

# ARTIK Gateway Modules

Wei Xiao

July 31, 2018

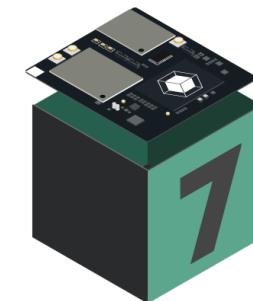
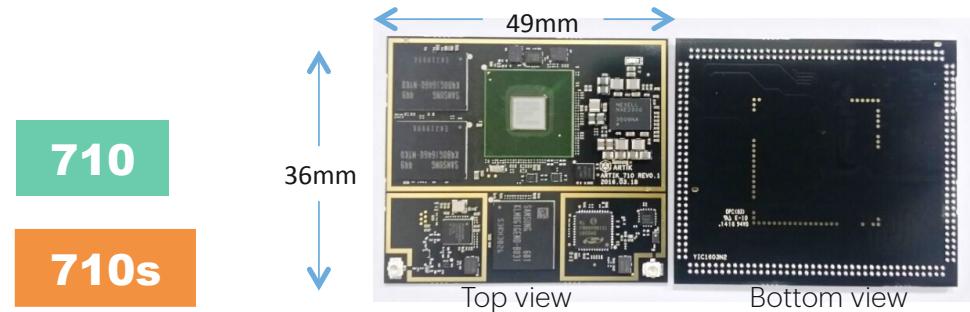
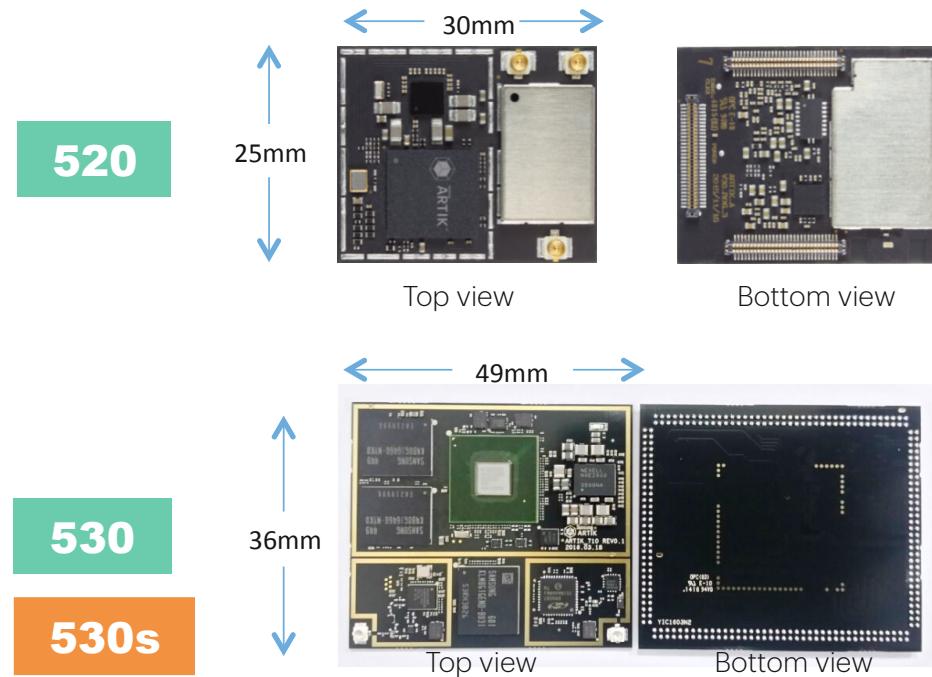


# Agenda

- ARTIK Gateway Module Overview
- ARTIK Gateway Module Development
- ARTIK End-to-end Solution
- ARTIK Gateway Module Use Cases and Ecosystem
- ARTIK Security

# ARTIK Gateway Module Overview

# ARTIK High-end module



# Samsung ARTIK™ 530/530s (512 MB, 1 GB) mid-range gateway

## Secure, fully-integrated IoT solution



- Industrial and home gateways
- Voice-controlled speakers
- Building zone controllers
- Display-based healthcare monitors



<b>Processor</b>	CPU: 4x ARM® Cortex® A9 @ 1.2 GHz GPU: 3D graphics accelerator
<b>Memory</b>	DRAM: 512 MB/1 GB DDR3 Flash: 4 GB eMMC v4.5
<b>Multimedia</b>	Camera I/F: 4-lane MIPI CSI up to 5MP Display: HDMI 1.4 a , 4-lane MIPI DSI or LVDS (1280 x 720 @ 60 fps) Audio: 2x I2S audio input/output
<b>Connectivity</b>	WLAN (Wi-Fi): IEEE 802.11 b/g/n single-band SISO Bluetooth: 4.2+ Smart 802.15.4: Zigbee, Thread Ethernet: 10/100/1000 Base-T MAC (external PHY required)
<b>Security</b>	Secure element, EAL Level 5, unique device certificate and keys, PKI with mutual authentication to cloud, hardware crypto engine; secure boot*, KMS*, TEE*, *S-modules
<b>I/O</b>	GPIO, UART, I2C, SPI, USB Host, USB OTG, HSIC, ADC, PWM, I2S, JTAG
<b>Temperature range</b>	-25° to 85° (°C)
<b>Size</b>	36 mm W x 49 mm H x 3.4 mm D

# Samsung ARTIK™ 710/710s high-end gateway

## Secure, fully-integrated IoT solution

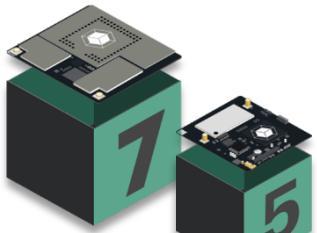
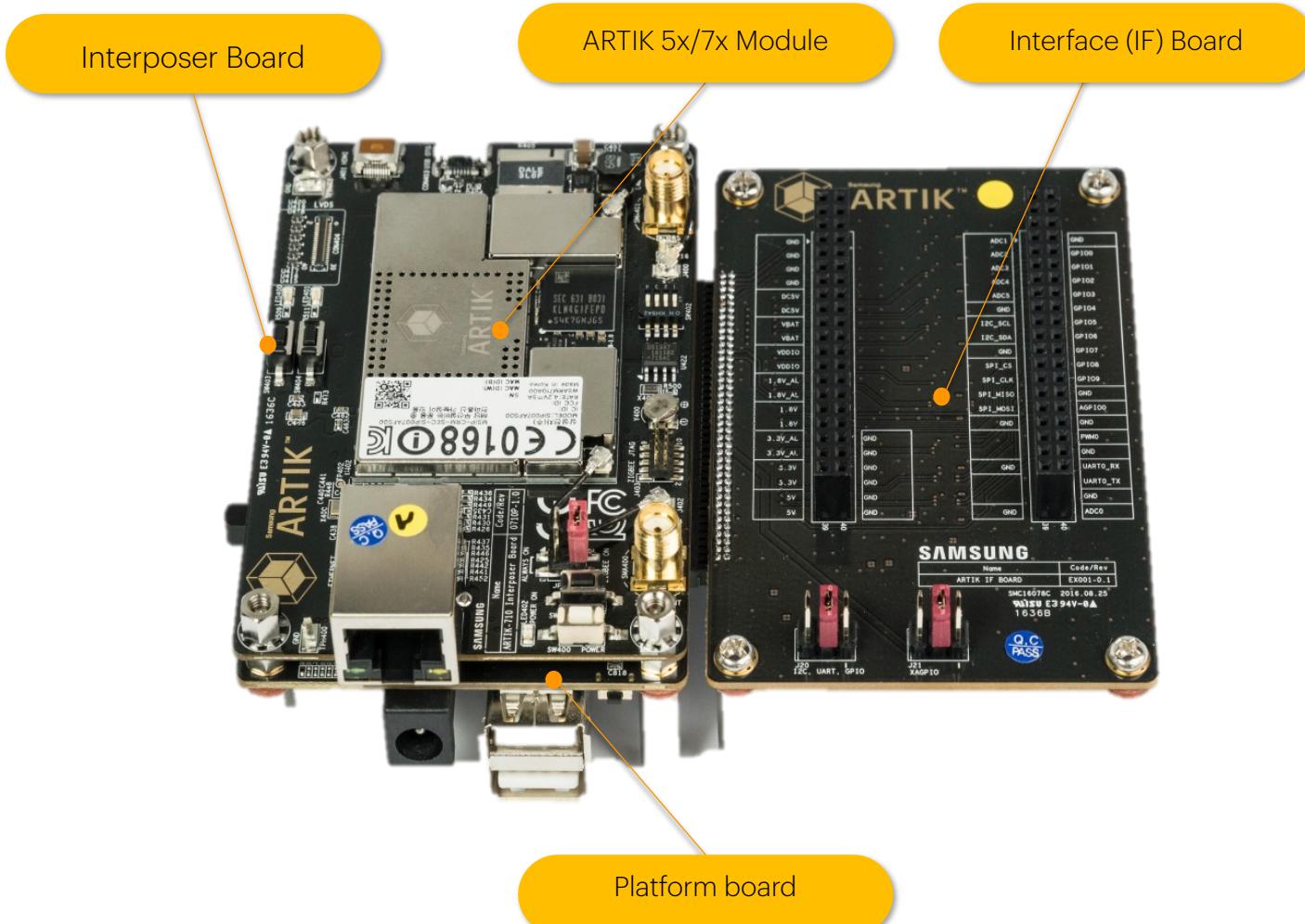


- High-end gateways
- Cameras
- Human-machine interface
- Machine learning

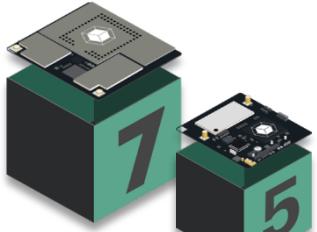
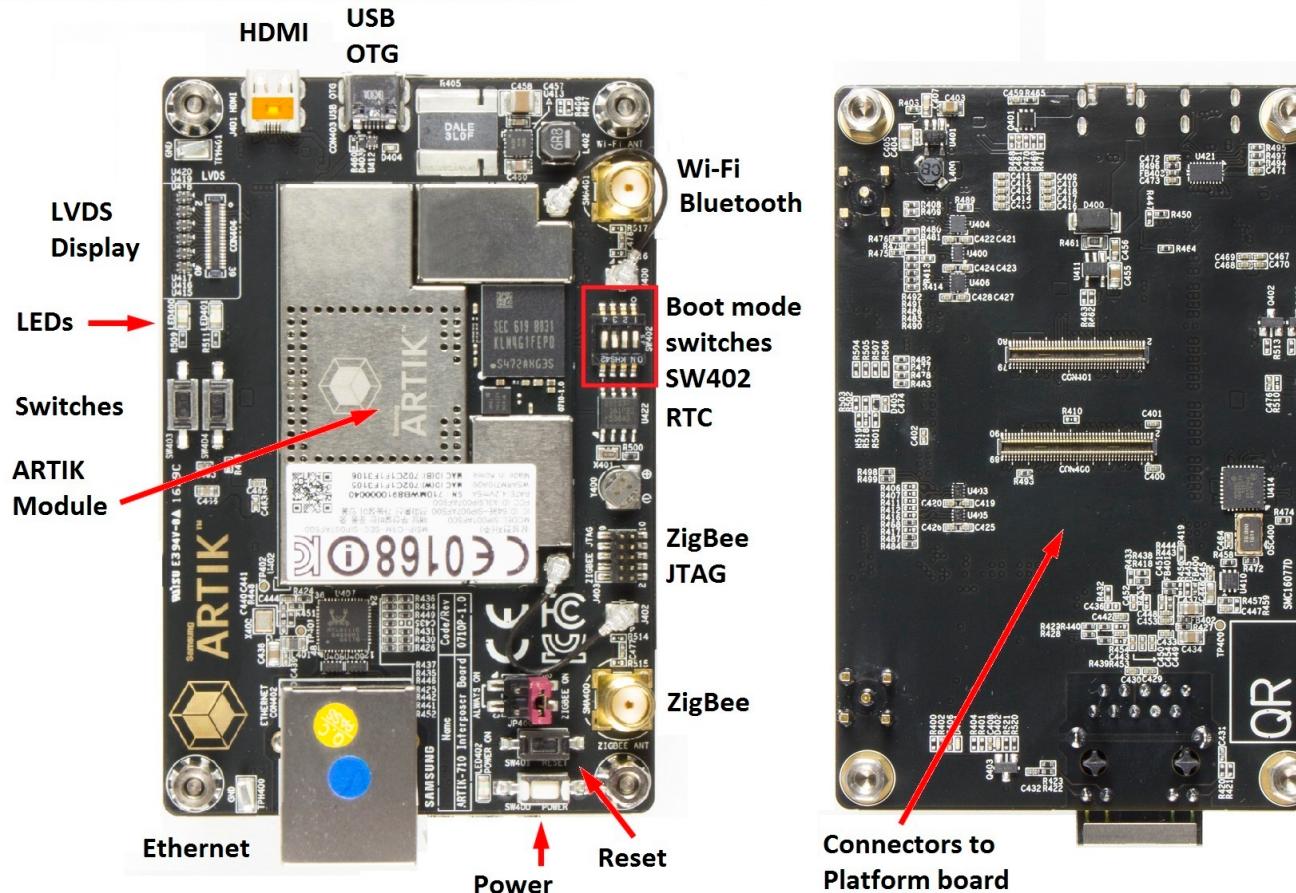


<b>Processor</b>	CPU: 8x ARM® Cortex® A53 @ 1.4 GHz GPU: 3D graphics accelerator
<b>Memory</b>	DRAM: 1 GB DDR3 @ 800 MHz Flash: 4 GB eMMC v4.5
<b>Multimedia</b>	Camera I/F: 4-lane MIPI CSI Display: 4-lane MIPI DSI up to FHD@24 bpp, LVDS, HDMI v1.4 Audio: I²S audio interface
<b>Connectivity</b>	WLAN (Wi-Fi): IEEE 802.11 b/g/n/ac Bluetooth: 4.1+ Smart 802.15.4: Zigbee, Thread Ethernet: 10/100/1000 Base-T MAC (external PHY required)
<b>Security</b>	Secure element, EAL Level 5, unique device certificate and keys, PKI with mutual authentication to cloud, hardware crypto engine; secure boot*, KMS*, TEE*, <small>*S-modules</small>
<b>I/O</b>	GPIO, I²C, I²S, SPI, UART, PWM, SDIO, USB 2.0, JTAG, analog input
<b>Temperature range</b>	0° to 70° (°C)
<b>Size</b>	36 mm W x 49 mm H x 3.4 mm D

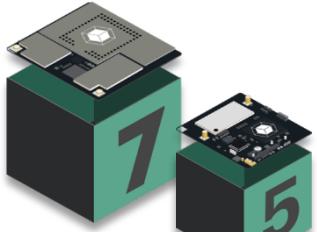
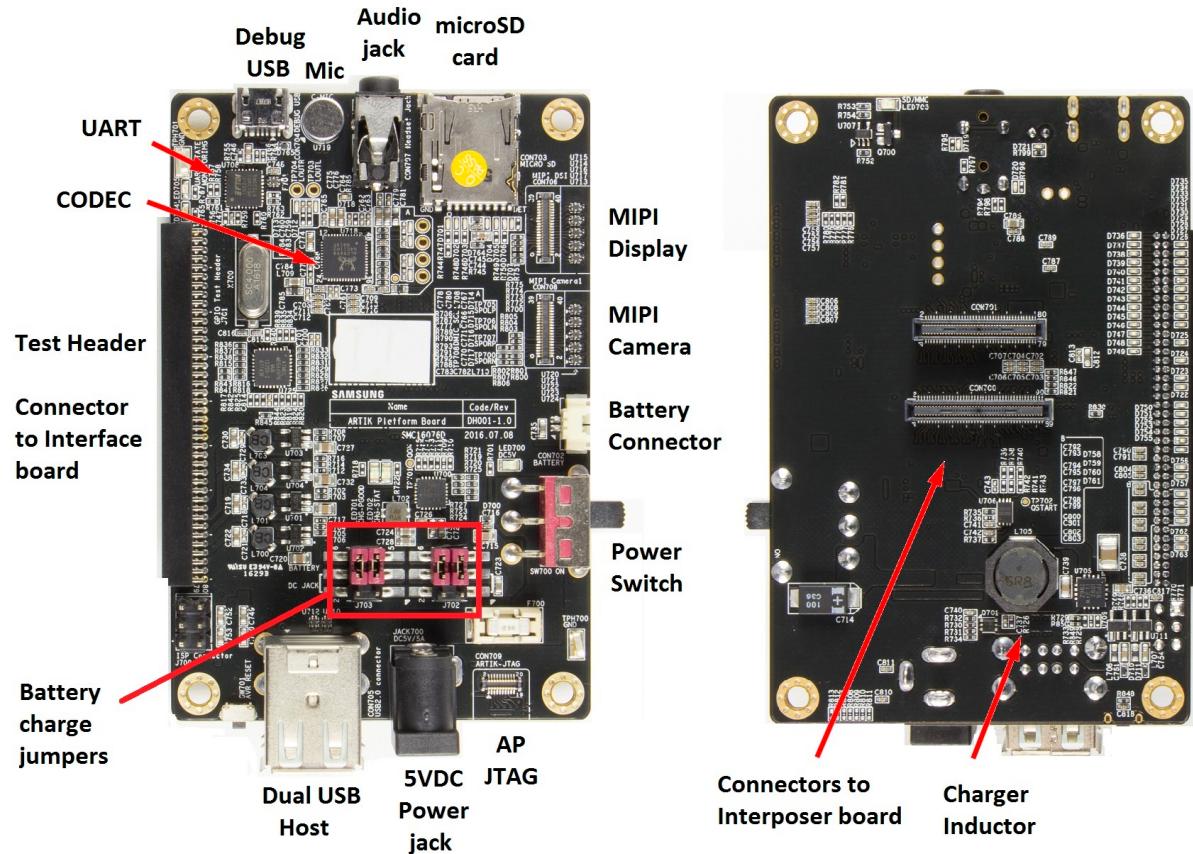
# ARTIK High-end module development board



