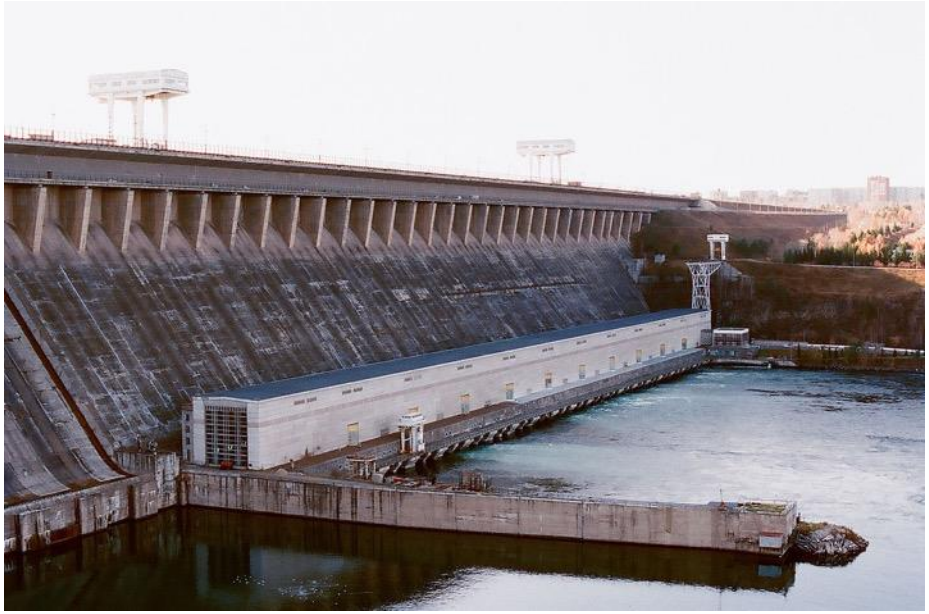
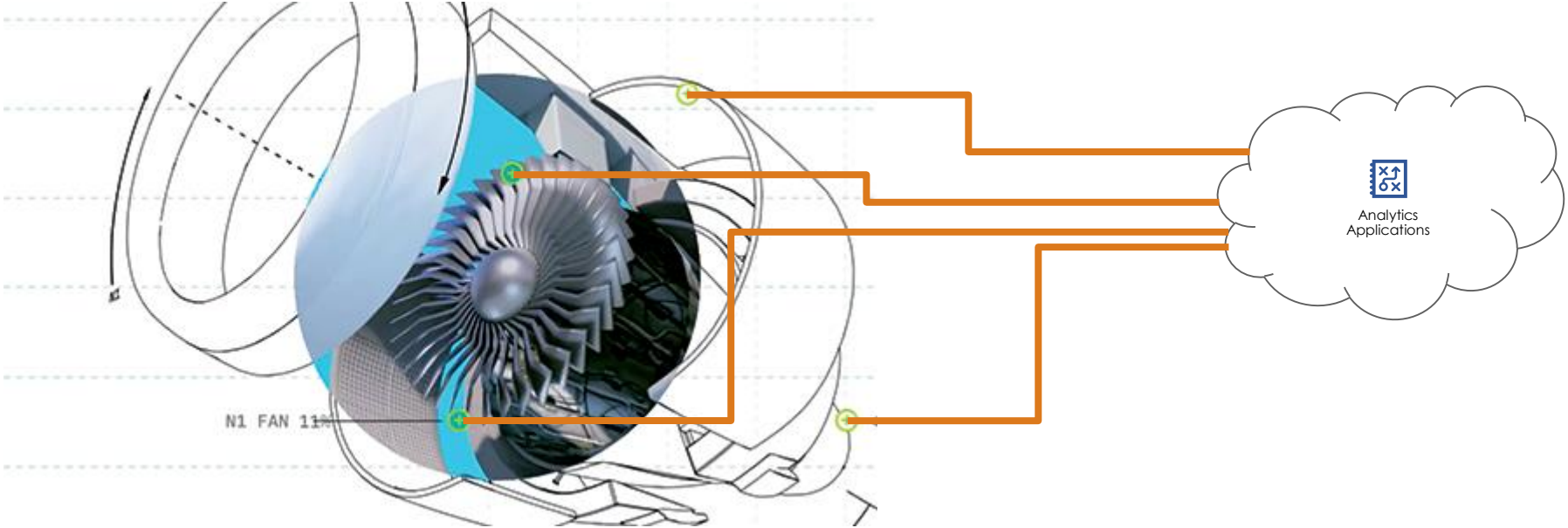
Challenges in Securing Industrial IoT and Critical Infrastructure

Brecht Wyseur, CARDIS 2018, November 14, Montpellier

Outline of this Talk

- Industrial IoT Intro
  - Industrial IoT use cases
  - Why connect *things*? Business models
- IT/OT security challenges
  - IT/OT convergence
  - Constraints
  - Compliance needs
- Key Management for IoT
  - From Root of Trust to Trusted Functions
  - Local Decision Making
  - H2020 FENTEC





- **Improve business efficiency** by collecting data from traditionally unconnected devices *ensuring that the data is authentic and can be trusted to make operational decisions.*
- **Automate critical decision making and guarantee safety** by executing remote commands *that devices can trust.*

Des trains entièrement automatiques en circulation dès 2023

SNCF, September 12, 2018

Reduce cost with autonomous (and centrally controlled) operations *while preventing cyberthreats that could harm safety*

Increase fleet performance & infrastructure capacity with efficient decision making & traffic control *based on data that can be completely trusted*

Industrial IoT – Industry 4.0

Operations Efficiency

- Production optimization
- Production planning & scheduling
- Productivity modelling
- Statistical Quality Control
- Inventory Optimization

Maintenance Efficiency

- Condition monitoring
- Predictive Maintenance
- Maintenance Planning & Scheduling
- Reliability-Centered Maintenance
- Root Cause Analysis / Anomality detection

Service Efficiency

- Remote management / Remote services
- Field service management
- Materials management (spare parts/inventory)
- Service Life Cycle management
- Supply chain analytics

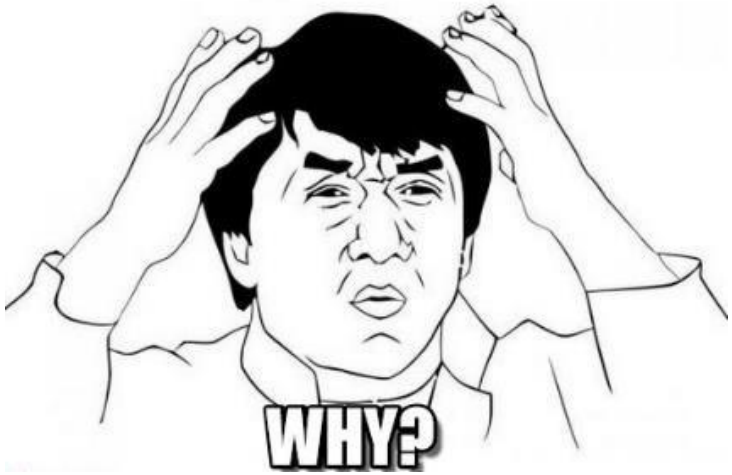
Information Efficiency

- Information Modeling
- Data quality framework
- Asset life cycle information model
- Machine-born data management & analytics
- Knowledge management

Energy Efficiency

- Energy management
- Resource efficiency
- Asset Sustainability Index
- Safety Performance (Alarm Management)
- Regulatory / Standards compliance

CONNECTED FOR SMARTER IRONING



Outline of this Talk

- Industrial IoT Intro
  - Industrial IoT use cases
  - Why connect *things*? Business models
- IT/OT security challenges
  - IT/OT convergence
  - Constraints
  - Compliance needs
- Key Management for IoT
  - From Root of Trust to Trusted Functions
  - Local Decision Making
  - H2020 FENTEC

WHY CONNECT *THINGS?*

OPERATIONS EFFICIENCY

- Production optimization
- Production planning & scheduling
- Productivity modelling
- Statistical Quality Control
- Inventory Optimization

MAINTENANCE EFFICIENCY

- Condition monitoring
- Predictive Maintenance
- Maintenance Planning & Scheduling
- Reliability-Centered Maintenance
- Root Cause Analysis / Anomality detection

