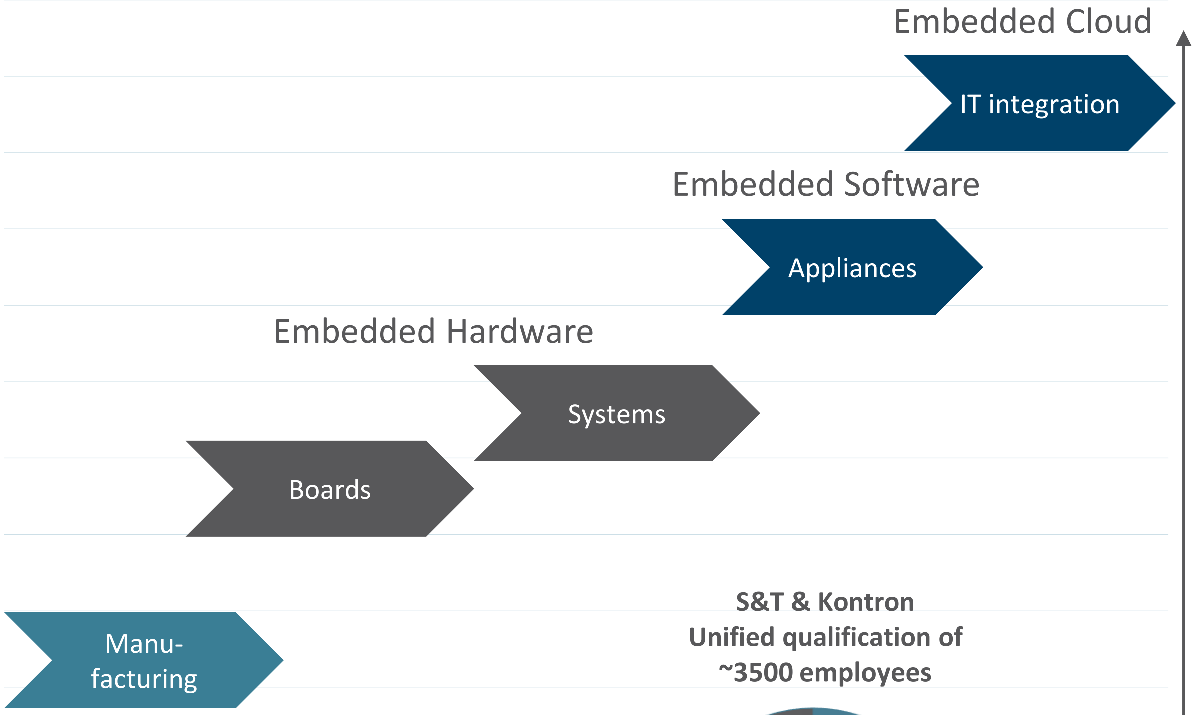
Securing LoRa™ Networked Rail IoT Systems

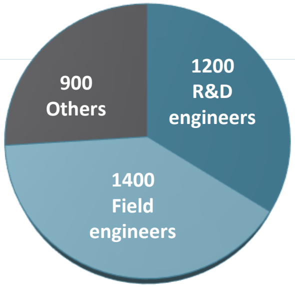
Valentin Scinteie

Transportation Business Development Manager, Kontron America

WHO WE ARE
E2E IOT SOLUTIONS FROM EDGE TO CLOUD TO ENTERPRISE



S&T & Kontron
Unified qualification of
~3500 employees



s&t

- Application Software (1800 Engineers)
- Security SW for IoT solutions and private cloud offering
- IoT head end Systems – Embedded Cloud

kontron

- Installed base > 4 Mio. embedded Computers (operating)
- Strong embedded computer portfolio
- Security SW for IoT solutions and private cloud offering

Innoconn
An Innovative Foxconn Member

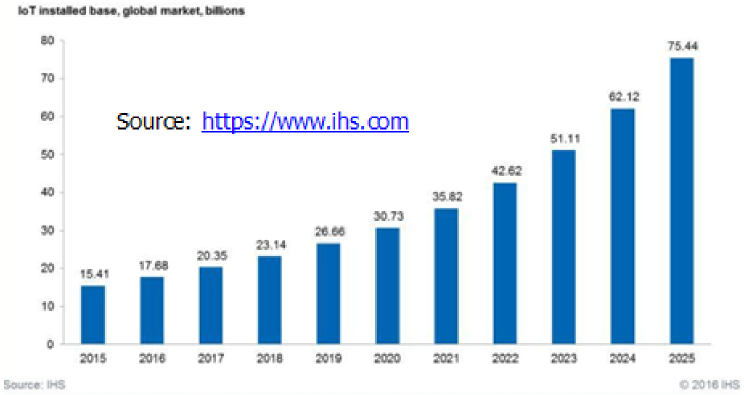
- #1 electronic assembly
- Strong Hardware Engineering
- Leader in Server farms (embedded Cloud)

Agenda

- IoT LPWAN Networks
- LoRa^{TM}
- Rail Use Case
- Network Security Considerations

