

Closing Remarks

- Akraino IoT Area Webinar / Regional Developer Meetup - Africa

Tina Tsou, TSC Chair, Akraino
September 15, 2021



Recap

- › **Welcome Remarks** - [Tina Tsou](#), TSC-Chair, Akraino
- › **Introduction to Akraino** - [Ike Alisson](#) , Akraino Documentation Sub-committee TSC Chair

- › **Speaker:** Stephen Ozoigbo, Arm
- › **Title of Talk:** (E³)NGAGE - Arm's Africa Engagement

- › **Speaker:** Andile Ngcaba, Inq.
- › **Title of Talk:** EDGE Technologies in Africa

- › **Speaker:** Erik Hersman, BRCK
- › **Title of Talk:** Rugged Internet of Things

- › **Speakers:** Bart Renka, Arm & Stephen Ozoigbo, Arm
- › **Title of Talk:** Fireside Chat - V2X Opportunities in Emerging Markets: Leveraging the Arm Ecosystem



Recap – Cont'

- › **Speaker:** Olivier Bernard, Arm
- › **Title of Talk:** **Unlocking the Edge's Potential with Project Cassini**

- › **Speaker:** [khemendra kumar](#), Huawei
- › **Title of Talk:** **Enterprise Edge Lightweight and IOT (ELIOT) Blueprint**

- › **Speaker:** Li Mingxuan, China Unicom
- › **Title of Talk:** **EdgeFaaS for Open Edge Scenarios**

- › **Speaker:** Dr. Hideyuki Saso, Tokyo Institute of Technology
- › **Title of Talk:** **Introduction of the Cross-ministerial Strategic Innovation Promotion Program (SIP)**

- › Closing Remarks - [Tina Tsou](#)



Blueprint Families

- › ELIOT: Edge Lightweight and IoT Blueprint Family
 - › ELIOT AIoT in Smart Office Blueprint
 - › ELIOT IoT Gateway Blueprint
 - › ELIOT SD-WAN/WAN Edge/uCPE Blueprint
- › IIoT at the Smart Device Edge (family)
 - › Predictive Maintenance (with a Thermal Imaging Camera, vibration sensors, etc.)
- › Project Cassini - IoT and Infrastructure Edge Blueprint Family
 - › Smart Cities
 - › Software Defined Camera (SDC)
- › More blueprints out of this webinar...



Security

- › PARSEC, the opensource CNCF project has been adopted for edge deployments as it offers a common API that abstracts secure roots of trust which are required to protect devices outside of the datacenter. This enables the cloud native principle of being able to freely move your applications from one platform to another while maintaining level of security that was not possible in the past.
- › Building on this abstraction, PARSEC can mediate access to hardware security primitives and create isolated key stores for a multi-tenancy environment.
- › Starting your project with the right platform for security will accelerate your deployments and scale.

- › Come read about Parsec at: <https://parallaxsecond.github.io/parsec-book>
- › And talk to the experts during our weekly community calls (see github).
- › Or join us on the CNCF slack channel: <https://cloud-native.slack.com>
- › [PARSEC \(Platform Abstraction for SECURITY\)](#)



APIs

- › IoT apps must run on a wide range of devices (not just mobile phones), be able to sustain functionality through loss of Internet connectivity, and often run on devices or platforms with substantial size, weight, and power consumption (SWaP) constraints. Due to this need for robustness, and the underlying variety of devices and OS, IoT applications utilize all types of interfaces, including API, CLI, and web GUI. In an edge computing scenario, remote sensors may connect with edge nodes that host containerized IoT apps.
- › The latest version of the API Portal (api.akraino.org) contains a new top-level category for IoT applications showing APIs both exposed and consumed by the ELIOT and IIoT at the Smart Device Edge Blueprint projects.

oneM2M IoT Service Layer (SL) Platform

oneM2M supported IoT Use Cases (UCs) - SAREF (Smart Applications REFerence) Ontology