SERVICE EFFICIENCY

- Remote management / Remote services
- Field service management
- Materials management (spare parts/inventory)
- Service Life Cycle management
- Supply chain analytics

INFORMATION EFFICIENCY

- Information Modeling
- Data quality framework
- Asset life cycle information model
- Machine-born data management & analytics
- Knowledge management

ENERGY EFFICIENCY

- Energy management
- Resource efficiency
- Asset Sustainability Index
- Safety Performance (Alarm Management)
- Regulatory / Standards compliance

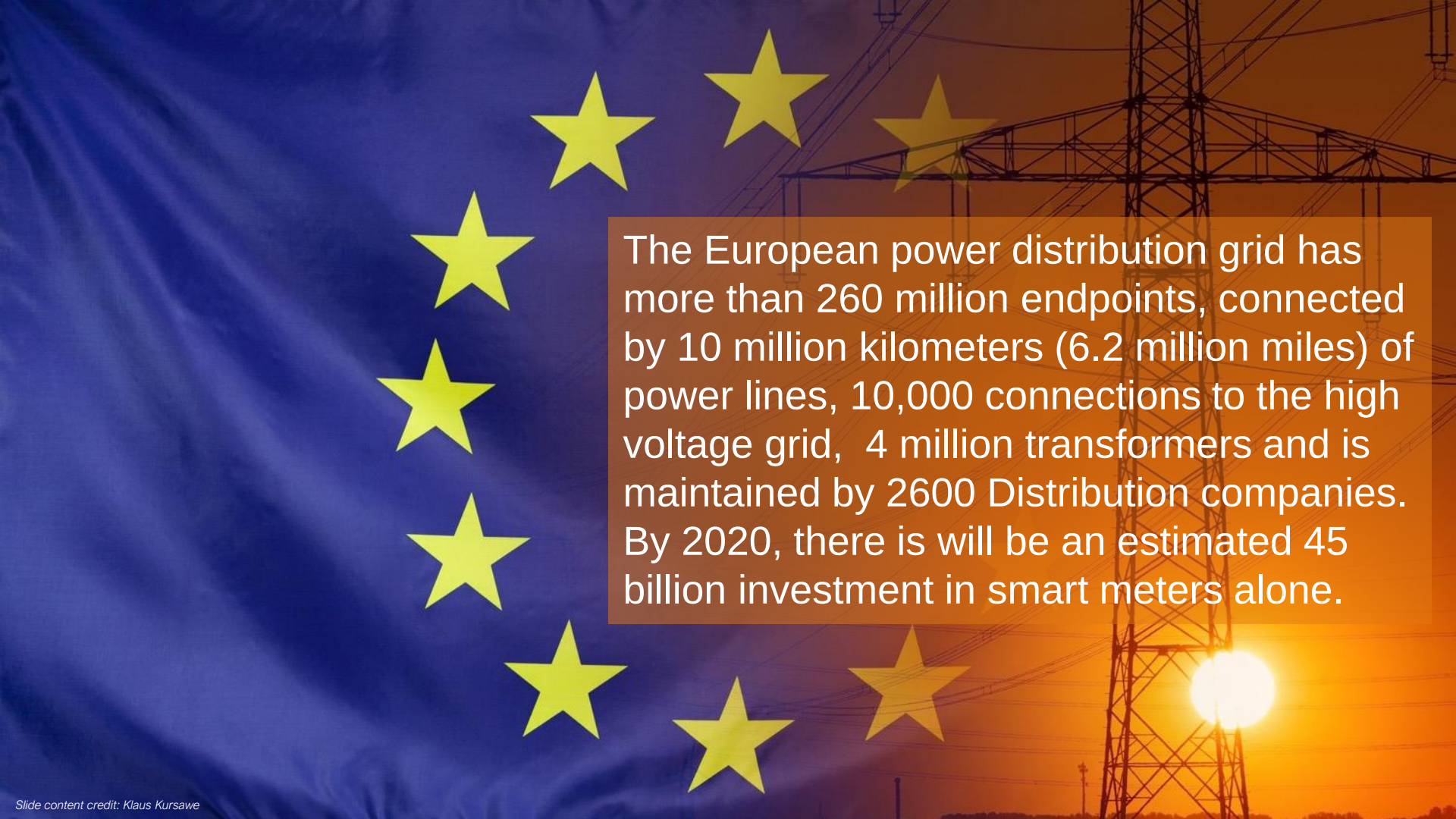
→ Increase efficiency using data analytics (Enisa / Industrie 4.0)*

New business models	Cost reduction	Aging workforce
Manage complexity	Compliance	Risk – failure is catastrophic
Brand reputation	Customer satisfaction	…

(*) Source: Industrial Internet Consortium

The most complex machine ever built, the space shuttle has more than 2.5 million parts, including almost 370 kilometers (230 miles) of wire, more than 1,060 plumbing valves and connections, over 1,440 circuit breakers, and more than 27,000 insulating tiles and thermal blankets.

BUT…



The European power distribution grid has more than 260 million endpoints, connected by 10 million kilometers (6.2 million miles) of power lines, 10,000 connections to the high voltage grid, 4 million transformers and is maintained by 2600 Distribution companies. By 2020, there is will be an estimated 45 billion investment in smart meters alone.

Slide content credit: Klaus Kursawe

Need for Security in IIoT

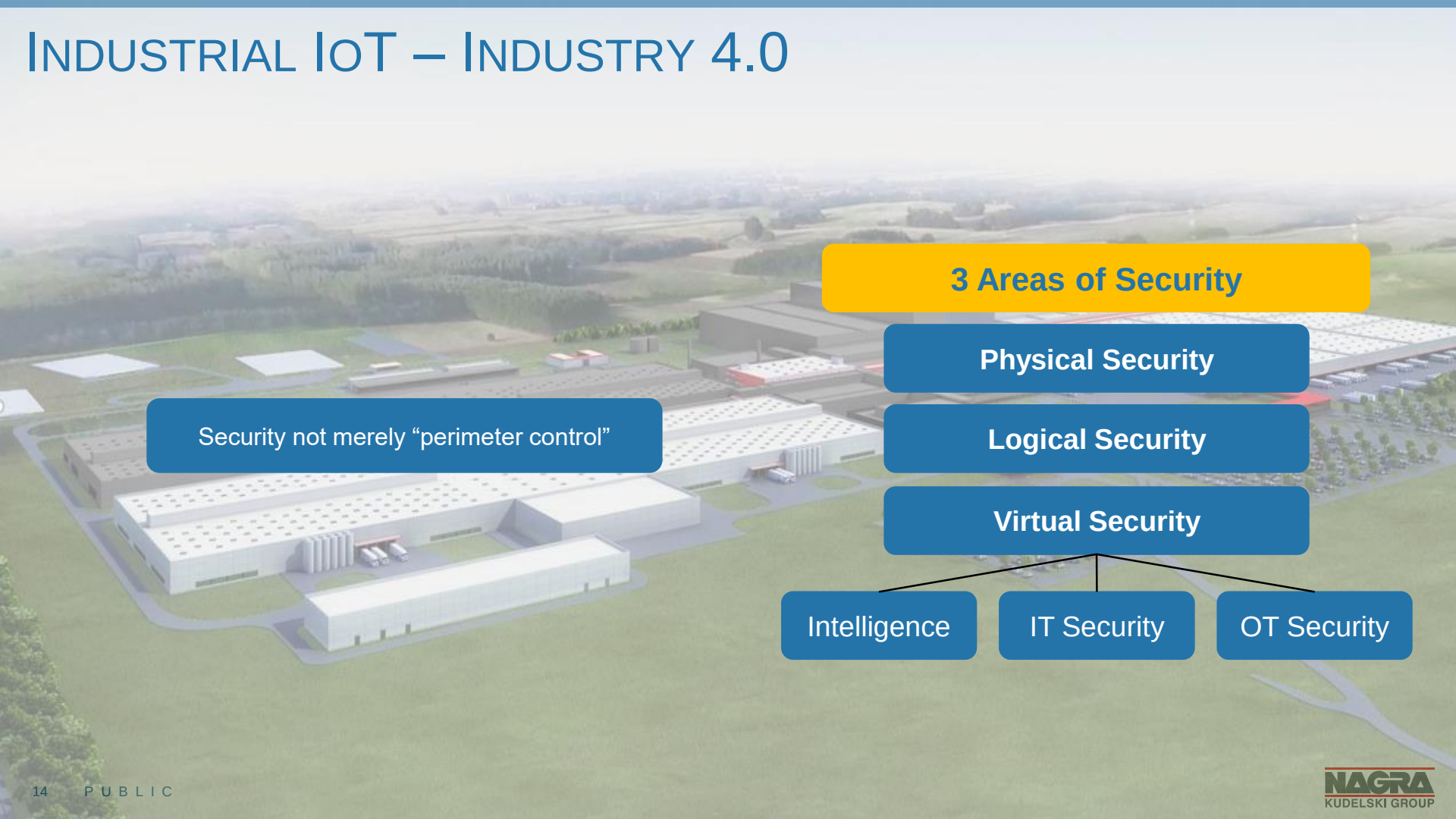
Saudi Arabian petrochemical plant attacked by Russian government-sponsored hackers last year to send a political message.

