Ngày RISC-V Việt Nam 2022
RISC-V Days Vietnam 2022

Root of Trust and OTA Software Upgrade for RISC-V RTOS IoT

Root of Trust và nâng cấp chương trình cho Hệ thống RISC-V RTOS qua mạng

Ngày 15 tháng 1 năm 2022
Hoan Huynh* and Shumpei Kawasaki**
*CÔNG TY TNHH SH CONSULTING VIỆT NAM
**SH Consulting K.K.

January 15, 2022
Hoan Huynh* and Shumpei Kawasaki**
* SH Consulting Vietnam Company Limited
**SH Consulting K.K. (Japan)

(c) SH Consulting KK 2019 2020 2021 2022

Agenda | Chương trình hôm nay

1. Introduction | Giới thiệu
2. Lightweight IoT in 2016 | IoT nhỏ gọn 2016
3. Bridge Structural Health Monitoring | Giám sát sức khỏe kết cấu cầu
4. Hardware Security | Bảo mật phần cứng
    1. What is Root of Trust Chip? | Root of Trust Chip là gì?
    2. Remote IoT Software Hardware Authenticity Proof | Bằng chứng xác thực phần cứng phần cứng IoT từ xa
5. Software Security | BẢO MẬT PHẦN MỀM
    1. Root of Trust Chip | Root of Trust
    2. OTA Software Update | Cập nhật phần mềm OTA
6. OTA Software Update Demo | Trình diễn cập nhật phần mềm bằng OTA
7. Future Directions and Summary | Định hướng dẫn trong tương lai và Tóm tắt

English — Shumpei

Vietnamese — Hoan

1. INTRODUCTION

1. GIỚI THIỆU

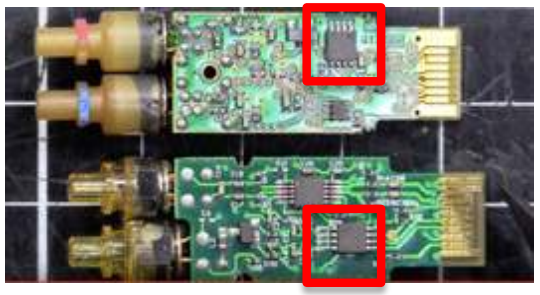
SH Consulting Backgrounds

Past Experience | Kinh nghiệm trong quá khứ của chúng tôi

Embedded Software and Hardware, Development Tools,

Flash MCU Chips, Video Games, Java Card™

Secure MCU Firmware, FIPS140 Certification



Wireless IoT | IoT không dây

2013 SH Consulting K.K.

2014 SH Consulting Vietnam Company Limited

2016 Lightweight Wireless IoT Product

2019 Integration of RISC-V, FreeRTOS Root of Trust

2021 Bridge Structural Health Analysis etc.

(c) SH Consulting KK 2019 2020 2021 2022

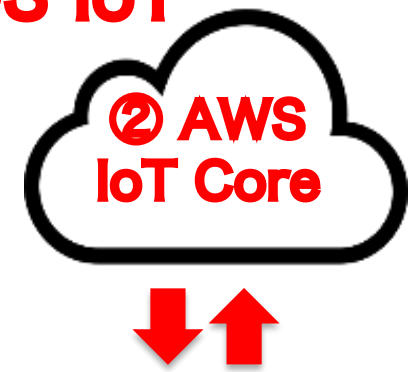
①Linux IoT vs. ②RTOS IoT

AI etc.

Remote Firmware Update (OTA)

① Linux IoT		
Linux	**64-bit CPU MMU**	>1GB Flash
Root of Trust RoT Chip	>64GB SSD Storage	>4GB DRAM

Power Consumption = 5W ~ **50W**

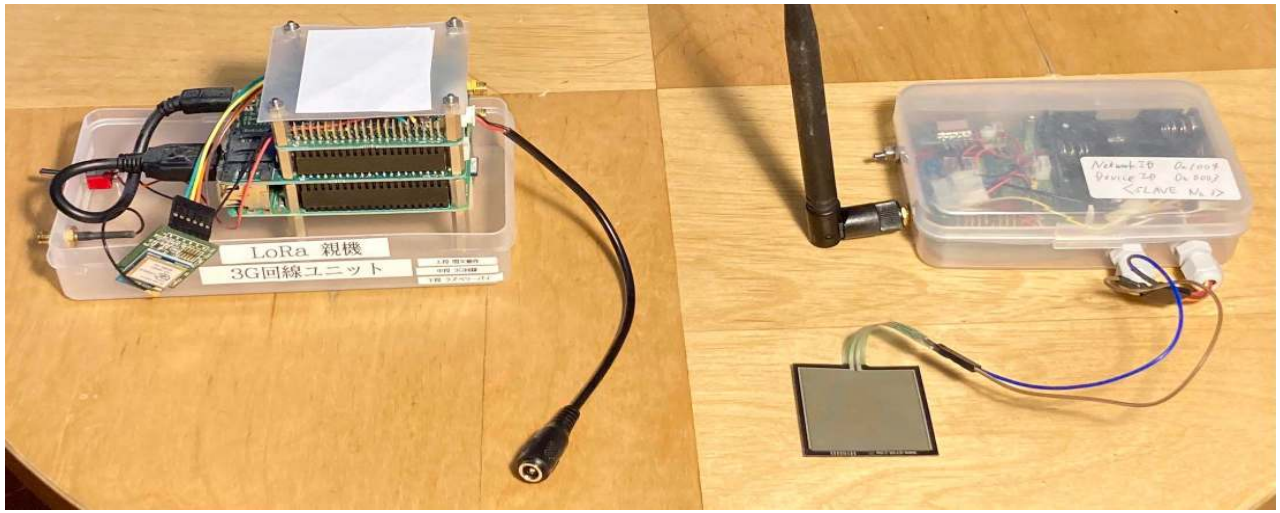


Sensor Actuator Data

Remote Firmware Update (OTA)

② RTOS IoT		
Realtime OS (RTOS)	**32-bit CPU No MMU**	>128KB Flash
Root of Trust RoT Chip	>1MB QPI Flash	>64KB RAM

