SYSGO
EMBEDDING INNOVATIONS

Security

A Universal Requirement

www.sysgo.com

SYSGO

EMBEDDING INNOVATIONS

Europe's No 1 in Real-Time Operating Systems

SYSGO at a Glance

SYSGO is an independent entity from the THALES group and Europe's No 1 in safe & secure operating systems. Since 1991, SYSGO has expertise in embedded devices and is one of the pioneers in embedded Linux. The main markets are Aerospace & Defense, Railway, Automotive, and Industrial Automation, where we are active with professional services mainly in customer systems that are following various certification standards.

Our RTOS & Hypervisor PikeOS is well-known in the market as a reliable and certifiable operating system including virtualization and multi-core support.

Our solutions significantly reduce cost, space, weight, time-to-market for our customers. We guarantee a reliable, long-term supported operating system as basis for their innovative products.

SYSGO offers long-term support for devices that need to run more than 20 years. As an European company, our products have no export restrictions and are ITAR free.

→ **www.sysgo.com/about-us**

Security - A universal Requirement

New sophisticated attacks are being discovered every day. In our connected world, actually almost all industry sectors are affected and attacks can target industrial systems, IoT devices, financial institutes, military facilities, smartphones, medical equipment, air planes, trains or connected cars. Due to HW and SW advancements as well as pressure to reduce cost, there is an increasing desire to house multiple systems on a single platform meeting various and independent Security requirements.

May it be requirements for the Common Criteria (Information Technology), Security (ISO 15408), IEC 62443 for Industrial Control Systems, EDSA (Embedded Device Security Analysis) or J3061 in Automotive: We know how to meet all necessary requirements with a component-based software design.

→ **www.sysgo.com/cc**

PikeOS as secure OS

PikeOS is an RTOS (real-time operating system) that offers a separation kernel-based hypervisor with multiple partitions for many other operating systems and applications. It enables you to build devices for environments with strong demands for Safety and Security. PikeOS is compliant with the highest Safety standards for Avionics, Space, Railway, Automotive, Medical and Industrial Automation markets.

Due to its separation kernel approach it is the first choice for systems that demand protection against cyber attacks. In addition to the broad usage within millions of IoT and edge systems, it has also been deployed within various high critical communication infrastructures.

PikeOS brings together virtualization and real-time by means of unique and never seen before technologies. It allows you to migrate numerous complex embedded circuit boards in to a single hardware. It does not stop when it comes to new hardware concepts such as Big SoCs (System on a Chip) with multiple heterogeneous processor cores. Finally, when it comes to certification, SYSGO offers a dedicated certification kit in order to help you face the certification authorities.

PikeOS runs on several architectures and supports the following guest operating systems and APIs:

PikeOS native, ARINC 653 (aka APEX), POSIX, Linux (e.g. ELinOS)

→ **www.sysgo.com/pikeos**

ELinOS as secure Linux Distribution

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 653 partition, setting up 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 application running in another partition with a higher criticality.

Linux operating systems can be run in hardware (bare metal) as well in para-virtualized mode.

→ **www.sysgo.com/elinos**

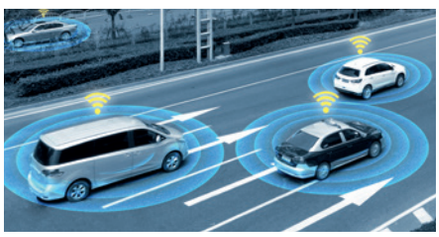
PikeOS Security Certification Kit

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

The Certkit is a bundle of evidence for a specific PikeOS version. It contains:

- Augmented Security Target
- Certificate
- Evaluation Technical Reports
- Interface Documents such as KERN-IF and PSSW-IF
- Safety Security Manual

The Certkit applies to the PikeOS Separation Kernel without BSP.



Secure Connectivity Platform

The platform utilizes a secure boot mechanism. Communication is assured by means of a Transport Layer Security (TLS) library. Cryptography and Storage is supported by executable binaries and configuration files that are digitally signed and stored on a secure Certified File System (CFS). The gateway's network Intrusion Detection System (IDS) is located within a separate partition, that monitors the network traffic.

