Secure container in IoT segment – Extend KATA to ACRN IoT hypervisor

Yu Wang, Intel SSP

Table of Contents

What is ACRN?

ACRN™ is a Big Little Hypervisor for IoT Development

ACRN™ is a flexible, lightweight reference hypervisor, built with real-time and safety-criticality in mind, optimized to streamline embedded development through an open source platform

ACRN Focus

Small Footprint

Built for Real-Time

Built for IoT

Safety Criticality

Adaptability

Truly Open Source

THE LINUX FOUNDATION

Virtualization User Cases for IoT

In-Vehicle-Infotainment

Robotics

Precision instrument

Industrial

THE LINUX FOUNDATION

Why introducing container to IoT?

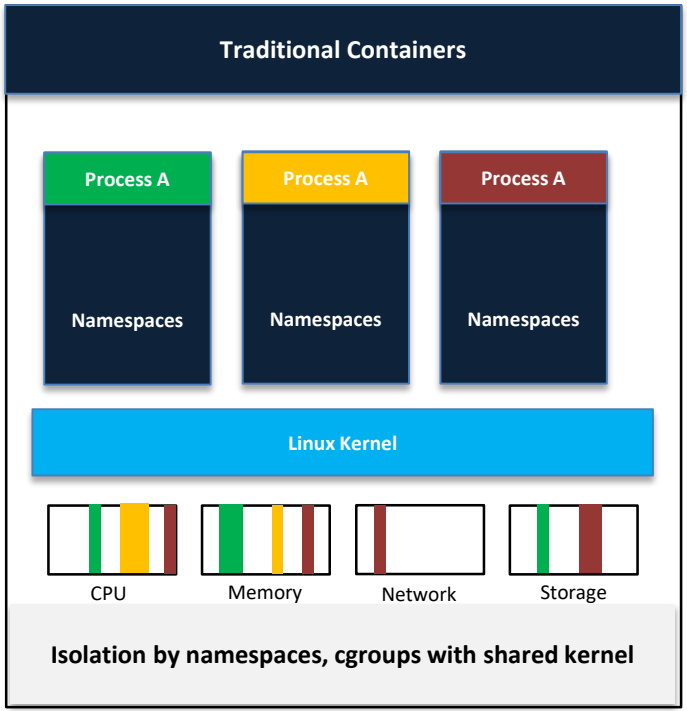
- Container technology is easy deployment, provide consistent behavior on any supported hardware platforms.
- More and more various of workloads need to be execute into single IoT embedded system, container technology provides isolation to avoid influence.
- Container image is built up from a serial of layers, can easy derives new features base on the mature container images. Accelerate the development of IoT production iteration with easy maintenance and upgradability.

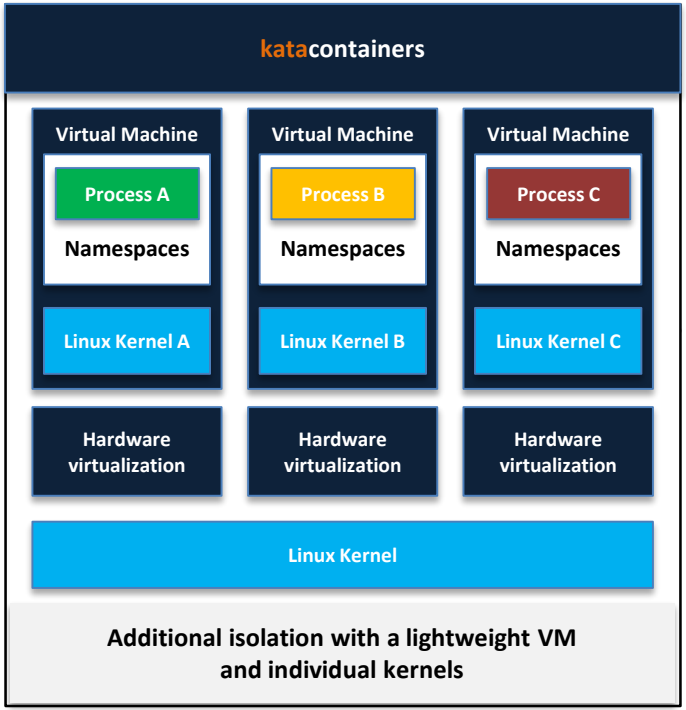
Container vs Virtual Machine

Virtual Machine	Container
Heavyweight	Lightweight
Limited performance	Native performance
Startup time in minute	Startup time in seconds
Allocates required memory	Requires less memory space
Hardware-level virtualization	OS virtualization
Fully isolated and hence more secure	Process-level isolation, possibly less secure

Container is not secure!!

