DIGITAL WE DAYS 2024

A PRACTICAL APPROACH TO SECURE IOT SOLUTIONS
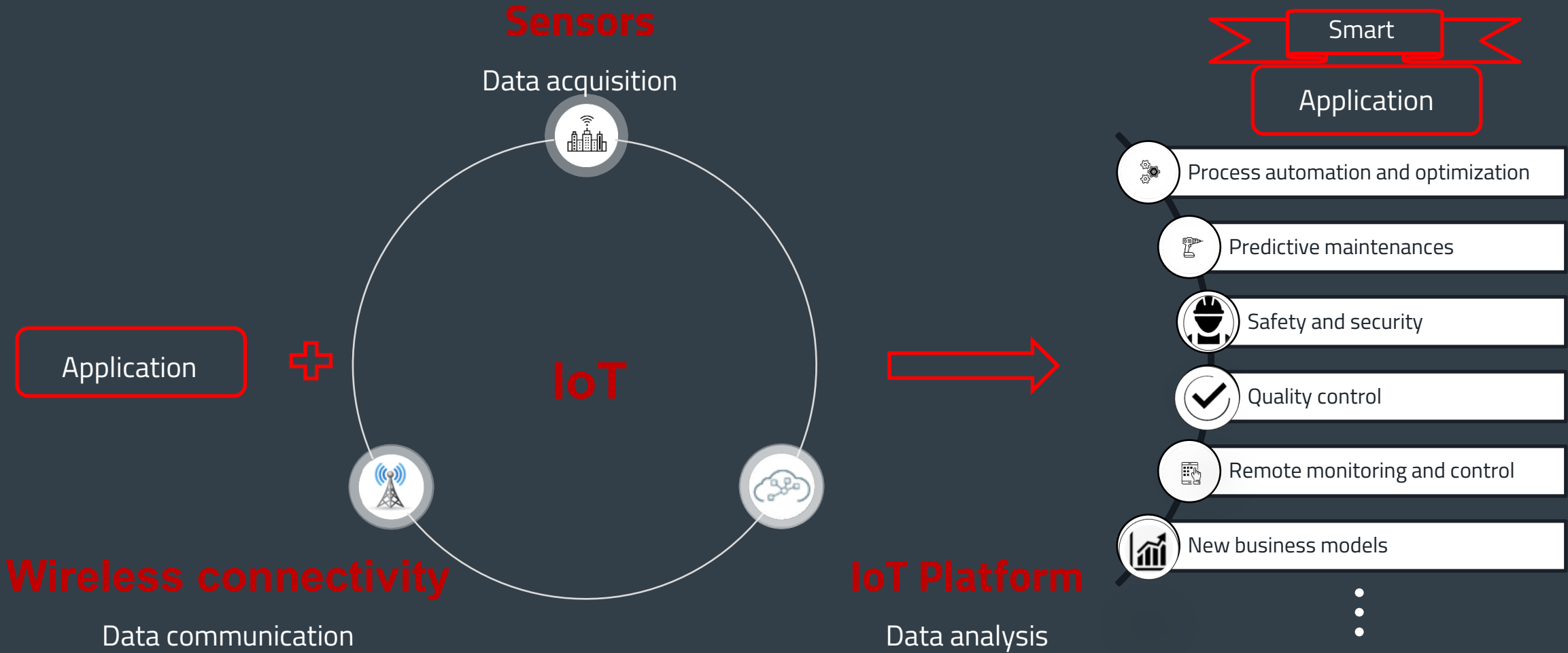
Pascal Baranger | Adithya Madanahalli

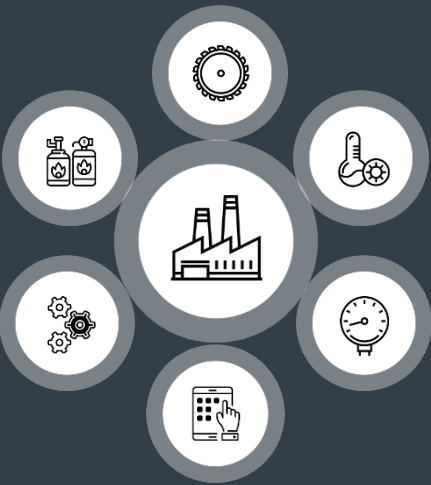**WÜRTH ELEKTRONIK** MORE THAN YOU EXPECT

AGENDA

- What is IoT?

- Components of an IoT System

- Cybersecurity in IoT

- Regulatory landscape – RED designated act on Cyber security

- Best practices for IoT

- Scalable & Secure cloud connectivity solution

- Rapid Prototyping tools

What is IoT?

IOT APPLICATION SIMPLIFIED

Sensors

Data acquisition

IoT

Application ➕

Wireless connectivity

Data communication

IoT Platform

Data analysis

Smart

Application

- Process automation and optimization
- Predictive maintenances
- Safety and security
- Quality control
- Remote monitoring and control
- New business models

WHAT IS AN IOT APPLICATION?