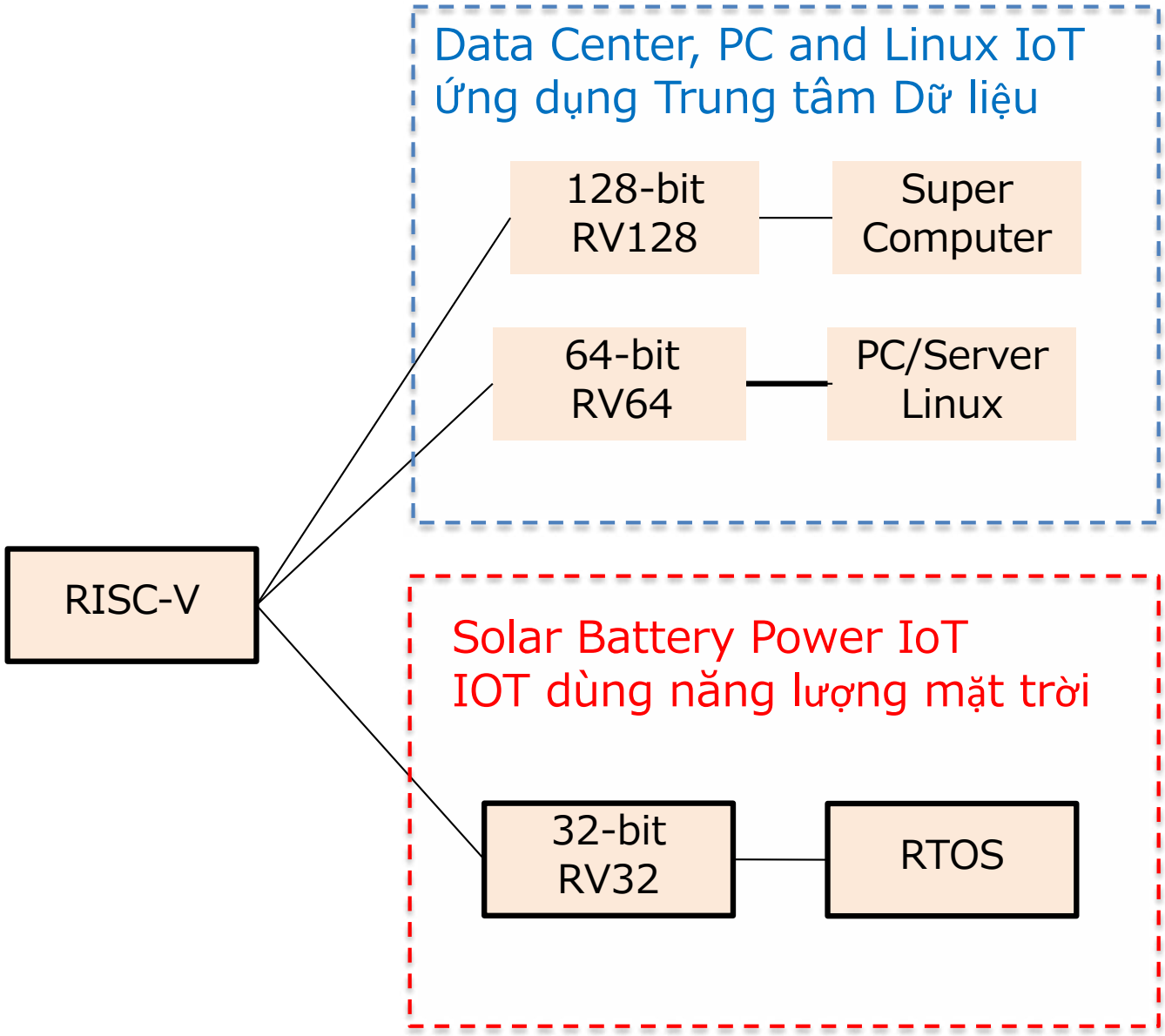
Power = **50mW ~ 180mW**



(c) SH Consulting KK
2019 2020 2021 2022

RISC-V Categories

Danh mục giải pháp RISC-V



Performance Important

Hiệu suất là Trọng tâm

Power Efficiency Important

Hiệu quả dùng năng lượng là trọng tâm

(c) SH Consulting KK 2019 2020 2021 2022

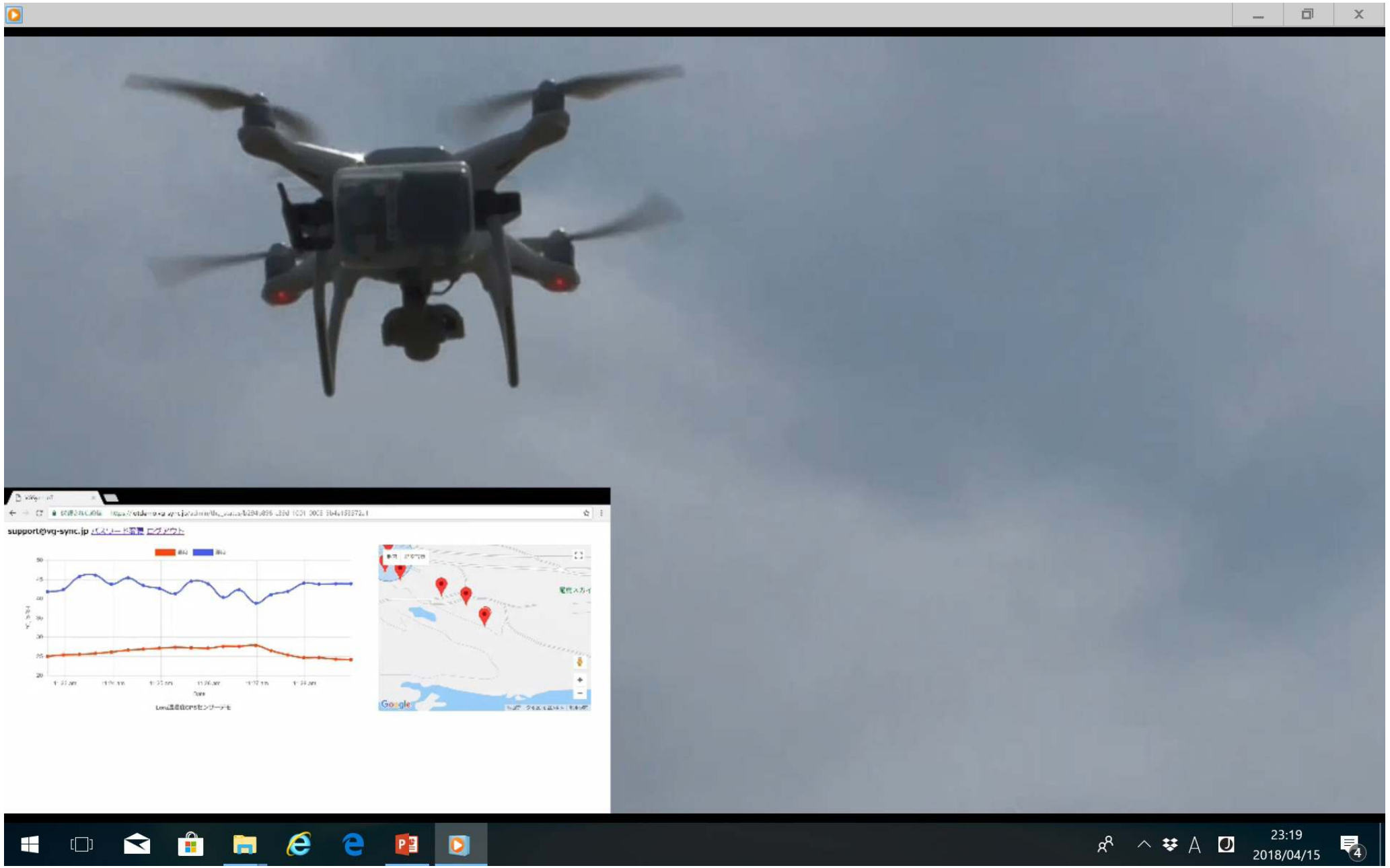
2. LIGHTWEIGHT IOT 2016

2. IOT NHỎ GỌN 2016

(c) SH Consulting KK 2019 2020 2021 2022

Sensing air quality near volcano by drone

Cảm biến chất lượng không khí gần núi lửa bằng máy bay không người lái



Volcanic ash detection using pressure sensors
Phát hiện tro núi lửa bằng cảm biến áp suất

Volcanic Eruption of Mt. Sakurajima Photo: Takahide Sumi
Có thể có được nhiệt độ đất p cho quyển F Mt. Sakurajima

(c) SH Consulting KK 2019 2020 2021 2022

Lightweight IoT (2016) | IoT không dây nhỏ gọn (2016)

Gateway Master

Communicates with Slaves
Uploads data to the cloud
PC, Android phone and tablet used for UI

Endpoint Slave (Sensor | Actuator)

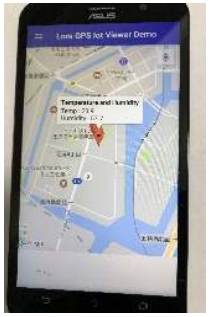
Very Light (180grams)
Dry-cell Batteries: batteries level detection
External/internal wire antenna options
Built-in temperature, humidity gauges and GPS
Standard I/O: ADC, UART, I2C, SPI, GPIO

Data Viewer

PC | Android phone | Tablet
Check sensor data and control actuators

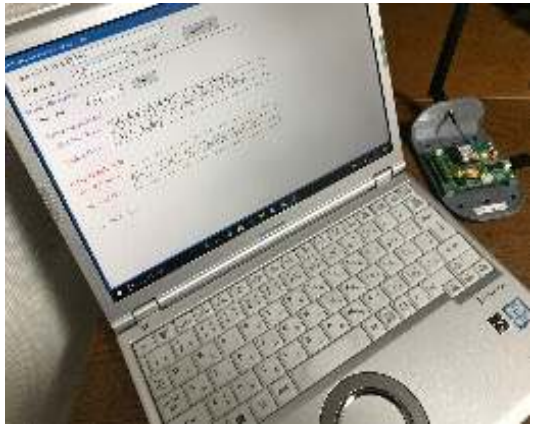
Due to its lightweight
used for drone transported in disaster areas.
(Note) LoRa wireless can operate in Japan,
US, Europe and Vietnam

