ARTIK Gateway Modules

Wei Xiao

July 31, 2018

SAMSUNG ARTIK™

Confidential

Agenda

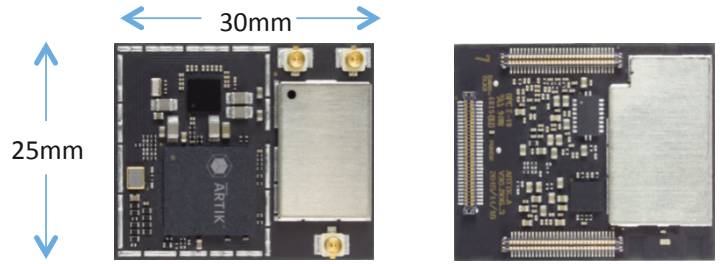
- ARTIK Gateway Module Overview
- ARTIK Gateway Module Development
- ARTIK End-to-end Solution
- ARTIK Gateway Module Use Cases and Ecosystem
- ARTIK Security

ARTIK Gateway Module Overview

Confidential

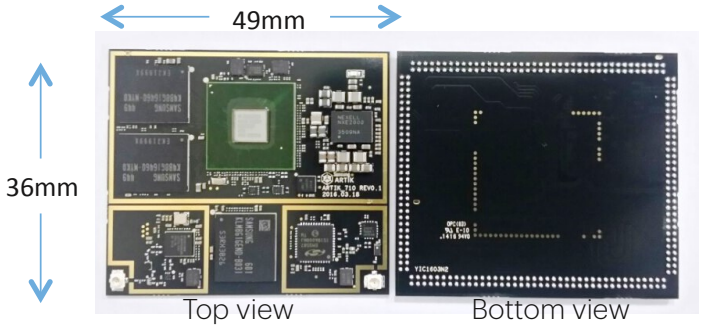
ARTIK High-end module

520



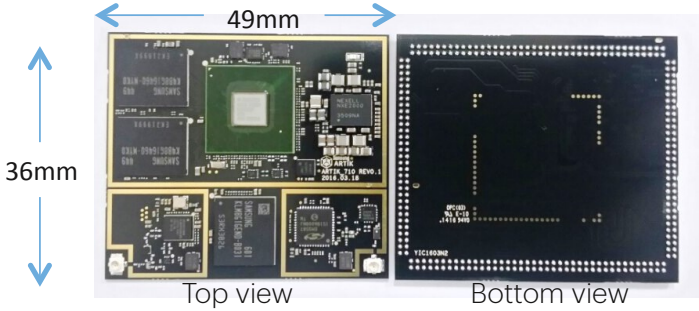
530

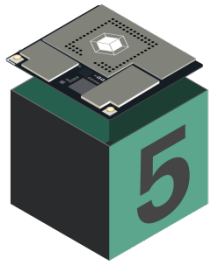
530s

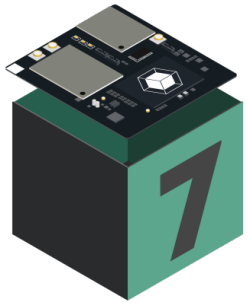


710

710s







SAMSUNG ARTIK™

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

SAMSUNG ARTIK™

Processor	**CPU:** 4x ARM® Cortex® A9 @ 1.2 GHz **GPU:** 3D graphics accelerator
Memory	**DRAM:** 512 MB/1 GB DDR3 **Flash:** 4 GB eMMC v4.5
Multimedia	**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
Connectivity	**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)
Security	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
I/O	GPIO, UART, I2C, SPI, USB Host, USB OTG, HSIC, ADC, PWM, I2S, JTAG
Temperature range	-25° to 85° (°C)
Size	36 mm W x 49 mm H x 3.4 mm D

Samsung ARTIK™ 710/710s high-end gateway

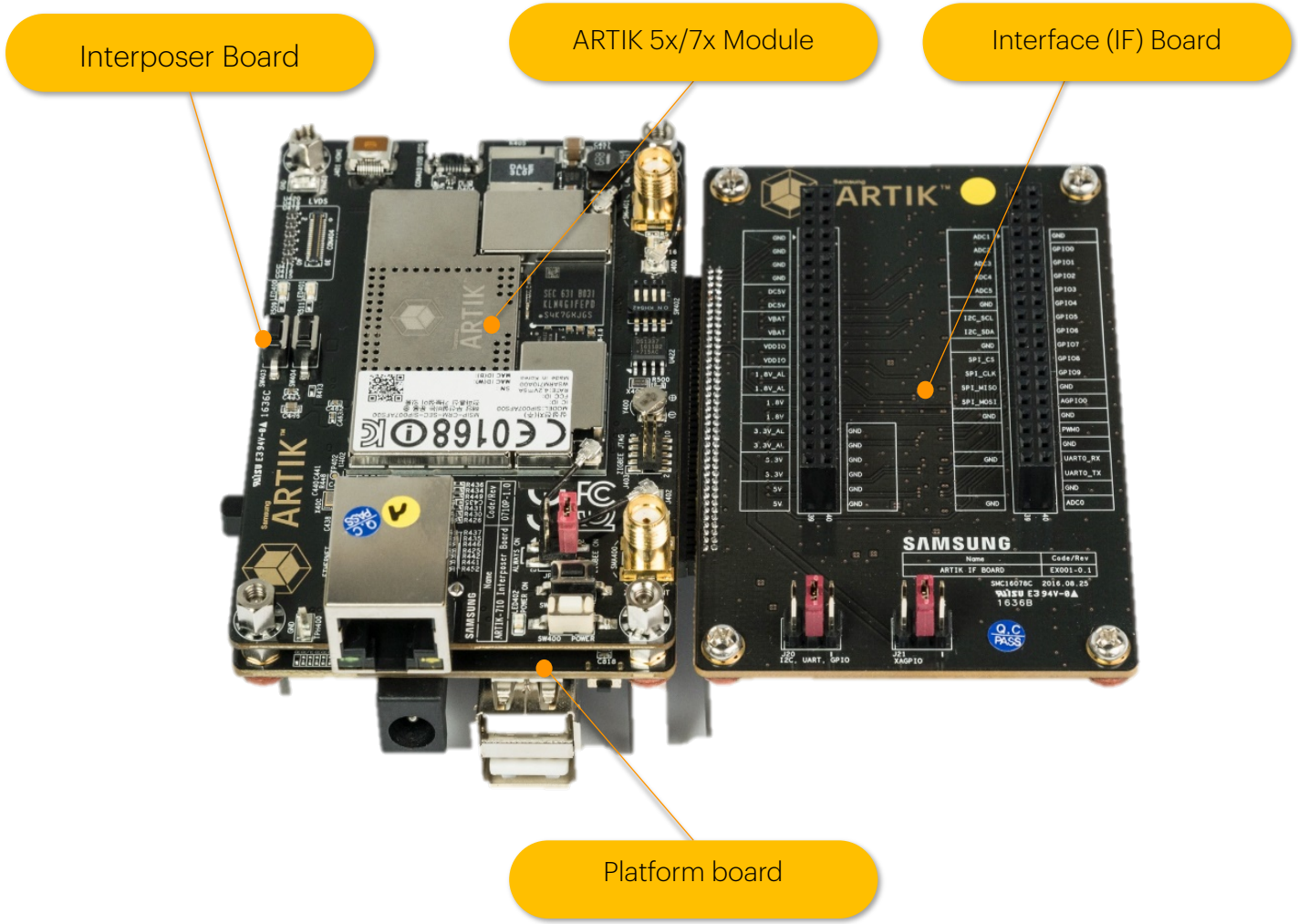
Secure, fully-integrated IoT solution

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

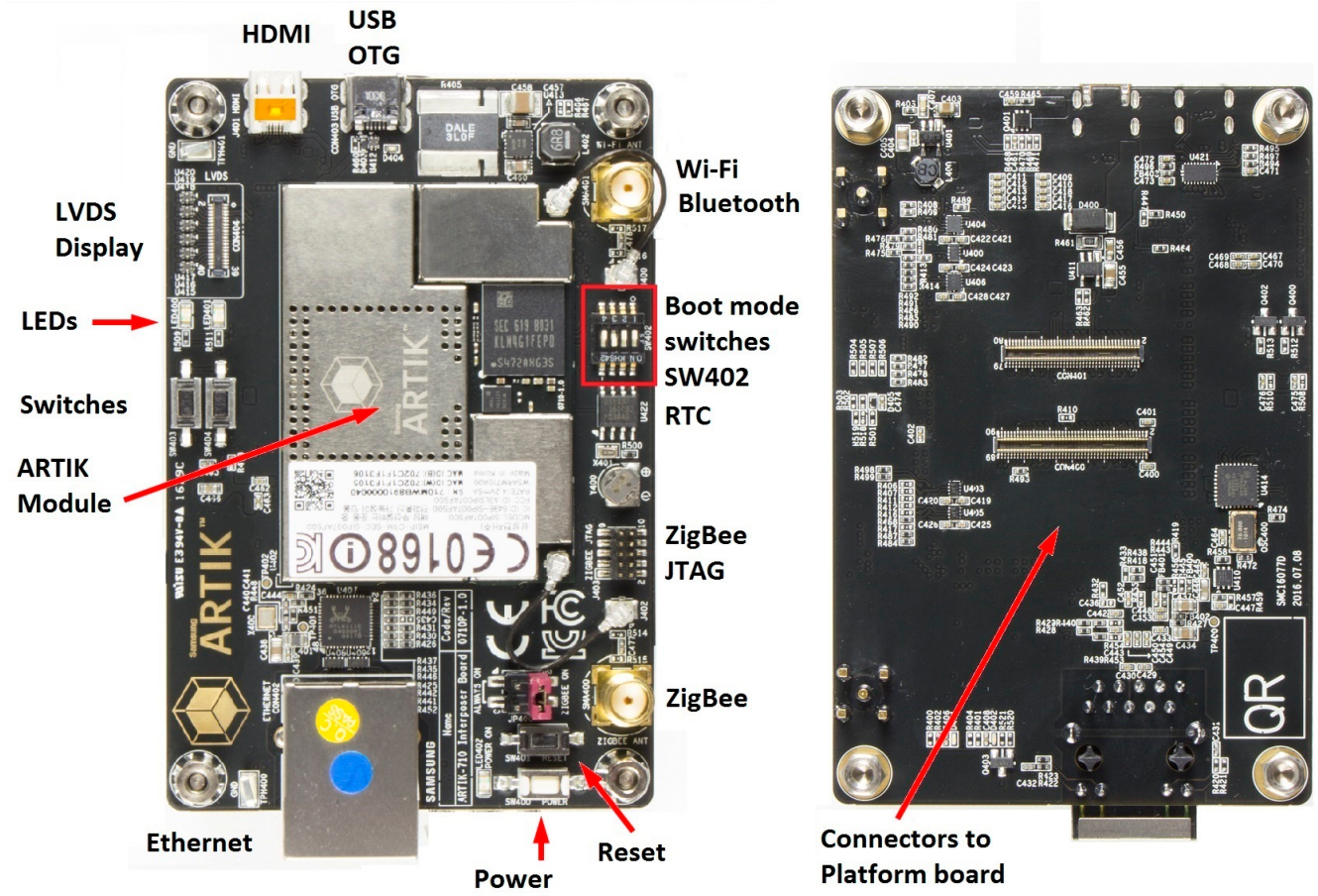
SAMSUNG ARTIK™

Processor	**CPU:** 8x ARM® Cortex® A53 @ 1.4 GHz **GPU:** 3D graphics accelerator
Memory	**DRAM:** 1 GB DDR3 @ 800 MHz **Flash:** 4 GB eMMC v4.5
Multimedia	**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
Connectivity	**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)
Security	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
I/O	GPIO, I²C, I²S, SPI, UART, PWM, SDIO, USB 2.0, JTAG, analog input
Temperature range	0° to 70° (°C)
Size	36 mm W x 49 mm H x 3.4 mm D