Industry + IoT = Smart industry

Farming + IoT = Smart farming

City + IoT = Smart city

Home + IoT = Smart home

Smart

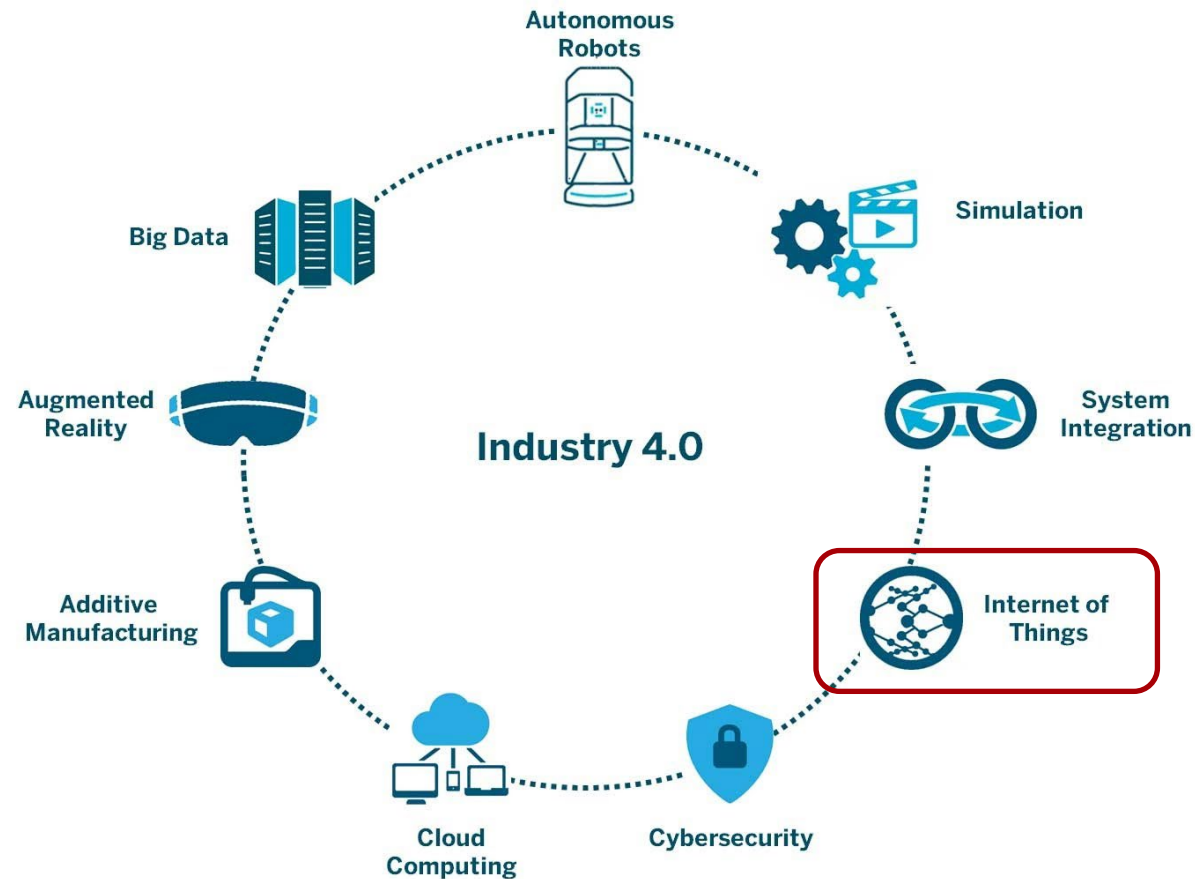Application ➕ IP Connectivity ➕ Data Platform ＝ IoT application
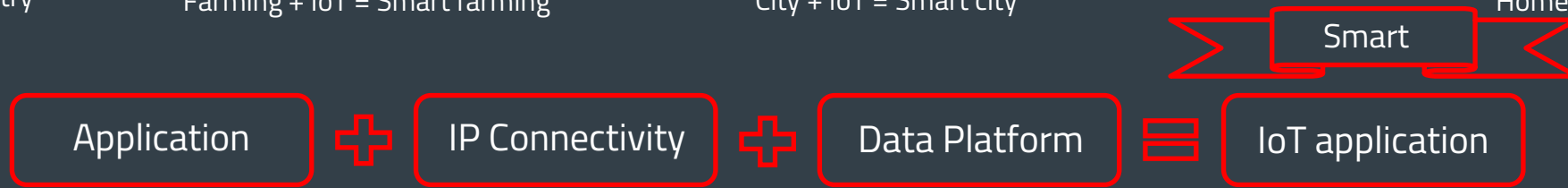
INDUSTRY 4.0

Source: Boston Consulting Group

The **Fourth Industrial Revolution**, **4IR**, or **Industry 4.0**,[1] conceptualizes rapid change to technology, industries, and societal patterns and processes in the 21st century due to increasing interconnectivity and smart automation. (Source: Wikipedia)

The **Internet of things** (**IoT**) describes physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network and be individually addressable. (Source: Wikipedia)

CONSTITUENTS OF AN IOT SYSTEM

User interface
- Data visualization
- Command and control

Data platform
- Data aggregation
- Data analysis
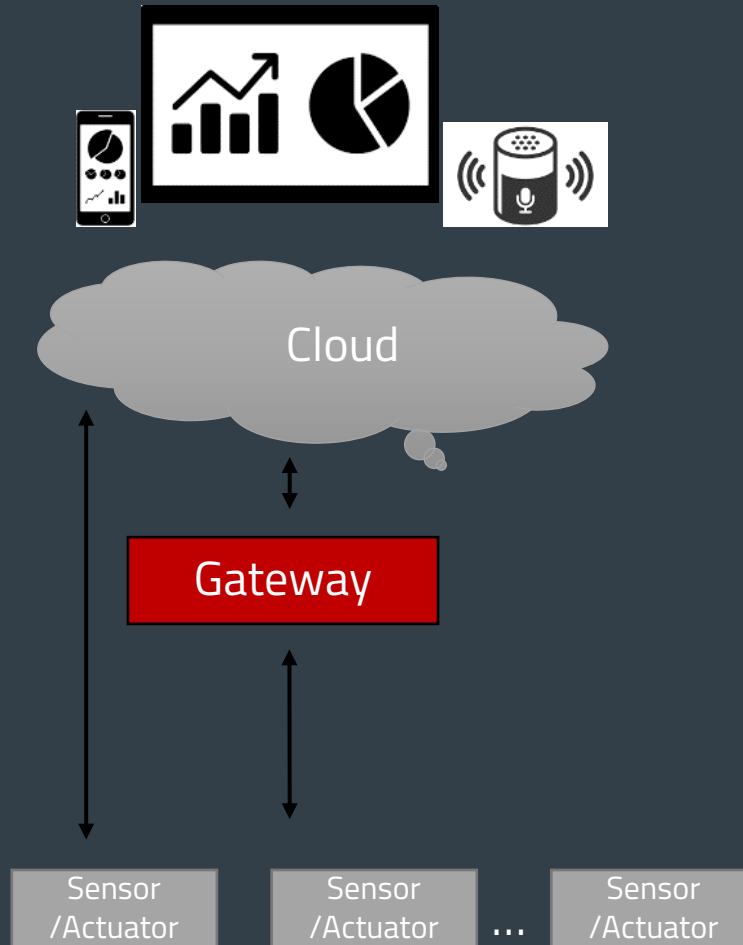- Data presentation

Gateway
- Bridge to the Internet
- Edge computing

Wireless connectivity
- Transfer data securely
- Flexibility and reachability

Sensors and actuators
- Measure physical environment
- Digitize measurements
- Actuate

