Hypervisor Market Overview

Franz Walkembach

for GENIVI® AMM, April 19th, 2018 (Munich)
Hypervisor Market Overview
What you can expect

- Quick introduction of SYSGO AG
- What are the market trends for hypervisor?
- Market size and main vendors
- Which use cases can be addressed?
- Which Hypervisor types are visible in the market?
  - With focus on MMU (less MPU)
- Which impact on Certification in automotive?
- Summary & Outlook
SYSGO AG
Embedded Software Technology Leader

Mission
“Be the leading European Operating System provider for devices in the Internet of Things: wherever safety and security matter, certified whenever needed.”

Founded 1991 (Mainz, Germany)
>80% Engineers have safety certification competences
Since 2012 independent entity from the Thales Group

Local Facilities in Germany, France, Czech Republic, UK

Global Worldwide distribution and support network
The Market - Automotive Market Trends

Security is not an option – Security is an integral system property

**ECU Consolidation**
- Safety/Security
- Interconnect: CAN, LIN, FlexRay, ETH
- Certification

**Virtual ECU**
- Safety/Security
- Certification
- High performance

**Cluster**
- High Safety
- High Security
- High Real-Time
- High Graphics
- Fast Boot
- Certification

**ADAS/Gateway**
- High Safety & Security
- Artificial Intelligence
- High Real-Time
- Low/No Graphics
- High Image Processing
- AUTOSAR
- Certification

**IVI**
- Low Safety
- High Security
- Medium Real-Time
- High Graphics
- High Connectivity
- Open OS (Android, Linux)
- No Certification
Hypervisor Market Overview
Global Market Overview

* Global Revenue of Embedded Hypervisors & Secure Operating Systems and Related Services (Millions of Dollars)
Source: VDC Research, 2016
Hypervisor Market Overview
Main vendors visible in the embedded market

<table>
<thead>
<tr>
<th>Open source</th>
<th>Proprietary</th>
</tr>
</thead>
<tbody>
<tr>
<td>• EPAM on XEN</td>
<td>• DDC-I (DEOS)</td>
</tr>
<tr>
<td>• General Dynamics (Oklabs)</td>
<td>• eSOL (eT-kernel)</td>
</tr>
<tr>
<td>• HIS (Wittenstein OpenRTOS)</td>
<td>• Greenhills (Integrity)</td>
</tr>
<tr>
<td>• Intel ACRM</td>
<td>• Harman/Samsung (Red Bend)</td>
</tr>
<tr>
<td>• Kernkonzept</td>
<td>• LynxOS</td>
</tr>
<tr>
<td>• KVM Linux</td>
<td>• Mentor Graphics (Nucleus)</td>
</tr>
<tr>
<td>• Micrium (Micro COS3)</td>
<td>• Open Synergy (COQOS)</td>
</tr>
<tr>
<td>• Siemens Jailhouse</td>
<td>• Perseus 64bit on ARM</td>
</tr>
<tr>
<td>• Sierraware on ARM</td>
<td>• QNX (Neutrino)</td>
</tr>
<tr>
<td>• Real-time Linux</td>
<td>• Real-time Systems</td>
</tr>
<tr>
<td>• Perseus 32bit on XEN</td>
<td>• SYSGO AG (PikeOS)</td>
</tr>
<tr>
<td>• XEN-project</td>
<td>• Wind River (VxWorks 653)</td>
</tr>
</tbody>
</table>
Hypervisor Market Overview
What is a Hypervisor?

- Virtual Machine Monitor
- Runs one or more virtual machines
- Each virtual machine is called a guest machine or personality
- Has a guest operating systems with a virtual operating platform
- Manages the execution of the guest operating systems

Acc. To Wikipedia
Hypervisor Market Overview
Hypervisor main use cases in automotive 1/2

- **Space / Weight / Power reduction by consolidation**
  - e.g. digital cluster and IVI on one hardware
- **Re-use of legacy code**
  - Use existing code of ECUs for new projects
- **Fast boot / Secure boot**
  - Boot via RTOS to get early access on e.g. CAN network
- **Configuration of Personalities**
  - Running open source stacks (Android/Linux) and/or RTOS in different partitions
  - Configure time schedules and memory allocation
Hypervisor Market Overview
Hypervisor main use cases in automotive 2/2

• Safety use cases
  • Define and separate safe from un-safe partitions

• Security use cases
  • Define communication flow and separate un-secure partitions

• Use of open source in a safe and secure environment
Hypervisor Market Overview
Some basics

- Emulation
- Applications running directly on hypervisor
- Fully virtualized OS with applications
- Para virtualized OS with API
Hypervisor Market Overview