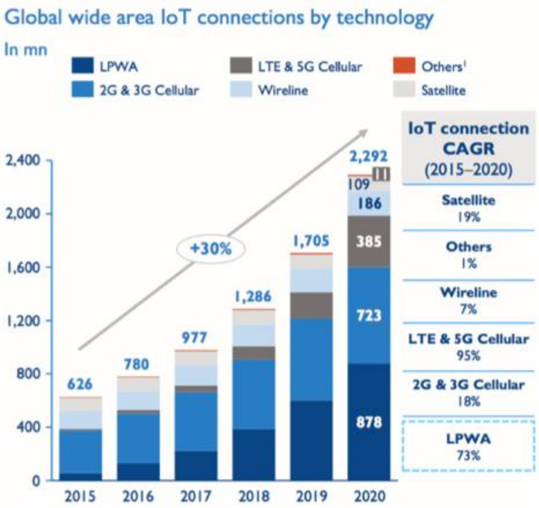
GENERAL CONTEXT OF IOT TODAY

- The world is all about being connected
  - About 20 billion devices today
  - 75 billion of devices forecasted for 2025



Source: https://www.ihs.com

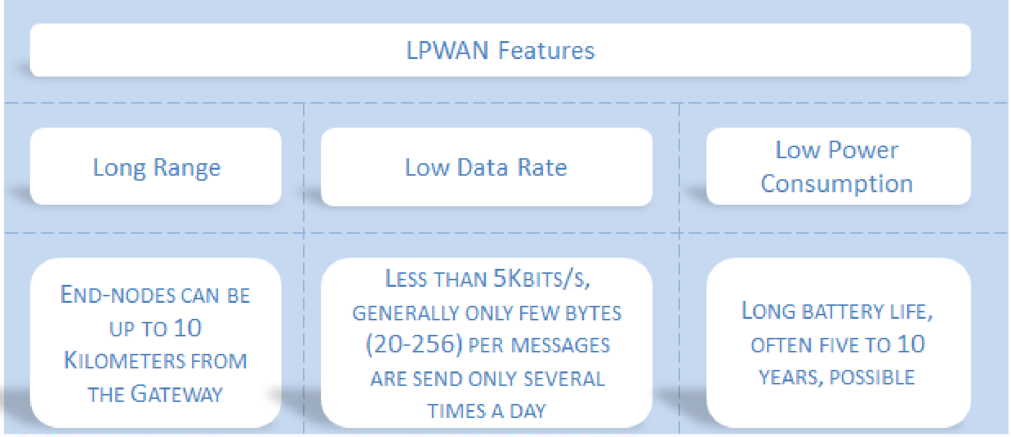
- +30% CAGR total growth all technologies
- +73% CAGR for connected objects using LPWA (Low-Power Wide-Area)



Source: SNS Research, Arthur D. Little

CONNECTED OBJECTS USING LPWA TECHNOLOGY ARE GROWING VERY FAST

WHAT IS A LPWAN (Low Power Wide-Area Network)?