Cloud

Gateway

Sensor /Actuator   Sensor /Actuator   …   Sensor /Actuator

Design considerations

Cloud domain
- High processing power
- Scalability
- Security
- Flexibility
- Data processing (AI & ML)

Security

Embedded domain
- Low processing power
- Small size
- Low power
- Higher range
- No/low installation effort
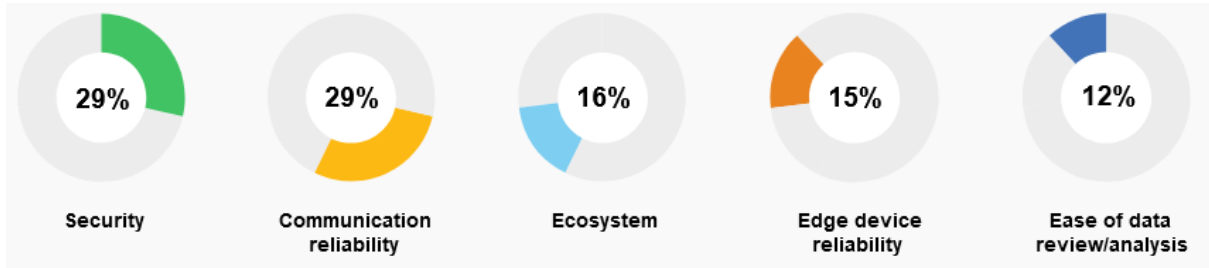
WE ASKED OUR CUSTOMERS

PROBLEM

Customers want (need) to connect their sensors, devices and machines, but don't know how.
They have no idea about connectivity, security and software and don't want to bother with it.
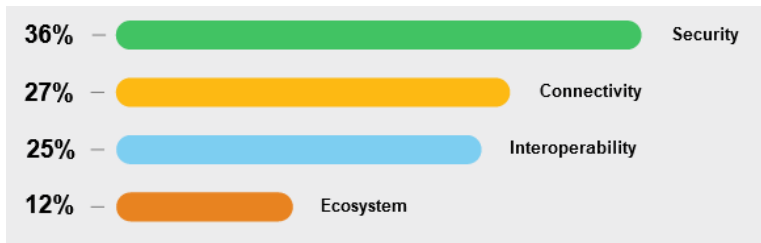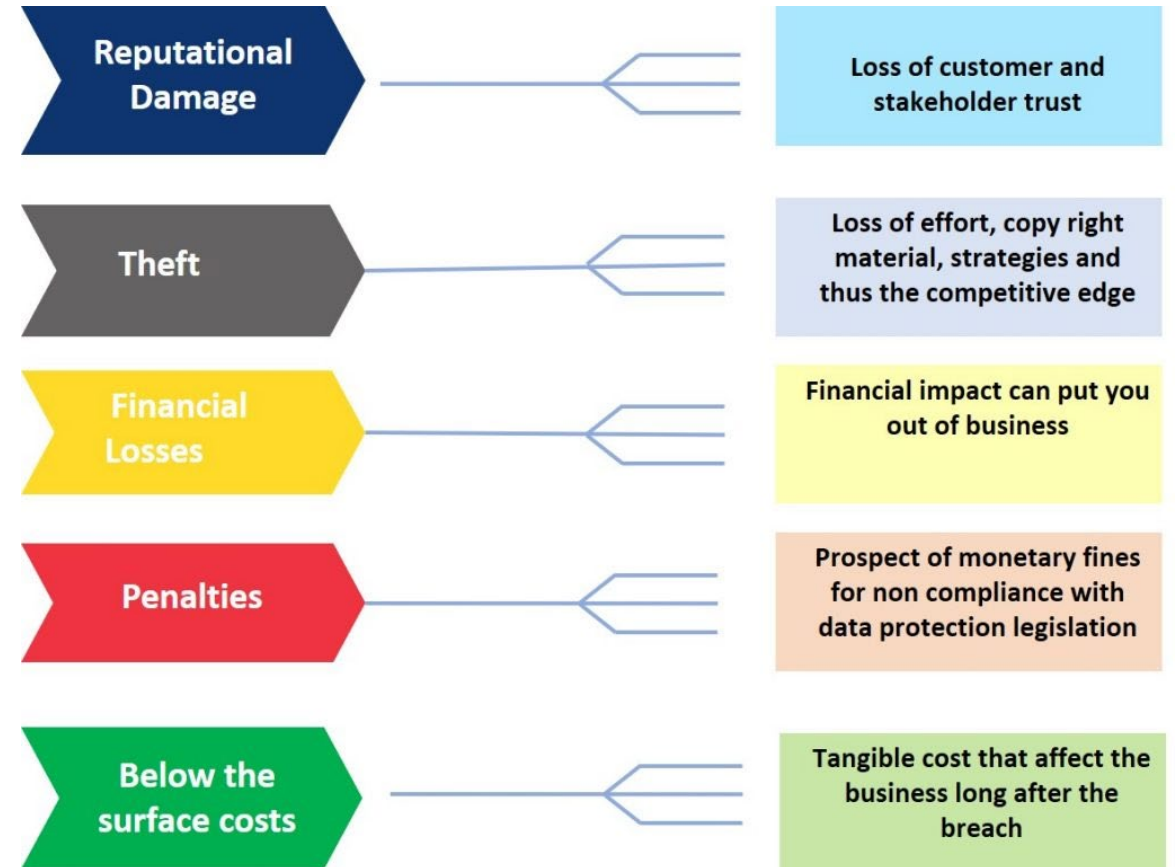
SURVEY TIME

What is the most important aspect to consider when developing IoT solutions?

29%	29%	16%	15%	12%
Security	Communication reliability	Ecosystem	Edge device reliability	Ease of data review/analysis

What is your key concern regarding IoT implementation?

- 36% — Security
- 27% — Connectivity
- 25% — Interoperability
- 12% — Ecosystem

Source: https://uk.farnell.com/iot-trends-2021

What are possible losses?