# ARTIK High-End Module Interposer Board



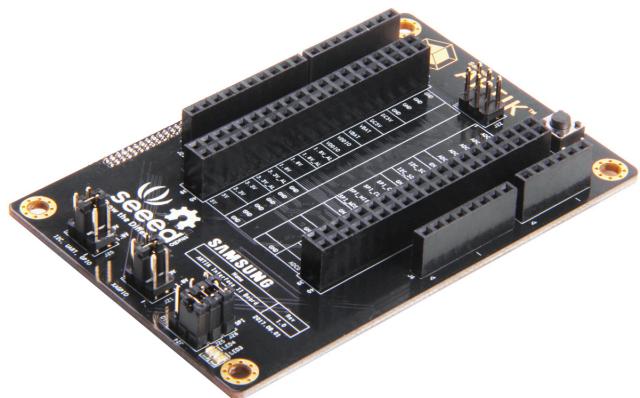
# ARTIK Gateway Module Platform Board



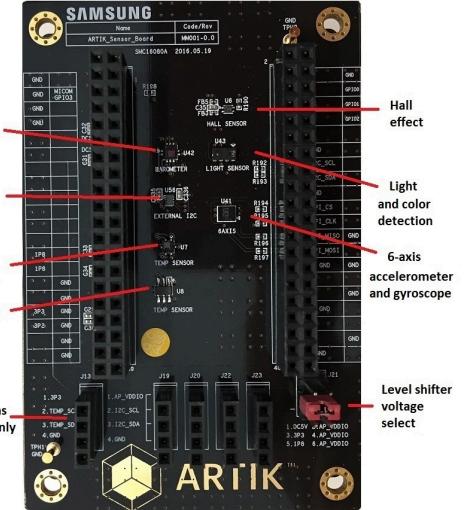
# ARTIK Gateway Module Expansion Boards



Interface Board

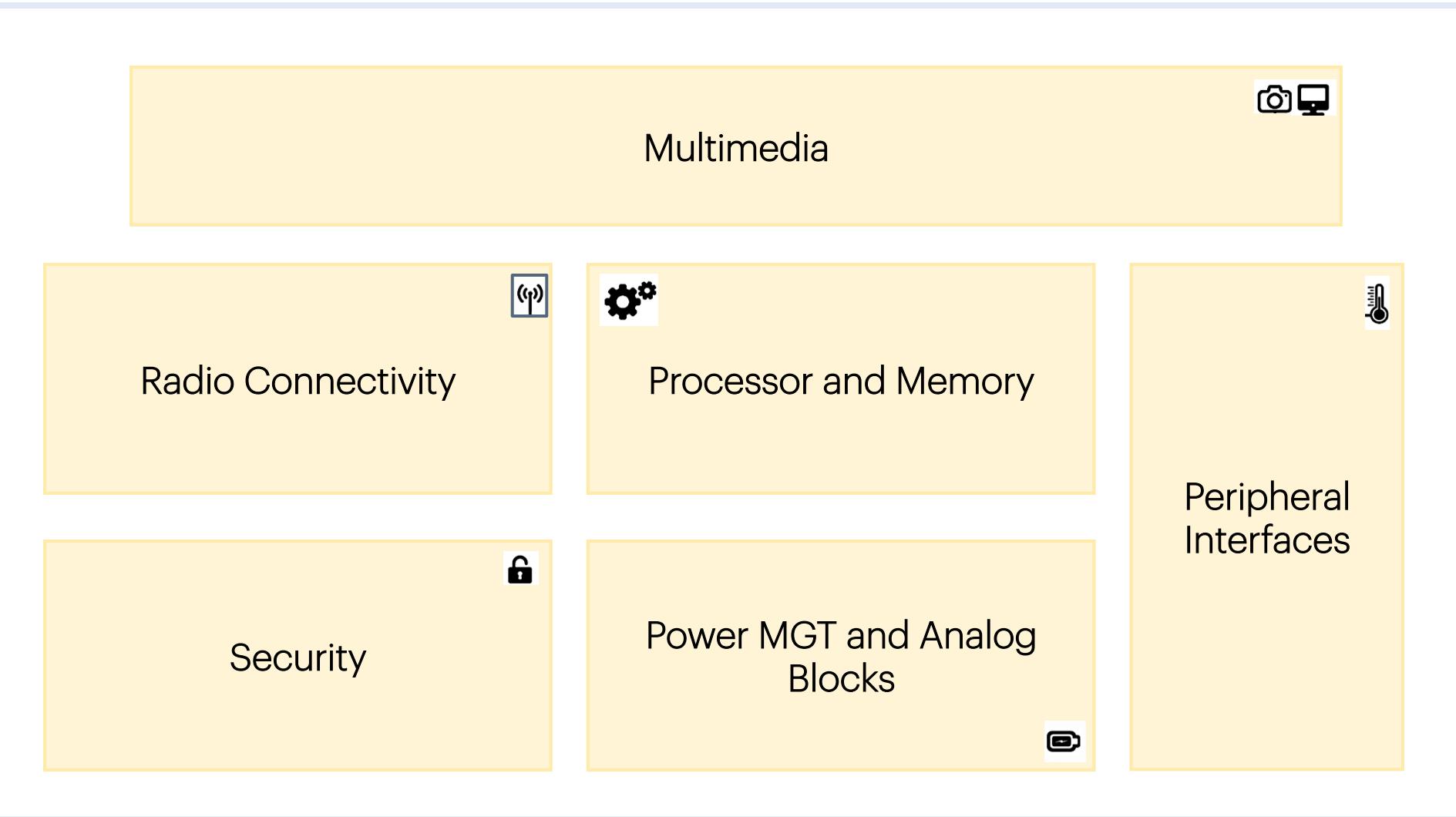


Interface Board II

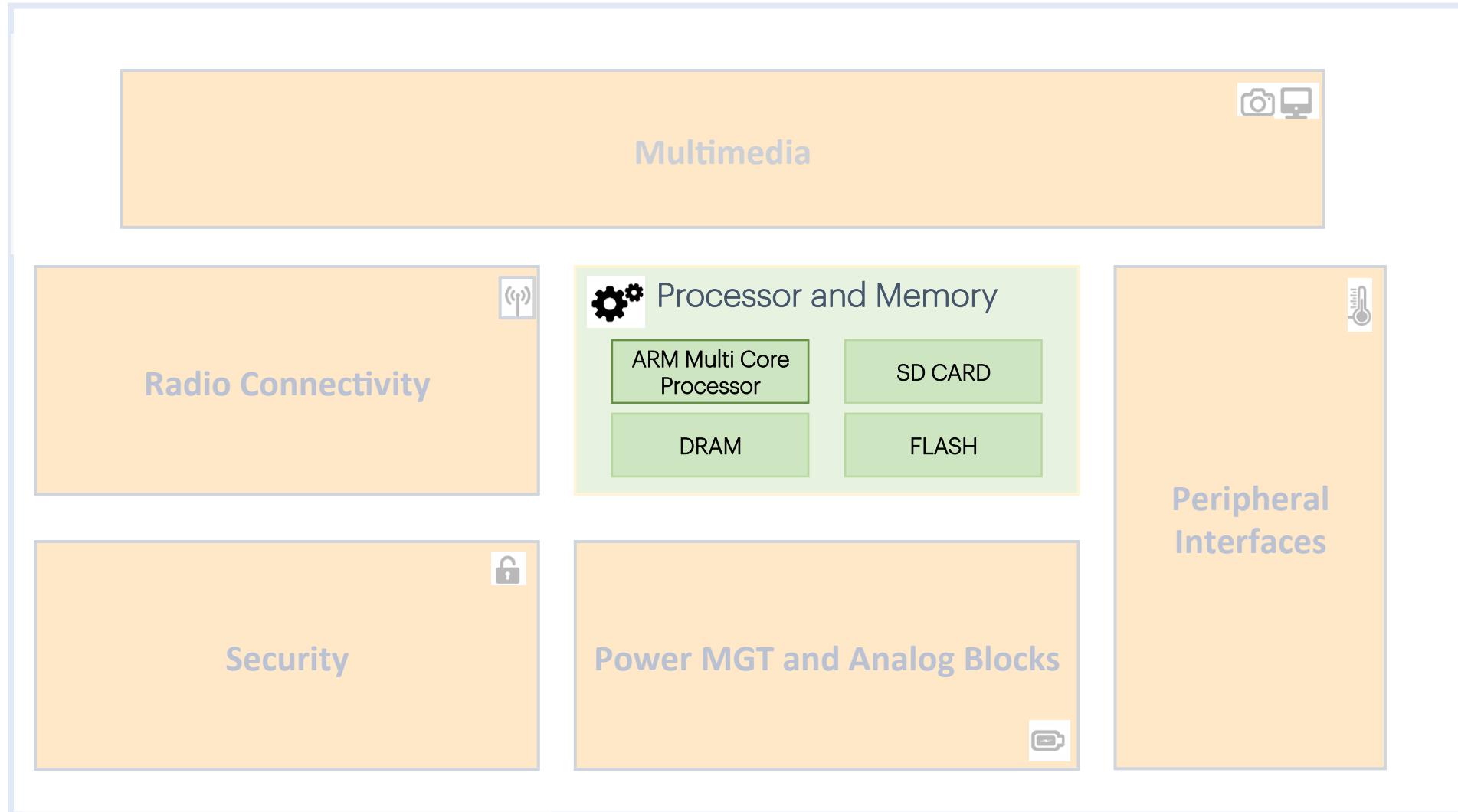


Sensor Board

# Product Details



# Product Details – Processor and Memory



# Radio Connectivity

Radio	Data Rate	520	530	710
BLE	<1Mbps	✓	✓	✓
BT	1-3Mbps	✓	✓	✓
ZigBee	10-100Kbps	✓	✓	✓
Thread	10-100Kbps	✓	✓	✓
Wi-Fi	10-100Mbps	✓	✓	✓
Ethernet		✓	✓	✓

\*Z-wave and Sigfox chip set is on 520 development boards

# Peripheral Interfaces + Power MGT & Analog blocks

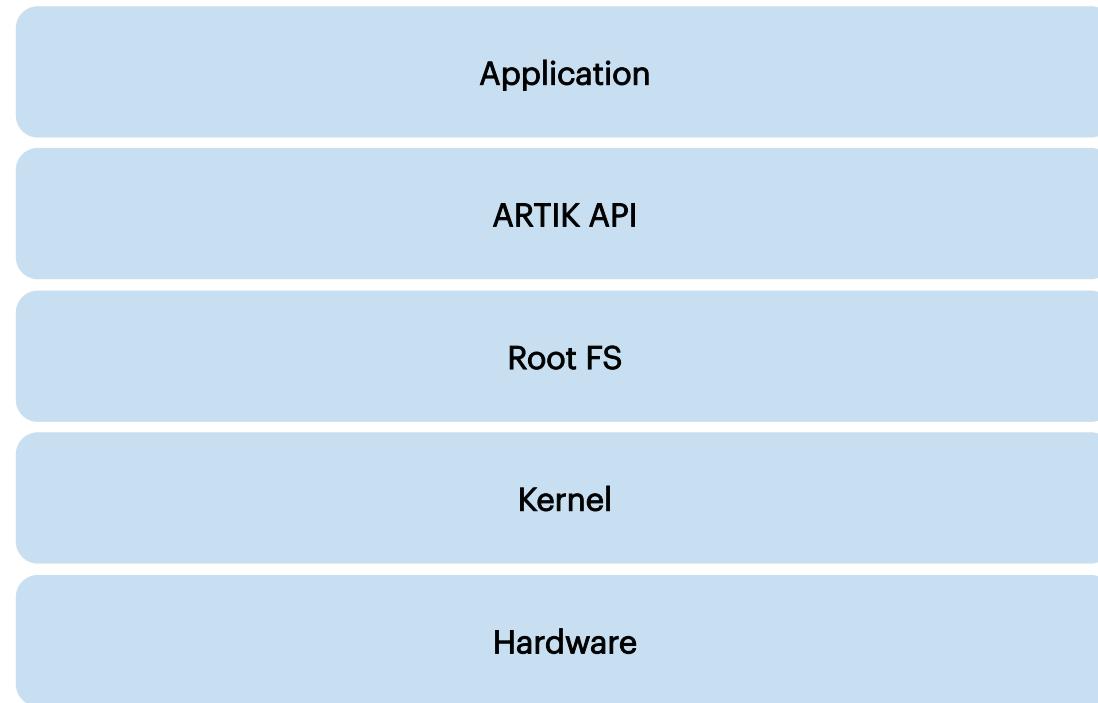
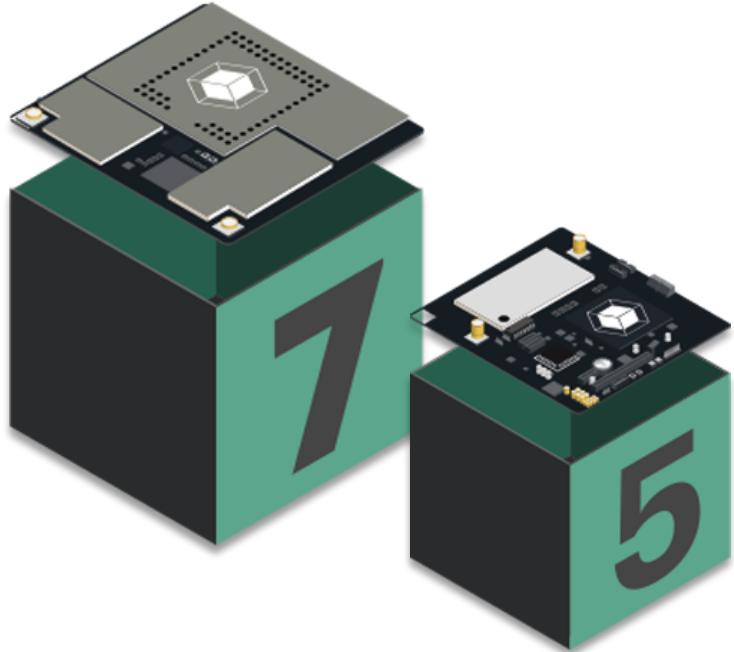
	<b>520</b>	<b>530</b>	<b>710</b>
Peripheral Interfaces	I2C	6	3
	SPI	2	2
	GPIO	100	107
	UART	2	3
	USB	USB 2.0*	USB 2.0
Analog and Power MGT	ADC	2	6
	PWM	2	2
	PMIC	✓	✓

\*USB device mode only for 520, rest of the module is both device and host mode.