What & Why is KATA?

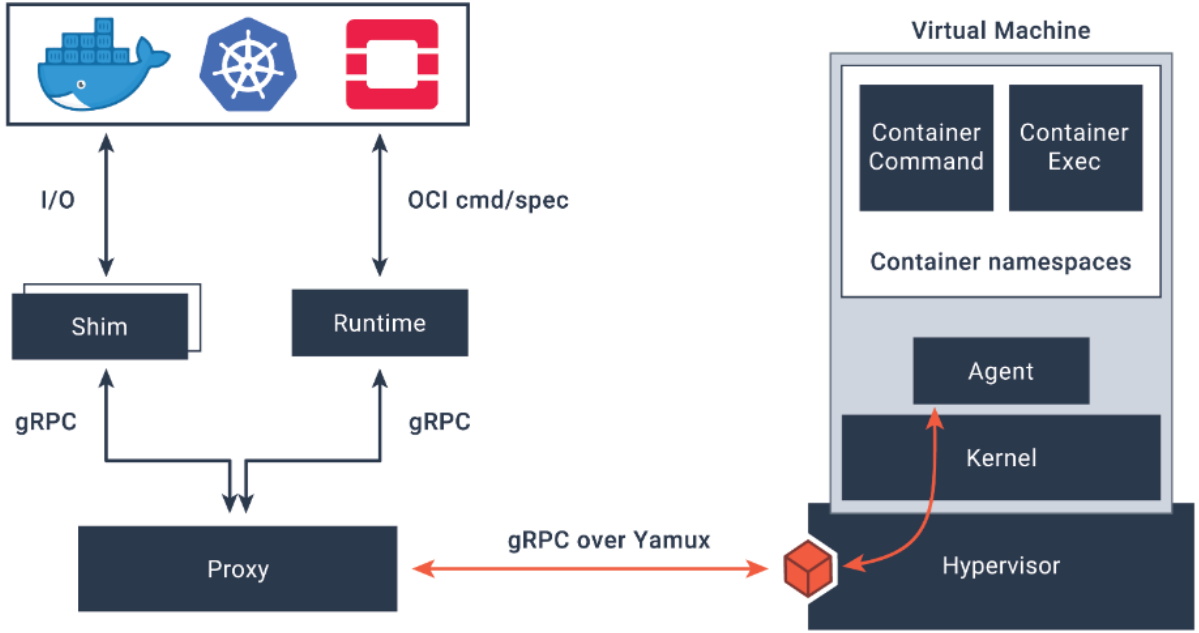




Kata provides a lightweight VM and individual kernel for additional isolation.

Utilize the hardware virtualization technology to provide more secure isolation.

What are included in KATA?



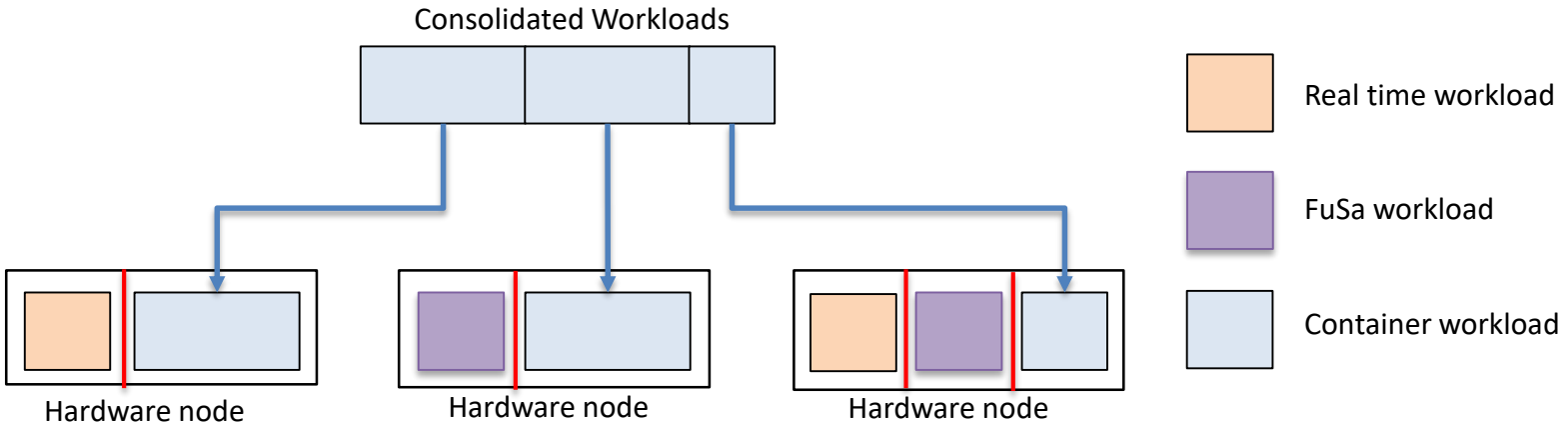
Kata-runtime: A OCI compatible runtime.