Reputational Damage → Loss of customer and stakeholder trust

Theft → Loss of effort, copy right material, strategies and thus the competitive edge

Financial Losses → Financial impact can put you out of business

Penalties → Prospect of monetary fines for non compliance with data protection legislation

Below the surface costs → Tangible cost that affect the business long after the breach

WHY SECURITY IN IIOT?
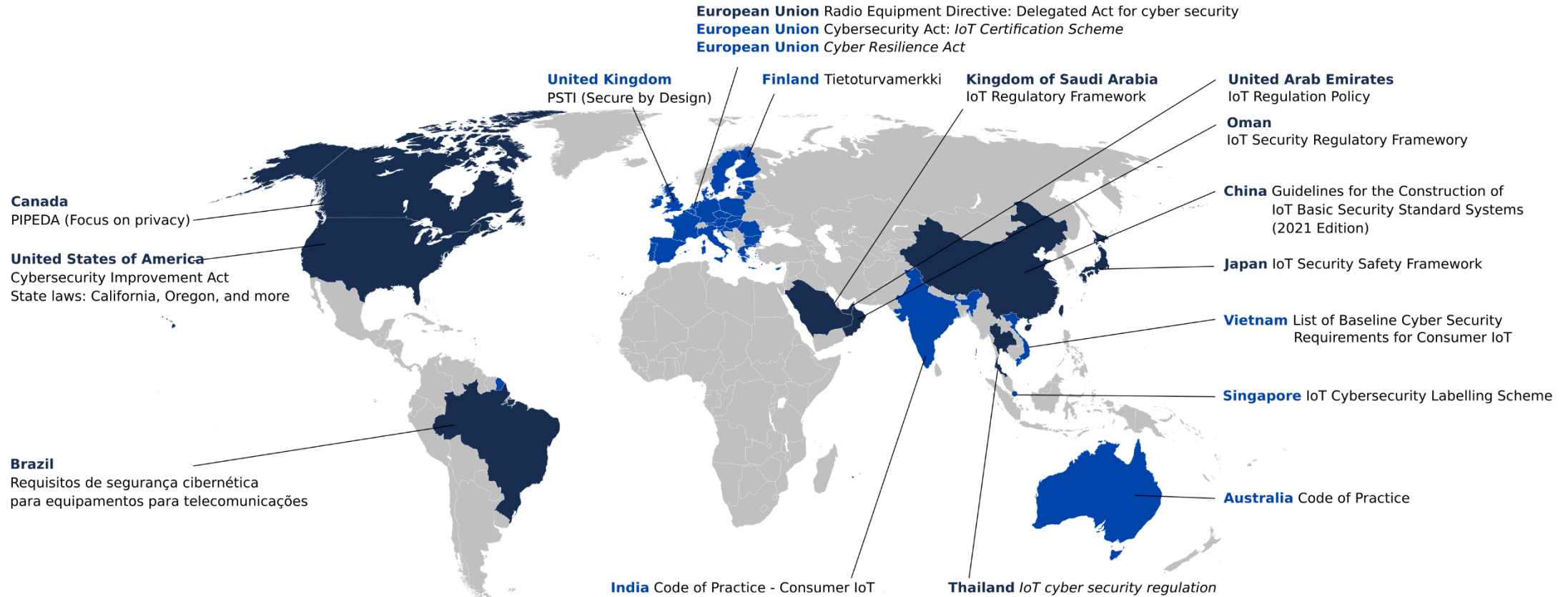
"The attackers used the smart water thermometer inside an aquarium to get a foothold in the network. They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud."

Hackers exploit casino's smart thermometer to steal database info

Nothing is safe.

By Kellen Beck on April 15, 2018

IOT REGULATORY LANDSCAPE

European Union Radio Equipment Directive: Delegated Act for cyber security
European Union Cybersecurity Act: *IoT Certification Scheme*
European Union *Cyber Resilience Act*

United Kingdom
PSTI (Secure by Design)

Finland Tietoturvamerkki

Kingdom of Saudi Arabia
IoT Regulatory Framework

United Arab Emirates
IoT Regulation Policy

Oman
IoT Security Regulatory Framewory

Canada
PIPEDA (Focus on privacy)

China Guidelines for the Construction of
IoT Basic Security Standard Systems
(2021 Edition)

United States of America
Cybersecurity Improvement Act
State laws: California, Oregon, and more

Japan IoT Security Safety Framework

Vietnam List of Baseline Cyber Security
Requirements for Consumer IoT

Singapore IoT Cybersecurity Labelling Scheme

Brazil
Requisitos de segurança cibernética
para equipamentos para telecomunicações

Australia Code of Practice

India Code of Practice - Consumer IoT

Thailand *IoT cyber security regulation*

Source – Cetome GitHub Repository :https://github.com/cetome/panorama

RADIO EQUIPMENT DIRECTIVE

- Officially "2014/53/EU" (Radio Equipment Directive – in short "RED") – Binding throughout European Economic area (EEA) since 13.06.2016

- Applicable to all radio equipment

Essential Requirements
3.1 a Health & Safety
3.1b EMC
3.2 Efficient use of radio spectrum
3.3 a to c Interoperability
3.3 d to f Cybersecurity

Added since 2021

RADIO EQUIPMENT DIRECTIVE

(3.3) Additional requirements Article based on categories of equipment

- (a) Compatibility with accessories
- (b) Interworking via networks with other radio equipment
- (c) EU-wide interconnection via interfaces of appropriate type
- (d) Network protection
- (e) Protection of personal data and privacy
- (f) Protection against fraud
- (g) Ensuring access to emergency services
- (h) Facilitating operation for people with disabilities
- (i) Ensuring software
- (j) Specification for the charging function

Jan 2022: Delegated regulation on Cybersecurity **2022/30/EU**, enforcing compliance requirements to RED Articles 3.3 (d), (e) and (f)

RED DELEGATED ACT FOR CYBERSECURITY

Subcomponent: Radio Module

3.3 d Network protection	• Prevent misuse of network leading to degradation of service • All devices which can **communicate over the internet directly or via an internet – connected device**	✓
3.3 e Data privacy	• Safeguards personal data and enhances privacy of the user • All devices that communicate **over the internet** and process **personal data, traffic data and/or location data**	✗
3.3 f Fraud protection	• Fraud protection • All devices which can communicate **over the internet directly or via an internet – connected device** that enables transfer of **money, monetary value or virtual currency**	✗

WE

TIMELINE

Jan 2022
- 2022/30/EU published
- Articles 3.3(d), (e) and (f) enforced

Feb 2022
Transition period activated

202?
Harmonized norm issued

202?
Articles 3.3(d), (e) and (f) Mandatory

Transition period?