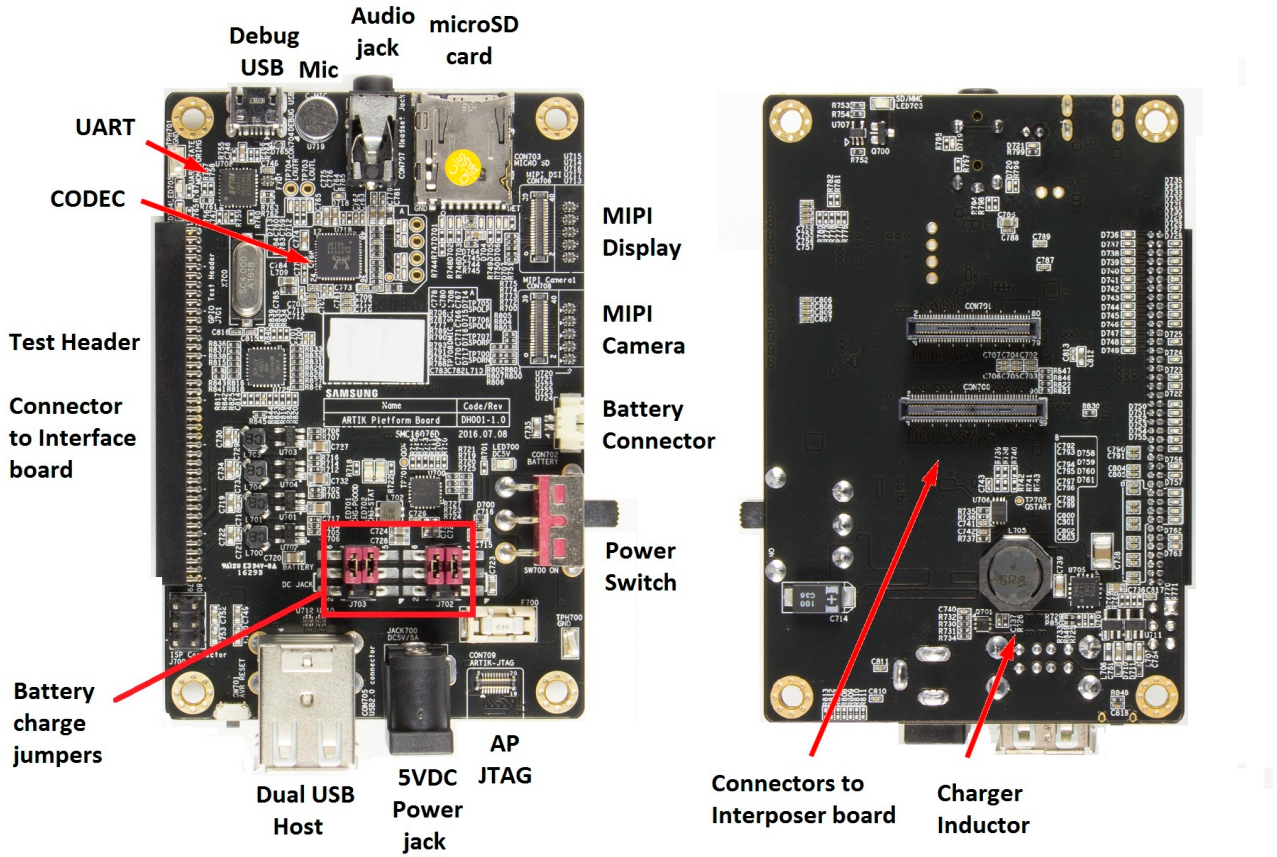
ARTIK High-end module development board



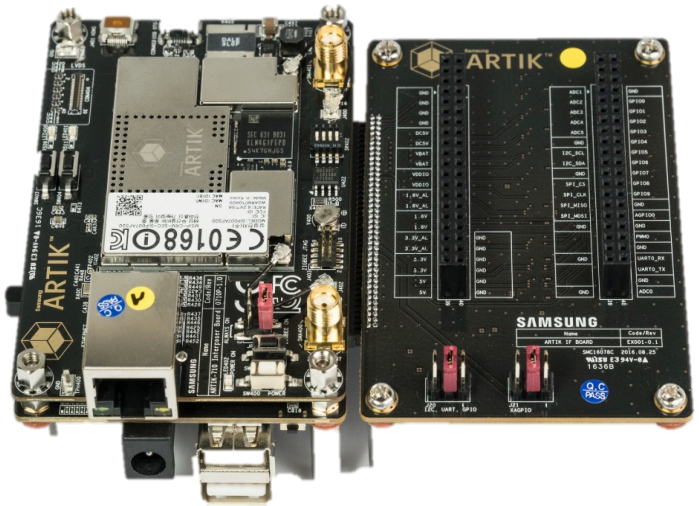
ARTIK High-End Module Interposer Board



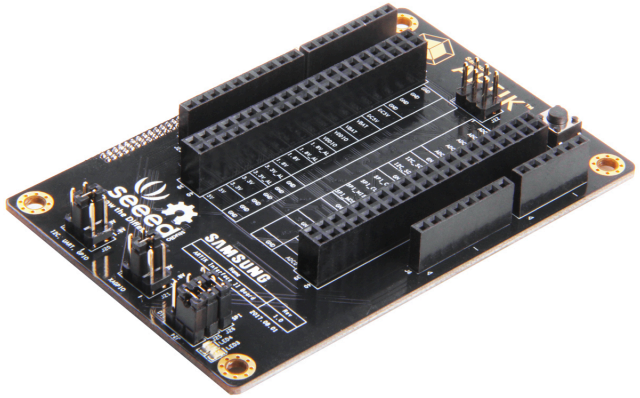
ARTIK Gateway Module Platform Board



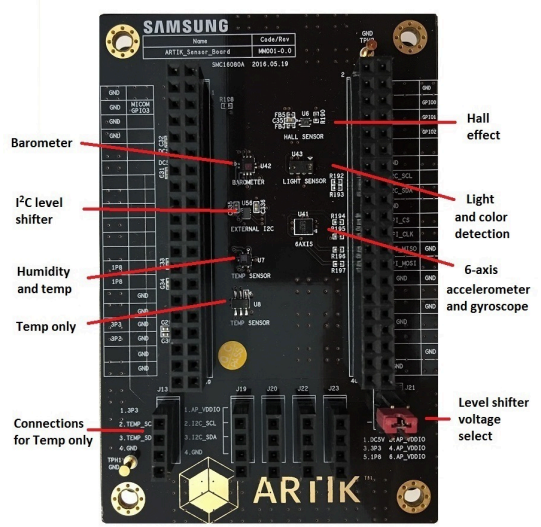
ARTIK Gateway Module Expansion Boards



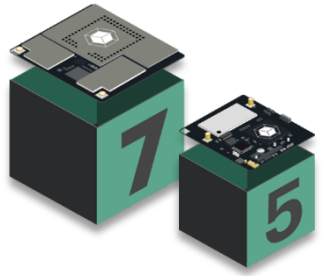
Interface Board



Interface Board II

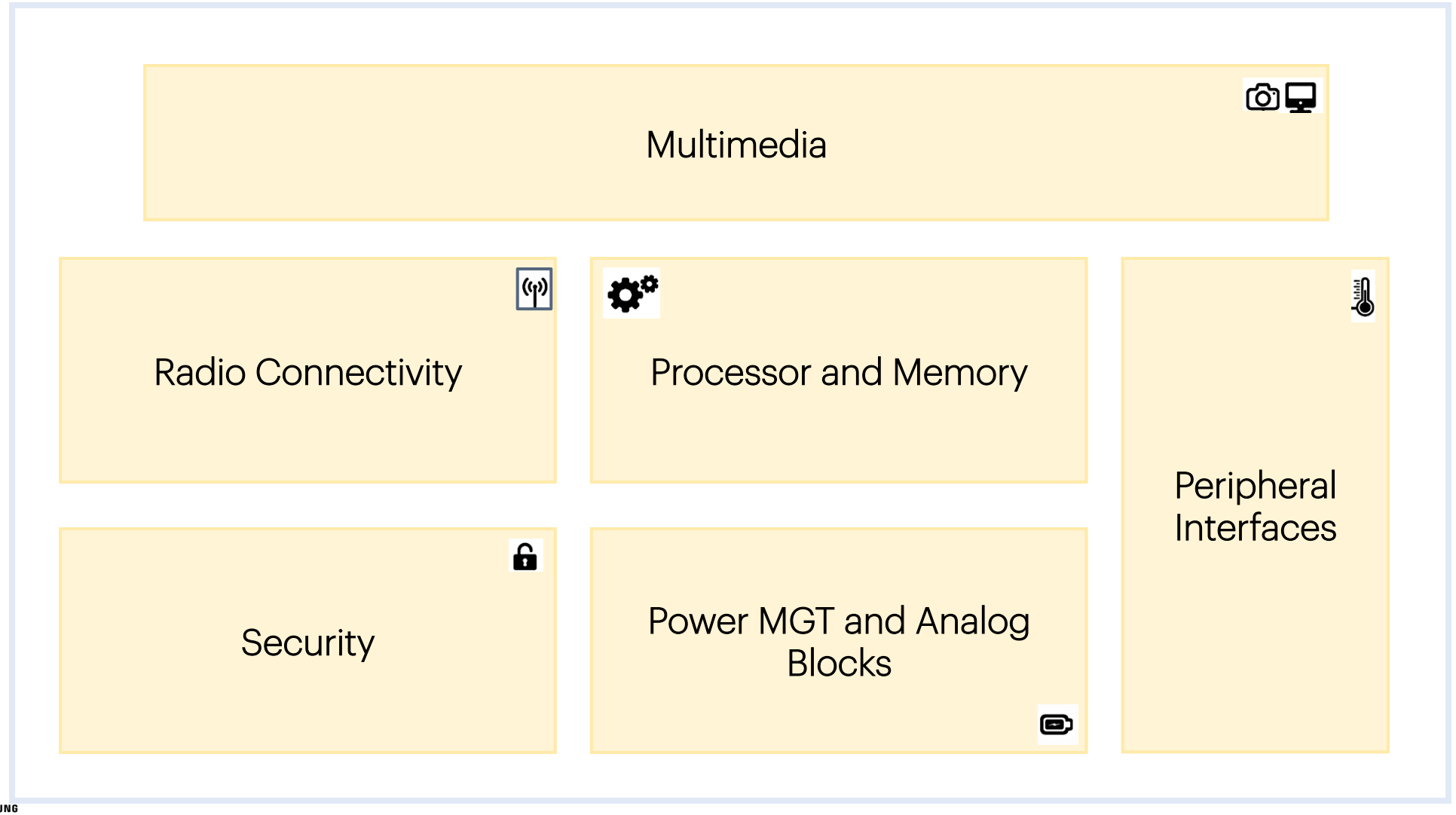


Sensor Board



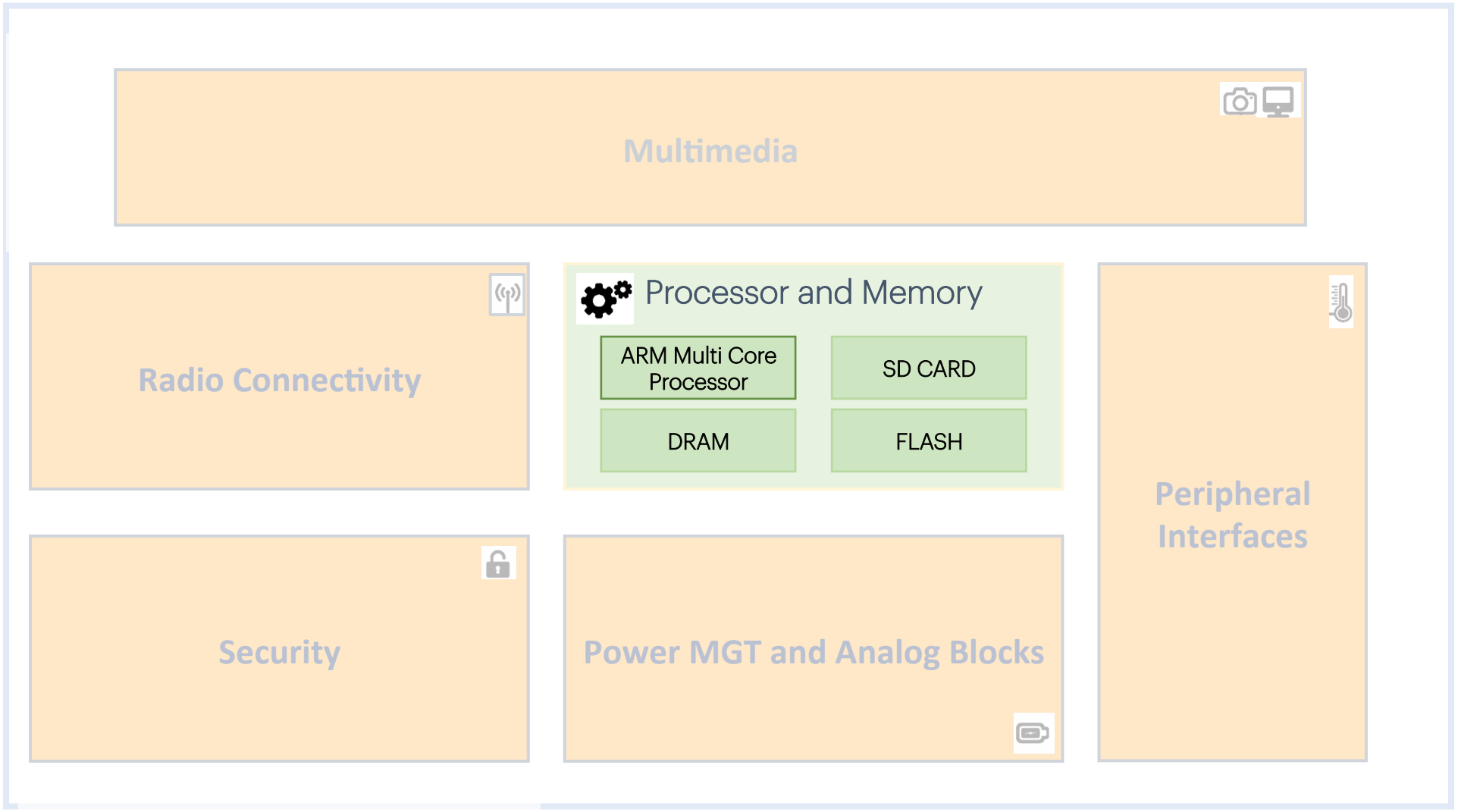
SAMSUNG ARTIK™

Product Details



SAMSUNG ARTIK™

Product Details – Processor and Memory



SAMSUNG ARTIK™

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

SAMSUNG ARTIK™

Peripheral Interfaces + Power MGT & Analog blocks

		520	530	710
Peripheral Interfaces	I2C	6	3	3
	SPI	2	2	2
	GPIO	100	107	108
	UART	2	3	3
	USB	USB 2.0*	USB 2.0	USB 2.0
Analog and Power MGT	ADC	2	6	6
	PWM	2	2	2
	PMIC	✓	✓	✓

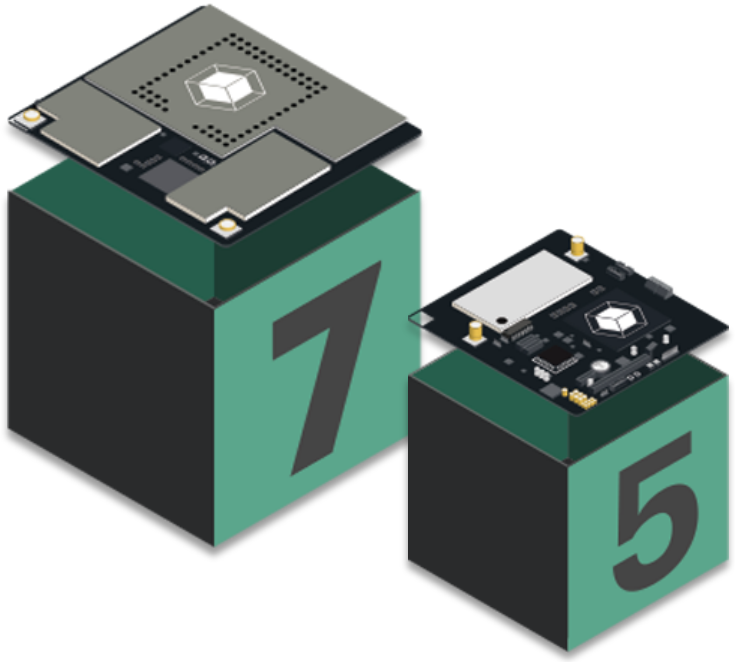
*USB device mode only for 520, rest of the module is both device and host mode.