Emulation

- Complete hardware emulation
- Different hardware platforms can be emulated
- Main drawbacks:
  - performances impacted
  - I/O are emulated
  - MMU is emulated
  - all in supervisor mode is emulated, …
- Ex.: Bochs, Qemu, …
Hypervisor Market Overview
Classical virtualization

- Hardware virtualization but without any processor emulation
  - target processor must be identical to virtualized processor
- Allow some Operating Systems (Guest OS) to be hosted with no modification
- Main drawbacks: same as emulation
- Ex.: VMWare, VirtualBox, Adeos, …
Hypervisor Market Overview
Para-virtualization

- GuestOSs must be adapted
- How to communicate safely between Operating Systems?
- Need to host a Real-Time Kernel as a GuestOS when real-time is required
  - some solutions do not offer real-time support at all with a micro-kernel
- Main drawbacks:
  - no hard real-time support possible
  - solution barely suitable for critical embedded systems, …
- Ex.: XEN, z/VM, VLX, …
Hypervisor Market Overview
Example of Space Separation

Security by separation and controlled information flow

Privileged Partition
- Restart/Shutdown
- Direct Mapping of Physical Resources
- Change Scheduling

Hypervisor

MMU
Map Memory to Partitions

No Error Propagation

Guaranteed Access to Assigned Resources

Connectivity
Linux

HMI
Android

Early Boot
CAN-Bus

System Part. Health Mon. CBIT
Native

Address Space

Static Configuration of OS Resources

IOMMU
Memory access for DMA Devices
Hypervisor Market Overview
Time Partitioning

A) Priority based scheduler
• Static or dynamic configuration of:
  • Execution order
  • Duration
• Deterministic Hard Real-time
• Shortest response time
  • Dedicated thread with superior priority
• Best possible CPU usage

B) Cyclic scheduler
• E.g. Round Robin
Hypervisor Market Overview
Multiplexed Virtual Serial

- Every virtual board has access to serial port
  - On Intel with emulated devices, other arches with stub drivers
- IDE can show all tabs
  - IO to each guest individually
- Easy way of bringing up guests
Hypervisor Market Overview

Linux based hypervisor

Abbildung 3.1-1: Aufbau von RT-Linux
Hypervisor Market Overview

Hypervisor versus Linux Containers

- Hypervisor allows real-time with a virtual machine monitor (Note: Linux containers do not protect from user to kernel privilege escalation attacks)
- It allows Linux or other OS to run in one of the partitions as a guest OS
- It virtually allows that any and all real-time tasks have priority over Linux kernel tasks
- Secure boot scenarios are possible with low boot times

* Another Linux or Android OS
System Safety
Software Standards for Safety Related Systems

International (Generic)
- IEC 61508(-3)
  Functional safety of electrical / electronic / programmable electronic safety related systems
- ISO/IEC 15504
  SPICE / Automotive SPICE
- ISO/IEC 12207
  Software lifecycle processes

Medical
- IEC 62304
  Software for medical equipment

Process Industry
- IEC 61511
  Safety systems for the process industry sector

Avionic
- DO 178B/C
  Software considerations in airborne systems

Machines
- ISO 13849
- IEC 62061
  Machine safety

Railway
- EN 50128
  Software for railway equipment

Nuclear Power
- IEC 60880
  Nuclear plants – Software aspects of process control

Gas Detection
- EN 50271
- EN 50402
  Functional safety of gas measurement and detection equipment

Automotive
- ISO DIS 26262-6/-8
  Functional safety of “road vehicles”
Compliance to the ISO 26262 SW Phase Model

NOTE: Within the figure, the specific clauses of each part of ISO 26262 are indicated in the following manner: "m-n", where "m" represents the number of the part and "n" indicates the number of the clause, e.g. "4.7" represents Clause 7 of ISO 26262-4.
Hypervisor Market Overview
Summary & Outlook

- Hypervisors have a major play in safe and secure embedded systems
- Wide set of use cases are possible
- There are many different HV variants
- Automotive market is just starting to use HV
- The market density of hypervisor vendors is increasing
- They are often combined with an RTOS offering (partially included)
- Hypervisors vary on
  - Supported architectures and number of BSPs
  - Time and/or space separation
  - MMU or MPU support
  - Feature details and specification
  - Configuration in the tool chain
  - Supported levels of safety and security software standards
Hypervisor Market Overview
Questions?

Franz Walkembach
VP Marketing & Product Strategy

focal.auto@sysgo.com

Contact
SYSGO AG
Am Pfaffenstein 14
55270 Klein-Winternheim
Germany
Phone: +49 6136 9948-0
sales-de@sysgo.com

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

SYSGO S.A.S.
Phone: +420 222 138 111
sales-cz@sysgo.com

SYSGO s.r.o.