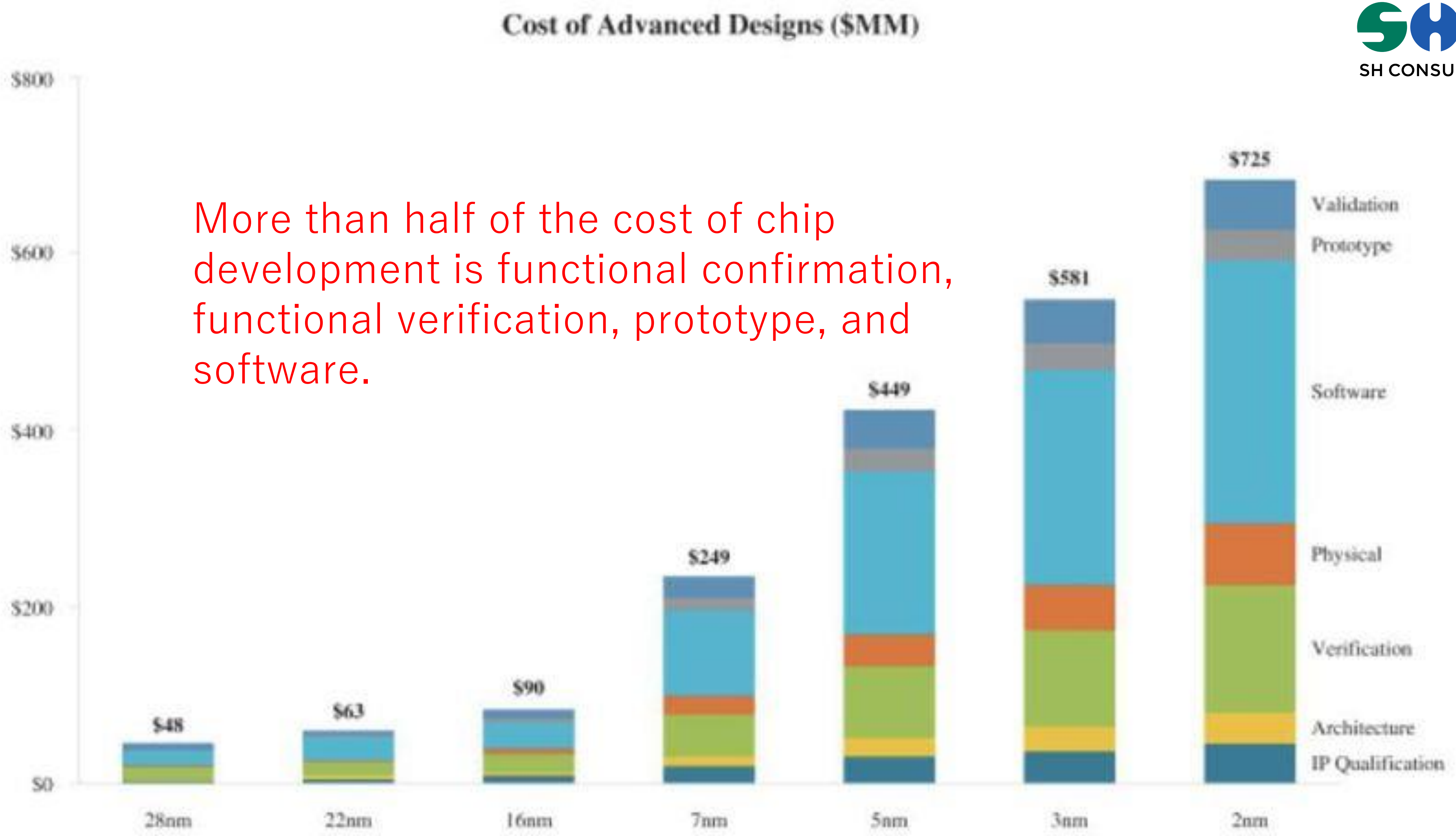
SH CONSULTING

SHC RISC-V Chip

2023/09/21

SHC Kawasaki

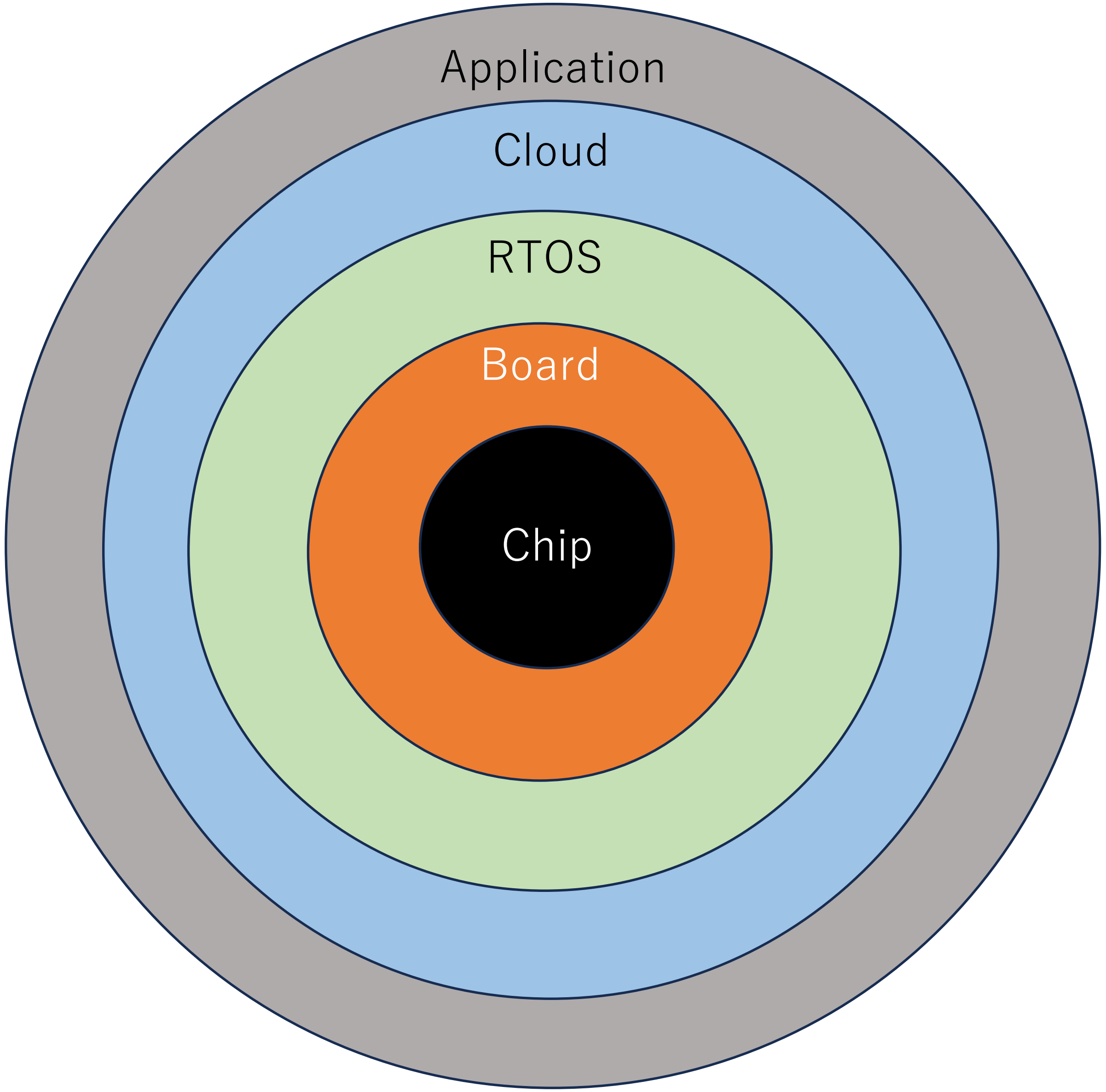


More than half of the cost of chip development is functional confirmation, functional verification, prototype, and software.

Source: IBS July 2022.

SHC RISC-V Chip scope

SH CONSULTING



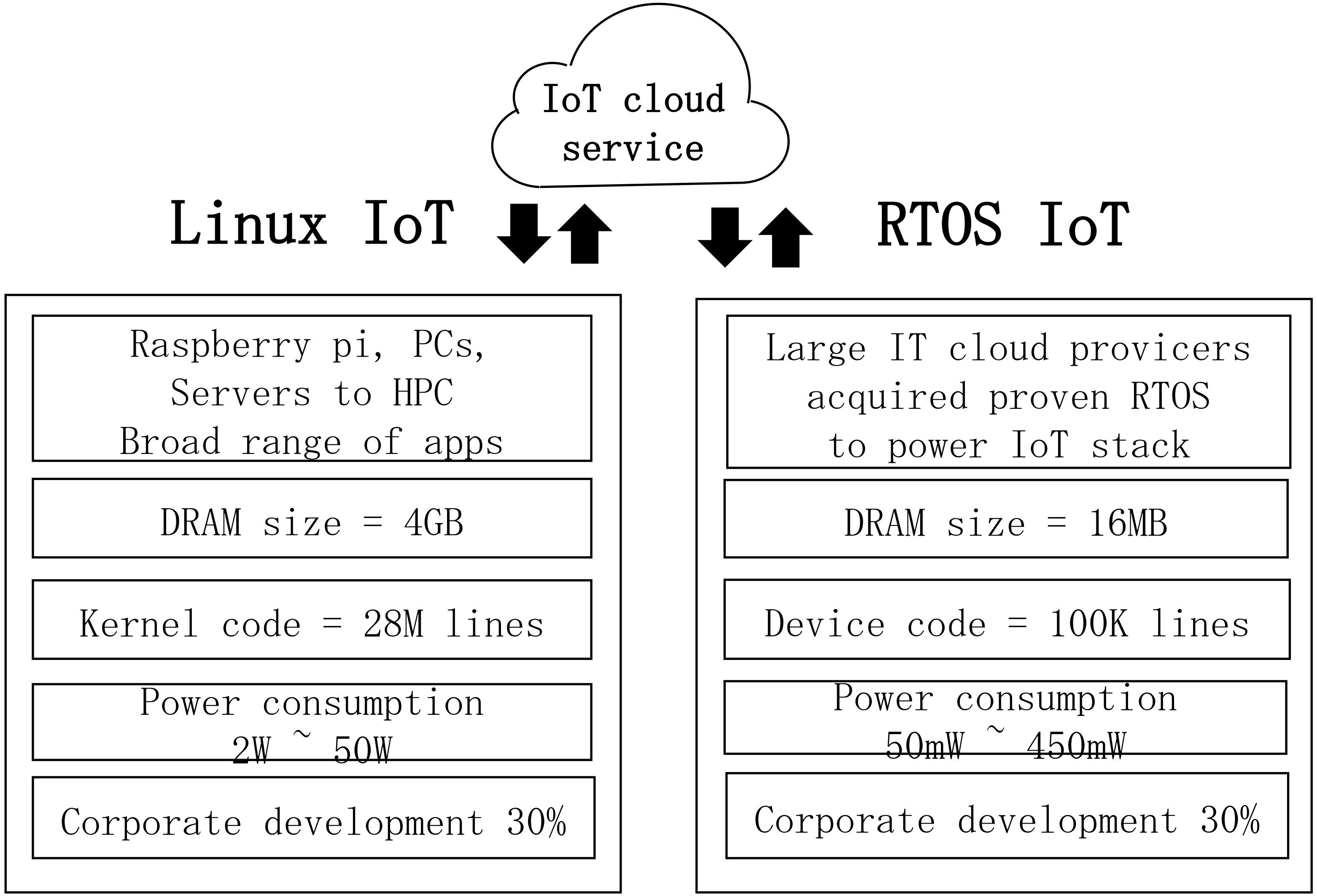
Linux and RTOS in IoT

Linux IoT products

Amazon Greengrass
2016-

Microsoft Azure
2008-

Google Android
Things
2016-2019
(withdrawed)