# Product Details - Multimedia

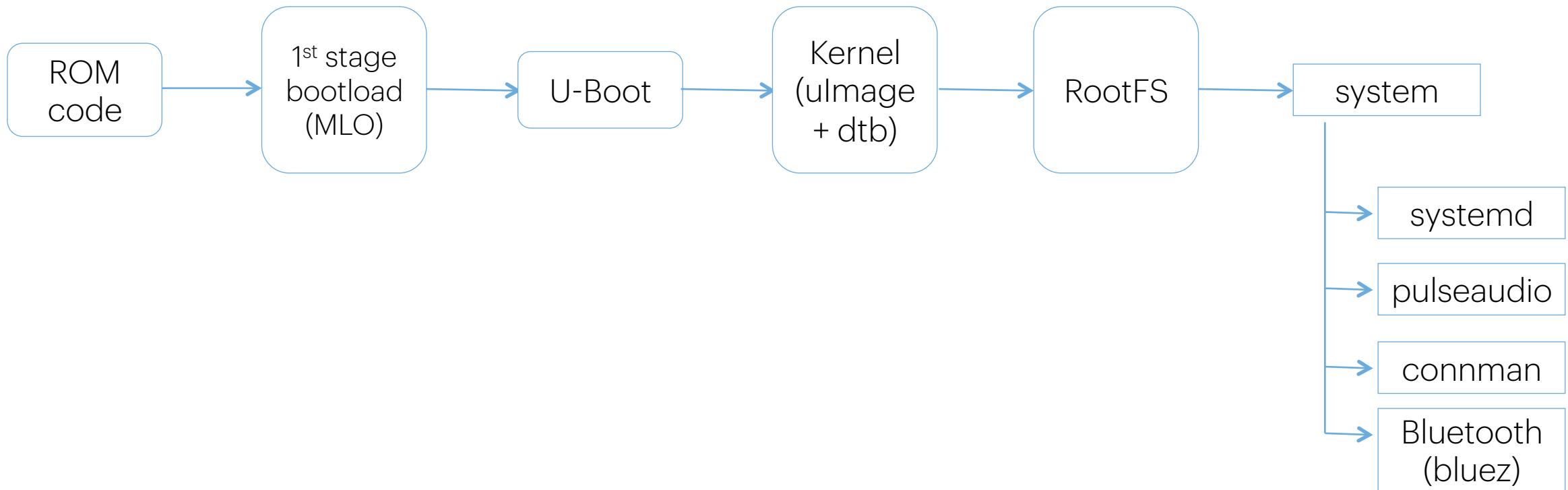
	<b>520</b>	<b>530</b>	<b>710</b>
I2S	1x	2x	2x
HDMI (audio + video)	n/a	1080p @ 60fps	1080p @ 60fps
MIPI – DSI	2-lane 540p @ 24bpp	4-lane 1080p @ 60fps	4-lane 1200p @ 24bpp
MIPI – CSI	2-lane 3MP @ 30fps	4-lane 1080p @ 30fps	4-lane 1080p @ 30fps
LVDS	n/a	720p @ 60fps	720p @ 60fps

# ARTIK Gateway Software Stack

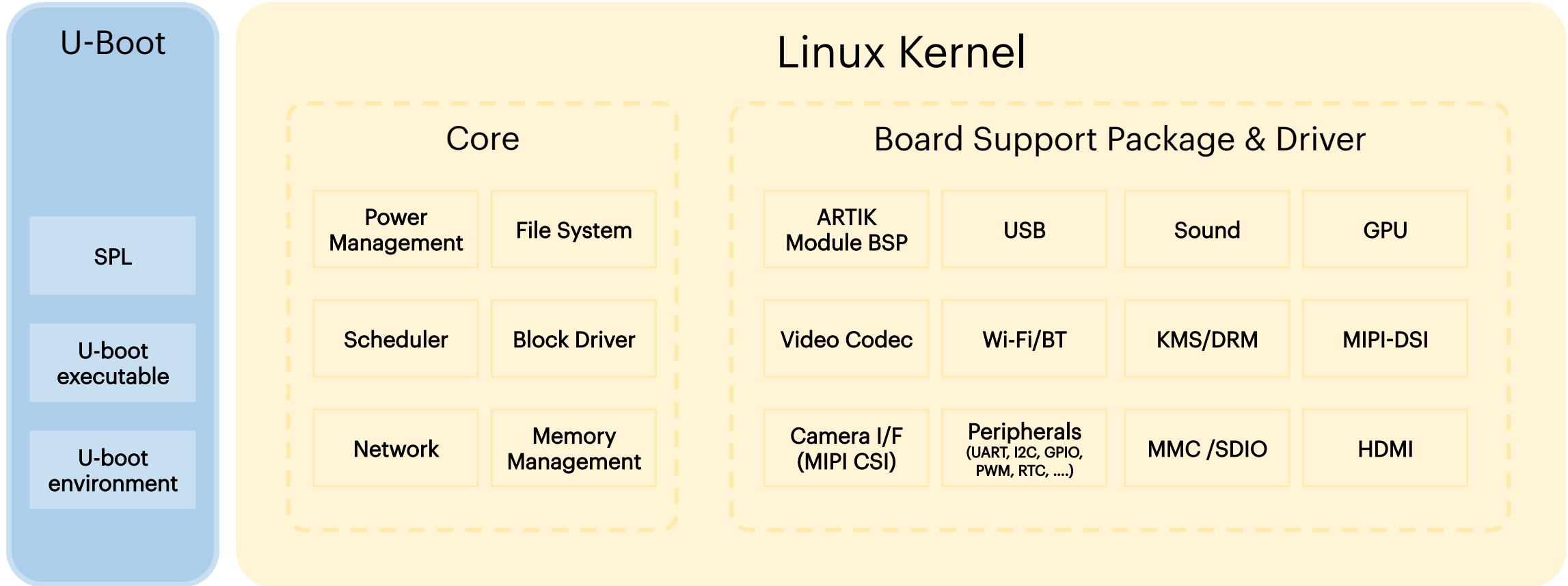


# Boot Modes and Sequence

## eMMC Boot Sequence

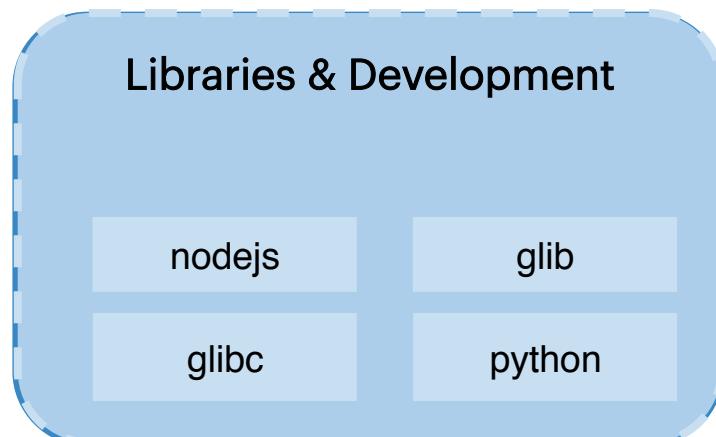
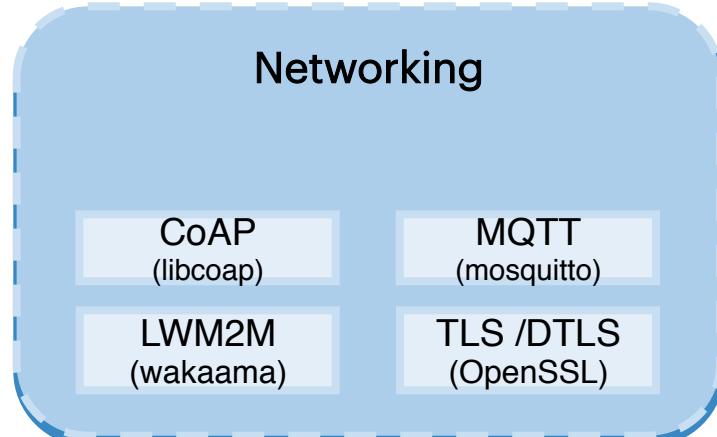
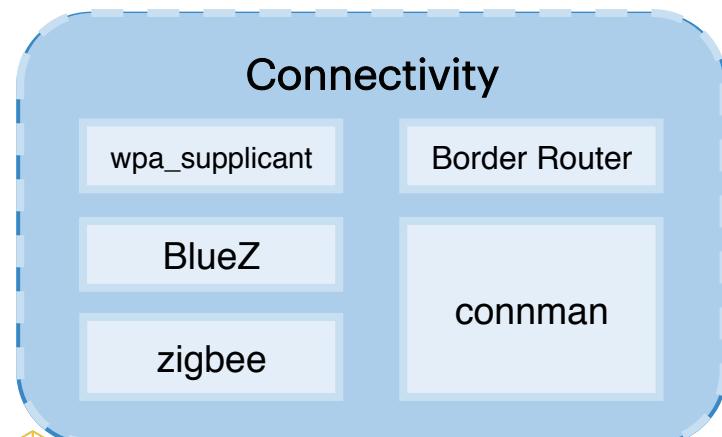
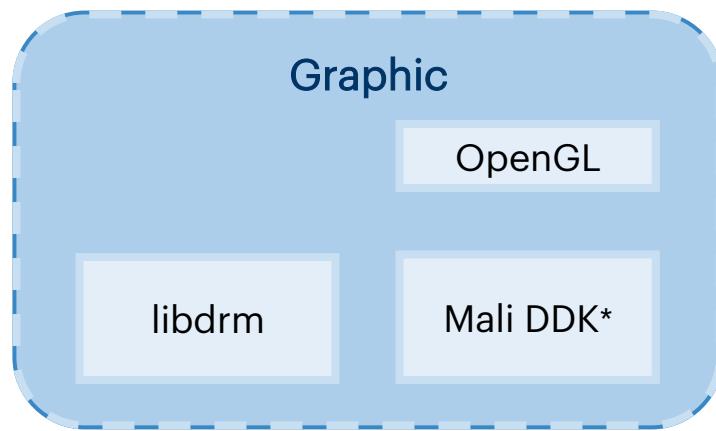
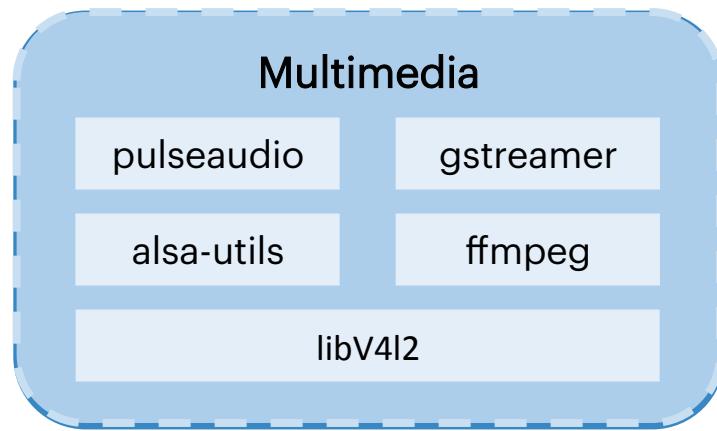
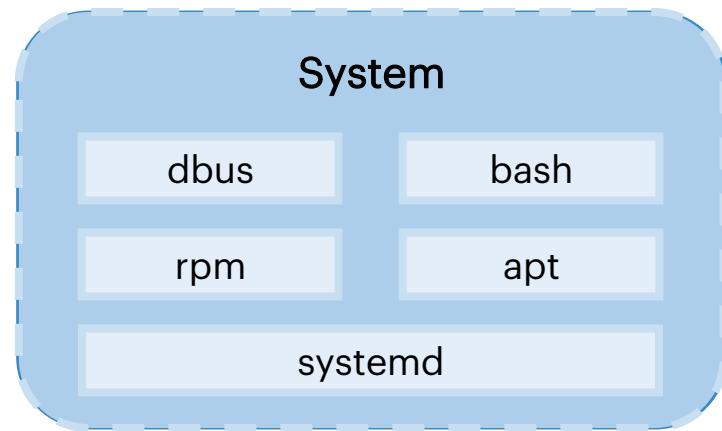


