HARDWARE SECURITY 101

DEEP DIVE INTO HARDWARE

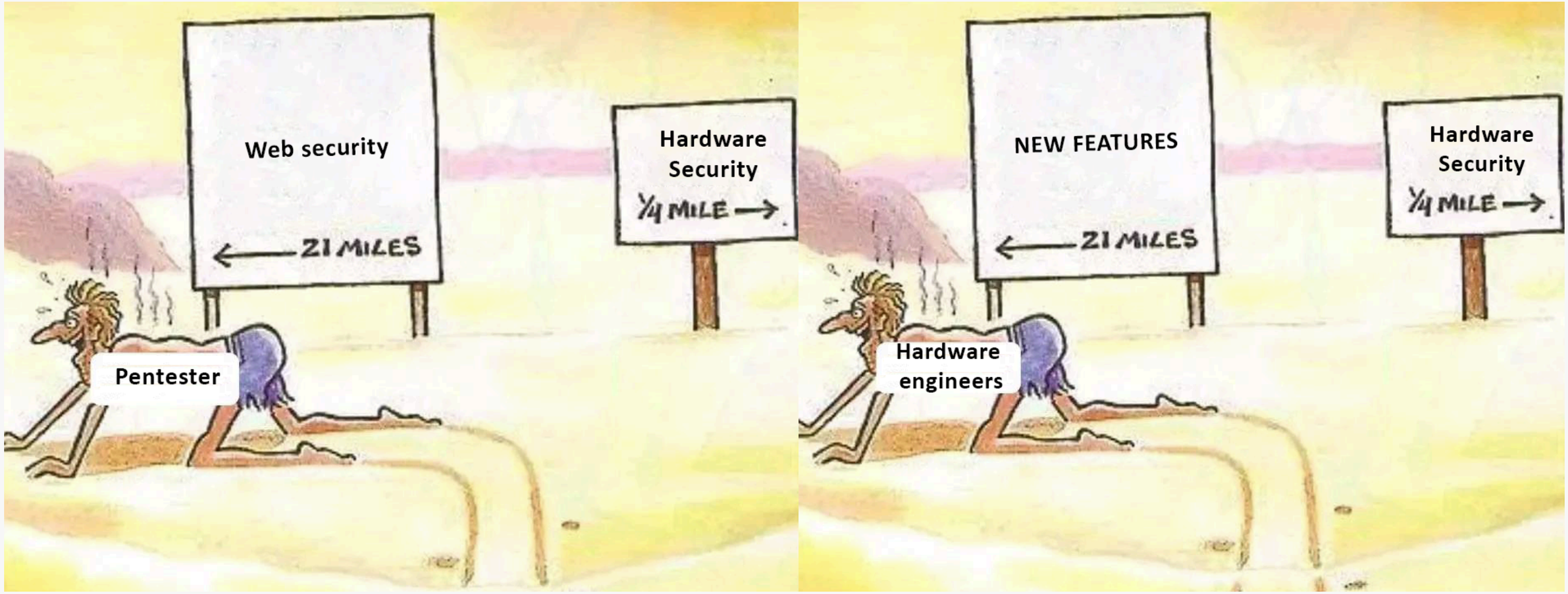
ABOUT ME

Computer hardware engineering

Founder of Beelog Tech
Inventor, IoT developer

Davgasuren

PROBLEM


Web security
21 MILES
Hardware Security
¼ MILE
Pentester
NEW FEATURES
21 MILES
Hardware Security
¼ MILE
Hardware engineers

