Safety Certification Kits

SYSGO & PikeOS

Over the years, SYSGO's experienced senior engineers have gathered a deep understanding regarding the bonds between architecture, design, implementation, verification and validation. As a consequence, we know how to handle complex software projects.

At every step during the project's entire life cycle, we can assist you and help avoiding common pitfalls, effectively escaping unnecessary loops and re-design at a late state. For example: The software does what it is expected to do ... however, it turns out that it is simply not testable.

Content

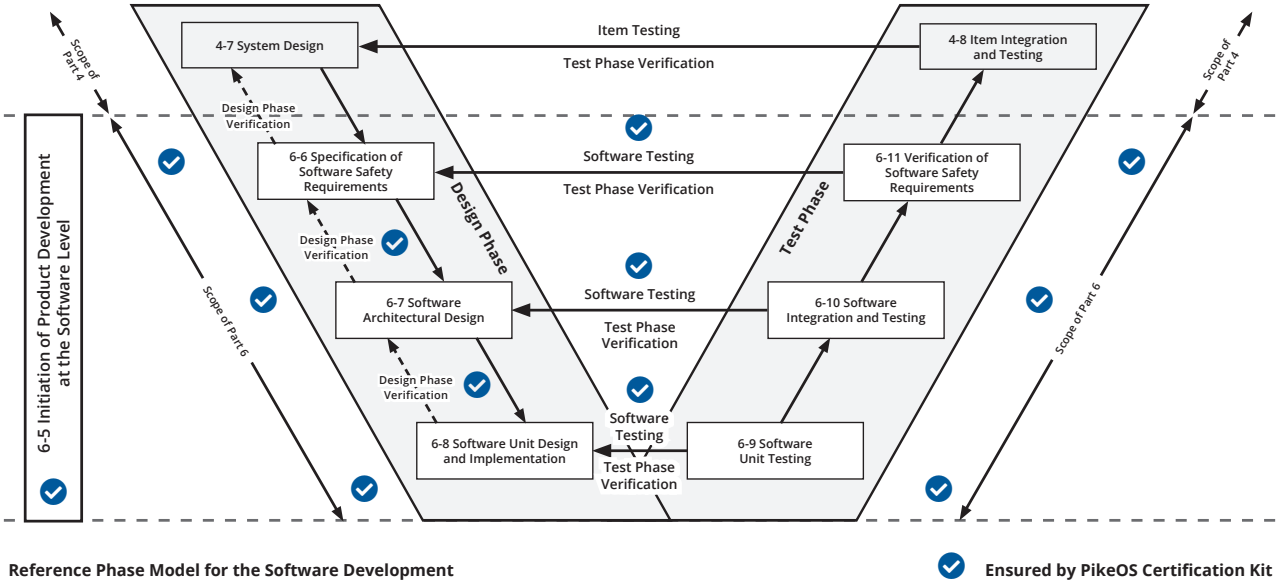

Figure 1: Example project life cycle according to ISO 26262 (Automotive)

1. Introduction & Safety Levels

We know how to implement consistent traceability spanning from the architecture down to the source code. You are planning to integrate our products into your development? That's where our Certification Kits come into play. They come with all necessary artifacts. For every relevant entity within those documents, we have allocated unique and unambiguous ID numbers - audited for completeness and integrity. The IDs can be embedded seamlessly into the overall project documentation.

Certification Kits are available for compliance with the following Safety Standards. The content of each Safety kit is tailored to fulfil the needs of the according standard.

DAL: Development Assurance Level
SIL: Safety Integrity Level
ASIL: Automotive Safety Level

Market	Standard	Safety Level	Assured SYSGO Level
Avionics	DO-178C	DAL A - DAL D	DAL A (highest)
Space	ECSS-E-ST-40C ECSS-Q-ST-80C	Category A - Category D	Category A (highest)
Railway	EN 50128, EN 50657	SIL 1 - SIL 4	SIL 4 (highest)
Automotive	ISO 26262	ASIL A - ASIL D	ASIL D (highest)
Industrial Automation	IEC 61508	SIL 1 - SIL 3 (SIL 4 only with hardware)	SIL 3 (highest for pure software)