Sophisticated “Triton” malware used to infiltrate industrial control systems and wipe all data.

Triton targeted the industrial control systems made by Schneider Electric which are used in 18,000 different plants around the world.

The August 2017 attack on the Saudi Arabian plant was designed to sabotage its operations and trigger an explosion.

INDUSTRIAL IOT – INDUSTRY 4.0



Security not merely “perimeter control”

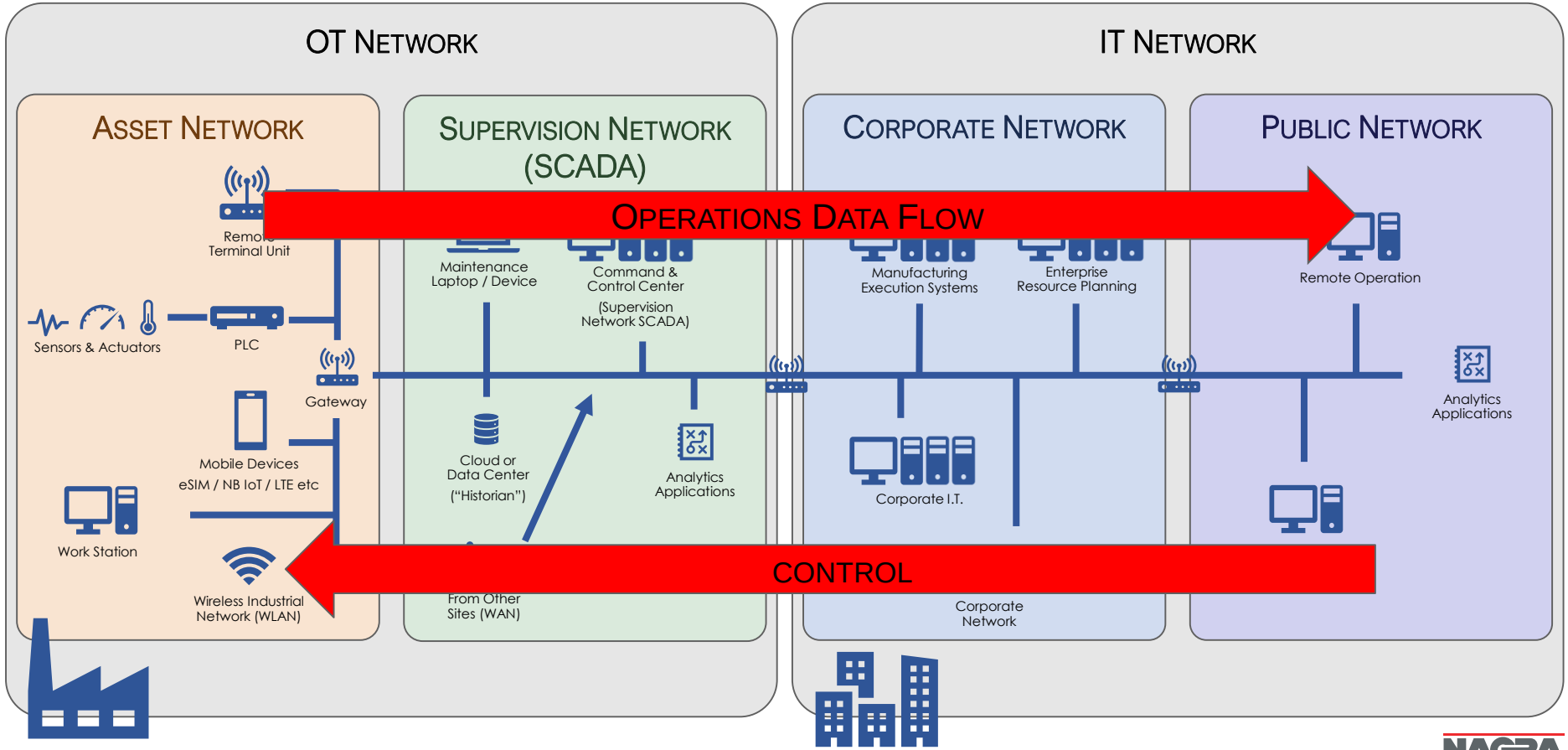
3 Areas of Security

- **Physical Security**
- **Logical Security**
- **Virtual Security**
  - Intelligence
  - IT Security
  - OT Security

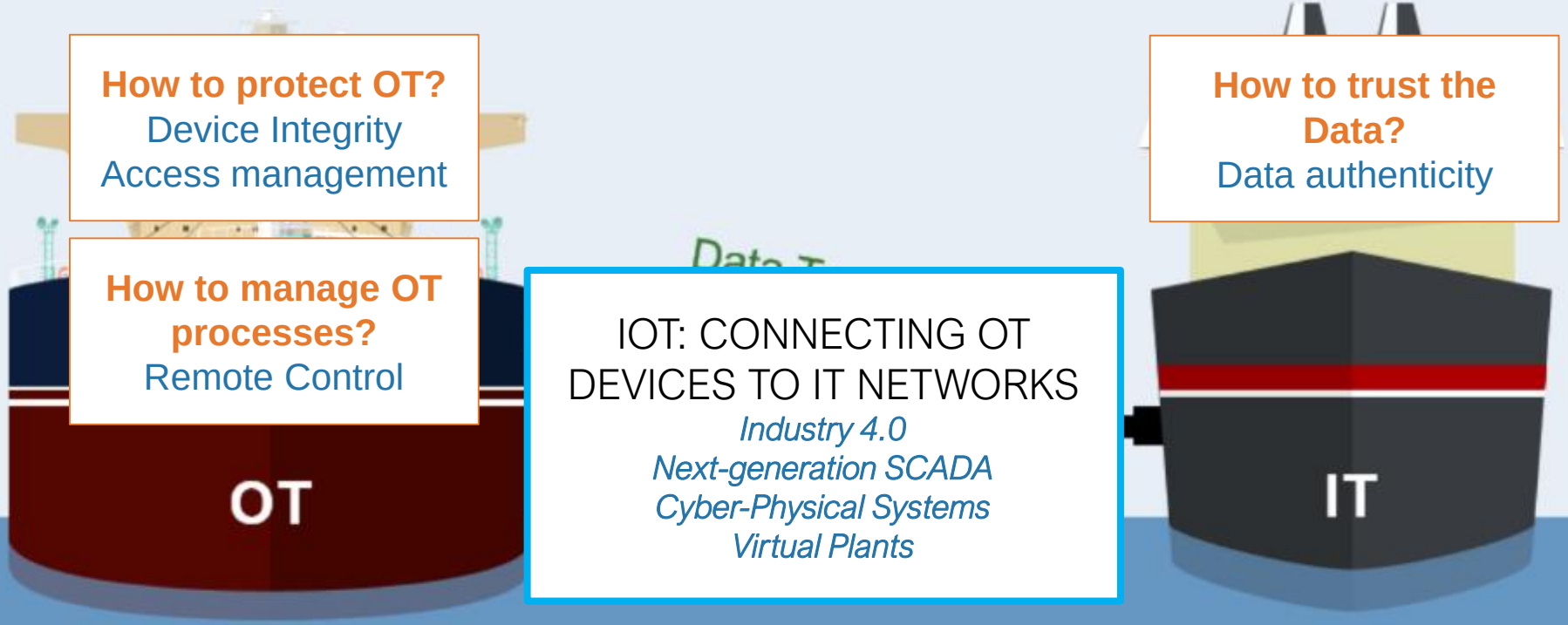
Step 1 – know what you have and what is happening

You can’t protect what you can’t see

Industrial Connectivity in Perspective



IT/OT Convergence



Focus on Safety of Physical Systems

Data to observe and manage processes

Data security focuses on authenticity

Focus on Data

Data security focuses on confidentiality

IT/OT Convergence – Constraints

- OT protocols versus IT protocols
  - OT protocols are mostly vendor specific
  - Not designed for security
  - Sometimes even not documented (no specs)

- Network constraints – datadiodes (e.g., for black-start systems)
  - No Diffie-Hellman…

- Performance
  - High-speed processing needed. E.g., PMCN protocol in Japan
  - Question: at what level to implement cryptographic algoriths ?