REAL LIFE PROBLEMS

REAL LIFE PROBLEMS

REAL LIFE PROBLEMS

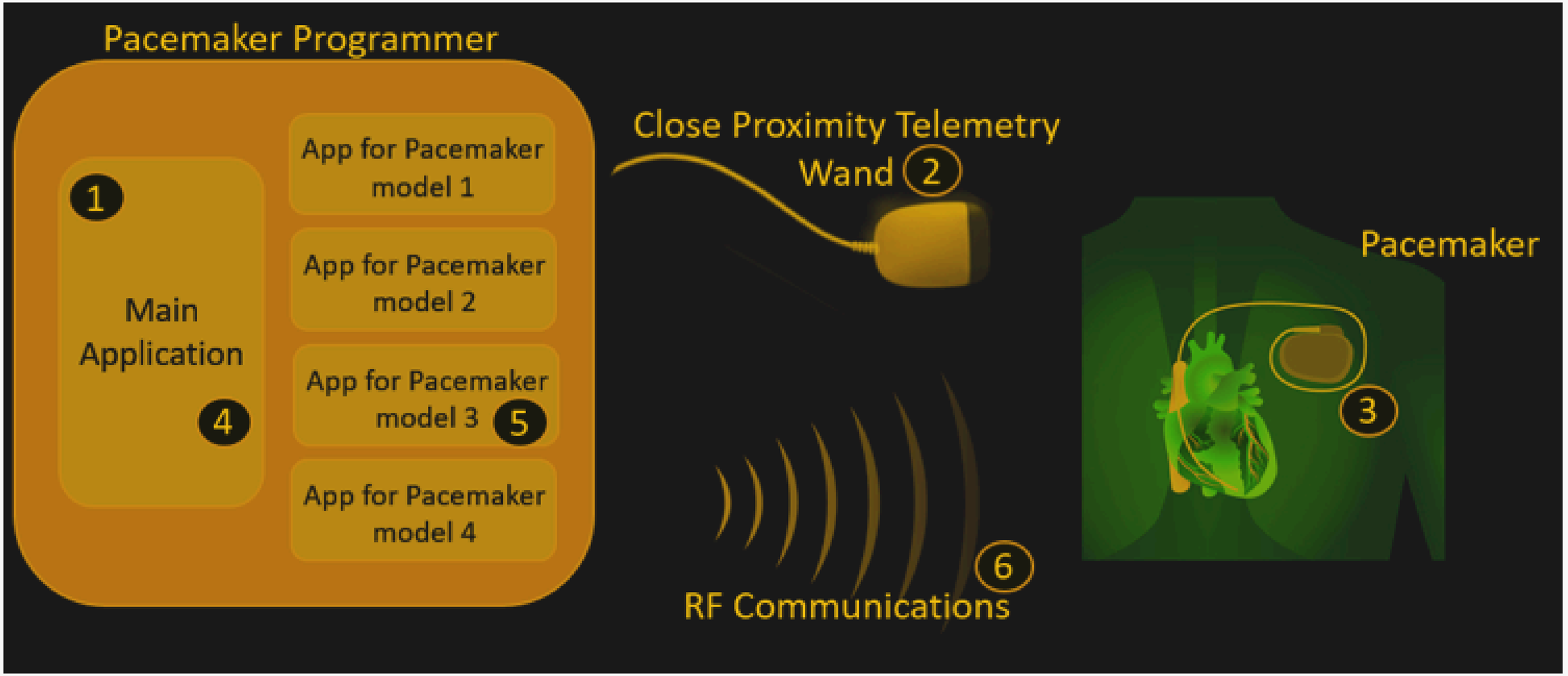
REAL LIFE PROBLEMS

REAL LIFE PROBLEMS

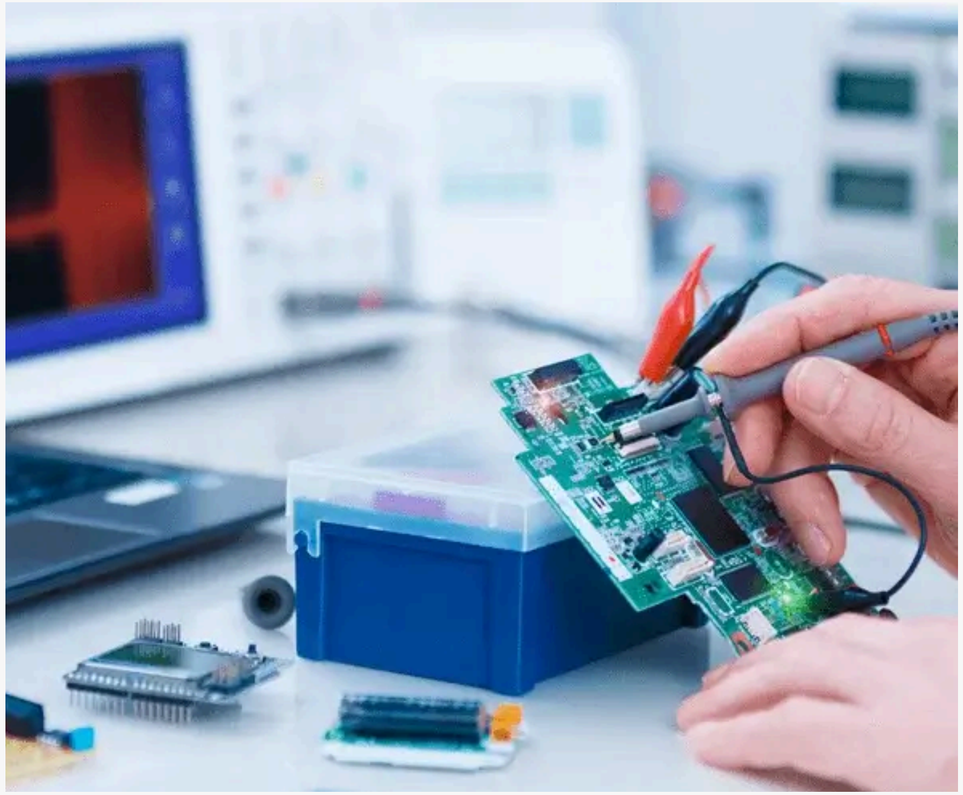
REAL LIFE PROBLEMS

REAL LIFE PROBLEMS

REAL LIFE PROBLEMS



HARDWARE IS HARD

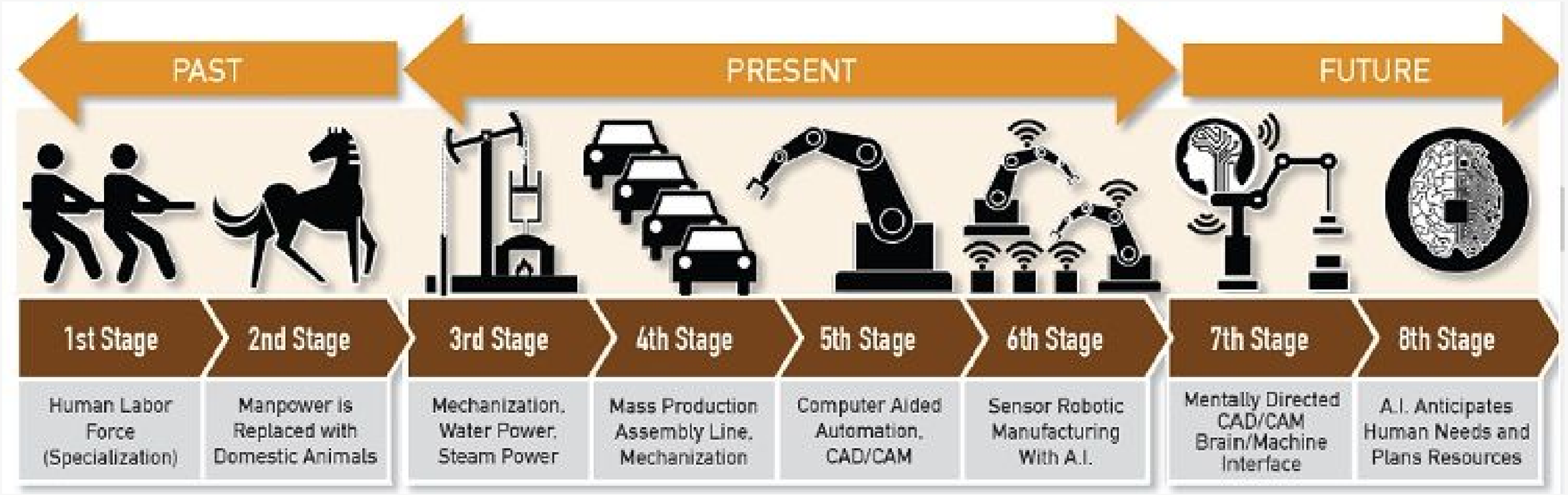


More moving parts

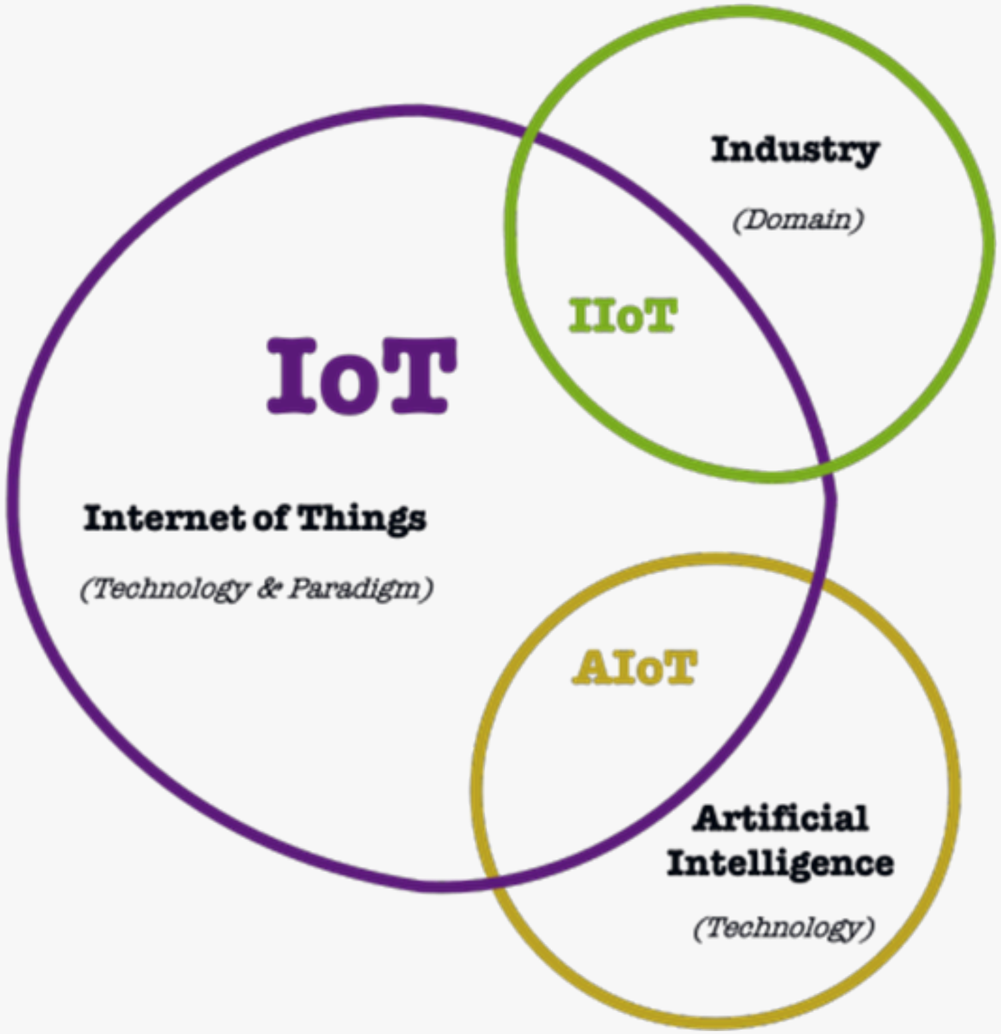
Need diverse skills

Requires longer lead times