IoT cloud service

Linux IoT

Raspberry pi, PCs,
Servers to HPC
Broad range of apps

DRAM size = 4GB

Kernel code = 28M lines

Power consumption
2W ~ 50W

Corporate development 30%

RTOS IoT

Large IT cloud provicers
acquired proven RTOS
to power IoT stack

DRAM size = 16MB

Device code = 100K lines

Power consumption
50mW ~ 450mW

Corporate development 30%

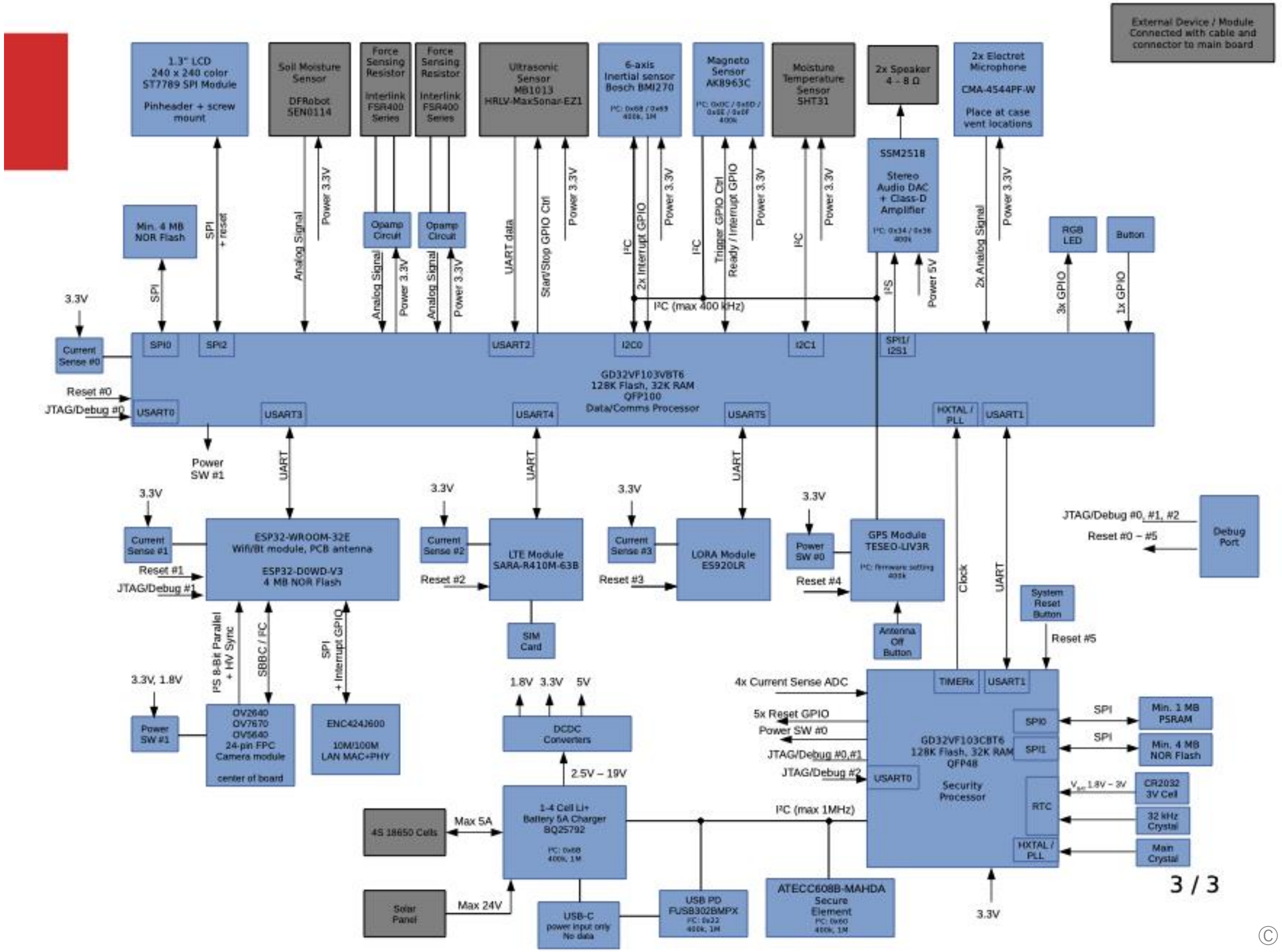
RTOS IoT products

Amazon FreeRTOS
2017-

Microsoft Azure
RTOS 2019-

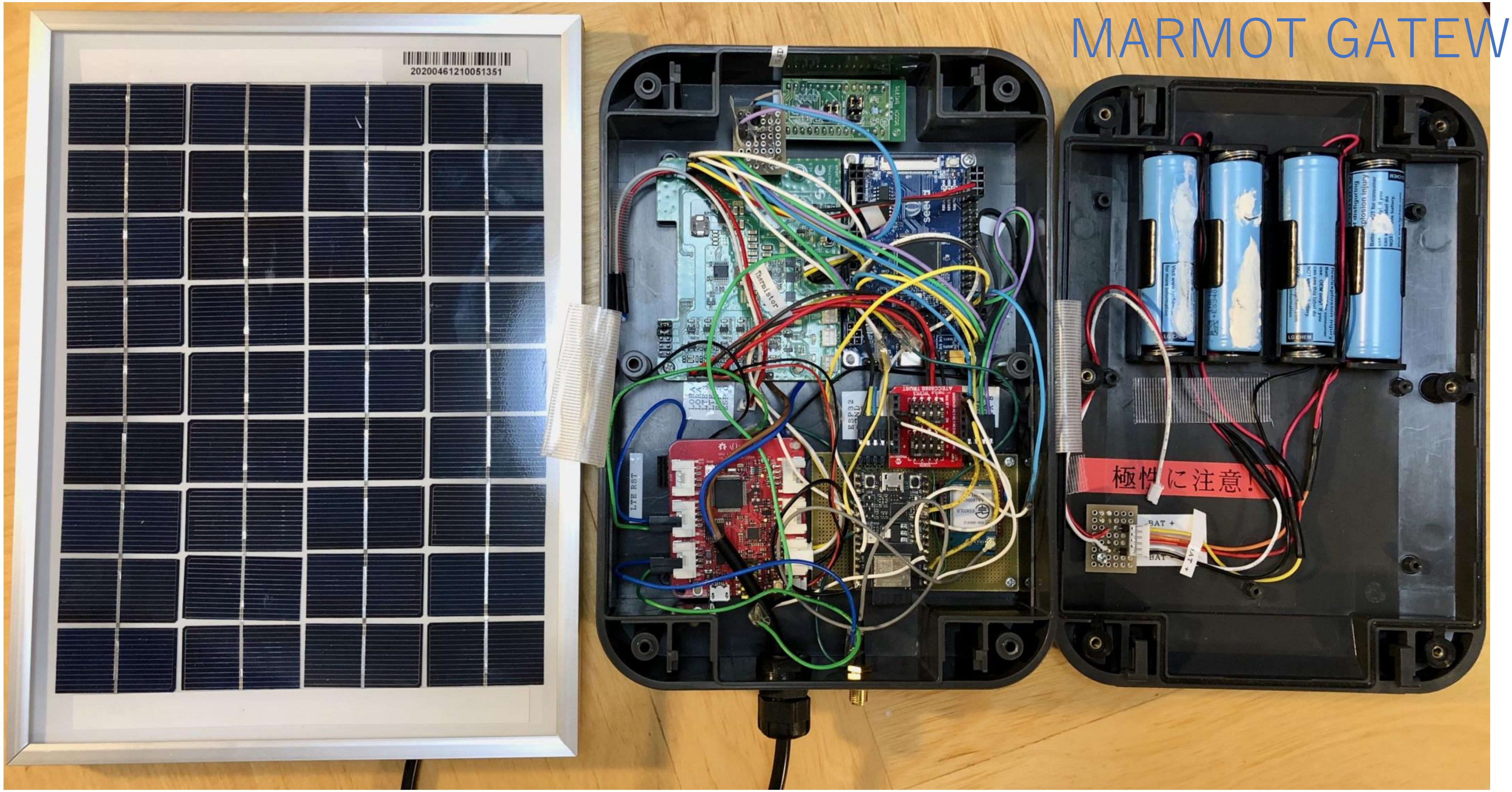
Google Fuchsia
2022new development

Concept 1 (2019) ⇨ Divide the system into small MCUs
Partially supplies power to only the operating parts to save power


External Device / Module Connected with cable and connector to main board
1.3" LCD 240 x 240 color ST7789 SPI Module Pinheader + screw mount
Soil Moisture Sensor DFRobot SEN0114
Force Sensing Resistor Interlink FSR400 Series
Force Sensing Resistor Interlink FSR400 Series
Ultrasonic Sensor MB1013 HRLV-MaxSonar-EZ1
6-axis Inertial sensor Bosch BMI270 I^2C: 0x68 / 0x69 400k, 1M
Magneto Sensor AK8963C I^2C: 0x0C / 0x0D / 0x0E / 0x0F 400k
Moisture Temperature Sensor SHT31
2x Speaker 4 – 8 Ω
SSM2518 Stereo Audio DAC + Class-D Amplifier I^2C: 0x34 / 0x36 400k
2x Electret Microphone CMA-4544PF-W Place at case vent locations
Min. 4 MB NOR Flash
SPI
SPI + reset
Analog Signal
Power 3.3V
Opamp Circuit
Opamp Circuit
Analog Signal
Power 3.3V
Analog Signal
Power 3.3V
UART data
Start/Stop GPIO Ctrl
Power 3.3V
I^2C
2x Interrupt GPIO
Power 3.3V
I^2C
Trigger GPIO Ctrl
Ready / Interrupt GPIO
Power 3.3V
I^2C
Power 3.3V
I^2S
Power 5V
2x Analog Signal
Power 3.3V
RGB LED
Button
3x GPIO
1x GPIO
I^2C (max 400 kHz)
3.3V
Current Sense #0
Reset #0
JTAG/Debug #0
SPI0
SPI2
USART2
I2C0
I2C1
SPI1/ I2S1
GD32VF103VBT6 128K Flash, 32K RAM QFP100 Data/Comms Processor
USART0
USART3
USART4
USART5
HXTAL / PLL
USART1
Power SW #1
UART
UART
UART
3.3V
Current Sense #1
ESP32-WROOM-32E Wifi/Bt module, PCB antenna ESP32-D0WD-V3 4 MB NOR Flash
Reset #1
JTAG/Debug #1
3.3V
Current Sense #2
LTE Module SARA-R410M-63B
Reset #2
SIM Card
3.3V
Current Sense #3
LORA Module ES920LR
Reset #3
3.3V
Power SW #0
GPS Module TESEO-LIV3R I^2C: firmware setting 400k
Reset #4
Antenna Off Button
Clock
UART
JTAG/Debug #0, #1, #2
Reset #0 – #5
Debug Port
System Reset Button
Reset #5
I^2S 8-Bit Parallel + HV Sync
SBBC / I^2C
SPI + Interrupt GPIO
3.3V, 1.8V
Power SW #1
OV2640 OV7670 OV5640 24-pin FPC Camera module center of board
ENC424J600 10M/100M LAN MAC+PHY
1.8V 3.3V 5V
DCDC Converters
2.5V – 19V
1-4 Cell Li+ Battery 5A Charger BQ25792 I^2C: 0x6B 400k, 1M
4S 18650 Cells
Max 5A
Solar Panel
Max 24V
USB-C power input only No data
USB PD FUSB302BMPX I^2C: 0x22 400k, 1M
ATECC608B-MAHDA Secure Element I^2C: 0x60 400k, 1M
I^2C (max 1MHz)
4x Current Sense ADC
5x Reset GPIO
Power SW #0
JTAG/Debug #0,#1
JTAG/Debug #2
TIMERx
USART1
USART0
GD32VF103CBT6 128K Flash, 32K RAM QFP48 Security Processor
SPI0
SPI1
RTC
HXTAL / PLL
SPI
SPI
Min. 1 MB PSRAM
Min. 4 MB NOR Flash
V_{bat} 1.8V – 3V
CR2032 3V Cell
32 kHz Crystal
Main Crystal
3.3V
3 / 3

Implementation 1 ⇨ Partially powered Secure RTOS IoT

MARMOT = Microdevice Architecture Resistant to Malware, Obstractions and Tampering



MARMOT GATEWAY

Concept 2 (2020) ⇨ Power supply status monitor + power supply chip for partial power supply

SH CONSULTING

Power Supply Unit Board (PSU)

電源ユニットの基板（PSU）

Six 3.3V power rails and grounds that can be turned on and off independently by software control

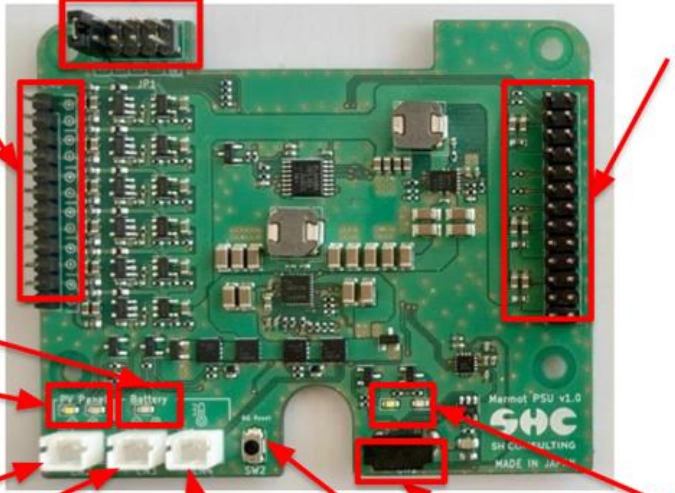
ソフトウェア制御により、6つの3.3V電源レールとグラウンドを独立してオン／オフ可能

Shunt terminals to specify lithium-ion battery serial configuration

リチウムイオン電池直列構成指定用シャント端子

The 26-pin header contains an I2C interface to control the following four ICs and interrupt request pins from these ICs: (1) an IC to control MPPT of solar panel voltage and current, charge/discharge control of lithium-ion battery, and integrated control of USB-C protocol, (2) an IC to control GPIO to turn on/off six power islands, (3) a buck regulator IC for 3.3V power supply, and (4) an IC to control USB-C protocol. The header also includes output pins for measuring the current consumption of the six power rails supplied by the PSU, which are to be connected to an analog-to-digital converter.

