GENIVI®

Xen Project Automotive and Embedded Overview

April, 2018

Lars Kurth

Chairman, Xen Project Advisory Booard

Agenda

Ecosystem Overview

Xen Project Capabilities and Challenges

The Elephant in the Room: Safety Certification

GENIVI®

SOFTLAYER an IBM Company
ORACLE CLOUD
Amazon Lightsail
kt
CITRIX
SUSE
ORACLE
amazon web services
Tencent 腾讯
HUAWEI
inspur 浪潮
rackspace the open cloud company
DATAPIPE
Alibaba Cloud aliyun.com
ZEDEDA
NXP
XZD XENZYNQ DISTRIBUTION
CISCO
Bitdefender
DORNERWORKS
epam
ais
Xen Project
atihita
GlobalLogic
Bromium
aggios
BAE SYSTEMS
OpenXT
QUBES OS A REASONABLY SECURE OPERATING SYSTEM
AFRL THE AIR FORCE RESEARCH LABORATORY LEAD | DISCOVER | DEVELOP | DELIVER
CRUCIBLE
ais
XILINX
TRIITUS CORPORATION
BAE SYSTEMS
galois

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**.

GENIVI®

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

GENIVI®

Agenda

Ecosystem Overview

Xen Project Capabilities and Challenges

The Elephant in the Room: Safety Certification

Automotive Requirements vs. Xen Project

Compute Requirements	Xen Project
C1: Static resource partitioning and flexible on-demand resource allocation (CPU, RAM, GPU and IO)	Core functionality, multiple schedulers, GPU/co-processor sharing, memory ballooning, etc.
C2: Memory/IO bus bandwidth allocation and rebalancing	**WIP:** Effort by several parties to enable Hard RT support on Xen

Peripherals Requirements	Xen Project
P1: 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).	Via GPU sharing (and **WIP** co-processor sharing), PV Drivers (PV DRM)
P2: Inputs shall be routed to one or multiple execution environments depending on current mode, display configuration (for touchscreens), active application (for jog dials & buttons), etc.	Via PV Drivers (PV KBDFRONT)
P3: 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.	Via PV Drivers (PV SOUND)
P4: Network shall be shared between execution environments. Virtual networks with different security characteristics shall be supported (e.g., traffic filtering and security mechanisms).	Via PV Drivers & Disaggregation Xen Security Modules
P5: Storage shall support static or shared allocation, together with routing of dynamic storage devices (USB mass storage).	Via PV Drivers

GENIVI®

Automotive Requirements vs. Xen Project, continued

Security Requirements	Xen Project
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)

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

GENIVI®

Automotive Requirements vs. Xen Project, continued

Performance and Power Consumption Requirements	Xen Project
PP1: Virtualization performance overhead shall be minimal: 1-2% on CPU/memory benchmarks, up to 5% on GPU benchmarks.	Arm: fulfils requirements x86: not verified
PP2: Predictability shall be guaranteed. Minimal performance requirements shall be met in any condition (unexpected events, system overload, etc.).	Different scheduler options with different trade-offs. Benchmarks with recommendations in progress. Possibly some code changes will be up streamed.
PP3: 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.	Arm: Proven by both GlobalLogic and EPAM
PP4: Execution environments startup order shall be predictable.	Core functionality
PP5: Advanced power management shall be implemented with flexible policies for each execution environment.	Arm: Partially implemented (not yet up-streamed). Further work by EPAM, XILINX and Aggios planned.

GENIVI®

Agenda

Ecosystem Overview

Xen Project Capabilities and Challenges

The Elephant in the Room: Safety Certification

GENIVI®

Our Approach for now:

Make it easier for down-streams to Safety Certify

MISRA Compliance

1 Identify compliance partner that is willing to work with the project ➜ PRQA

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.

Dom0

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

Lead Community Member

- EPAM
- Dornerworks 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, Dornerworks, 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*

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*

2 Formalize relationship between vendor and the project

4 Complete MISRA compliance work for majority of issues.

Stage 2:

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

Code Size: Where are we starting from

Arm

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

Components	K SLOC
/xen/common	33.4
/xen/arch/arm	19.8
/xen/drivers	16.0
Total	**69.3**

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

Calculation	K SLOC
x86 with everything enabled	**325**
x86 PVH for Intel only, no server features	**128**

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

GENIVI®

Thank you!

Visit GENIVI at http://www.genivi.org or http://projects.genivi.org

Contact us: help@genivi.org