SYSGO
EMBEDDING INNOVATIONS

Avionics Solutions
for Safe & Secure IMA and beyond

www.sysgo.com

SYSGO
EMBEDDING INNOVATIONS

#1 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

Integrated Modular Avionics – The Foundation for Aerospace Projects

The Integrated Modular Avionics (IMA) initiative is a set of standards and methods in order to replace divergent electronic airborne systems by standard components. The IMA concept targets both hardware and software and considers Safety aspects right from the start by following the according Safety standards.

Nowadays, IMA systems are present in modern aircrafts, such as the Boeing 777 and the Airbus A350. By reusing proven and tested components, IMA is considered to increase the overall Safety while being cost-effective.

The requirements defining the IMA operating system are described by the ARINC 653 standard. Major topics are virtualization and separation of applications, communication and health monitoring. The standard does not only address the configuration of an IMA system, but also provides an application programming interface (API) called APEX.

PikeOS: RTOS & Hypervisor

PikeOS is based on a microkernel with the performance of a traditional real-time operating system. This includes a hypervisor that provides partitions which can host different guest operating systems – from a simple yet highly critical control task to a full-fledged operating system like Linux. Customers can start with a platform development using RTOS and later add hypervisor functionality.

As a consequence, applications with mixed-criticality can coexist on the same platform. Complex systems, consisting of multiple devices in the past, can now be consolidated on a single hardware platform while assuring safe execution. This saves weight, energy consumption and reduces the bill of material. The PikeOS hypervisor runs on x86 as well as ARM or PowerPC and can easily be adapted to other CPU architectures.

PikeOS – ARINC 653 and beyond

PikeOS has been developed to be ARINC 653 compliant from the very beginning. The PikeOS DNA contains the ARINC standard's concepts, which includes the APEX API, resource and time partitioning (aka "virtualization"), queuing and sampling ports, as well as health monitoring. Moreover, PikeOS has been enhanced by elaborated details which go way beyond the original standard – some examples:

- Multiple APEX partitions may run inside the same virtual machine, which is also called "resource partition".
- Applications are not limited to the APEX API. Instead, a vast number of APIs are available; even entire guest OSs can be virtualized.
- The ARINC concepts of communication channels and health monitoring have been generalized in order to make those available to all supported guest OSs.
- Shared memory can be safely assigned to authorized resource partitions.
- The PikeOS configuration allows to decouple the assignment of resource partitions from time partitions, allowing to create more flexible systems compared to the original standard.
- The introduction of a special time partition allows to build priority-based systems. This enables highly reactive system as well as the usage of otherwise wasted computational power.
- Multi-core handling is neatly integrated into the time partition configuration management.

ARINC 664 – Avionics Networking

The IMA concept is not limited to a single computer system, it also covers networking between multiple machines. These days, full-duplex Ethernet with enhancement on redundancy and deterministic quality of service is being used.

The technology is described by the ARINC 664 (Part 7) standard. The benefit of using Commercial-off-the-Shelf (COTS) Ethernet components is to lower overall costs and obsolescence issues for the aircraft network. Hardware components, cables and test equipment for Ethernet are field-proven and much more affordable than the previously used Avionics-specific solutions. Ethernet itself won't meet Avionics network requirements.

Therefore, ARINC 664 extends the Ethernet standard by adding Quality of Service (QoS), redundancy and deterministic behaviour with a guaranteed dedicated bandwidth. This Avionics data network was first used in the Airbus A380 and A400M. Airbus and Boeing will extend the usage of ARINC 664 in future developments.

All of the mentioned aspects require a robust real-time operating system (RTOS) platform to allow applications to run in a safe and secure manner, meeting Safety standards like DO-178C. With PikeOS, developers have access to a hard real-time hypervisor-based on a separation kernel, which is certified to the DAL A level of the DO-178C Safety standard.

Use Cases

IMA (Integrated Modular Avionics), Graphics and GPU Compute, In-Cabin Entertainment System, AFDX® compliant Networks, Data Server in Cockpit, Primary Flight Display, ...

→ www.sysgo.com/avionics

Common Criteria & DO-356 – Security becomes an Objective

With the increasing connectivity of aircrafts, Security becomes an important topic for Avionics. As a consequence, the RTCA (Radio Technical Commission for Aeronautics) has released the new standard DO-356A: "Airworthiness Security Methods & Considerations", which is a practical guide for the implementation of Security within airborne electronic systems. This document refers to another well-known standard: "Common Criteria for Information Technology Security Evaluation (CC/CEM)". Although the CC/CEM were not developed for airborne systems, a mapping from DO-356 to Common Criteria can be defined.

Common Criteria (CC) is an international standard (IEC 15408) for computer Security certification and has evolved to be of widespread importance. Common Criteria defines a framework in which computer system users specify their Security requirements, vendors implement it and testing laboratories evaluate the products Security to determine if they actually meet the claims.