26ピンヘッダは、以下の4つの ICを制御するI2Cインターフェースと、これらの ICからの割込要求端子を含みます：（1）太陽光パネルの電圧・電流の MPPT制御、リチウムイオン電池の充放電制御、USB-Cプロトコルの統合制御を行うIC、（2）6つの電源島をON/OFFするGPIOを制御するIC、（3）3.3V給電用バックレギュレータIC、（4）USB-Cプロトコル制御IC。また、PSUから供給される6つの電源レールにおける消費電流を測定するための出力端子も搭載しており、これらはアナログ／デジタルコンバータに接続されます



Lithium ion battery charge state indicator LED

リチウムイオン電池充電状態表示用LED

PV panel state indicator LED

太陽光発電パネル状態表示LED

PV Panel Input Terminals

太陽光発電パネル入力端子

Lithium-ion battery charging/discharging port

リチウムイオン電池充放電口

Thermistor terminals for battery temperature measurement

電池温度測定用サーミスタ端子

USB-C Port Activity Indicator LEDs

USB-C端子状態表示用LED群

USB-C Port

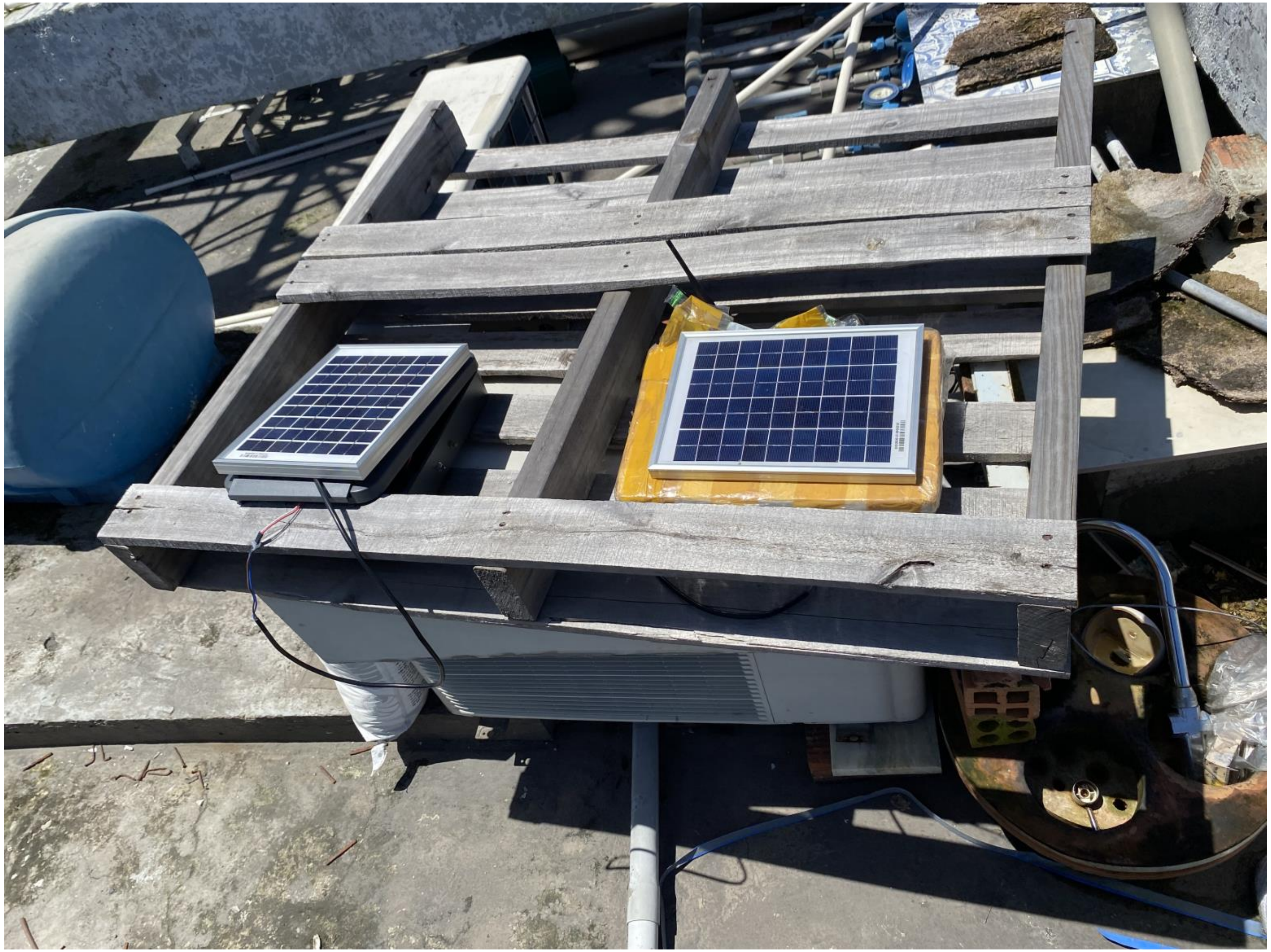
USB-C端子

Reset Button (Not a Usual System Reset as Critical States are Preserved)

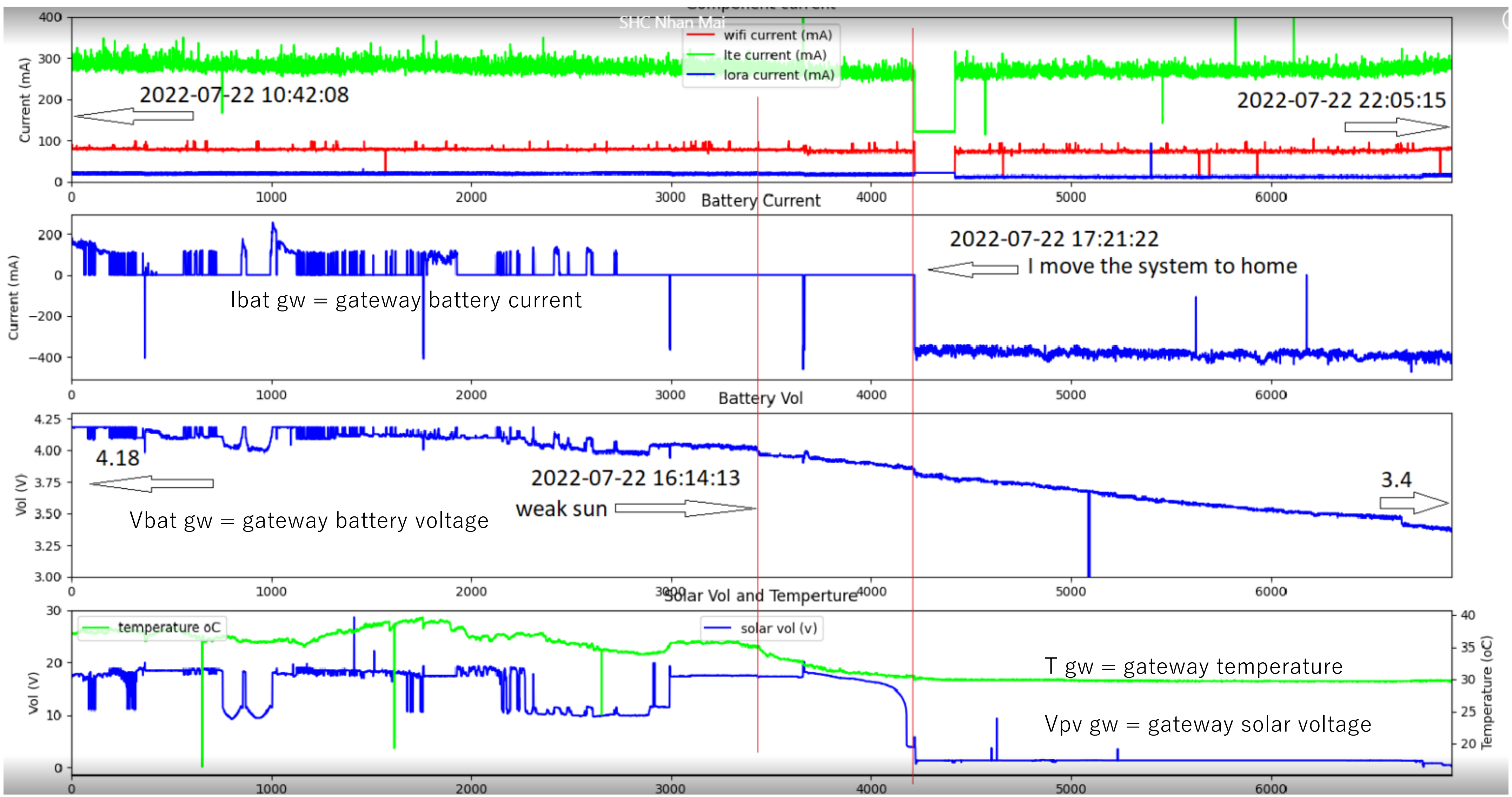
リセットボタン（通常のシステムリセットとは異なり、重要な状態は保持される。）

RISC-V 協会 ALLIANCE JAPAN

Implementation 2 (2022) ⇨ MARMOT SENSOR ENDPOINT (Right) and GATEWAY (Left)



MARMOT Gateway Current Consumption 2022/07/22



2022-07-22 10:42:08

2022-07-22 22:05:15

2022-07-22 17:21:22

I move the system to home

Ibat gw = gateway battery current

4.18

2022-07-22 16:14:13

weak sun

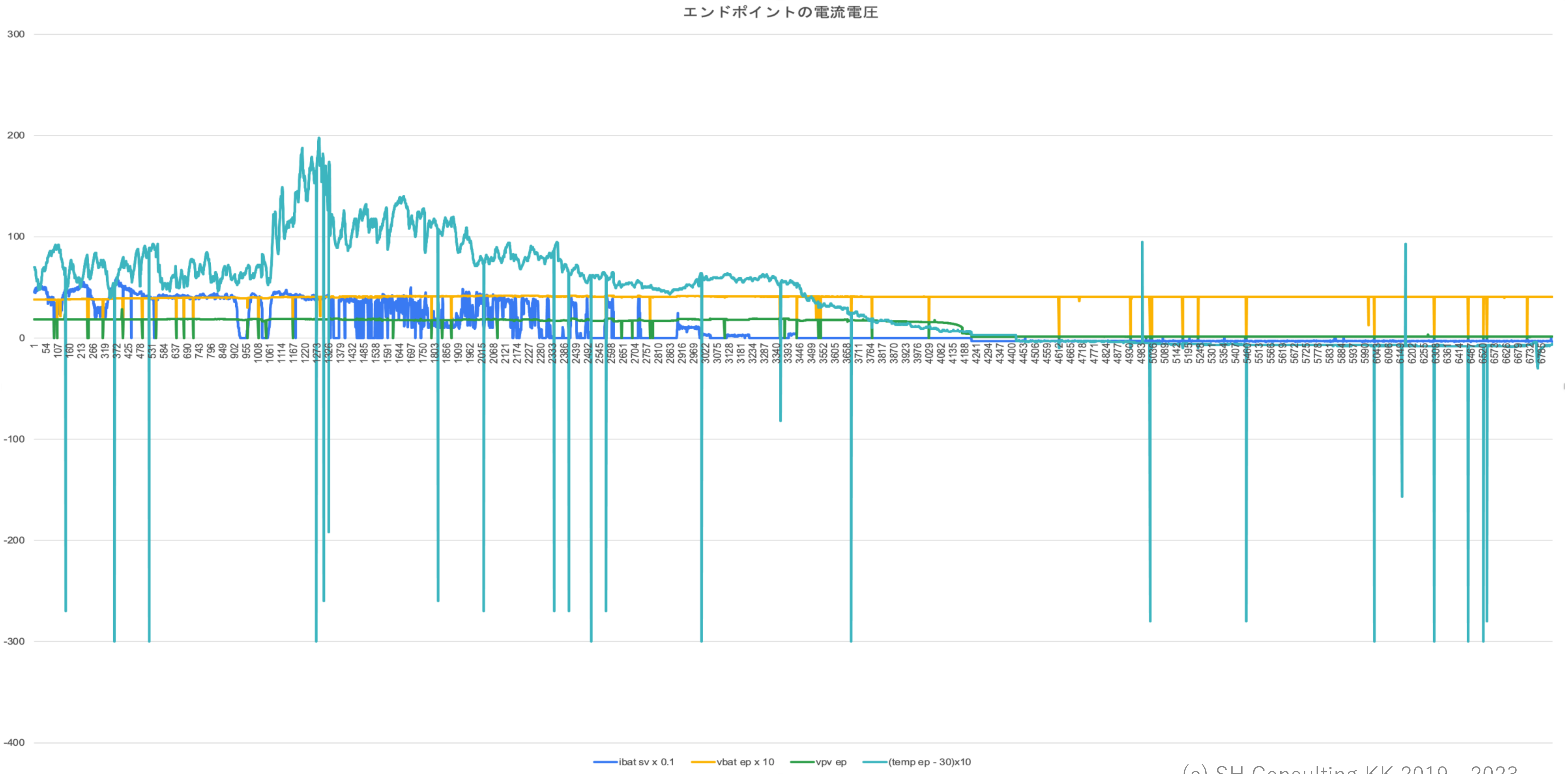
3.4

Vbat gw = gateway battery voltage

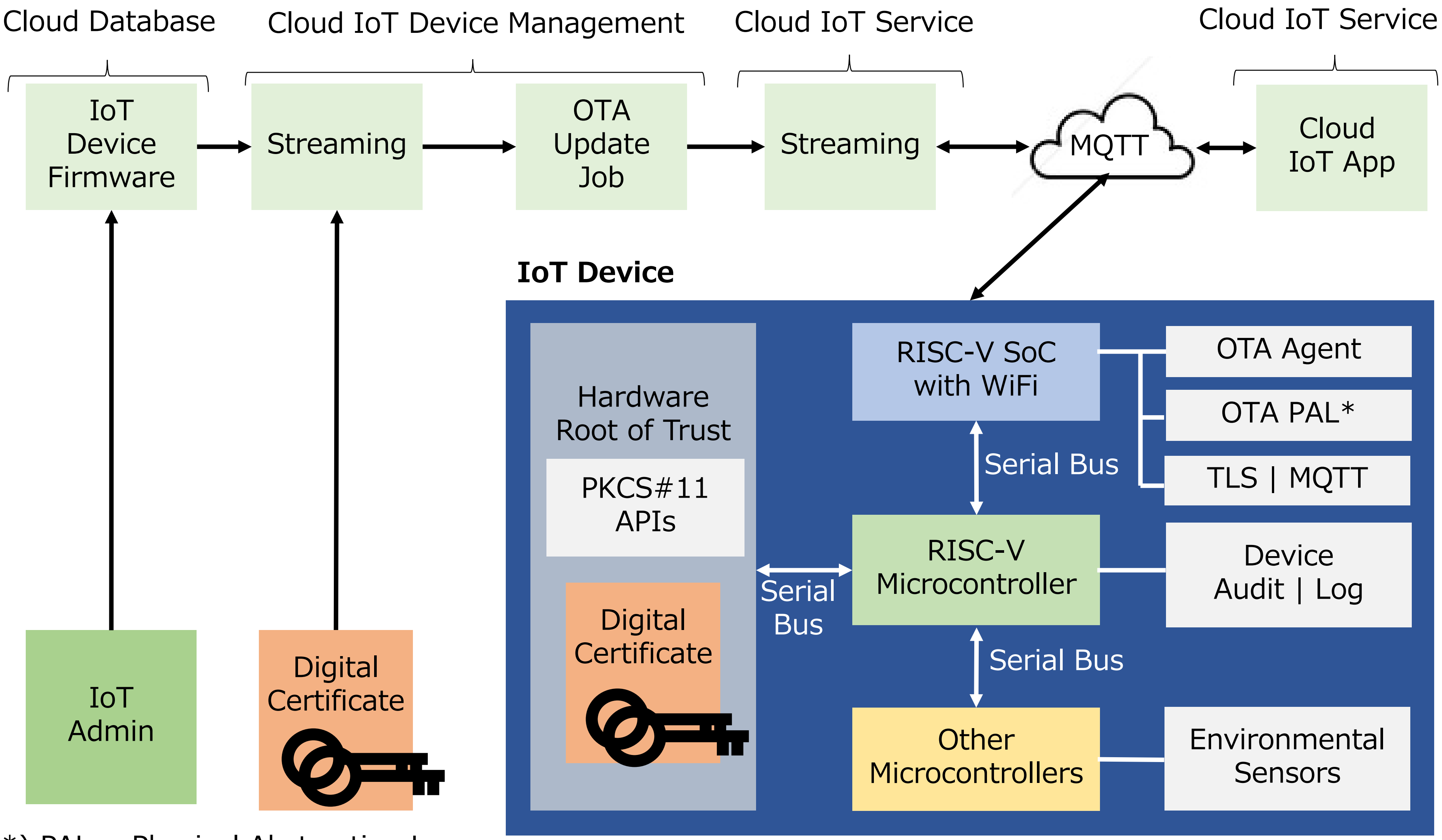
T gw = gateway temperature

Vpv gw = gateway solar voltage

MARMOT Endpoint Current Consumption 2022/07/22



Marmot AWS Remoto OTA Software Updade 2021



*) PAL = Physical Abstraction Layer

Statistics from FreeRTOS RISC-V Porting 2021

SHC ported FreeRTOS to RISC-V and calculated the required memory size for each.

