Zephyr® Project
Developer Summit

# Project Ocre
# Extending Cloud Native Beyond the "Linux Barrier" to MCUs Using Wasm

Jason Shepherd & Stephen Berard, Atym

THE LINUX FOUNDATION

#EmbeddedOSSummit

# About Us

atym

> 50 years combined experience building connected solutions and driving industry standards

**Jason**
Atym CEO

**Stephen**
Atym CTO

ZEDEDA DELL Technologies THE LINUX FOUNDATION

Schneider Electric Microsoft APC

EOSS EMBEDDED OPEN SOURCE SUMMIT

# Embedded development is difficult

Talent is difficult to find and retain, **only 19% of developers program in C**

Monolithic images complicate IP protection. **IP theft costs industry >$500B/year**.

**Silicon swaps delay projects by months** due to vendor-specific HW coupling

Developing common functionality at **$25-40/line of code** detracts from adding customer value

Companies lack skills to build secure devices. **Security attacks average $330k per incident.**

# And it’s only getting more complicated

Increasing device capability

Edge computing

Rise of AI

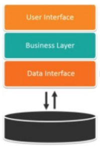
New security threats and regulations

Growing talent gaps

The ‘90s called and want their embedded development tools back.

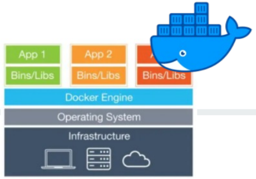
# It’s time to modernize the embedded space

