Agenda

Ecosystem Overview
Xen Project Capabilities and Challenges
The Elephant in the Room: Safety Certification
Examples: Defense/Embedded

**OpenXT**
www.openxt.org

FOSS Platform for security research, security applications and embedded appliance integration building on Xen & OpenEmbedded

Part fork of Xen Project, but significant effort to un-fork has started in 2017.

**Several key players:** AIS, Apertus Solutions, BAE Systems, U.S. Air Force Research Laboratory

**Virtuosity**
dornerworks.com

Consultancy with embedded/avionics/medical focus. Maintains Virtuosity Hypervisor with support for a XILINX and NXP Arm SoCs.

**Product variant of Virtuosity for defence/avionics use-cases.** 2nd generation product (predecessor = ARLX released in 2015).

- **Certification packages for:** DO-178, IEC 62304, ISO 26262
- **Standards:** ARINC 653, Vehicular Integration for C4ISR/EW Interoperability (VICTORY), Future Airborne Capability Environment (FACE™)

**XenZynq**
xilinx.com

Xen Zynq Distribution originally developed by Dornerworks. Latest product incarnation is called Virtuosity Hypervisor.

Investing in Xen Functionality related to power management and managing heterogeneity in general.
Examples: Automotive

**EPAM**
epam.com

Product: **Fusion**
Scalable & secure software deployment platform for distributed (cloud+vehicle) automotive service products. Uses isolated Xen VM in vehicles to deploy service containers.

**Ongoing Contributions:**
- PV drivers: input, sound & DRM
- Xen OP-TEE support
- Co-processor (GPU) sharing framework
- Hard real-time support research
- Power Management & HMP
- RTOS Dom0 / Dom0-less system
- Safety certification

**GlobalLogic**
globallogic.com

Product: **Nautilus**
Pioneered Xen based automotive solution. Used to be very active within the Xen Project from 2013 - 2016, but recently has been primarily product focused.

**Misc**
Automotive vendors that occasionally contribute to and engage with the Xen Project.

**Renesas**
HW enablement in Xen. Test Platforms for Xen Project CI.

**Bosch Car GmbH**
Code Contributions since 2015

**LG, ADIT, Samsung**
Not much information
Agenda

Ecosystem Overview

Xen Project Capabilities and Challenges

The Elephant in the Room: Safety Certification
## Automotive Requirements vs. Xen Project

### Compute Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Xen Project</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>C1</strong>: Static resource partitioning and flexible on-demand resource allocation (CPU, RAM, GPU and IO)</td>
<td>Core functionality, multiple schedulers, GPU/co-processor sharing, memory ballooning, etc.</td>
</tr>
<tr>
<td><strong>C2</strong>: Memory/IO bus bandwidth allocation and rebalancing</td>
<td><strong>WIP</strong>: Effort by several parties to enable Hard RT support on Xen</td>
</tr>
</tbody>
</table>

### Peripherals Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Xen Project</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>P1</strong>: GPU and displays shall be shared between execution environments supporting both fixed (each one talks to its own display or to a specified area on a single display) and flexible configurations (shape, z-order, position and assignment of surfaces from different execution environments may change at run time).</td>
<td>Via GPU sharing (and <strong>WIP</strong> co-processor sharing), PV Drivers (PV DRM)</td>
</tr>
<tr>
<td><strong>P2</strong>: Inputs shall be routed to one or multiple execution environments depending on current mode, display configuration (for touchscreens), active application (for jog dials &amp; buttons), etc.</td>
<td>Via PV Drivers (PV KBDFRONT)</td>
</tr>
<tr>
<td><strong>P3</strong>: Audio shall be shared between execution environments. Sound complex mixing policies for multiple audio streams and routing of dynamic source/sink devices (BT profiles, USB speakers/microphones, etc.) shall be supported.</td>
<td>Via PV Drivers (PV SOUND)</td>
</tr>
<tr>
<td><strong>P4</strong>: Network shall be shared between execution environments. Virtual networks with different security characteristics shall be supported (e.g., traffic filtering and security mechanisms).</td>
<td>Via PV Drivers &amp; Disaggregation Xen Security Modules</td>
</tr>
<tr>
<td><strong>P5</strong>: Storage shall support static or shared allocation, together with routing of dynamic storage devices (USB mass storage).</td>
<td>Via PV Drivers</td>
</tr>
</tbody>
</table>
## Automotive Requirements vs. Xen Project, continued

<table>
<thead>
<tr>
<th>Security Requirements</th>
<th>Xen Project</th>
</tr>
</thead>
</table>
| **SE1**: Root of Trust and Secure boot shall be supported for all execution environments.| x86: TPM 2.0, Intel TXT, AMD SVM  
Arm: supported with OPTEE |
| **SE2**: Trusted Computing (discrete TPM, Arm TrustZone or similar) shall be available and configurable for all execution environments. | x86: in Xen; some extras in OpenXT  
Arm: OPTEE (WIP: up streaming) |
| **SE3**: Hardware isolation shall be supported (cache, interrupts, IOMMUs, firewalls, etc.). | Core functionality (except firewalls) |