INDUSTRIAL REVOLUTION



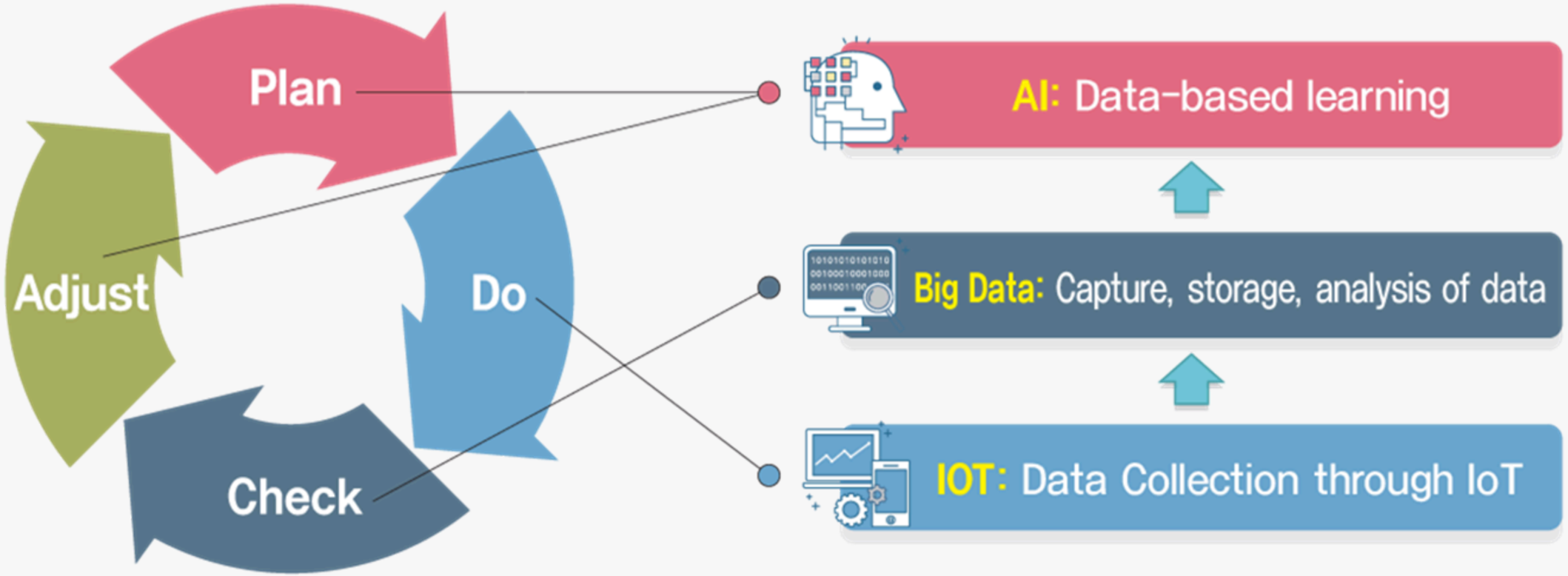
INDUSTRIAL REVOLUTION



Industrial Internet of things - IIoT

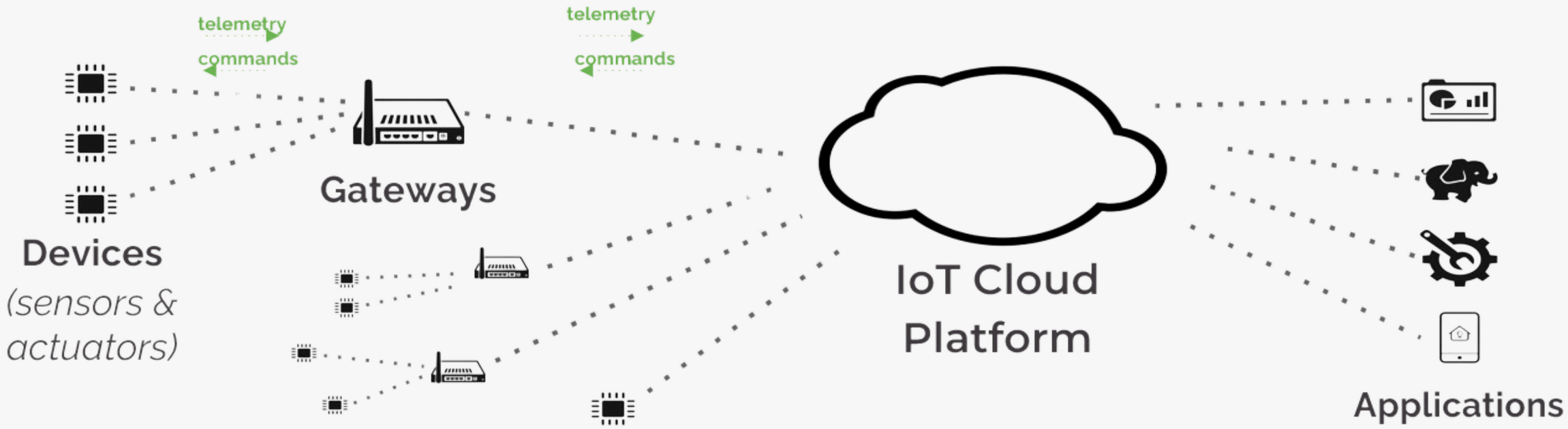
Artificial Intelligence of things - AIoT

VENDOR LOCK

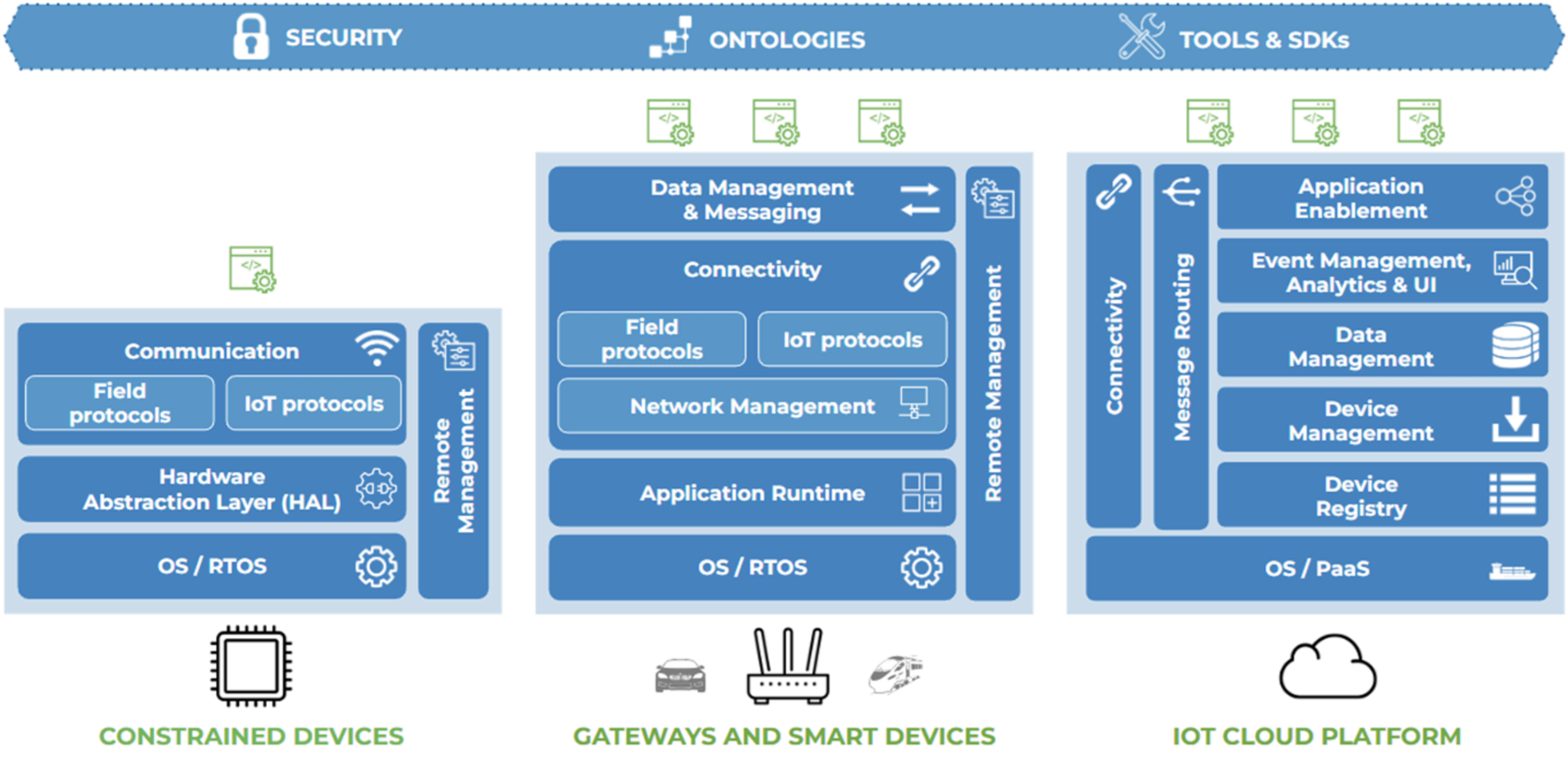

Plan
Do
Check
Adjust
AI: Data-based learning
Big Data: Capture, storage, analysis of data
IOT: Data Collection through IoT

