
THALES
Building a future we can all trust
Navigating cyber resilience in the expanding IoT landscape
Gregory Laloy
www.thalesgroup.com

Gregory **LALOY**

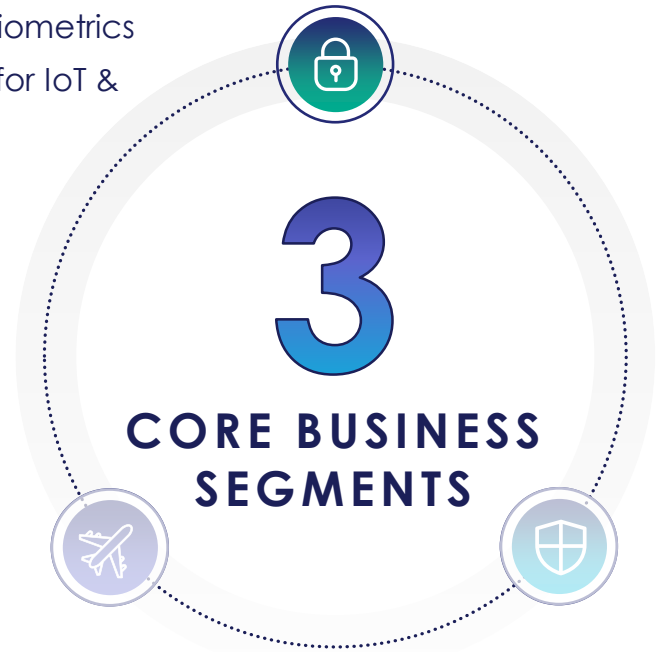
Head of IoT Product Line

THALES
Building a future we can all trust

Thales at a glance – Three core business segments

Cybersecurity and Digital Identity

- Cybersecurity
- Digital identity and biometrics
- Connectivity solutions for IoT & Consumer



Aerospace & Space

- Civil and military avionics
- Space programs
- Air traffic management

Defense & Security

- Land
- Air
- Sea
- Critical infrastructures

#1 eSIM IoT provider
Thales is **the market leader** on **industrial** and **automotive sectors**

DEPLOYMENT OF
600 Mu hardware
Root of Trust

CYBERSECURITY SOLUTIONS FOR
9 of the top 10
internet giants

The **ACQUISITION OF IMPERVA** makes us become a
Top 5 cybersecurity provider

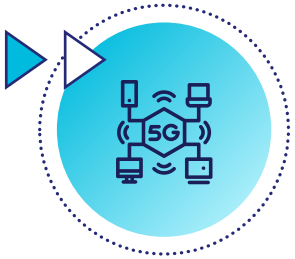
PROTECTION OF
400 critical sites
all over the world

The connected world keeps on growing

IT'S NOT
JUST PEOPLE

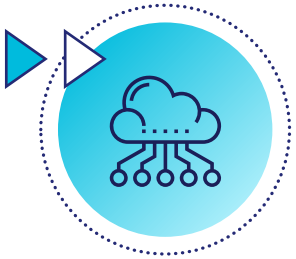
THE **IOT** MEANS
MORE **CONNECTED THINGS**

PRODUCING
HUGE AMOUNTS OF DATA



10x

More devices can connect per KM^2 with **5G compared to 4G** (ETSI)



24 billion

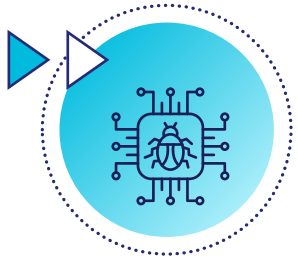
Connected IoT devices by 2050 (Ericsson)

Consequence surface attack is increasing **& Cyberattacks** are constantly growing

BILLIONS OF **DATA RECORDS** ARE EXPOSED EVERY YEAR

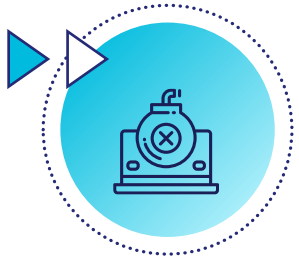
MOST BREACHES COME FROM **IDENTITY THEFT**

UNENCRYPTED DATA IS EASY TO EXPLOIT



300%

Increase in cyber-attacks on critical infrastructure in 2021[1]