Example of overall system configuration

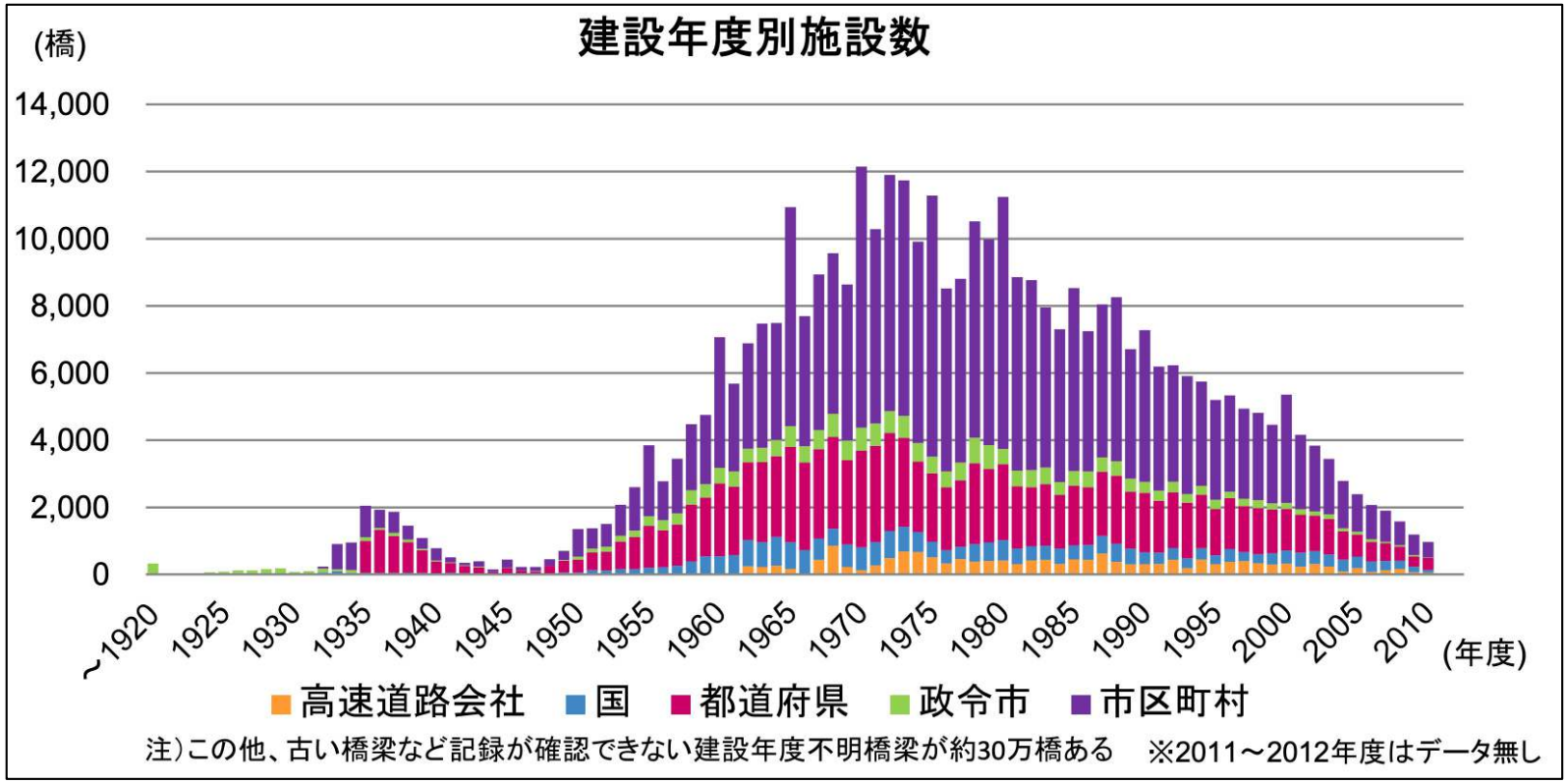


Examples of Android smartphone screens connected to Gateway Master (Google map, temperature temperature and humidity display)

Example of the operation screen of a PC connected to the Gateway Master



(c) SH Consulting KK 2019 2020 2021 2022



3. SINGLE-SPAN BRIDGE STRUCTURAL HEALTH MONITORING

GIÁM SÁT SỨC KHỎE CẤU TRÚC CẦU SINGLE-SPAN

The Jindo Bridge in South Korea has 663 wireless sensors

Souce: Wiki

(c) SH Consulting KK 2019 2020 2021 2022

Design Principles for Bridge SHM System

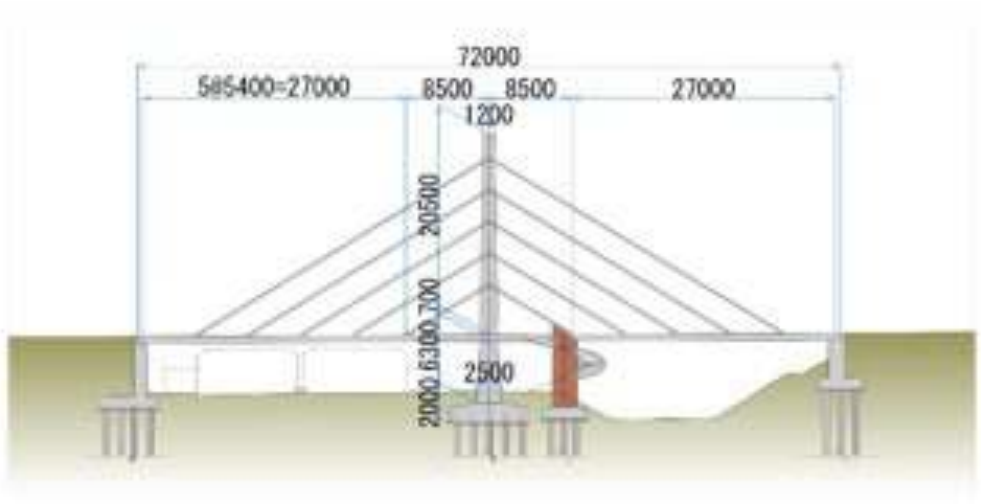
Nguyên tắc thiết kế cho hệ thống SHM Bridge

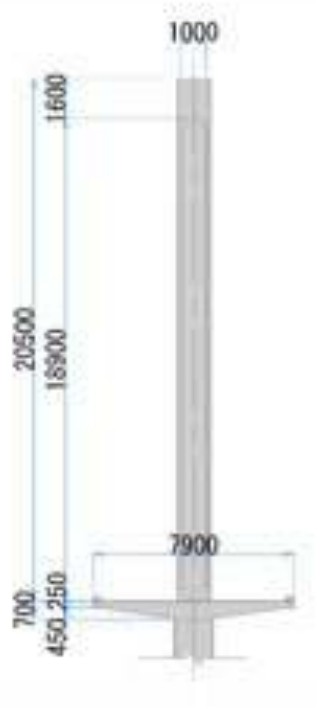
1. Long term use no maintenance e.g. five years
2. Full utilization of solar energy and lithium batteries
3. Simple deployments and remote software upgrade
4. Low annual lease fee for IoT box
5. Use inexpensive components e.g. RISC-V and custom ASICs
6. No compromise on system security
7. Edge and cloud service stack with push notification to smartphones and PCs

1. Sử dụng lâu dài không cần bảo trì vd: năm năm
2. Sử dụng đầy đủ năng lượng mặt trời và pin lithium
3. Triển khai đơn giản và nâng cấp phần mềm từ xa
4. Phí thuê hàng năm thấp cho hộp IoT
5. Sử dụng các thành phần rẻ tiền, ví dụ: RISC-V và ASIC tùy chỉnh
6. Không thỏa hiệp về bảo mật hệ thống
7. Edge và ngăn xếp dịch vụ đám mây với thông báo đẩy tới điện thoại thông minh và PC

(c) SH Consulting KK 2019 2020 2021 2022

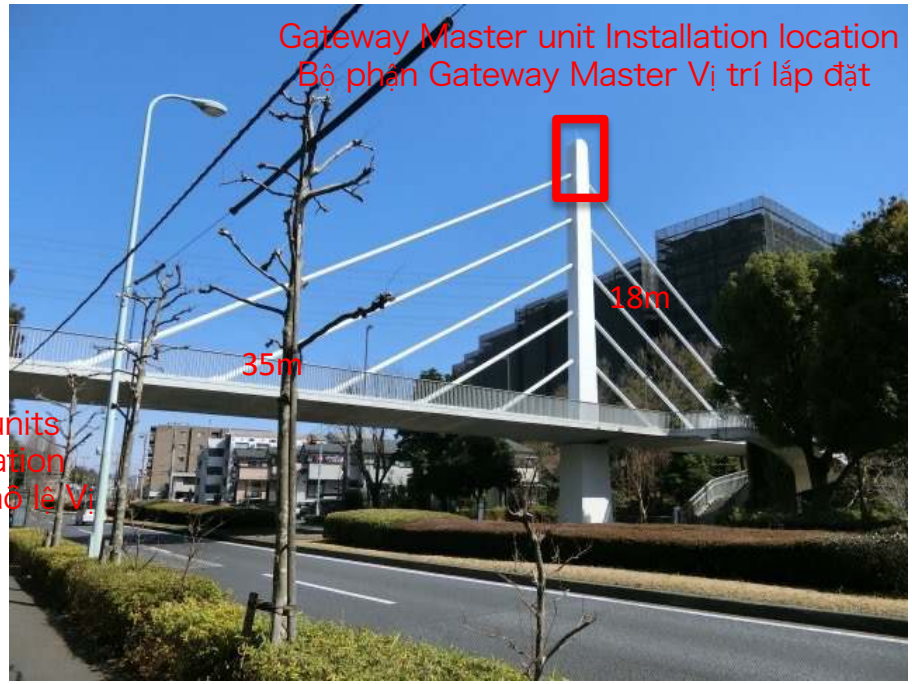
IoT installation and construction method
Phương pháp lắp đặt và xây dựng IoT