2. Avionics Qualification Kit for DO-178C

In order to comply with the applicable parts of the DO-178C, SYSGO generates all artefacts, which are required for the qualification of PikeOS operating system in regards to DO-178C running on specific architectures (e.g. ARM8, PPC, x86-64) and 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, TP, SWDP, SWVP, SQAP, SCMP)
- Software standards for requirements (RSTD), design (DSTD), code (CSTD, ASTD)
- Software high-level requirements documentation (HLRQ)
- Interface documentation (IF) for all PikeOS components
- Design documentation (DS) (architecture and low-level requirements) including component and module design
- Software verification and testing documentation (test case master (TC), test reports (TR) for all relevant architectures and reference boards
- Stack analysis (SANA), worst case timing analysis (TANA) and partitioning analysis reports (PANA) for PikeOS
- Structural coverage measurement documentation
  - Statement coverage (SW level A, B, C)
  - Decision coverage (SW level A, B)
  - MC/DC coverage (SW level A)
- Source-code-to-object-code coverage (STO, software level A). For software level A, the Gnat PRO C compiler from AdaCore is being used to support STO
- Traceability documentation with upward and downward traceability (TRACE)
- Safety manual for PikeOS (generic and processor architecture specific). The Safety manual describes the Safety requirements and the usage domain restrictions for using PikeOS to build a safe system. It also includes procedures for the integrator and application developer on how to use PikeOS in a safe and secure way
- Tool qualification reports for the tools used within the PikeOS development which need qualification based on requirements of DO-178C and DO-330 including operational requirements and user guidance
- Software delivery documentation (SCI, MDL, RMM)
- Software Component Accomplishment Summary (CAS) for the PikeOS. The SAS gives a compliance statement to the processes performed by SYSGO during the software life cycle to show compliance to DO-178C
- SYSGO provides a DO-178C compliance list with an analysis and a list of activities which are necessary to be executed by the user of PikeOS

Additional contracts can be agreed:

- to qualify customer board support packages (PSP + driver) to DO-178C
- to qualify other personalities of the PikeOS ecosystem (e.g. ARINC 653 (A653), POSIX, Certified File System (CFS), Certified UDP stack (CIP)
- Support the customer to execute integration activities to show correct PikeOS integration (PikeOS PSP validation) and adequate timing behavior (WCET) on customer board(s)

3. Space Qualification Kit for ECSS

In order to comply with the applicable parts of ECSS (ECSS-E-ST-40C / ECSS-Q-ST-80C), SYSGO generates all artefacts, which are required for the qualification of PikeOS operating system in regards to ECSS running on specific architectures (e.g. SPARC-LEON, ARM8, PPC, x86-64) and custom hardware.

The following list is a high level summary of the certification artefacts generated by SYSGO and mandated by the ECSS:

- Planning documentation (PSAC, TP, SWDP, SWVP, SQAP, SCMP)
- Software standards for requirements (RSTD), design (DSTD), code (CSTD, ASTD)
- Software high-level requirements documentation (HLRQ)
- Interface documentation (IF) for all PikeOS components
- Design documentation (DS) (architecture and low-level requirements) including component and module design
- Software verification and testing documentation (test case master (TC), test reports (TR) for all relevant architectures and reference boards
- Stack analysis (SANA), worst case timing analysis (TANA) and partitioning analysis reports (PANA) for PikeOS
- Structural coverage measurement documentation
  - Statement coverage (Cat. A, B, C)
  - Decision coverage (Cat. A, B)
  - MC/DC coverage (Cat. A)
- Source-code-to-object-code coverage (STO, SW level A). For SW level A, the PikeOS GCC and Gnat PRO C compiler from AdaCore is being used to support STO
- Traceability documentation with upward and downward traceability (TRACE)
- Safety manual for PikeOS (generic and processor architecture specific). The Safety manual describes the Safety requirements and the usage domain restrictions for using PikeOS to build a safe system. It also includes procedures for the integrator and application developer on how to use PikeOS in a safe and secure way
- Tool qualification reports for the tools used within the PikeOS development which need qualification based on requirements of ECSS, DO-178C and DO-330 including operational requirements and user guidance
- Software delivery documentation (SCI, MDL, RMM)
- SW Component Accomplishment Summary (CAS) for the PikeOS. The SAS gives a compliance statement to the processes performed by SYSGO during the software life cycle to show compliance to ECSS
- Establishment of a metrication system inline with ECSS requirements and delivery of a summary in the SAS
- SYSGO provides a ECSS compliance list with an analysis and a list of activities which are necessary to be executed by the user of PikeOS

Additional contracts can be agreed:

- to qualify customer board support packages (PSP + driver) to ECSS
- to qualify other personalities of PikeOS ecosystem (e.g. ARINC 653 (A653), POSIX, Certified File System (CFS), Certified UDP stack (CIP)
- Support the customer to execute integration activities to show correct PikeOS integration (PikeOS PSP Validation) and adequate timing behavior (WCET) on customer board(s)

4. Railway Certification Kit for EN 50128 and EN 50657

The following list is a high-level summary of the certification artefacts generated by SYSGO:

- Planning documentation (Safety Plan (SP), TP, 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
- Software verification and testing documentation (SVCP, SVR)
- Stack analysis, timing analysis and partitioning analysis reports for PikeOS
- Structural coverage documentation
  - Statement coverage (SIL 2)
  - Decision coverage (SIL 3)
  - MC/DC coverage (SIL 4)
- Traceability documentation
- Tool qualification reports for the tools used within the PikeOS development which need qualification including operational requirements and user guidance
- Software delivery documentation (SCI, MDL, RMM)
- Safety case for PikeOS. The Safety case describes the processes performed and the documentation generated by SYSGO during the software life cycle. It also includes procedures for the integrator and application developer on how to use PikeOS in a safe and secure way
- Validation report, showing completeness 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

Additionally specific certificates and assessment reports for EN 50128 / EN 50657 for the applicable hardware architecture will be provided (e.g. TÜV certificate).

Additional contracts can be agreed:

- to qualify customer board support packages (PSP + driver) to EN 50128/50657
- to qualify other personalities of PikeOS ecosystem (e.g. ARINC 653 (A653), POSIX, Certified File System (CFS), Certified UDP stack (CIP)
- Support the customer to execute integration activities to show correct PikeOS integration (PikeOS PSP Validation) and adequate timing behavior (WCET) on customer board(s)

5. Automotive Certification Kit for ISO 26262

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 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 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, and EN 50128.

The following list is a high level summary of the certification artefacts generated by SYSGO and required for the ISO 26262 certification of PikeOS:

- Planning documentation (Safety Plan (SP), TP, 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
- Software verification and testing documentation (SVCP, SVR)
- Stack analysis, timing analysis and partitioning analysis reports for PikeOS
- Structural coverage documentation
  - Statement coverage (ASIL A)
  - Decision coverage (ASIL B/C)
  - MC/DC coverage (ASIL D)
- Traceability documentation
- Tool qualification reports for the tools used within the PikeOS development which need qualification including operational requirements and user guidance
- Software delivery documentation (SCI, MDL, RMM)
- Safety case for PikeOS. The Safety case describes the processes performed and the documentation generated by SYSGO during the software life cycle. It also includes procedures for the integrator and application developer on how to use PikeOS in a safe and secure way
- Validation report, showing completeness 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

Additionally specific certificates and assessment reports for ISO 26262 for the applicable hardware architecture will be provided (e.g. TÜV certificate).

Additional contracts can be agreed:

- to qualify customer board support packages (PSP + driver) to ISO 26262
- to qualify other personalities of PikeOS ecosystem (e.g. ARINC 653 (A653), POSIX, Certified File System (CFS), Certified UDP stack (CIP)
- Support the customer to execute integration activities to show correct PikeOS integration (PikeOS PSP Validation) and adequate timing behavior (WCET) on customer board(s)

6. Industrial Automation Certification Kit for IEC 61508

The following list is a high-level summary of the certification artefacts generated by SYSGO:

- Planning documentation (Safety Plan (SP), TP, 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
- Software verification and testing documentation (SVCP, SVR)
- Stack analysis, timing analysis and partitioning analysis reports for PikeOS
- Structural coverage documentation
  - Statement coverage (SIL 2)
  - Decision coverage (SIL 3)
  - MC/DC coverage (SIL 4)
- Traceability documentation
- Tool qualification reports for the tools used within the PikeOS development which need qualification including operational requirements and user guidance
- Software delivery documentation (SCI, MDL, RMM)
- Safety case for PikeOS. The Safety case describes the processes performed and the documentation generated by SYSGO during the software life cycle. It also includes procedures for the integrator and application developer on how to use PikeOS in a safe and secure way
- Validation report, showing completeness 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

Additionally specific certificates and assessment reports for IEC 61508 for the applicable hardware architecture will be provided (e.g. TÜV certificate).