DEEP DIVE INTO HARDWARE DEVELOPMENT

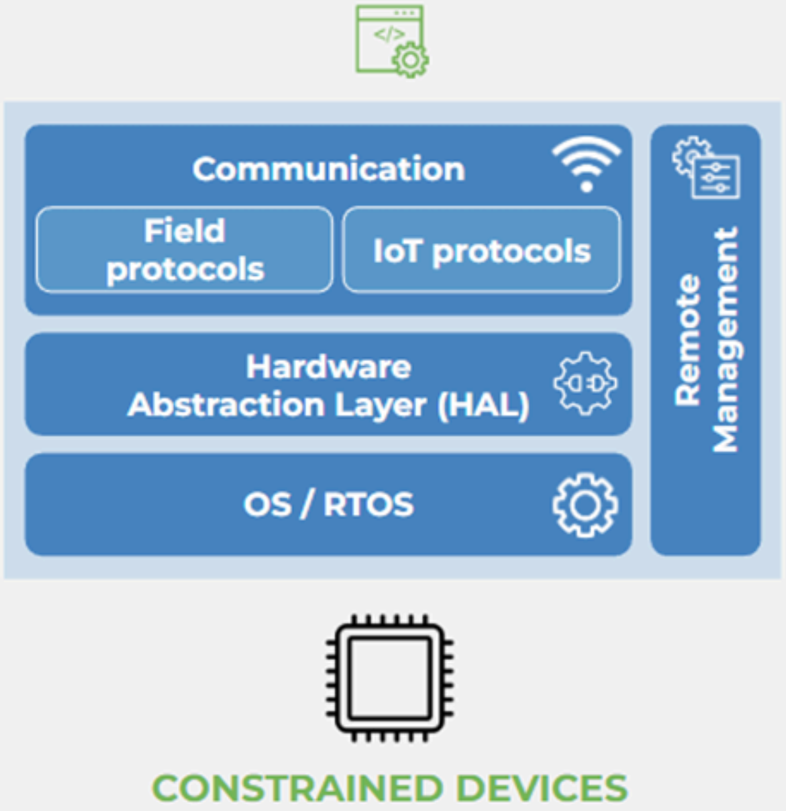
TYPICAL IOT ARCHITECTURE



IOT STACKS


SECURITY
ONTOLOGIES
TOOLS & SDKs
Communication
Field protocols
IoT protocols
Hardware Abstraction Layer (HAL)
OS / RTOS
Remote Management
Data Management & Messaging
Connectivity
Field protocols
IoT protocols
Network Management
Application Runtime
OS / RTOS
Remote Management
Connectivity
Message Routing
Application Enablement
Event Management, Analytics & UI
Data Management
Device Management
Device Registry
OS / PaaS
CONSTRAINED DEVICES
GATEWAYS AND SMART DEVICES
IOT CLOUD PLATFORM

IOT DEVICE STACK



OS / RTOS

- timers, tasks, file system, ...

Hardware Abstraction Layer (HAL)

- API enabling access to memory, GPIOs, MEMS, serial interfaces ,...

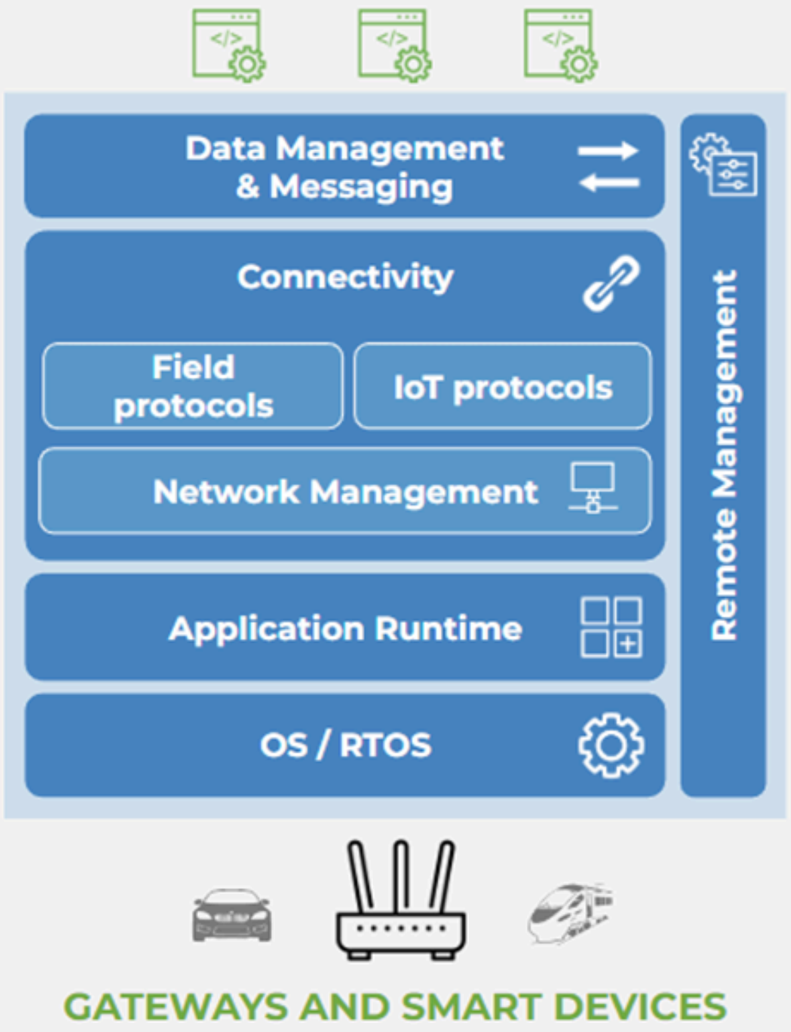
Communication

- Protocols such as Bluetooth, Z-Wave, Thread, CAN bus, MQTT, CoAP, ...

Remote Management

- over-the-air firmware upgrade, health monitoring, factory reset, ...

IOT GATEWAY STACK



Application Runtime

- Virtual Machine / Application container

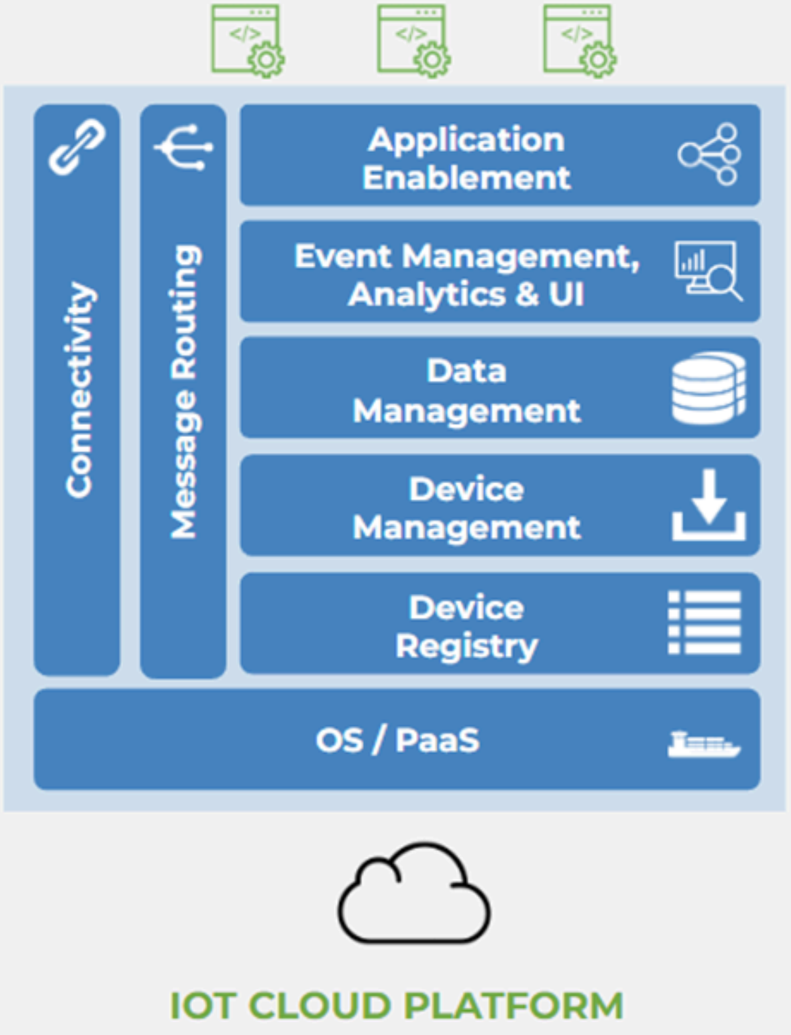
Network Management

- connect to different types of networks
- ensure reliability, security (VPN, firewall, ...)