Kata-shim: A CRI friendly shim.

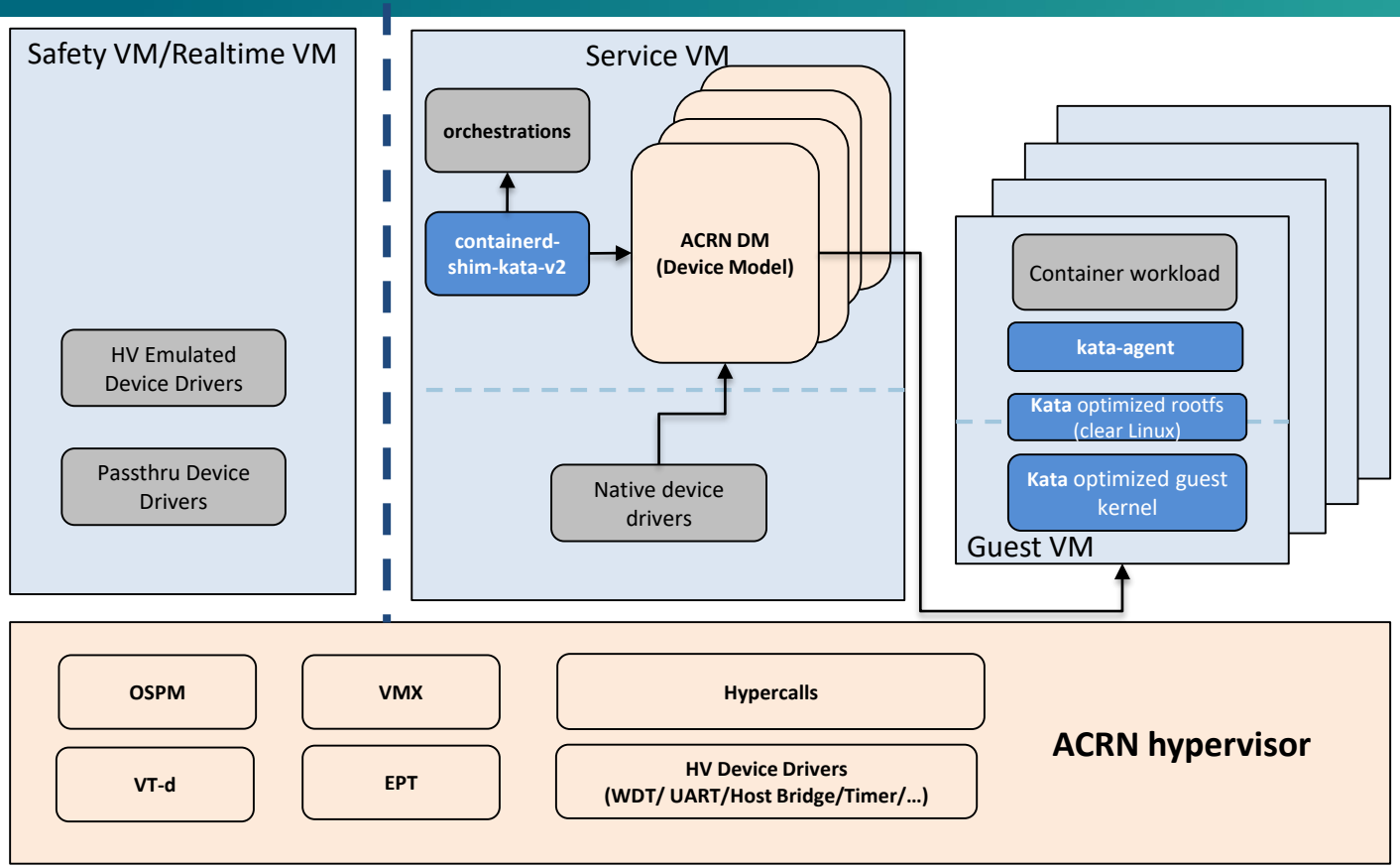
Kata-proxy: A multiplex to route between kata-shim/kata-runtime and kata-agent.

