SYSGO
EMBEDDING INNOVATIONS

SACoP

Secure Automotive Connectivity Platform

SYSGO is the European market leader in embedded real-time operating systems (RTOS) and has over 25 years of expertise in certifiable software, agile and responsive, with optional long-term support for all of our OS products. 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 update (OTA) mechanism and software life cycle management.

THE PLATFORM 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
- VLAN, 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 3+
- Extendable with APIs for PikeOS Native, POSIX, Linux, AGL, ...
- Management APIs (configuration, monitoring, log, user parameters)
- Secure Boot & Fast Boot
- Separation micro-kernel based hard real-time operating system
- Embedded virtualisation
- All PikeOS supported architectures
- Eclipse-based IDE CODEO
- Large software & hardware ecosystem
- Long term support

THE SECURE AUTOMOTIVE CONNECTIVITY PLATFORM

Targeted to the Automotive industry, SYSGO offers a complete and 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.

The PikeOS operation system has been chosen as the backbone of the Secure Automotive 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.

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 Hypervisor, certified according to Common Criteria EAL3+ and certifiable up to ASIL-D.

Read more → 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

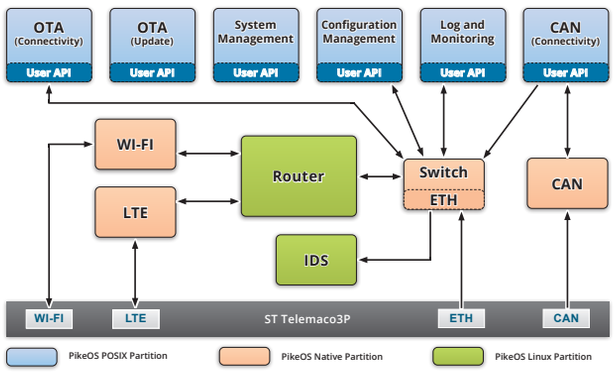

Figure 1: Inter-Partition communication within the telematics gateway

OPTIONAL GUEST OPERATING SYSTEMS

The platform supports the integration of the following guest operating systems:

- PikeOS native
- POSIX
- Linux (generic by means of hardware virtualization)
- AGL (Automotive Grade Linux)
- ELinOS, SYSGO's robust Embedded Linux distribution

DEVELOPMENT AND CONFIGURATION TOOLS

Developing embedded applications for a partitioned system requires a state-of-the-art cross-development tool chain, well designed and easy to use configuration tools, remote debugging with OS awareness (thread states, virtual address mappings, etc.), target monitoring, remote application deployment, and timing analyses tools. With CODEO, the Eclipse-based IDE, SYSGO offers a complete environment for embedded systems covering the whole development cycle from early simulation/emulation tools to software update mechanisms for deployed systems.

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 3+ 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
- Enabled freedom from interference mechanisms with regards to safe/unsafe or secure/unsecure critical functions
- High performance in:
  - Fast system reaction time via deterministic real-time behaviour
  - Multi-core applications
  - Task scheduling

Find more information also at www.sysgo.com/automotive

SYSGO Headquarters
Phone +49 6136 9948 500
sales-de@sysgo.com

SYSGO France
Phone +33 1 30 09 12 70
sales-fr@sysgo.com

SYSGO Czech
Phone +420 222 138 111
sales-cz@sysgo.com

SYSGO EMBEDDING INNOVATIONS