Data Management & Messaging

- local persistence (network latency)
- offline mode
- data analytics at the edge

IOT CLOUD PLATFORM STACK



Connectivity / **Message Routing**

- ingest and normalize huge amounts of data into an enterprise backend

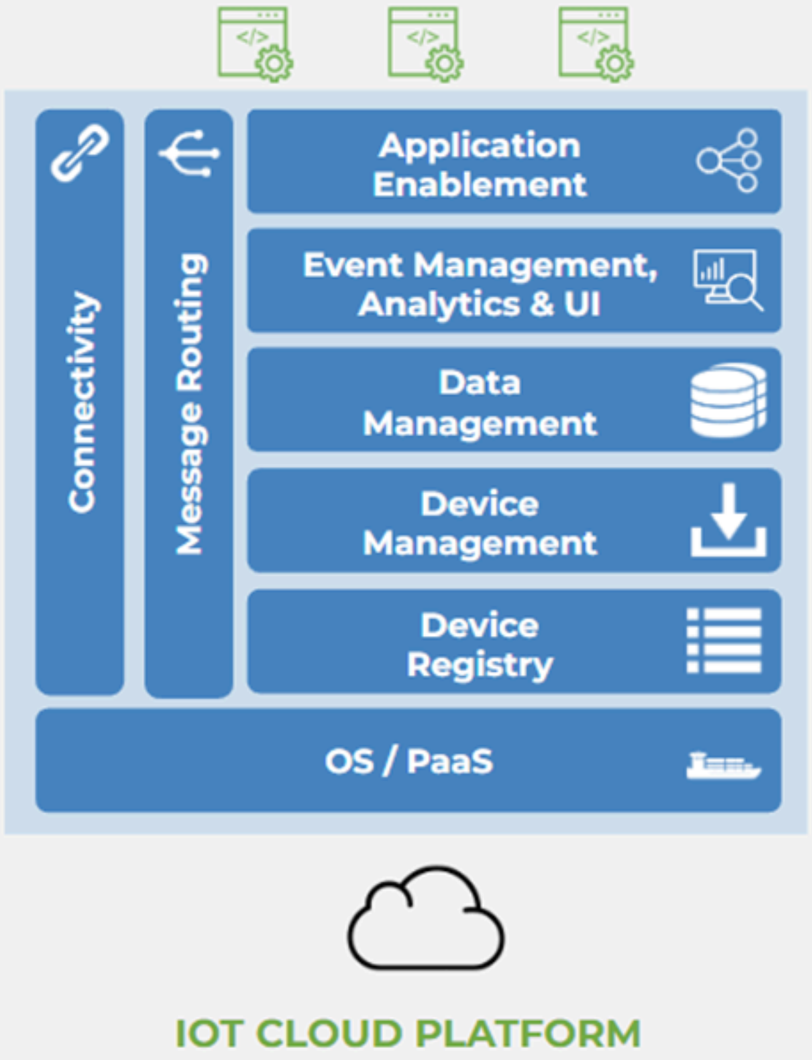
Device Registry / **Device Management**

- identify devices, allow for over-the-air software provisioning, configuration changes, ...

Data Management

- scalable data store, time series

IOT CLOUD PLATFORM STACK



Event Management, Analytics & UI

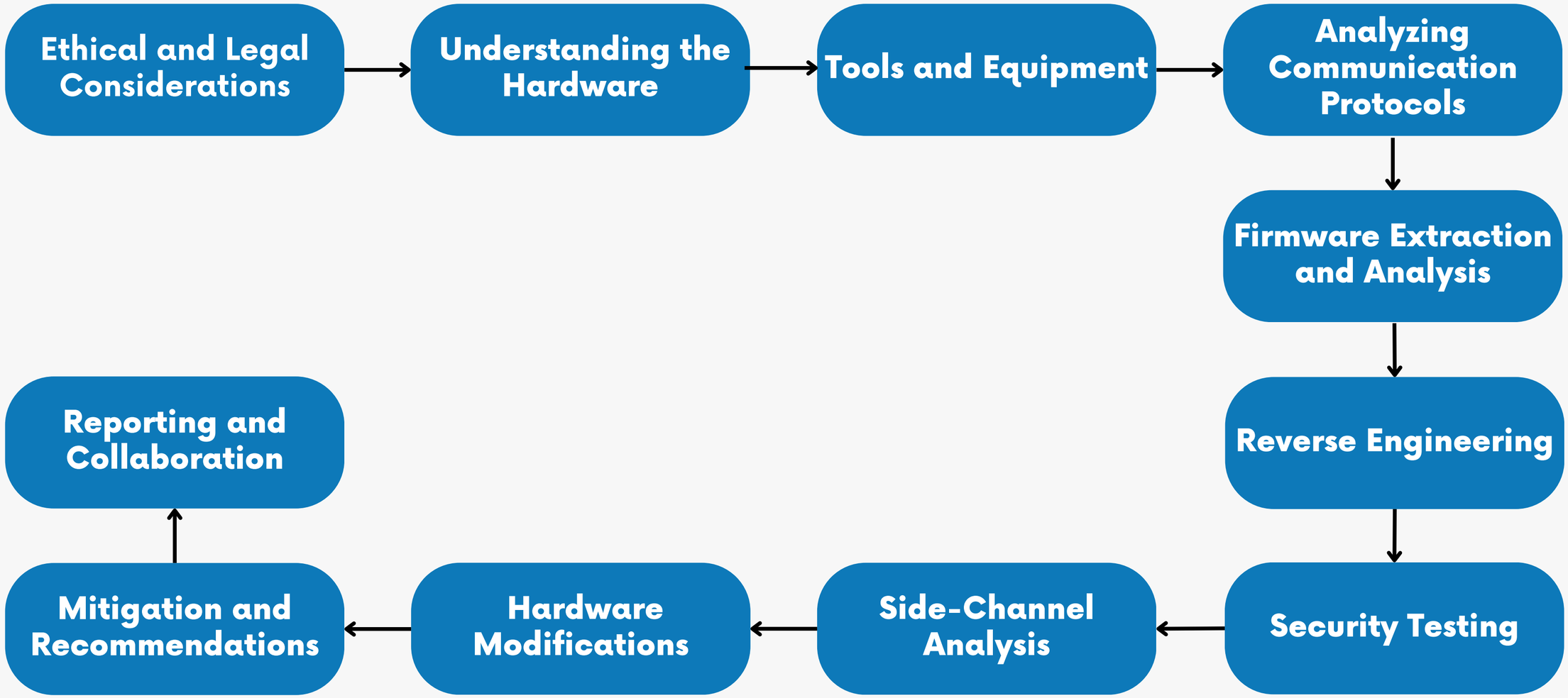
- scalable event processing
- create reports, graphs, dashboards, ...
- make decisions based on the data

Application Enablement

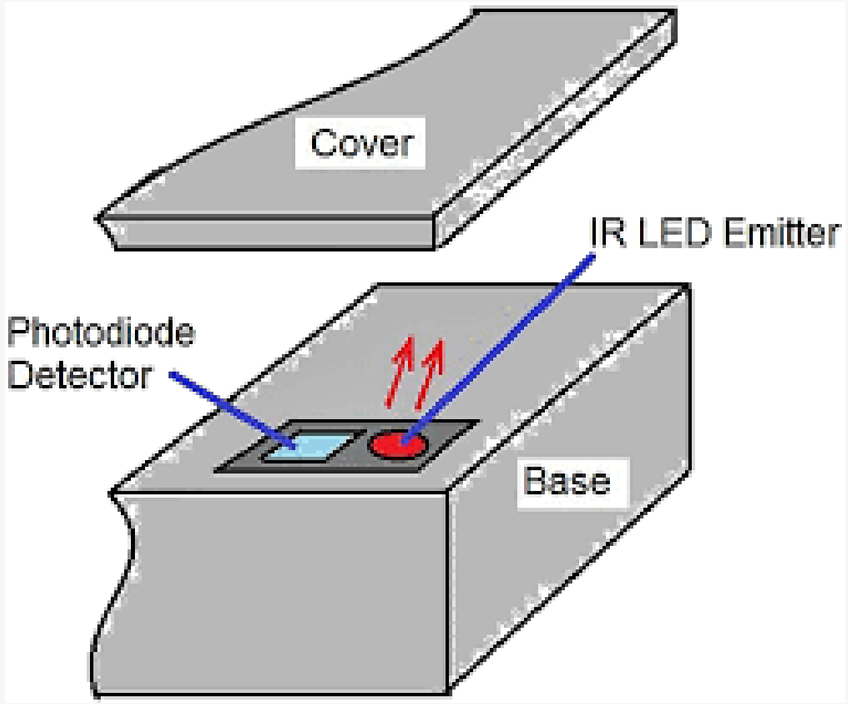
- expose API for application integration