Kata-agent: A process running in the VM as a supervisor for managing containers and processes running with those containers.

KATA+ACRN = secure container for IoT



KATA + ACRN high level architecture

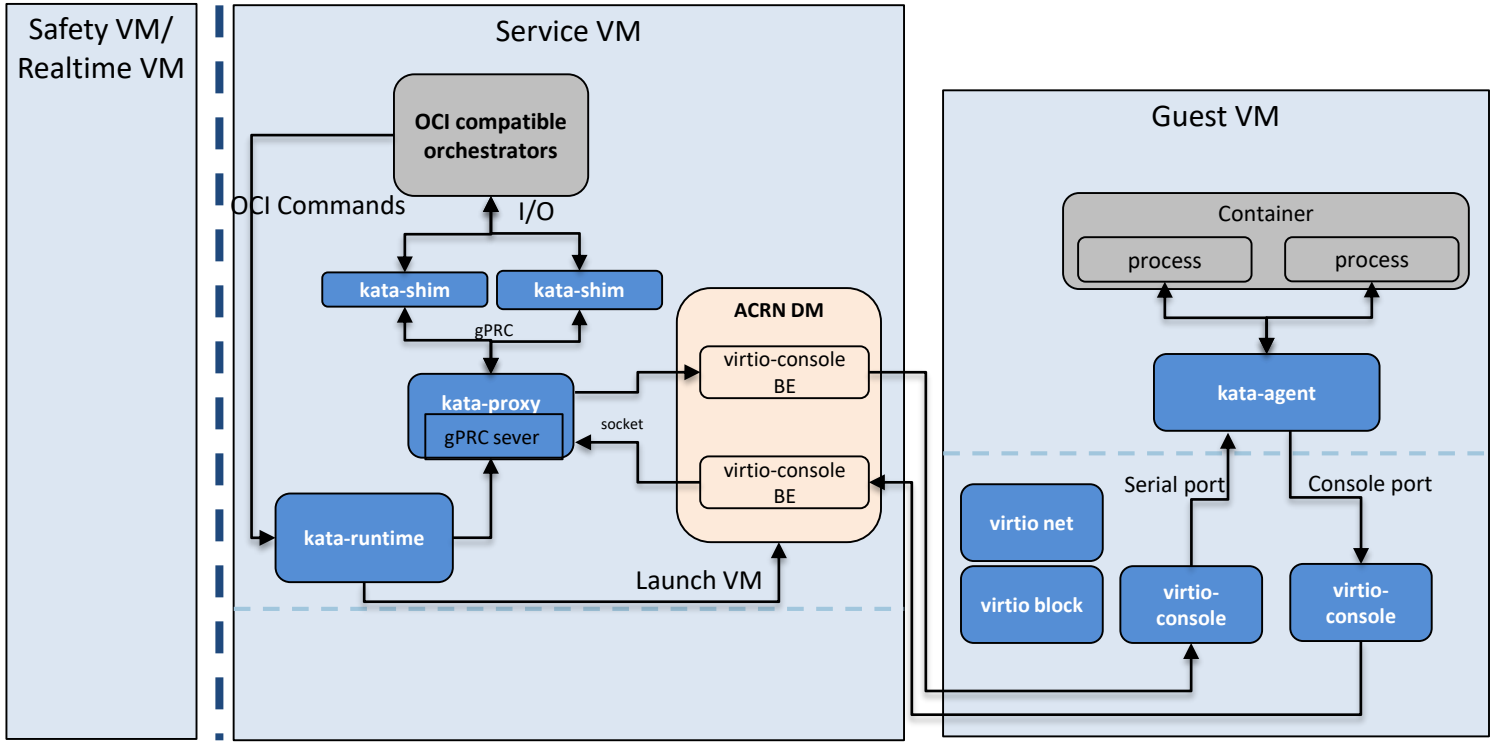


Acrn is a type-1 hypervisor. All Kata container's VM will share the same service VM.

