SYSGO Product Note

PikeOS

Certifiable RTOS with Hypervisor Functionality

PikeOS for MPU

Real-Time Partitioning for MPU Architectures

Introduction

The PikeOS operating system is a light-weight virtualization system that is capable of hosting nearly all industry standard operating systems and execution environments. It supports the most stringent real-time requirements emerging from Safety-related industries, even on multi-core processor hardware.

PikeOS is available for a whole range of embedded hardware architectures, such as x86, ARM, PPC and RISC-V, supporting systems with or without a Memory Management Unit (MMU).

www.sysgo.com/pikeos

www.sysgo.com/pikeos-for-mpu

Table of Contents

1. Base Products
2. Guest OSs, RTEs & APIs
3. Hardware Virtualization
4. Major Time Frame Synchonization
5. Guest OS on Demand
6. Driver Framework
7. Multi-Core Optimization
8. Additional Certifiable Components
9. Certification Kits
10. Board Support Packages (BSPs)
11. CODEO IDE and Tools
12. Development Host Computer Requirements
13. Support
14. Partner Ecosystem
15. Technical Data

1. Base Products

PikeOS

PikeOS is a real-time operating system (RTOS) and hypervisor designed to support critical applications requiring high levels of safety and security. Available since 2003, PikeOS (also known as PikeOS for MMU) has evolved from a microkernel with real-time capabilities to a mature platform of choice in the embedded safety and security domain. It combines real-time and virtualization uniquely, functioning as a type-1 hypervisor that executes directly on the bare metal.

PikeOS enables the concurrent execution of multiple operating systems and applications on a single hardware platform through its hypervisor capabilities. It ensures strong separation between these concurrent applications using time and space partitioning. This partitioning allows for precise resource allocation and isolation, enhancing both safety and security. PikeOS is certified for various safety standards, making it suitable for industries such as aerospace, automotive, industrial automation, and defense.

PikeOS for MPU

PikeOS for MPU is a real-time operating system (RTOS) is available since 2022, designed for systems providing high levels of safety and security. It shares much with its more extensive counterpart, PikeOS RTOS & Hypervisor, including the same native API, development environment (CODEO), and qualification processes.

The primary difference lies in the hardware targets and features. PikeOS for MPU is optimized for systems with limited resources (Memory Protection Units (MPUs) only), focusing on safety and security through time and space partitioning. Each partition is independently managed, ensuring separation of applications and secure allocation of resources like memory and CPU time.

PikeOS for MPU has been validated with respect to Security and Common Criteria or a similar approach can be used as Security standard. It maintains strict isolation between partitions to ensure secure operation in critical applications.

2. Guest OSs, RTEs & APIs

PikeOS Native

The PikeOS Native API is primarily designed to build para-virtualized guest operating systems. It provides a small but complete set of low level system calls that are optimized for performance, robustness, Safety and Security.

The PikeOS Native API is also the first choice when it comes to software to be certified at the highest certification levels.

ARINC 653 (aka APEX)

The PikeOS ARINC 653 is built upon the PikeOS native API and provides a complete and fully functional APEX API target for Avionics systems, in particular with respect to Integrated Modular Avionics (IMA). The ARINC 653 guest operating system is certifiable according to DO-178C DAL A.

POSIX

The POSIX API implements a subset of the PSE52 real-time controller system profile. It is a good choice for medium Safety-critical systems where a huge number of operating system services are required, but the use of Linux would still be too risky. It is often used for Automotive projects that require compliance to ISO 26262. The POSIX API is the backbone of the AUTOSAR adaptive solution.

Linux

When a large set of features is required, Linux is the operating system of choice. Although PikeOS has no restrictions on the Linux distribution to be hosted, the in-house ELinOS is recommended. It offers the most straight forward integration into a PikeOS virtual machine as well as dedicated extensions in order to directly use enhanced PikeOS features.

Linux operating system partitions are often used alongside a POSIX or ARINC 553 partition, setting up a an overall system with mixed criticality. The PikeOS hypervisor technology ensures that a running Linux OS has no impact on the certification aspects of an API with a higher degree of criticality. Linux operating systems can be run in hardware- as well as para-virtualized mode.

Windows

Windows integrates seamlessly into the PikeOS virtual environment, offering a stable platform for applications that require extensive user interfaces and broad hardware compatibility. This integration leverages native Windows drivers and subsystems within a secure, virtualized PikeOS environment.

3. Hardware Virtualization

The PikeOS hardware virtualization solution allows the execution of a complete guest operating system inside a partition without the need of modifying it. Hardware virtualization is available for the ARM architecture.

VirtIO

Enables VirtIO for enhanced I/O virtualization, ensuring efficient device integration and optimized throughput across virtual environments.

HW-Virt on x86 and ARM

Implements hardware virtualization using VT-X and AMD-V extensions to achieve efficient CPU and memory isolation, enhancing system security and performance scalability.

4. Major Time Frame Synchronization

PikeOS implements advanced algorithms for major time frame synchronization, ensuring microsecond-level accuracy across distributed real-time systems. This feature coordinates the execution of operations precisely on schedule to meet stringent real-time deadlines, critical for the functionality of Safety- and mission-critical applications.