IOT HARDWARE DEVELOPMENT PROCESS

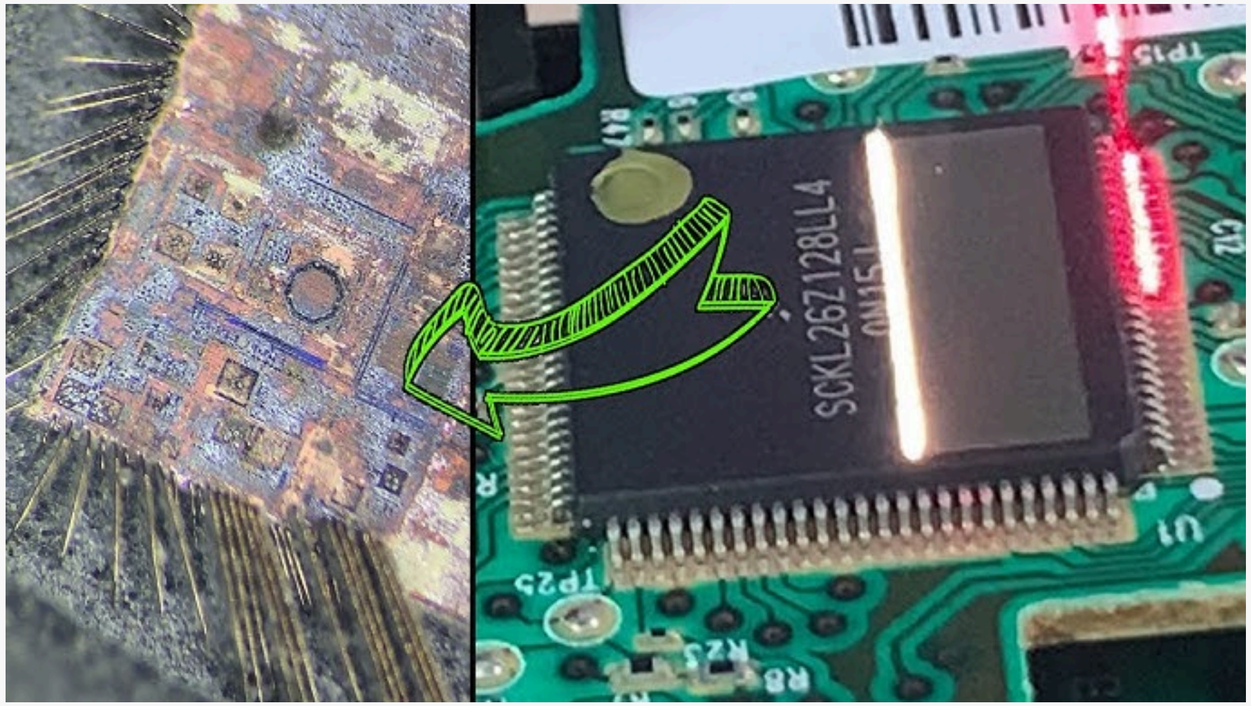
HOW TO HACK A HARDWARE - HANDS ON GUIDE



BEST PRACTICES

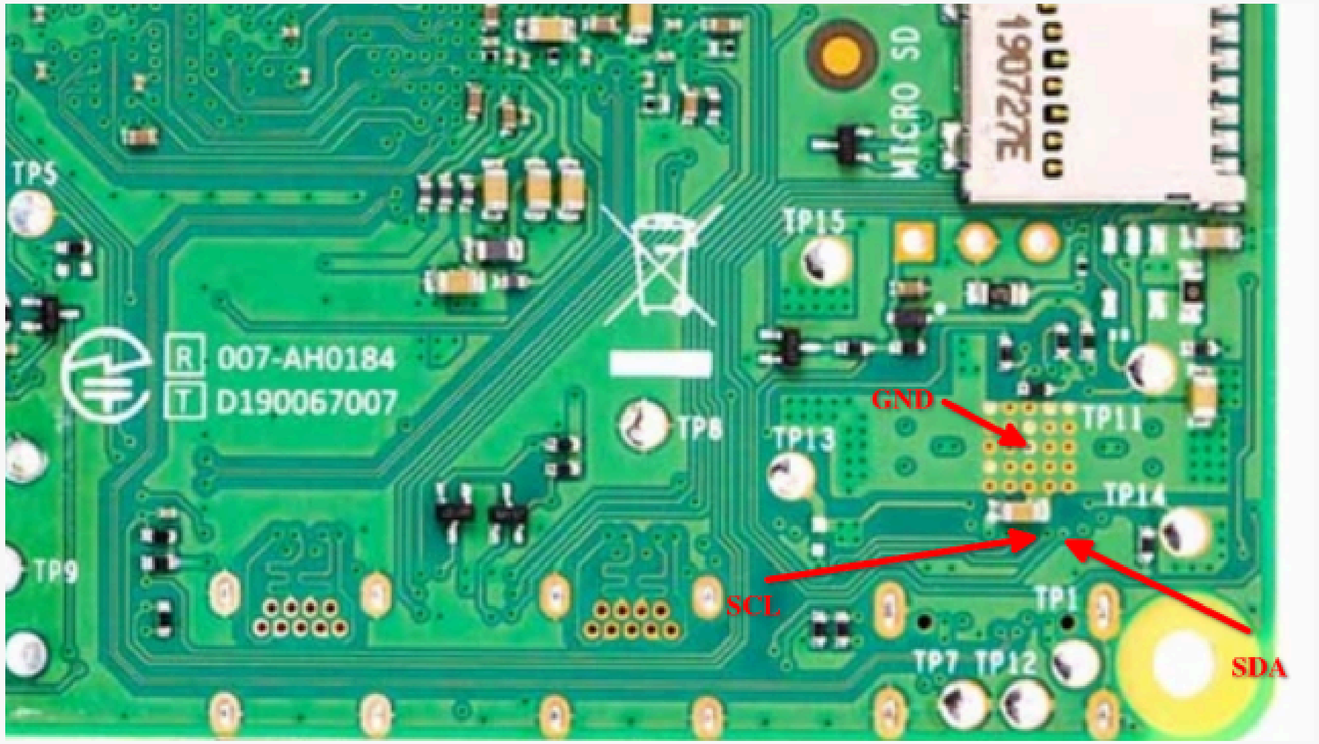


Tamper detection



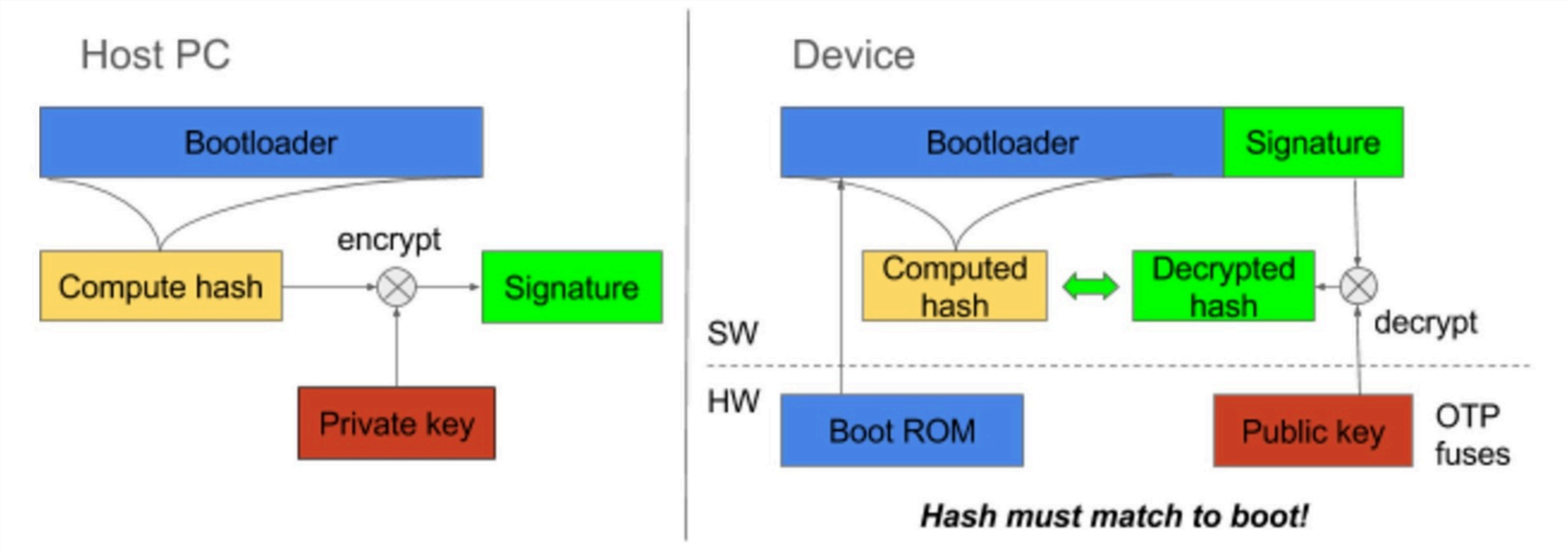
Remove chip mark

BEST PRACTICES



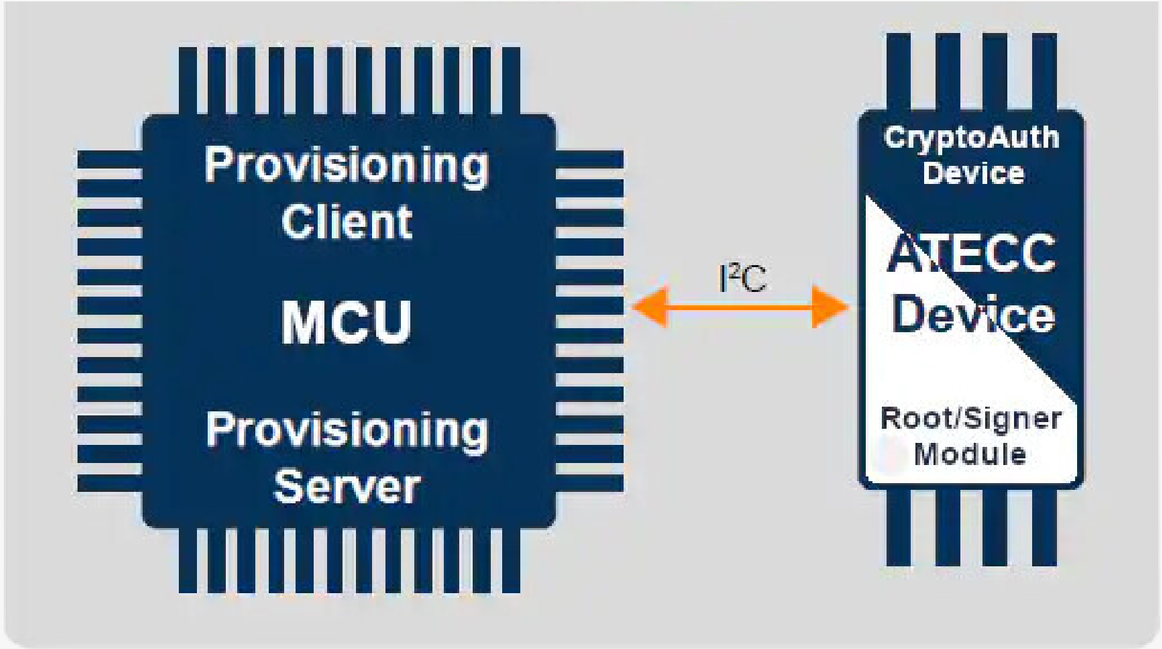
Remove silk screen and test point from PCB Board