# U-Boot and Linux Kernel Architecture

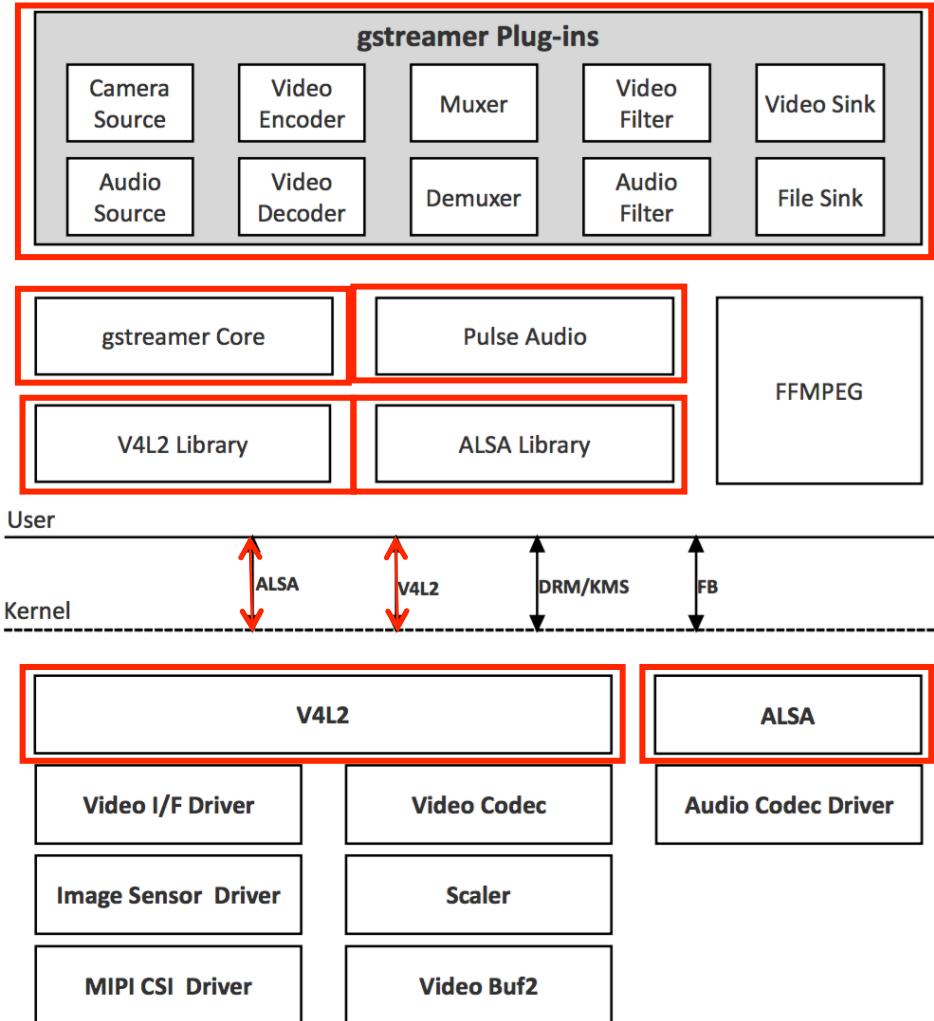


# Architecture of Rootfs

## Rootfs

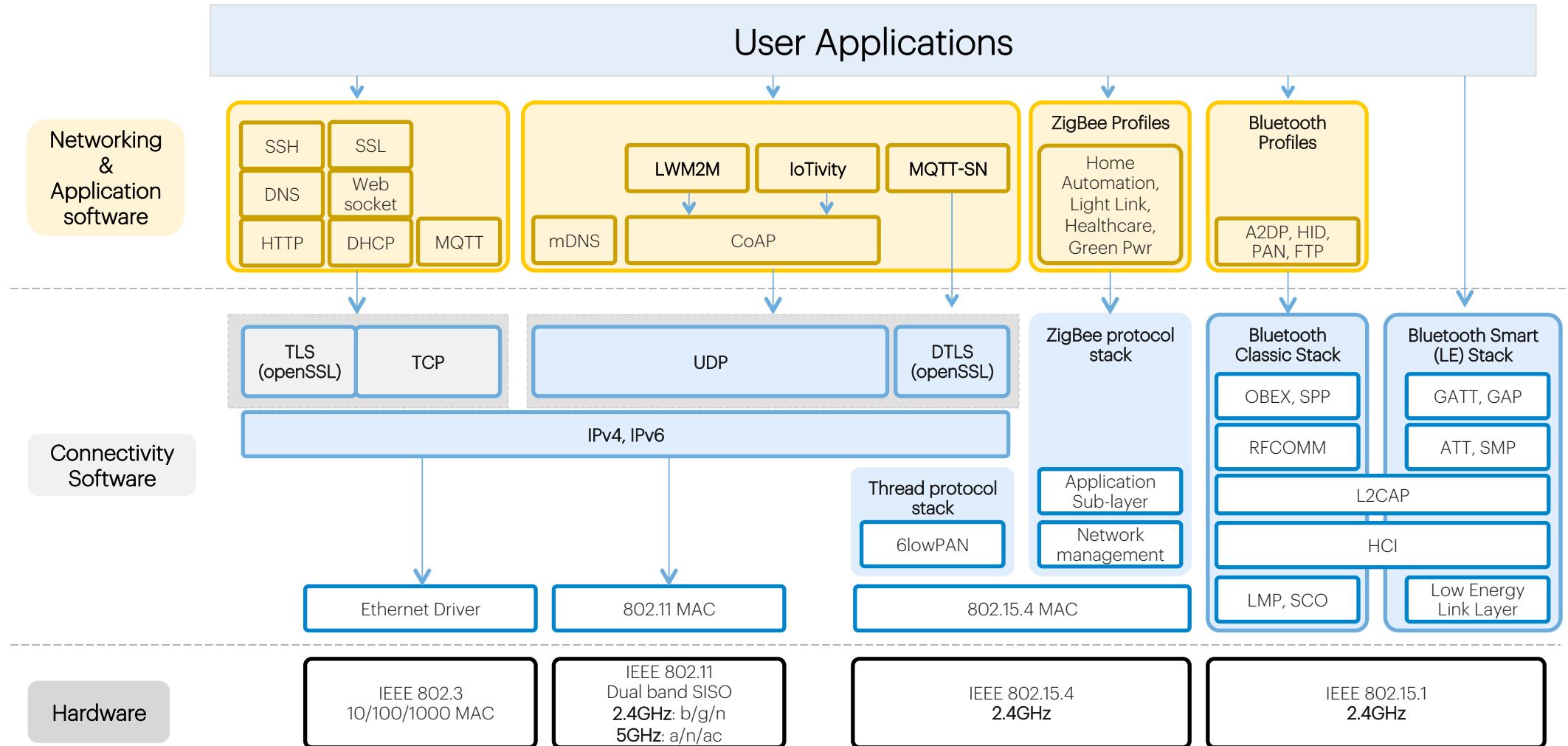


# Multimedia Architecture

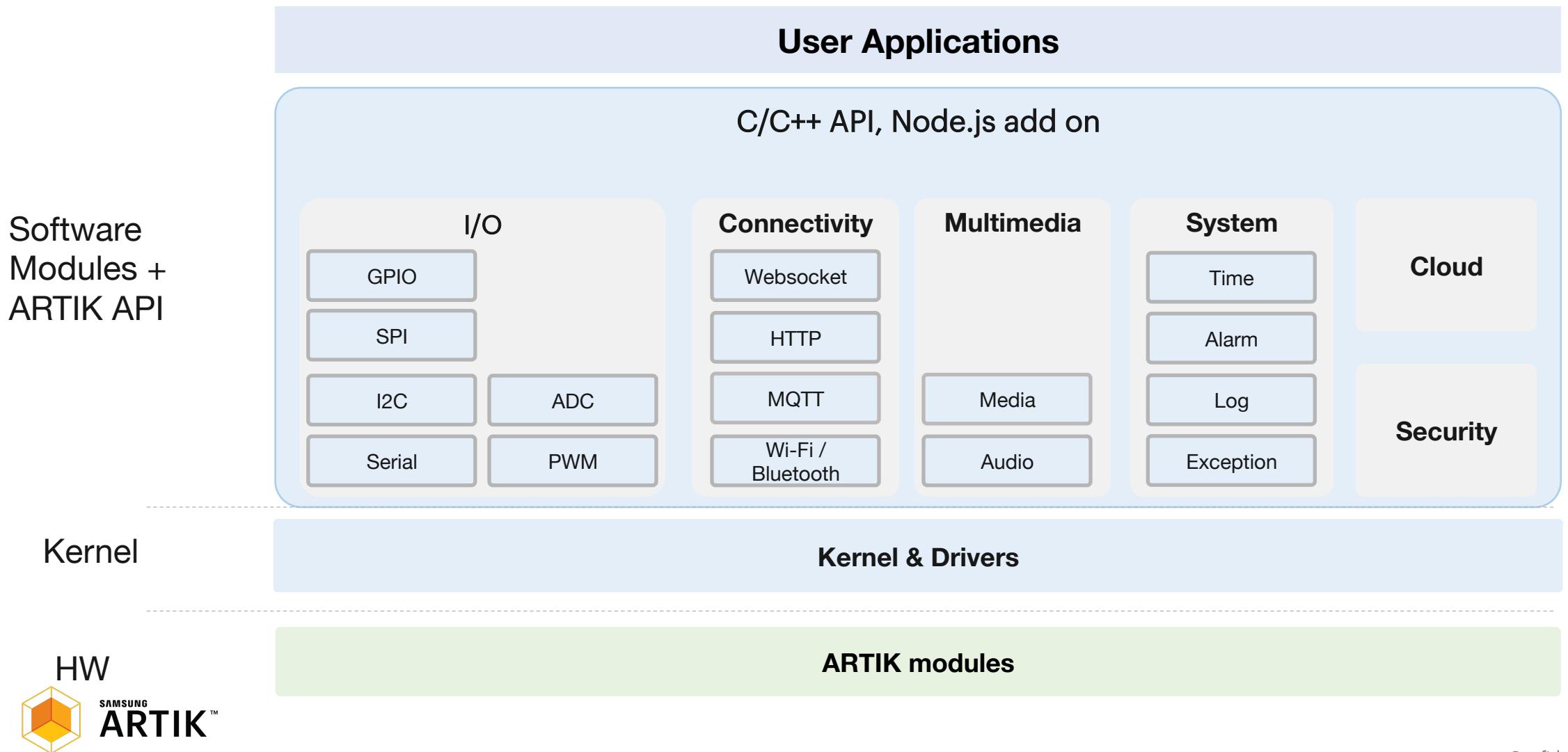


- ALSA lib is a framework that provides a software API for audio device drivers
- Pulse Audio is based on ALSA lib for supporting sound. It runs a sound server.
- Video for Linux Version 2 (V4L2) is collection of device drivers and API for supporting real-time video capture on Linux systems

# Network Stack



# ARTIK SDK (5, 7 series)



# ARTIK Gateway Module Development

# ARTIK IDE

workspace1 - C/C++ - ARTIK IDE

File Edit Source Refactor Navigate Search Project Run Samsung ARTIK Window Help

No Launch Configurations on: --- Quick Access C/C++

Project Explorer artik053s Binaries Includes Debug artik\_adc.c artik\_onboarding\_cloud.c artik\_onboarding\_config.c artik\_onboarding\_lwm2m.c artik\_onboarding\_rest.c artik\_onboarding\_wifi.c artik\_onboarding.c artik\_onboarding.h

An outline is not available.

Problems Tasks Console Properties Search

CDT Build Console [artik053s]

```
arm-none-eabi-gcc -D_TINYARA_ -I"C:/ARTIK/SDK/A053/v1.6/libsdk/extra/include" -I"C:/ARTIK/SDK/A053/v1.6/^-^
bash.exe: warning: could not find /tmp, please create!
Finished building: ../artik_onboarding_wifi.c

Building target: artik053s
Invoking: ARTIK GCC C Linker
arm-none-eabi-ld -T"C:/ARTIK/SDK/A053/v1.6/common/scripts/flash.ld" -nostartfiles -nodefaultlibs -L"C:/ARTIK/SDK/A053/v1.6/^-^
bash.exe: warning: could not find /tmp, please create!
Finished building target: artik053s

/usr/bin/make --no-print-directory post-build
add header and add tailer
arm-none-eabi-objcopy -O binary ./"artik053s" ./tinyara.bin;"C:/ARTIK/SDK/A053/v1.6/common/tools/s5jchksum.|^-^
bash.exe: warning: could not find /tmp, please create!
```

12:13:27 Build Finished (took 5s.891ms)

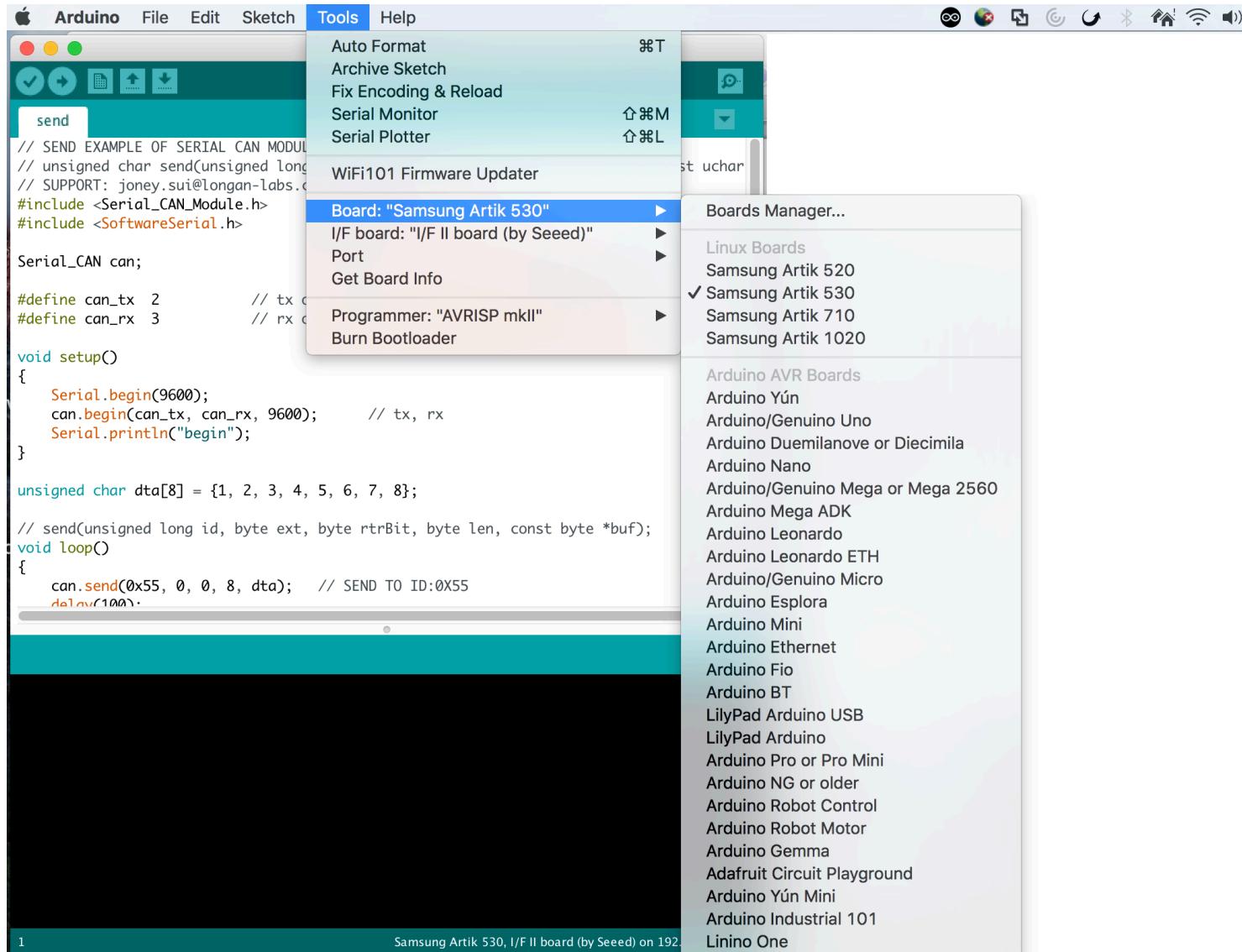
Activate Windows  
Go to Settings to activate Windows.

SAMSUNG ARTIK™



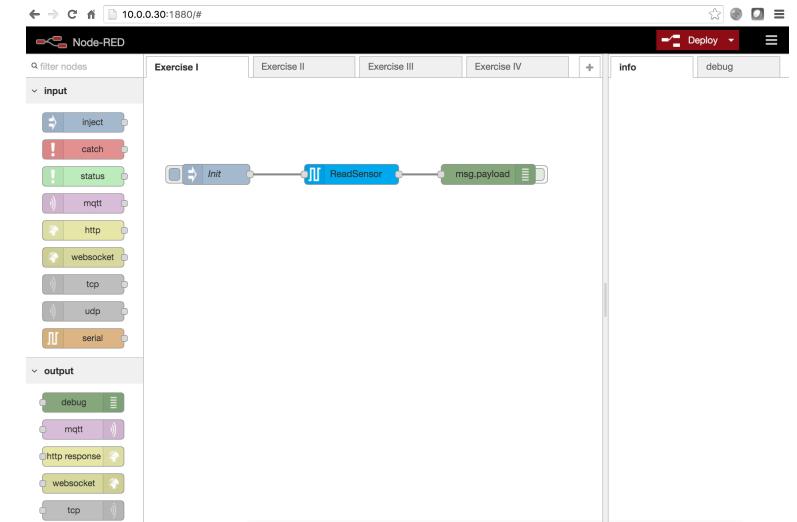
gcc-arm-linux-gnueabihf

# Arduino



# Node-RED

- A visual tool for wiring the internet of things, based on Node.js
- Utilizes flow programming technique
- Construct program flow by drag-and-drop
- You have the option not to write code
- Growing ecosystem
- Cloud-based solutions: IBM Bluemix, Front end Node-RED



# Native Development

- C/C++: Most popular programming languages for embedded devices. e.g, ARTIK SDK
- Python: Rich libraries
- JS: Node.js is the most popular JavaScript runtime for high-end IoT devices.
- Java: e.g, Eclipse Kura etc.

# 3<sup>rd</sup> party Libraries/APIs

- Connectivity: bluez, wpa\_supplicant, Silicon Labs(ZigBee, Thread)
- Multimedia: PyAudio, OpenCV, Speech Recognition etc.
- ML frameworks: TensorFlow (Lite) etc.

# 3<sup>rd</sup> party Frameworks, Solutions

Gateway Solutions:



Communication Protocols/Frameworks:

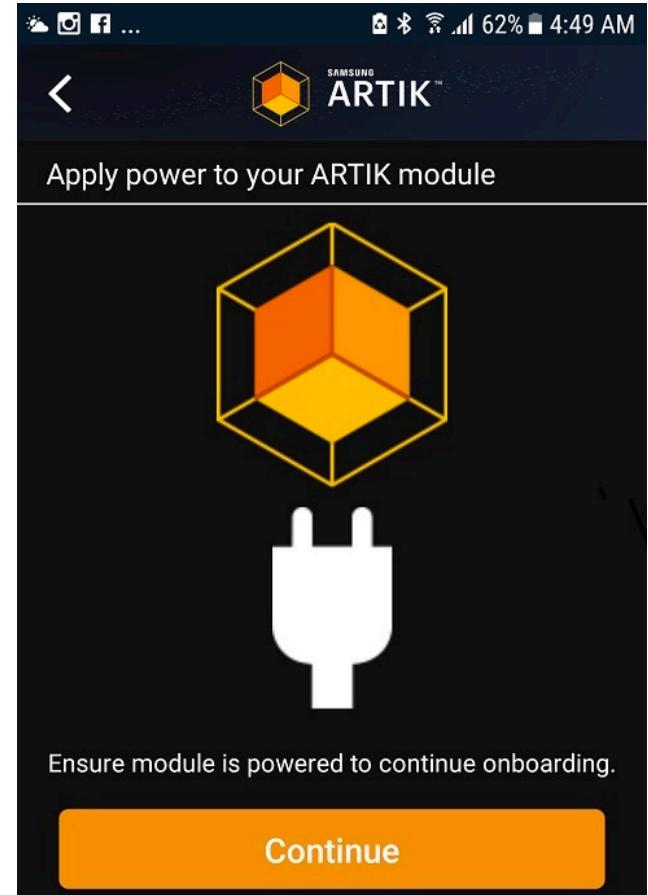
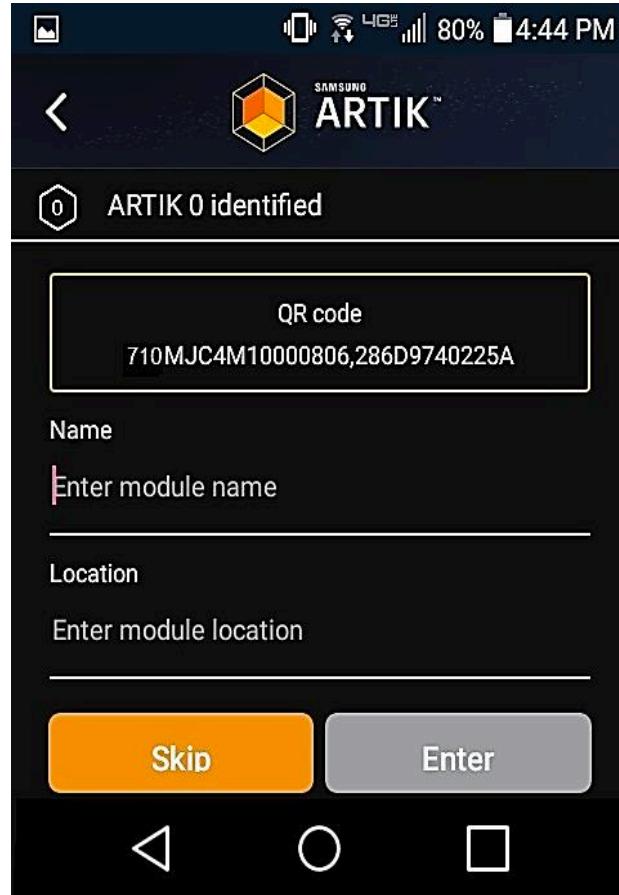
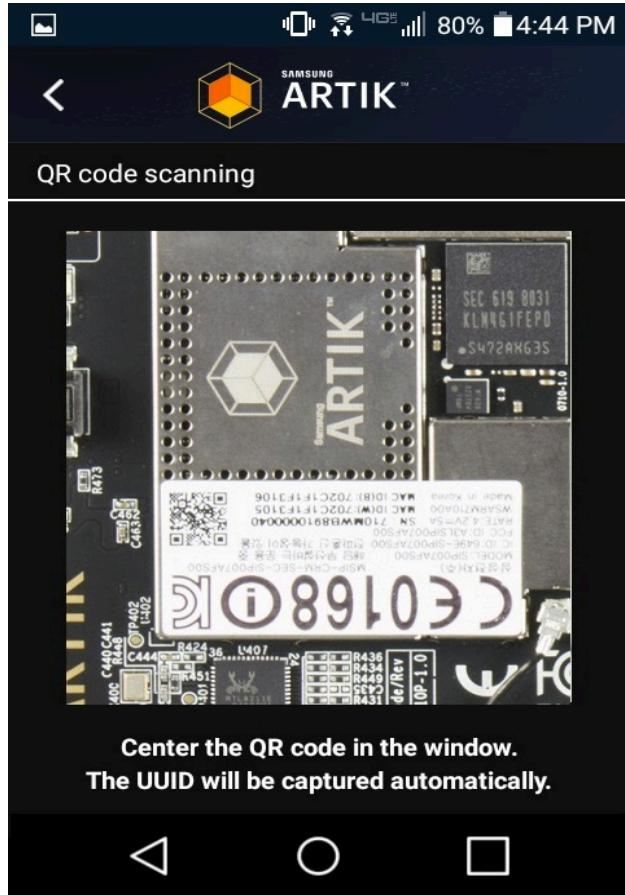


# ARTIK End-to-end solution

# ARTIK Gateway Onboarding

- Support BLE onboarding on Gateway modules
  - QR code contains device information like MAC address, through which the mobile app learns the BLE service UUID of the ARTIK controller.
  - Mobile App scans for BLE devices and matches the service UUID with the one from the QR code.
  - Connection Manager connects ARTIK Gateway to WiFi.
  - Mobile App interacts with BLE on-boarding service through BLE GATT profile.