SAMSUNG ARTIK™

Product Details - Multimedia

	520	530	710
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



Application

ARTIK API

Root FS

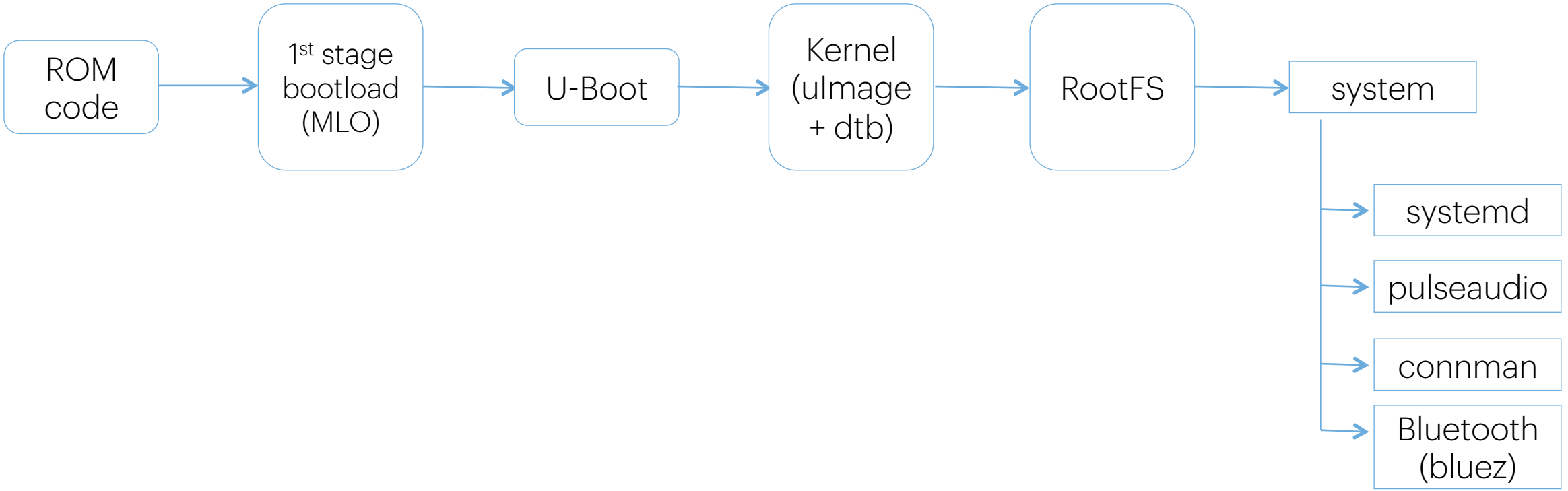
Kernel

Hardware

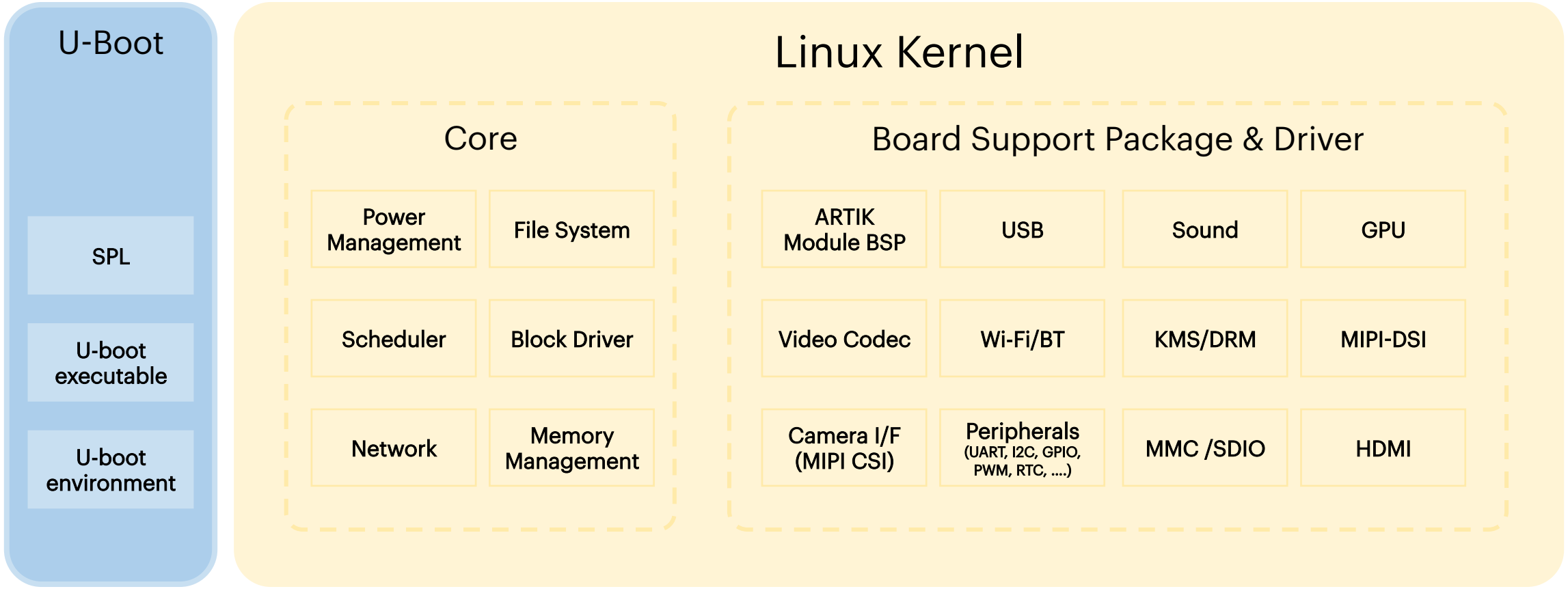
SAMSUNG ARTIK™

Boot Modes and Sequence

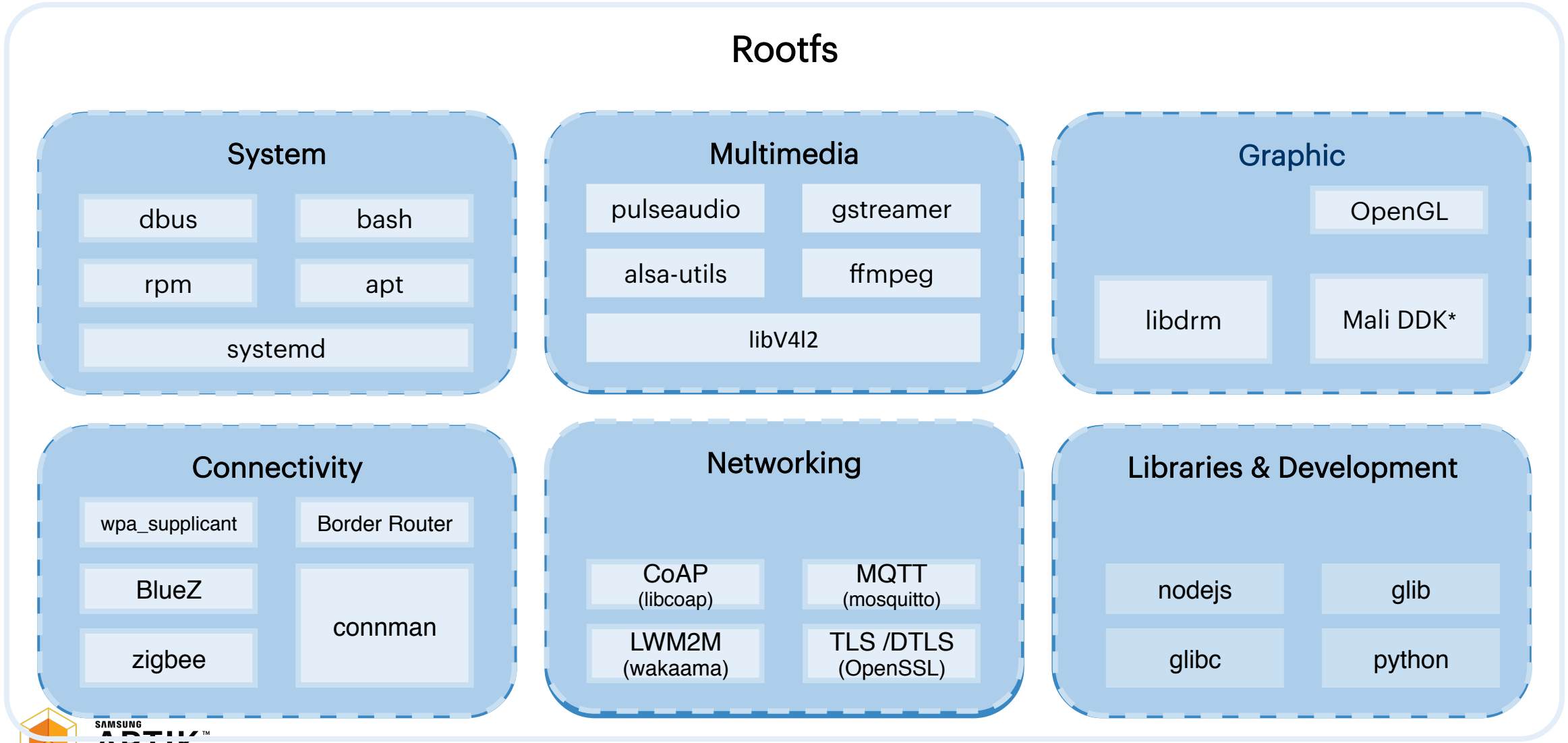
eMMC Boot Sequence



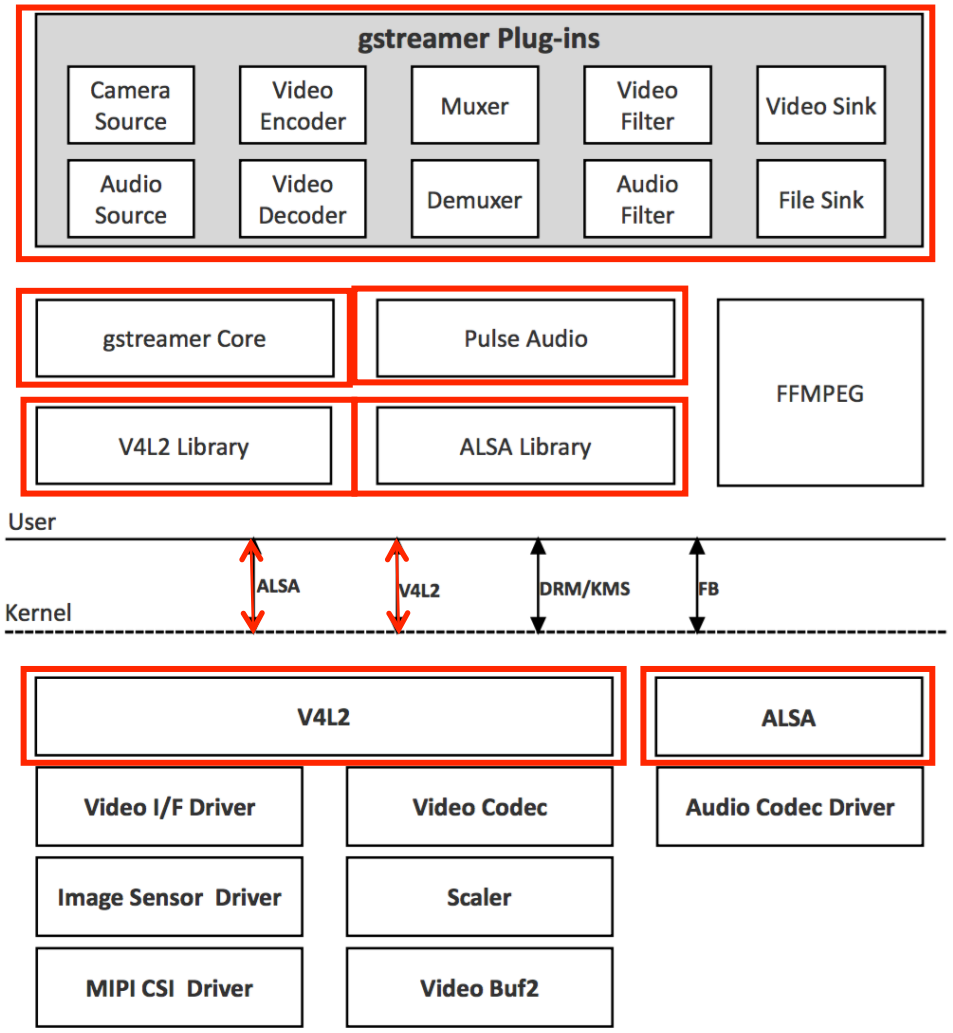
U-Boot and Linux Kernel Architecture



Architecture of Rootfs



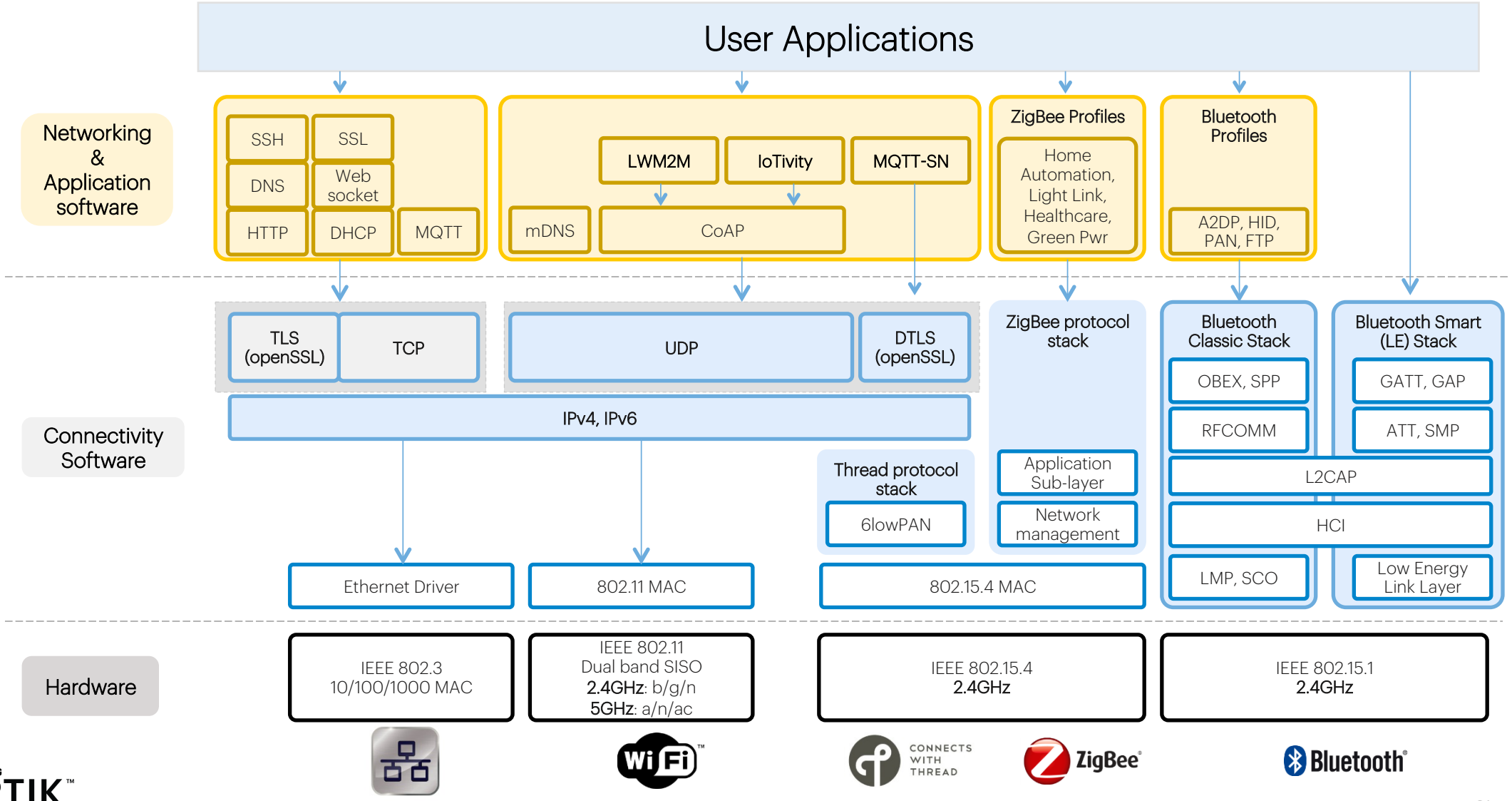
Multimedia Architecture



- 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

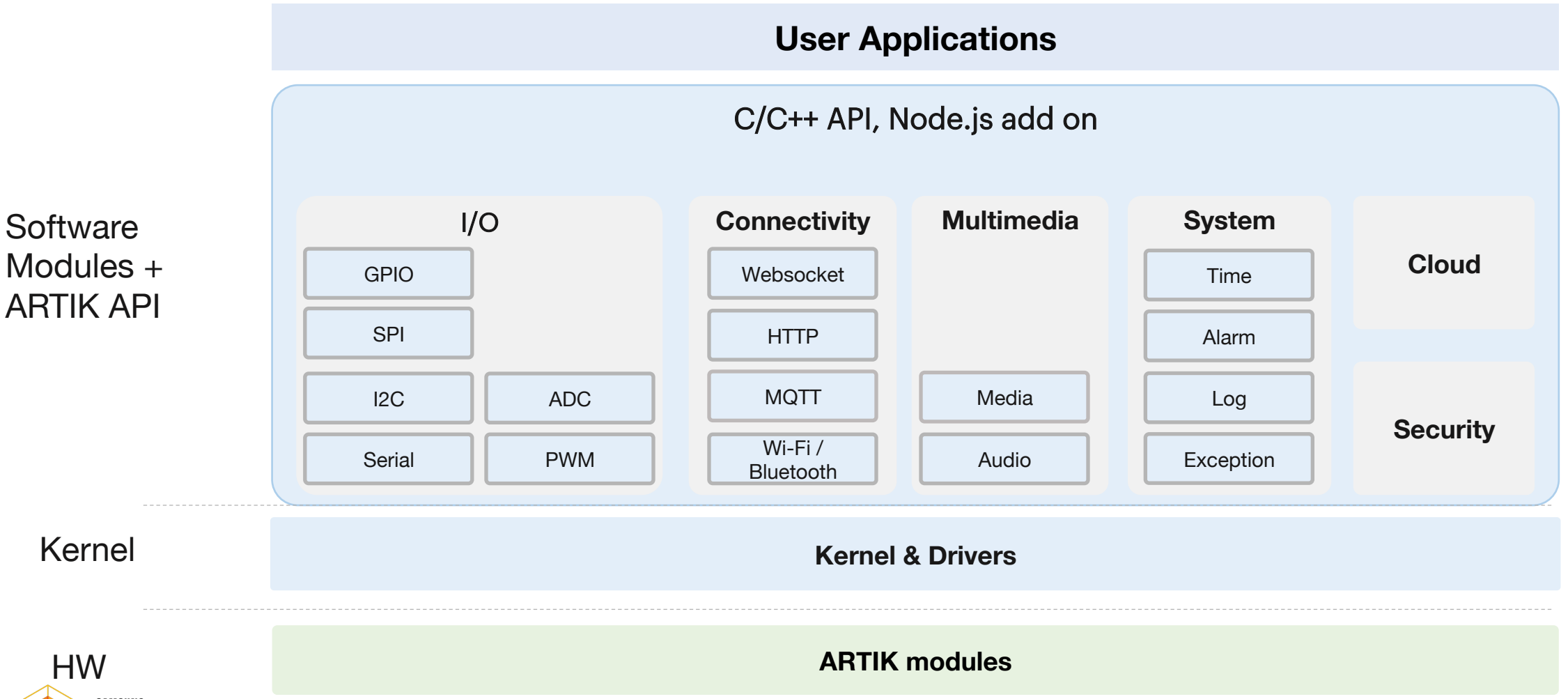
SAMSUNG ARTIK™

Network Stack



SAMSUNG ARTIK™

ARTIK SDK (5, 7 series)