① Secure connection to AWS using ATECC608A (commercially available secure MCU)

Flash: 219.5KB + size of the program body

RAM: 32.87KB is required.

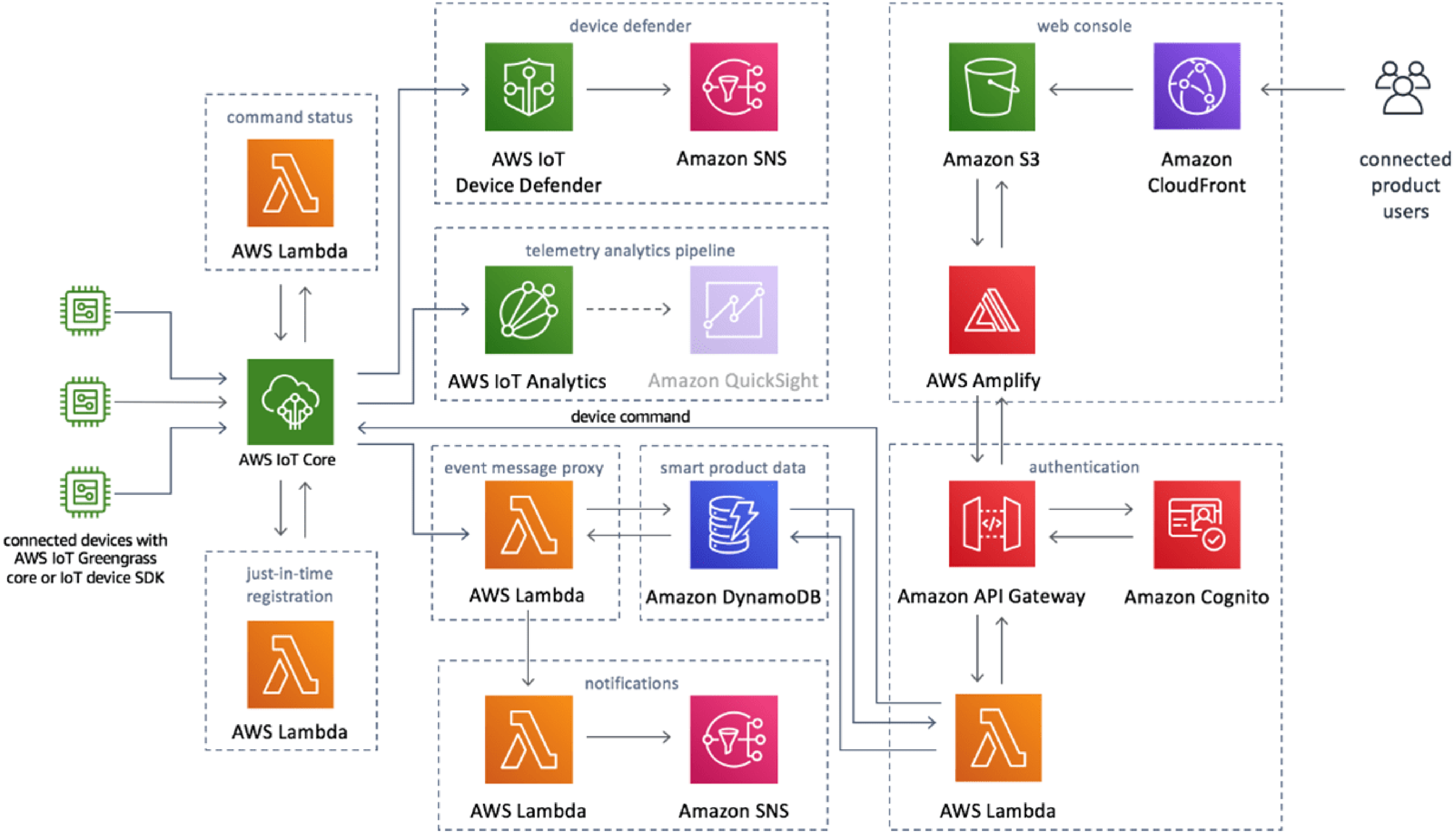
② OTA

Flash: 251.36KB + firmware size = minimum 500KB or more required

RAM: 36.07KB

Is necessary.

Relationship between AWS IoT, AWS IoT Core, and AWS cloud services



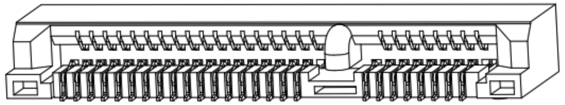
Concept 3 (2022) ⇨
Large capacity external memory support

SH CONSULTING

1 Configuration (# of Build)
5G Gateway | Endpoint (40)
utilizes Present PSU Units

*) Actuator / Sensor I/O
ADC, DAC, GPIO,
4-Channel Timer Comparator

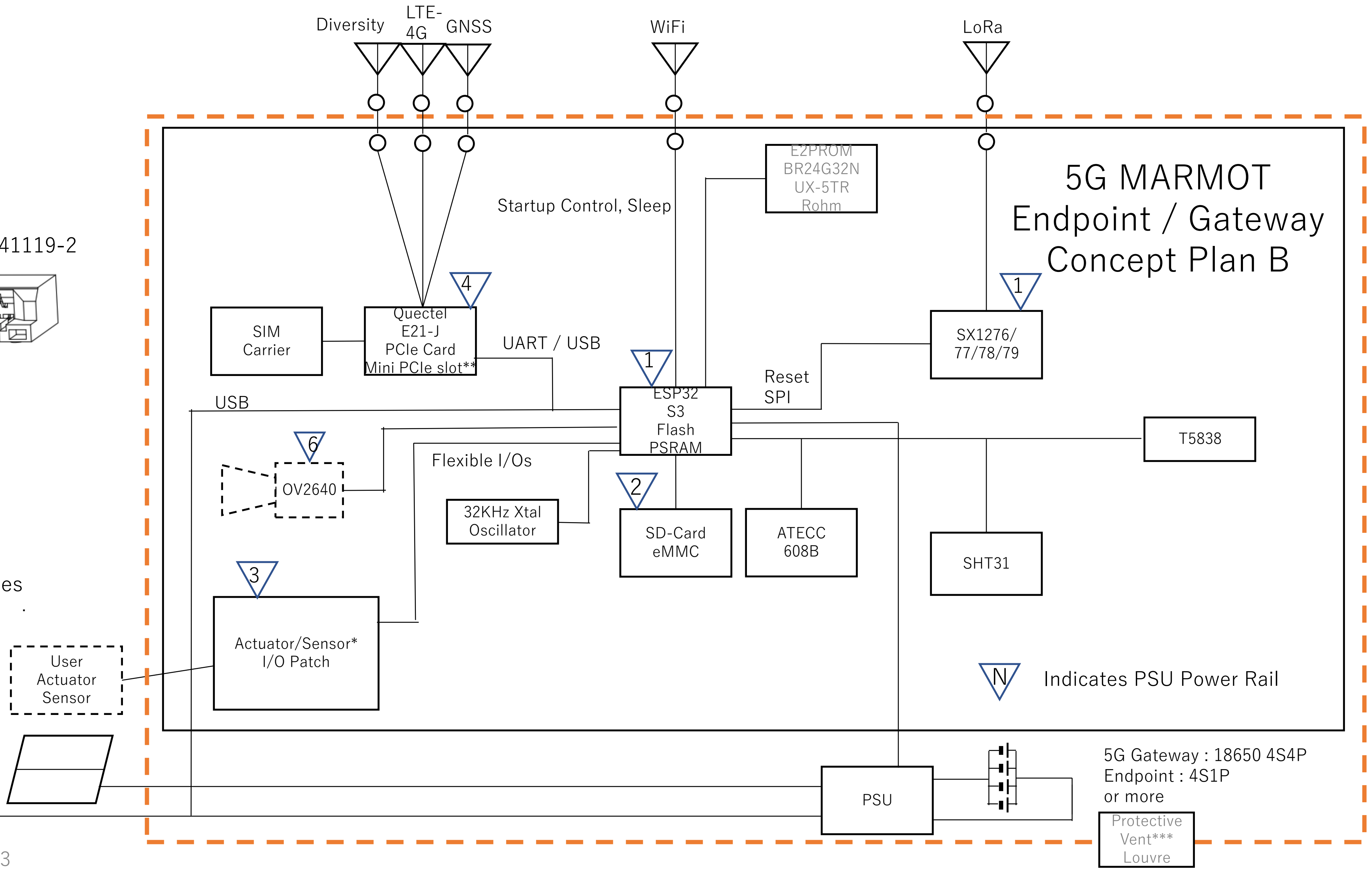
**) Mini PCIe Slot
TE Connectivity AMP Connectors 2041119-2



***) Takachi PMF-12HAB

***) Takachi Louver with hood V series
V60/V60S/V80/V80S

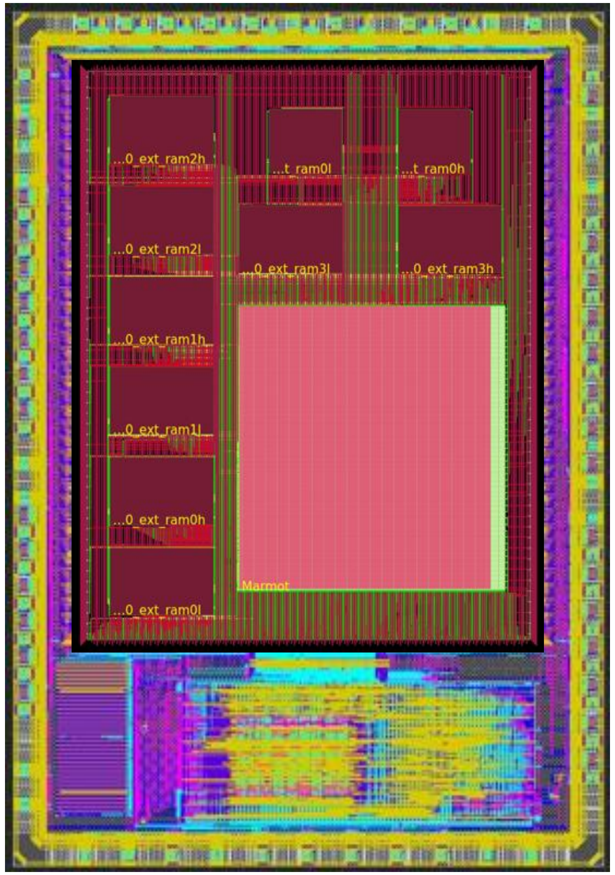
USB Power Adaptor
/ PC Used as LoRa Master / Host