→ www.sysgo.com/sacop

Video: Security Functionalities

→ www.sysgo.com/security

Secure Partition Communication
Dedicated communication channels can be defined by Queuing ports, Sampling ports or PikeOS file system.

Data Diode
Sometimes, data streams are intended to flow in one direction only, e.g. between partitions with different classification levels with the use of dedicated communication channels with uniform direction.

Health Monitoring
PikeOS contains an ARINC 653 compatible HM subsystem. The HM may detect several malfunctions such as memory violations, Processor exceptions, time partition violations, or error injections, etc

Secure Boot / Update & Chain of Trust
Building a chain of trust from trusted hardware to bootloader to PikeOS operating system to system partition and user partitions. A secure update can be supported with PikeOS. It is a start of the secure lifecycle with multiple software updates via local, wired or wireless update mechanisms, such as patches over the air. Secure update at PikeOS level can specifically target single partitions leaving the rest of the platform unchanged.

Other supported Use Cases

Transport Layer Security, Intrusion Detection System, Software Cryptography.

Common Criteria

Security standards are defined by the CC (Common Criteria), an international standard for Security requirements. The CC defines multiple levels of Security in the form of Evaluation Assurance Levels (EALs) from EAL 1 to 7 for the software development-specific requirements in regards to Security.

Approaches to enforcing Security must be layered and incremental to address an evolving environment populated by resource-ful attackers. Again, this applies to both military and commercial applications.

In 2022, PikeOS 5.1.3 has been certified according to the CC EAL 5+ level.

Partner Voice

"This partnership with one of the world's most innovative and certification experienced providers in the embedded technology is a win-win partnership for Karamba and SYSGO. We expect our collaboration on Host IDPS to improve both Karamba and SYSGO's status as leaders in embedded systems solutions for the rapidly-evolving connected car market."

Ami Dotan
Co-Founder and CEO
Karamba Security

Move. Unite. Excite.
We are SYSGO

Security-based Customers

- Astronautics (ATOS)
- Dassault Aviation
- IAI
- MBDA
- Powell
- Roche
- RUAG
- Selectron
- Thales
- Wabtec

MILS – Multiple Independent Levels of Security

Due to hardware and software advancements as well as cost containment pressures, there is an increasing desire to house multiple systems on a single platform that can meet diverse and independent Security requirements. This need led to the development of the MILS (Multiple Independent Levels of Security) architecture. While initially developed with defense systems in mind, MILS concepts are relevant to many different industry sectors that require Security from different types of threats to be managed in a cost-effective manner.

MILS offers a suitable architecture for applications as diverse as Medical, Industrial, and financial systems. Furthermore, MILS provides a framework to design and evaluate systems that can support multiple applications with various criticality on a single hardware platform. PikeOS can be used to implement systems following the MILS approach.

Whitepaper Download

We offer a wide range of whitepapers covering Safety & Security, secure updates for high assurance mixed-criticality systems, successful multi-core certification, and more.

→ www.sysgo.com/whitepapers

Security Partners

wolfSSL and SYSGO have teamed up to integrate wolfSSL's SSL/TLS crypto library into PikeOS. With this integration, wolfSSL also brings a FIPS crypto library to PikeOS Separation Kernel in a pre-integrated bundle that ensures robust, lightweight Security for your project's architecture.

→ www.sysgo.com/wolfssl

Karamba's software products protect connected embedded devices throughout their lifecycles in Automotive, Energy and Industrial Control systems. One product offers a runtime integrity technology (called XGuard) pre-integrated in selected SYSGO OS products starting with SACoP (SYSGO Secure Automotive Connectivity Platform). The software integrity is required in the UN ECE WP29 2020 regulation and thus a needed requirement.

→ www.sysgo.com/karamba

Products & Bundles

Products, Certification Kits, Bundles, BSPs

→ www.sysgo.com/products

Documents & Resources

Use Cases, Whitepapers, Articles, Press & Videos

→ www.sysgo.com/resources

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