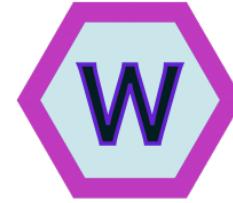
# Onboarding app



# Device Management and LWM2M stack

- Lightweight M2M (LWM2M) is a device lifecycle management specification
- Provides a specification for functions like: firmware upgrade, provisioning of certificates, access control policies, connectivity monitoring etc.
- Based on CoAP protocol
- LWM2M allows the use of UDP for communication between client and server
- DTLS security for communication between an LWM2M client and ARTIK Cloud server(an LWM2M server).

# Eclipse Wakaama



- Eclipse Wakaama is an open source implementation of the OMA LWM2M protocol in C language.
- Includes 3 layers: LWM2M Protocol, CoAP and DTLS layer.
- Implements LWM2M Client, LWM2M Server and LWM2M Bootstrap Server.



# Device Management

The screenshot displays the ARTIK Device Management interface across four panels:

- Left Panel (Device Types):** Shows a sidebar with various device categories and a selected "Device Management" item.
- Top Center Panel (Philips Respironics):** A "Device Management / Properties" page with a sub-section titled "Server Properties". It explains how server properties can be custom-defined and stored in the ARTIK cloud services. A "ADD SERVER PROPERTIES" button is present.
- Middle Center Panel (Device Properties):** A "Device Properties" table showing a list of properties with their types and values. Properties include: akc (Group), update (Boolean, None), device (Group), availablePowerSources (Long, None), batteryLevel (Long, %), batteryStatus (Long, %), currentTime (Long, None), deviceType (String, None), errorCode (Long, None), factoryReset (Boolean, None), firmwareVersion (String, None), hardwareVersion (String, None), manufacturer (String, None), memoryFree (Long, bit\*8000), memoryTotal (Long, None), and modelNumber (String, None). A "Support" button is at the bottom right.
- Right Panel (artik053):** A "Device Management" page showing a list of devices. The "Device Management" menu item in the sidebar is highlighted with a red box. The main table lists four devices:

DEVICE ID	SERIAL NUMBER	CREATED	CONNECTION STATUS	LAST CONNECTED
6941eac41a604a8a8a64a4fb2f7e5930	No Data	15/Nov/17 05:45 PM	Never connected	Never
f64ac03cbd414b2882b207e97e6b02c	No Data	23/Nov/17 02:05 AM	Never connected	Never
5a9c3df6af9448e683b864b189dc6990	No Data	14/Jan/18 09:30 PM	Never connected	Never
3d96739259dd4bb5b2f8dfc32817fe39	1234567890	Yesterday at 05:57 PM	Active (websocket)	04/Feb/18 07:59 PM

# Device Management

### Upload a New OTA Update Image

OTA-update-sample-app-1.2.0-armhf-signed.tar.xz (5.02 KB) Delete

**TYPE** Application

**VERSION** v1.2-0

**DESCRIPTION** Signed OTA application image

**UPLOAD**

### Step 1 of 2: Choose Image File

SEARCH FOR KNOWN OTA UPDATE IMAGES

FILE	UPDATE TYPE	VERSION	SIZE	UPLOAD TIME
ota-edge-node-a05x-v1.5.3.bin Image to be OTAAed for Lab exercise	Edge Node	v1.5.3	567.87 KB	28/Jul/17 09:54 PM

Showing 1 to 1 of 1 OTA Update Images

**NEXT** CANCEL

### Step 2 of 2: Perform/Schedule Update

**Selected Image** ota-a05x-firmware-1.5.4.bin (568 KB) CHANGE

UPDATE TYPE	VERSION	UPLOAD TIME
Edge Node	1.5.4	19/Jun/17 10:47 AM

**Device** 1 Device in ARTIK 053

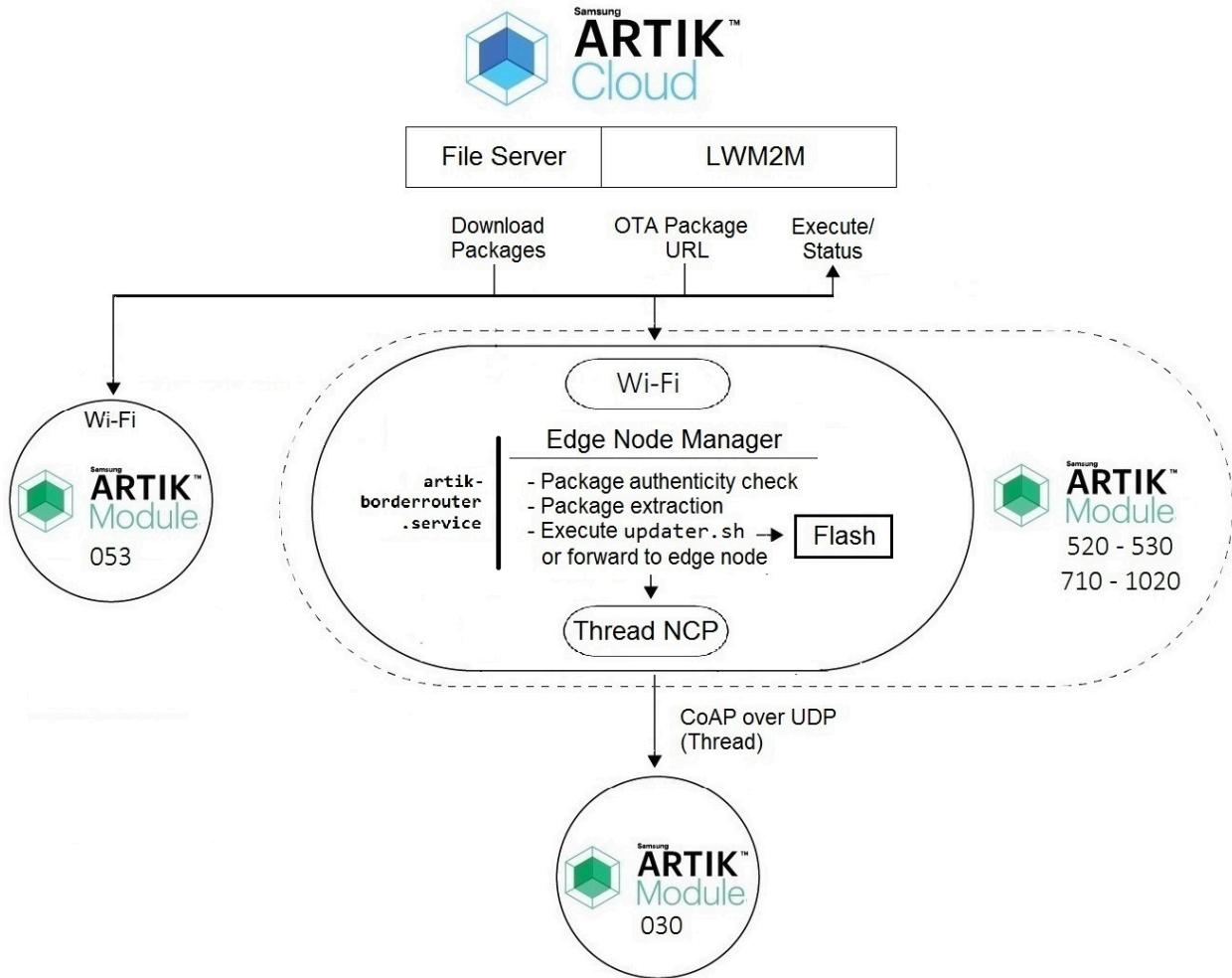
**Schedule (Optional)** Perform this OTA update with the selected image immediately, or specify a time to schedule for a time in the future.

**DATE & TIME** Select a date and time

**TIMEZONE** (UTC+01:00) Paris

**PERFORM OTA UPDATE** CANCEL

# Edge Node Manager



Manages the connection to edge devices

Manages the OTA on edge devices

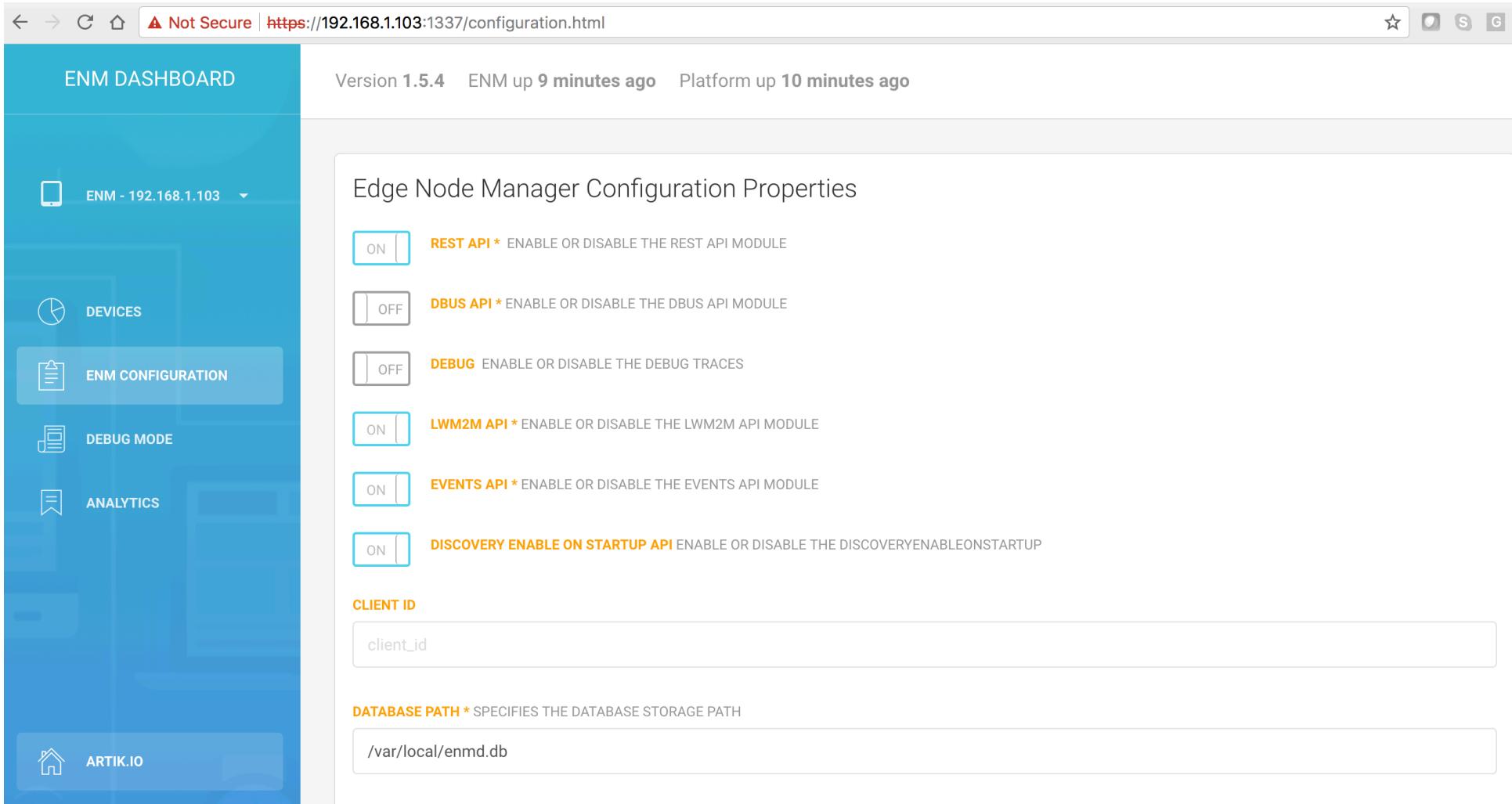
# Edge Node Manager Dashboard

The screenshot shows the ENM DASHBOARD interface. At the top, it displays the version as Version 1.5.4, with the message "ENM up 17 minutes ago" and "Platform up 17 minutes ago". On the left sidebar, there are four main menu items: DEVICES (selected), ENM CONFIGURATION, DEBUG MODE, and ANALYTICS. At the bottom of the sidebar is the ARTIK.IO logo. The main content area contains a table listing detected devices. The table has columns for DEVICE, UUID, STATE, OS, FIRMWARE VERSION, HARDWARE MODEL, CLOUD, DETAILS, and DELETE. Two devices are listed:

DEVICE	UUID	STATE	OS	FIRMWARE VERSION	HARDWARE MODEL	CLOUD	DETAILS	DELETE
Edge Node Manager - 192.168.1.103	d2dd0fd8-6764-418f-9a29-702c1f378685	Online	UNRELEASED	1.5.4-1	ARTIK530S	X		
marka020	d2dd0fd8-6764-418f-9a29-000b5727c0db	Online	3.5.2	1.0.3	ARTIK-020			

Below the table is a "Refresh" button and an "AUTO-REFRESH EVERY 10 SECONDS" checkbox. A message at the bottom indicates "2 Devices detected". At the very bottom of the dashboard, there are links for "Home" and "Company", and a copyright notice: "© 2017 Samsung ARTIK, The ARTIK End-to-end IoT Platform".

# Edge Node Manager Dashboard (Cont.)



The screenshot shows the ENM DASHBOARD configuration page. The left sidebar lists navigation options: ENM - 192.168.1.103, DEVICES, ENM CONFIGURATION (selected), DEBUG MODE, ANALYTICS, and ARTIK.IO. The main content area displays the Edge Node Manager Configuration Properties. It includes sections for REST API, DBUS API, DEBUG, LWM2M API, EVENTS API, and DISCOVERY ENABLE ON STARTUP API, each with an enable/disable switch. Below these are fields for CLIENT ID (containing "client\_id") and DATABASE PATH (containing "/var/local/enmd.db"). The top status bar indicates Version 1.5.4, ENM up 9 minutes ago, and Platform up 10 minutes ago.

ENM DASHBOARD

Version 1.5.4 ENM up 9 minutes ago Platform up 10 minutes ago

### Edge Node Manager Configuration Properties

**REST API \*** ENABLE OR DISABLE THE REST API MODULE  
 ON  OFF

**DBUS API \*** ENABLE OR DISABLE THE DBUS API MODULE  
 ON  OFF

**DEBUG** ENABLE OR DISABLE THE DEBUG TRACES  
 ON  OFF

**LWM2M API \*** ENABLE OR DISABLE THE LWM2M API MODULE  
 ON  OFF

**EVENTS API \*** ENABLE OR DISABLE THE EVENTS API MODULE  
 ON  OFF

**DISCOVERY ENABLE ON STARTUP API** ENABLE OR DISABLE THE DISCOVERYENABLEONSTARTUP  
 ON  OFF

**CLIENT ID**  
client\_id

**DATABASE PATH \*** SPECIFIES THE DATABASE STORAGE PATH  
/var/local/enmd.db

# ARTIK Gateway Module

## Use Cases and

## Ecosystem

# Customer Use Cases



**Legrand:** Global residential and commercial digital building infrastructure

**Challenge:** Transform product line to meet new connected digital mkt requirements.  
Fast time to mkt. Interoperability.

**Products:** ARTIK Ox, ARTIK 5/7 secure system-on-modules, ARTIK cloud services

**Why ARTIK?** Reduced product development time. Built-in software eliminated internal dev skills roadblock. Security allows them to meet new customer reqs. Interoperability expands switch capabilities, helped them get POC with Marriott "Room of the Future".