BEST PRACTICES



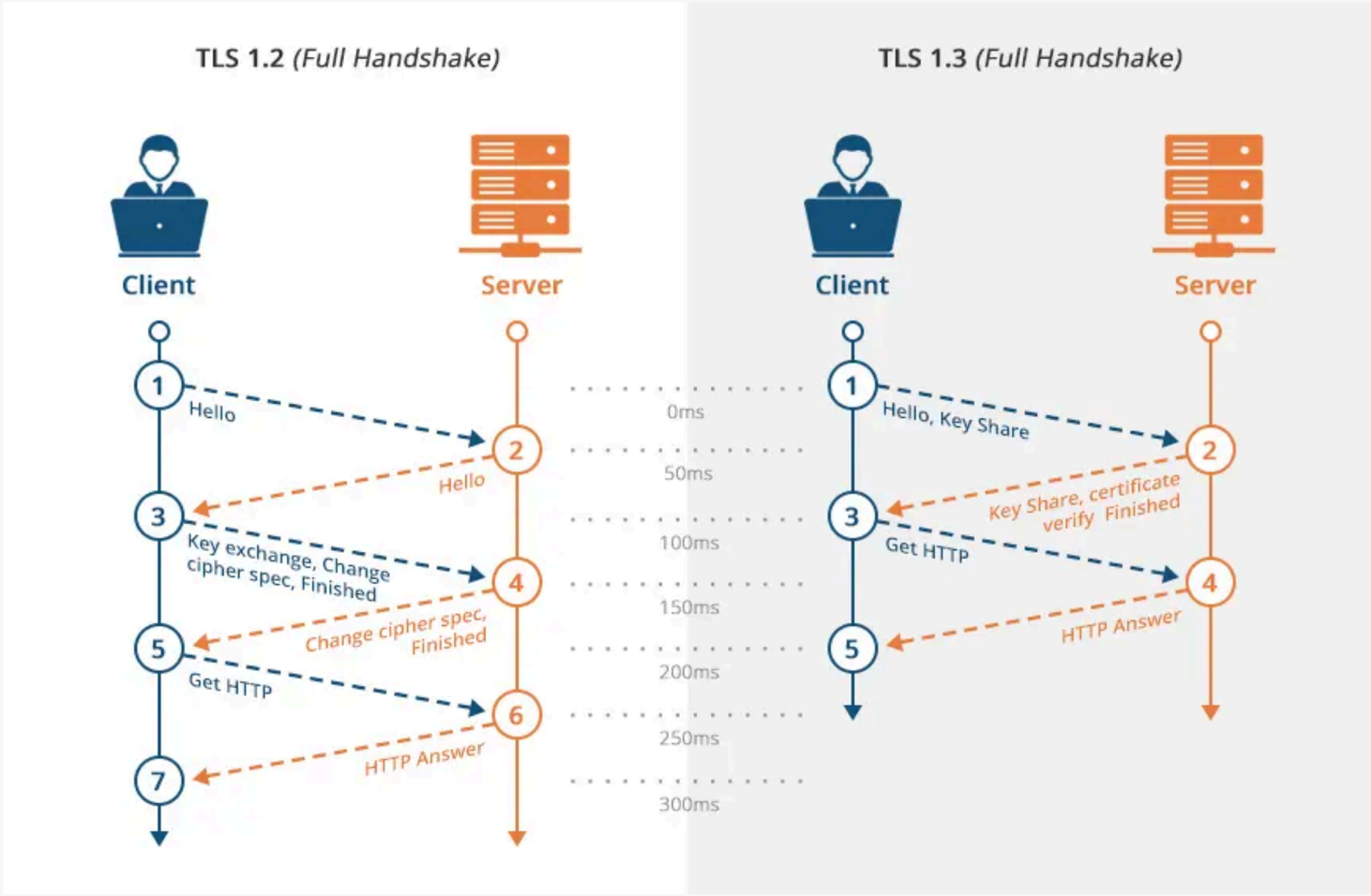
Secure boot and encrypt data storage

BEST PRACTICES



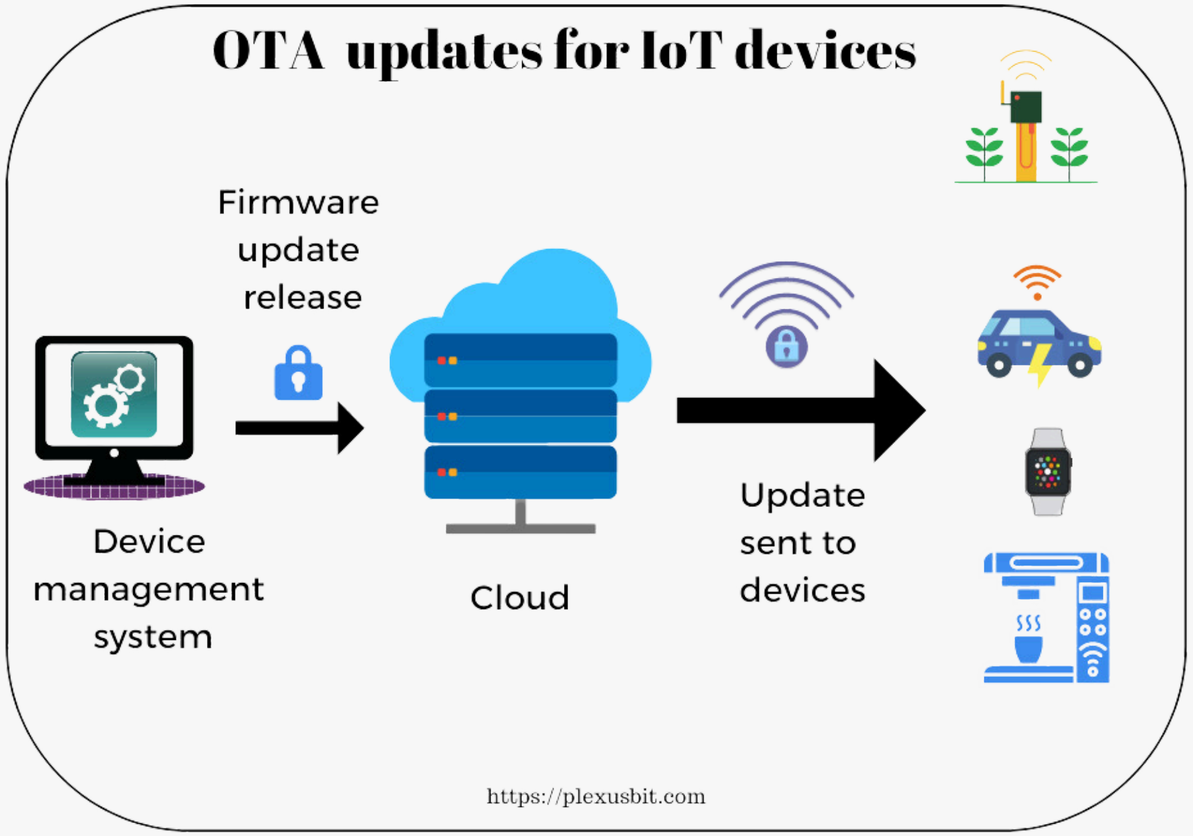
Using crypto Authentication chip

BEST PRACTICES



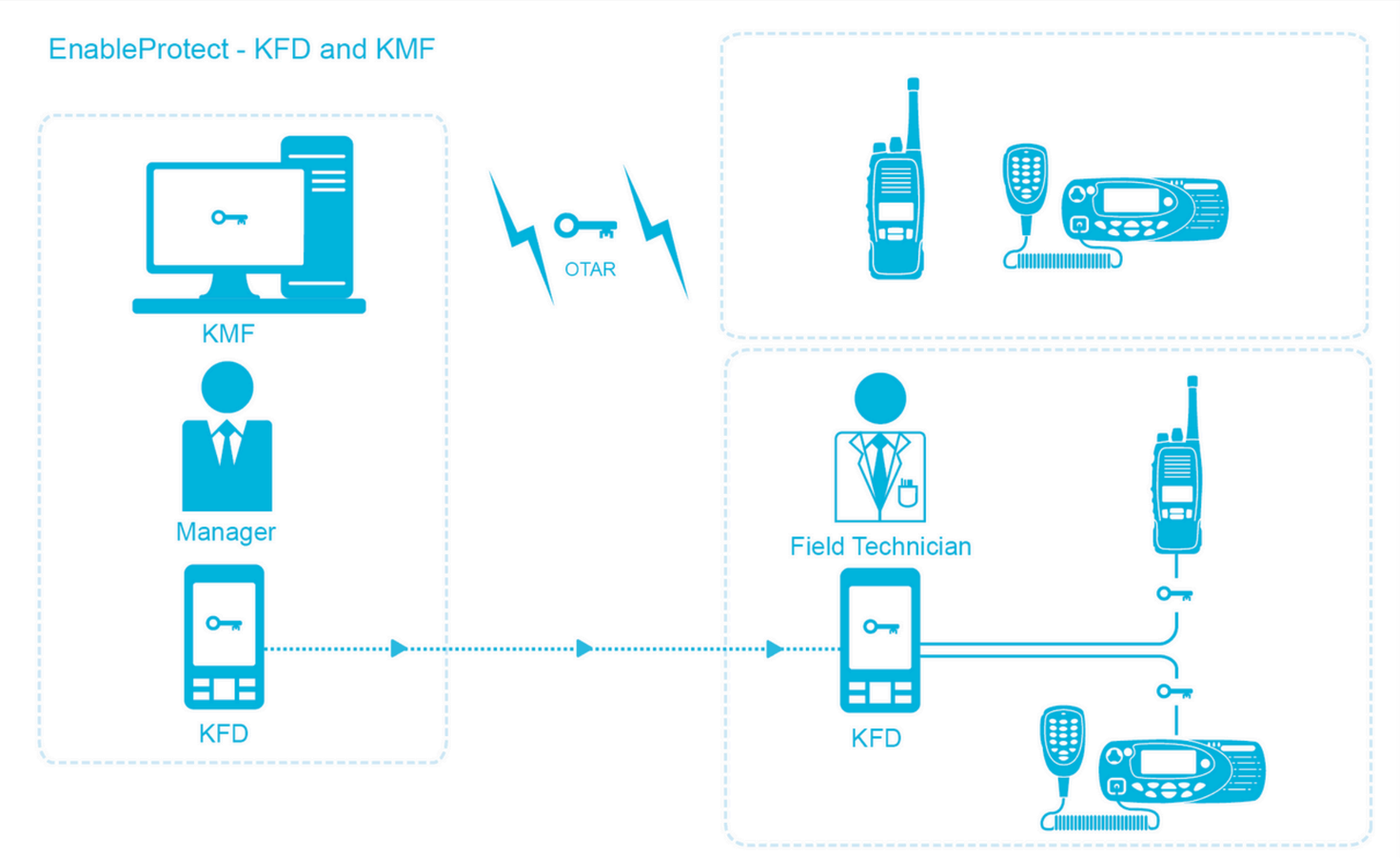
Using secure messaging protocol