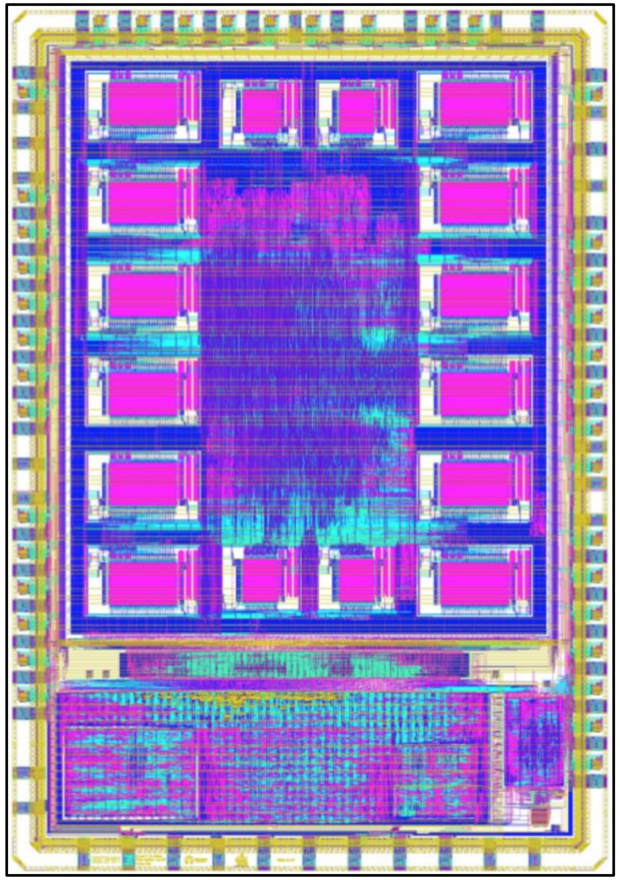
Utilization of open source technology

SH CONSULTING

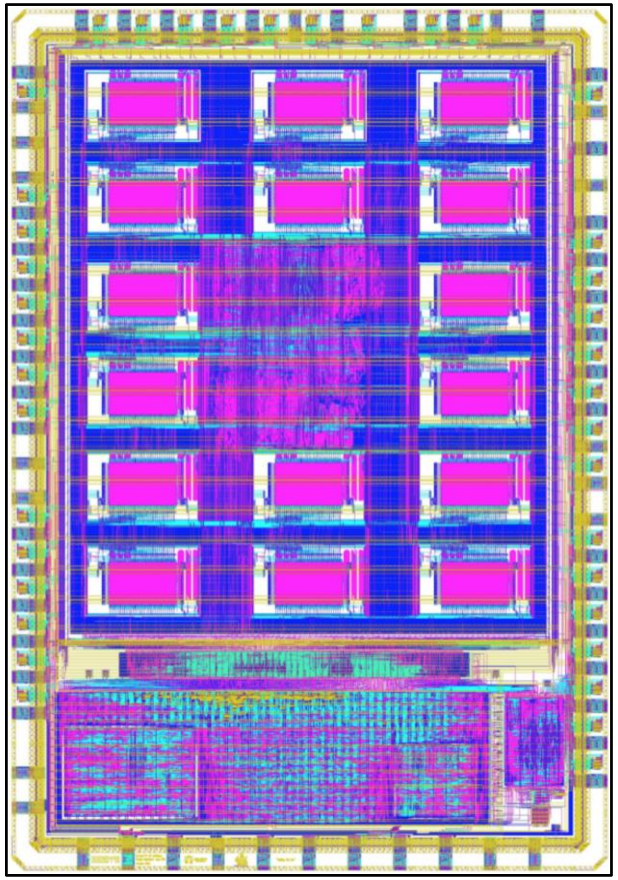
June 2022
MPW shuttle 6
Power management RISC-V



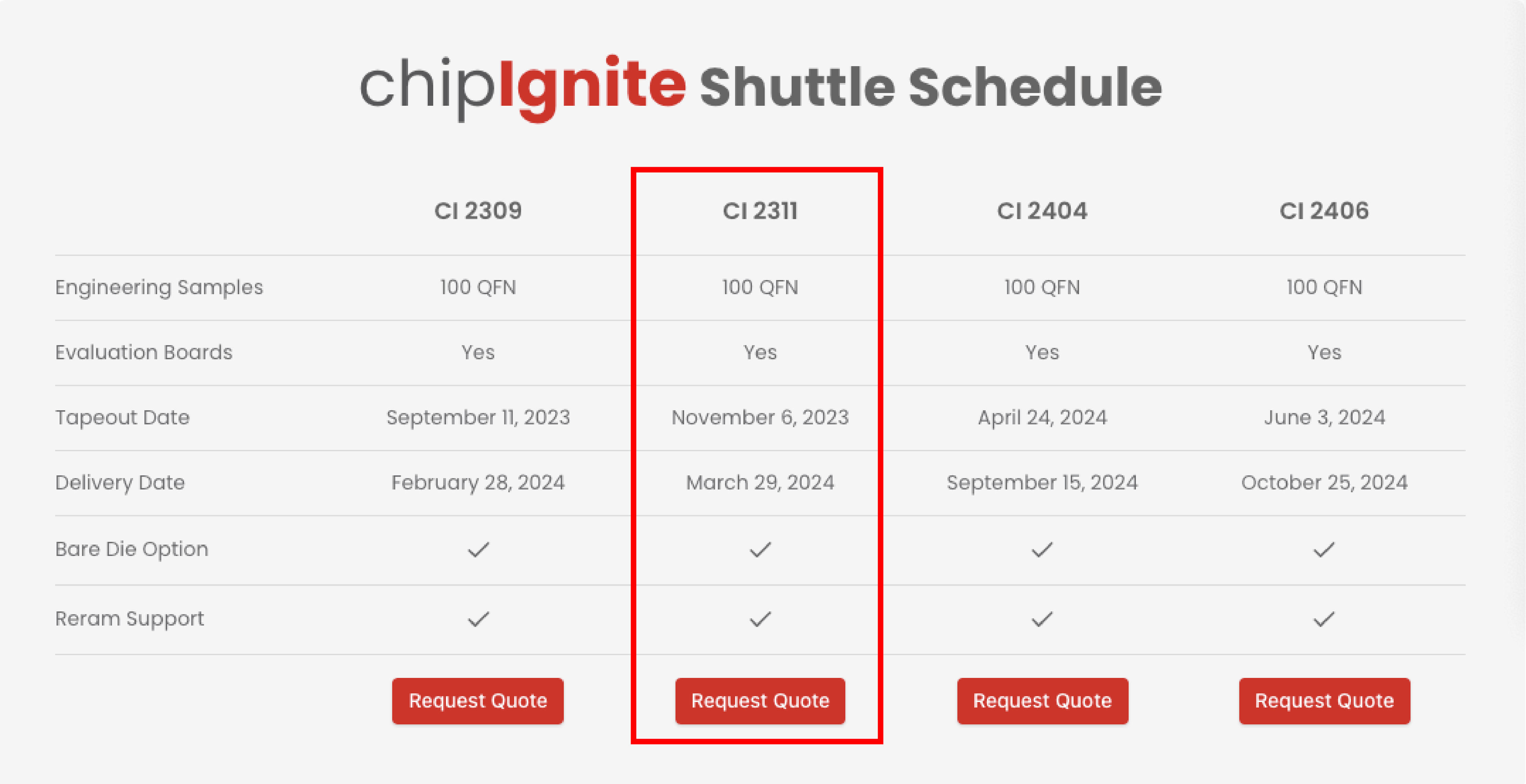
September 2022
MPW Shuttle 7
Power management RISC-V



December 2022
MPW Shuttle 8
Motor control SH2



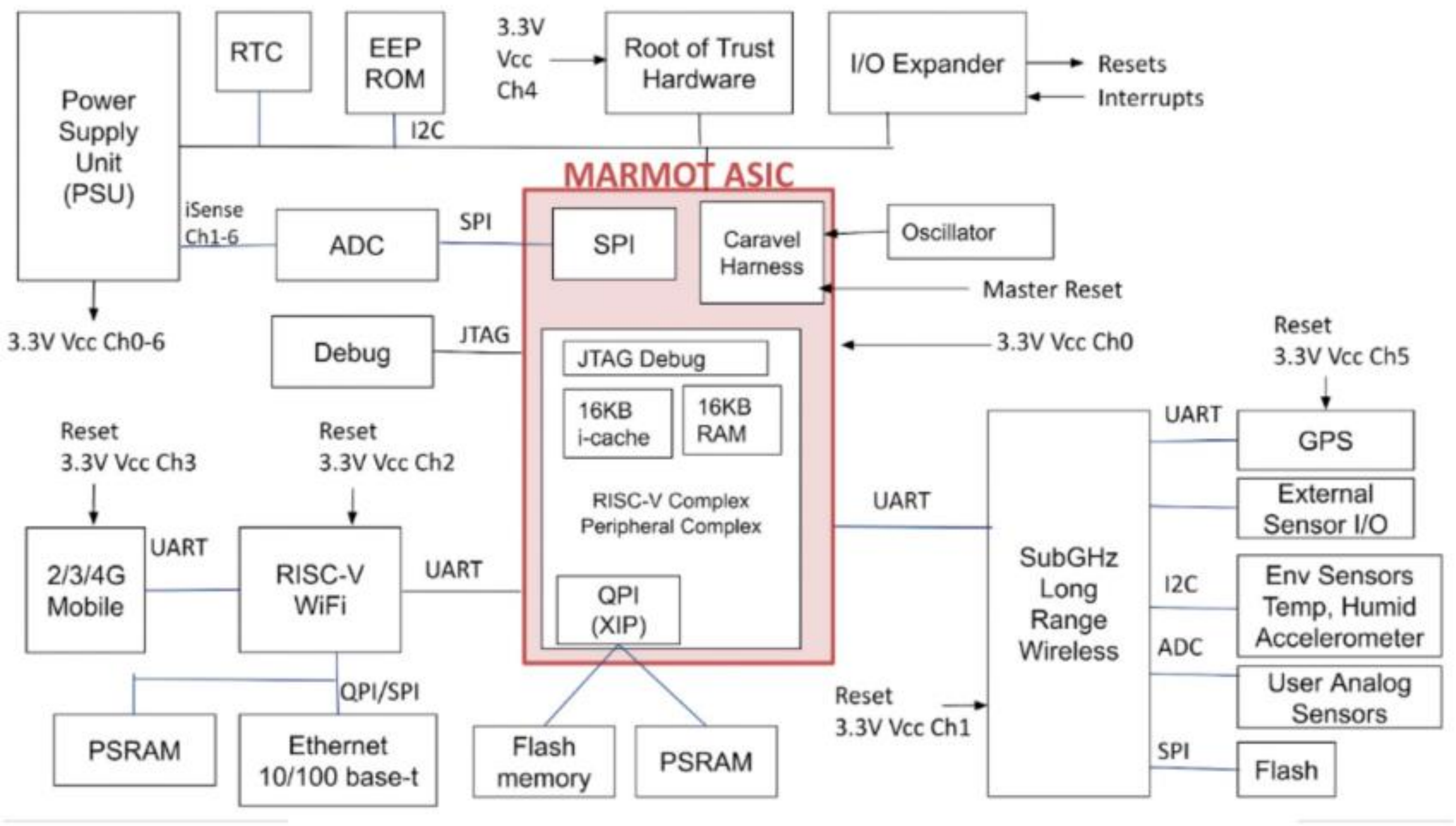
JASA chip manufacturing leveraging eFabless ChipIgnite



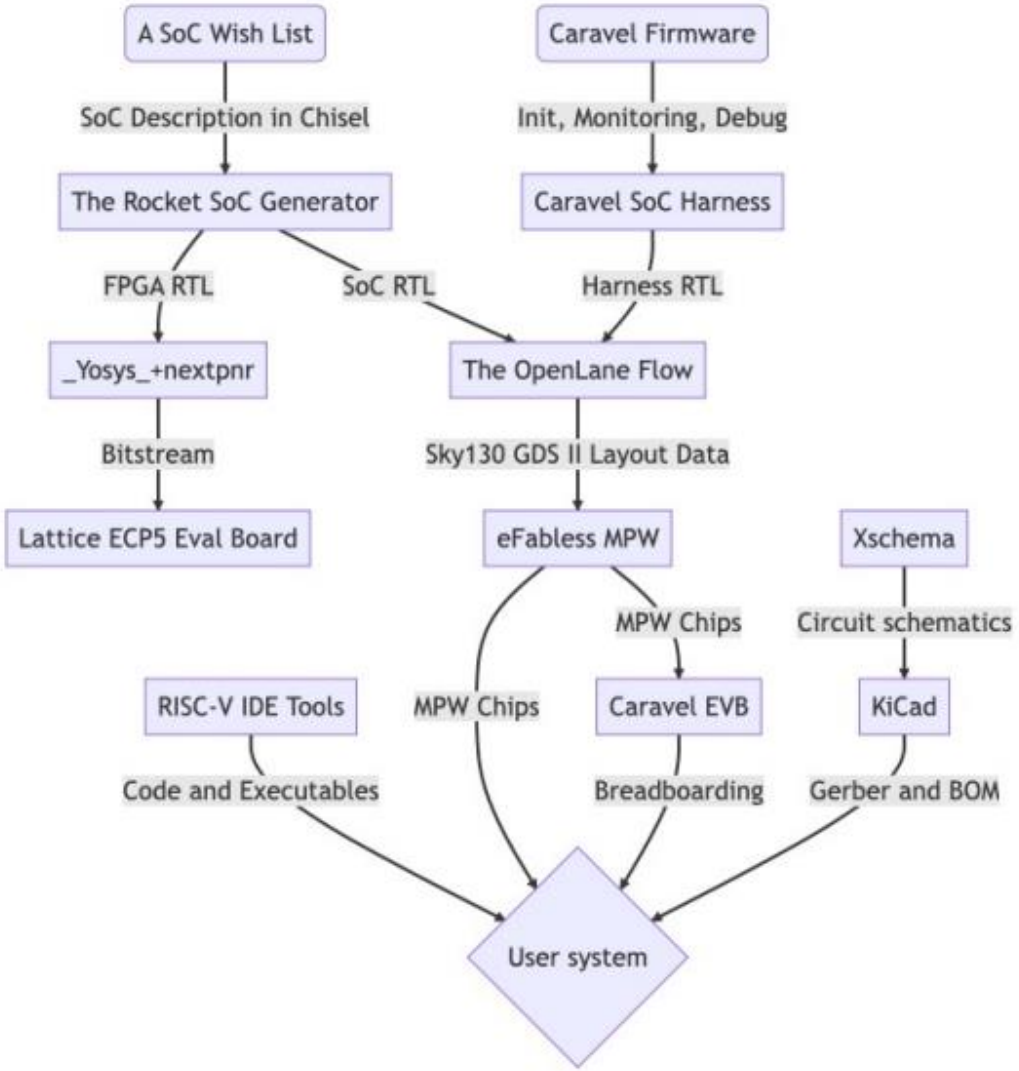
chipIgnite Shuttle Schedule

	CI 2309	CI 2311	CI 2404	CI 2406
Engineering Samples	100 QFN	100 QFN	100 QFN	100 QFN
Evaluation Boards	Yes	Yes	Yes	Yes
Tapeout Date	September 11, 2023	November 6, 2023	April 24, 2024	June 3, 2024
Delivery Date	February 28, 2024	March 29, 2024	September 15, 2024	October 25, 2024
Bare Die Option	✓	✓	✓	✓
Reram Support	✓	✓	✓	✓
	Request Quote	Request Quote	Request Quote	Request Quote