Per Kata VM be launched by separated acrn-dm in service VM for providing mediator supports.

The guest VM executes the Kata provided highly performance optimized kernel and rootfs.

KATA + ACRN low level architecture



Acrn device model exports two PCI virtio console devices to guest VM, and provides UNIX domain socket interfaces for Kata host side services.

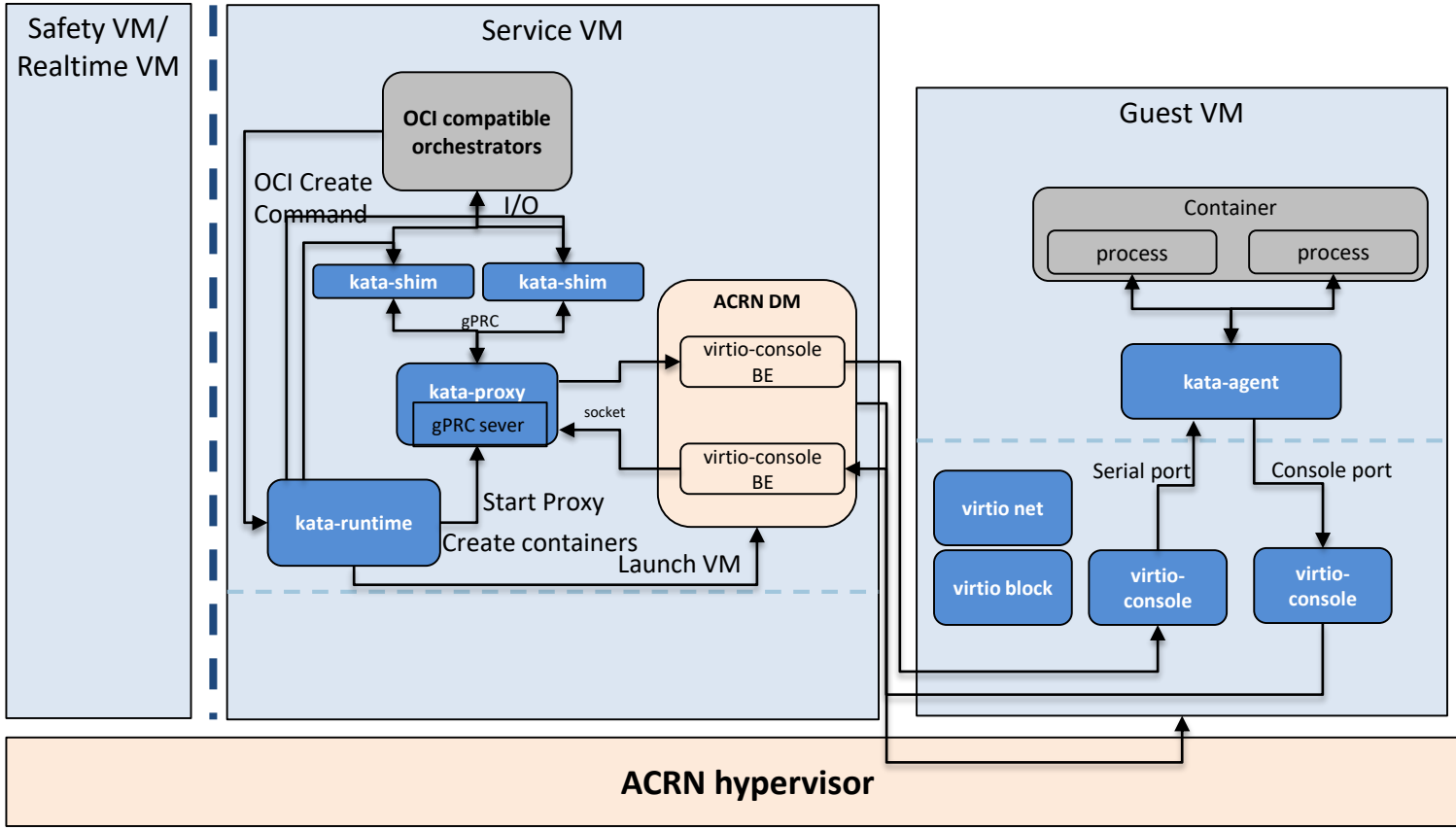
The Acrn guest VM is created by kata-runtime who will spawn the kata-proxy.