By reducing jitter and ensuring that time-critical tasks meet their deadlines, PikeOS enhances system reliability and determinism in environments where timing accuracy is paramount.

5. Guest OS on Demand

The following partition types are available on demand:

Market	Standard
Certified POSIX	Available for PikeOS 3.1/3.4 in certification context only. Also planned for PikeOS 5.1.x
RTEMS	Available for PikeOS 3.4 on SPARC
Android	Available only as customized engineering services
Autosar classic	Partner solution possible via Vector
Autosar adaptive	Partner solution possible via Vector
Java	Available via partner Aicas “Jamaica”. Requires POSIX or Linux guest OS

6. Driver Framework

As a virtualization solution, PikeOS offers different realms where user device drivers can be implemented:

- As user space application with direct memory mapped access to the hardware I/O resources. The application may either directly utilize the hardware exclusively on its own or offer access to other user space applications by means of the file provider API.
- As system extension in the PikeOS system software. This method is still available for PikeOS 5.x, but is marked as deprecated
- Within the PSP (KLDD). These are small drivers that are typically used during board bring up (e.g. serial console) and usually specific to the according PSP
- Within the PikeOS kernel (KDEV). Character-, block-drivers and volume providers are available

Standard PikeOS BSPs come at least with an Ethernet and serial driver. The whole range of PikeOS drivers comprises:

- CAN
- DIO
- I2C
- RTC
- Watchdog
- SPI
- PCI/PCIe
- QSPI
- NAND Flash
- NOR Flash
- MMC Mass Storage
- SATA
- GPU
- USB Mass Storage
- AFDX

7. Multi-Core Optimization

PikeOS implements cache coloring to strategically partition the CPU cache among running processes. This technique minimizes cache contention by ensuring that different cores or processes do not frequently access the same cache lines, thereby reducing cache thrashing and improving cache utilization efficiency. This results in enhanced performance and predictability for multi-core systems.

8. Additional Components

Certifiable File System (CFS)

The CFS is a PikeOS component that provides a fail safe file system with more functionality than the PikeOS native file system. In addition to the basic file operations implemented by the internal PikeOS file providers, the CFS can also handle directories and file manipulations. It is still a simplified file system compared to standard Linux file systems and is certifiable within the scope of Safety projects.

Certifiable IP-Stack (CIP)

CIP is a UDP/IP networking stack compatible with the standard RFC specifications. It is available for the POSIX and PikeOS APIs and provides a standard socket interface. CIP is certifiable within the scope of Safety projects.

Certifiable Math Library (CML)

The CML provides various mathematical functions of the C standard library. CML is certifiable within the scope of Safety projects.

AFDX® Data Network End System

"Avionic Full-Duplex Switched Ethernet" (ARINC 664 Part 7) is a deterministic aircraft data network bus system for Avionics systems. The network is based on standard IEEE 802.3 Ethernet technology. SYSGO's implementation is software-based and runs on COTS (Commercial-Off-The-Shelf) hardware.

PikeOS drivers are available. All artefacts required to process a DO-178C certification are available. The currently available documents will cover a certification up to Level A. The software stack can also be used stand-alone out of the context of an operating system, e.g. on switches.

9. Certification Kits

PikeOS Certification Kits (CertKits) provide all necessary artefacts to prove the compliance of PikeOS to all objectives of the Safety and Security standards. By using the PikeOS CertKit, SYSGO customers can focus on the certification of their application(s).

- C/C++ Code Editor
- Syntax Highlighting
- Code Completion
- Source Navigation
- Type Hierarchy
- Call Graph
- Include Browser
- Macro Definition Browser

These Certification Kits are available (see table below).

10. Board Support Packages (BSP)

A list of supported PikeOS BSPs is available here:
www.sysgo.com/pikeos-bsp

Each approved BSP comes at least with Serial and Ethernet driver, but may contain more. Please contact SYSGO for more information.

11. CODEO IDE and Tools

The Eclipse-based IDE CODEO supports system architects with graphical configuration tools, provides all the components software engineers need to develop embedded applications and includes comprehensive little helpers to finish embedded projects in a time-saving and cost-efficient way: Guided configuration, remote debugging (down to the hardware instruction level), target monitoring, remote application deployment, and timing analyses.

Market	Standard	Assured Safety Level	Explanation
Automotive	ISO 26262	ASIL A – ASIL D	Automotive Safety Integrity Level
Avionics	DO-178C	DAL E – DAL A	Development Assurance Level
Space	ECSS	Category A - B	European Cooperation for Space Standardization
Functional Safety (General, Industrial Automation)	IEC 61508	SIL 1 – SIL 3	Safety Integrity Level
Railway Signalling & Rolling Stock	EN 50128, EN 50657	SIL 1 – SIL 4	Safety Integrity Level

Common Criteria: Security certification according to Common Criteria EAL 5+ (PikeOS 5.1.3)

Of course, CODEO provides standard application development features such as compiler, assembler and linker.