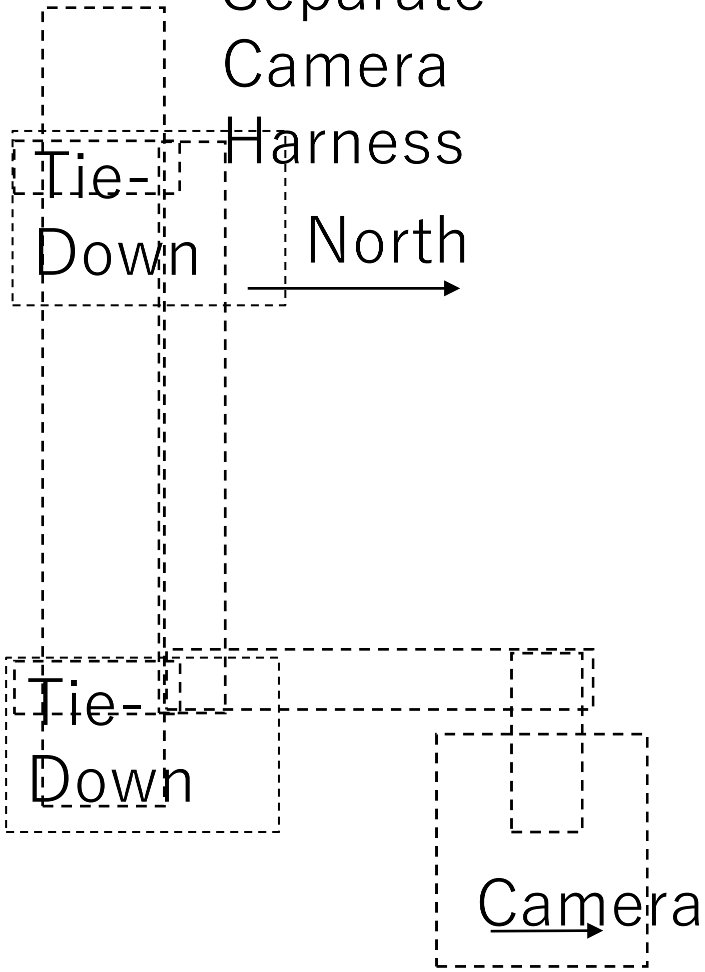
MARMOT chip spec



JASA chip design flow



Marmot Gateway device deployment example



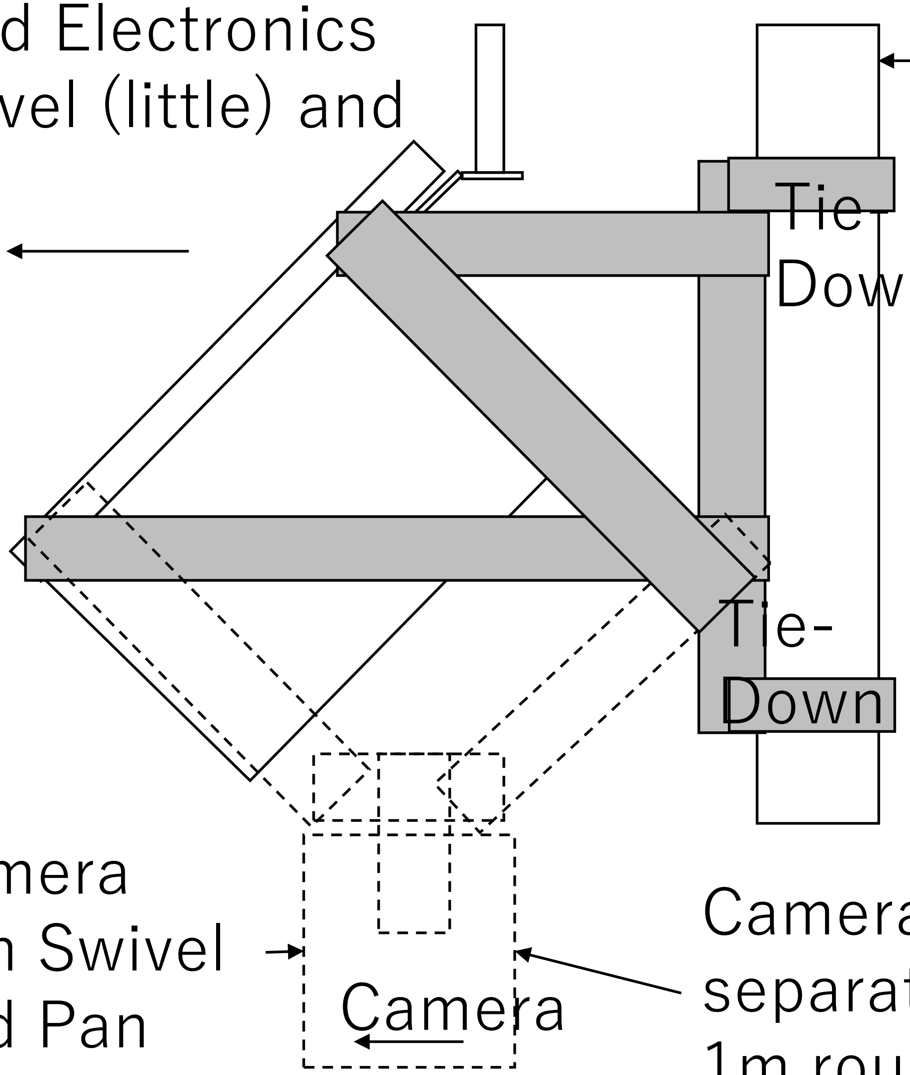
Separate Camera Harness

Tie-Down

North

Tie-Down

Camera



Solar and Electronics Can Swivel (little) and Pan

South

Round Pole

Tie-Down

North

The harness system can be also bolted down to a surface.

Tie-Down

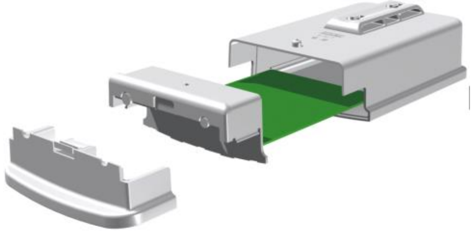
Camera Can Swivel And Pan

Camera

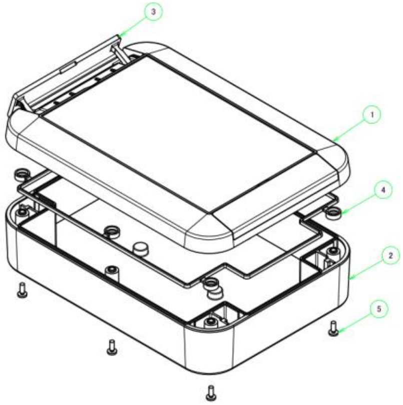
Camera can be separated by 1m round cord

MARMOT Endpoint deployment example

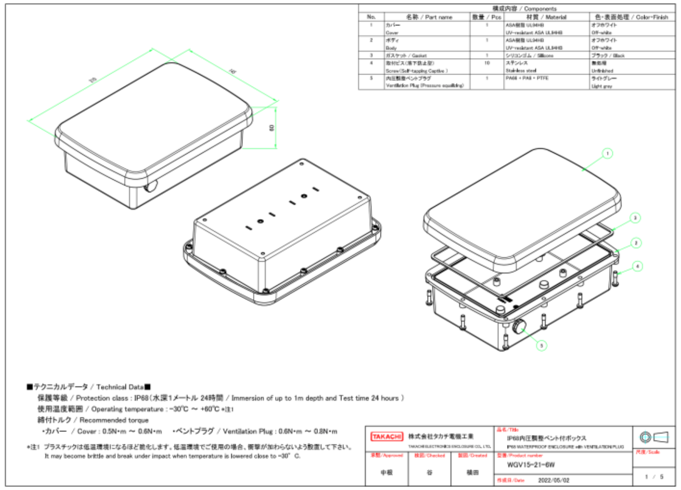
Enclosure A
OB13-21-6W



Enclosure B
WP15-21-6



Enclosure C
WGV15-21-6W



構成内容 / Components				
No.	名称 / Part name	数量 / Pcs	材質 / Material	色・表面処理 / Color・Finish
1	カバー Cover	1	ASA樹脂 UL94HB UV-resistant ASA UL94HB	オフホワイト Off-white
2	ボディ Body	1	ASA樹脂 UL94HB UV-resistant ASA UL94HB	オフホワイト Off-white
3	ガスケット / Gasket	1	シリコンゴム / Silicone	ブラック / Black

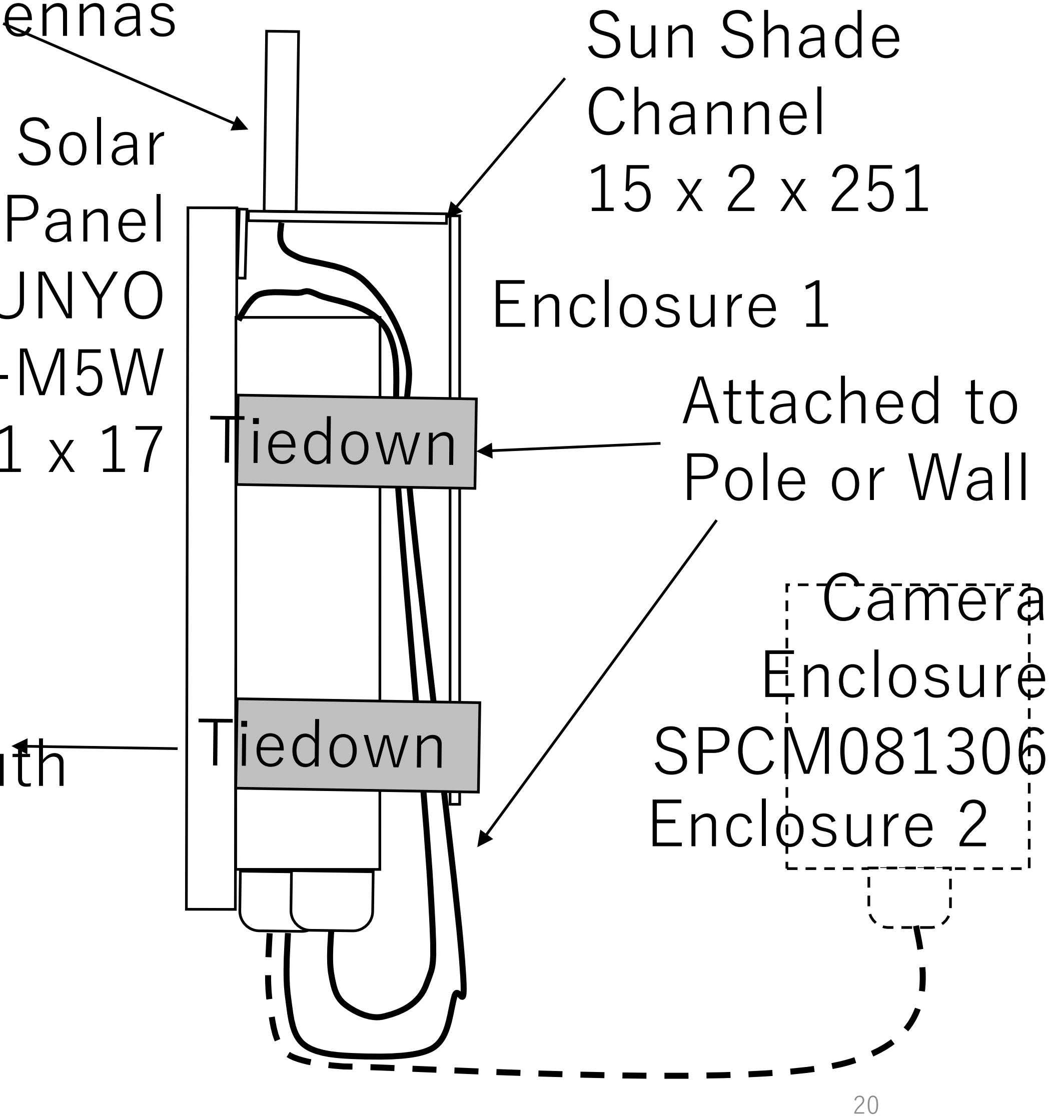
4	取付ビス(落下防止型)
	Screw(Self-tapping Captive)
		10	ステンレス
			Stainless steel
				無処理
				Unfinished

5	内圧調整ベントプラグ Ventilation Plug (Pressure equalizing)	1	PA66 + PA6 + PTFE	ライトグレー Light gray

■テクニカルデータ / Technical Data■
保護等級 / Protection class : IP68（水深1メートル 24時間 / Immersion of up to 1m depth and Test time 24 hours）
使用温度範囲 / Operating temperature : −30℃ ～ +60℃ *注1
締付トルク / Recommended torque
・カバー / Cover : 0.5N・m ～ 0.6N・m　・ベントプラグ / Ventilation Plug : 0.6N・m ～ 0.8N・m

*注1 プラスチックは低温環境になるほど脆化します。低温環境でご使用の場合、衝撃が加わらないよう設置して下さい。
It may become brittle and break under impact when temperature is lowered close to −30° C.