- Legacy – System duration

- Safety
  - Safety first, security after – or could we combine this?

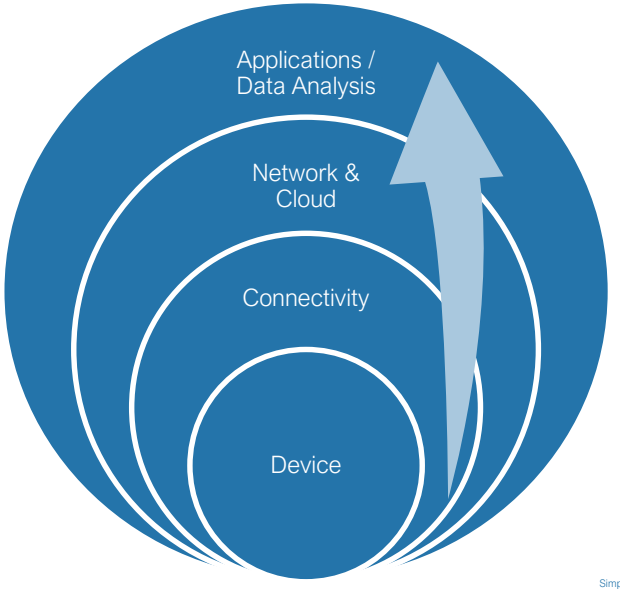
INDUSTRIAL IOT – IOT CYBER SECURITY CHALLENGES

Issues To Be Dealt With

- Multi Layered IoT Ecosystems
- 3rd Party Vendors
- Stakeholder Awareness
- Equipment Lifecycle
- Service & Maintenance
- Data & Process Integrity
- Connected Devices

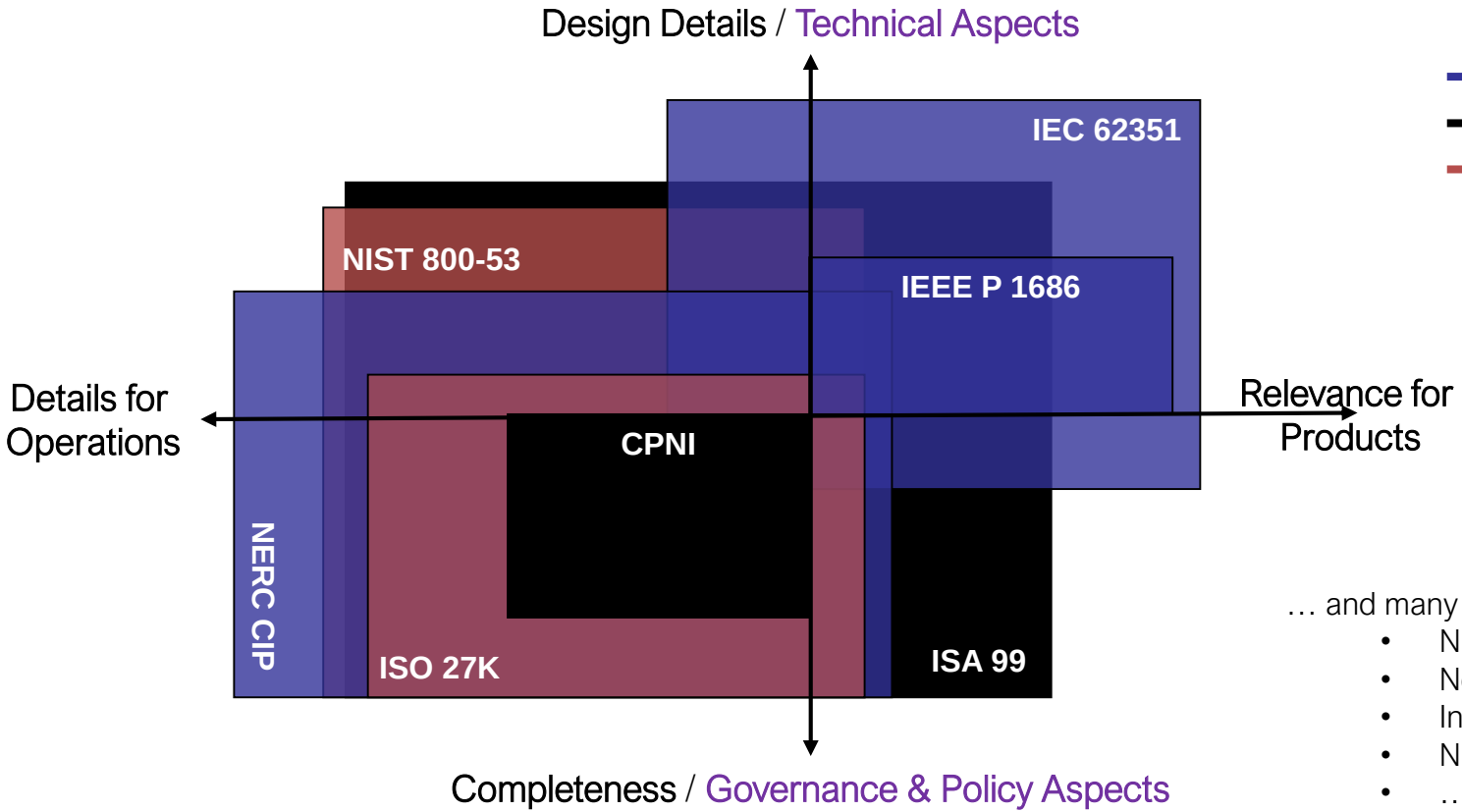
Non-Exhaustive

Layers of IoT Cyber Security Challenges



Simplified Overview

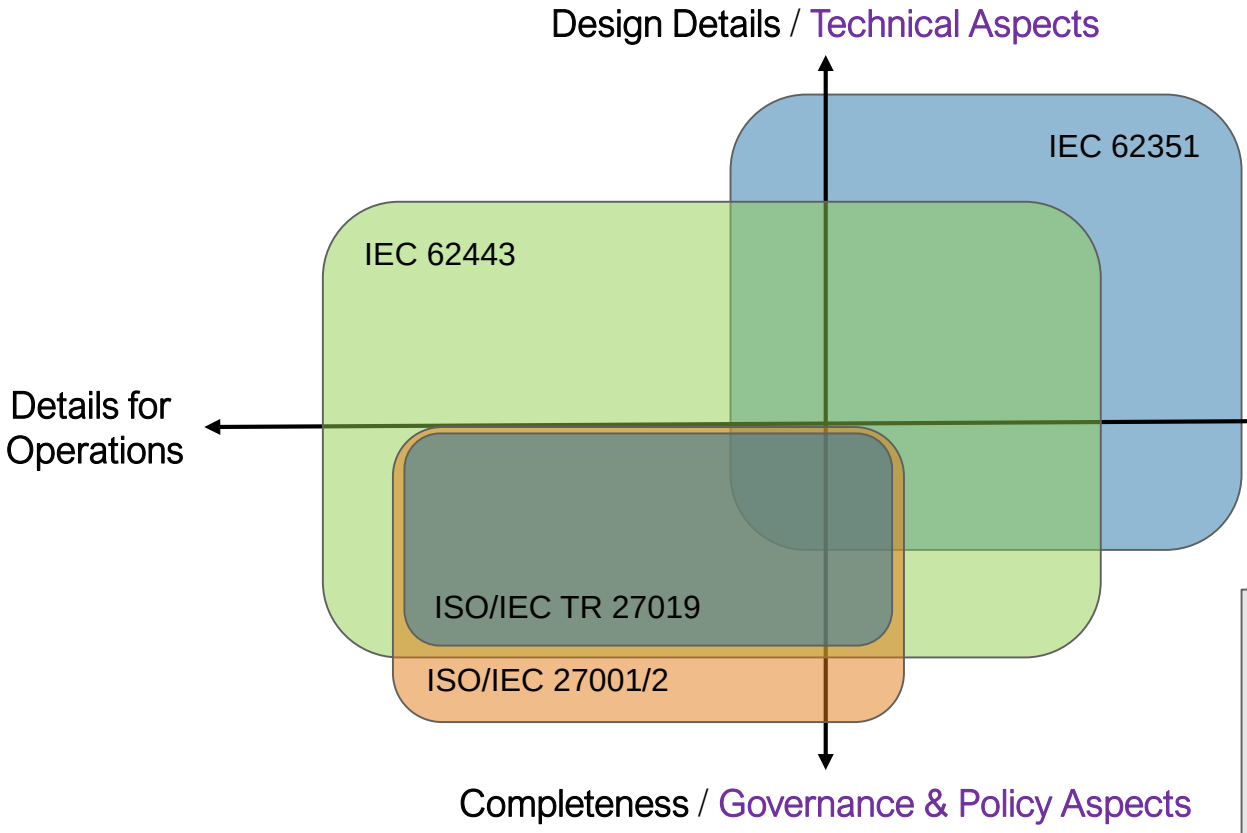
Compliance – To Enforce Cyber Security Expenditure?