LPWAN Features

Long Range

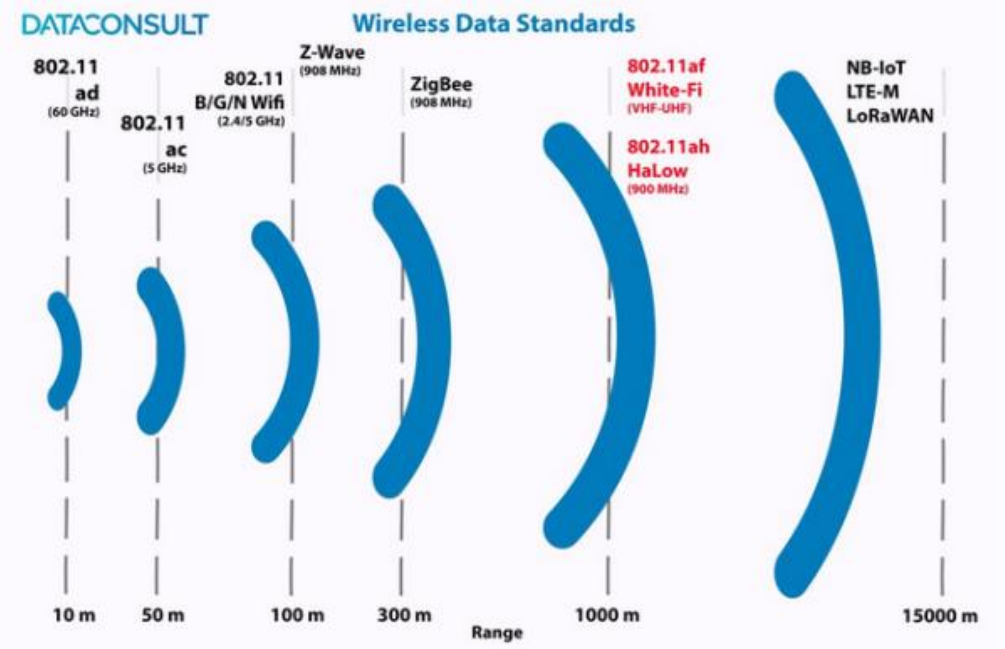
Low Data Rate

Low Power Consumption

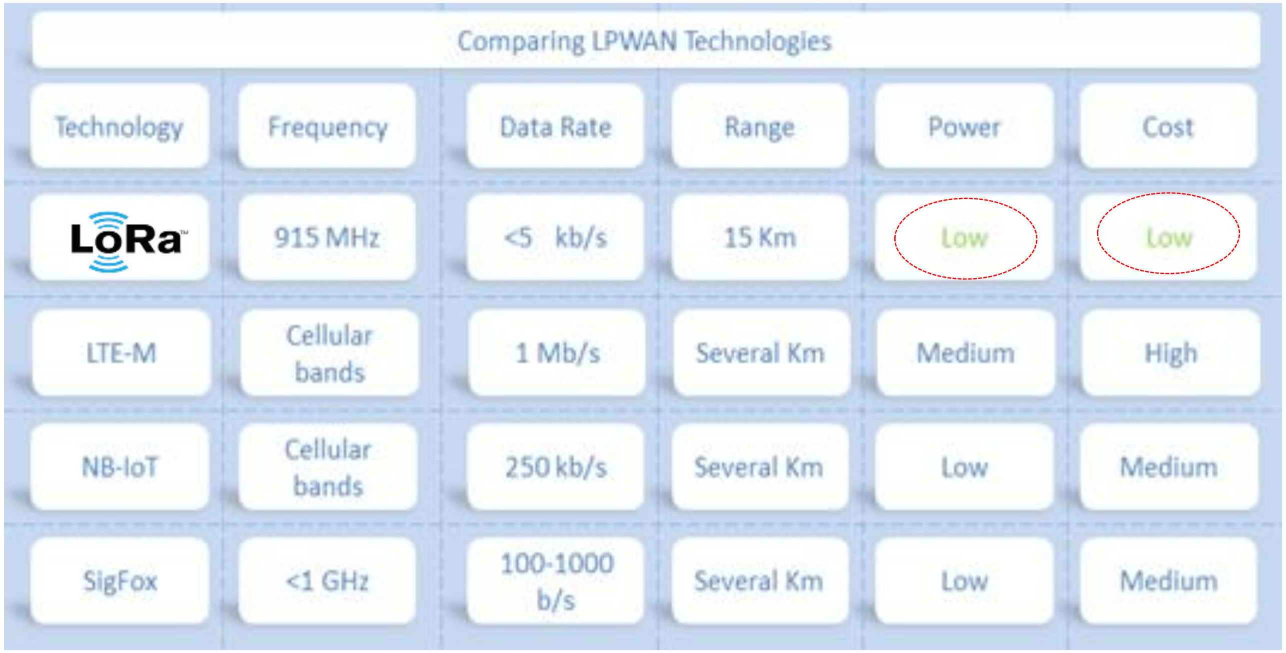
End-nodes can be up to 10 Kilometers from the Gateway

Less than 5Kbits/s, generally only few bytes (20-256) per messages are send only several times a day

Long battery life, often five to 10 years, possible



WHAT IS A LPWAN (LOW POWER WIDE-AREA NETWORK)? HOW TO CHOOSE THE RIGHT TECHNOLOGY?



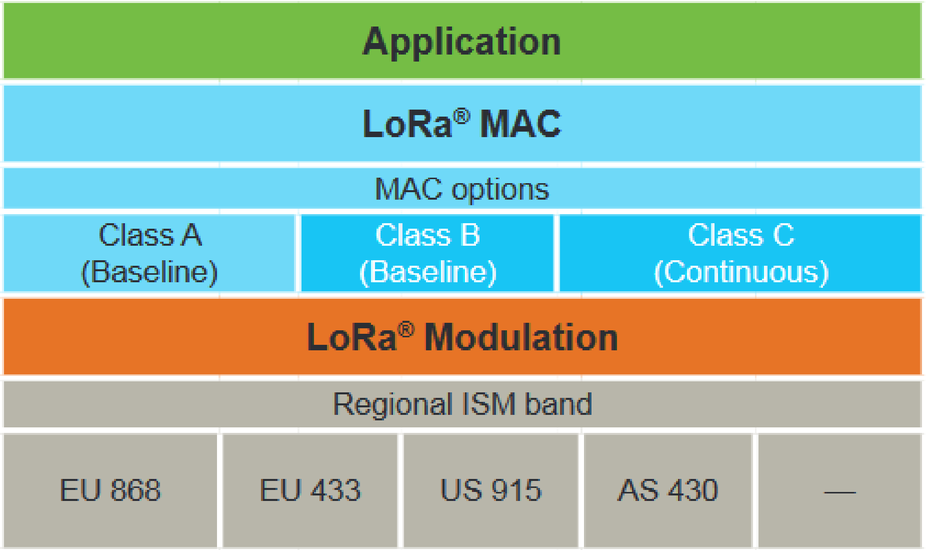
Comparing LPWAN Technologies

Technology	Frequency	Data Rate	Range	Power	Cost
LoRa	915 MHz	<5 kb/s	15 Km	Low	Low
LTE-M	Cellular bands	1 Mb/s	Several Km	Medium	High
NB-IoT	Cellular bands	250 kb/s	Several Km	Low	Medium
SigFox	<1 GHz	100-1000 b/s	Several Km	Low	Medium