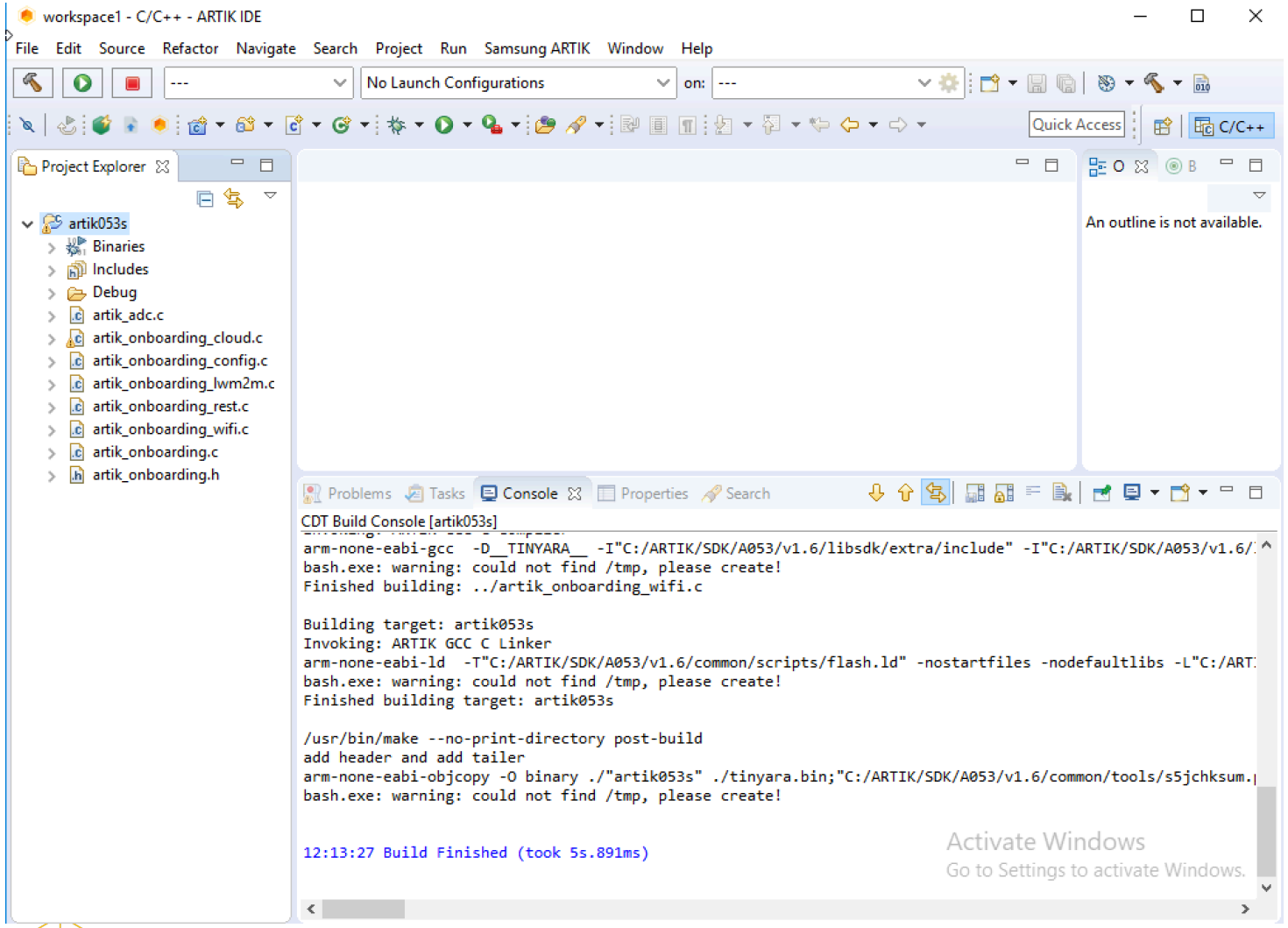
SAMSUNG ARTIK™

Confidential

ARTIK Gateway Module Development

Confidential

ARTIK IDE

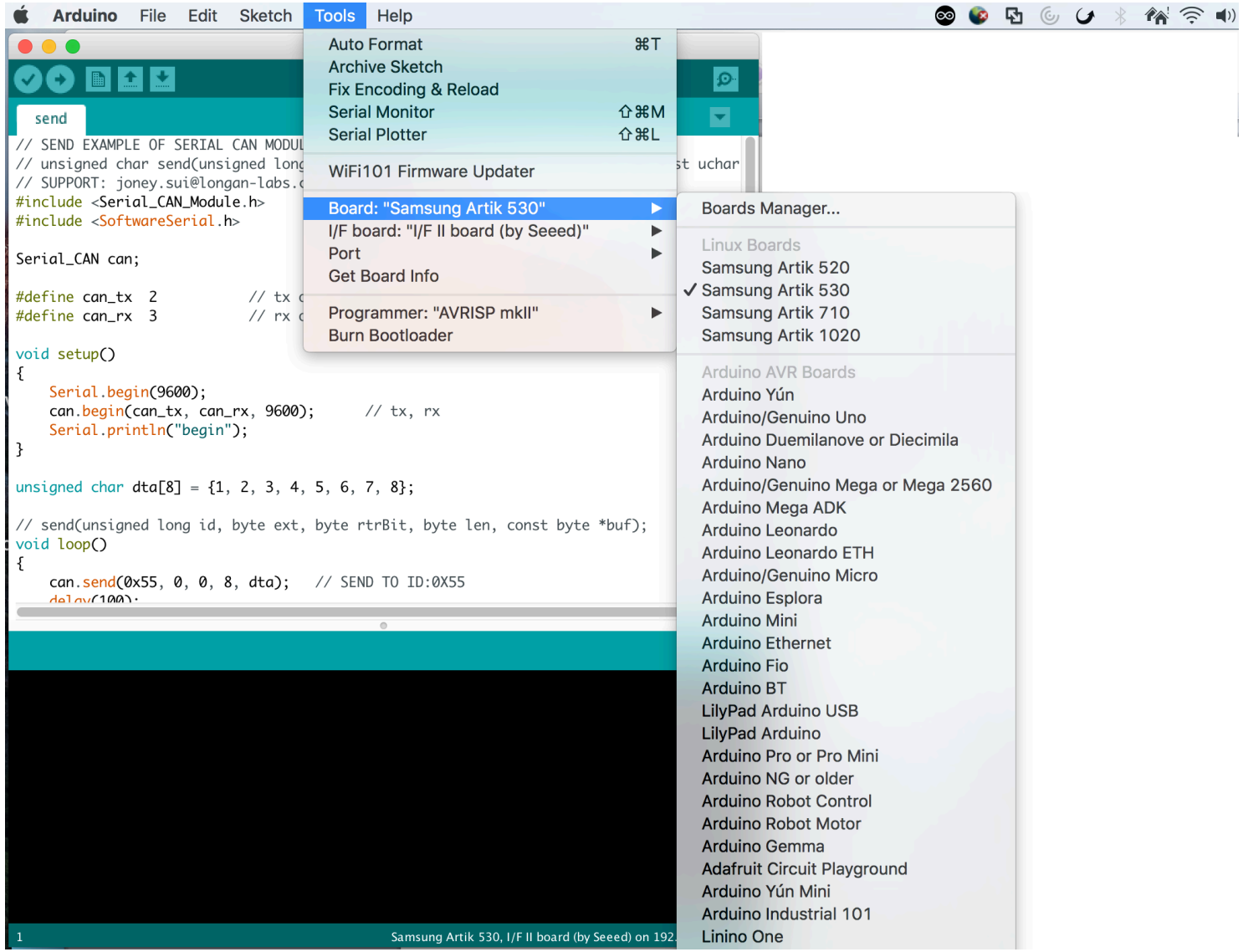


SAMSUNG ARTIK™ IDE

gcc-arm-linux-gnueabihf

SAMSUNG ARTIK™

Arduino

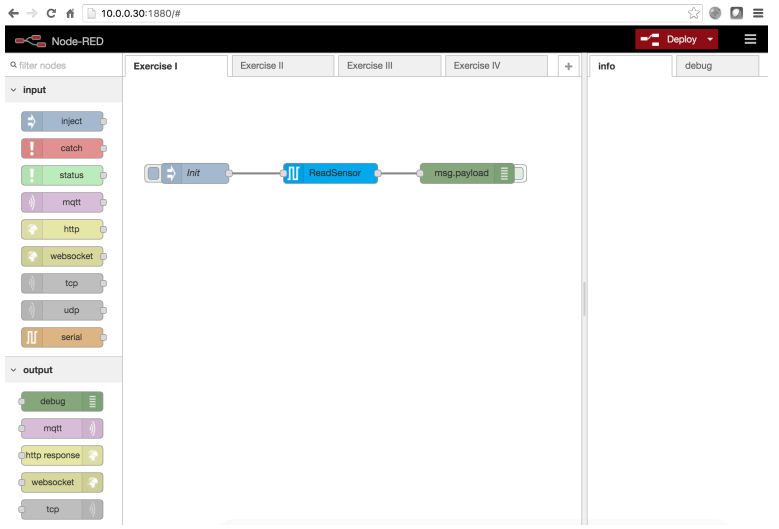


SAMSUNG ARTIK™

Confidential

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



SAMSUNG ARTIK™

Confidential

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.

3rd party Libraries/APIs

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

3rd party Frameworks, Solutions

Gateway Solutions:

AWS Greengrass

kura™

EDGE X FOUNDRY™

Communication Protocols/Frameworks:

MQTT.ORG

IoTivity

Wakaama

eclipse smarthome

OPC UA™

Modbus

thingworx®

amazon web services

Microsoft Azure

SAP® Certified
Built on SAP Cloud Platform

vmware®

IBM Bluemix™

SAMSUNG ARTIK™

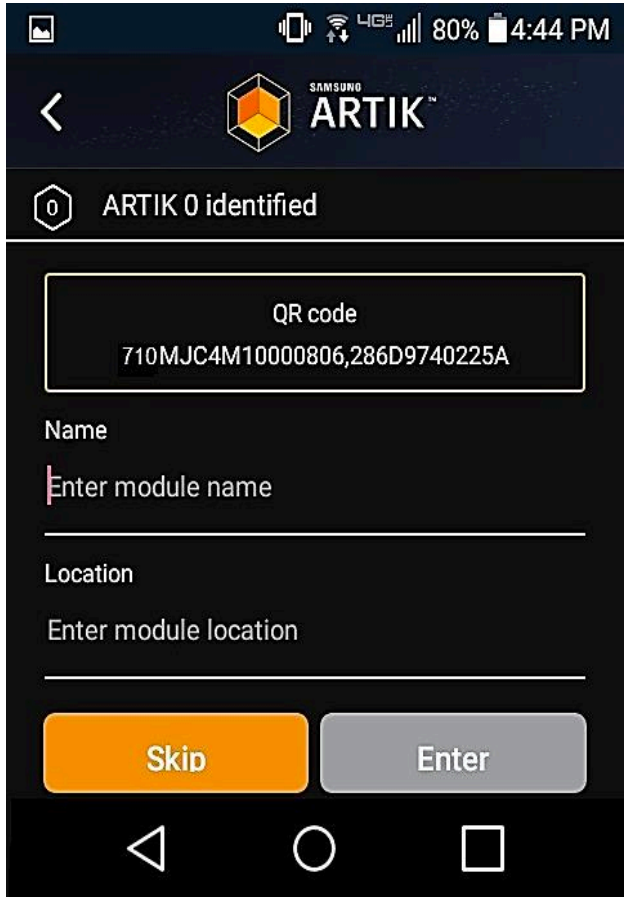
ARTIK End-to-end solution

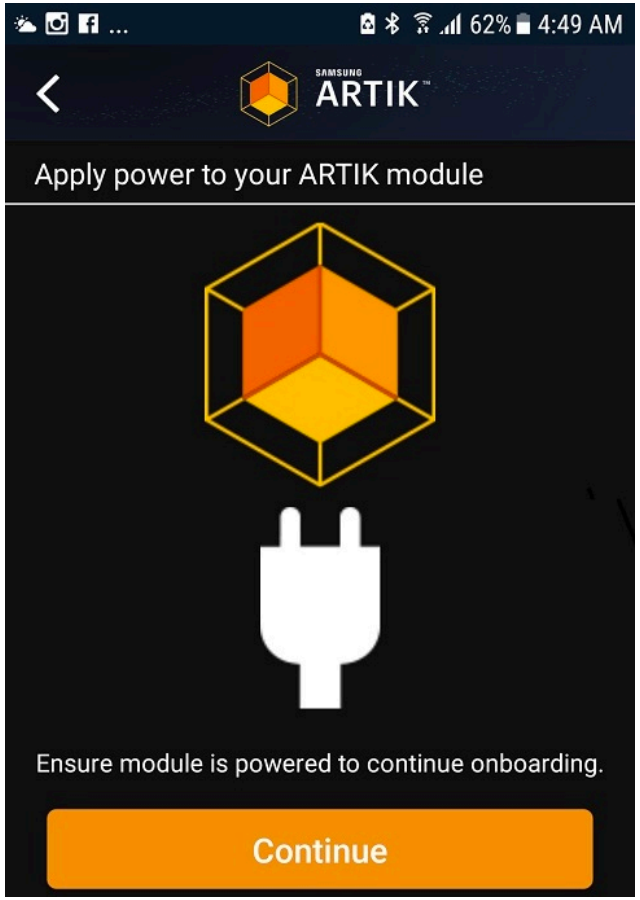
Confidential

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





SAMSUNG ARTIK™

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).