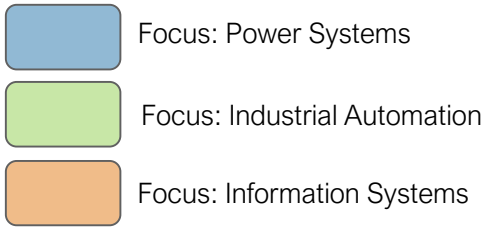


… and many others

- NIS Directive
- Network codes
- Industrial Internet Consortium
- NIST Cybersecurity Framework
- …

IACS Cyber Security

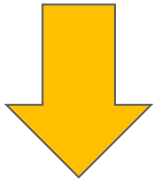




Key Standards

- IEC 62443 – System Security
- IEC 62351 – Communication Security
- ISO/IEC 27001/27019 – Security Management

COMPLIANCE-BASED SECURITY



RISK-BASED SECURITY

How to quantify system-level cyber resilience?

"Metrics" Working Group

WORLD ECONOMIC FORUM

NAGRA KUDELSKI

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Technische Hochschule Brandenburg University of Applied Sciences Institute of security and safety

ACER Agency for the Cooperation of Energy Regulators

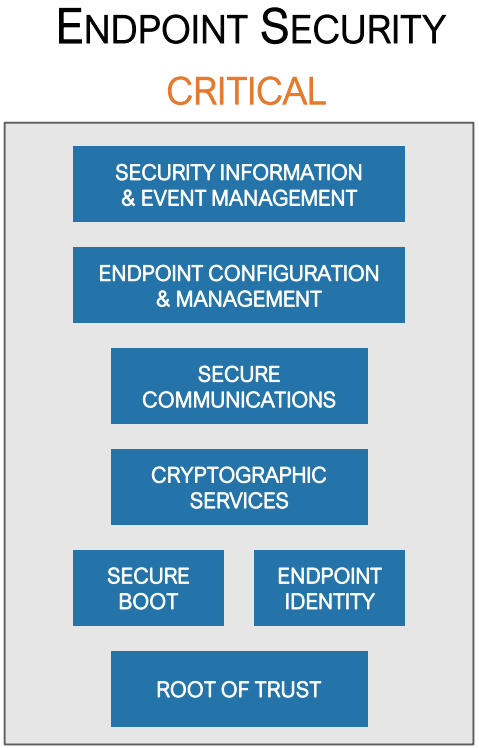
Argonne NATIONAL LABORATORY

IBERDROLA

enel

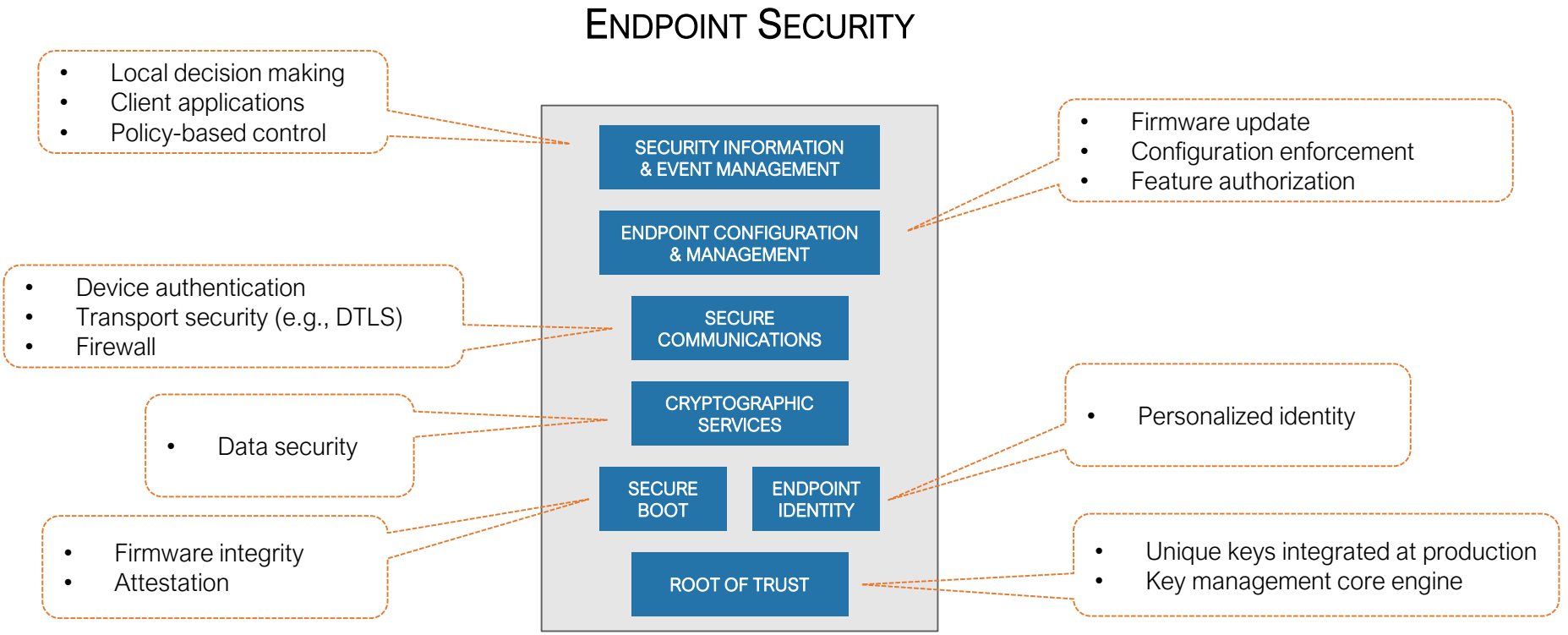
Charter of Trust For a secure digital world

Industrial Internet Consortium (IIC) Endpoint Protection Model[1]



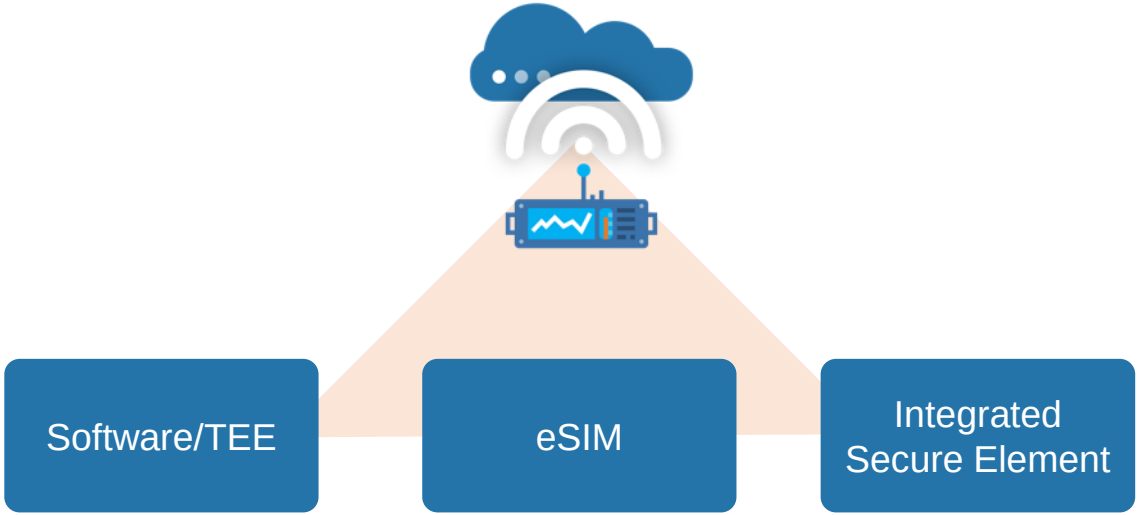
(1) https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf

KUDELSKI IOT ENDPOINT PROTECTION MODEL

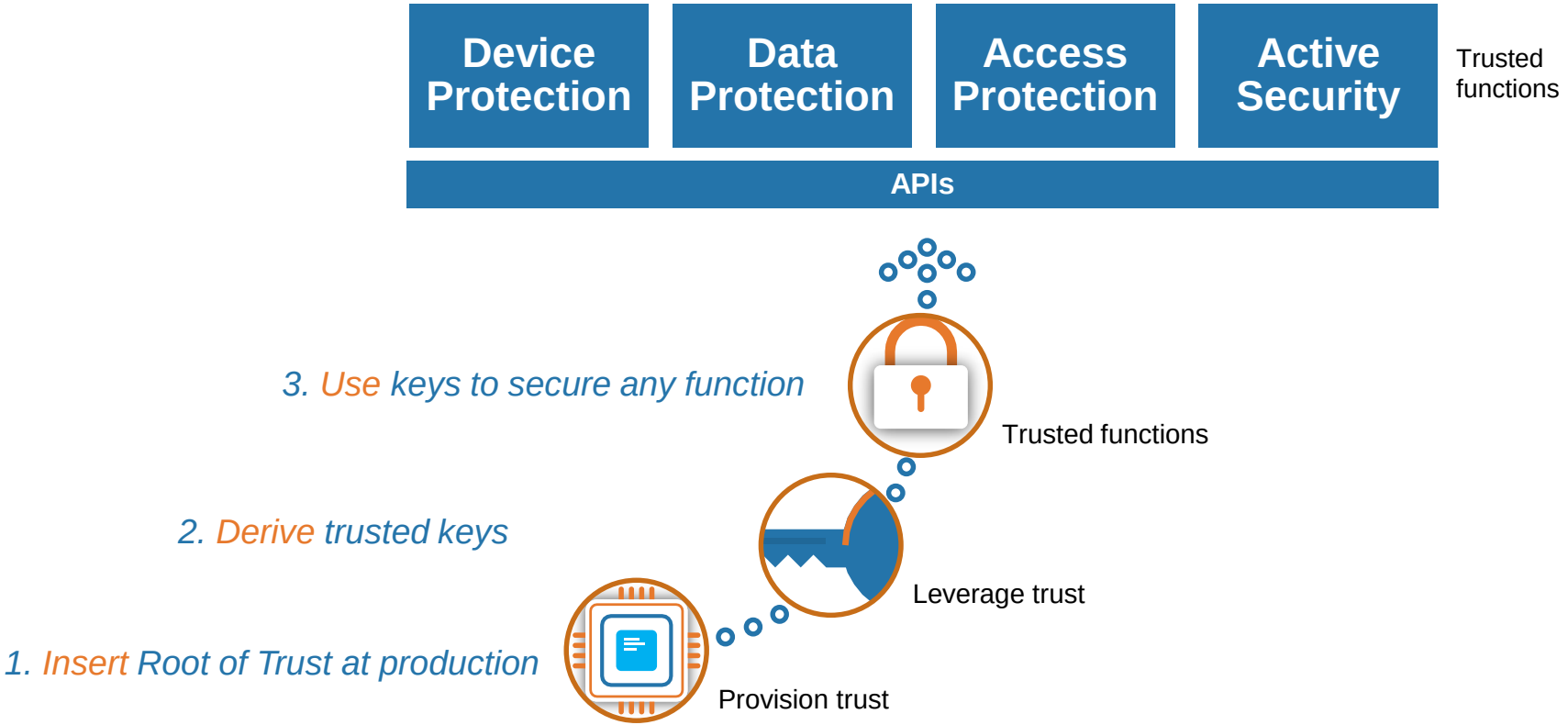


PROTECTING THE TRUST

What kind of RoT? There is no single RoT that solves all use-cases



How we create trust to drive secure functions



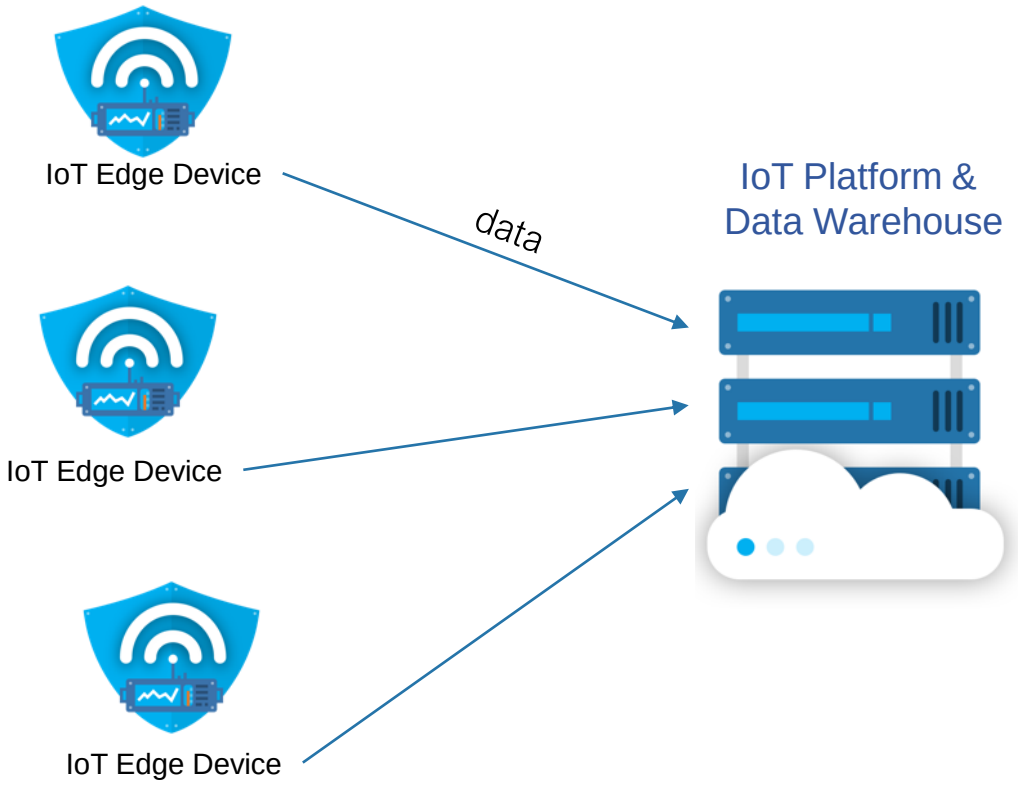
Functional Use Case: Data Collection

CUSTOMER NEED / PAIN

- Data authenticity and non-repudiation
- Data confidentiality (privacy)
- Local decision making

BUSINESS USE CASES ENABLED

- Predictive Maintenance
- New billing models (e.g., pay-per-use)
- Process Monitoring