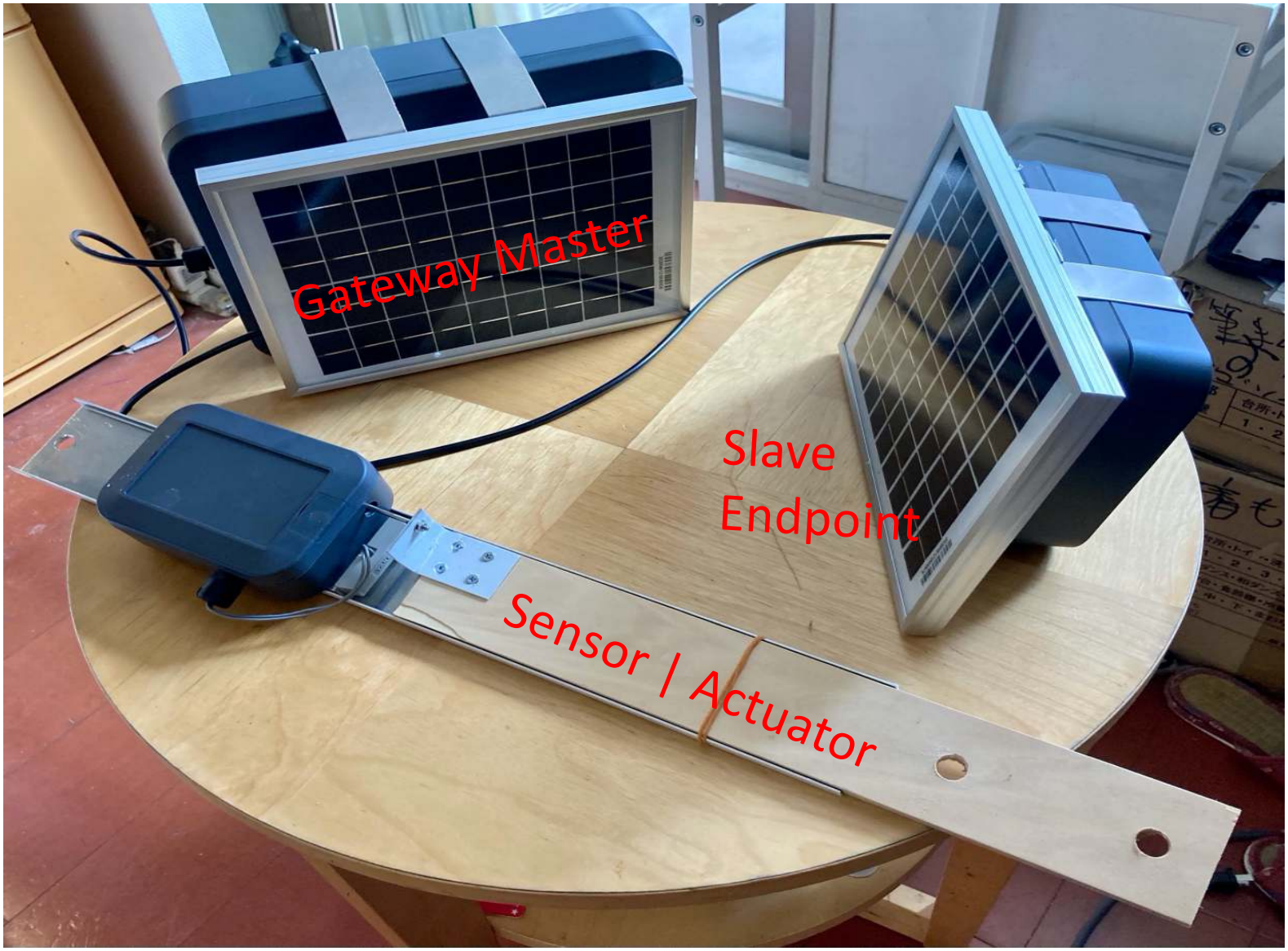
Expansion joint Backside
Khe co giãn Mặt sau

Slave Sensor units Installation location
Đơn vị cảm biến nô lệ Vị trí lắp đặt



Structural Health Monitoring of Bridge Span
Giám sát sức khỏe kết cấu của nhịp cầu

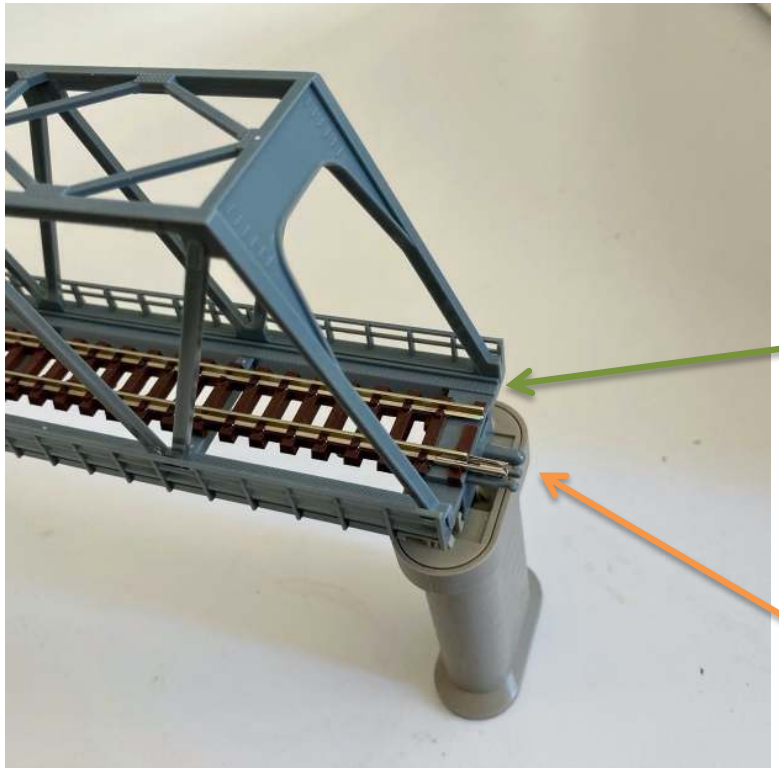
Early Prototype | Nguyên mẫu ban đầu



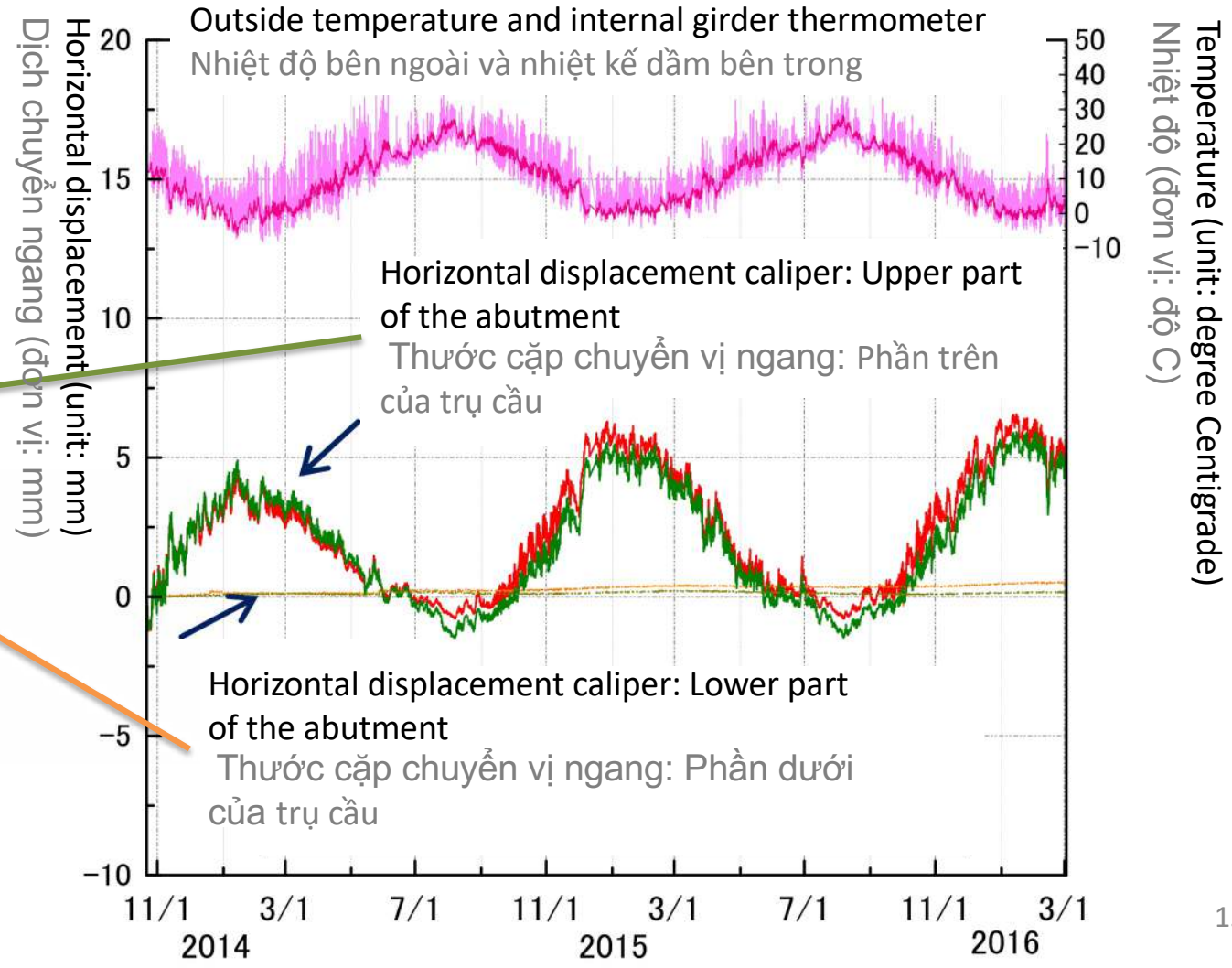
(c) SH Consulting KK
2019 2020 2021 2022

Structural Health Monitoring of Bridge Span

Giám sát sức khỏe kết cấu của nhịp cầu



Data Source: Yusuke Takano etal., Japan Railway Construction, Japan Transport Agency, “Behaviour of GRS-integrated bridges with long bridge lengths as a function of temperature” 2016.



Long-Term (2+ years) Dynamic Measurement of Horizontal Displacement of Bridge Span

Tự động đo lường dài hạn về khoảng cách ngang của nhịp cầu

(c) SH Consulting KK 2019 2020 2021 2022

15

Marmot system | Hệ thống Marmot

Terminal Apps

Sensor | Actuator Data, GPS, Temp, Humidity etc.