kata-proxy will connect to kata-agent over virtio consoles.

kata-proxy will offer access to the VM kata-agent to multiple kata-shim and kata-runtime clients associated with the VM.

THE LINUX FOUNDATION

KATA + ACRN low level architecture



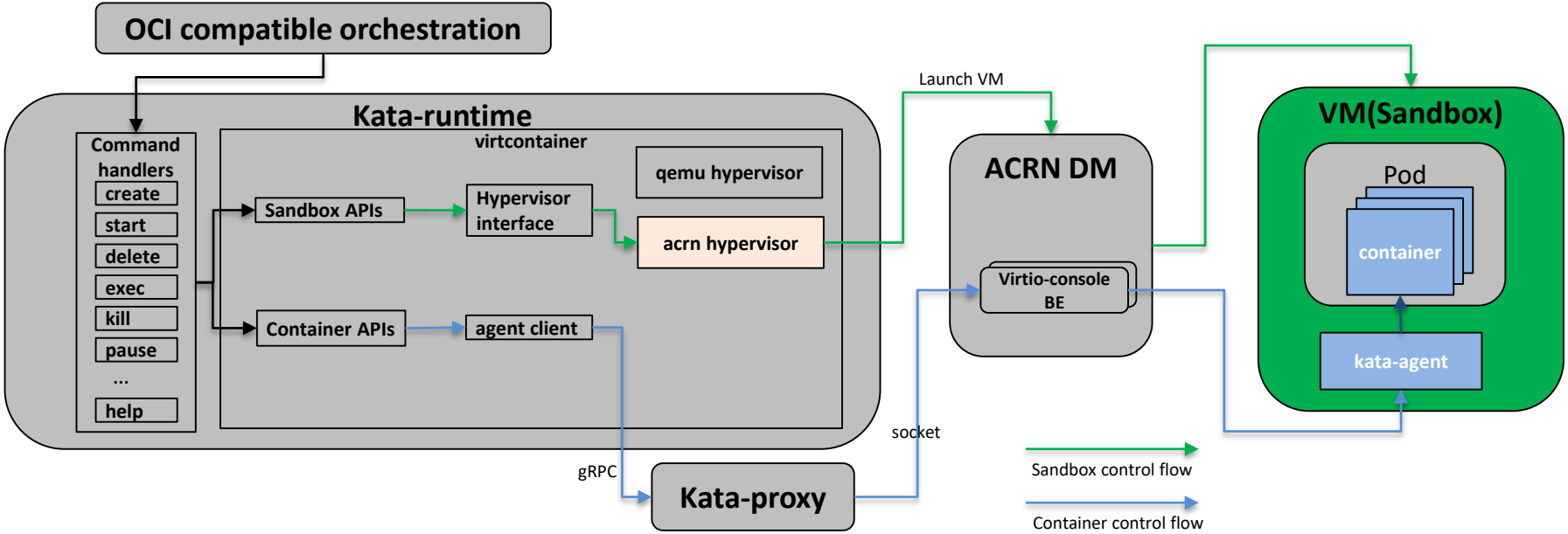
Acrn device model exports two PCI virtio console devices to guest VM, and provides UNIX domain socket interfaces for Kata host side services.

The Acrn guest VM is created by kata-runtime who will spawn the kata-proxy.

kata-proxy will connect to kata-agent over virtio consoles.

kata-proxy will offer access to the VM kata-agent to multiple kata-shim and kata-runtime clients associated with the VM.

How to extend KATA to ACRN?