- TCO (Total Cost of Ownership)
  - LoRa^{TM} free band, free use model
  - Cellular model
  - Operator model

WHAT IS LoRaWAN™ VS LoRa™

- LoRaWAN™ defines the communication protocol and system architecture
- LoRa® defines the physical layer to enable the long-range communication link



Application

LoRa® MAC

MAC options

Class A (Baseline) | Class B (Baseline) | Class C (Continuous)

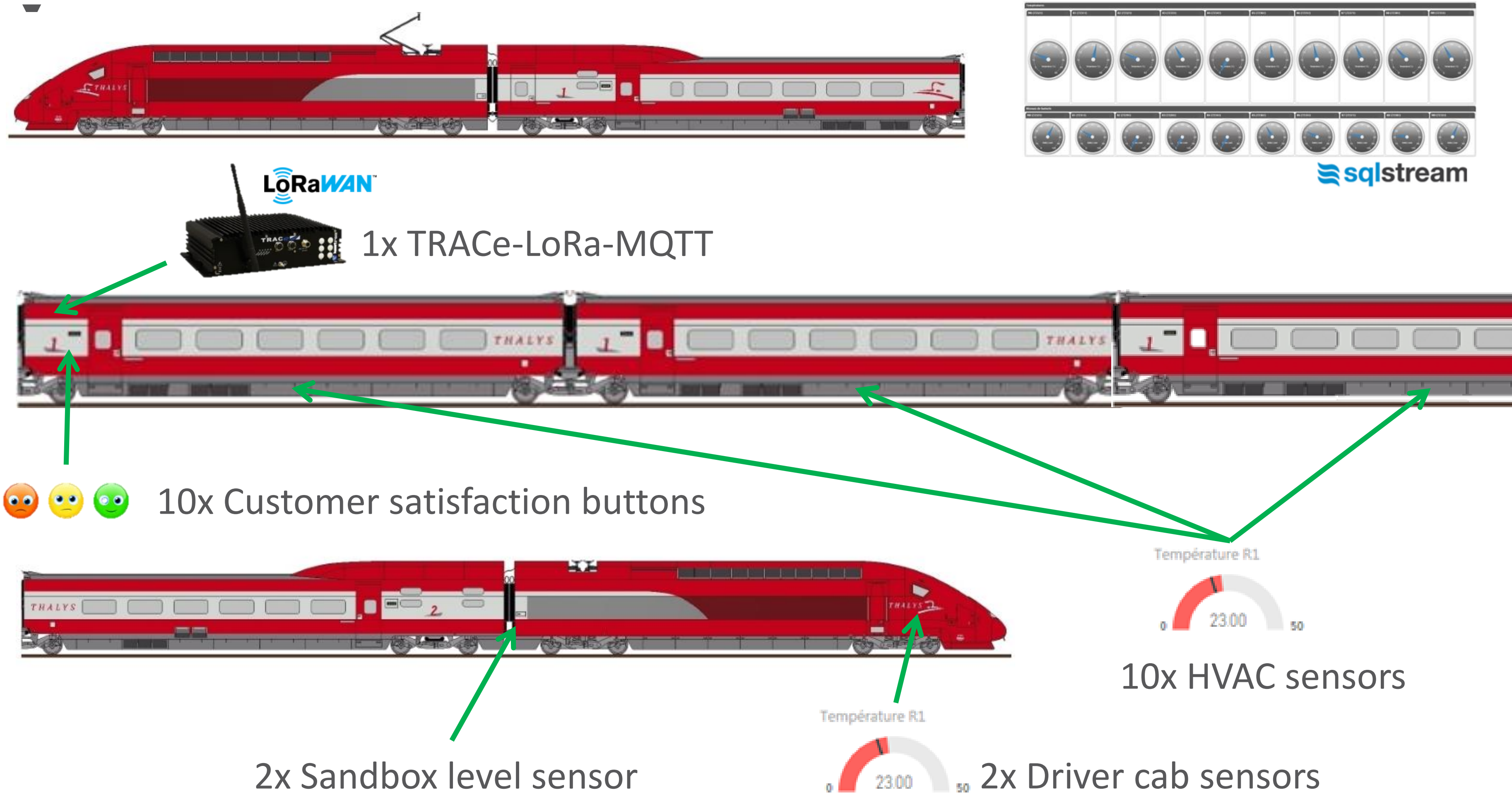
LoRa® Modulation

Regional ISM band

EU 868 | EU 433 | US 915 | AS 430 | —

Class A: Bi-directional communications. Uplink Tx is followed by 2 downlink Rx windows
Class B: In addition to the Class A (random Rx) windows, devices open extra Rx windows at scheduled times.
Class C: nearly continuously open Rx windows, only closed when transmitting