- Visual Debugging Tools, Views displaying
  - Memory
  - Registers
  - Disassembly

The PikeOS workflow defines two different working places, the Integrator Suite and the Application Suite.

Integrator Suite

The Integrator Suite comprises tools that are required to setup and manage virtual machines (aka resource partitions). Amongst others, these are:

- **Graphical Editor for the Virtual Machine Initialization Table (VMIT)**
  Allows to statically define the resource partitions for a PikeOS system. The definition comprise I/O and memory resources as well as processor affinity and processor time constraints. Inter-partition communication can be established by means of shared memory, drivers, ports and channels. The VMIT editor provides a graphical representation for each of those entities and allows to configure the system in a very detailed way.

- **Graphical Editor for the ROM-Image Builder**
  While the VMIT Editor configures the statically assigned resources, the ROM image builder configures the system- and user-files that are present on the running PikeOS system. In addition to services and daemons, the system-files typically consist of the PikeOS kernel and the PikeOS System Software. Both are available in different versions, such as certified and non-certified, debug and non-debug versions. User files typically consists of executables and data files. Except for system limits in terms of storage memory there is no constraint on what the user may add to the system. The ROM-Image Builder also allows to
  configure user-properties that can be read at runtime and provides the developer to hierarchically build up a tree of system settings.

- **Project Editor**
  Both the VMIT-Editor and the ROM-Image Builder are very enhanced tools and allow to setup a system in a very distinct way. In addition, there are cross reference and dependencies between both them. Therefore the project editor provides a top level view on the system and adjusts the the major items in the VMIT- and ROM-Image Builder accordingly. E.g. the project editor assumes that an application running in a partition requires an executable file and automatically provides a placeholder in the ROM-Image builder. It also creates all cross-references and access rights automatically. In case the integrator is not contended with the settings, the details can be changes in the two low-level tools. The project editor recognizes the changes and would not override them. However, the integrator is warned in case of inconsistencies or dangling ends.

The Integrator Suite also contains user-guided wizards for a quick project-start as well as validation tools for certification issues. The VMIT- as well as the ROM-Image builder are validated tools with regards to a DO-178C certification.

Developer Suite

The developer Suite comprises all tools that are required for application development. In general, two tool-chains are available:

- **GCC C/C++ based cross compiler**
  Applicable to all kinds to application types, certifiable up to DO-178C DAL B.

- **AdaCore GNAT Pro C/C++ compiler**
  Applicable for certification projects that a require a design assurance level of DAL A. In addition to C/C++, the Ada language is available for PikeOS native applications and ARINC 653 partition types.

Each guest operating system and API comes with its own developer suite. The tool-chain is fully integrated into the development IDE and the necessary compiler switches, header files and libraries are managed automatically based on the according guest operating system.

The developer suite also provides these tools:

- Graphical application setup wizards
- Project Editor: Allows to switch between debugging/ executable mode. Also allows to configure additional components and libraries. The project editor also manages the required compiler settings.
- Graphical debugger
- Static analysis tools
- Dynamic analysis tools (system-, application- and user-defined tracing)
- Muxa: Allows to multiplex communication methods (e.g. Ethernet, serial) between multiple start- and end-points. This is especially useful in case you are debugging multiple partitions with multiple consoles and debugging ports at the same time.

12. Development Host Computer Requirements

- CODEO supports 64-bit Linux distributions
- CODEO supports Windows 10/11 (64-bit)

13. Support

Standard support for the first year is included in standard product pricing. It contains analysis of reproducible errors in and malfunctioning of software developed by SYSGO and provision of known error corrections, as well as support in preparing work-around solutions.

Optional "Premium Support" offers additionally direct access to a dedicated support engineer and limited hours of consulting. "Long-Term Support" offers a retaining ability to rebuild the selected frozen version, a limited number of consulting hours, a dedicated phone number and access to a wide data base of corrections, updates, demo programs and others.

Certified product versions profit from "Product Cert Support" and "Long-Term Cert Support" that includes Safety and Security bulletins that inform the customer of vulnerabilities or Safety risks. Customer support is reserved to customers owning a valid support contract.

For more information, please get in contact with our SYSGO Sales team at www.sysgo.com/contact

14. Partner Ecosystem

SYSGO is committed to establish the technological and business partnerships that will help its customers to achieve their goals. SYSGO is currently working with about 100 partners worldwide. A list of available partners that help to enhance the value, can be found here:
www.sysgo.com/partners

15. Technical Data

Description	Value
Maximum Number of Resource Partitions	256
Maximum Number of Time Partitions	256
Maximum Number of Tasks	1023
Maximum Number of Threads	4096
Maximum Number of CPUs	32-64, based on processor architecture

All product and service names mentioned are the trademarks of their resp. companies. National product specifications may vary. Data contained in this document serves informational purposes only and are subject to change without notice. SYSGO GmbH shall not be liable for errors or omissions with respect to the materials. Warrenties are only set forth in the express warranty statements accompanying SYSGO products and services, if any.