IoT Service Terminals

Cloud Services

AWS IoT Core | S3

Device Management

New Firmware for RISC-V wifi, RISC-V Microcontroller, Long Range Wireless

Firmware Update

IoT Device Administrator

MQTT | OTA Firmware Update

Slave Endpoint

Hardware RoT

ESP32 C3 RISC-V SoC w/ WiFi

GD32V RISC-V MCU

920MHz Long Range Wireless

Power Supply Unit

Environmental Sensors

Sensors Actuators

Controlled devices e.g. LED

Sensors / Actuators

920MHz Long-Range Wireless

Gateway Master

2G/3G/4G

ESP32 C3 RISC-V SoC w/ WiFI

Hardware RoT

920MHz Long Range Wireless

GD32V RISC-V MCU

100Mbps Ethernet

Environmental Sensors

Power Supply Unit

(c) SH Consulting KK 2019 2020 2021 2022

4. HARDWARE SECURITY
4. BẢO MẬT PHẦN CỨNG

Cyber Attacks against IoT → Countermeasures

Các cuộc tấn công mạng chống lại IoT → Các biện pháp đối phó

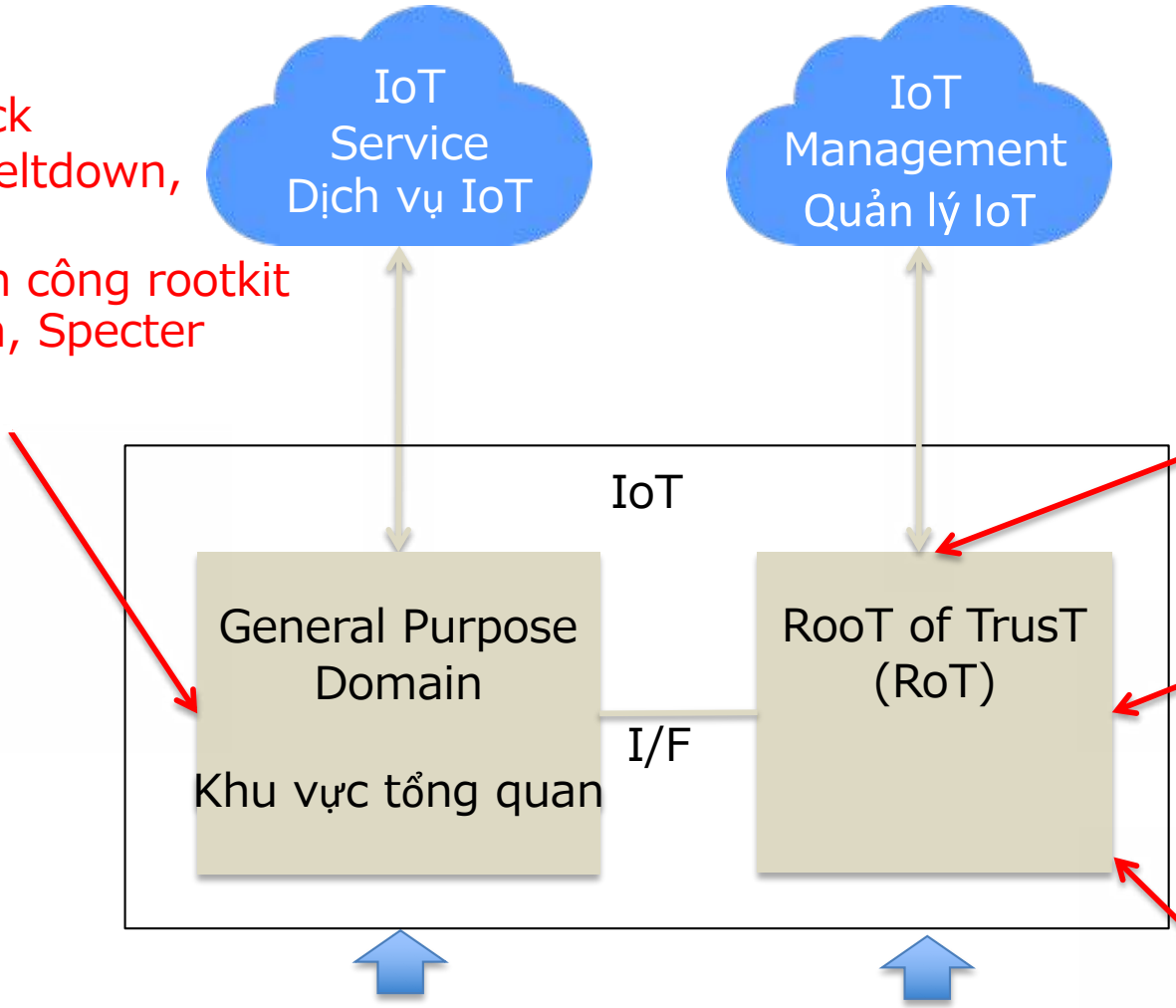
Source: Microchips

Software Attacks DDoS Malicious Code Injection Malicious Access to Memory / Keys Intellectual Property Theft	Tấn công bằng phần mềm DDoS Chèn mã độc hại Truy cập độc hại vào bộ nhớ / khóa Trộm cắp tài sản trí tuệ	TrustZone Secure Boot TrustZone Khởi động an toàn
Communication Attacks Man-in the middle attacks Unprotected encryption keys	Tấn công bằng thông tin liên lạc Tấn công bằng cách xen giữa Khóa mã hóa không được bảo vệ	Crypto Accelerator Secure Key Storage Lưu trữ bộ mã hóa an toàn
Vulnerable Firmware Upgrades Malware replacing genuine program Unprotected key storage for bootloaders	Nâng cấp chương trình cơ sở dễ bị tổn thương Phần mềm độc hại thay thế chương trình chính hãng Lưu trữ khóa không được bảo vệ vào bộ nạp khởi động	Secure Bootloader Secure Key storage Hardware Root of Trust Bộ khởi động an toàn Lưu trữ khóa an toàn Phần cứng gốc của sự tin cậy
Physical Attacks Microprobing Side-channel attacks	Tấn công bằng vật lý Lấy thông tin của bộ xư lý Các cuộc tấn công bằng kênh bên	Chip-level tamper resistance Silent access Chống giả mạo cấp độ chip Truy cập thầm lặng

(c) SH Consulting KK 2019 2020 2021 2022

Separate Chip to protect keys to counter physical and side-channel attack
Chip riêng biệt để bảo vệ các phím để chống lại cuộc tấn công vật lý và kênh bên

Rootkit attack
Example: meltdown, Specter
Ví dụ cho tấn công rootkit : mealtdown, Specter



Chip opening, peeling, etc.
Microscope, SEM, optical tester
Mở chip, bong tróc, v.v.
Kính hiển vi, SEM, máy kiểm tra quang học

Power glitches
on reset pin
clock pin
Temperature
Sự bất thường trên chân reset, xung nhịp nhiệt độ

Power analysis attacks, etc.SPA、DPA、CPA
Các cuộc tấn công phân tích công suất, v.v.SPA 、 DPA 、 CPA

Performance
Innovation
Đổi mới hiệu suất

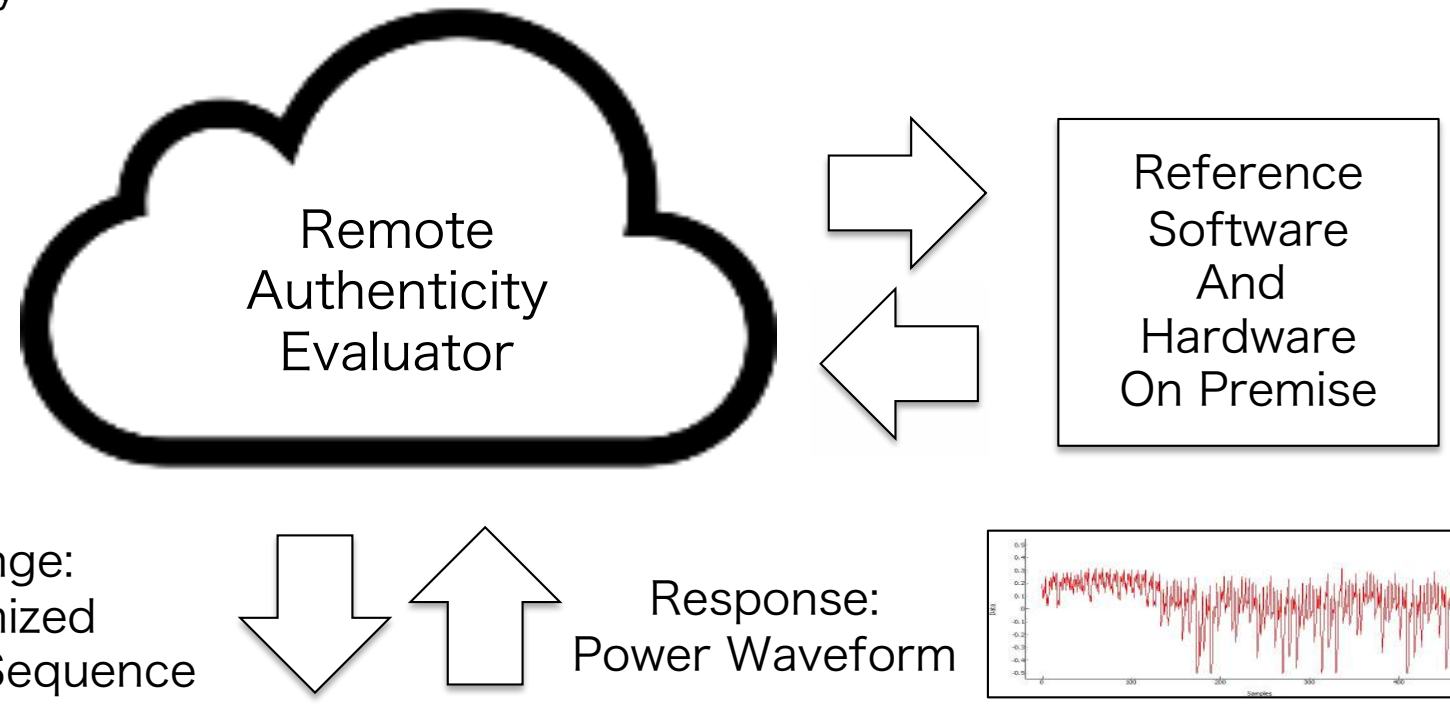
Proven Practices
Tamper Proof
Thực tiễn đã ghi nhận bằng chứng cho sự giả mạo