$4.7M

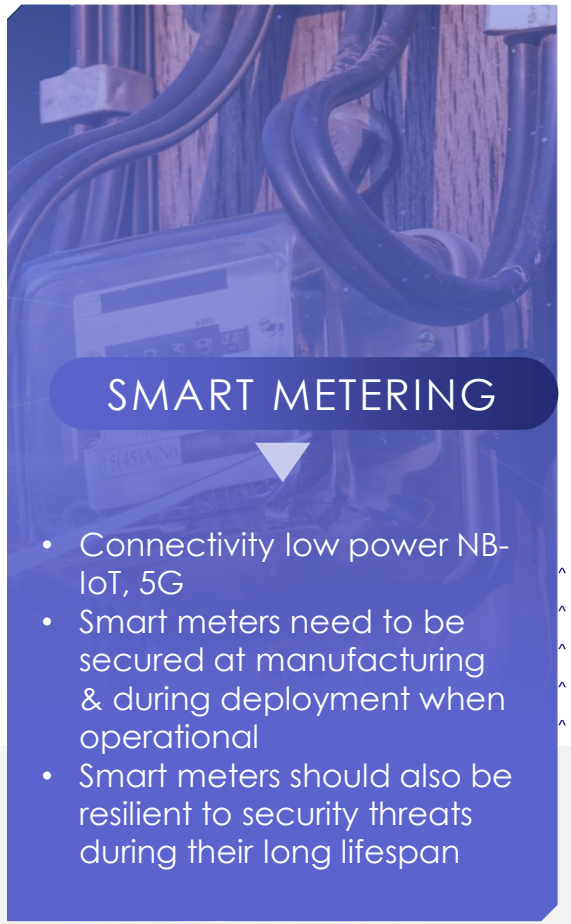
Was the **average cost of cyber-attacks** in the energy sector in 2023[1]

ONLY 20%

Organizations encrypt 60% or more of **their data** in the cloud[1]

1. *Source: World Economic Forum, Thales 2023 Data Threat Report*

Connectivity & IoT Security at work



SMART METERING

- Connectivity low power NB-IoT, 5G
- Smart meters need to be secured at manufacturing & during deployment when operational
- Smart meters should also be resilient to security threats during their long lifespan

AUTOMOTIVE

- Connectivity 5G, V_2x
- Telematics data to be protected on top of the car itself
- Car needs to be monitored remotely and its software updated, all securely thanks to specific Secure Element

TRACK & TRACE

- Connectivity 5G, NB-IoT, power efficiency, satellite
- Secured device to Cloud is a must
- Ensure Track & trace devices are integrated securely in larger IoT ecosystem incl. secure interaction with other IoT devices

HEALTHCARE

- Connectivity 5G, Private Network
- Secure and reliable connectivity is necessary with full control on data
- Patient safety & data confidentiality shouldn't be compromised and need to be protected

WHAT THE **IoT MARKET** SAYS

Large IoT device OEM

- I need to build a long-life IoT device & keep my manufacturing & logistics TCO under control
- I need to scale globally and also adapt to meet specific requirements with only one product variant (SKU)
- I need to implement the proper level of security in my IoT devices and comply with **cybersecurity regulations**

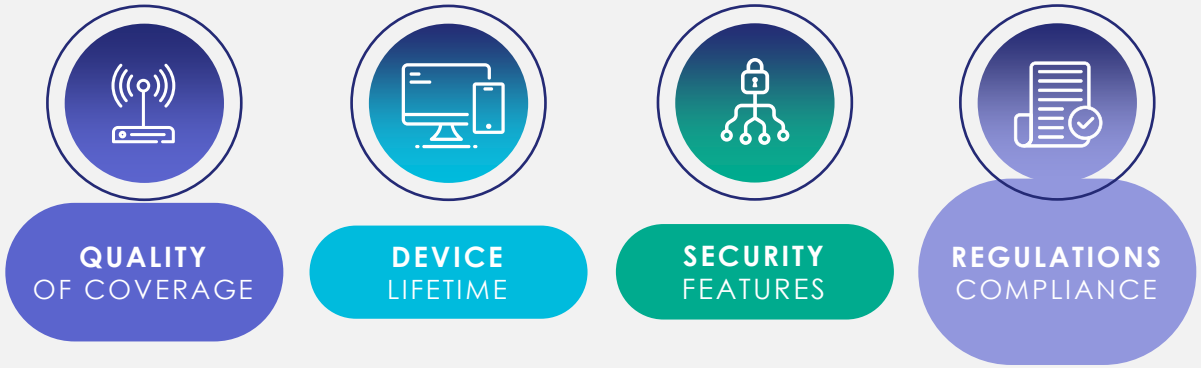
Leading IoT Service provider

- I need to deploy and manage securely a fleet of connected and battery-powered IoT devices over their lifespan
- I need to scale globally and simplify my deployment with only one product variant for various local markets
- I need to use local connectivity but I can't depend on a single connectivity provider
- I need to avoid service disruption and comply with **cybersecurity regulations**