TAKACHI 株式会社タカチ電機工業 TAKACHI ELECTRONICS ENCLOSURE CO., LTD.			品名/Title IP68内圧調整ベント付ボックス IP68 WATERPROOF ENCLOSURE with VENTILATION PLUG	尺度/Scale
承認/Approved 中根	検図/Checked 谷	製図/Created 横田	型番/Product number WGV15-21-6W 作成日/Date 2022/05/02	1 / 5



7 Antennas

Antenna Holder /
Sun Shade
Channel
15 x 2 x 251

Solar
Panel
SUNYO
SY-M5W
185 x 251 x 17

Enclosure 1

Tiedown

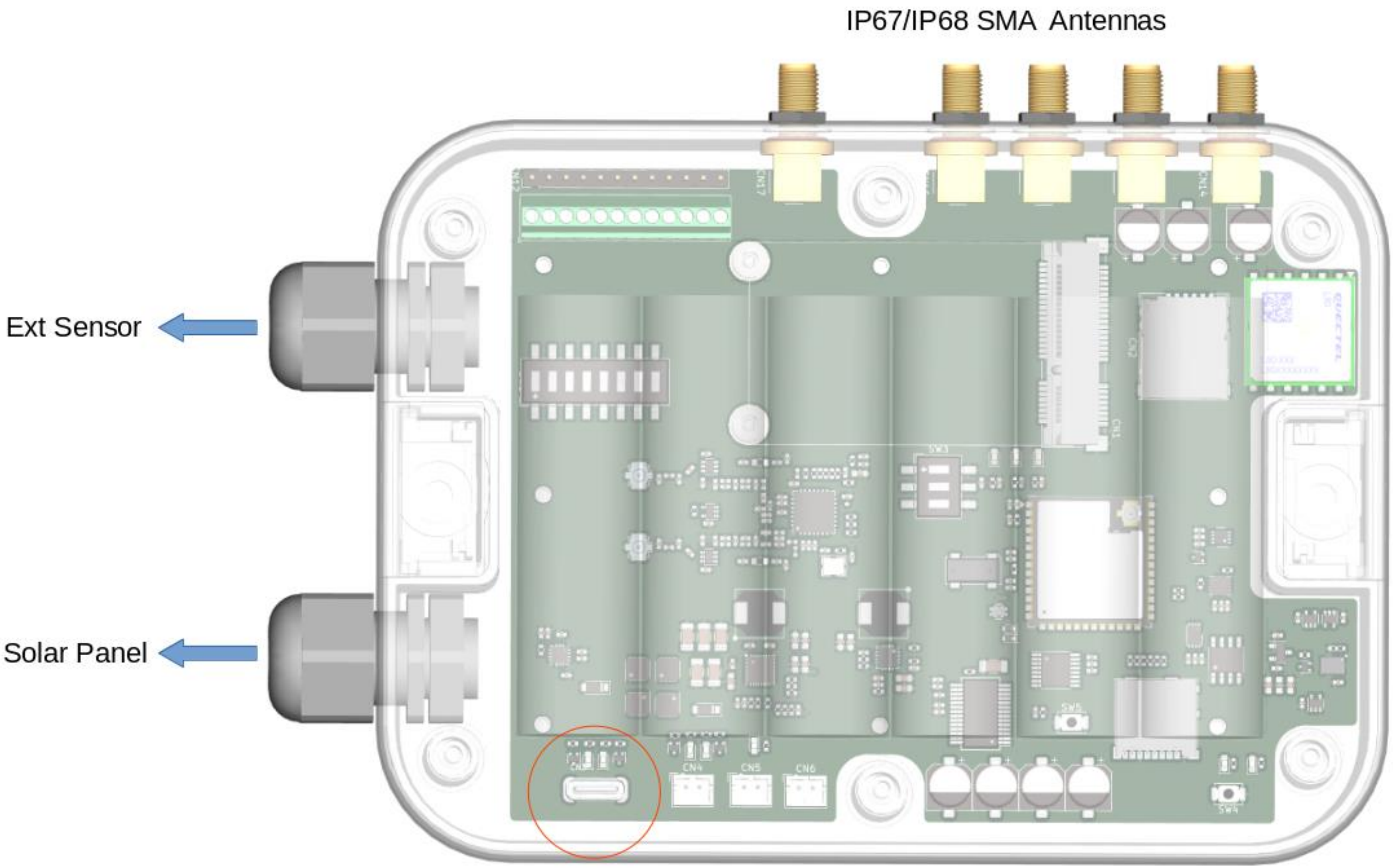
Attached to
Pole or Wall

Camera
Enclosure
SPCM081306
Enclosure 2

South

Tiedown

MARMOT Gateway ｜ Endpoint device

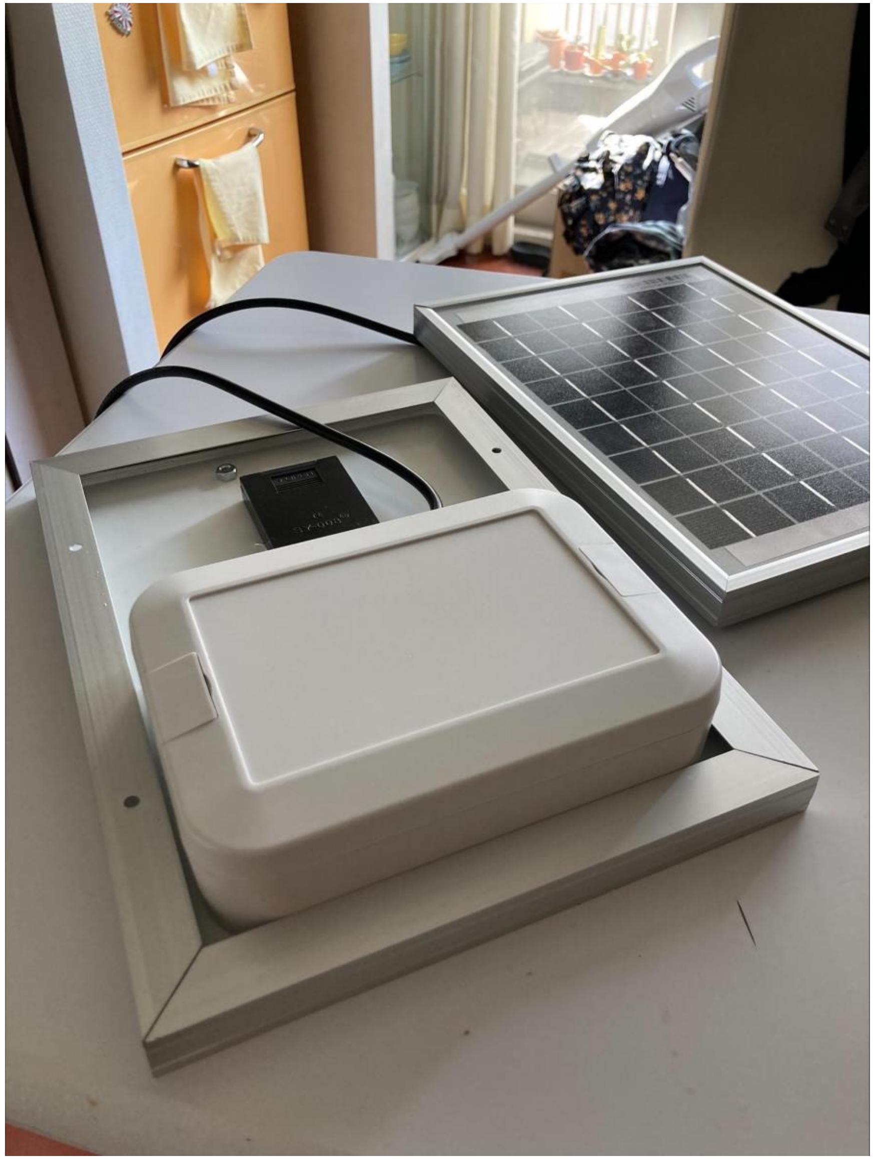


IP67/IP68 SMA Antennas

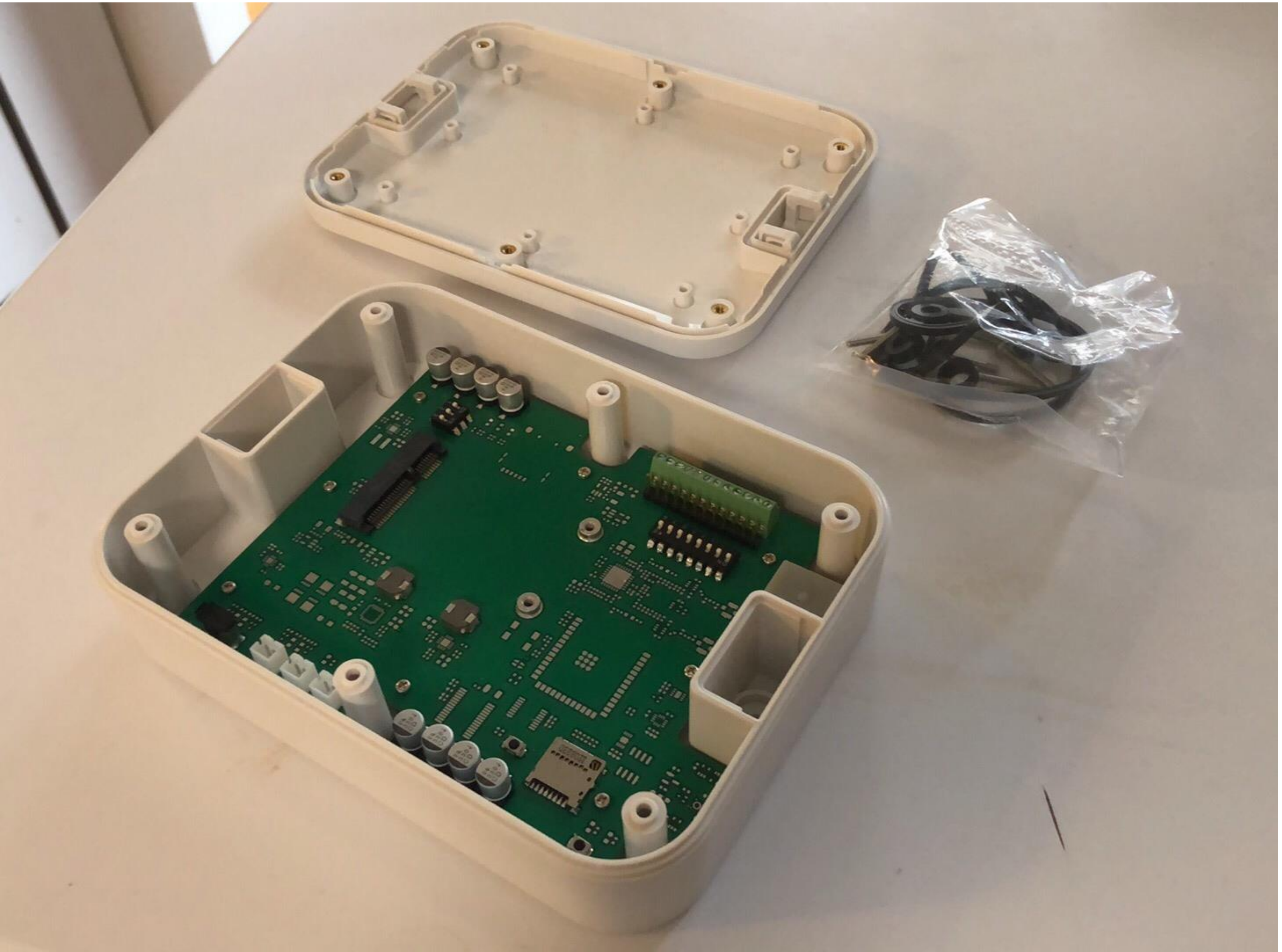
Ext Sensor

Solar Panel

MARMOT Gateway | Endpoint
Solar Panel integration

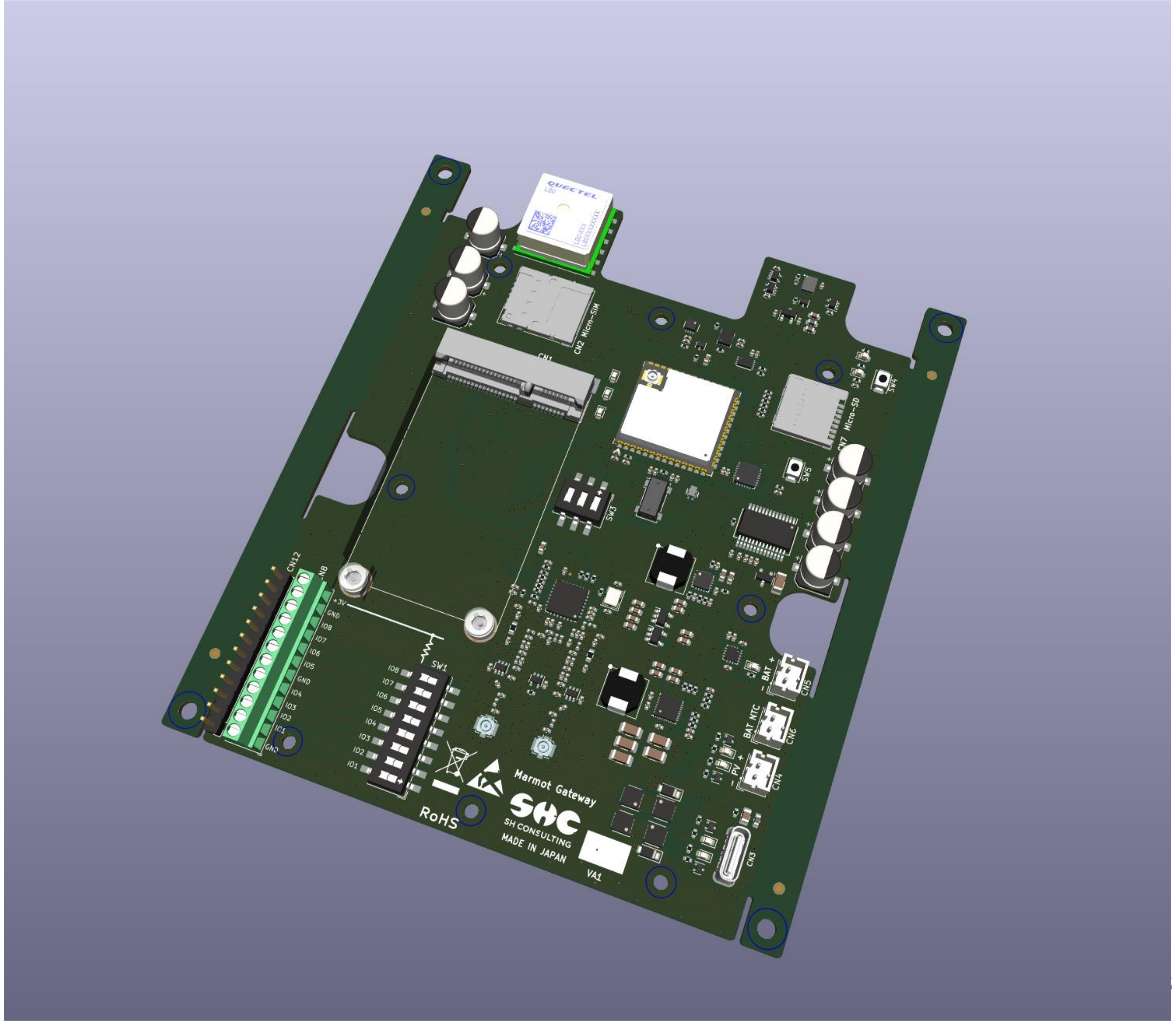


MARMOT Gateway ｜Endpoint
1 board + case assembly



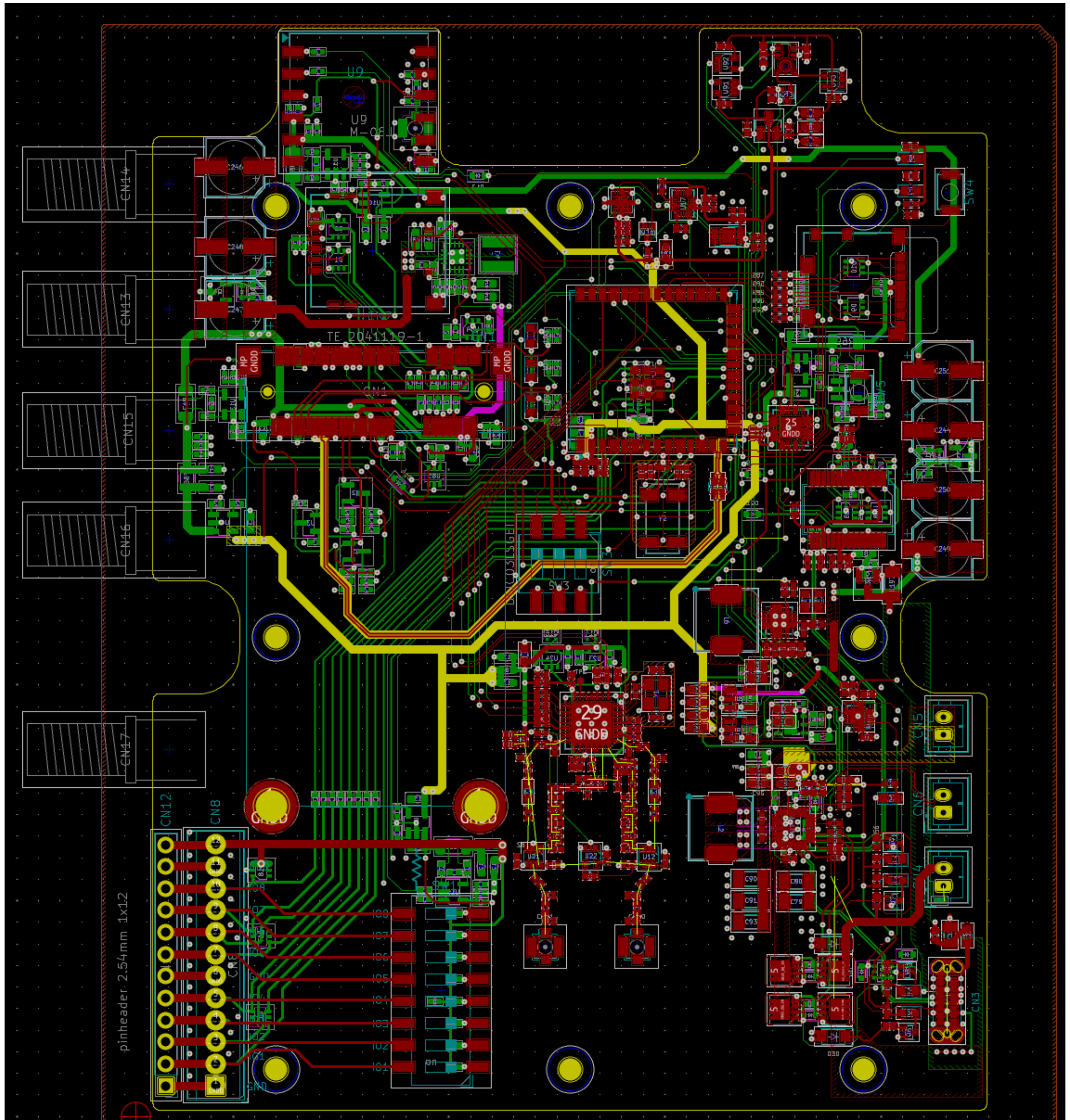
Case specifications
Takachi Electric Industry Co., Ltd.
WP11-15-4
IP68 waterproof box
IP NETWORK PLASTIC BOX
Standard price 1000 yen
Vent + Groud processing scheduled

MARMOT Gateway ｜ Endpoint 1 board solution



1枚基盤コスト ＝
LTE 無線モジュール＋
ESP32 無線モジュール＋
LoRa 1 piece base cost =
LTE wireless module +
ESP32 wireless module +
LoRa wireless module +
GPS wireless module +
10～15 USD BOM +
Board + Assembly
We are currently estimating the first lot of 5 pieces in Japan.

Single board layout floorplan



- Power control, communication, and processing are integrated in 1 board.
- When we measured operating current, power consumed by the wireless communication modules are dominant. Internal MCU power consumption is not dominant.
- The network, wireless protocols, and security software stack is large and convoluted.
- Initial schemes to reduce operating power partially power was not very effective.
- The design was done using KICAD.

Comparison of IoT cloud services

- AWS IoT:
  - IoT Core: Easy device connectivity to the cloud
  - IoT Device Defender: Security auditing and monitoring of IoT configurations
  - IoT Analytics: Analyzing IoT data
  - IoT Greengrass: Run Lambda functions locally and send MQTT messages on devices
- Azure IoT:
  - IoT Hub: Provides bidirectional communication between IoT applications and their managed devices
  - IoT Central: A SaaS solution to connect, monitor, and manage IoT assets
  - IoT Edge: Executing cloud intelligence directly on IoT devices
- Google Cloud IoT:
  - IoT Core: A managed service that connects, manages, and ingests data from devices.
  - Edge IoT: Edge computing functions running on Android Things and Cloud IoT Edge

Comparison of IoT cloud services: Integration of cloud service

- AWS IoT: Powerful integration with other AWS services such as Lambda, SageMaker, and Kinesis.
- Azure IoT: Seamless integration with other Azure services such as Azure Functions, Azure Stream Analytics, and Azure Machine Learning.
- Google Cloud IoT: Can be integrated with other Google Cloud services such as Pub/Sub, Dataflow, and AI Platform.

主要IoTサービス比較: 開発ツール

- **AWS IoT**: AWS IoT Device SDKを提供。
- **Azure IoT**: 複数の言語でのSDK提供。Azure IoT Workbenchツールもサポート。
- **Google Cloud IoT**: Cloud IoT Device SDKを提供。

Components of Azure Sphere

- Azure Sphere MCUs (Microcontroller Units): Custom chips developed by Microsoft's hardware partners based on Microsoft specifications. MCUs constitute real-time and application processors with embedded network connectivity. Contains security technology configured by Microsoft to provide ROT of on-chip hardware.
- Azure Sphere OS: An operating system designed specifically for IoT applications. A customizedversion of Linux built by Microsoft to provide multiple layers of security. Azure Sphere OS consists of a custom Linux kernel, a hardware abstraction layer, and a set of security services that provide a secure software environment for applications.
- Azure Sphere Security Service: Cloud-based service performs device-to-device and device-to-cloud communication. Certificate-based authentication is used, and only authenticated devices can connect to Azure Sphere services. Detect new threats and push OS and app updates to devices.

Azure Sphere features and benefits

A project from Microsoft, it sets IoT security standards and ensures that devices are secure by default and remain secure throughout their lifecycle.

- End-to-end security: Azure Sphere provides security at every layer from hardware to OS to cloud.
- Over Air Updates (OTA): Azure Sphere supports OTA updates. Security patches and application updates can be pushed remote devices.
- App development: Developers can use Visual Studio to create applications for Azure Sphere and leverage Azure services e.g. analytics and databases.
- Secure device authentication: Azure Sphere devices use certificate-based authentication to ensure secure communication with the cloud.
- Continuous security improvements: Devices benefit from continuous security improvements, threat detection, and security notifications.

Azure Sphere MCUs
(Azure Sphere Microcontroller Unit)

- Azure Sphere MCUs are manufactured to MS specifications. The company is partnering with semiconductor companies to manufacture custom chips. Partners producing Azure Sphere MCUs include:
- MediaTek: MT3620 was the first Azure Sphere certified MCU. It integrates an ARM Cortex-A7 application processor, an ARM Cortex-M4 I/O subsystem, and provides built-in support for Wi-Fi.
- NXP Semiconductors: NXP is working with Microsoft to make its i.MX 8 series chips compatible with Azure Sphere. Designed for graphics, machine learning, and various IoT apps.