(c) SH Consulting KK 2019 2020

Remote IoT Software Hardware Authenticity Proof

Bằng chứng xác thực phần cứng phần cứng IoT từ xa

This Research is underway
with NEDO grant
U.S. patent 16/910,103
pending

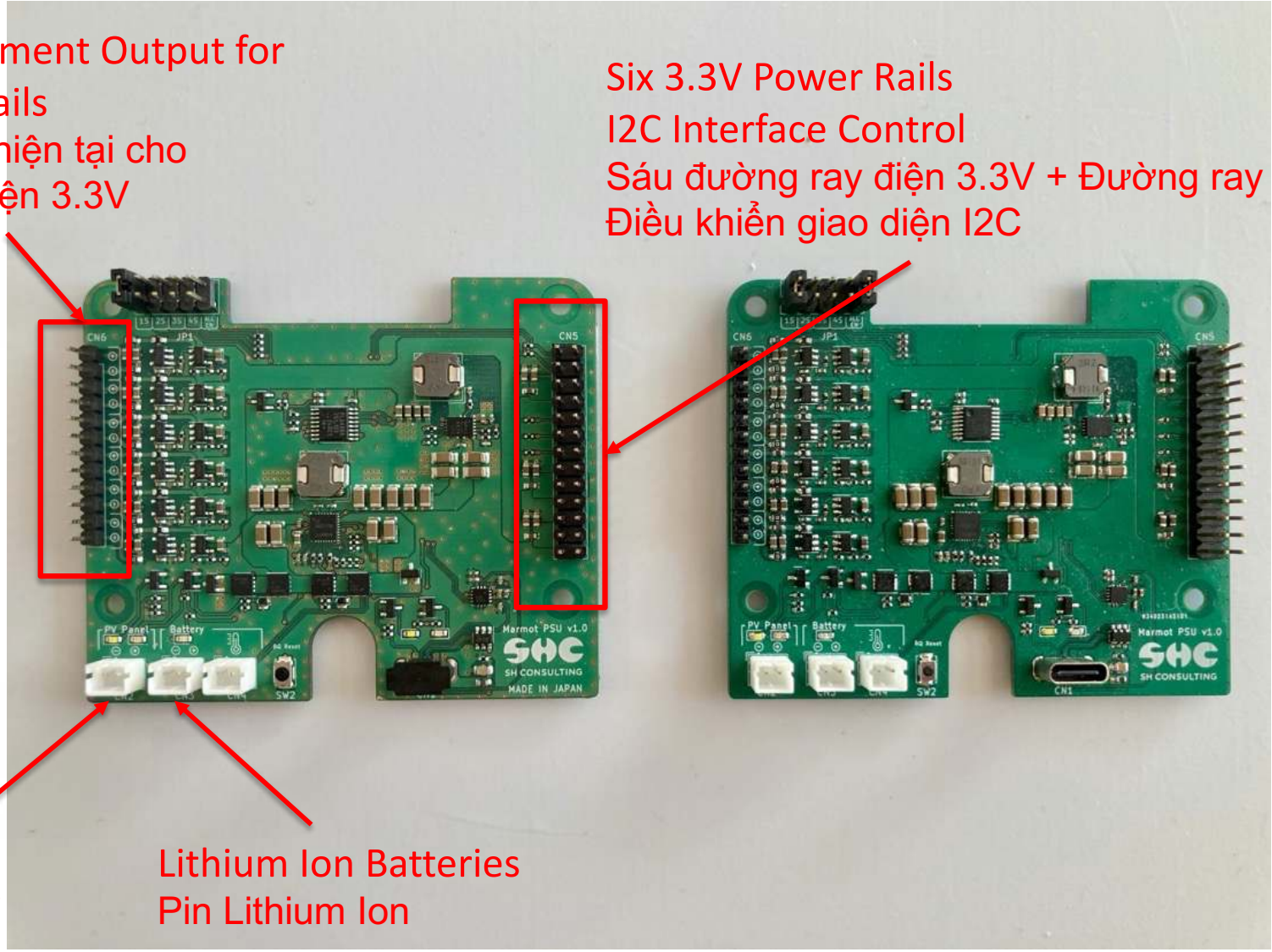


(c) SH Consulting KK 2019 2020 2021

Power Supply Board (PSU)
Bảng cung cấp điện (PSU)

Current Measurement Output for
Six 3.3V Power Rails
Đầu ra đo lường hiện tại cho
Sáu đường ray điện 3.3V

Six 3.3V Power Rails
I2C Interface Control
Sáu đường ray điện 3.3V + Đường ray mặt đất
Điều khiển giao diện I2C



PV Panel Inputs
Đầu vào bảng PV

Lithium Ion Batteries
Pin Lithium Ion

(c) SH Consulting KK 2019 2020 2021 2022

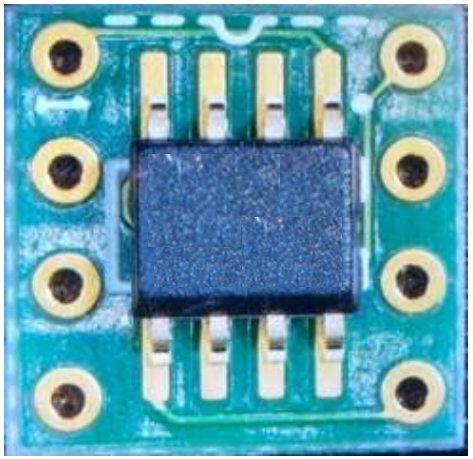
5. SOFTWARE SECURITY
5. BẢO MẬT PHẦN MỀM

Root of Trust

- For IoT placed in public, natural and outdoor spaces, physical attacks cannot be ruled out.
- Secure key storage = Base point of trust = lightweight coprocessor
  - Key management, key generation and random number generation functions.
  - Has a secure storage area that applies tamper-resistant techniques against physical attacks such as decomposition stripping, and side-channel attacks such as current analysis.
  - Provides a modular environment for integrating key provisioning, secure boot, firmware upgrades, authentication and other secure services into the MCU platform.

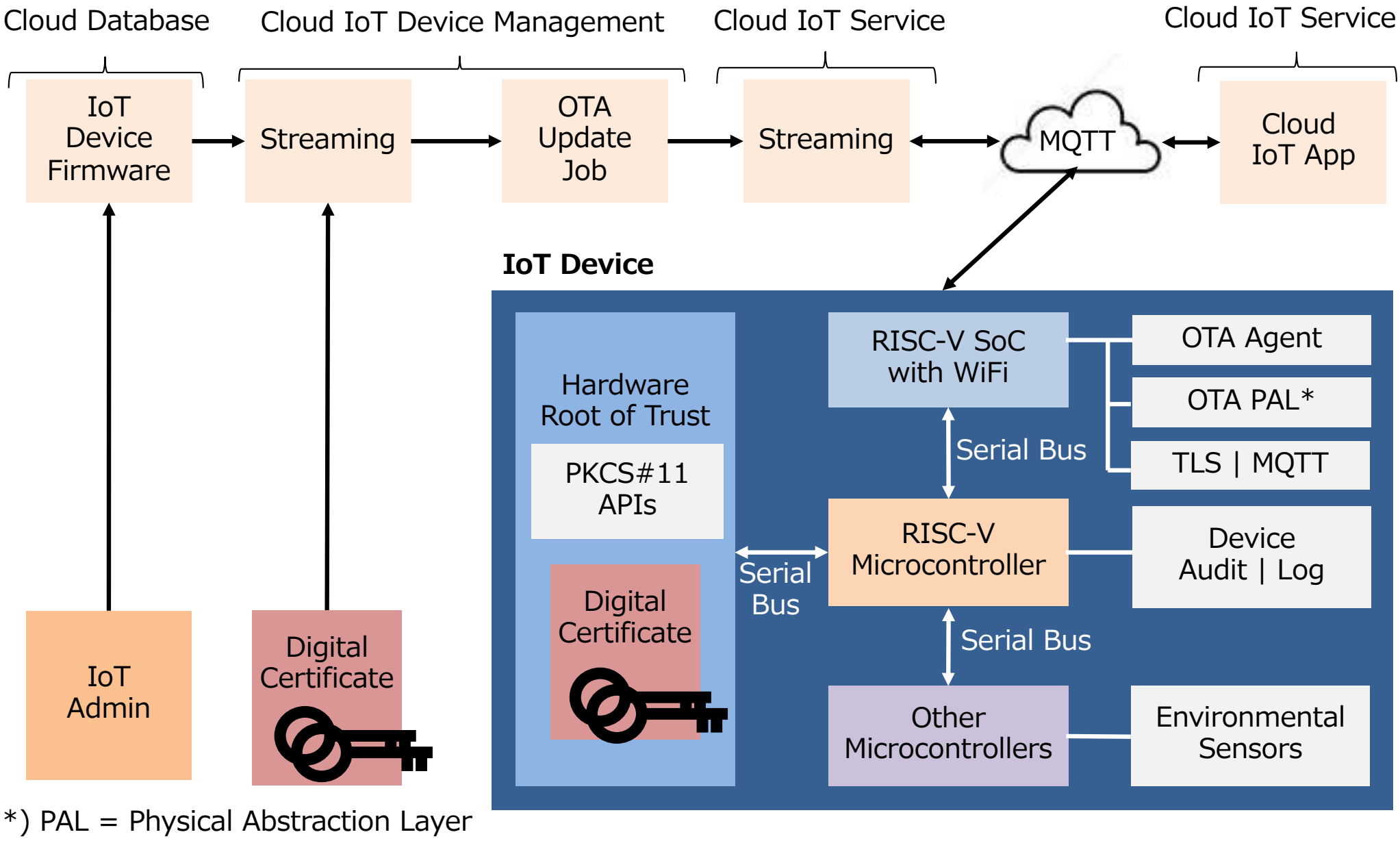
- Đối với IoT được đặt trong không gian công cộng, tự nhiên và ngoài trời, không thể loại trừ các cuộc tấn công vật lý.
- Lưu trữ khóa an toàn = Điểm tin cậy cơ bản = bộ đồng xử lý nhỏ gọn
  - Chức năng quản lý khóa, tạo khóa và tạo số ngẫu nhiên.
  - Có khu vực lưu trữ an toàn áp dụng các kỹ thuật chống giả mạo chống lại các cuộc tấn công vật lý như loại bỏ phân tách và các cuộc tấn công kênh bên như phân tích hiện tại.
  - Cung cấp môi trường mô-đun để tích hợp cung cấp khóa, khởi động an toàn, nâng cấp chương trình cơ sở, xác thực và các dịch vụ bảo mật khác vào nền tảng MCU.