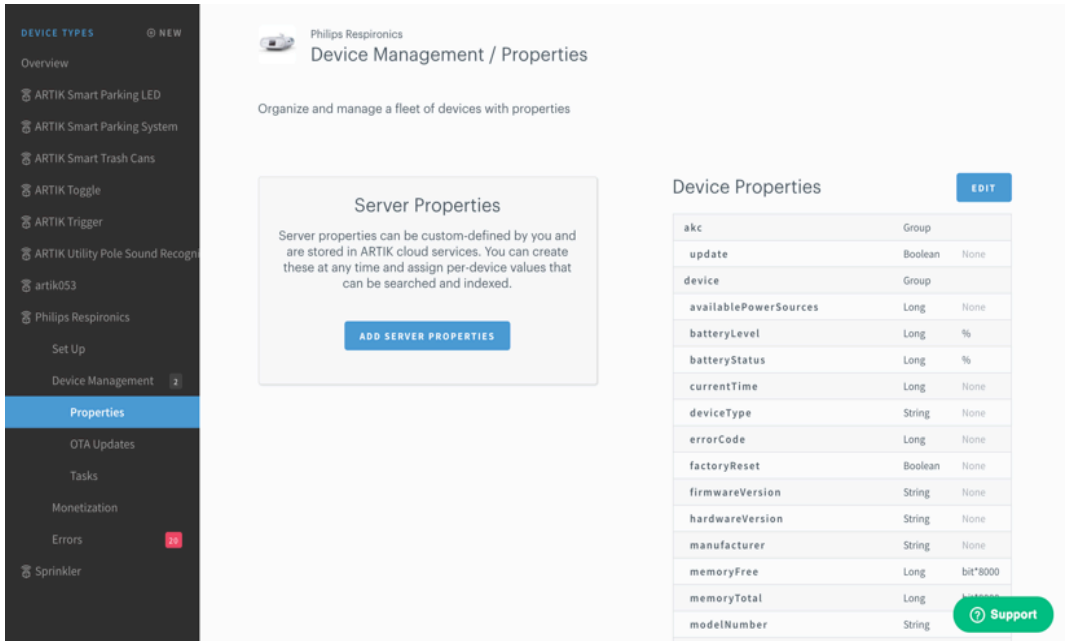
SAMSUNG ARTIK™

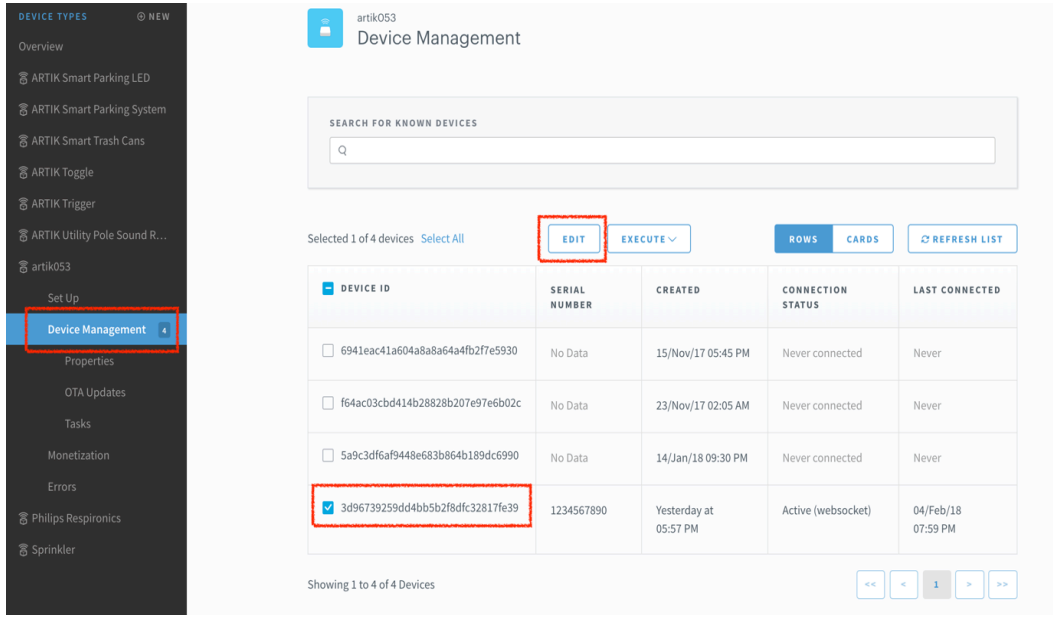
Eclipse Wakaama

- 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.