No Harmonized norm => Likely to be postponed

Current deadline (already postponed once by 1 year) **1st August 2025**
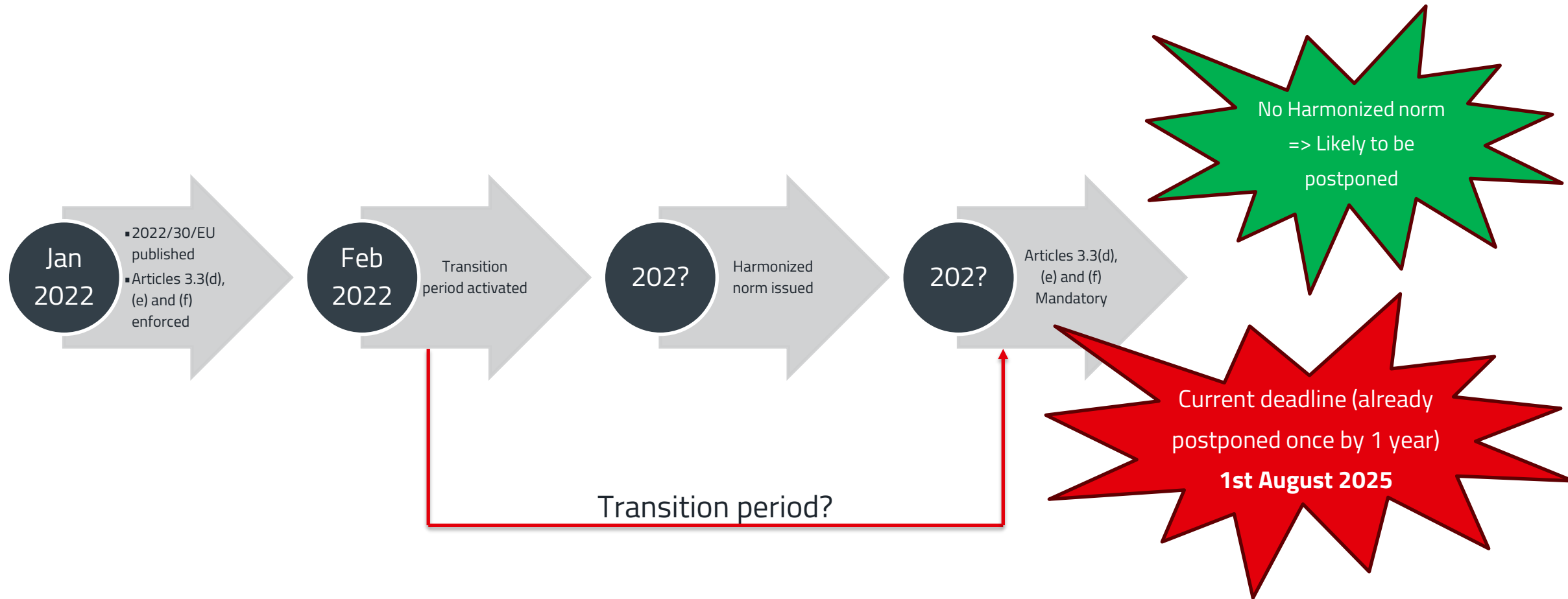
STATUS – HARMONIZED STANDARD

- **CEN/CENELEC** has been given the mandate to draw up the standards

- Three draft standards are currently circulating for comment among the parties involved.

  - 3.3 (d) -> EN 18031-1

  - 3.3 (e) -> EN 18031-2

  - 3.3 (f) -> EN 18031-3

DRAFT of EN 18031-1 was rejected by EU in January 2024
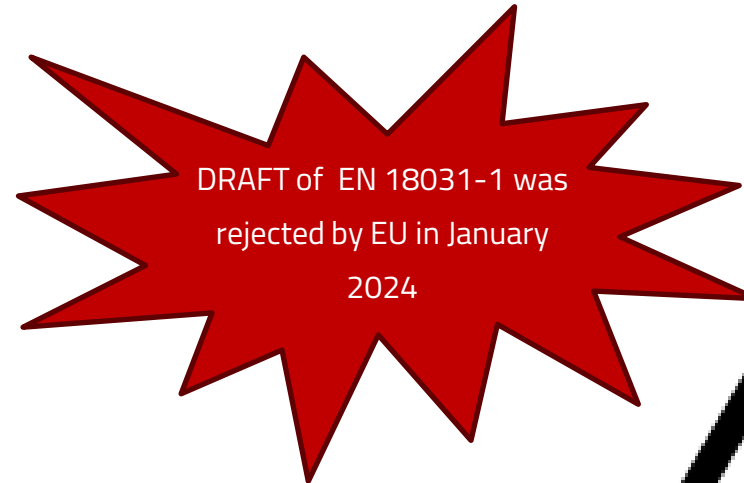
HOW TO BE COMPLIANT?
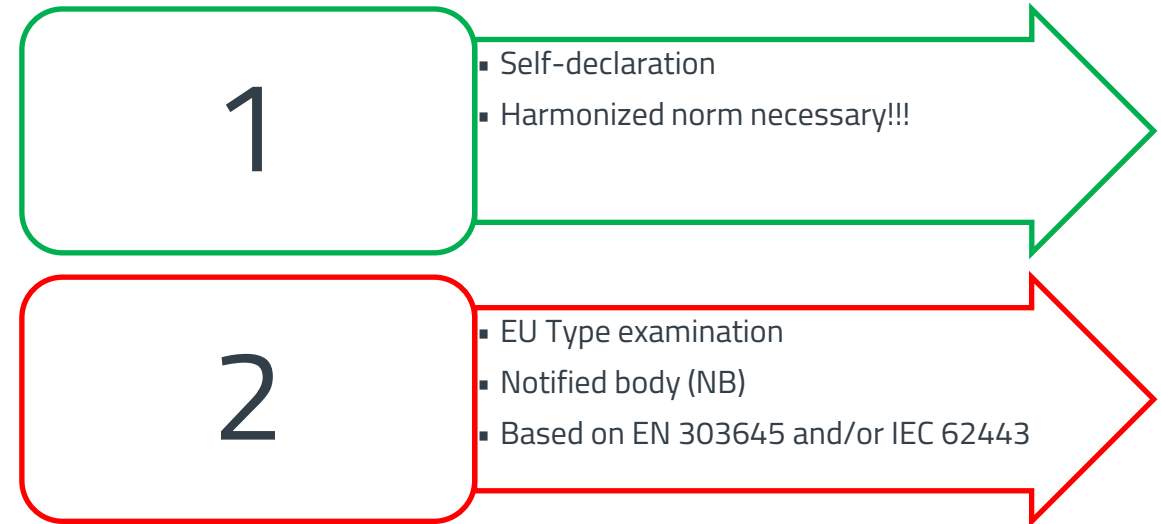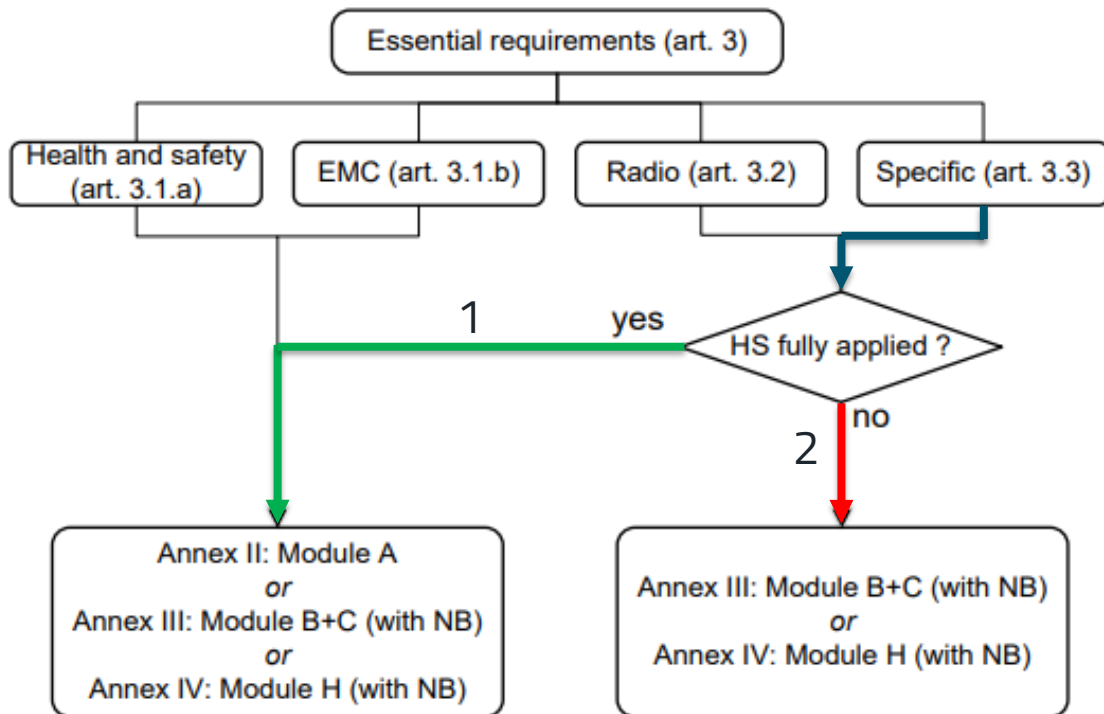
COMMON CYBERSECURITY SPECIFICATIONS