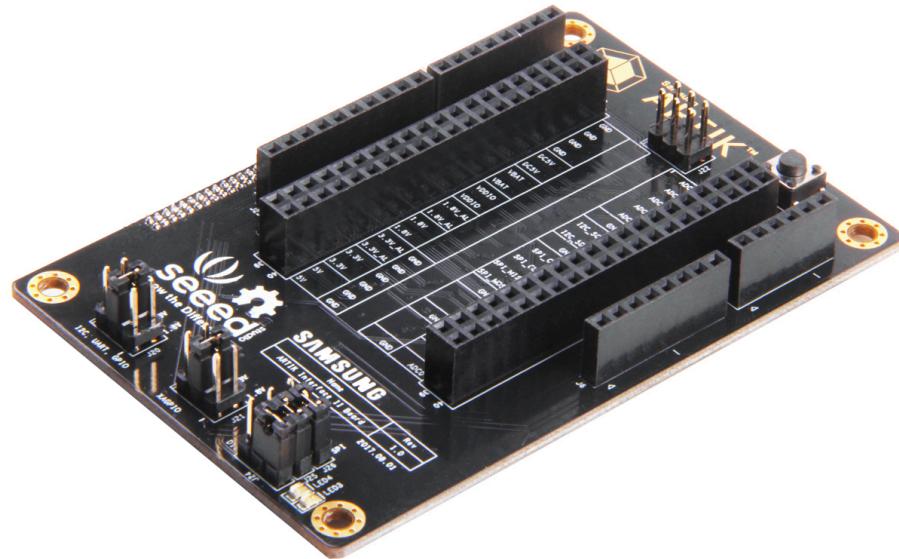
**NDA Customer:** Factory automation provider

**Challenge:** Retrofit customer OT to meet requirements for Industry 4.0, enable access to data and create digital twins for more efficient operations. Ensure secure operations.

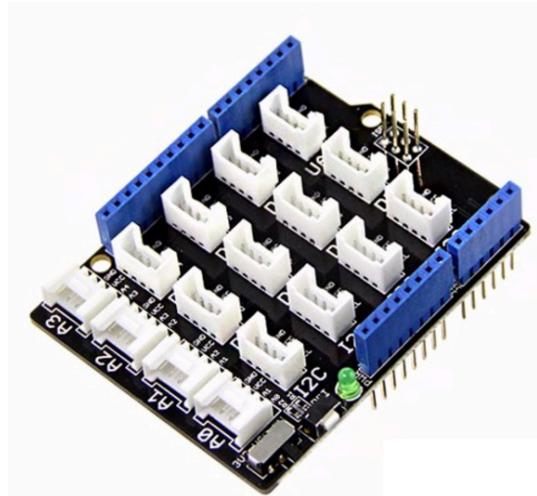
**Products:** ARTIK 05x and 530s secure system-on-module, ARTIK Cloud service, PTC ThingWorx

**Why ARTIK?** Secure gateway solution for their industrial gateway with access to local sensors, ability to do local processing and edge node management, ARTIK Cloud service for onboarding, device management & OTA, data management via integration with PTC Thingworx front end application.

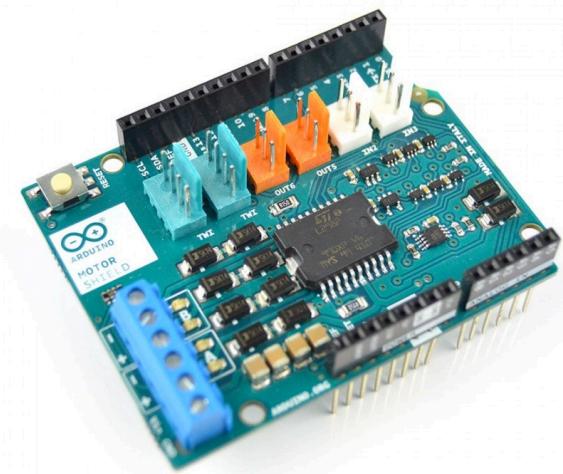
# Arduino Shields



Arduino IF II board



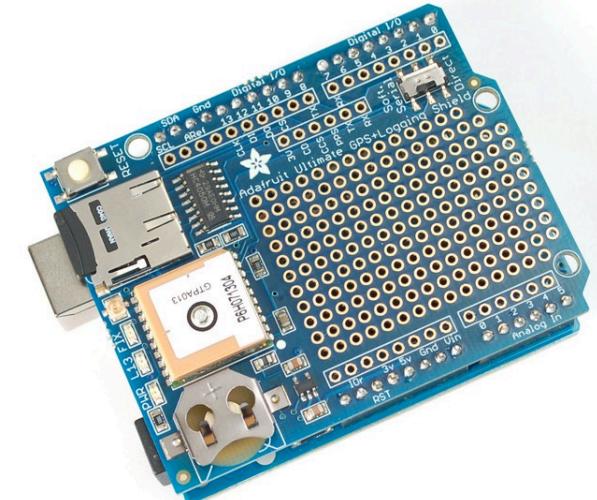
Base Shield



Motor Shield



Relay Shield



GPS Logger Shield

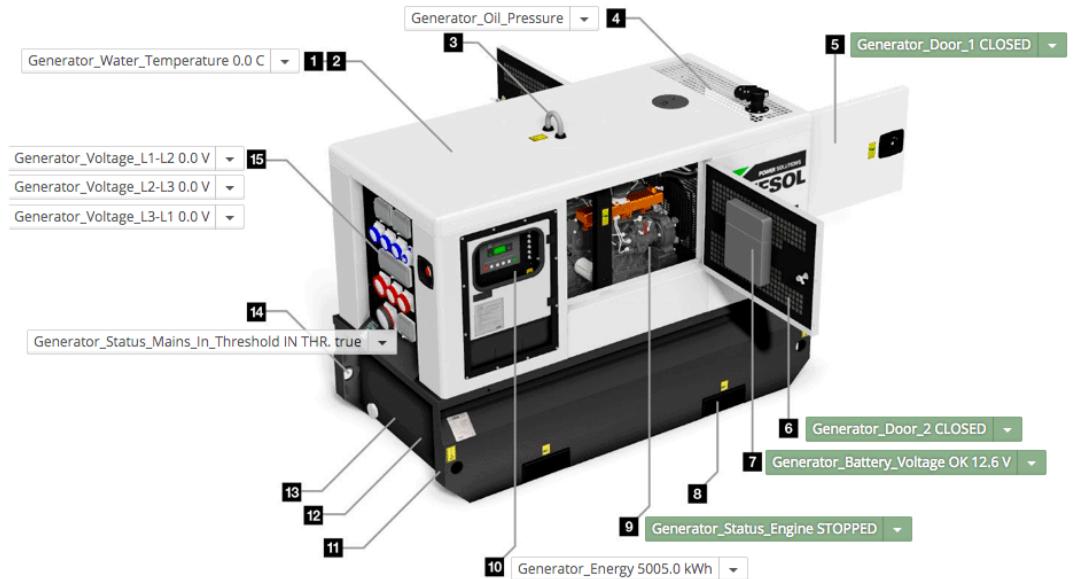
# Kitra GTI ARTIK 710s

Use Kitra GTI as the Industrial IoT Gateway device

**Use case:** Industrial IoT Gateway device, hubs, freight management

**Hardware:** ARTIK 710S

**Software:** Based on your solution



# Long-range Connectivity

## ARTIK 530s with Multi-tech

Provide LTE support on ARTIK 530s with Multi-tech modem and Twilio SIM. Send a text message to Twilio phone number and receive real-time readings from sensors attached to ARTIK 530s.

**Use case:** Smart city, remote data transmission and monitoring systems, freight management

**Hardware:** ARTIK 530s, Multi-tech modem, Twilio SIM card, (optional) screen LCD

**Software:** Twilio APIs, Qt for UI



# Facial Recognition Security Camera

## ARTIK 530s

Uses ARTIK 530s and camera accessories for facial recognition. Non-enrolled faces will trigger alerts. Motion detection and video capture can be enabled.

**Use case:** Home surveillance, access control system

**Hardware:** ARTIK 530s, OV5640 5M Auto Focus USB camera, 10.1" PCAP Touch Screen LCD, sensors

**Software:** OpenCV, Kairos face recognition APIs, Qt



# Voice Enablement

## ARTIK 530s SoM and Google Assistant

Run Google Assistant or Amazon AVS on ARTIK530s. Use voice commands to control peripherals or sensors attached to ARTIK.

**Use case:** Voice-controlled gateway, home and building products

**Hardware:** ARTIK 530s, speaker, (optional) LCD

**Software:** Google Assistant SDK or Alexa Voice Service Device SDK. Can develop additional Google Actions or Alexa skills to extend basic capabilities.



# Machine Learning Inference

## ARTIK 5x/7x

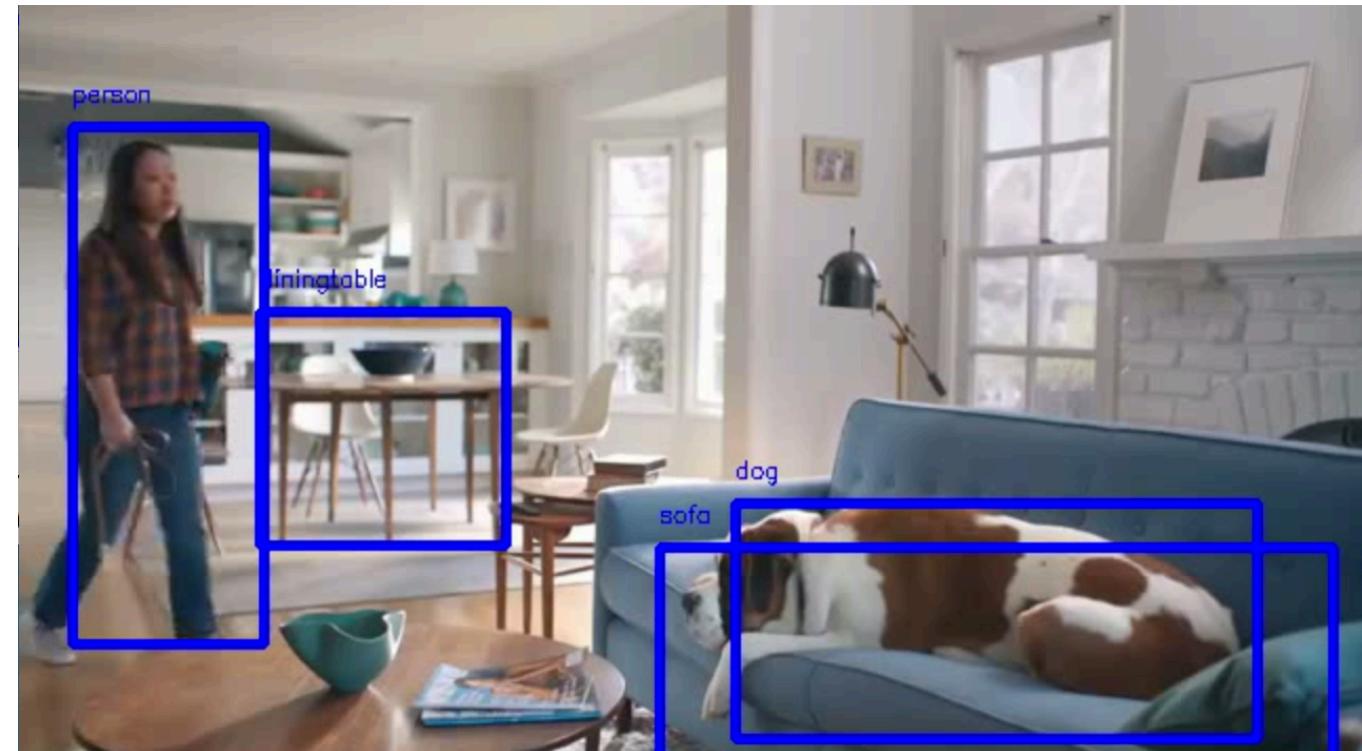
Run Machine Learning Inference on ARTIK gateway devices

**Use case:** Smart Factory, Smart Building etc.

**Hardware:** ARTIK 5x/7x

**Software:** Tensorflow Lite;

AWS Greengrass ML Inference;



# ARTIK Security



# Security Questionnaire

## How do you provide security across all attack surfaces?

Question	ARTIK 5/7/053
Do you support secure communication from device to device or device to cloud? How do you secure communication? Are you using TLS1.2 or higher?	Yes, HTTPs using TLS 1.2
How do you establish identity of device?	Using unique certificate on each device
How does the device establish identity of cloud?	Both device and cloud are chained to ARTIK Root CA and can verify each other certificates
Do you have mutual authentication when enabling secure communication?	Yes
Do you have the infrastructure to inject unique key and certificate in each device to establish unique identity per device? How much does it cost?	Yes (Done at Samsung factory. Cost included in module)
How do you protect your certificate, keys? Are your certificate and keys safe if software is hacked?	Specialized HW on module (secure element)
Is your certificate infrastructure secure? How do you secure your Root Certificates? How much does it cost?	Yes (Root CA secured by 3 <sup>rd</sup> party security vendor)
How do you guarantee your firmware integrity?	Secure Boot

# Non-S vs. S Modules

- Same HW specifications other than security features
- "S" type modules can be identified by **blue** labeling