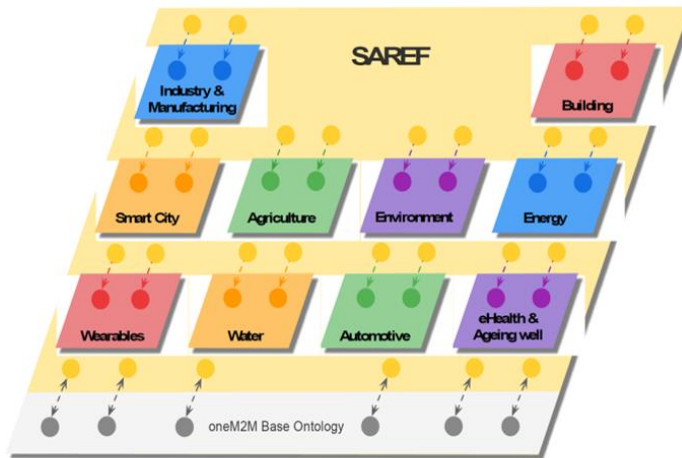
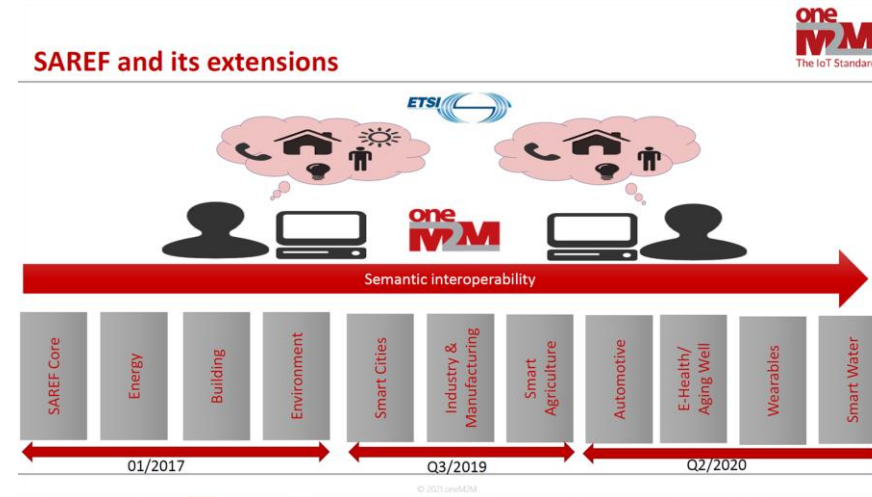
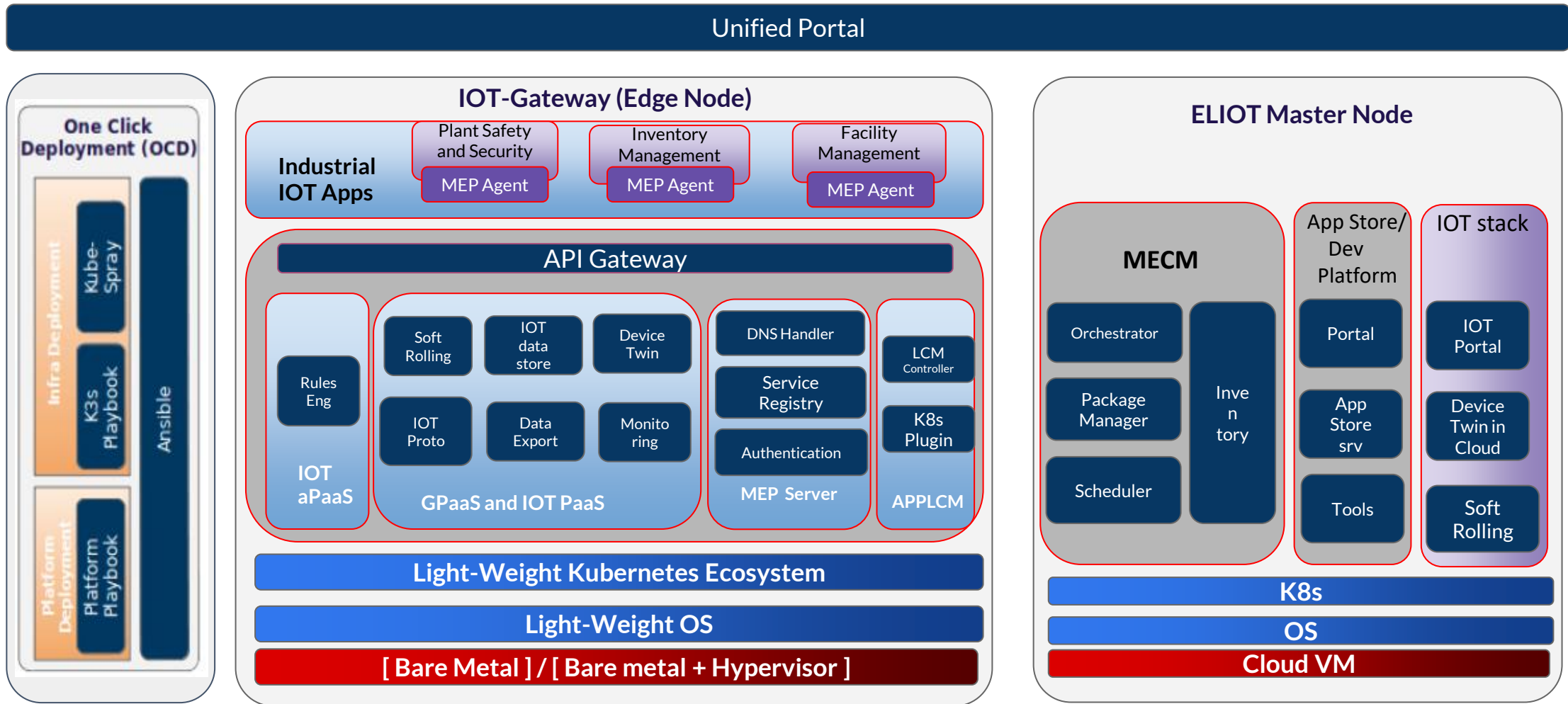