Software

- No universal default password
- Ensure that personal data is secure
- Validate input data

Hardware

- Securely store security parameters and sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity

Policies

- Implement a reporting system
- Keep software updated
- Examine telemetry data
- Make it easy to delete user data
- Make installation and maintenance easy
- Explain content and purpose of personal data stored

DESIGNING A SECURITY CONCEPT FOR AN EMBEDDED DEVICE

Common minimum-security requirements for IIoT device
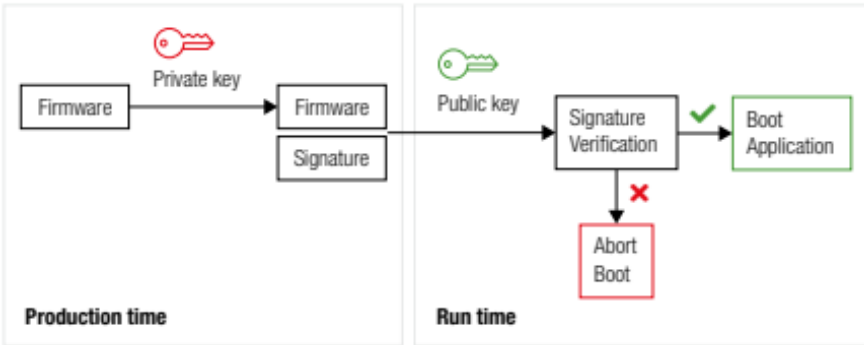
Secure production

Secure boot
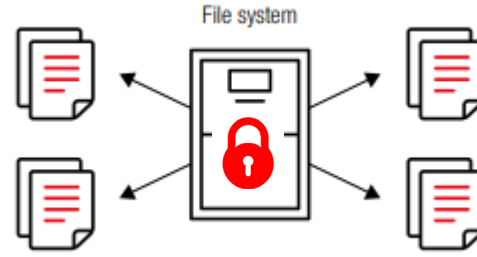
Secure storage
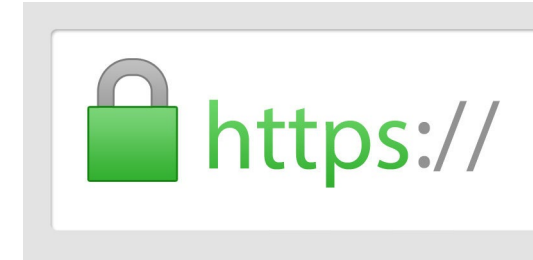
Secure connection

Secure root of trust
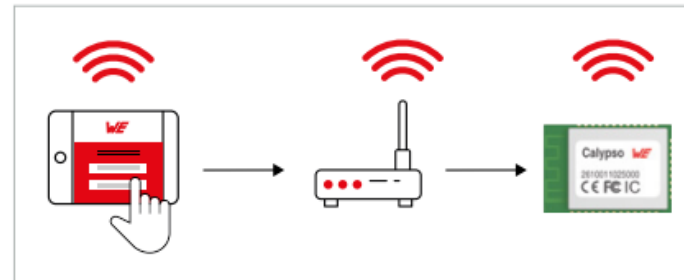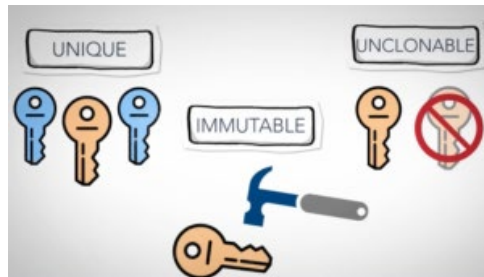
Secure FOTA

Security by design not an afterthought!

