ACRN/KATA:
Secure Container Solution for Software-defined Cockpit

Jason Chen, Intel SSP
What is ACRN™ - The Big Little Hypervisor for IOT

A flexible, open-source, lightweight hypervisor for IOT workload consolidation

A Linux Foundation Project Launched in March 2018

https://projectacrn.org
Agenda

- ACRN Introduction
- Challenge from Vehicle Development
- Vision: Solution and Use Cases
- ACRN/Kata on Vehicle
Value Proposition

**Small Footprint**
- Optimized for IOT class solutions
- Significantly smaller footprint than datacenter targeted hypervisors

**Heterogeneous Workloads Consolidation**
- Real time & Non-Real time
- Functionally Safe & non-safe

**Open-source with Flexible Licensing**
- BSD license enables proprietary Guest OS
- True Open source with a vibrant Community
ACRN 1.0

Ready for Production
- Released in May 2019

Key Features
- Safety and Security Isolation (Cluster + IVI)
- Extensive Sharing Capabilities
  - Graphics, media, USB, audio, camera etc.
  - Advanced DMA/graphics buffer sharing
- Multiple OS Support
  - Clear Linux, Yocto, Ubuntu
  - Android, AGL, AliOS
- MISRA-C Compliance
Challenge – Complex Software

Explosion in Software Lines of Code
- Today vehicle 100M lines of code
- Near future vehicle 200M – 300M lines of code
- Up to 1 billion lines of code for level 5 auto driving

Varieties of Software Category
- Instrument cluster, In-vehicle Infotainment, ADAS, V2V...
- Various execution environment – SOCs, OSs..

The Trends:
Consolidation based on Virtualization and Containerization
Challenge – Safety and Security

Safety
- Functional Safety
- Mixed-Criticality
- Fault Detection and Tolerance

Security
- Untrusted applications
- Secret protection

The Trends:
Multi-nodes, safety separation, secure/isolated execution environment
Challenge – Software Update & Deployment

**Frequently Update**
- Improved Performance Every Day
- Minimizes Security Risks

**Dynamic Deployment**
- Cabin Connectivity
- Remote Updating Service

**The Trends:**
Containerization, Orchestration, Cloud/Edge Connectivity
Solution

Secure Container

+  
Orchestration

+  
Multiple Compute Nodes

+  
Virtualization
Our Vision

Traditional Embedded

• Isolated System
• Multiple Native OS & SOC

Virtualized SDC

• Isolated System
• Mixed OSs on single SOC
• Consolidation through virtualization

Virtualization & Orchestration

• Cloud Connectivity & Compute
• Multi Nodes
• Orchestration for App/Services Deployment
• Container Models for Workload Isolation
Use Case – Fault Tolerance

Node1
- Game
- TellTale
- Display as Service
- ACRN Hypervisor

Node2
- Movie
- Security Gateway
- Navigation
- ACRN Hypervisor

High Severity Workload
Low Severity Workload
Use Case – Fault Tolerance

Node 1
- ACRN Hypervisor
- Game
- TellTale
- Display as Service

Node 2
- ACRN Hypervisor
- TellTale
- Security Gateway
- Display as Service

Fault

High Severity Workload

Low Severity Workload
Use Case – Dynamic Workload Deployment

Cloud

Data Analysis/Training

AI Workload

New AI algorithm OTA

KVM
openstack.

KVM
openstack.

kata containers

THE LINUX FOUNDATION
We Need Secure Container - ACRN+KATA

ACRN + Kata

- ACRN is design for vehicle SDC solution
- Increasing orchestration requirements for vehicle
- Future vehicle need Secure Container
- Kata is designed for Secure Container
What’s KATA

Traditional Containers

- An open source project hosted by the OpenStack Foundation
- Each container/pod isolated by a quick-to-boot and lightweight VM
- Support industry standards including OCI container format, Kubernetes CRI interface

Kata Containers
Advantage of KATA

**Security/Isolation**
- Dedicated kernel, isolation of network, I/O and memory, and utilize hardware-enforced isolation with VT extensions.

**Performance/Speed**
- Delivers consistent performance as standard Linux containers; increased isolation with the performance tax of standard virtual machines.
Support Kata on ACRN

- Kata to support ACRN
- ACRN-DM to support Kata
- ACRN add-on to Kata: CPU Sharing
Looking Forward – Solution in ACRN 2.0

Hybrid-Mode
- Partition + Shared

VM Type
- Safety VM
- Real-time VM

Kata Container

More OS Support:
- Zephyr, VxWorks, RT-Linux, Windows

FUSA Certification
Call for Participation

https://projectacrn.github.io/index.html

Joining ACRN Community Today!!!
Questions?