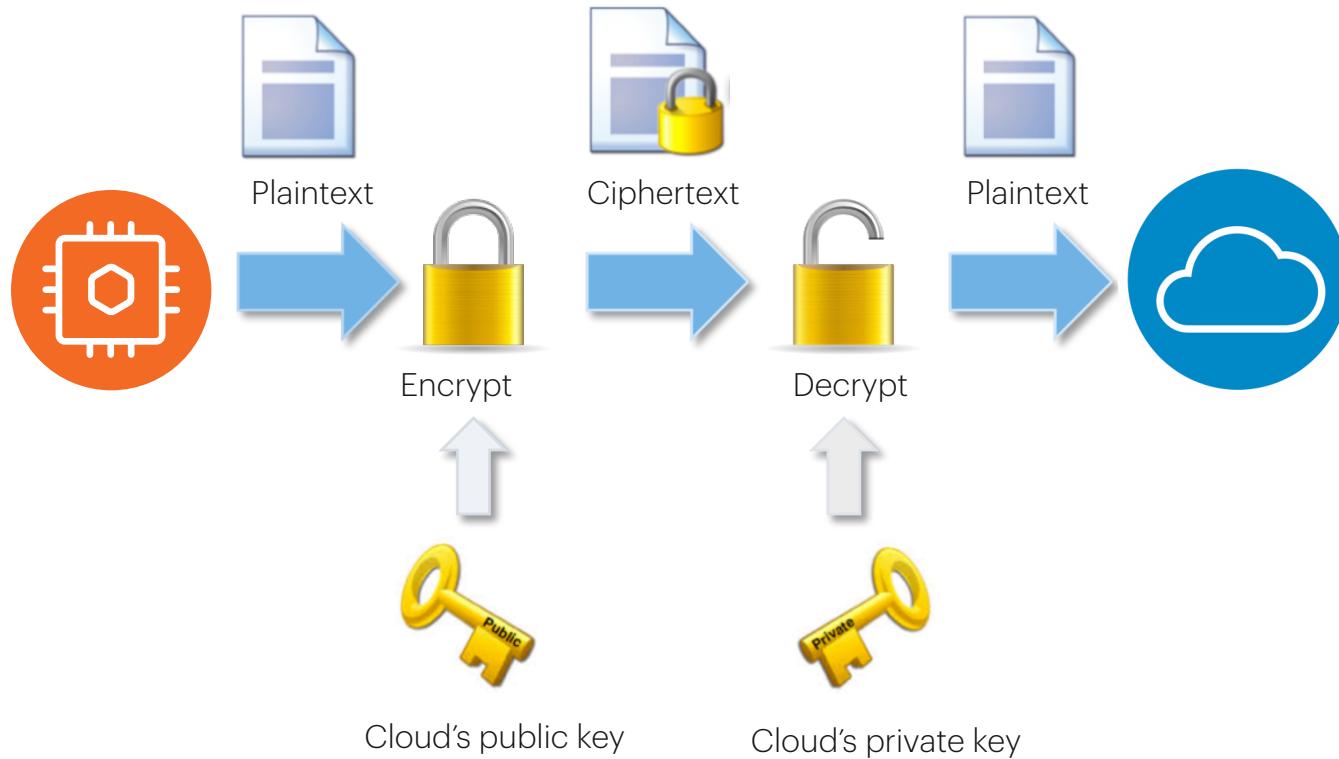
Standard module



"S" module

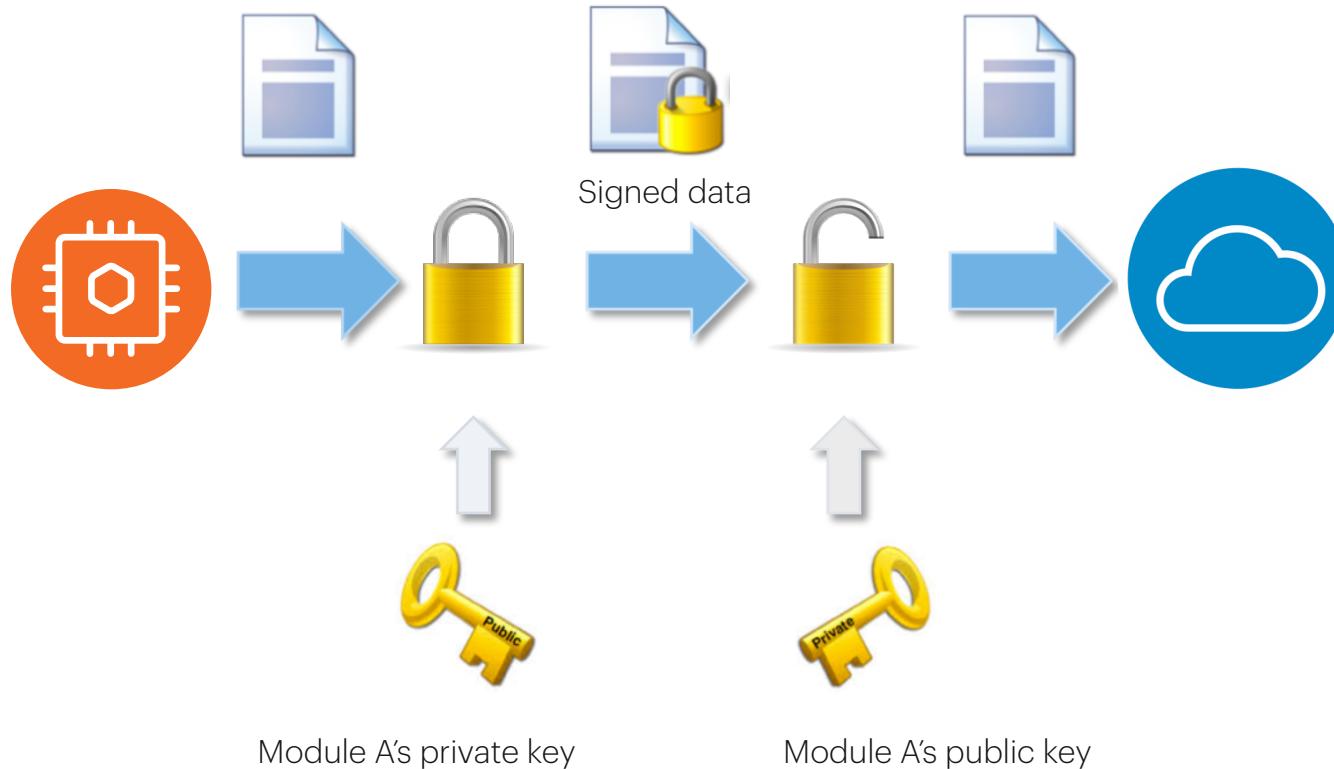


# Encryption and Decryption



Different keys are used to encrypt and decrypt messages

# Signature

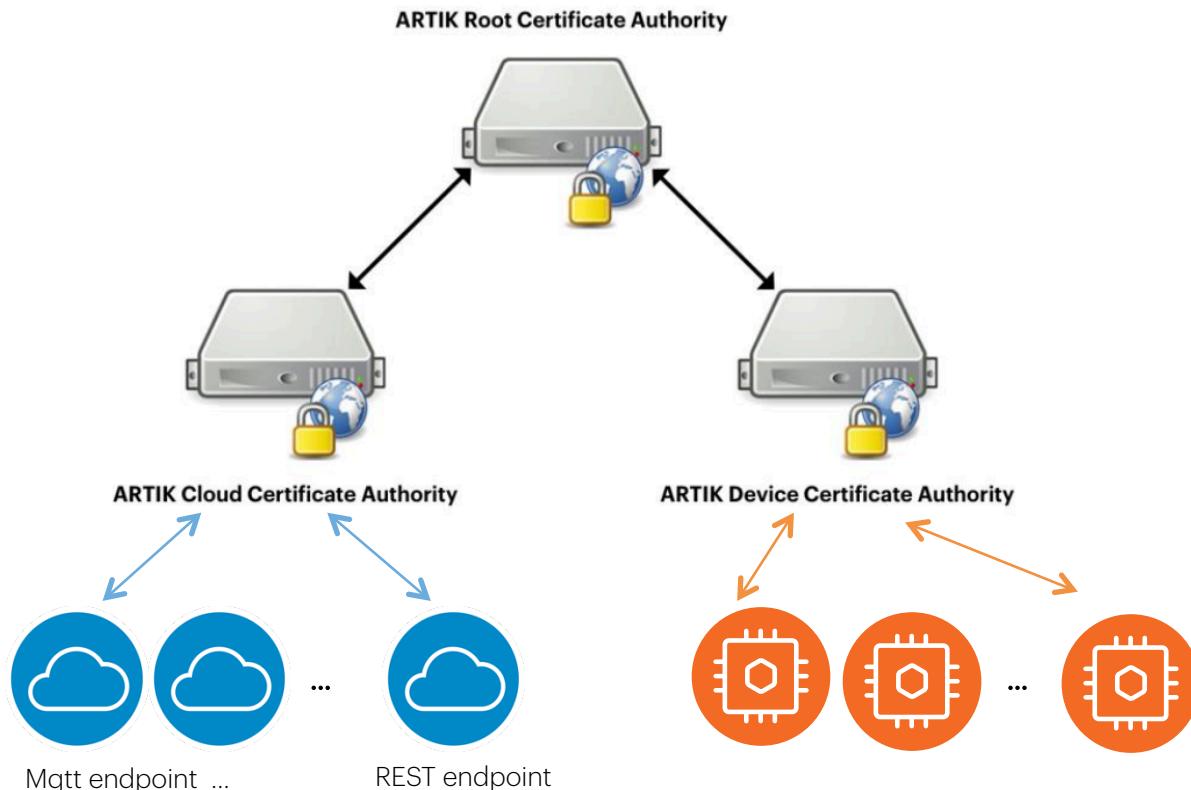


# Public Key Infrastructure (PKI)

- A Public Key Infrastructure (PKI) supports the distribution and identification of public encryption keys, establishing authenticity and trust in a system.
- ARTIK provides its own PKI, which is used to generate and apply unique certificates and key pairs to each ARTIK Module during manufacturing.

# ARTIK Root CA

- PKI's core concept is (Digital) Certificate. Issued by a **Certificate Authority**, e.g, GlobalSign, Symantec
- ARTIK Root CA



# Mutual Authentication

- Each ARTIK module is provisioned with:
  - An unique private key
  - Its associated certificate containing a public version of the key.
  - An ARTIK Root CA certificate
- ARTIK Cloud's server certificate is also rooted to the ARTIK Root CA certificate
- At connect time, server and client exchange certificates for mutual authentication

# Post Provisioning

- If you want to connect your ARTIK Module to a 3<sup>rd</sup> party Cloud service or implement a link between ARTIK modules, you need to generate your own certificate/key-pair
- We can use Post Provisioning to post provision customer credentials(key, certificate) to Secure Element

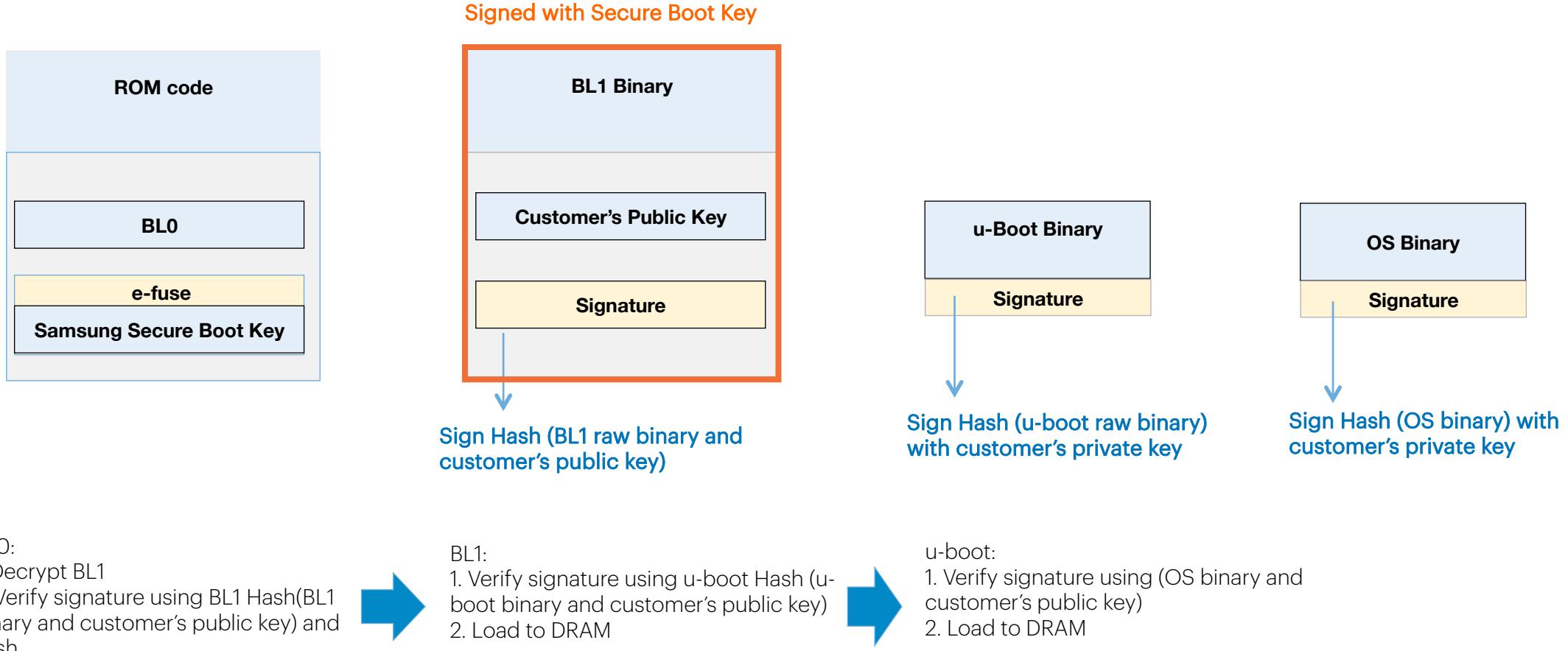
# Secure Communication

		ARTIK module (05x, 5, 7)	ARTIK S-module (053s, 055s, 530s, 710s)	Comments
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to authorized cloud and vice versa
	Post Provisioning		✓	Provision with your own keys and certificates
Device protection/ secure code execution	KMS infrastructure for code signing		✓	Key Management Service
	Code verification key in HW		✓	Secure key storage
	Secure boot (check for authorized code)		✓	Boot image verification
	JTAG access locked		✓	Lock out debug access
Data protection/ Secure storage	Secure OS (separate normal & secure operations)		✓	Hardware enforced secure applications via TEE
	Security Lib API (27 API calls)	Limited(random number generator, get cert and signature)	✓	Key Manager, Authentication, Secure Storage, Post Provisioning, Encrypt/Decrypt
	Secure storage		✓	Encrypt data stored on Flash

# Secure Boot

- Secure Boot adds cryptographic checks to each stage of the boot process.
- The first element in the boot process authenticates the second, the second verifies the third.
- Authentication is based on digital signature verification.
- **Chain of Trust:** Every component can be authenticated before being executed.

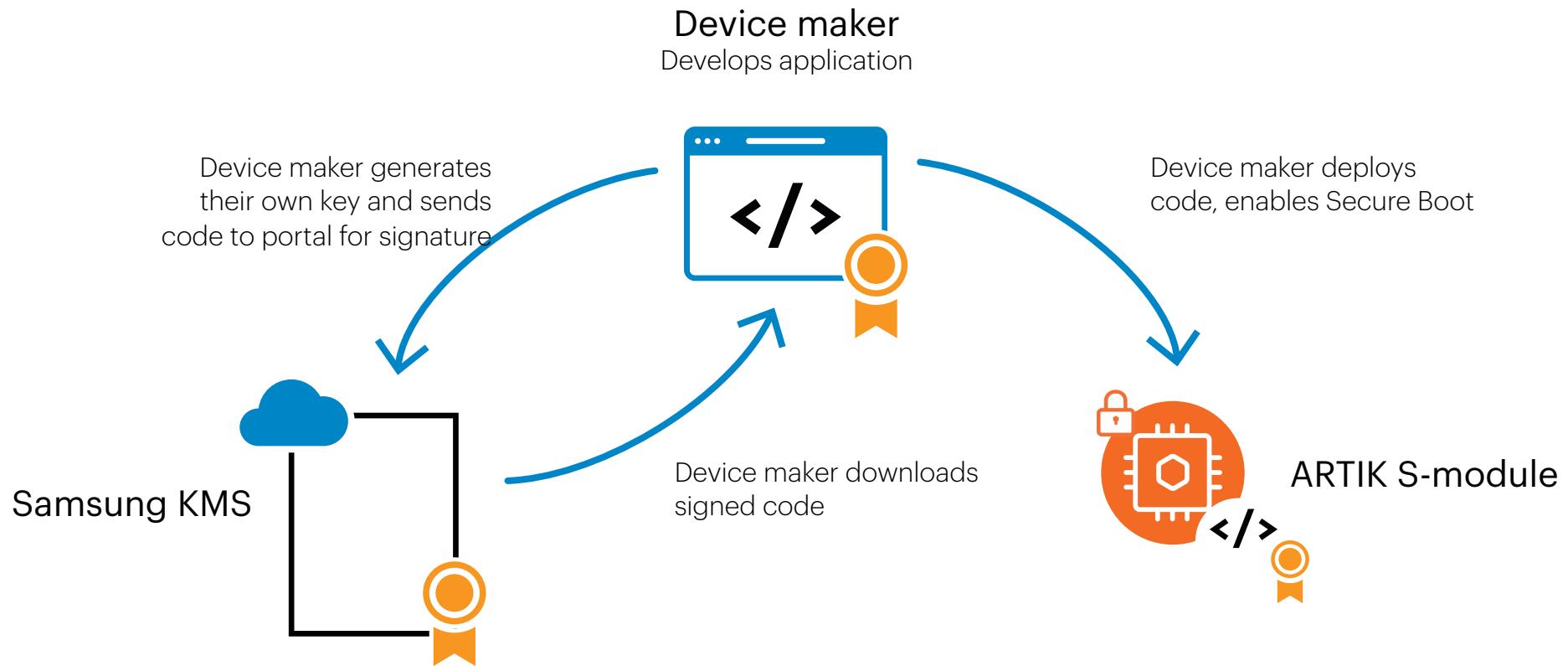
# Secure Boot for ARTIK 05x S-Module



NEW

# Samsung ARTIK™ Key Management System(KMS)

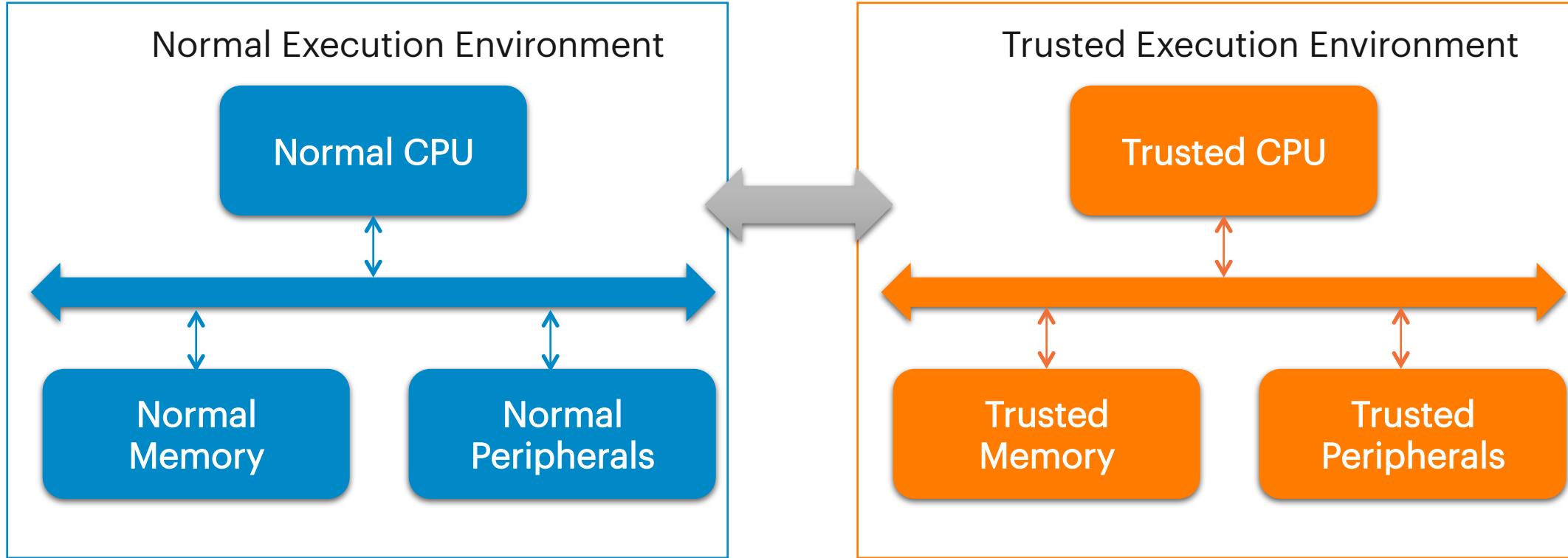
## Code signing portal manages key signing