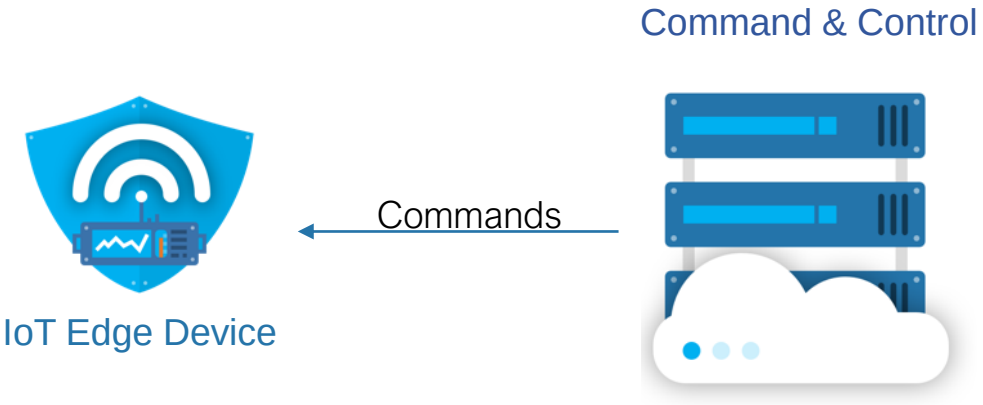
Functional Use Case: Remote Control

CUSTOMER NEED / PAIN

- Protect devices against malicious control (firewall and command authenticity)

BUSINESS USE CASES ENABLED

- Firmware updates
- Process control and automation (Industry 4.0)
- Device revocation or re-securization
- Out-of-band device operation



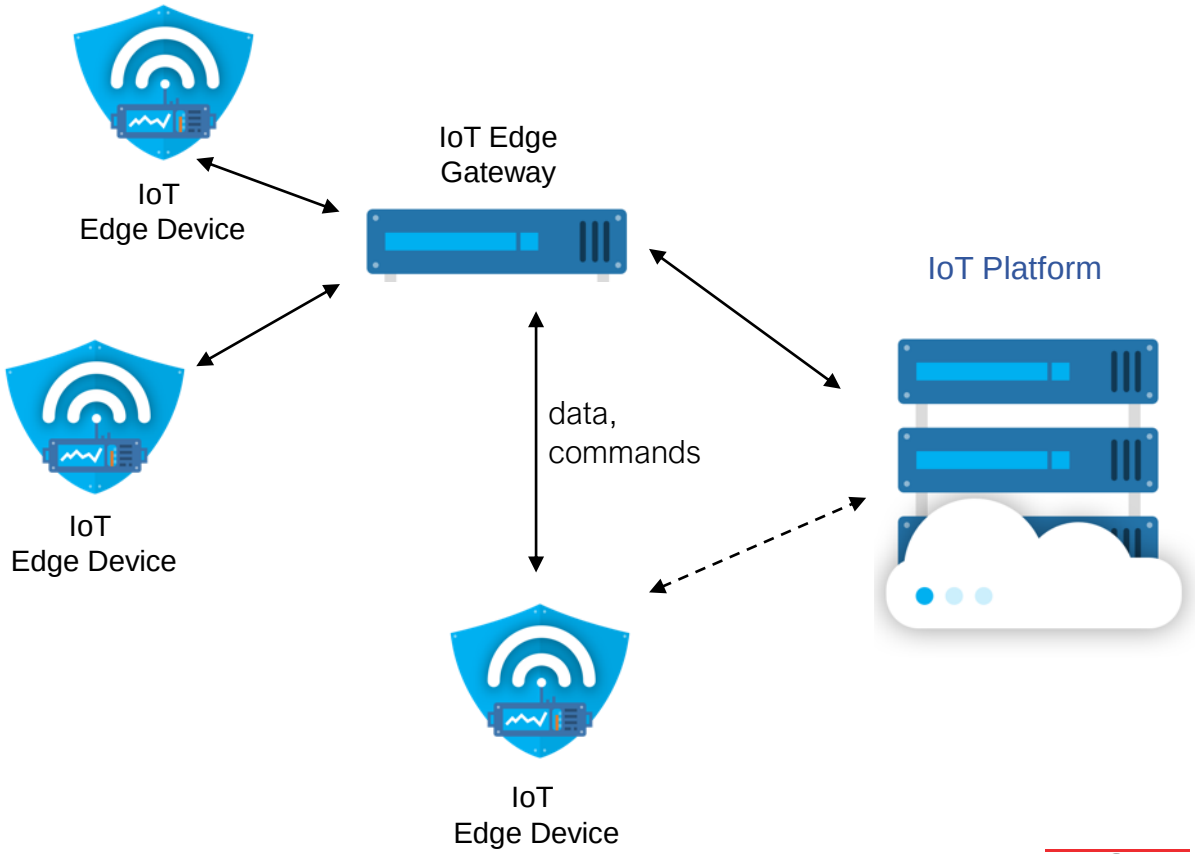
Functional Use Case: Device-to-Device Comms

CUSTOMER NEED / PAIN

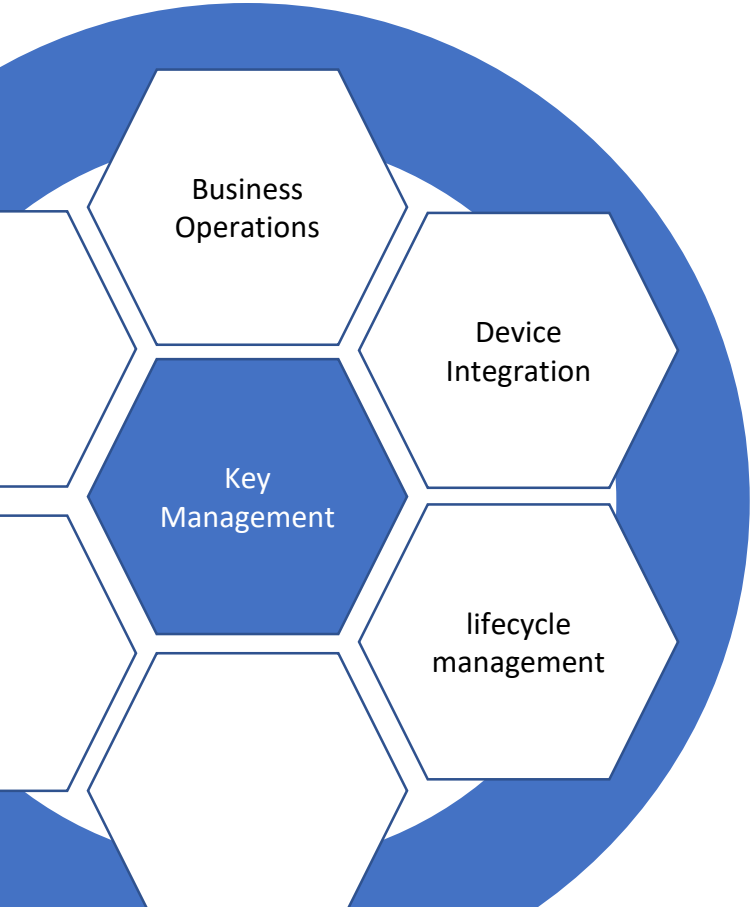
- Efficient and secure device management (linked with workflow management systems)

BUSINESS USE CASES ENABLED

- Local Maintenance
- IoT sub-system communication
- Decentralized communication



Core Technology: Key Management



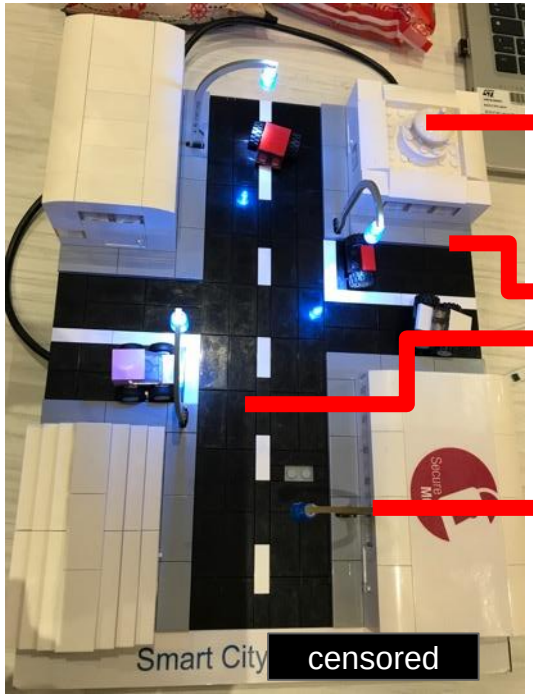
1. Foundations – enable core trust anchors in the system
   - Unique keys and identifiers in every system component
   - Control over the component security supply chain
   - Robust implementations w.r.t. threats
   - Segmentation and risk mitigation