- Qualcomm: Announced collaboration with Microsoft on Azure Sphere. The company aims to produce cellular-connected MCU solutions. It facilitates IoT devices that require cellular connectivity, such as in remote areas.

AWS IoT Core Overview (Introduction)

AWS IoT Core is a service for people looking to build IoT on the AWS platform. Process and route large numbers of devices and real-time communication messages to AWS endpoints and other devices.

- Connectivity: Supports HTTP, WebSockets, and MQTT, a lightweight communication protocol designed specifically for low-bandwidth connected devices. It also supports MQTT over WebSockets protocol.
- Security: Provides mutual authentication and encryption at all points of connection, so no data is exchanged between your device and AWS IoT Core without verification and authentication. Use X.509 certificates for authentication.
- Device Registry: There is a device registry to track devices connected to your app. Organize devices, manage metadata, and quickly search and navigate device lists.
- Device Shadow: A JSON document for storing and retrieving current state information of a device. Allows apps to interact with offline devices.

AWS IoT Core Overview (continued)

- Rules Engine: Provides message processing and integration with other AWS services. It can evaluate incoming messages published to AWS IoT Core and transform and deliver them to another device or cloud service based on defined business rules.

- Integration with AWS Services: AWS IoT Core integrates with other AWS services to enable actions such as writing data to Amazon DynamoDB, invoking Lambda functions, or sending data to Amazon Kinesis.

- SDK: AWS provides a software development kit (SDK) for embedding AWS IoT Core functionality into your devices. These SDKs make it easy for devices to connect, authenticate, and exchange messages with AWS IoT Core.

AWS IoT CoreSecurity

IoT devices will increase and be integrated into work. AWS IoT Core's security mechanisms provide the robustness to ensuring a secure IoT ecosystem.

- Mutual Authentication: Supports mutual authentication where the server and device confirm each other's identity. No data is exchanged between the device and AWS IoT Core without a verified identity. For this purpose, devices use X.509 certificates. AWS IoT Core allows you to create, deploy, and manage these certificates.
- Encryption: All data sent between your device and AWS IoT Core is encrypted using Transport Layer Security (TLS). It also provides encryption for stored data.
- Authentication: Fine-grained authorization is performed using AWS Identity and Access Management (IAM). User can set policies to determine what devices and users can do (e.g. publish or subscribe to topics).
- Root of Trust (RoT): RoT is a trusted function within a computer that is always trusted by the device's operating system. AWS IoT Core works with AWS IoT Device Defender to help device manufacturers establish security by implementing a hardware root of trust on their devices.

SH CONSULTING

AWS IoT Core Security (continued)

- Device Shadow: Uses a JSON document called a “device shadow” to store and retrieve the current state of a device. This acts as a reliable intermediary between the app and the device, even when the device is temporarily unreachable.
- AWS IoT Device Defender: AWS IoT Device Defender allows for continuous auditing of IoT configurations. Monitor IoT device activity and identify anomalies and potential security breaches.
- Diverse device support: Support a wide variety of devices, from constrained devices (such as simple sensors) to computationally capable edge devices.
- Secure device onboarding: AWS IoT Core provides secure and scalable device onboarding without manually provisioning each device.
- Over-the-Air (OTA) updates: Supports OTA updates when combined with AWS IoT Device Management.

Microchip RoT (Root of Trust) integration on AWS IoT Core

- Secure Element: A secure element chip, such as Microchip's ATECC608A, is a cryptographic device that stores private keys in a protected hardware environment. The chip is designed to keep private keys used in cryptographic operations safe from physical and software-based attacks.

- Provisioning: Microchip's secure provisioning solutions help IoT devices securely and uniquely identify themselves in the cloud. ATECC608A's Trust Platform provides devices pre-provisioned with unique keys and certificates, allowing devices to be securely authenticated by AWS IoT Core from the moment they are taken out of the box.

- End-to-end security: Integrating Microchip's Secure Element chip with AWS IoT Core creates an end-to-end secure connection. Private keys stored in the secure element are used in TLS secure sessions with AWS IoT Core to ensure data confidentiality between IoT devices and the cloud.

Microchip’s RoT (Root of Trust) integration on AWS IoT Core (continued)

- Mutual Authentication: Mutual authentication is achieved with a private key securely stored on Microchip's RoT device and a corresponding certificate registered with AWS IoT Core. This not only verifies the device by the cloud, but the device also verifies the authenticity of the AWS IoT endpoint.

- Integration with AWS IoT SDK: Microchip provides software libraries and integrations that make it easy to work with AWS IoT Core. By combining the AWS IoT SDK with libraries provided by Microchip, developers can accelerate the deployment of secure IoT applications.

- Lifecycle Management: The combination of Microchip's RoT solution and AWS IoT Core provides secure device lifecycle management to ensure devices are safe from manufacturing, provisioning, deployment, and finally decommissioning.