BEST PRACTICES



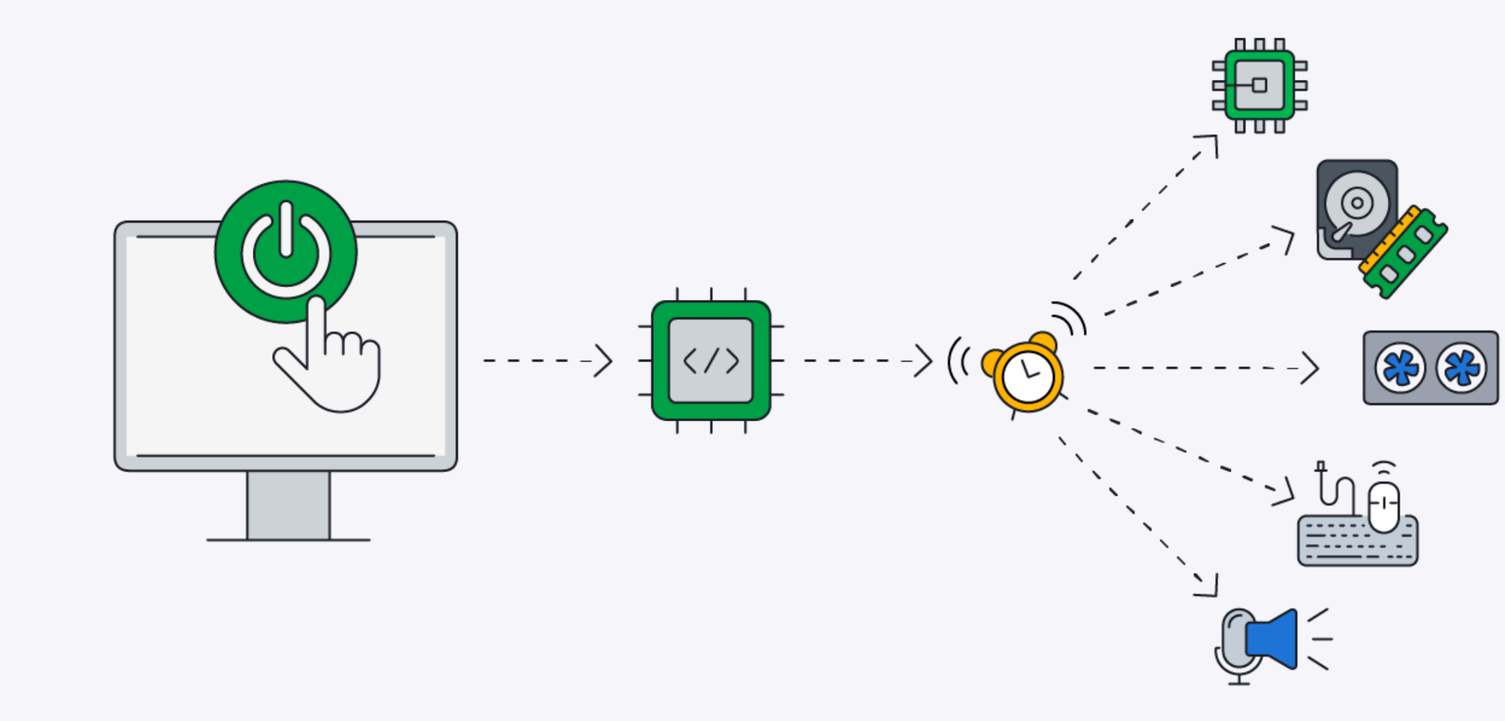
Secure OTA update

BEST PRACTICES



Encrypted Radio Communication Protocol

BEST PRACTICES



Chip architecture
Peripherals
Interrupts
RTOS
Memory Management
Test & Debug

THANK YOU

FOR COMING