SYSGO
EMBEDDING INNOVATIONS

SACoP

Secure Automotive Connectivity Platform

The Secure Automotive Connectivity Platform relies on the PikeOS hypervisor technology and offers a base system that protects the critical internal vehicle infrastructure from the outside world by means of fire walling and intrusion detection systems. In addition, the platform is prepared for common use cases, such as an Over-The-Air (OTA) update mechanism and software life cycle management.
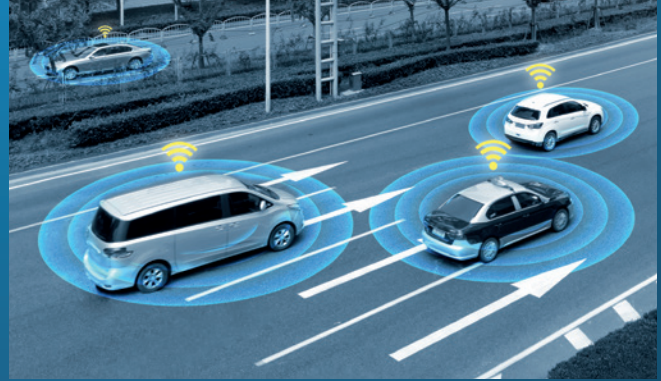
V2V

V2X

Safe and secure RTOS basis

Pre-configured Network Settings

Optional Guest OSs

Multi-Core Support

SACOP AT A GLANCE

- Component-based ready-to-use Automotive gateway

- Firewall to protect domains with variable degree of criticality

- Intrusion Detection System (IDS)

- Support for several networks, e.g. 4G/5G, Wi-Fi, Ethernet & CAN

- IPv6, VLAN and IP-multicast

- Over-The-Air (OTA) updates

- Certifiable File System (CFS) up to ASIL-B

- Safety certification to ISO 26262

- Security certification to CC EAL 5+

- Extendable with APIs for PikeOS Native, POSIX, Linux, AGL, ...

- Management APIs (configuration, monitoring, log, user parameters)

- Secure Boot & Fast Boot

- Microkernel based hard real-time operating system

- Embedded virtualisation

- All PikeOS supported architectures

- Eclipse-based IDE CODEO

- Large SW & HW ecosystem

ABOUT THE PLATFORM

Targeted to the Automotive industry, SYSGO offers a ready-to-use system for all communication needs involved in transportation. That includes Vehicle-to-Vehicle (V2V), and Vehicle-to-Infrastructure (V2X) as well as car internal communication. In particular the communication with the outside world requires deterministic and accurate response times that can only be achieved by means of an underlying real-time operating system.

The electronic systems inside a modern car are able to take control over critical systems, such as the steering and braking gear. This significantly improves the Safety during the operation of car, but at the same time exposes the risk of un-authorised access. As a consequence, the Safety of a vehicle must be accompanied by Security measures. Therefore, the connectivity platform contains a gateway utilising a robust routing system implementing a firewall and an intrusion detection system.

Especially in the Automotive industry, the frequency of model changes and functionality updates is extremely high. The list of desired features is growing year by year. This usually requires the combination of existing software components with completely new and partially incompatible application programming interfaces. Maintaining a stable software basis while being able to follow the desires of the end user is a challenge. This is where virtualisation comes into play. The connectivity platform is extendable easily by adding an arbitrary number of guest operating systems without compromising Safety or Security.

PikeOS is the backbone of the connectivity platform, as it naturally fulfils the substantial requirements of determinism and real-time, Security, Safety and virtualisation. As a Type 1 hypervisor, it directly runs on the embedded hardware and makes the overall system as performant as possible. Another performance boost comes through the multi-core support, which has proven its maturity in recent Railway projects.

P Learn more: www.sysgo.com/pikeos

www.sysgo.com

GATEWAY INTERFACES

In the example of a gateway, the supported default configuration communicates to the outside world by means of a 4G/5G network. A firewall protects the vehicle internal Wi-Fi hotspot, which is available to the passenger's convenience. The internal communication lines, such as CAN and Ethernet are available to the hotspot by means of dedicated and surveillance channels only. The gateway supports Virtual Local Area Networks (VLAN).

SECURITY

The platform utilises 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. In addition to Security aspects, this approach demonstrates the ability of PikeOS to resolve licensing issues by means of software isolation.

OVER-THE-AIR (OTA) UPDATES

The platform allows the update of software and firmware components of the entire system by means of secure communication via TLS (FIPS-certified). Update files are signed digitally.

CERTIFIED BASE SYSTEM

PikeOS 5.1.3 is certified according to Common Criteria EAL 5+ and certifiable up to ASIL D.
www.sysgo.com/common-criteria

CFS

• Certifiable File System (ASIL B)

AUTOMOTIVE API

• Crypto services
• Management API
• Secure Automotive communication API
• VLAN, IPv6, IP-multicast
• Router supporting firewall
• Secure OTA

IDS

• Network Intrusion Detection System
• Optional CAN Intrusion Detection System

SECURITY MAINTENANCE

• Security monitoring (CVE's)
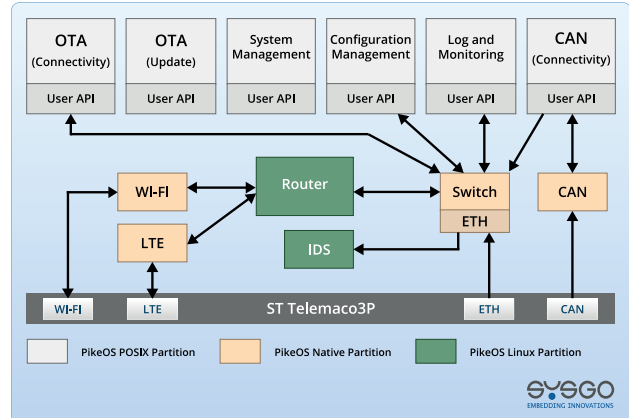• Long term support

Figure 1: Inter-Partition communication within the telematics gateway

OPTIONAL GUEST OPERATING SYSTEMS

Supported guest operating systems:
• PikeOS native • POSIX • AGL (Automotive Grade Linux)
• Linux (generic by means of hardware virtualization)

E ELinOS, SYSGO's robust Embedded Linux distribution: www.sysgo.com/elinos

BENEFITS

• Robust Automotive development platform with API compatibility to ELinOS, PikeOS native, POSIX or CFS
• Reduced time-to-market via:
  • Included pre-certified components according to ISO 26262 or Common Criteria EAL 5+ or FIPS
  • Pre-integrated Security components such as secure boot, IDS, TLS or CFS
  • Pre-configured network settings and infrastructure
  • Re-use of existing legacy code from previous projects
• Freedom of interference mechanisms with regards to safe/unsafe or secure/unsecure critical functions
• High performance in:
  • Fast system reaction (deterministic real-time behaviour)
  • Multi-core applications
  • Task scheduling

DEVELOPMENT & CONFIGURATION TOOL

CODEO is an Eclipse-based IDE and offers a complete environment for embedded systems covering the whole development cycle from early simulation and emulation tools to software update mechanisms for deployed systems.

C Learn more: www.sysgo.com/codeo

Founded in 1991, SYSGO became a trusted advisor for Embedded Operating Systems and is the European leader in hypervisor-based OS technology offering worldwide product life cycle support. We are well positioned to meet customer needs in all industries and offer tailor-made solutions with highest expectations in Safety & Security. More information at www.sysgo.com/sacop