- Kata-runtime heavily utilizes the virtcontainer which provides a generic, runtime-specification agnostic, hardware-virtualized containers library.
- The virtcontainer abstracts the operations for the sandbox and container on different hypervisor solution. Adds a new hypervisor operation instance for Acrn.

Call for Participation

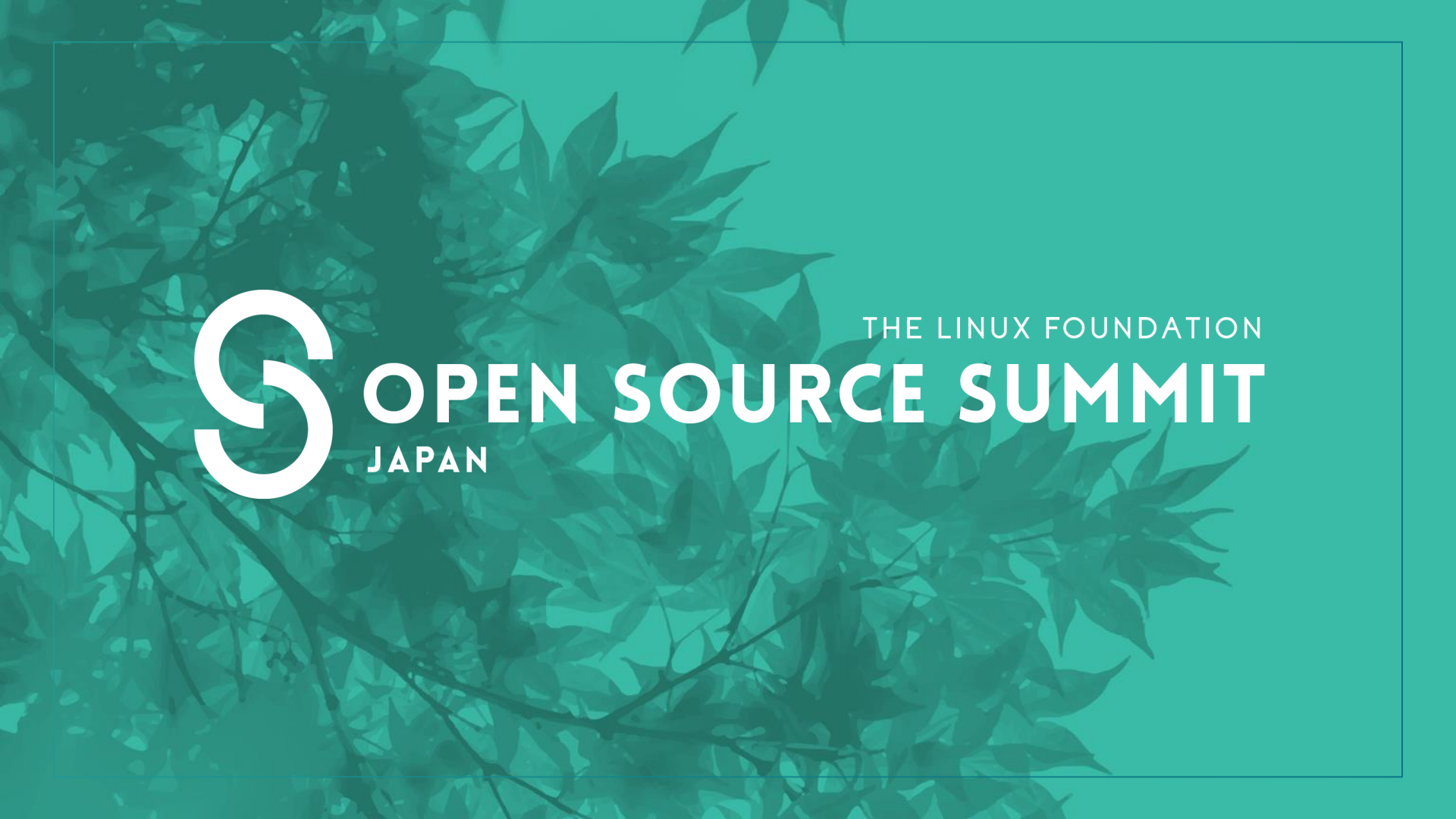
https://projectacrn.github.io/index.html

https://projectacrn.org

Joining ACRN Community Today!!!

THE LINUX FOUNDATION

Questions?


THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
JAPAN