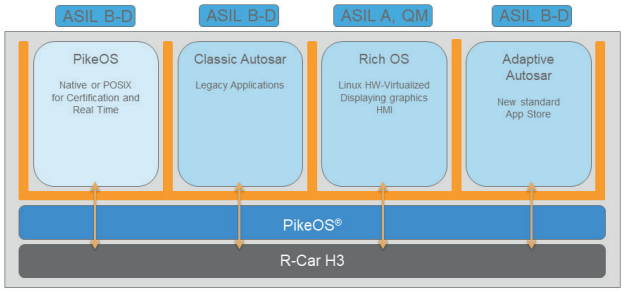
Business Solution

ISO 26262 Compliance Sheet for PikeOS®

The Certified Safe & Secure Hard Real-Time Hypervisor

PikeOS – The Certified Safe and Secure Real-time Hypervisor

PikeOS is the ideal platform to build safe & secure automotive applications that need to be ISO 26262 certified. A project benefits from the fact, that PikeOS shows compliance to ISO 26262 up to ASIL D and has achieved IEC 61508, EN 50128 and DO-178B certifications in multiple equipment up to the highest safety levels. Additionally PikeOS shows compliance to security standards like Common Criteria for Information Technology Security Evaluation (CC).



PikeOS, mixing diff. ASIL Level Applications and combining AUTOSAR classic & adaptiv

I. INTRODUCTION

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

The PikeOS Certification Kit (CertKit) provides all necessary artifacts 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 compliance confirmation or certification of their own applications.

A PikeOS Board Support Package implements software support for the customer's hardware and will require its own certification artifacts. The BSP typically consists of the "Platform Support Package" (PSP) and a number of drivers. SYSGO has the in-house expertise and tools to develop and certify customer BSPs.

If SYSGO customers want to develop their own PSP, the PikeOS/PSP Validation Kit provides the tooling to re-run a subset of the PikeOS test-suites together with the customers PSP to validate the correct coexistence of both components.

II. PIKEOS CERTIFICATION KIT (CERTKIT) CONTENTS

SYSGOs PikeOS CertKit offering includes the following documents:

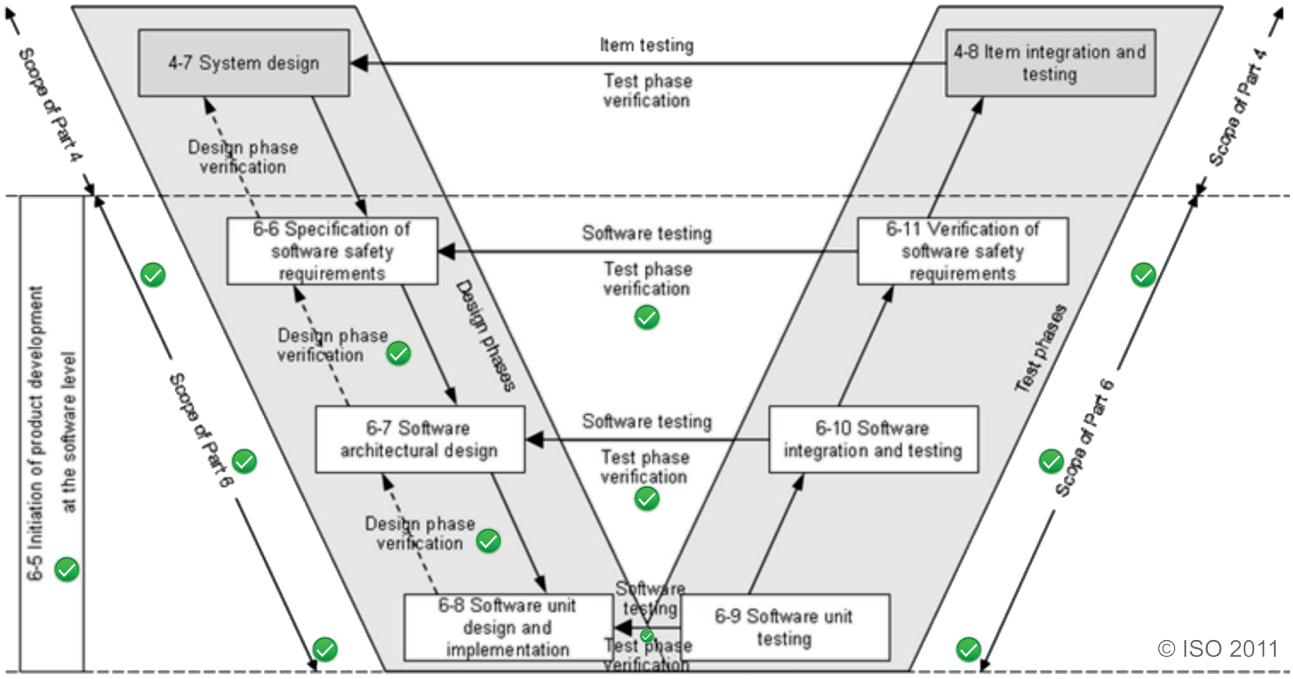
- Certification Kit User Manual which describes the usage and installation of PikeOS in a certifiable environment
- The Safety Case for PikeOS describes the processes performed and the documentation generated during the software lifecycle. The Safety Case includes a Compliance Matrix to show compliance to relevant ISO 26262 objectives
- The Validation Report for PikeOS, showing completeness of the development, verification and validation processes
- The 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 TUEV SÜD as a notified body

III. 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 artifacts) form the basis of the PikeOS ISO 26262 CertKit for automotive applications.

PikeOS is designed as a 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 installations 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 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 ISO 26262 but also enable the compliance to other industry standards like IEC 61508, EN 50128 and DO-178C.



Reference phase model for the software development

= Ensured by PikeOS CERT Kit

The following list is a high level summary of the certification artifacts 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. TUEV 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 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 or the certification authorities/notified bodies.

IV. PIKEOS SOURCE CODE INSPECTION

Source code inspection is typically not required for a certification in regards to ISO 26262. 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. If requested, a source code inspection can be agreed for reviews and audits by SYSGO customers or the certification authorities/notified bodies.

V. SYSGO CERTIFICATION SERVICES

The PikeOS CertKit is complemented with a certification services. The main objective of this certification service is to establish communication and understanding between SYSGO, the customer and the certification authorities/notified bodies 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.

VI. SYSGO CERTIFICATION SUPPORT AND MAINTENANCE

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

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.

VII. CERTIFIED PIKEOS ADD-ONS/OPTIONAL COMPONENTS

PikeOS and its middleware components were certified according to various industry standards (e.g. EN 50128, EN 61508, DO-178B/C and ISO 26262). Certification artifacts are available for the following PikeOS components:

- **PikeOS Native Cert Personality:** The PikeOS Native Cert personality provides a direct API for PikeOS.
- **PikeOS POSIX Cert Personality:** The PikeOS POSIX Cert personality provides a PSE51 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 guaranties 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