USE CASE: HIGH SPEED TRAIN



1x TRACe-LoRa-MQTT

10x Customer satisfaction buttons

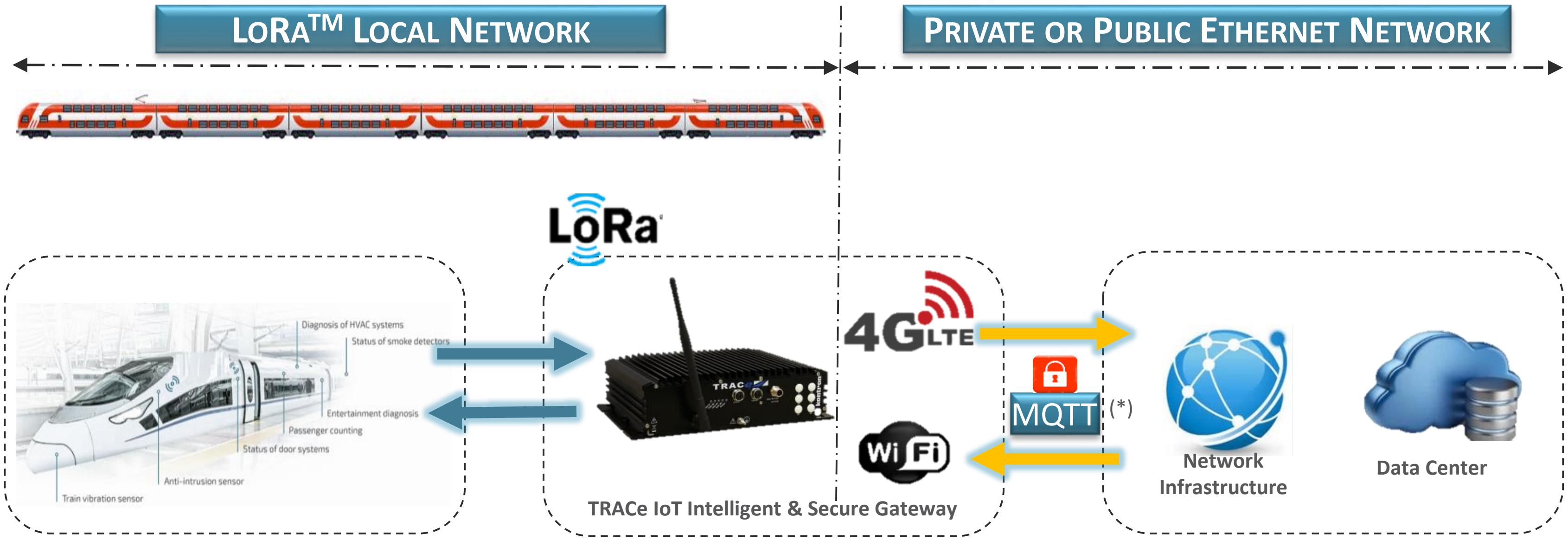
10x HVAC sensors

2x Sandbox level sensor

2x Driver cab sensors

Wireless data communication proven up to 300Km/h

USE CASE: HIGH SPEED TRAIN



- Vibration sensors
- Door diagnostic sensors
- Emotions button
- Passenger counting
- Smoke/ Fire detection
- Energy consumption sensor
- Tank levels
- …