Server architectures have evolved dramatically over the past 25 years…

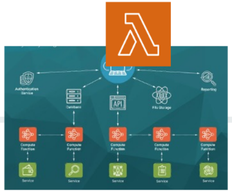


**Monolithic Server**

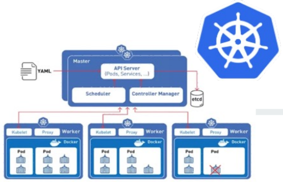
**Virtual Machines**
~2000



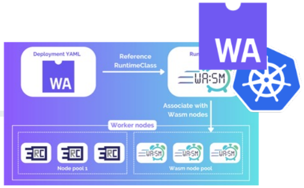
**Containers**
2013



**FaaS**
~2014



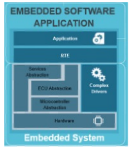
**Kubernetes**
2014



**Wasm + Kubernetes**
2021

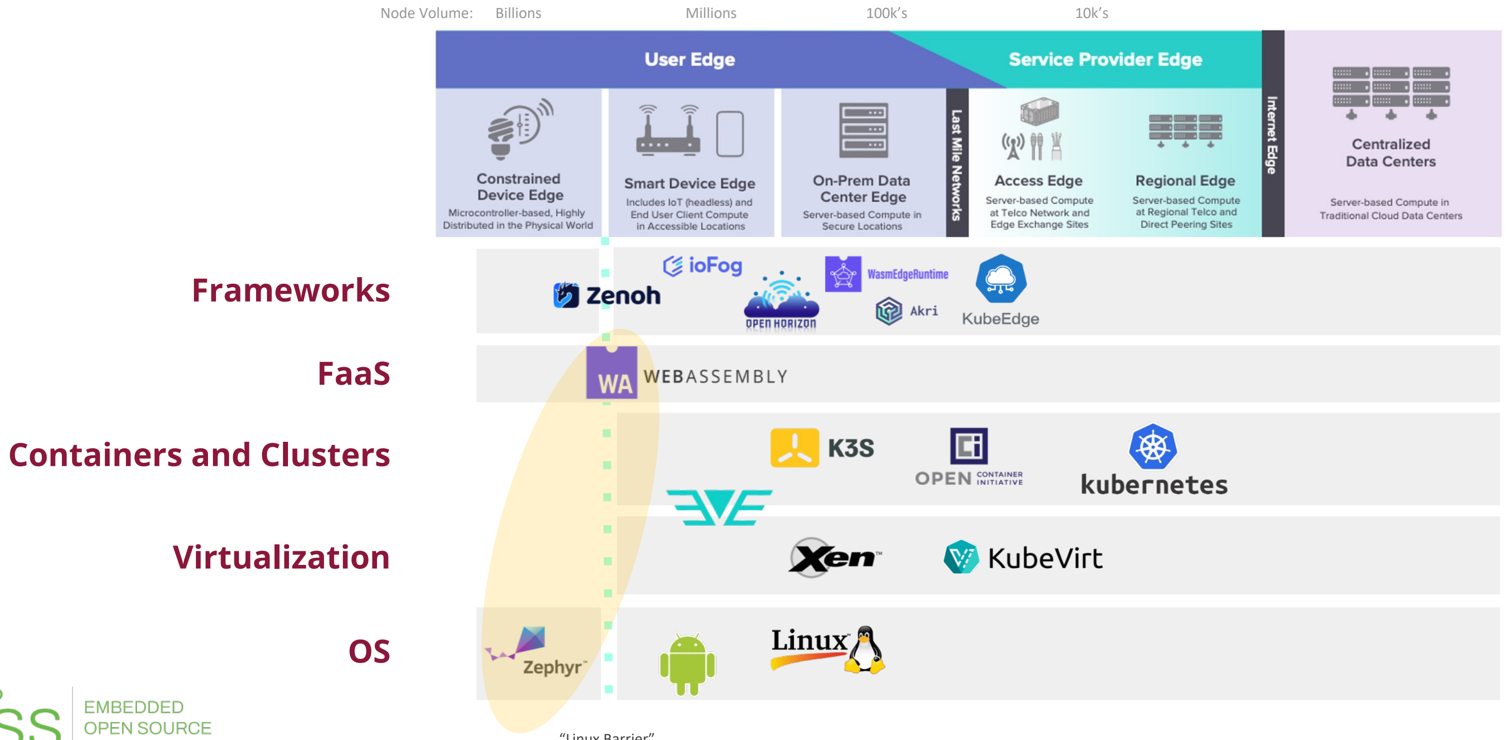
…meanwhile, the embedded space has remained largely the same.

**Monolithic Embedded**



# We’ve reached the technology tipping point

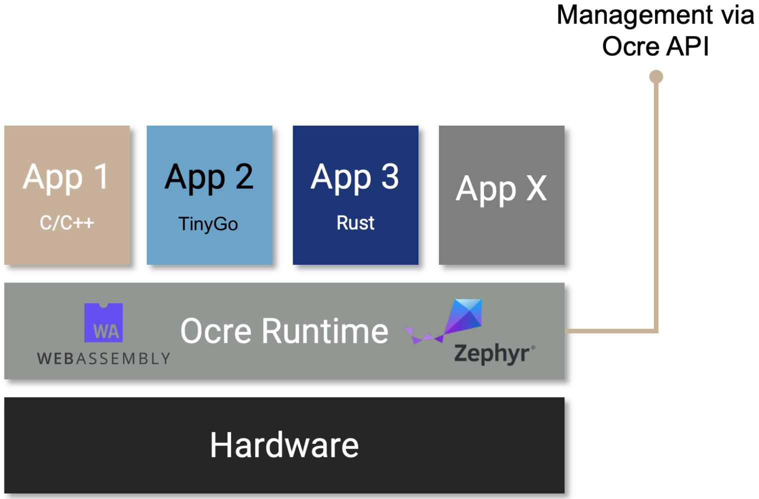
WebAssembly (Wasm) makes cloud-native dev possible for devices that can’t support Linux or technologies like Docker and Kubernetes