SAMSUNG ARTIK™

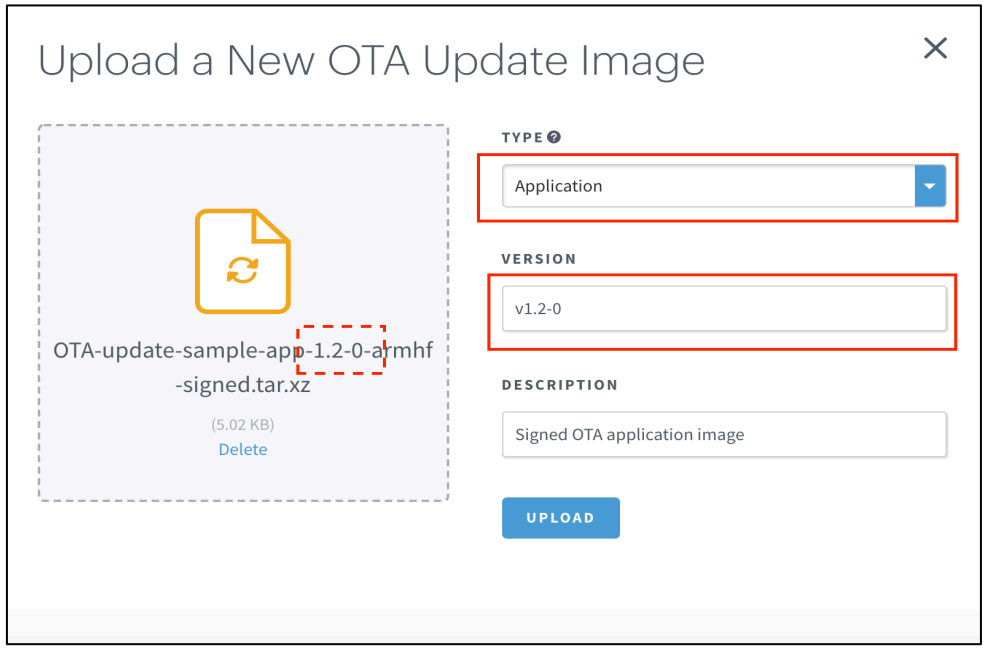
Device Management

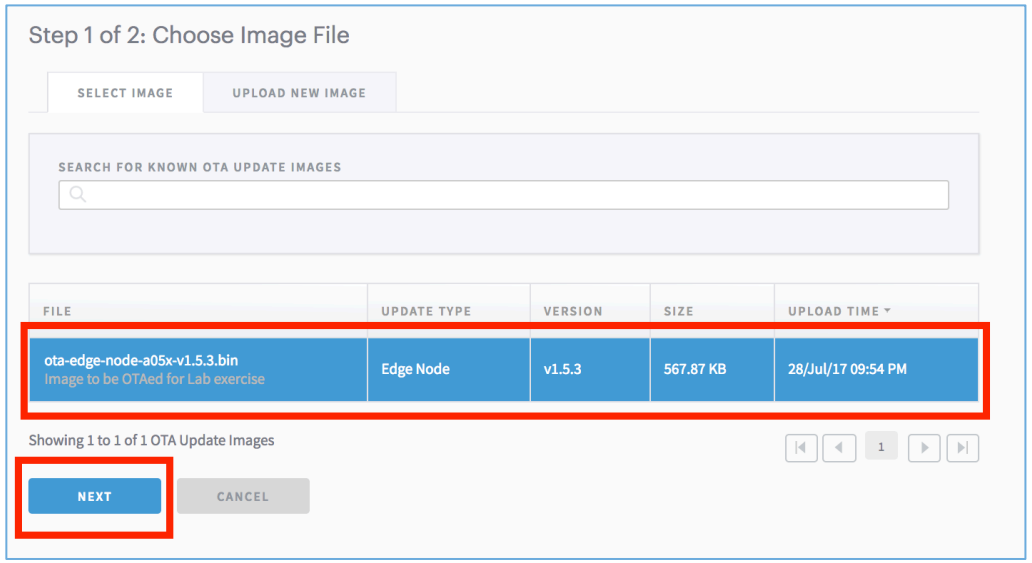


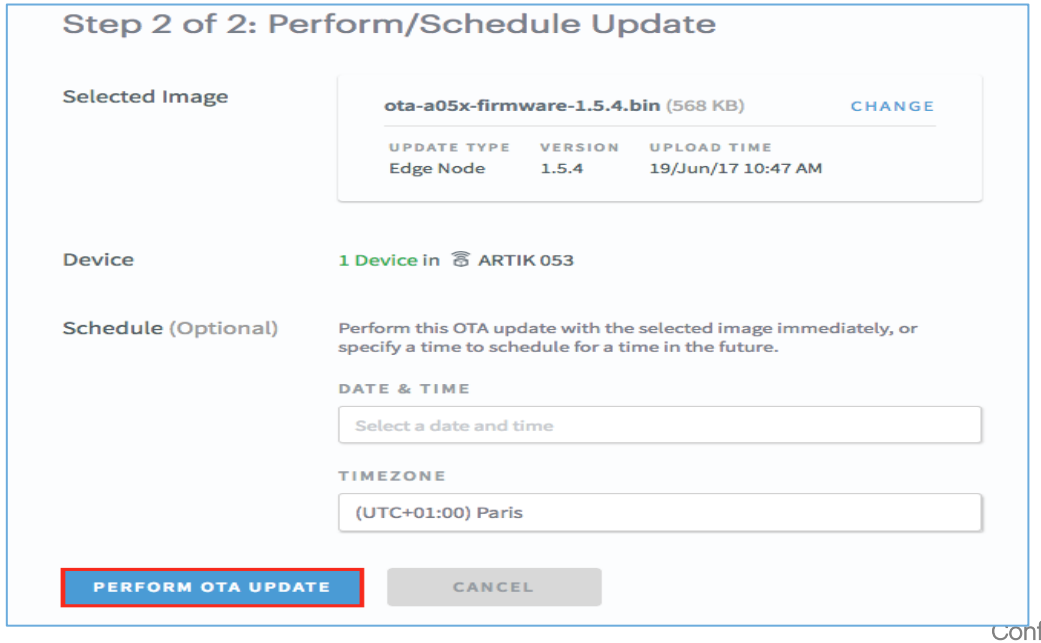


SAMSUNG ARTIK™

Device Management



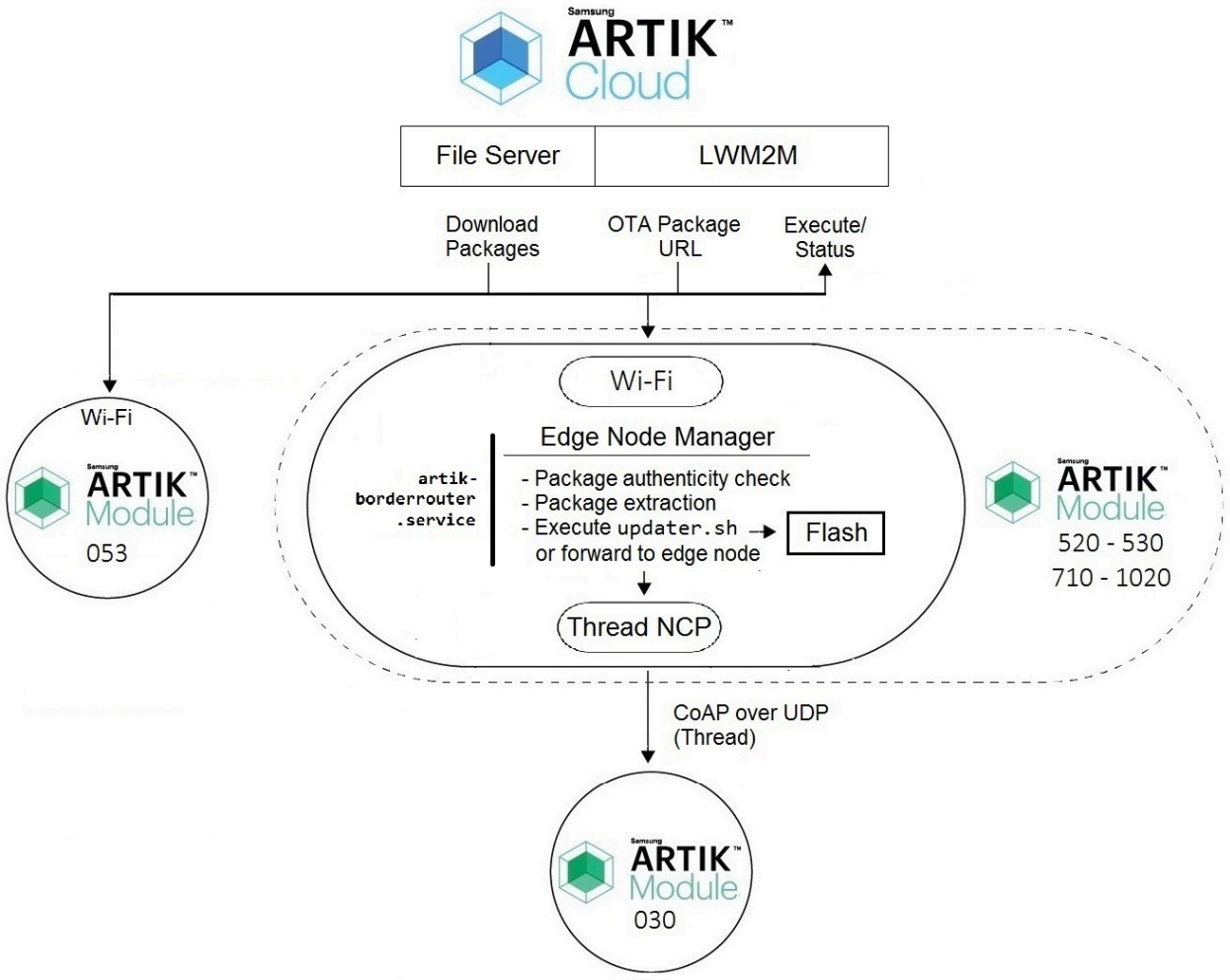




SAMSUNG ARTIK™

Confidential

Edge Node Manager

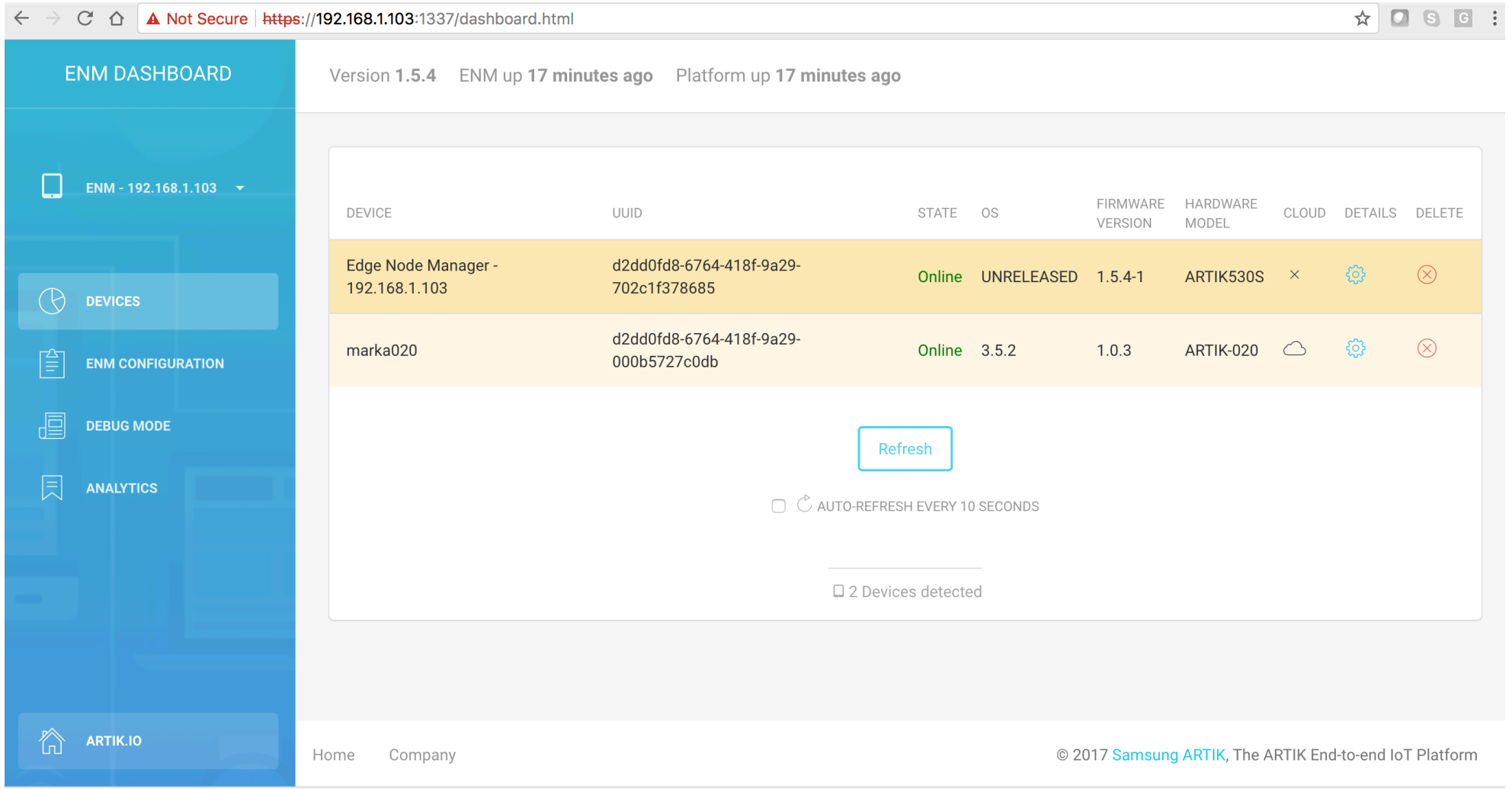


ARTIK Edge Node Manager

Manages the connection to edge devices

Manages the OTA on edge devices

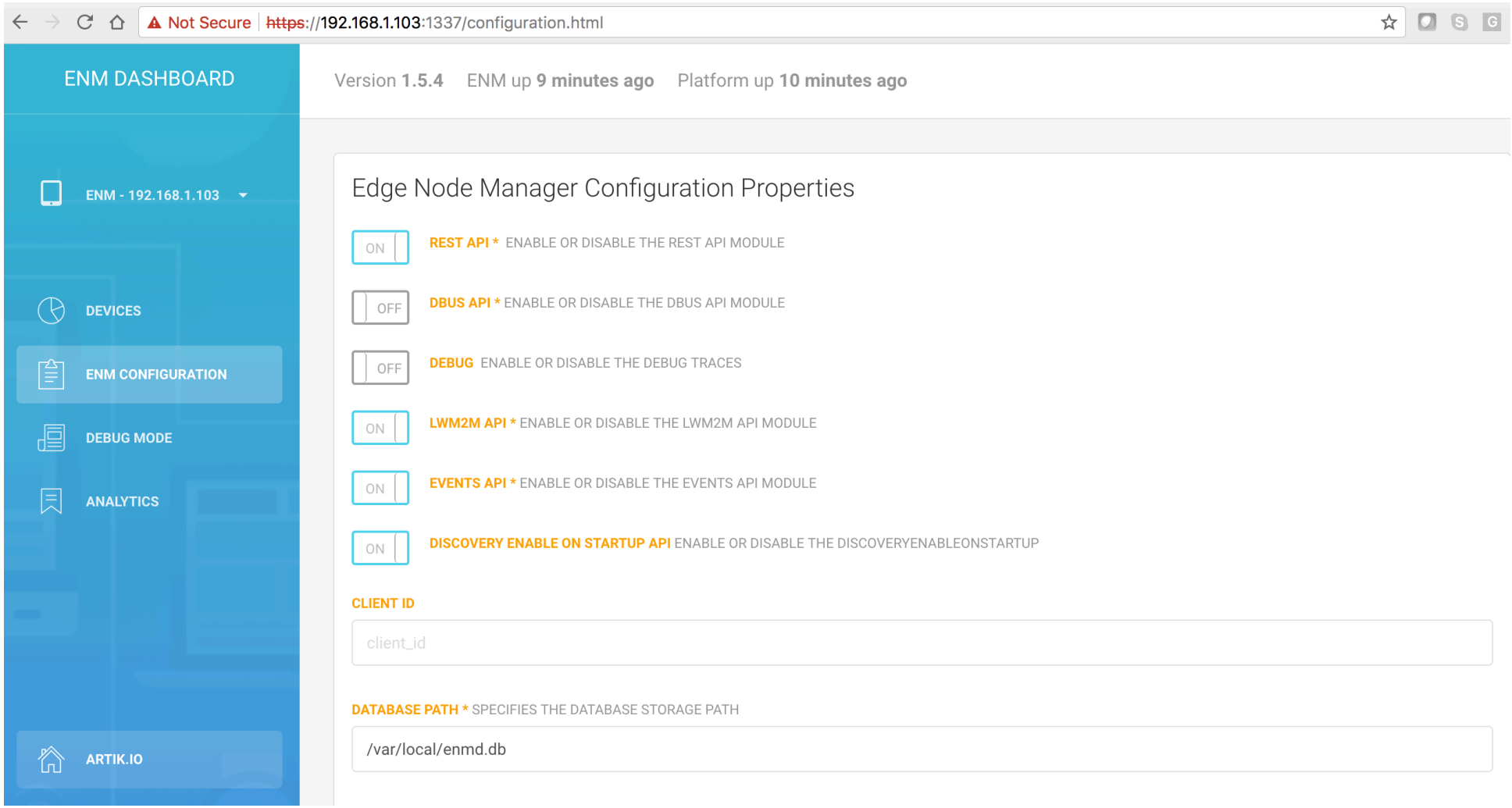
Edge Node Manager Dashboard



SAMSUNG ARTIK™

Confidential

Edge Node Manager Dashboard (Cont.)



SAMSUNG ARTIK™

ARTIK Gateway Module Use Cases and Ecosystem

Confidential

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 0x, 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. Interoperabilty expands switch capabilities, helped them get POC with Marriott “Room of the Future”.

NDA Customer: Factory automation provider

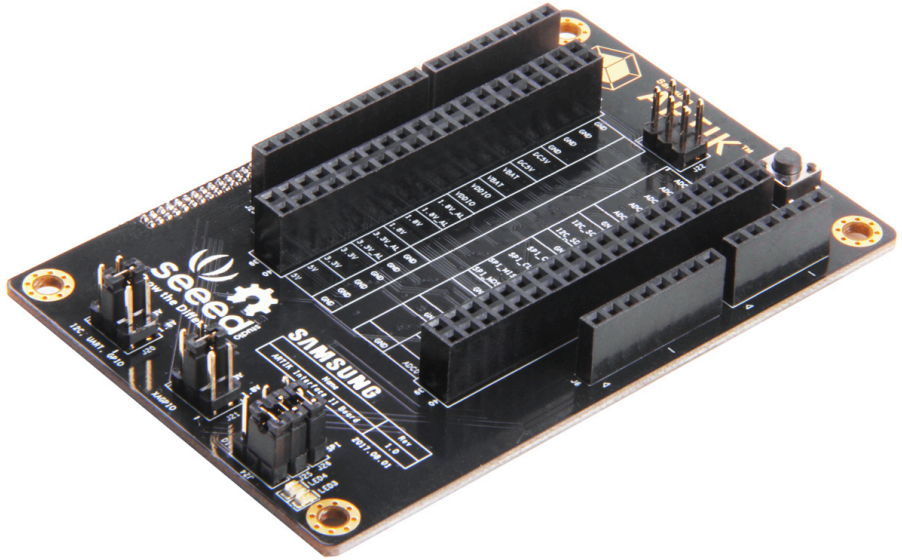
Challenge: Retrofit customer OT to meet requirements for Industry 4.0, enable access to data and create digital twins for more efficient operations. Ensure secure operations.

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

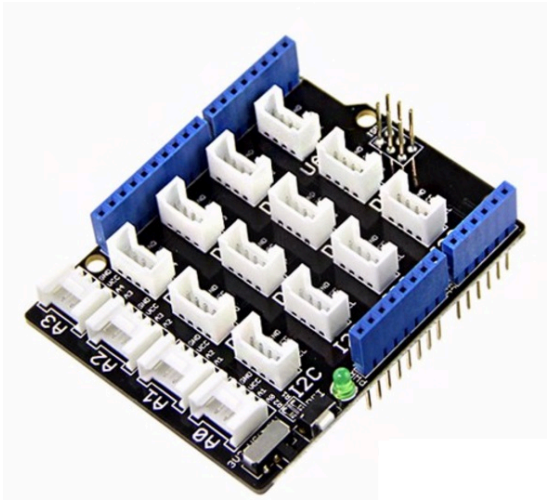
Why ARTIK? Secure gateway solution for their industrial gateway with access to local sensors, ability to do local processing and edge node management, ARTIK Cloud service for onboarding, device management & OTA, data management via integration with PTC Thingworx front end application.

SAMSUNG ARTIK™

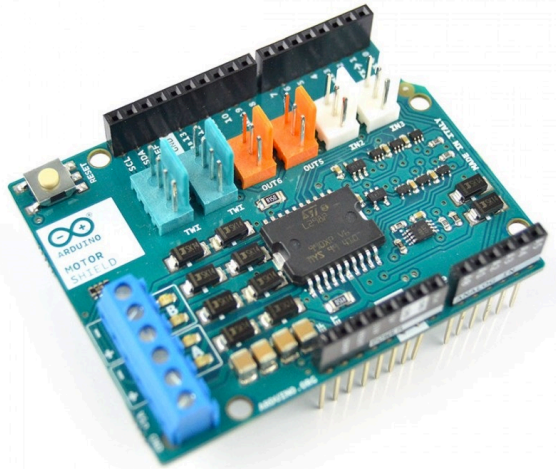
Arduino Shields



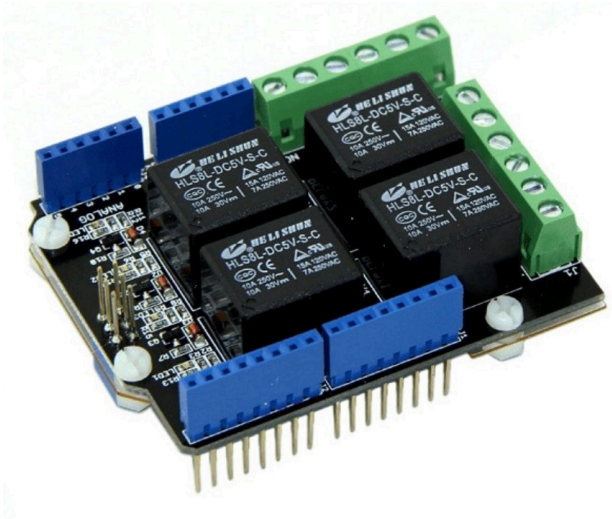
Arduino IF II board



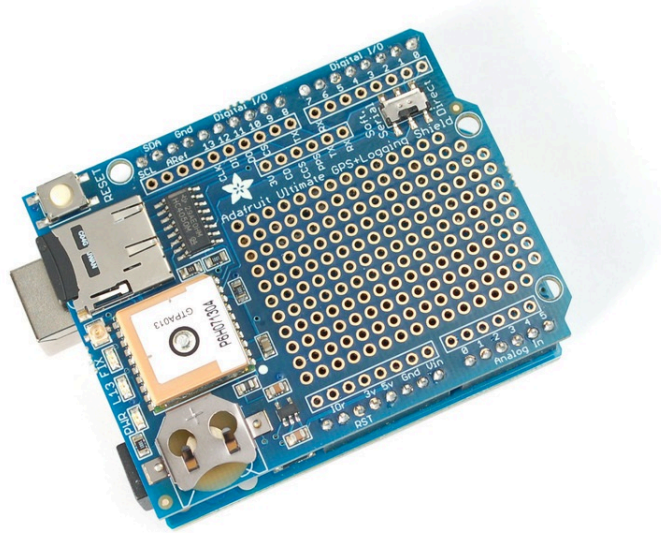
Base Shield



Motor Shield



Relay Shield



GPS Logger Shield

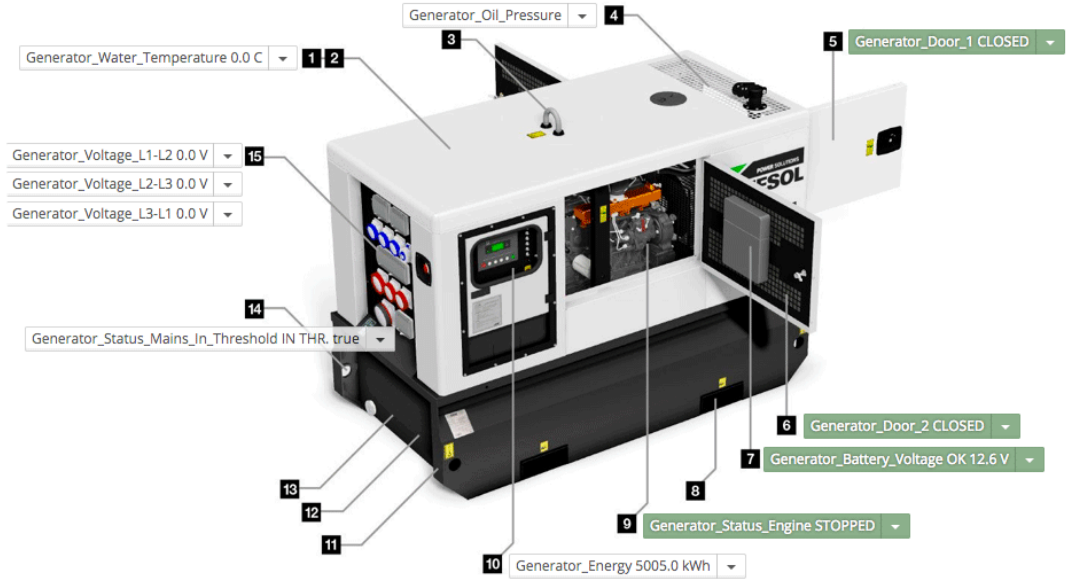
Kitra GTI
ARTIK 710s

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



SAMSUNG ARTIK™

Confidential

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

SAMSUNG ARTIK™

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

SAMSUNG ARTIK™

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.

SAMSUNG ARTIK™

Confidential

Machine Learning Inference
ARTIK 5x/7x

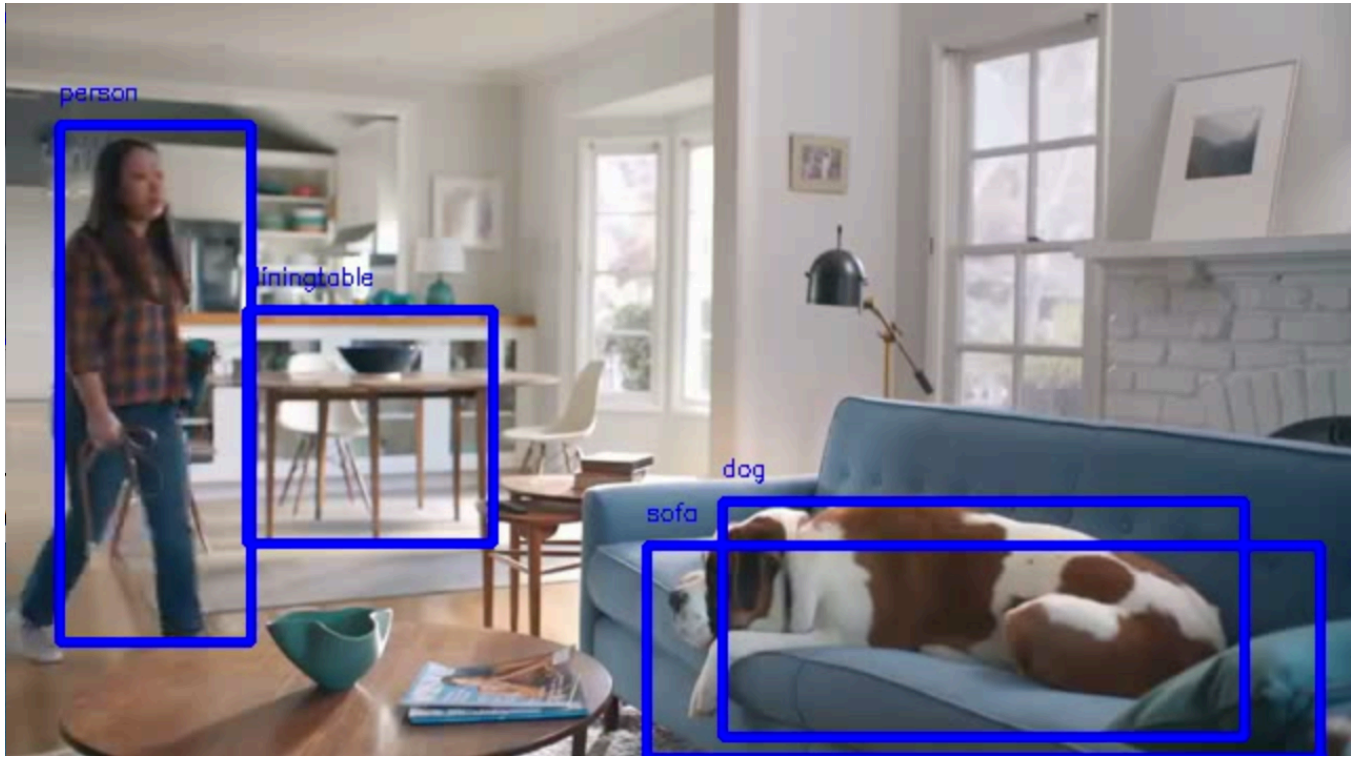
Run Machine Learning Inference on ARTIK gateway devices

Use case: Smart Factory, Smart Building etc.