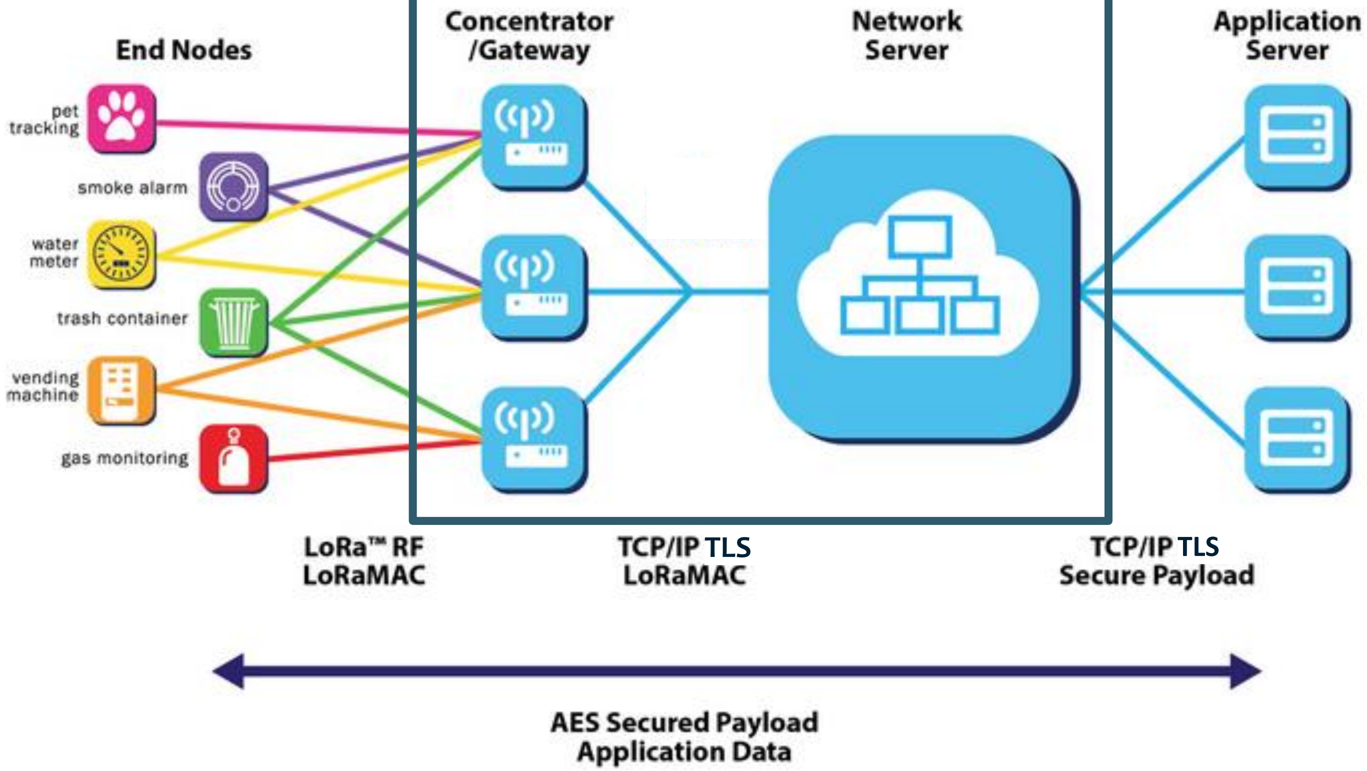
Edge Analytics

- Stream Analytics
- Fleet/Asset management
- Preventive maintenance
- Remote rolling stock devices management
- Real-time traffic information
- …

SECURITY CONSIDERATIONS
Typical LoRa^{TM} NODES AND GATEWAYS TOPOLOGY

▼

- Base components are: [End Nodes] – [Gateway] – [Network Server]



SECURITY CONSIDERATIONS
KONTRON SEC-LINE EMBEDDED COMPUTER SECURITY

SEC-Line Modules	TRUSTED BOOT	AUTHENTICATION WITH TPM	APPROTECT	SECURE BOOT
Primary Function	Protect system SW during boot	Authenticate system HW during TLS secure connections	Protect application integrity, confidentiality and IP	Boot only signed software from the BIOS firmware
Security Mechanism	TPM	TPM	WIBU	BIOS
	HW-based with secure elements			SW-based
Service	SOFTWARE Vulnerability watch			

SECURITY CONSIDERATIONS
EMBEDDED COMPUTER SECURITY BASED ON HARDWARE

Principle of a « secure element »

CRITICAL OPERATIONS HAPPEN INSIDE THE SECURE ELEMENT WHICH CANNOT BE ATTACKED

1. Security of the application: APPROTECT

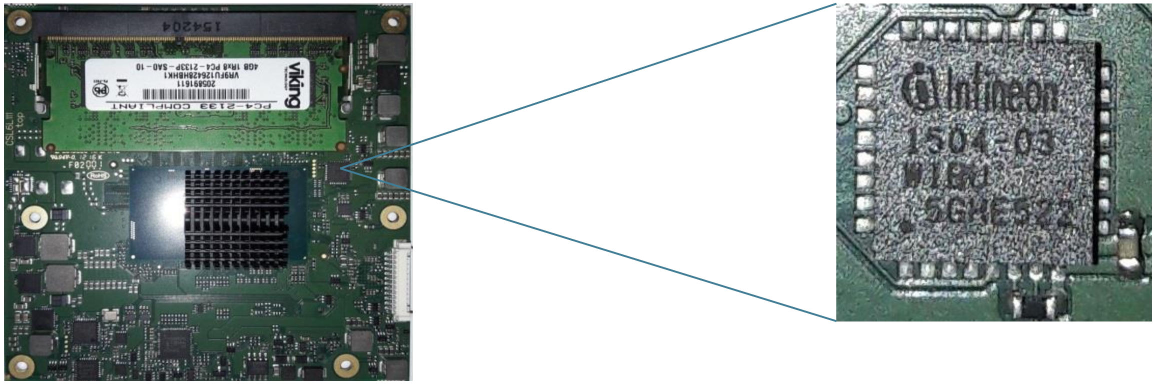
Secure element from WIBU

2. Security of the system software: TPM
   - Remote attestations of the boot code
   - SSL/TLS authentication on the network

Secure element TPM (Trusted Platform Module)
Standardized by TCG Trusted Computing Group

SECURITY CONSIDERATIONS
SECURITY OF THE APPLICATION: APPROTECT

The LoRa server integrity is protected with APPROTECT, avoiding unwanted hacks and simplifying updates with the WIBU « secure element »