Node Volume:
Billions
Millions
100k’s
10k’s
User Edge
Service Provider Edge
Constrained Device Edge
Microcontroller-based, Highly Distributed in the Physical World
Smart Device Edge
Includes IoT (headless) and End User Client Compute in Accessible Locations
On-Prem Data Center Edge
Server-based Compute in Secure Locations
Last Mile Networks
Access Edge
Server-based Compute at Telco Network and Edge Exchange Sites
Regional Edge
Server-based Compute at Regional Telco and Direct Peering Sites
Internet Edge
Centralized Data Centers
Server-based Compute in Traditional Cloud Data Centers
Frameworks
FaaS
Containers and Clusters
Virtualization
OS
Zenoh
ioFog
OPEN HORIZON
WasmEdgeRuntime
Akri
KubeEdge
WA
WEBASSEMBLY
K3S
OPEN CONTAINER INITIATIVE
kubernetes
Xen
KubeVirt
Zephyr
Linux

“Linux Barrier”
~256MB Memory

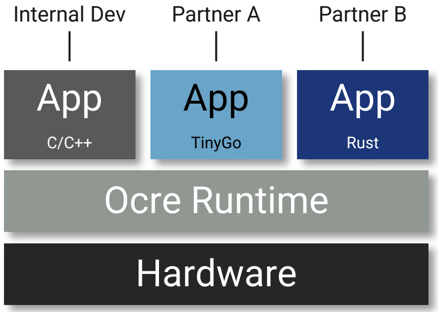
# Introducing Project Ocre

- **Managed container runtime** supporting OCI-like app containerization
- **Up to 2000x lower footprint** than a Linux-based container runtime like Docker
- Supports apps written in **any programming language**
- **Zero trust security**, rooted in silicon
- **To be hosted in LF Edge** within the Linux Foundation with the Apache 2.0 license



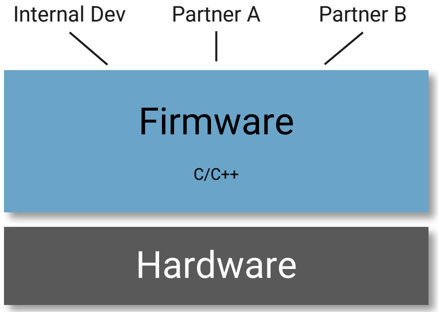
# Ocre app containerization vs. traditional embedded dev

## Ocre Containerization



- IP protected in isolated containers
- Supports asynchronous app development lifecycles
- Developers can code in preferred language and merge at deployment
- Hardware complexity abstracted