Root of Trust Chip
= Secure Microcontroller



- A Hardware root of trust chip is used in Marmot IoT systems to create device certificate with below advantages:
  - Generate shorter key, lower power consumption and lower on memory usage
- Root of Trust chip được dùng trong những hệ thống IoT của chúng tôi gần đây đe tạo chứng chỉ cho thiết bị với những thuận lợi sau:
  - Tạo ra khóa ngắn hơn, tiêu thụ ít năng lượng và dùng bộ nhớ nhỏ hơn.

AWS IoT Core OTA Software Upgrade Architecture
Kiến trúc nâng cấp phần mềm AWS IoT Core OTA



*) PAL = Physical Abstraction Layer

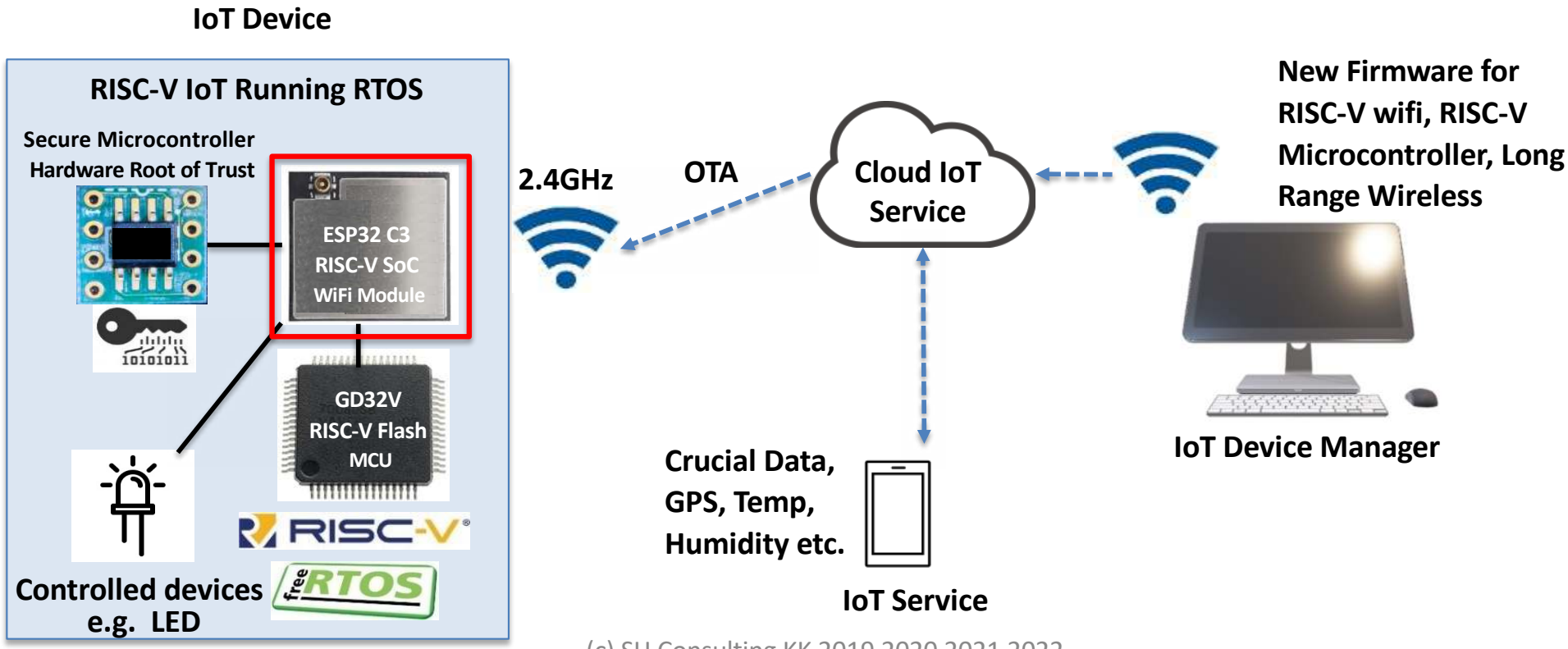
(c) SH Consulting KK 2019 2020 2021 2022

6. OTA SOFTWARE UPDATE DEMO

6. TRÌNH DIỄN CẬP NHẬT PHẦN MỀM OTA

DEMO 1 : OTA FOR ESP32 C3 RISC-V WIFI Module

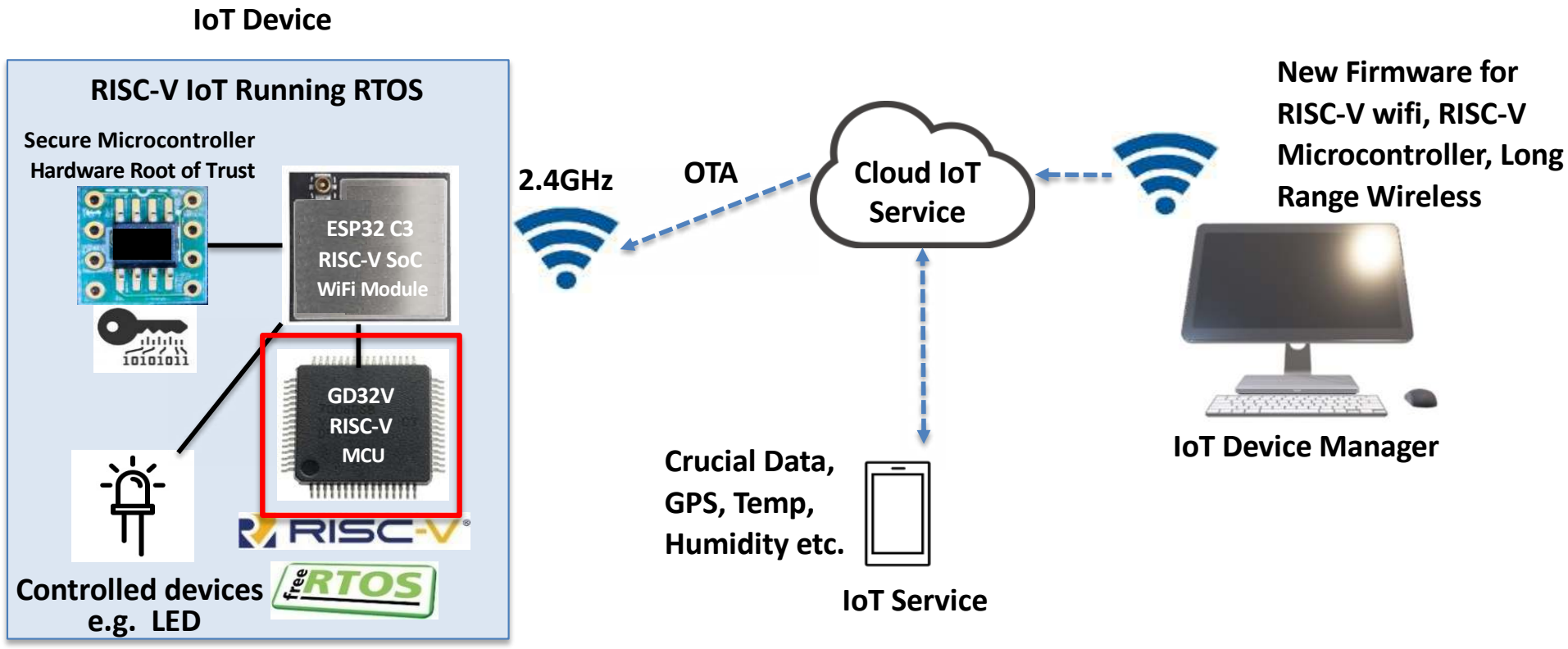
- ESP32 C3 RISC-V wifi module is used in the Marmot System.
  RISC-V Wifi là một phần của hệ thống Marmot.
- Is used to connect system to IoT AWS with Root of Trust.
  Được dùng để kết nối an toàn với IoT AWS.
- The firmware can be upgraded by OTA.
  Chương trình có thể được nâng cấp qua mạng.