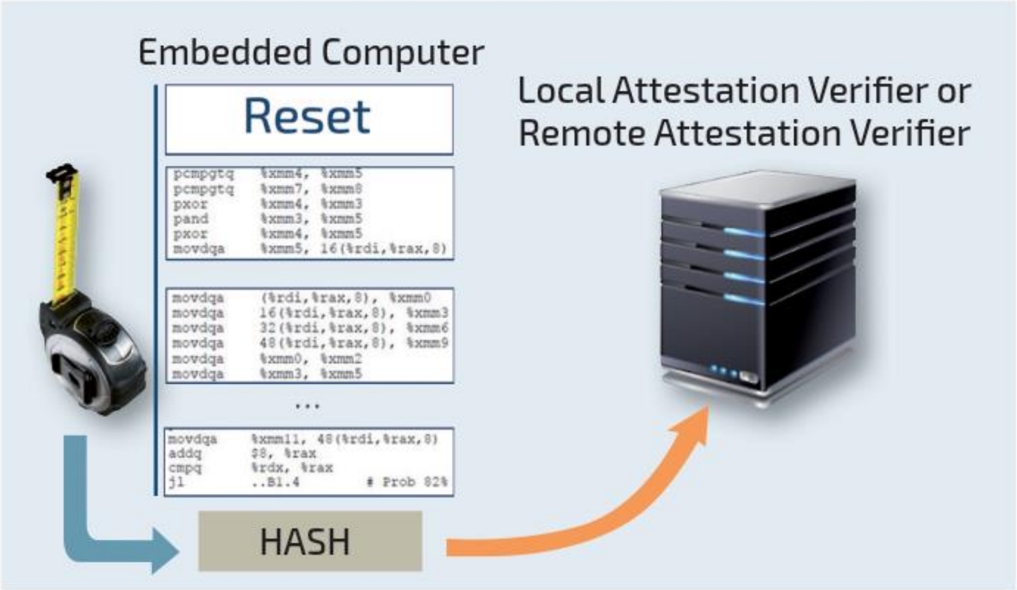


- Application integrity
- Protection against unauthorized copy
- Protection against reverse engineering
- Enforcement of software licenses (allows new business models like pay per use)

SECURITY CONSIDERATIONS
TRUSTED BOOT WITH TPM TO DETECT SYSTEM SOFTWARE ALTERATION

▼

Based on TPM secure element, equipped on Kontron boards



```
pcmpgtq   %xmm4, %xmm5
pcmpgtq   %xmm7, %xmm8
pxor      %xmm4, %xmm3
pand      %xmm3, %xmm5
pxor      %xmm4, %xmm5
movdqa    %xmm5, 16(%rdi,%rax,8)
```

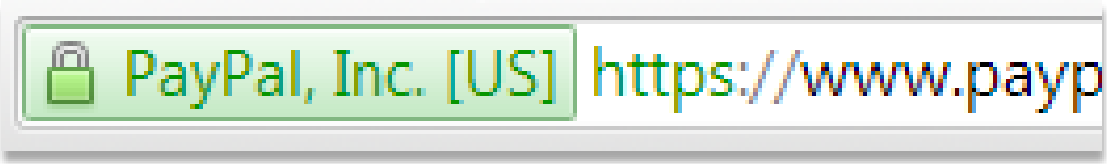
```
movdqa    (%rdi,%rax,8), %xmm0
movdqa    16(%rdi,%rax,8), %xmm3
movdqa    32(%rdi,%rax,8), %xmm6
movdqa    48(%rdi,%rax,8), %xmm9
movdqa    %xmm0, %xmm2
movdqa    %xmm3, %xmm5
```

...

```
movdqa    %xmm11, 48(%rdi,%rax,8)
addq      $8, %rax
cmpq      %rdx, %rax
jl        ..B1.4          # Prob 82%
```

- In case of unexpected hash of the boot code, the device is disconnected
- Remote update of the device can still happen to restore correct operation