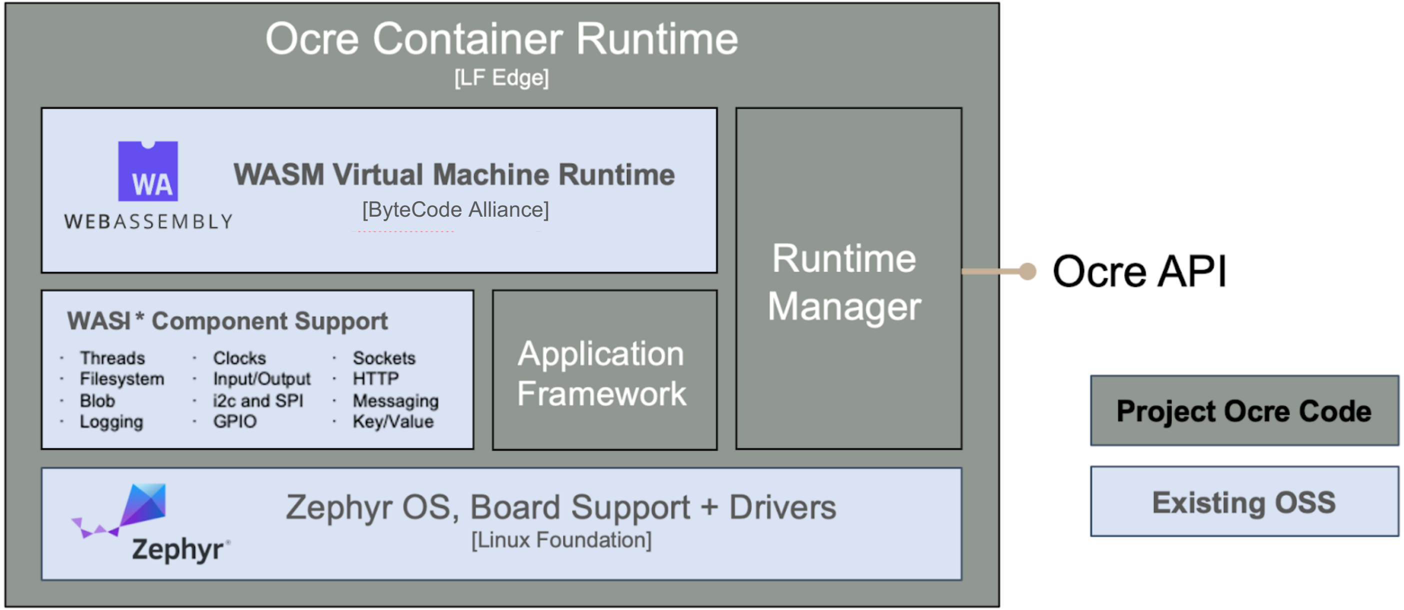
## Traditional Embedded



- IP exposed as raw source code
- Any supply chain change requires recompile and monolithic update
- Developers must code in same language (e.g. C/C++) and deeply understand hardware

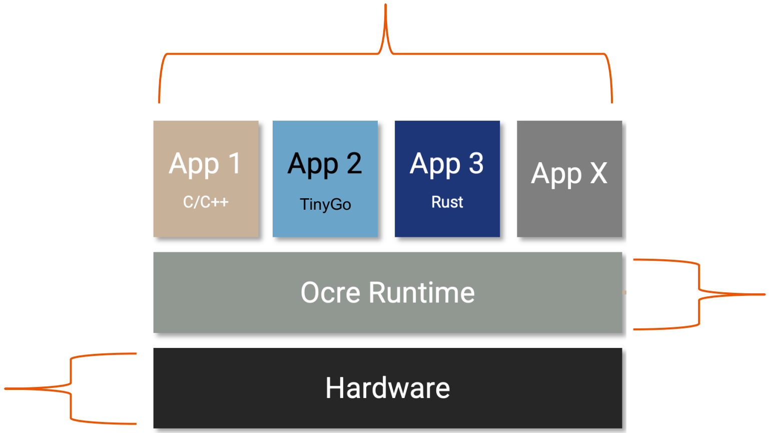
# Ocre architecture

WebAssembly (Wasm) makes cloud-native dev possible for devices that can't support Linux or technologies like Docker and Kubernetes



# Performance and footprint

- Smallest individual app is ~300 *bytes* of flash, limited by Atym packaging
- Largest app size and quantity deployed per device is limited by HW capability
- Device memory and processing requirements are driven by app needs



- 256KB of memory and flash

- Any processor architecture (e.g. Arm, x86, RISC-V)

## Performance

Dependent on application processing needs

Negligible impact for typical event-driven telemetry use cases

No impact to battery life due to event-driven architecture

# Ocre closely follows OCI design patterns

| | Ocre Containers | OCI Containers |
|---|---|---|
| ***Compute*** | • Portable, instruction set independent code<br>• Requires Wasm engine to execute (no specific OS dependency)<br>• Packaged as a Wasm module<br>• Scheduled using native threads<br>• Fine-grained resource controls | • Platform-specific code<br>• Requires Linux kernel to execute<br>• Packaged as a tar file system<br>• CFS (default) scheduling or real-time scheduler<br>• Resource controls for limiting CPU, memory, etc. |
| ***Storage*** | • Resource files (blobs)<br>• Simulated filesystem (POSIX-like)<br>• No direct filesystem access | • Layered, union filesystem<br>• POSIX filesystem calls<br>• OS filtered filesystem access (chroot) |
| ***Networking*** | • Managed socket API<br>• Naming and service location<br>• Inter-container messaging | • L2 virtual networking interface w/bridge, host, & VLAN support<br>• Naming (DNS) and service locations<br>• Advanced routing, NAT, and address configuration |
| ***Security*** | • Full isolation through virtualization<br>• Default-deny permissions model with fine-grain controls<br>• Container validation through digital signature | • OS-level isolation through groups<br>• Default-allow permissions model<br>• Container validation through digital signature |