<table>
<thead>
<tr>
<th>Safety Requirements</th>
<th>Xen Project</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SA1</strong>: System monitoring shall be supported to attest and verify that the system is correctly running.</td>
<td>Can be implemented through VMI in Hypervisor, agents outside or through a hybrid</td>
</tr>
<tr>
<td><strong>SA2</strong>: Restart shall be possible for each execution environment in case of failure.</td>
<td>Core Functionality</td>
</tr>
<tr>
<td><strong>SA3</strong>: Redundancy shall be supported for the highest level of fault tolerance with fall-back solutions available to react in case of failure.</td>
<td>WIP: This has to be analysed in scope of &quot;safety certification&quot; initiative, as well as &quot;dom0-less&quot; Xen and &quot;minimal&quot; Kbuild</td>
</tr>
<tr>
<td><strong>SA4</strong>: Real time support shall be guaranteed together with predictive reaction time.</td>
<td>Different scheduler options with different trade-offs. WIP: Benchmarks with recommendations and Hard RT support.</td>
</tr>
</tbody>
</table>
## Automotive Requirements vs. Xen Project, continued

<table>
<thead>
<tr>
<th>Performance and Power Consumption Requirements</th>
<th>Xen Project</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PP1:</strong> Virtualization performance overhead shall be minimal: 1-2% on CPU/memory benchmarks, up to 5% on GPU benchmarks.</td>
<td>Arm: fulfils requirements x86: not verified</td>
</tr>
<tr>
<td><strong>PP2:</strong> Predictability shall be guaranteed. Minimal performance requirements shall be met in any condition (unexpected events, system overload, etc.).</td>
<td>Different scheduler options with different trade-offs. Benchmarks with recommendations in progress. Possibly some code changes will be up streamed.</td>
</tr>
<tr>
<td><strong>PP3:</strong> Execution environments fast boot: Less than 2 seconds for safety critical applications, less than 5 seconds for Instrument Cluster, and 10 seconds for IVI. Hibernate and Suspend to RAM shall be supported.</td>
<td>Arm: Proven by both GlobalLogic and EPAM</td>
</tr>
<tr>
<td><strong>PP4:</strong> Execution environments startup order shall be predictable.</td>
<td>Core functionality</td>
</tr>
<tr>
<td><strong>PP5:</strong> Advanced power management shall be implemented with flexible policies for each execution environment.</td>
<td>Arm: Partially implemented (not yet up-streamed). Further work by EPAM, XILINX and Aggios planned.</td>
</tr>
</tbody>
</table>
Agenda

Ecosystem Overview
Xen Project Capabilities and Challenges
The Elephant in the Room: Safety Certification
Our Approach for now:
Make it easier for down-streams to Safety Certify

**Stage 2:**
Create shared certification artefacts under the guidance/with support from certification partner. Adapt development processes, where feasible.

**MISRA Compliance**
1. Identify compliance partner that is willing to work with the project ➔ PROA
2. WIP: Formalize relationship between vendor and the project
3. Iteratively address compliance issues within the Xen Project community: start with potentially controversial and high impact issues.
4. Complete MISRA compliance work for majority of issues.

**Dom0**
RTOS (e.g. FreeRTOS) as Dom0, or Dom0-less stack with minimal management tools.

**Lead Community Member**
- EPAM
- Dorrnerworks as collaborator

**Minimal Xen**
Create minimal Kbuild for Xen as a reference, using Renesas R-Car as starting point.

**Lead Community Member**
- Stefano Stabellini
- EPAM, Dorrnerworks, XILINX and others as collaborators

**Certification Partners**
1. WIP: Identify possible certification partners and understand the framework they are willing to work with.

   **Note:** Dornerworks is a possible partner given past certification experience on Xen

2. Formalize relationship between vendor and the project

   Reliable data about achievable minimal code size and community challenges that need to be resolved.

   **Note:** Dom0 and Minimal Xen do not need to be complete to get sufficient data.
Code Size: Where are we starting from

**Arm**

Full ARM 64 and 32 bit, with **everything** enabled.

<table>
<thead>
<tr>
<th>Components</th>
<th>K SLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>/xen/common</td>
<td>33.4</td>
</tr>
<tr>
<td>/xen/arch/arm</td>
<td>19.8</td>
</tr>
<tr>
<td>/xen/drivers</td>
<td>16.0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>69.3</strong></td>
</tr>
</tbody>
</table>

Xen on ARM64 with ACPI (used in servers) and ARM32 disabled is **~60K SLOC** today.

**Future:**

A minimal Xen configuration for a small set of boards should be in the order of **40K to 50K SLOC**, smaller if common code can be aggressively removed via Kconfig.

**x86**

On x86 Xen, there is little configurability today, but

<table>
<thead>
<tr>
<th>Calculation</th>
<th>K SLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>x86 with everything enabled</td>
<td>325</td>
</tr>
<tr>
<td>x86 PVH for Intel only, no server features</td>
<td>128</td>
</tr>
</tbody>
</table>

However, the **128K SLOC** figure includes most Intel SKUs. Focusing on the latest hardware only should reduce this significantly.

**Cost Example:** DO-178C, 45K SLOC

- DAL E (0.11 h/SLOC): ~2.4 man years ... ASIL-A
- DAL C (0.20 h/SLOC): ~4.5 man years ... ASIL-B/C
- DAL A (0.67 h/SLOC): ~15 man years ... ASIL-D

Hours for vendor with certification experience

**Perspective:** Total Xen Community Dev Effort

2014 - 2017: ~41 to ~50 man years per year

*Using conservative COCOMO model*