Figure 11: SAREF and its extensions

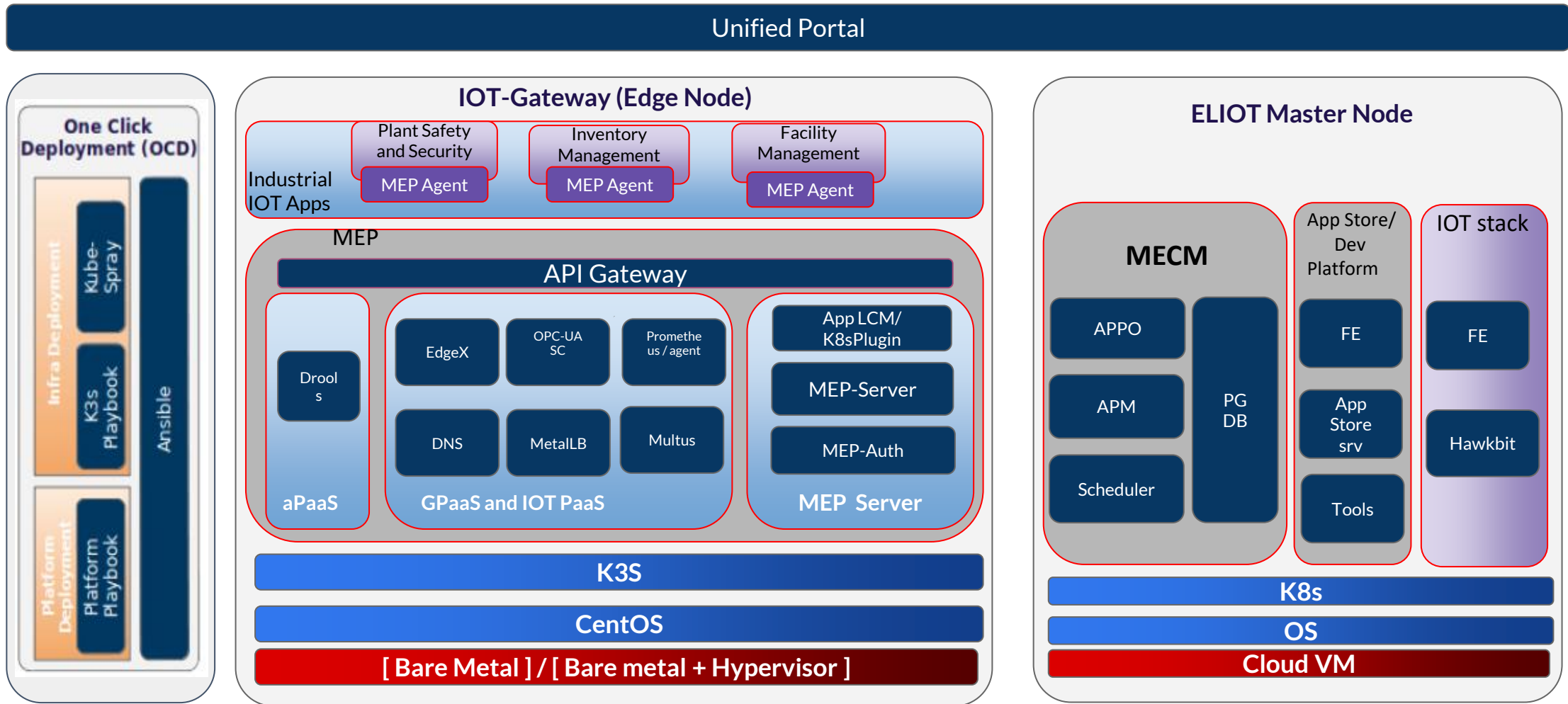


1. Blueprints under IoT Area choose to comply with oneM2M IoT Service Layer (SL) Platform
2. If oneM2M IoT Service Layer (SL) Platform has ecosystem page, IoT Area blueprints can participate.

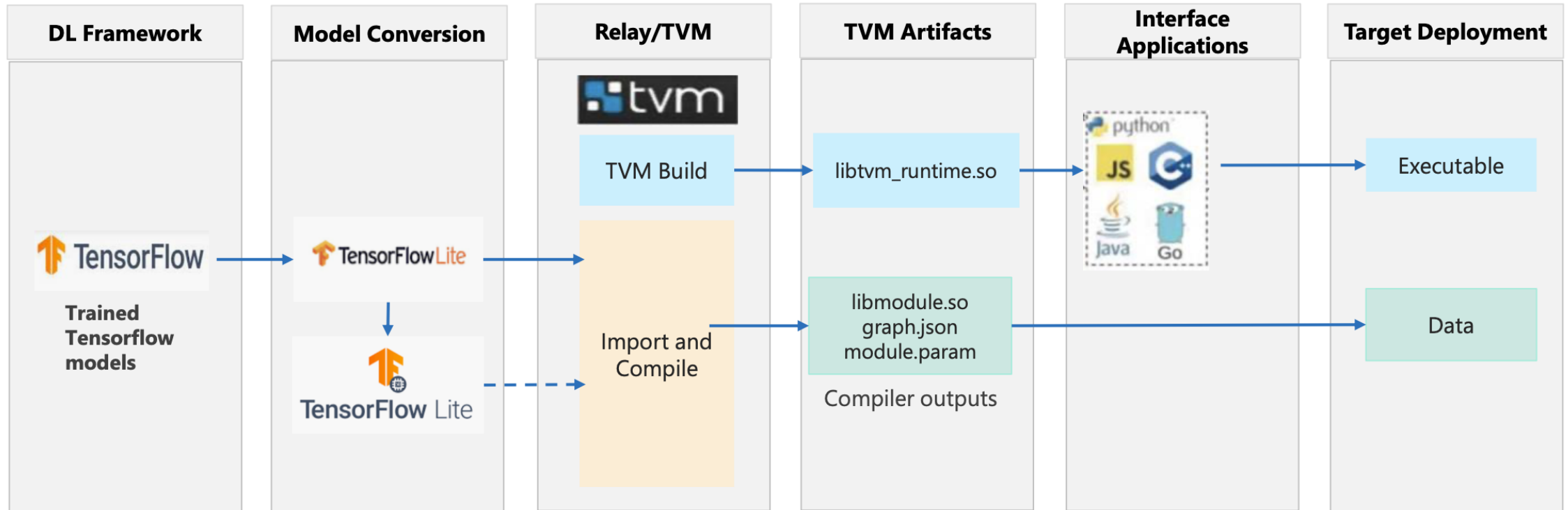
ELIOT Platform Architecture



ELIOT Software Architecture



Developing ML Applications for Smart Cameras



@Graphics: re-build this image/diagram - logos attached in a separate folder

Ensuring Secure Deployments of Smart Cameras with PSA



1

Analyze



Methodically
developed

2

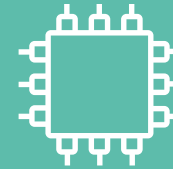
Architect



Open
architecture

3

Implement



Open Source
(TF-M, TF-A, OP-TEE)