# Baseline Wasm security benefits

WA

WEBASSEMBLY

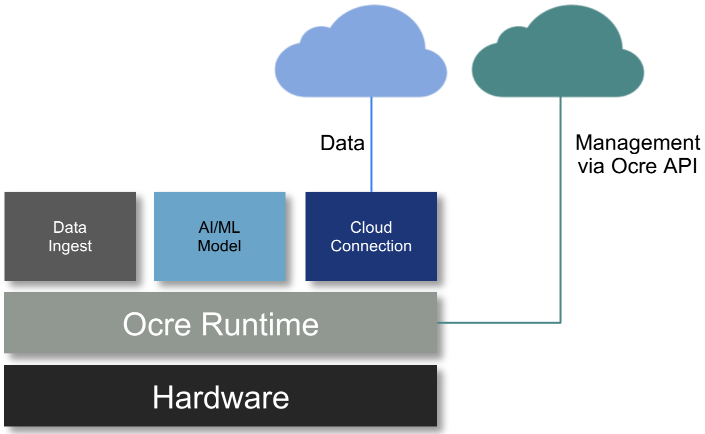
- Containerized applications/ modules sandboxed from host and others by default
- Access between apps only possible based on permissions
- Apps can only access specified device memory; can’t do callstack jumps and buffer overruns
- Individual containers can be terminated if abnormal behavior is detected

00010010
101001101
00010010
111001001
00010010

- Monolithic image typically accesses the entire available memory space
- Code can jump to accessing arbitrary addresses or execute in data memory
- Entire device is compromised with a single code bug or security breach

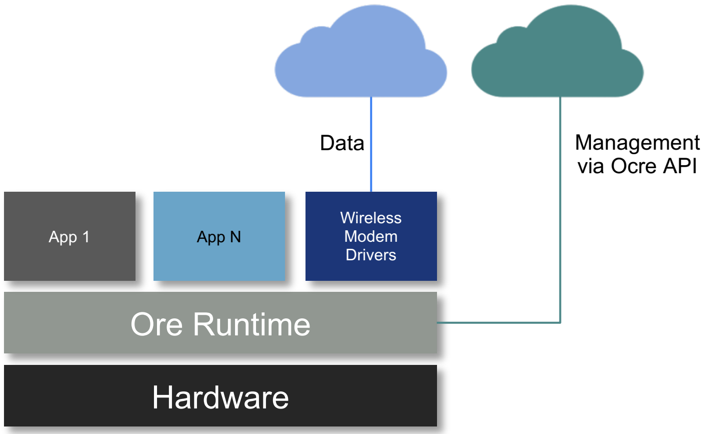
# Example deployment patterns

## IoT Analytics / Computer Vision



- IoT workloads (e.g. predictive maintenance, cold chain logistics, building automation)
- AI can be telemetry-driven or computer vision / voice recognition

## Device Driver Abstraction



- Abstract certified functionality (e.g. cellular modem drivers) from core runtime
- Apps can be updated without impacting regulatory certifications

# DEMO

# Summary

- Ocre is a tiny  (~256KB) container runtime for constrained devices
- Built with a combination of Zephyr and WebAssembly
- Code drops by June to seed Project Ocre in LF Edge
- Stay tuned for more details!
    - In the meantime, feel free to reach out at info@atym.io

OCRE

# Q&A

# Zephyr® Project

## Developer Summit

EOSS

EMBEDDED
OPEN SOURCE
SUMMIT