Hardware: ARTIK 5x/7x

Software: Tensorflow Lite;

AWS Greengrass ML Inference;



SAMSUNG ARTIK™

ARTIK Security

SAMSUNG
ARTIK™

Confidential

Security Questionnaire

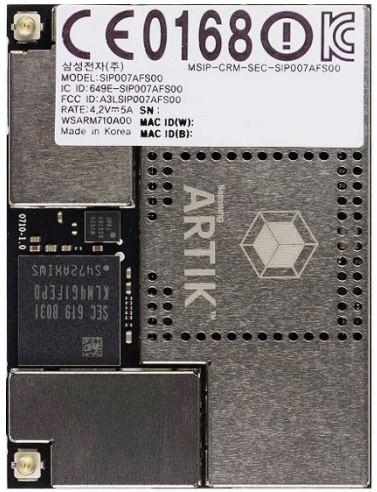
How do you provide security across all attack surfaces?

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 3rd party security vendor)
How do you guarantee your firmware integrity?	Secure Boot

Non-S vs. S Modules

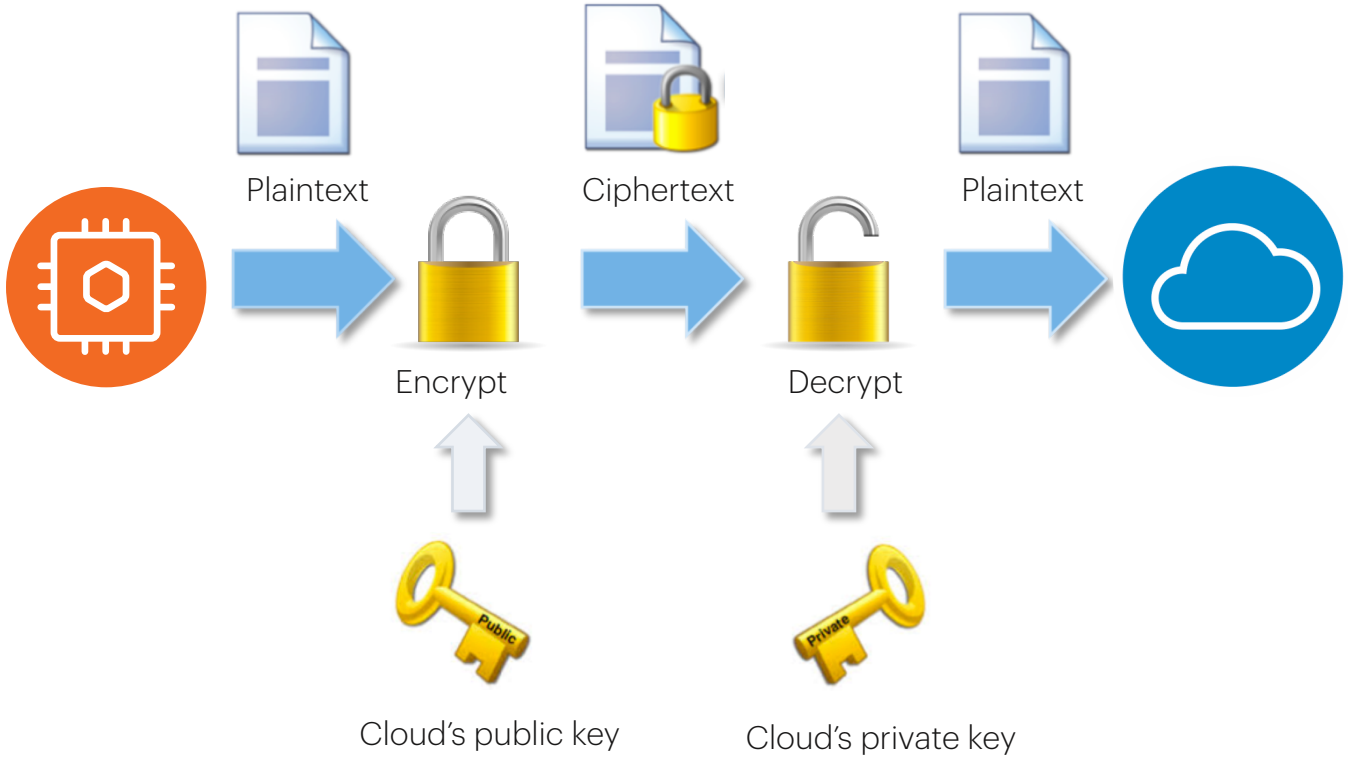
- Same HW specifications other than security features
- "s" type modules can be identified by blue labeling

Standard module



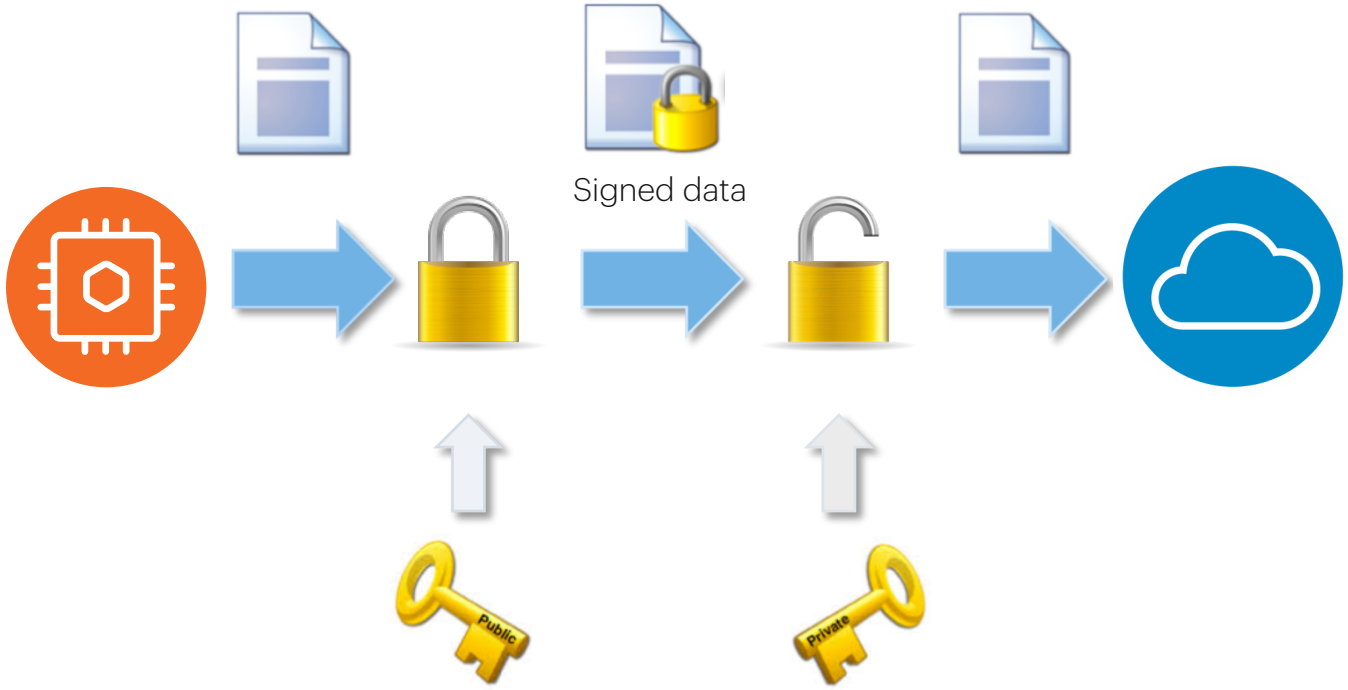
"S" module

Encryption and Decryption



Different keys are used to encrypt and decrypt messages

Signature

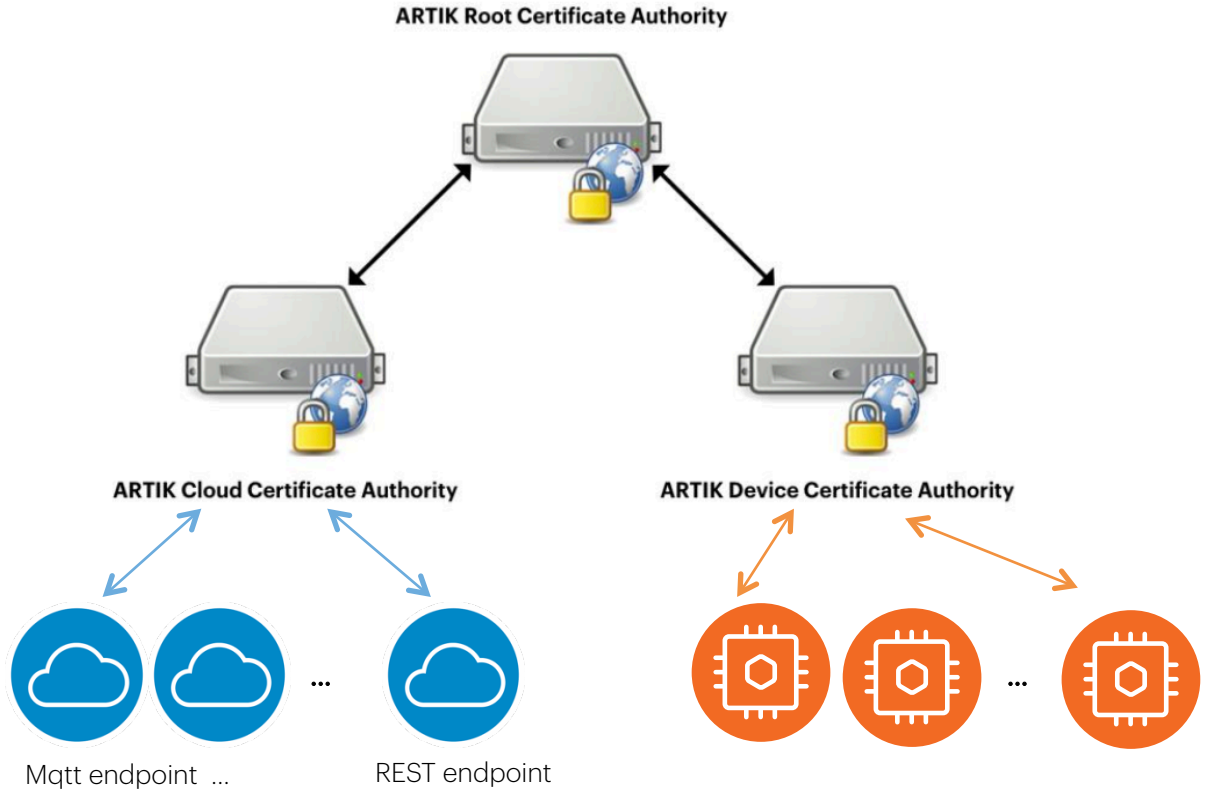

Signed data
Public
Private
Module A's private key
Module A's public key

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 3rd 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

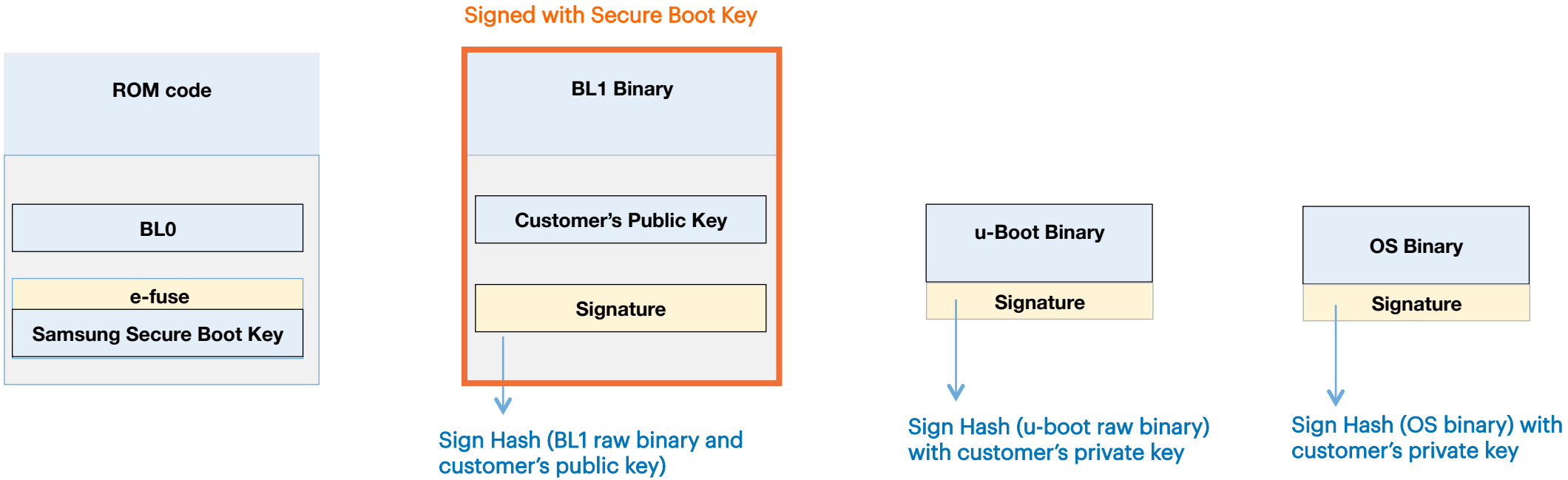
		ARTIK module (05x, 5, 7)	ARTIK S-module (053s, 055s, 530s, 710s)	Comments
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to 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

SAMSUNG ARTIK™

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



BL0:
1. Decrypt BL1
2. Verify signature using BL1 Hash(BL1 binary and customer's public key) and hash

BL1:
1. Verify signature using u-boot Hash (u-boot binary and customer's public key)
2. Load to DRAM