2. Operations – enable business features
   - Link keys – devices – users – business
   - Enable complex use-cases
   - Operate over different network topologies
   - Customize business service offering

3. Lifecycle – manage product security in time
   - Network topologies and constraints are changing in time
   - New technologies and software are changing
   - Trust in devices can change in time
   - Threat response is required

NAGRA KUDELSKI GROUP

Move Intelligence to the Edge



Traffic Management Controller (TMC)

Gateway

Local Decision Making

Bringing intelligence into the Edge to improve safety

- Ensure safe state
- Ensure authentic TMC commands
- Override TMC commands

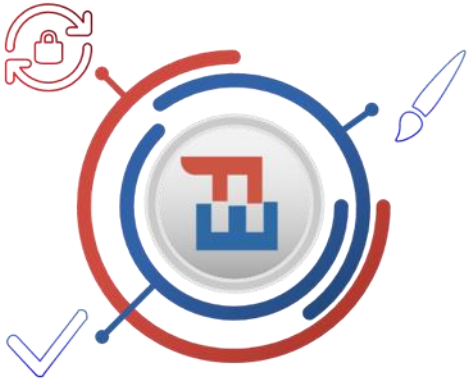
Horizon 2020

Grant agreement No 78010

FENTEC

Functional ENcryption TEChnologies

Implement a unified **cryptographic API** of Functional Encryption systems



Design **functional encryption systems** with varying functional, security, **hardware** and **software** requirements

Validate and **demonstrate** FENTEC technologies and **solutions**

Consortium

Atos

ENS

Hochschule Flensburg University of Applied Sciences

KU LEUVEN

UNIVERSITY OF HELSINKI

KUDELSKI SECURITY

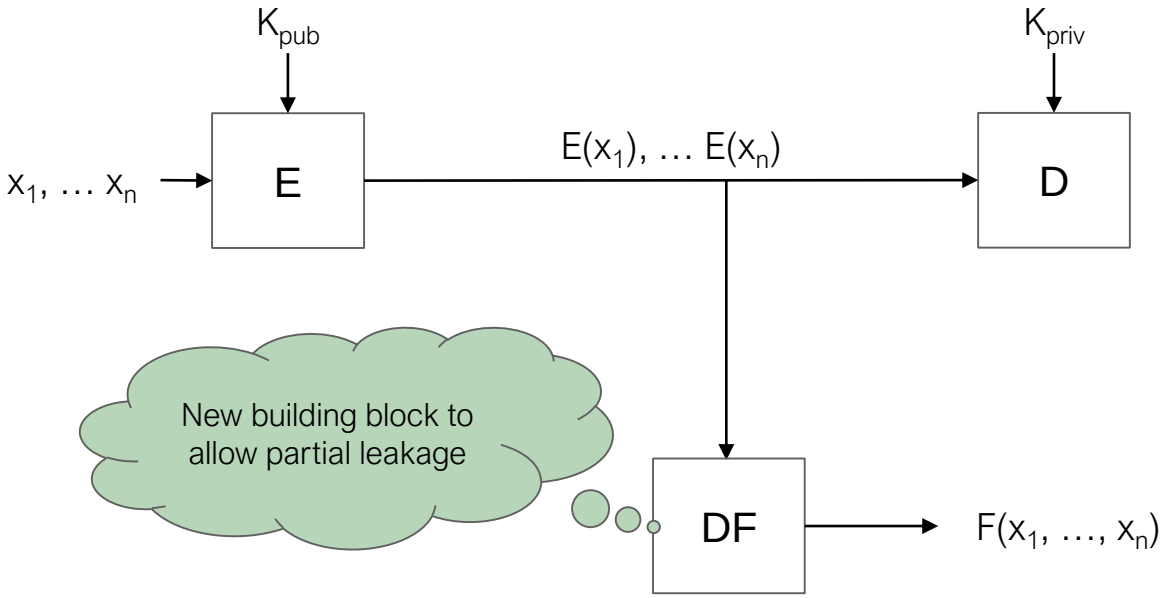
XLAB

THE UNIVERSITY OF EDINBURGH

WALLIX TRACE, AUDIT & TRUST

cnrs

FUNCTIONAL ENCRYPTION

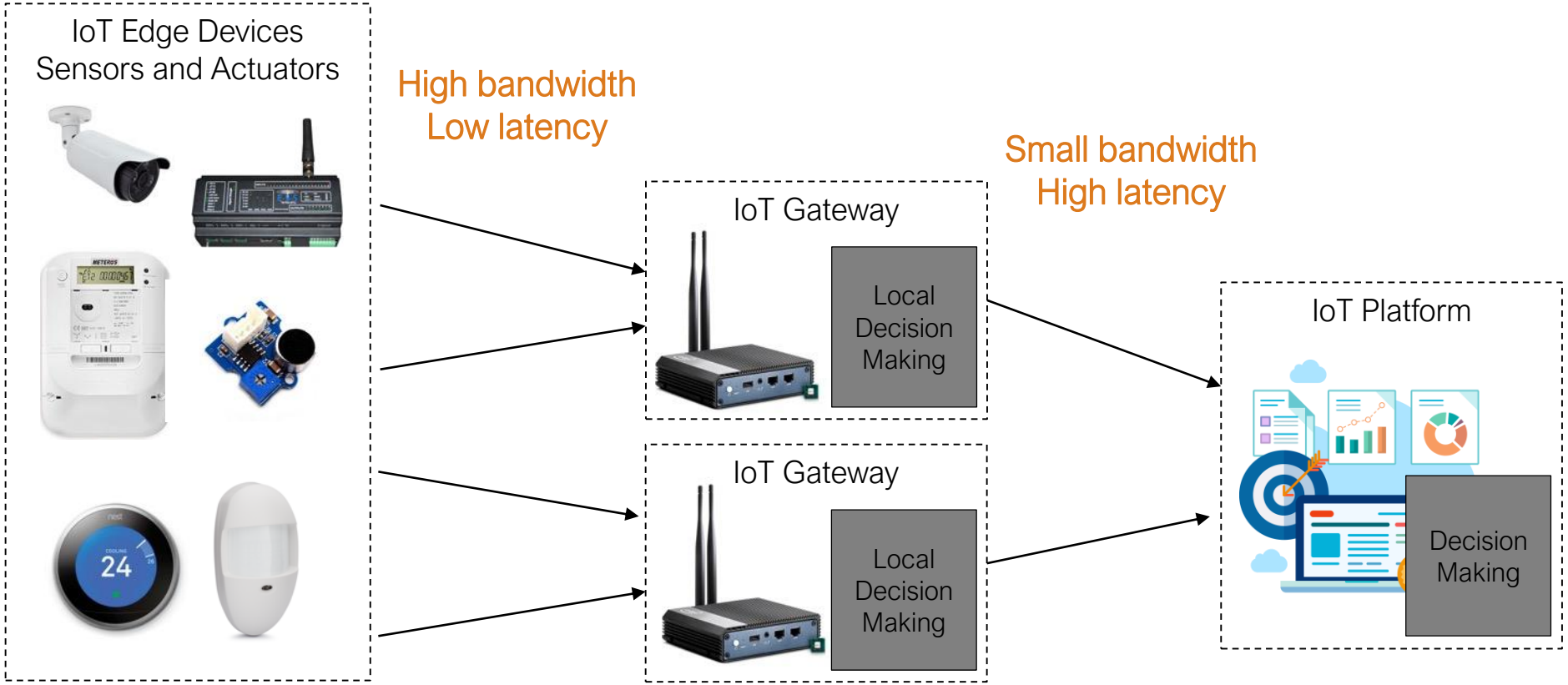


DF ← Functional Encryption circuit generator(K_{priv}, $K_{i,pub}$, F)

FENTEC
Functional ENcryption TEChnologies

NAGRA
KUDELSKI GROUP

Functional Encryption For Local Decision Making



Security as a Business Enabler

Security is like the brakes on your car.

- Their **function** is to **slow you down.**
- But their **purpose** is to **allow you to go fast.**

Industrial IoT – today we are buying a new car – unique opportunity to get a really good one!

Slide credit: Klaus Kursawe

NAGRA
KUDELSKI GROUP

THANK YOU!

www.kudelski-iot.com
iot.nagra.com