Cellular, the most reliable global connectivity for IoT

TOP 4

most important features required in **IoT**



Source: Arthur D. Little for Thales

CELLULAR IOT IS GROWING - IOT IS MOVING TO eSIM

2027 Annual Shipments Incl. Auto, excl. China

eSIM/iSIM adoption is being embraced

Entreprises are or plan to adopt eSIM for greater flexibility

SGP.32 eSIM and 5G eRedCap

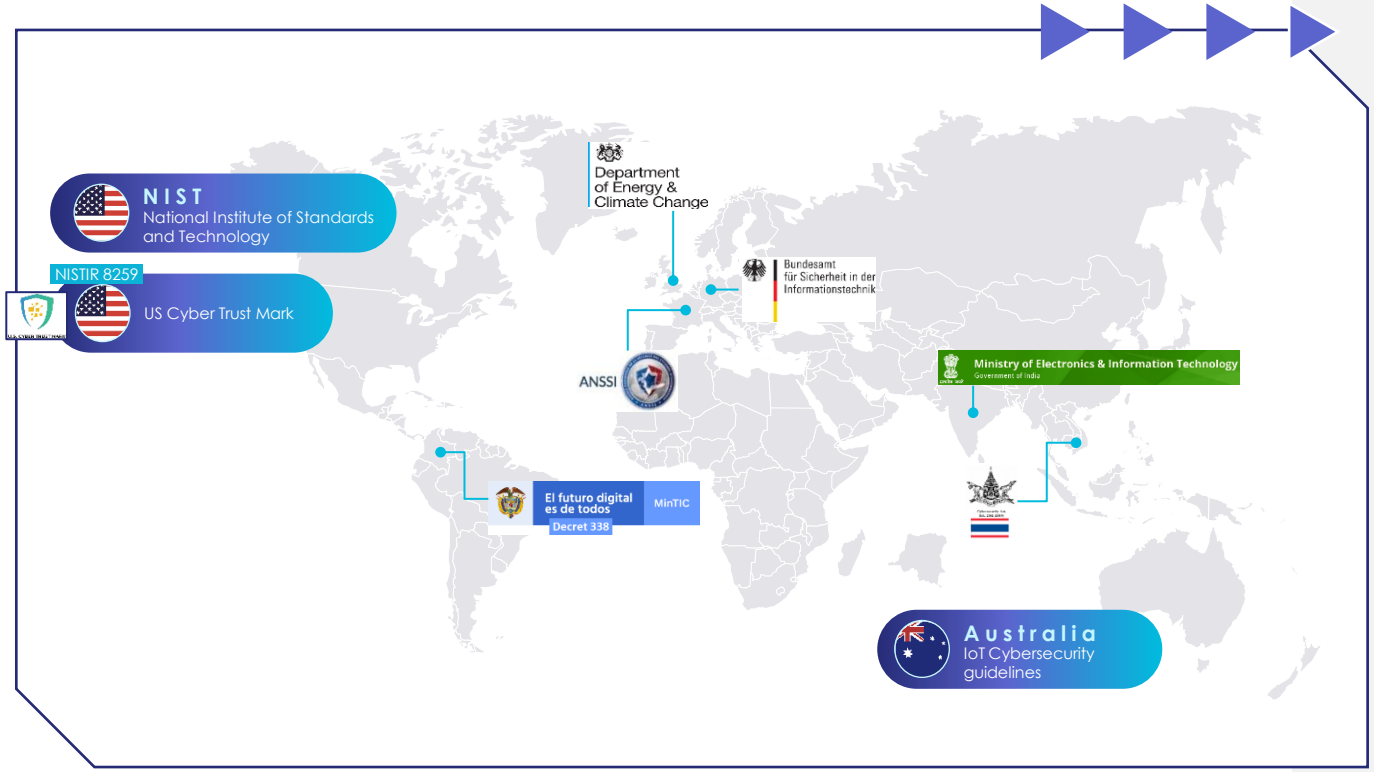
Enables

Secure

Resilient

Massive IoT deployments

IoT Security
REGULATION OVERVIEW



US FOOD & DRUG ADMINISTRATION

CYBERSECURITY RESILIENT ACT

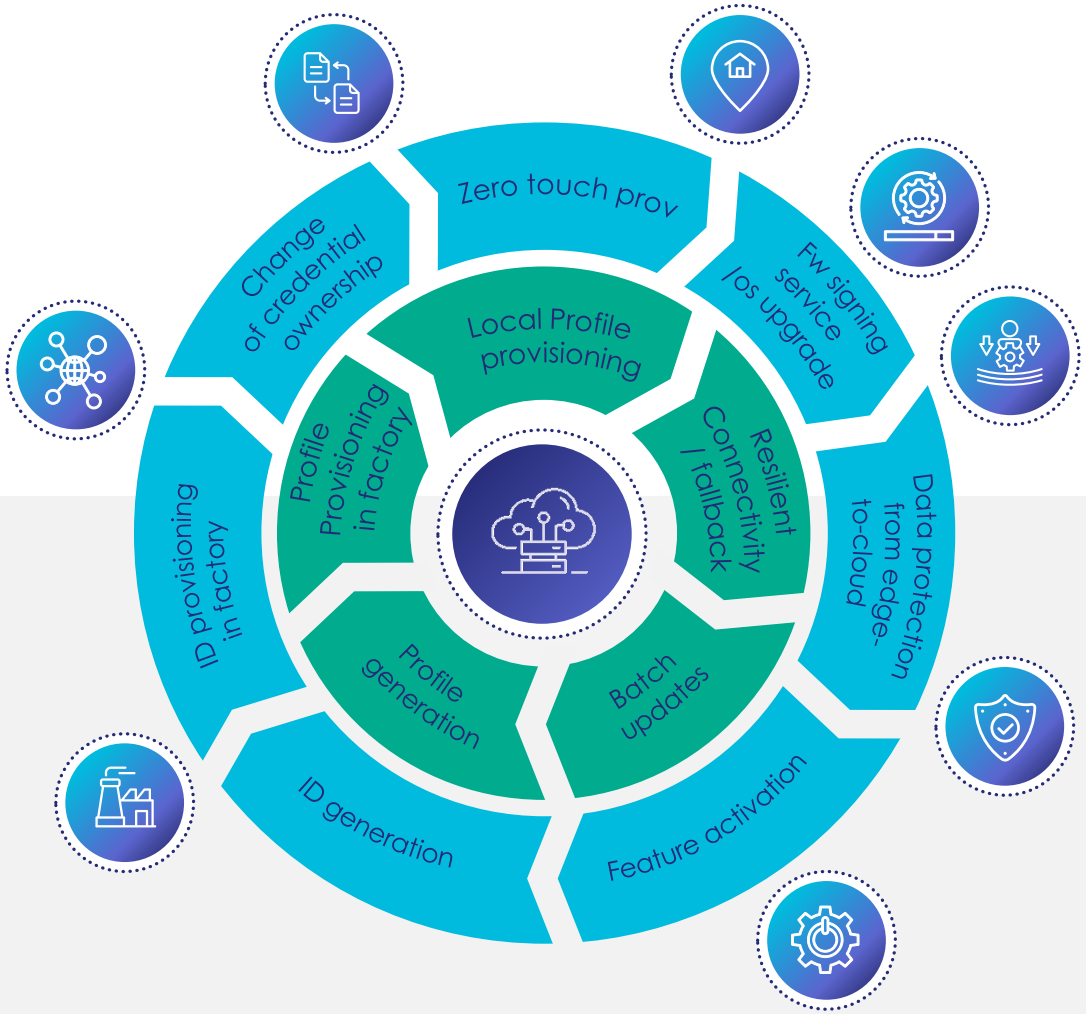
ISO SAE 21434 ROAD VEHICLES CYBERSECURITY ENGINEERING

- **IEC 62443** Cybersecurity of Industrial Installations
- **RED** Radio Equipment Directive
- **GDPR** General Data Protection Regulation
- **EPCIP** European Programme for Critical Infrastructure Protection
- **NIS2** Network and Information System Security

Manufacturer's obligation