4

Certify



Enabling
trust

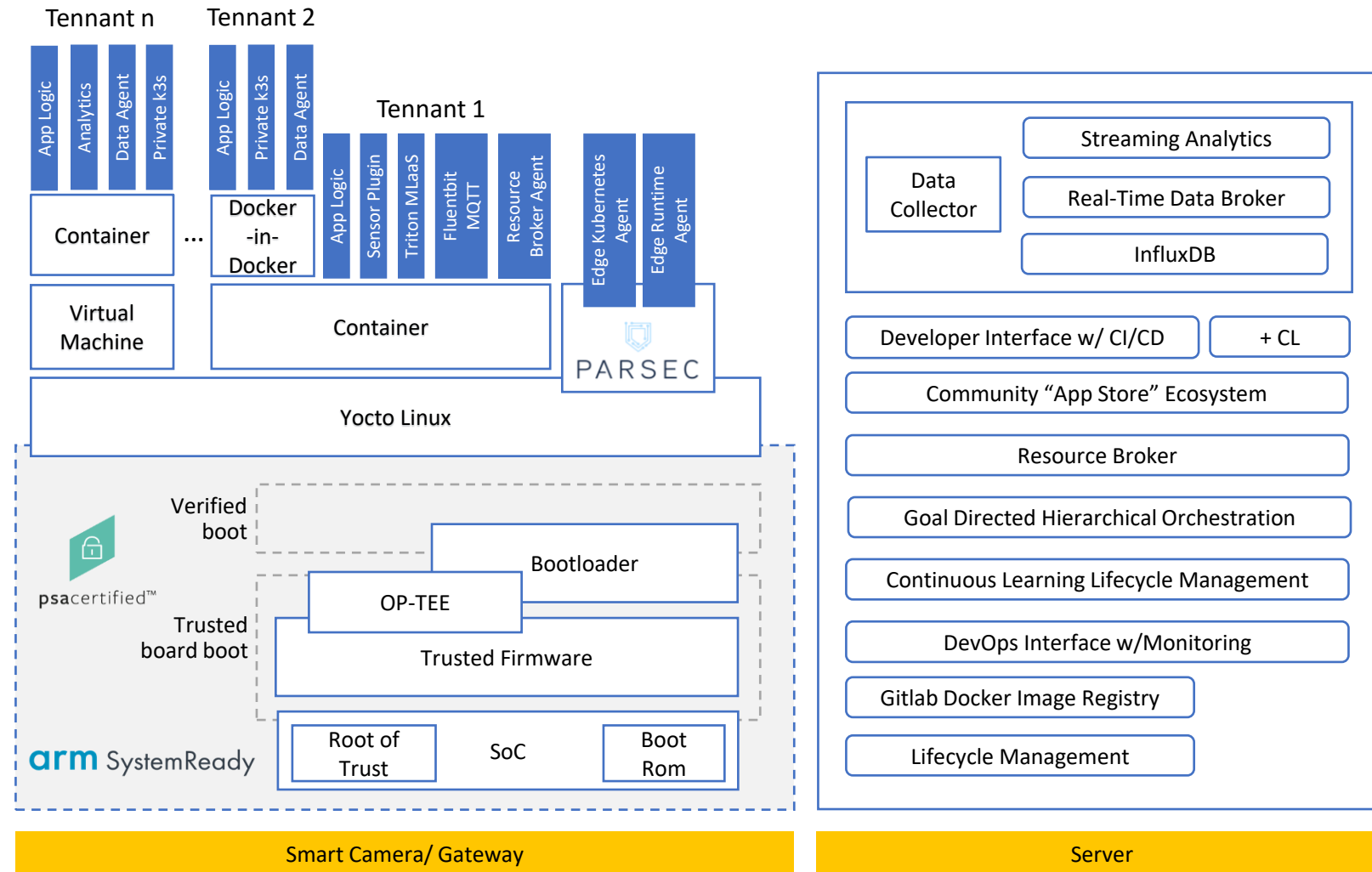
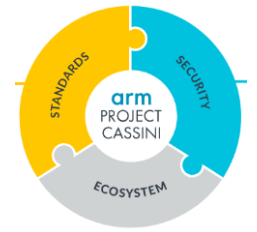
PSA Certified is an independent collaborative effort using open-source threat models and government best practices



psacertified™

Smart City Proof of Concept Using SMARTER Cloud Native Stack

Learn more about this PoC at https://www.youtube.com/watch?v=t0KNmApyNdl&ab_channel=Arm



Thank you
See you next time