CALYPSO WI-FI MODULE

Secure IoT ready

- ✓ 10 byte non-tamperable unique device ID

- ✓ Secure boot

- ✓ Secure storage – Encrypted file system to store certificates and other credentials

- ✓ Secure Wi-Fi connection – WPA3

- ✓ Secure socket – TLSv1.2

- ✓ Hardware accelerated crypto engine

- ✓ Secure Firmware over the air update
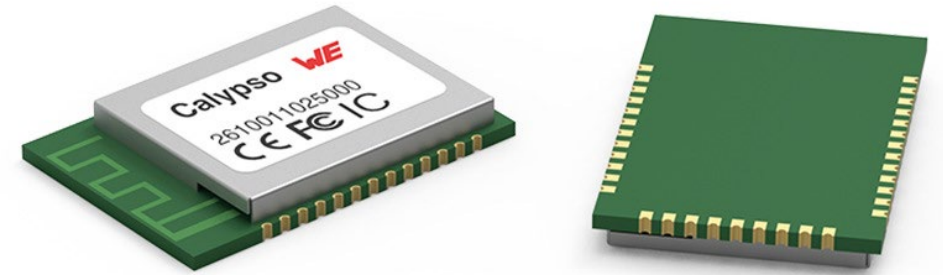
A good basis for secure end application !!!
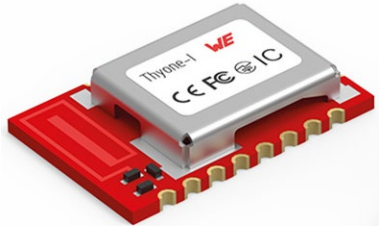
PROTEUS-III BLUETOOTH® LE 5.1 MODULE

Secure IoT ready

✓ Non-tamperable unique device ID

✓ Secure boot

✓ Secure BLE connection - LESC

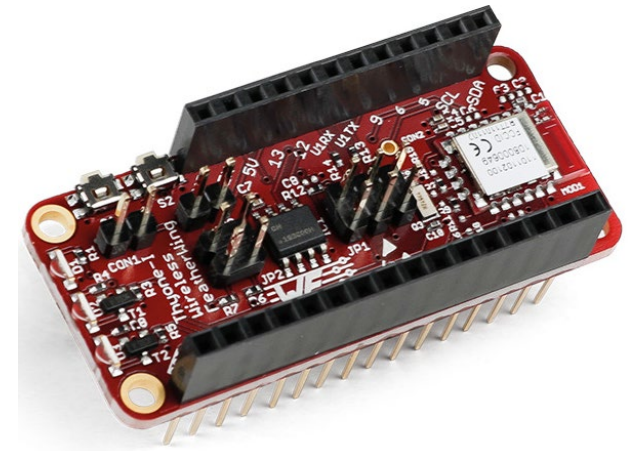✓ Hardware accelerated crypto engine

✓ Secure Firmware over the air update

A good basis for secure end application !!!

THYONE-I WIRELESS MODULE

Secure IoT ready

+

Microchip

ATECC608B

→

CE FC IC ⊕

2.4 GHz Proprietary
Wireless connectivity

Cryptographic co-processor

IIoT ready wireless
connectivity

- Nano SIM size
- Low power
- Range up to 750 m
- Broadcast, Multicast , Unicast
- Mesh capable

- 72 bit UDID
- Secure key storage
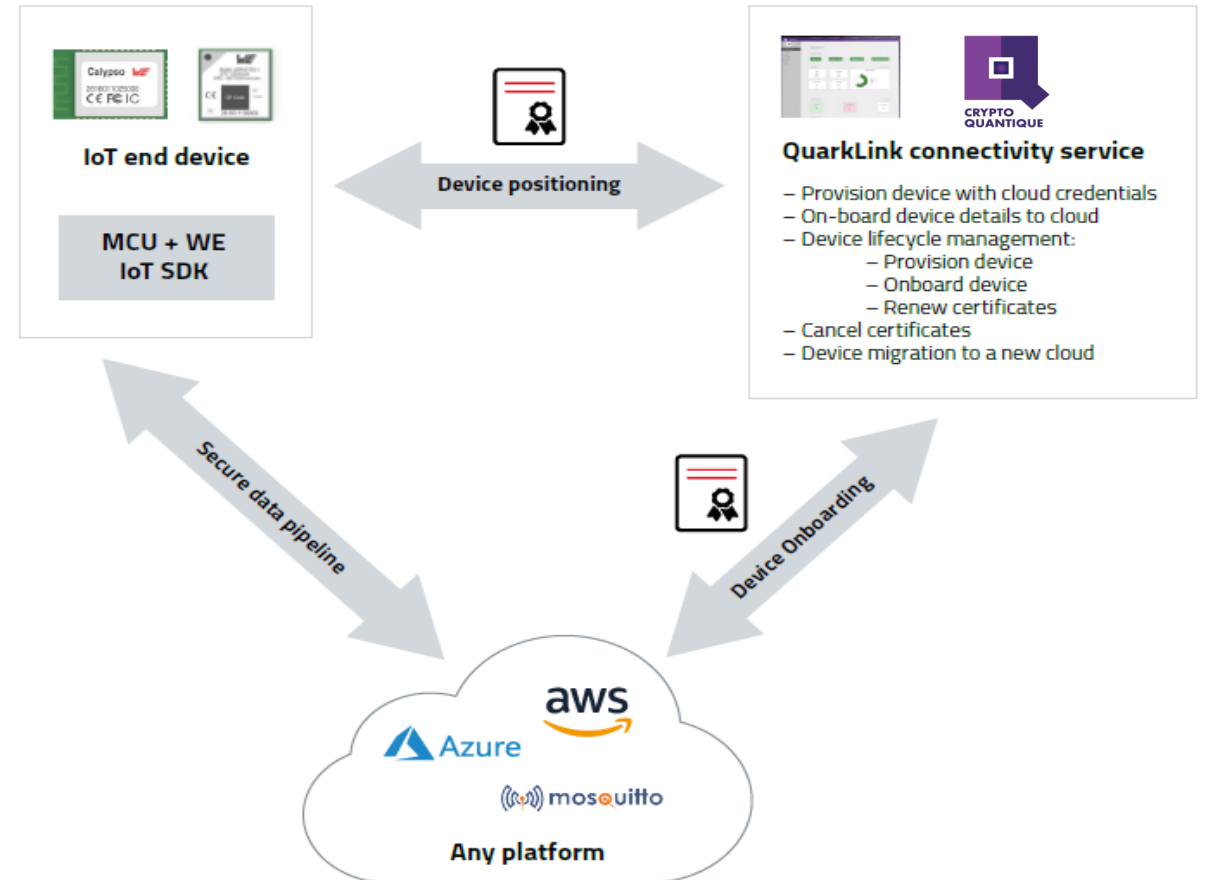- AES-128
- SHA256
- ECDH, ECC
- Secure boot

A good basis for secure end application !!!

