Using Hypervisor Technology to Secure Automotive Connectivity

Jose Almeida, Director Automotive Business Line
jose.almeida@sysgo.com

Embedded World
25 February 2020 - Nuremberg
DEVELOPING LOCALLY
ACTING GLOBALLY

- SYSGO is the leading European operating system vendor for embedded systems.
- As a trusted advisor, we provide safe and secure technologies and services to be part of high-end software solutions in any IoT device worldwide.
- Founded in 1991 – more than 29 years experience in certification of safety critical systems
- Member of the Thales Group
PRODUCTS AND SERVICES

As the leading European manufacturer of embedded operating systems, we have supported safety and security critical applications in the aerospace, automotive, railway and IIoT industries for more than 25 years. We work closely with our customers throughout their product life cycle.

**PikeOS®**  
Separation Kernel based RTOS with integrated and certified virtualization technology (Hypervisor)

**ELinOS**  
Industrial grade Linux Distribution for embedded systems with real-time extensions

**Board Support Packages**  
Adaptation to the selected architecture, board specific initialization and drivers

**Certification Kits**  
Extensive collection of certification artefacts for all major generic and industry-specific standards

**Professional Services**  
We make sure customers can optimize use our technology from prototyping to certification

(C) 2020 SYSGO GmbH | www.sysgo.com
PikeOS
Certified RTOS & HV

- **Hard Real-Time Operating System and Hypervisor**
  - With safe and secure virtualization, mixed criticality with multiple guest operating systems and highly portable, supporting all important CPU architectures

- **Guest operating systems**
  - Can run in parallel partitions on a single or multicore processor to serve specific use cases,

- **Mixed criticality**
  - Strict spatial and time partitioning

- **Eclipse based CODEO**
  - A comprehensive integrated development environment supporting C/C++

- **Without any export restriction**
Different Security Needs

Data Security – Privacy

Security for Safety
CONNECTED CAR – ATTACK SURFACE ELDORADO
OTHER PERSPECTIVE
LEARNING FROM IT SECURITY
• Network Isolation (Physically or VLAN based)
• Dedicated Access Control for Critical Services
  • Dedicated gateways
  • Diversification of HW & SW
• DMZ
• Proxy
  • Protocol Break
• Dedicated Gateway Server for Each Service
  • Outbound traffic vs Inbound traffic
• Intrusion Detection System
  • You need to monitor what happens
What is a Connectivity Gateway?
Traditional Linux Based Approach

- Limited access control capabilities
- No STRONG separation between Applications
- Large code base, impossible to audit
- No separation between drivers

User (user mode)

Kernel (supervisor mode)

SoC / Custom Hardware

Target Boot Loader

Monolithic Linux kernel

Applications

Drivers

CPU1
Serial
CAN
Hardware
Ethernet
HSM
Storage
But More and More Features Needed
Linux Approach Still Works
But …

• Who develops the different applications?
  • What happens when integration applications developed by different companies (who takes care of the final integration)
  • What are the interferences between the applications? And who can control the interferences?

• What is the life cycle of these applications?
  • For safety and security reasons each application may have its own life cycle.

• How to test the system?
  • What are the applications dependencies to middleware’s or libraries?
  • How many packages are installed when building Yocto Linux?
HYPERVISOR
SECURE
COMMUNICATION
KEY FEATURES
Security by separation

- **PikeOS Native Guest**
- **Posix Guest**
- **Linux Guest**
- **Mixed Guest OS (POSIX, Linux, Native)**

**User (user mode)**
- User level Drivers
  - Ethernet Driver

**Kernel (supervisor mode)**
- Strong Static Separation
- Shared Drivers
- PikeOS Native Guest
- Posix Guest
- Networking
- HSM Driver
- Storage Driver

**SoC / Custom Hardware**
- CPU1
- Serial
- CAN
- Ethernet
- HSM
- Storage

**Target Boot Loader**

**Small code base, ISO 26262 & CC Certified**

**PikeOS Safe and Secure Separation Kernel and Hypervisor**

**Strong Static Separation**

**Mixed Guest OS (POSIX, Linux, Native)**

**Statically Defined communication Channels**

**Security by separation**
• Usage of different run-time environments
• Limit HW direct hardware access
• Statically Configured Communication Flow
• User level drivers
• Protocol break between for certain communications

Hypervisor Based Software Diversification
Reduce Common Vulnerability Risk
Run-time Environment Separation
Indirect interactions between applications

- Dedicated Guest OS per function
- Minimal environment matching functional need
- No common framework between each Guest OS
- Simplify update of each function

Cloud Connectivity (AWS, Azure, Custom)
HWVirt Yocto Based Linux
HWVirt ELinOS (Linux)

IDS
HWVirt ELinOS (Linux)

Router/Firewall

(C) 2020 SYSGO GmbH | www.sysgo.com
Traffic control
Software Network Switch
Traffic control
Software Network Switch

- Isolated in a PikeOS partition
- Static configuration
- Configurable number of ports
- Per port mirroring capability
- Routing based on VLAN + IP
- Support for VLAN
  - VLAN tagging may be forced per channel
    - Incoming traffic
    - Outgoing traffic
  - VLAN tagging may be set outside of the switch when supported by external elements
Software Switching Usage

Example
Hardware Support
ARMv8 Execution Privileges

Secure World
- User Mode (EL0)
- Supervisor Mode (EL1)

Normal World
- User Mode (EL0)
- Supervisor Mode (EL1)
- Hypervisor Mode (EL2)

Monitor Mode (EL3)
Take away

- Secure Hypervisor Provides Security Foundation
- Enables Implementing on a SOC Traditional IT Security Policy
- Enforce Multiple Barriers Policies
- Enables Integration of Security Frameworks (IDS)
- Support Increase Number of Application Hosted in a Gateway
  - Independence Between Applications
  - Integration strategy
  - Facilitate Independent Testing
- Hardware Software Coupling is key for the System Security