Additional contracts can be agreed:

- to qualify customer board support packages (PSP + driver) to IEC 61508
- to qualify other personalities of PikeOS ecosystem (e.g. ARINC 653 (A653), POSIX, Certified File System (CFS), Certified UDP stack (CIP)
- Support the customer to execute integration activities to show correct PikeOS integration (PikeOS PSP Validation) and adequate timing behavior (WCET) on customer board(s)

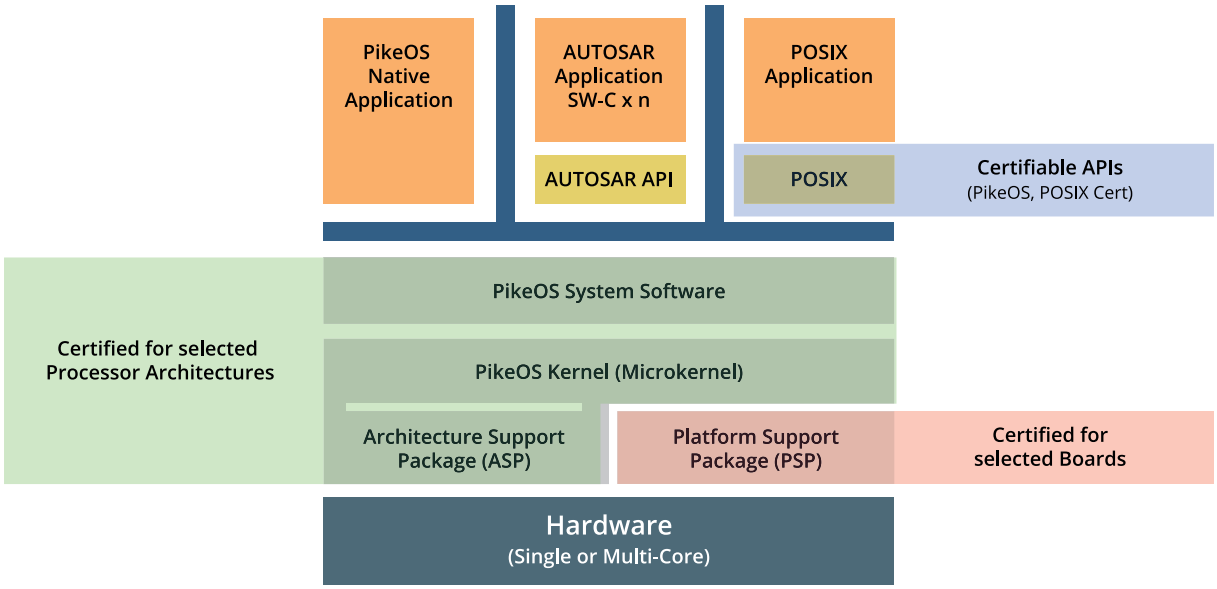

Figure 2: Certifiable and certified components in a running PikeOS System

7. Certified Components

The architecture of a PikeOS example system is shown in figure 2. The green sections are part of the PikeOS operating system and fully covered by each certification kit. The yellow certifiable APIs are ready for certification in the context of the particular project. However, SYSGO also provides some pre-certified execution environments, such as ARINC 653 which is already covered by the Avionics certification kit.

In addition, certification artefacts for some selected platform support packages are ready to use. Nonetheless, most certification projects will come along with customized hardware. In case the customer opts to develop and validate the required platform support package on its own, SYSGO provides the according tools.

8. PikeOS / PSP Validation Kit

The integration of a custom PSP 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 / PSP 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.

9. 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.

10. Certified PikeOS Add-ons / Optional Components

In addition to PikeOS and its middleware components certification artefacts are also available for the following PikeOS components:

- PikeOS Native Guest OS provides a direct API for PikeOS
- PikeOS POSIX Guest OS provides a PSE51 and PSE52 conform API for PikeOS
- ARINC 653 Guest OS 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

11. 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, and TÜV as a “notified body”) 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.

12. 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 (Quality Management), and in 2016 we achieved the certification against DIN EN ISO / IEC 27001:2017 (Information Security Management).

Since 2022 the PikeOS Separation Kernel Version 5.1.3 is also certified according to Common Criteria EAL5+.

SYSGO Headquarters
+49 6136 9948 500

SYSGO France
+33 1 30 09 12 70

SYSGO Czech Republic
+420 222 138 111

sales@sysgo.com

www.sysgo.com