- Cyber considered in planning, design, development, production, delivery, maintenance
- Vulnerabilities and security updates handled for the life-time of the product

Seamless connectivity and security lifecycle management for IoT devices

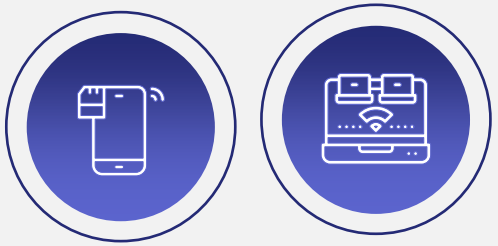


Optimize operations
Reduce risk

- Zero trust approach, security by design, PKIaaS
- Optimized logistic
- Freedom, ability to maintain connectivity providers and security schemes
- Resilience and service continuity
- Compliance with regulations & standards (RED, CRA, SGP.32)
- Post Quantum Cryptography

Take away

CYBERSECURITY IS KEY
AND CRITICAL FOR
ANY IOT DEPLOYMENT
(security by design)



THE **eSIM**
IOT STANDARD SGP.32
ENABLES **SECURE**
AND **MASSIVE IOT**
(Powered by Thales)

THALES
TURNS NEW STANDARDS
INTO **PRACTICAL**
AND **SECURE SERVICES**

Secure Solutions for a Connected World

THANK YOU

THALES
Building a future we can all trust

Future-Ready with IoT