(c) SH Consulting KK 2019 2020 2021 2022

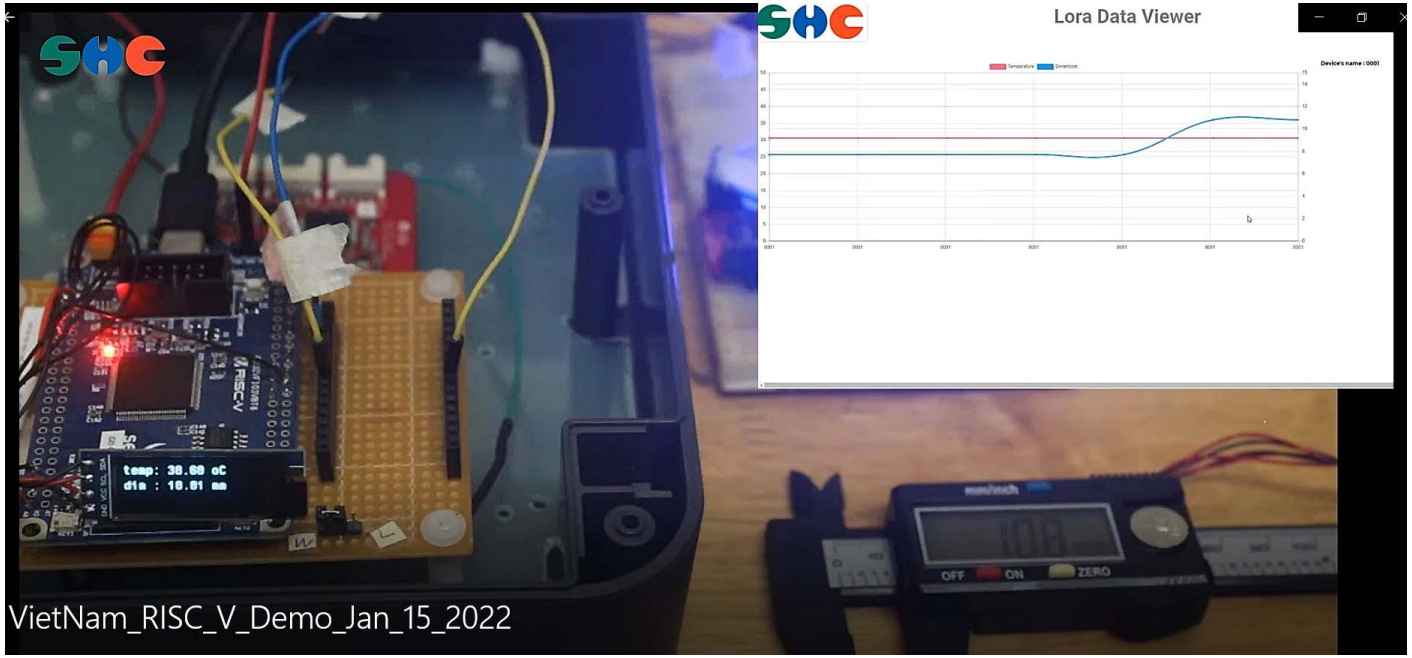
DEMO 2 : OTA FOR GD32V RISC-V MCU

- GD32V is main controller of Marmot system.
  Đây là bộ xử lý chính của hệ thống Marmot.
- Can be upgrade firmware using OTA though RISC-V wifi module by UART.
  Có thể nâng cấp chương trình qua mạng thông qua khối RISC-V Wifi dùng UART.



(c) SH Consulting KK 2019 2020 2021 2022

DEMO 3 : DIGTAL CALIPER DEMO FOR STRUCTURAL HEALTH MONITORING



- This demo shows a technical element of Marmot System, transmission of data to cloud.
  Trình diễn này cho thấy một phần kỷ thuật hệ thống Marmot, truyền dữ liệu đến cloud.
- Lora Slave Module sends data from digital caliper connected to a physical structure to Marmot System and then upload to AWS IoT. User can see behavior of digital caliper with web app.
  Dữ liệu từ thước kẹp số cái được kết nối vật lý với khối Lora Slave được gởi đen Marmot dùng Lora và sau đó sẽ được gởi lên AWS IoT. Người dùng có thể quan sát được trạng thái của thước kẹp số bằng một ứng dụng web.

(c) SH Consulting KK 2019 2020 2021 2022

7. FUTURE DIRECTIONS AND SUMMARY

7. ĐỊNH HƯỚNG TRONG TƯƠNG LAI VÀ TÓM TẮT

Marmot IoT services | Dịch vụ Marmot IoT

Services | Dịch vụ	Present Status | Hiện trạng	Future Directions | Dự định trong tương lai
Unit Installation | Cài đặt đơn vị	Supplier Configures and Install units | Cấu hình cho nhà cung cấp và cài đặt thiết bị	Customers configure and install units | Cấu hình khách hàng và cài đặt đơn vị
Application Development | Phát triển ứng dụng	Supplier Provides Customer Applications | Nhà cung cấp đã cung cấp ứng dụng cho khách hàng☆	Customer programs device using APIs | Khách hàng lập trình thiết bị với API
Cloud Connectivity | Kết nối đám mây	PC or Raspberry Pi provides WiFi or Ethenet connectivity☆| PC hoặc Raspberry Pi cung cấp kết nối WiFi hoặc Ethernet	Gateway Master provides LTE, WiFi and Ethernet connectivity | Gateway Master cung cấp kết nối dung LTE, WiFi và Ethernet.
Transaction Logging | Ghi nhật ký trao đổi	Gateway Master logs as custom feature| Gateway Master ghi nhật ký dưới dạng tính năng tùy chỉnh	Master and Slave log transactions to their flash memories | Nhật ký trao đổi của Master và Slave được gởi đến bộ nhớ flash
Cloud Storage, Data Visualization, AI etc. | Lưu trữ đám mây, Trực quan hóa dữ liệu, AI, v.v.	Cloud service leverages VB Sync IoT☆☆ | Dịch vụ đám mây tận dụng VB Sync IoT	Leverages AWS IoT Core, S3 and Lambda ☆ | Tận dụng AWS IoT Core, S3 và Lambda
IoT Security Management | Quản lý bảo mật IoT	Standard Network Security | An ninh mạng tiêu chuẩn	Root of trust chip stores device keys. Malware detection circuit. | Root of trust chip lưu trữ các khóa thiết bị. Mạch phát hiện phần mềm độc hại.
Maintenance | Bảo dưỡng	Replace Dry-Cell Batteries every 1 to 6 months | Thay pin Dry-Cell sau mỗi 1 đến 6 tháng	Up to 5 years of service period using Solar Power | Thời hạn sử dụng lên đến 5 năm sử dụng năng lượng mặt trời

(c) SH Consulting KK 2019 2020 2021 2022

7. Summary
7. Bản tóm tắt

1. In contrast to Linux, RTOS consumes less power and can be powered by solar, lithium, etc.
2. For IoT device security, root-of-trust chips are being integrated.
3. We are conducting a research of remotely detecting malware and hardware implant by measuring chip current.
4. RTOS device authentication and OTA software update are in progress.
5. We are contemplating a custom ASIC chip with open silicon.

(c) SH Consulting KK 2019 2020 2021 2022

7. Summary
7. Bản tóm tắt

1. Ngược lại với Linux, RTOS tiêu thụ ít điện năng hơn và có thể được cung cấp năng lượng bằng năng lượng mặt trời, lithium, v.v.
2. Đối với bảo mật thiết bị IoT, các Root of trust chip đang được tích hợp.
3. Chúng tôi đang nghiên cứu khả năng phát hiện phần mềm độc hại bằng cách đo dòng điện của chip.
4. Đang thực hiện xác thực thiết bị RTOS và cập nhật phần mềm từ xa không dây.
5. chúng tôi đang có kế hoạch thiết kế chip MCU an toàn với silicon mở.

Acknowledgments

This result was obtained as a result of "Secure Open Architecture Fundamental Technology and Its AI Edge Applied Research and Development" commissioned by the New Energy and Industrial Technology Development Organization (NEDO) (JPNP16007).

Kết quả này có được là kết quả của "Công nghệ cơ bản về kiến trúc mở an toàn và Nghiên cứu và phát triển ứng dụng AI Edge của nó" do Tổ chức Phát triển Công nghệ Công nghiệp và Năng lượng Mới (NEDO) (JPNP16007) ủy quyền.

THANK YOU

These PSU boards are currently characterized.

(c) SH Consulting KK 2019 2020 2021 2022