# Device Protection

		<b>ARTIK module (05x, 5, 7)</b>	<b>ARTIK S-module (053s, 055s, 530s, 710s)</b>	Comments
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to authorized cloud and vice versa
	Post Provisioning		✓	Provision with your own keys and certificates
Device protection/ secure code execution	KMS infrastructure for code signing		✓	Key Management Service
	Code verification key in HW		✓	Secure key storage
	Secure boot (check for authorized code)		✓	Boot image verification
	JTAG access locked		✓	Lock out debug access
Data protection/ Secure storage	Secure OS (separate normal & secure operations)		✓	Hardware enforced secure applications via TEE
	Security Lib API (27 API calls)	Limited(random number generator, get cert and signature)	✓	Key Manager, Authentication, Secure Storage, Post Provisioning, Encrypt/Decrypt
	Secure storage		✓	Encrypt data stored on Flash

# Trusted Execution Environment on 5/7x (TEE)



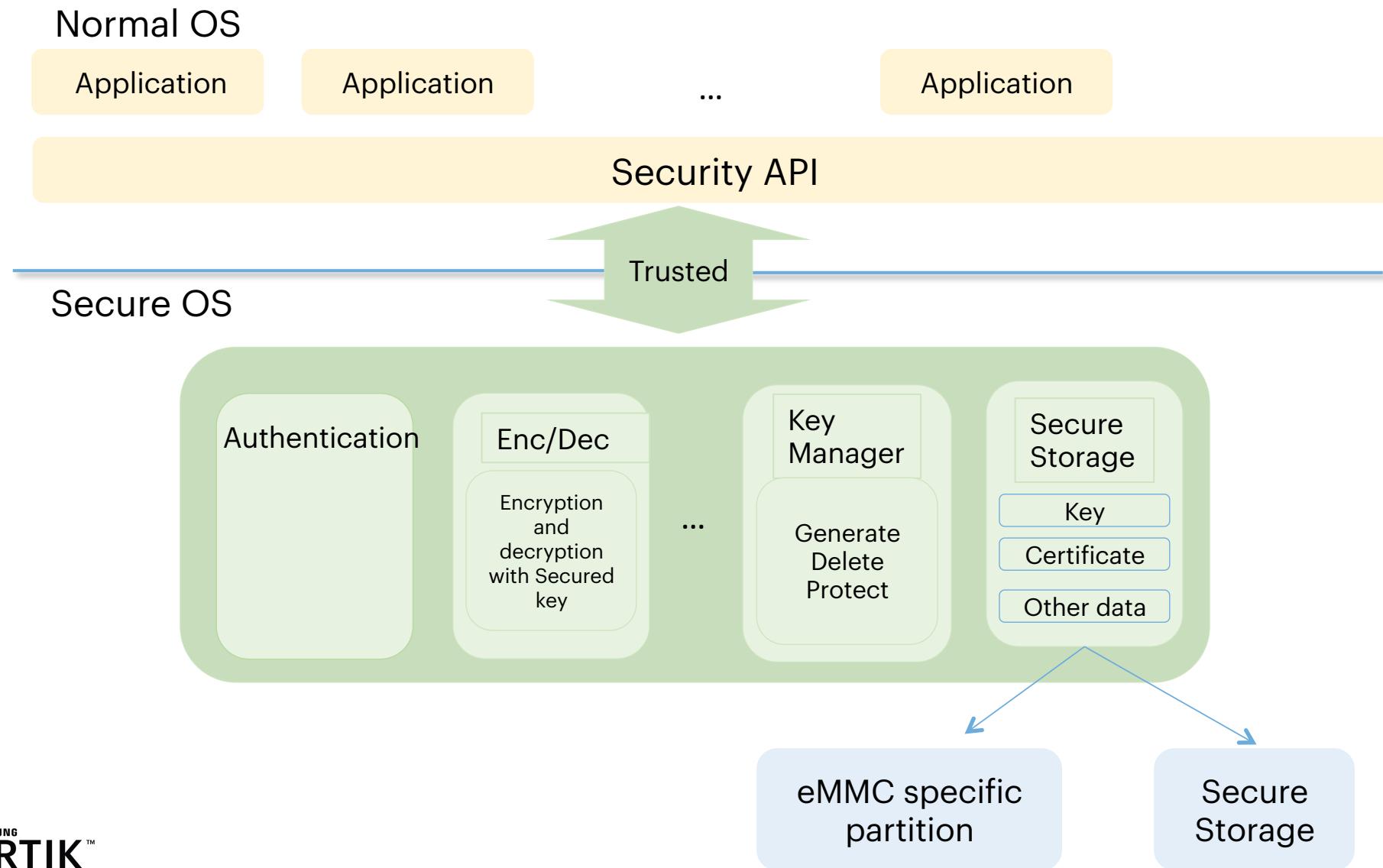
- ARTIK 5 and 7 module families support Trusted Execution Environment(TEE)
- Samsung TEE implementation is based on ARM TrustZone hardware architecture
- TEE provides a fully-isolated and secured operation environment

# Secure Storage – Secure Element

Secure Element – an isolated storage device that supports 2 slots of ECDSA key pairs (16 AES 128-bit keys).

- The Secure Element provides high levels of security as hardware with anti-tamper measures.
- It includes cryptographic services such as random-number generation, key/data secure storage, and certificates handling and processing.
- All communication from the Secure Element to the processor is secured and encrypted.
- Uses Power glitch detector, Active Shield removal detector etc. technologies to achieve the highest level of security and protection.
- The Secure Element meets the Common Criteria (CC) certification for security and for Evaluation Assurance Level (EAL) 5.

# ARTIK SEE Architecture

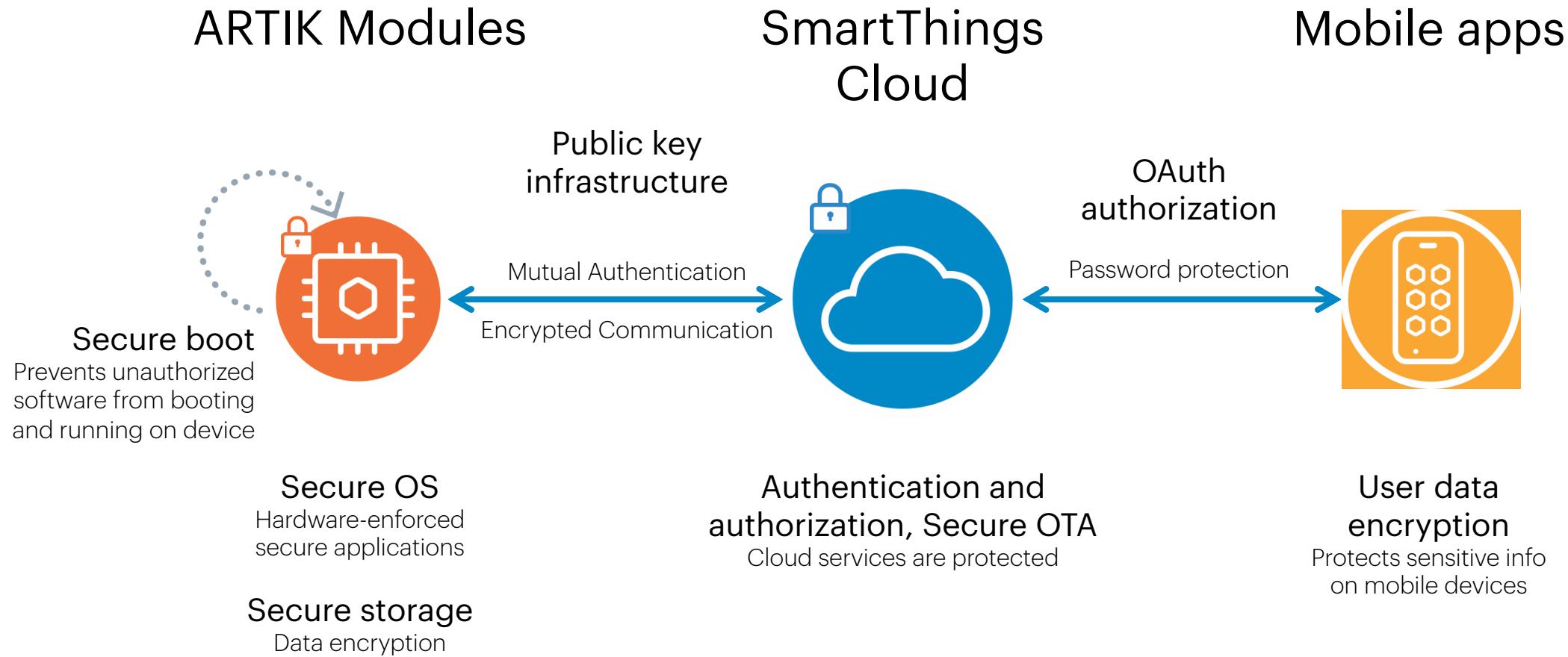


# Device Protection

		<b>ARTIK module (05x, 5, 7)</b>	<b>ARTIK S-module (053s, 055s, 530s, 710s)</b>	<b>Comments</b>
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to authorized cloud and vice versa
	Post Provisioning		✓	Provision with your own keys and certificates
Device protection/ secure code execution	KMS infrastructure for code signing		✓	Key Management Service
	Code verification key in HW		✓	Secure key storage
	Secure boot (check for authorized code)		✓	Boot image verification
	JTAG access locked		✓	Lock out debug access
Data protection/ Secure storage	Secure OS (separate normal & secure operations)		✓	Hardware enforced secure applications via TEE
	Security Lib API (27 API calls)	Limited(random number generator, get cert and signature)	✓	Key Manager, Authentication, Secure Storage, Post Provisioning, Encrypt/Decrypt
	Secure storage		✓	Encrypt data stored on Flash

# Samsung ARTIK™ End-to-end Platform Security

## End-to-end protection for you and your customers



# ARTIK Training Tues

# Samsung ARTIK™ Training Tues

2-hour training sessions every other Tues starting from Aug, 14th

**Level 1: ARTIK Fundamentals** (Lecture with interactive exercises. No ARTIK hardware is required)

L1\_1: ARTIK Intro: ARTIK Intro and guide audience through online resources

L1\_2: ARTIK 310 Intro

**Level 2: ARTIK HW/SW Features** (Lecture + hands-on)

L2\_1: Onboarding + OTA

L2\_2: Cloud communication

L2\_3: Security

L2\_4: HW Interfaces

L2\_5: Connectivity

**Level 3: ARTIK Applications and Solutions** (mostly hands-on. )

L3\_1: How to use ARTIK Cloud for device management and AWS for data management (05x hands-on)

L3\_2: Use TensorFlow Lite on ARTIK 5x for Machine Learning Inference(5x hands-on)

L3\_3: Build a Google Assistant/AVS voice-enabled gateway for smart home(5x hands-on)



# Training Schedule

2018

**January**

S	M	T	W	T	F	S
1	2	3	4	5	6	
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

**February**

S	M	T	W	T	F	S
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28			

**March**

S	M	T	W	T	F	S
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

**April**

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

**May**

S	M	T	W	T	F	S
	1	2	3	4	5	
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

**September**

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

**October**

S	M	T	W	T	F	S
		1	2	3	4	5
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

**November**

S	M	T	W	T	F	S
		1	2	3	4	5
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

**December**

S	M	T	W	T	F	S
		1	2	3	4	5
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					



Level 1



Level 2



Level 3

**Date**

Aug 14th

**Topics**

Level 1 - ARTIK Intro

Aug 28th

Level 2- Onboarding and OTA

Sep 11th

Level 2- Cloud Communication

Sep 25th

Level 3- Use ARTIK Cloud for device management and AWS for data management

Oct 9th

Level 1 -ARTIK Intro (repeated content)

Oct 23rd

Level 2- Security

Nov 13th

Level 2 - ARTIK Hardware Interface

Nov 27th

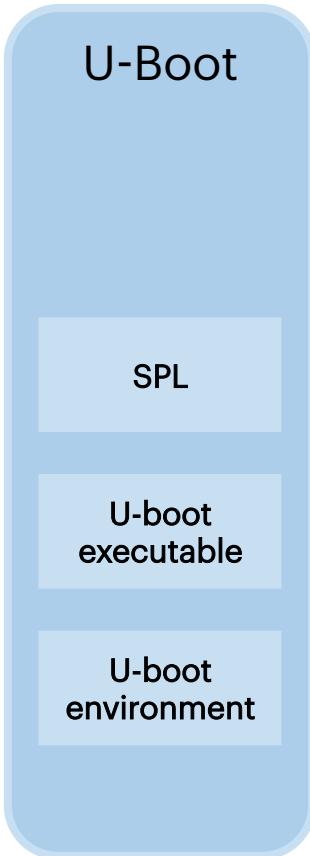
Level 3- Use TensorFlow Lite on ARTIK 5x for Machine Learning Inference

Dec 11th

Level 1- ARTIK 310 Intro

# APPENDIX

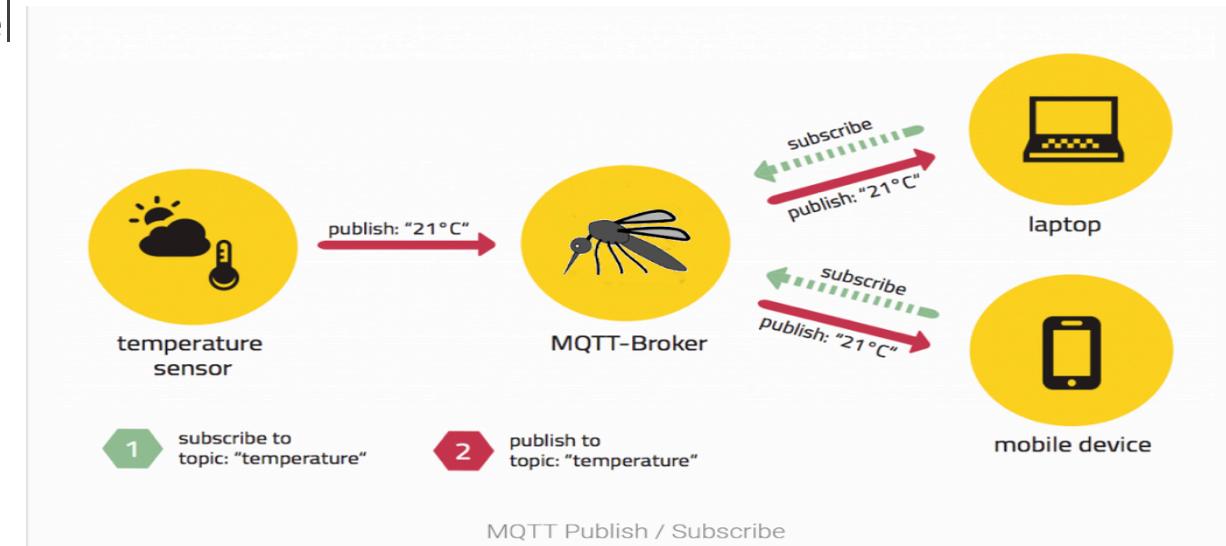
# U-Boot



Boot Stage#	Terminology #1	Terminology#2	Program Name
1	Primary Program Loader	-	ROM Code
2	Secondary Program Loader(SPL)	1 <sup>st</sup> stage bootloader	U-boot SPL
3		2 <sup>nd</sup> stage bootloader	U-boot
4			kernel

# Message Queue Telemetry Transport (MQTT)

- MQTT history
- Light-weight messaging protocol, rides on TCP
- Broker / Clients architecture
- Publication / Subscription messaging model
- No pre-defined format for payload



# Message Queue Telemetry Transport (MQTT)

- In general, a MQTT client can be both a publisher & subscriber at the same time
- A MQTT client can run on any device from a micro controller up to a server. MQTT C client code only takes 30KB, Java code is about 100KB.
- MQTT client libraries are available for a huge variety of programming languages, e.g, C/C++, Arduino, Java, JavaScript, Android, iOS, C#, .NET

<https://github.com/mqtt/mqtt.github.io/wiki/libraries>

- MQTT client: Eclipse Paho



MQTT.fx (available for Win/MacOS/Linux) etc.

# Message Queue Telemetry Transport (MQTT)

- MQTT Broker is responsible for receiving all messages, filtering them, and sending the messages to all subscribed clients.
- It holds the session of all persistent clients including subscriptions and missed messages
- Authentication and authorization of clients.
- Self Hosted MQTT brokers:

Eclipse Mosquitto



HiveMQ(licensed)



- Cloud based MQTT brokers:

AWS



IBM Bluemix



HiveMQ ([broker.hivemq.com](http://broker.hivemq.com))



Microsoft Azure



Eclipse Mosquitto ([test.mosquitto.org](http://test.mosquitto.org))



# CoAP

- Similar to HTTP, but designed for the needs of constrained devices
- Runs over UDP
- Client/server model
- Supports resource discovery
- Supported by ARTIK Cloud service