SECURITY CONSIDERATIONS AUTHENTICATION WITH TPM TO SECURE NETWORK CONNECTIONS

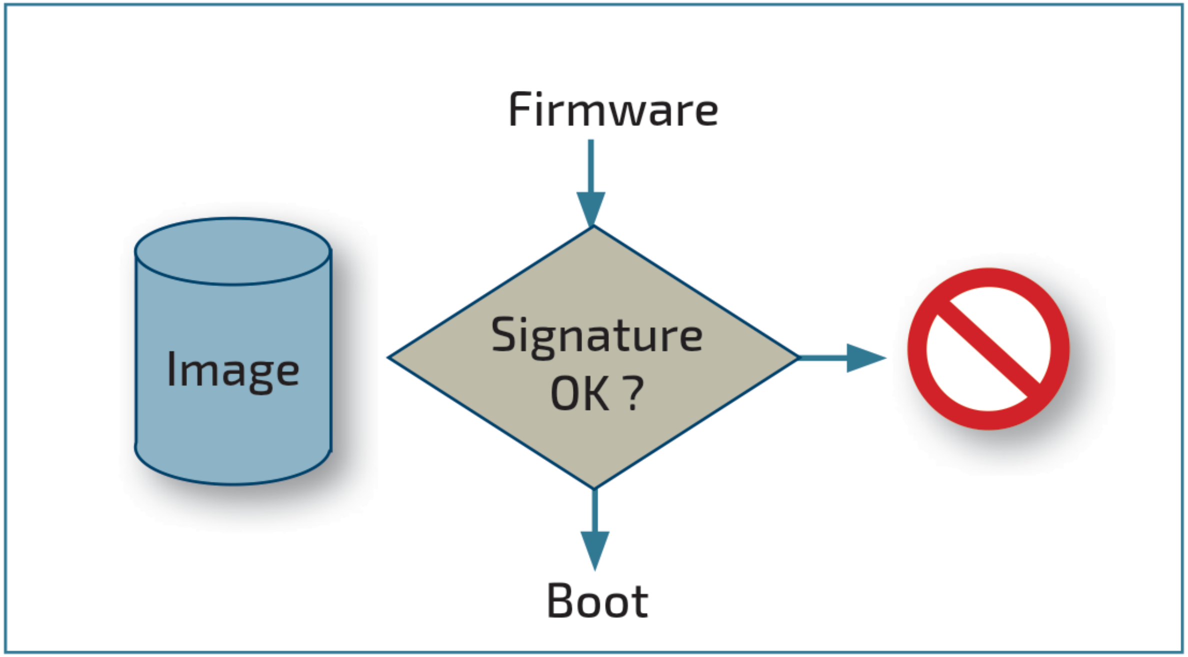


PayPal, Inc. [US] https://www.payp

- SSL/TLS authentication of the device to initiate secure network communications: https, …
- Critical operations for authentication happening inside the TPM secure element
- Need for strong authentication, both Servers and embedded Clients authenticate
- Use of classical x509 certificates, customizable validity duration
- Supported algorithms for authentication: RSA2048, ECC256, SHA1, SHA256

SECURITY CONSIDERATIONS SECURE BOOT TO RESTRICT BOOT TO SIGNED IMAGES

- Purely software security strategy at the BIOS level
- Prevents booting of a binary which is not properly signed
- The list of allowed signatures is stored in the BIOS firmware as a set of certificates and can be updated from a BIOS configuration menu.



SECURITY CONSIDERATIONS TAKE-AWAYS

APPROTECT

- Protect application integrity, confidentiality and IP

TRUSTED BOOT (TPM)

- Protect system SW during boot

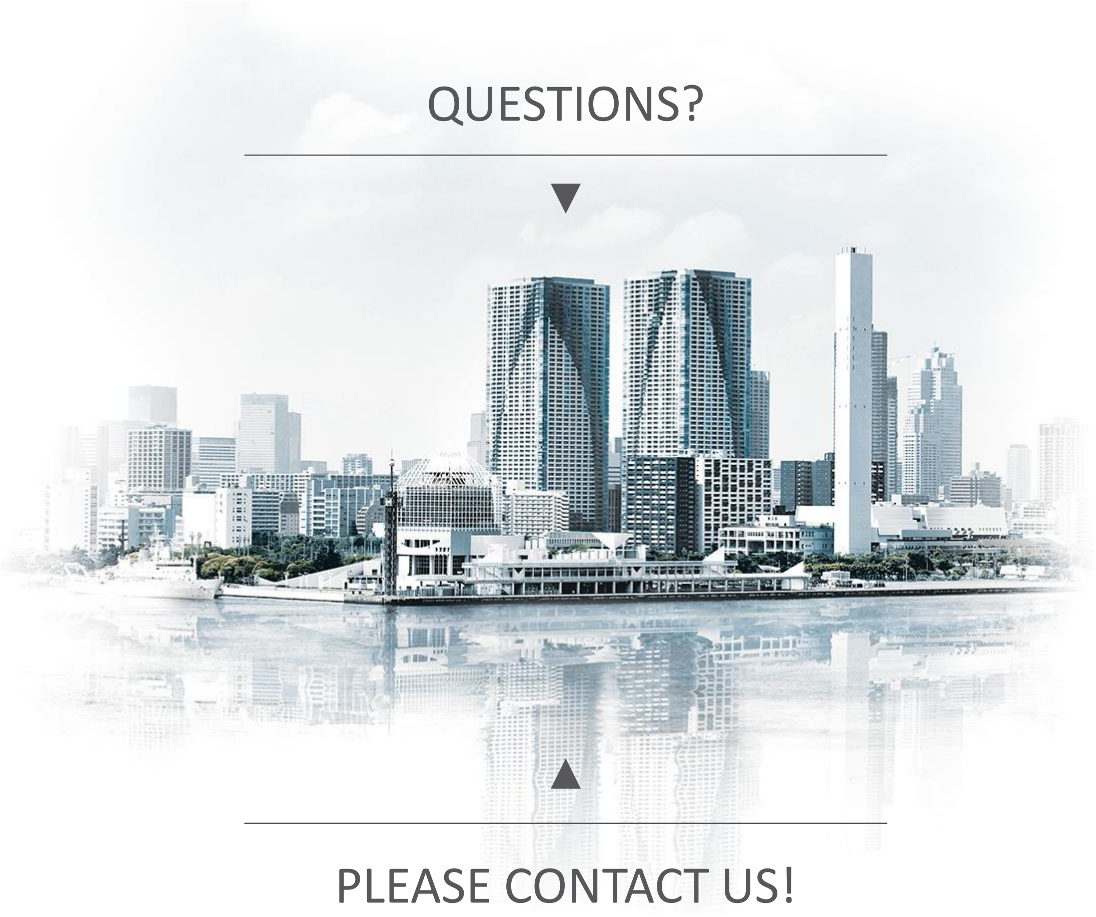
SSL/TLS NETWORK AUTHENTICATION (TPM)

- Authenticate system HW during TLS secure connections (provide associated certificates and private keys)

SECURE BOOT

- Boot only signed software from the BIOS firmware

OPTIONAL SOFTWARE VULNERABILITY WATCH



QUESTIONS?

▼

▲

PLEASE CONTACT US!

Valentin Scinteie
Business Development Manager
valentin.scinteie@kontron.com