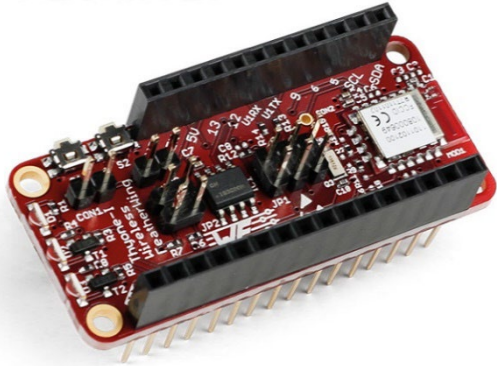# ZERO TOUCH SECURE – CLOUD CONNECTIVITY

- Secure and scalable cloud connectivity

- HW/SW Platform independent

- Real time provisioning and on-boarding in the field

- Zero-trust supply chain

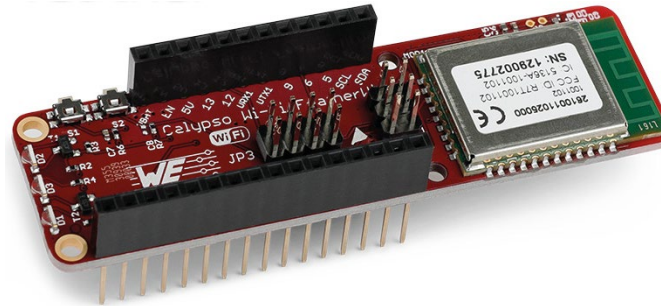- Complete Device life cycle management

- Secure by design!

IoT end device

MCU + WE
IoT SDK

Device positioning

QuarkLink connectivity service
- Provision device with cloud credentials
- On-board device details to cloud
- Device lifecycle management:
    - Provision device
    - Onboard device
    - Renew certificates
- Cancel certificates
- Device migration to a new cloud

Secure data pipeline

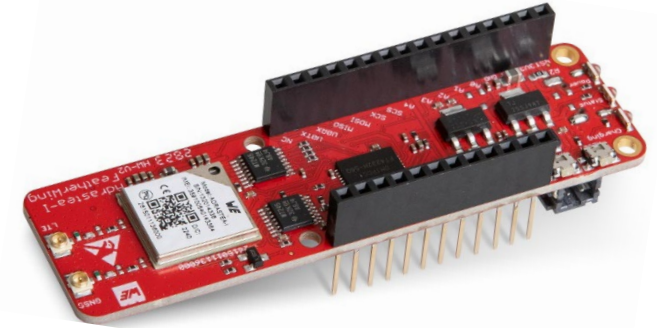*Device Onboarding*

aws
Azure
mosquitto
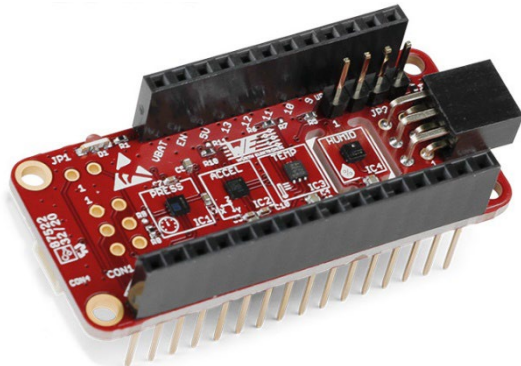**Any platform**

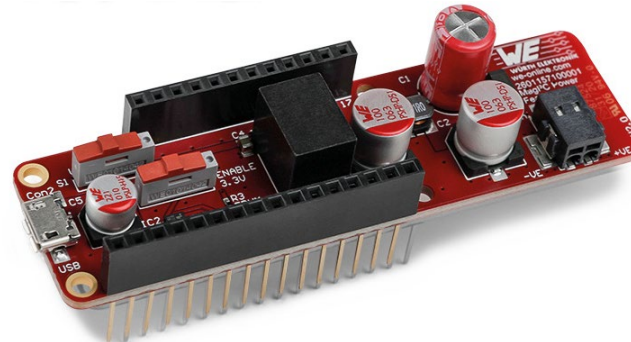2.4GHz Radio FeatherWing
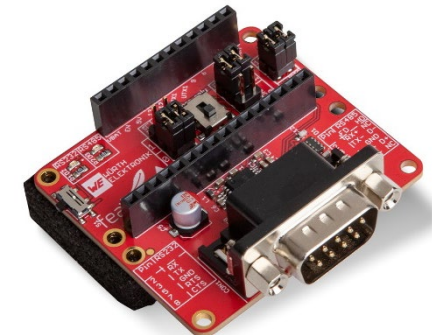
WiFi FeatherWing

Cellular FeatherWing

Sensor FeatherWing

Industrial Power Supply FeatherWing

RS232/RS485 FeatherWing

Very common and well developed **prototyping standard**!

PRACTICAL EXAMPLE USING CALYPSO IOT KIT

Solution – The engineer's way

Würth Elektronik eiSos offers a secure and high-performance solution for **rapid prototyping**, from the **sensor to the cloud**, that takes the customer by the hand and connects their devices and machines simply, securely and time-efficiently.

WE take care of IoT so that the customer can focus on his/her application.

Interested?
Check out our Wi-Fi Calypso IoT Design Kit!

LIVE DEMO:
YouTube – Würth Elektronik Group –
"How to get started with the
Microsoft Azure Certified Calypso IoT Design Kit?"

https://www.youtube.com/watch?v=d7C_oA74eXU

Questions

& Answers

We are here for you now!
Ask us directly via our chat or via E-Mail.

digital-we-days@we-online.com
wcs@we-online.com