The PikeOS Separation Kernel Version 5.1.3 is currently the only Separation Kernel worldwide that holds a Common Criteria EAL5+ certification for its separation performance.

→ www.sysgo.com/cc

PikeOS for Avionics

Today's Avionics software applications are developed with respect to Integrated Modular Avionics (IMA). On the software side, IMA is backed by the ARINC 653 standard. SYSGO's PikeOS is not only fully compliant to ARINC 653, but also enhances the standard's philosophy with significant additions.

Talking about connectivity and SYSGO's implementation of the ARINC 664 standard, PikeOS is ready to take control of an aircraft's communication nodes, internally as well as to the outside world. With respect to that, Security has started to become an issue. Certification authorities have acknowledged the link between Security and Safety and with the DO-356 standard, they have built a bridge to the Common Criteria evaluation.

Modern computing is no longer conceivable without multi-core processing and those CPUs will appear in Avionics pretty soon. PikeOS has already included multi-core handling in its time partitioning management, addressing the major topics of the CAST-32A paper, such as cache interferences.

Customer Voice

"SYSGO offers a perfect complementary portfolio to our platforms with field-proven RTOSs and a unique software-based AFDX implementation that has already been DO-178B certified."

Patrizio Bollini
Marketing and Programs
Director at Sirio Panel

Move. Unite. Excite.
We are SYSGO

Avionics Customers

- Airbus
- Astrium
- DASSAULT
- Curtis-Wright
- Embraer
- ESA
- GosNIIAS
- KMW
- MBDA/LFK,
- Meggit
- RheinMetall
- Rockwell Collins
- SAFRAN
- Sirio Panel
- TAI
- Zodiac Aerospace

CAST-32A – Multi-Core ready to become Airborne

Single-core processors and controllers have been the de facto standard for Aviation software since the early beginnings when computers were utilized in flight systems. However, the development of electronic hardware has progressed and has led to more sophisticated and centralized systems like Integrated Modular Avionics (IMA). On the software side, this approach has been backed up by the introduction of operating systems that support robust time and resource partitioning.

With success of the partitioning model and multi-core processors becoming more present, the certification authorities have started to broaden their level of acceptance. Nowadays, both the EASA (European Union Aviation Safety Agency) and FAA (Federal Aviation Administration) give advice to implement multi-core systems which are compliant to the DO-178C standard. With regard to that, the Certification Authorities Software Team (CAST), an international group of certification and regulatory authority representatives (EASA, FAA), published a guideline named CAST-32A, describing the conditions, that would allow the use of multi-core processors in airborne systems.

With PikeOS, any multi-core scheduling use case can be seamlessly realized on a high abstraction level (“time partition schemes”). PikeOS itself is designed to satisfy any Symmetric Multiprocessing (SMP) and Asymmetric Multiprocessing (AMP) needs, while tooling even allows to build systems, that are in between. The PikeOS documentation progressively enters upon CAST-32A issues and guides the applicant to build compliant and robust systems, also in regard of IMA.

The most controversially discussed topic of CAST-32A is referenced as “Interference Channels and Resource Usage”. In PikeOS, the cache handling is implemented in a CPU hardware specific component, called Platform Support Package (PSP). Generally spoken, PikeOS PSPs provide enough flexibility to allow the partitioning of shared caches, e.g. by assigning different sets of a multiple-way associative cache to individual partitions, if supported by the hardware.

In order to be prepared for worst case scenarios, PikeOS provides the technical means to implement monitoring of the cache bandwidth in order to shut down erroneous applications. Apart from these technical methods applicable at runtime, the cache effects can be eliminated at architecture level.

For example: Applications can be ordered into groups with the same software level. By ensuring that Safety-critical processes are running in parallel, the cache can be invalidated at the start of the critical time frame.

Contention may also occur when applications executing on different cores are entering the kernel space at the same time, potentially accessing the same data structures. Traditionally, the access to the entire kernel memory is protected by a global lock, allowing only one core at a time to execute OS services. To reduce the impact of this kind of interference channel, PikeOS uses fine-grained locking, that significantly reduces the probability of applications requesting the same lock at the same time.

CAST-32A Whitepaper

→ www.sysgo.com/wp-cast32a

Products & Bundles

Products, Certification Kits, Bundles, BSPs

→ www.sysgo.com/products

Documents & Resources

Use Cases, Whitepapers, Articles, Press & Videos

→ www.sysgo.com/resources

Rel. 1.3 (PUBLIC) © 2022-11 by SYSGO GmbH. SYSGO, ELinOS, PikeOS, and CODEO are trademarks or registered trademarks of SYSGO GmbH. All other products, logos and service names are the trademarks of their resp. owners.