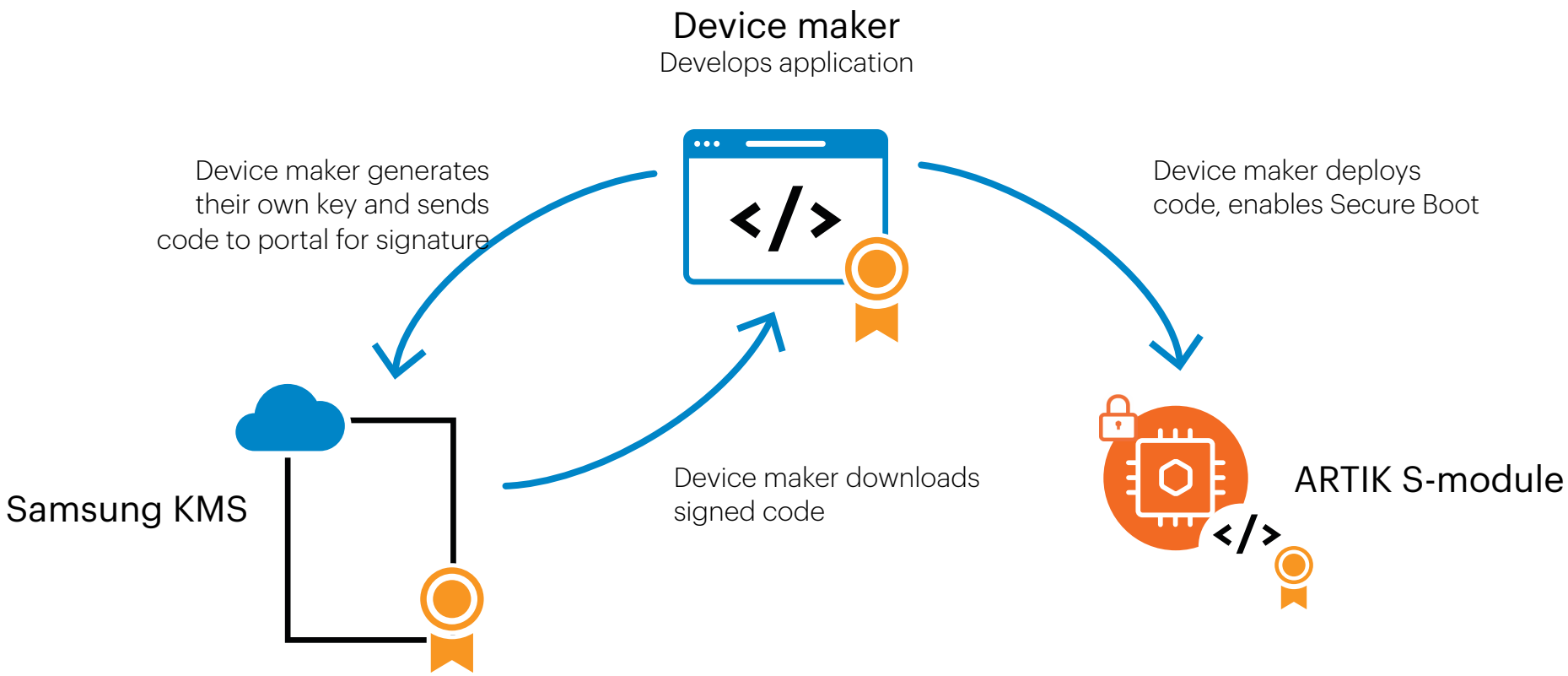
u-boot:
1. Verify signature using (OS binary and customer's public key)
2. Load to DRAM

SAMSUNG ARTIK™

NEW

Samsung ARTIK™ Key Management System(KMS)

Code signing portal manages key signing



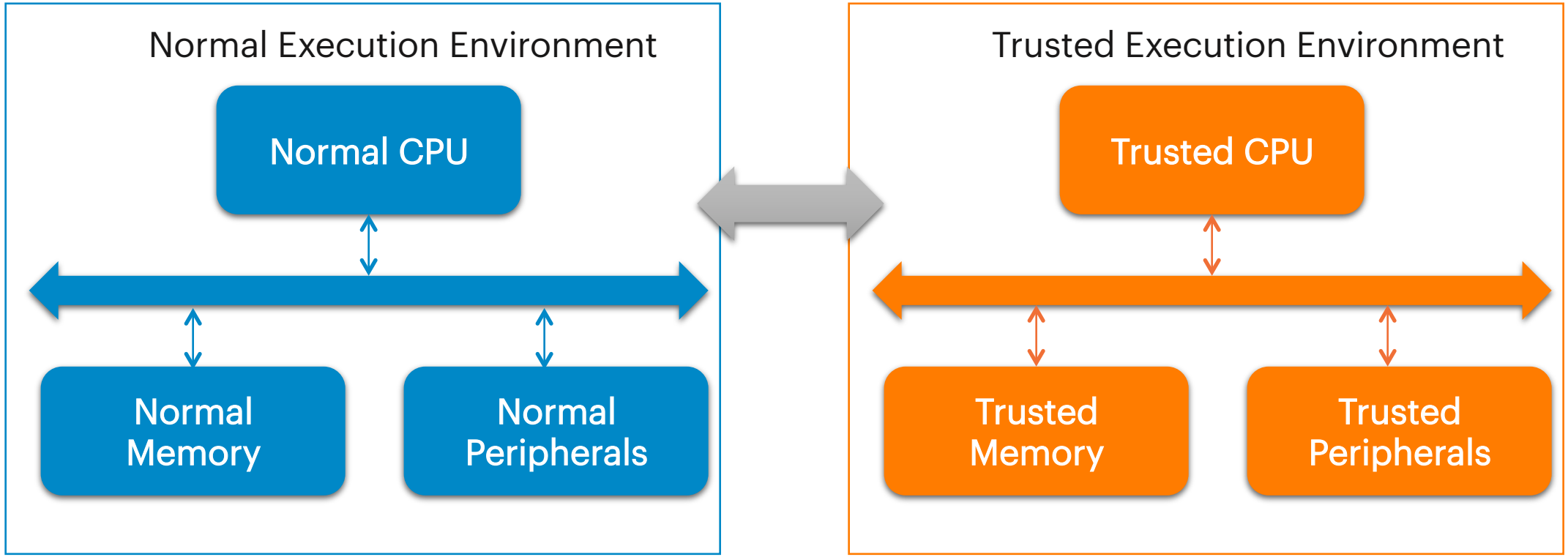
SAMSUNG ARTIK™

Device Protection

		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

SAMSUNG ARTIK™

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

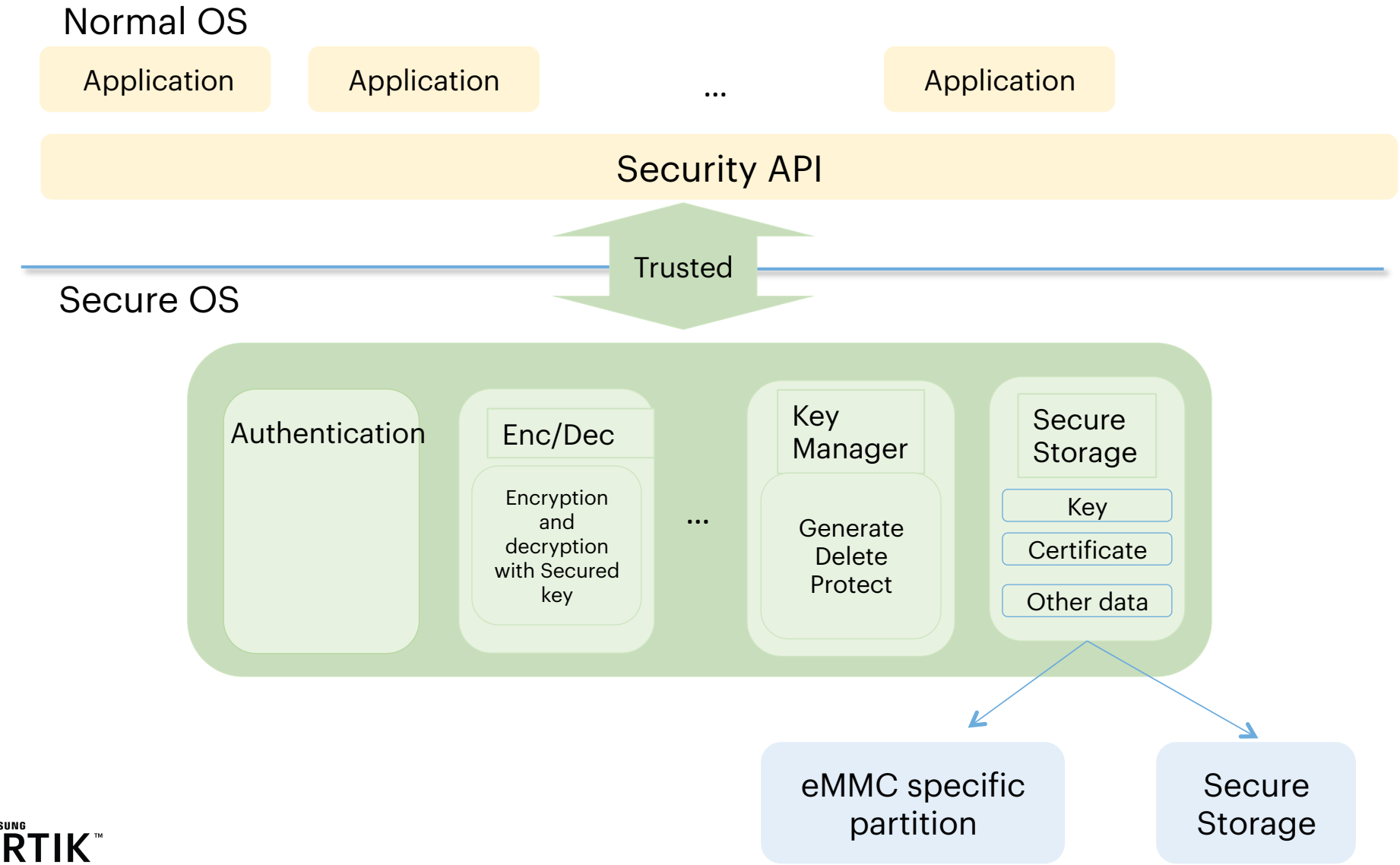
SAMSUNG ARTIK™

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

		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**

SAMSUNG ARTIK™

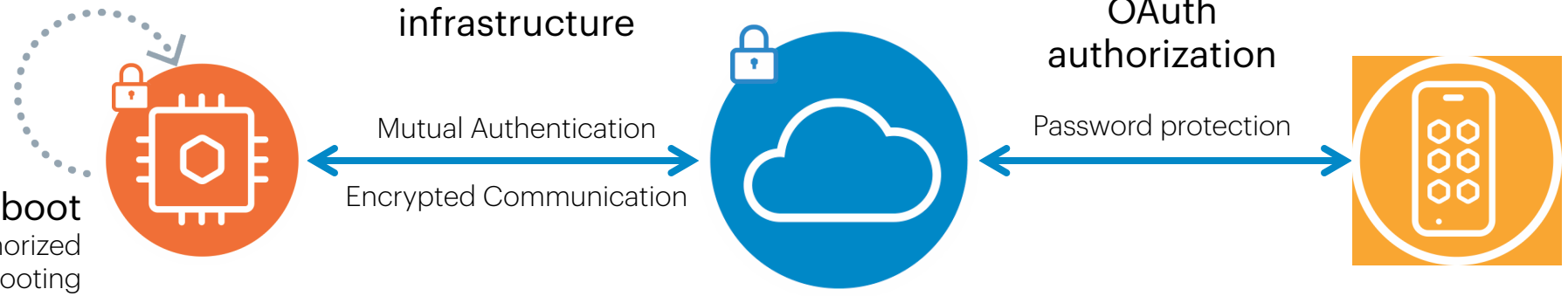
Samsung ARTIK™ End-to-end Platform Security

End-to-end protection for you and your customers

ARTIK Modules

SmartThings Cloud

Mobile apps



Secure boot
Prevents unauthorized software from booting and running on device

Secure OS
Hardware-enforced secure applications

Secure storage
Data encryption

Authentication and authorization, Secure OTA
Cloud services are protected

User data encryption
Protects sensitive info on mobile devices

SAMSUNG ARTIK™

ARTIK Training Tues

Confidential

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)

SAMSUNG ARTIK™

Confidential

Training Schedule

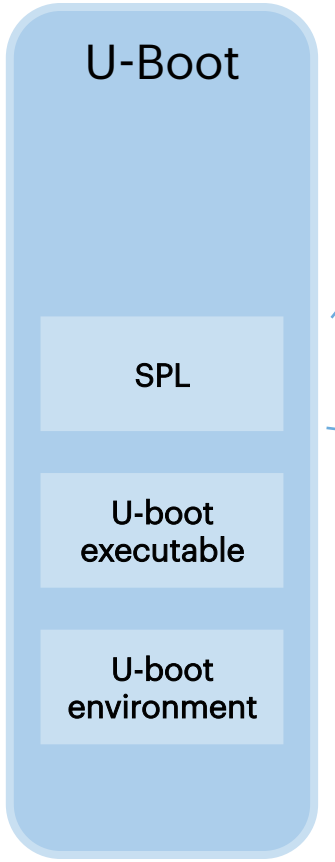
Date	Topics
Aug 14th	Level 1 - ARTIK Intro
Aug 28th	Level 2- Onboarding and OTA
Sep 11th	Level 2- Cloud Communication
Sep 25th	Level 3- Use ARTIK Cloud for device management and AWS for data management
Oct 9th	Level 1 -ARTIK Intro (repeated content)
Oct 23rd	Level 2- Security
Nov 13th	Level 2 - ARTIK Hardware Interface
Nov 27th	Level 3- Use TensorFlow Lite on ARTIK 5x for Machine Learning Inference
Dec 11th	Level 1- ARTIK 310 Intro

SAMSUNG ARTIK™

APPENDIX

Confidential

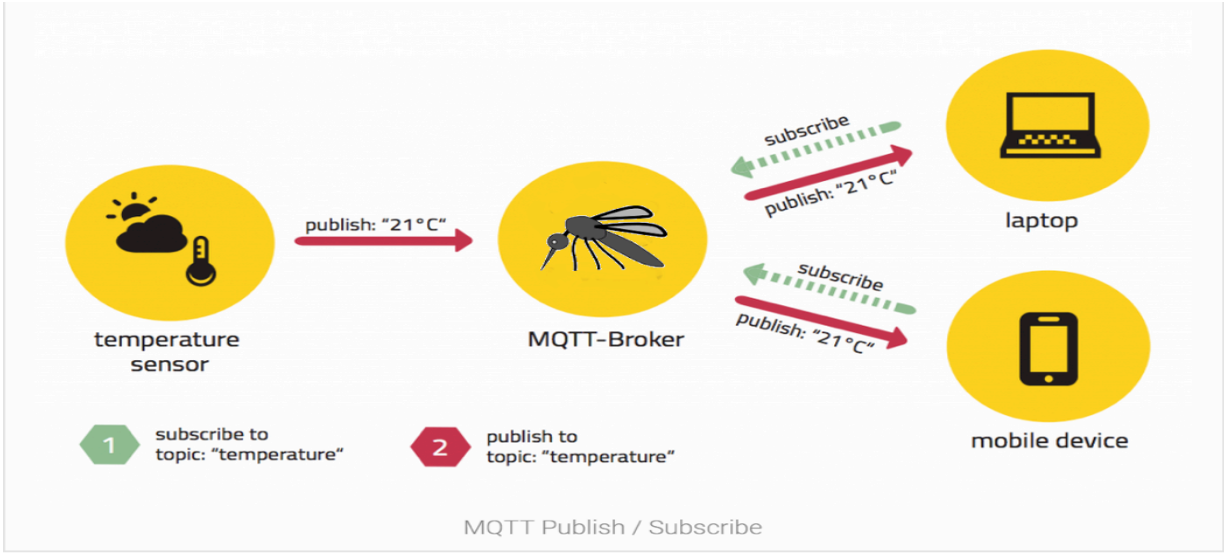
U-Boot



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



MQTT Publish / Subscribe

SAMSUNG ARTIK™

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.

SAMSUNG ARTIK™

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) 

  Microsoft Azure 

  Eclipse Mosquitto (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

SAMSUNG ARTIK™

dential