THALES

Securing Communications on the Field

PROTECTING GEO-DISTRIBUTED COMPUTING IN UNTRUSTED ENVIRONMENT

OLIVIER GILLES, DAVID FAURA, DANIEL GRACIA PEREZ
THALES RESEARCH & TECHNOLOGY FRANCE

IIoT versus IoT

Common technologies

- **Connectivity / dynamicity**
- **Open** source/protocols/networks
- **Data** as an asset

Different needs

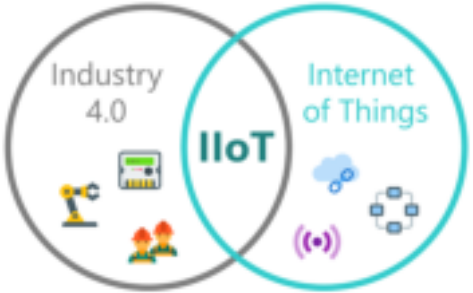
- **Criticality** : must be safe & secure
- Possibly **unfriendly environment**
- Mainly **Machine-to-Machine:** real time support

Different goals

- **Reactivity** to clients/suppliers
- Process **optimization**

Specific security challenges

- Safety and security often conflict
- Low resources
- Attract state-level attackers



Military specificity

- Mostly consistent with Industry 4.0
- **Low-availability networks**

THALES

Use Case: Maintenance for railway industry

Preventive maintenance

- Periodic inspection
- Expensive and error-prone

Reactive maintenance

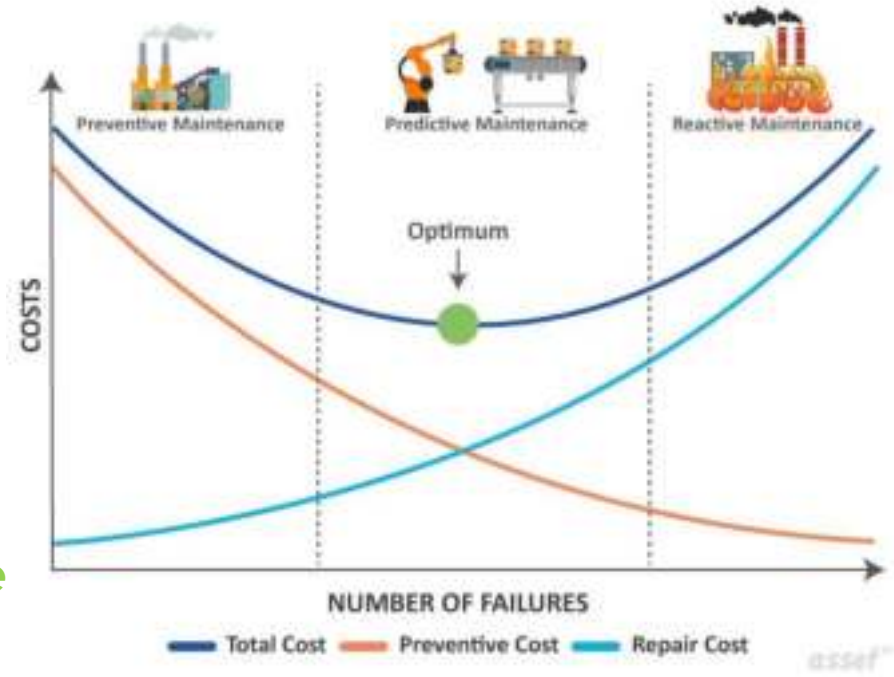
- Repair when fail
- Disruption of service, risk of major accident

Specifity of railway: difficult access

- Long distance between isolated sensors
- ***Human intervention even more expensive***

➢ ***IIoT + AI allows predictive maintenance***

➢ *Optimization retroaction loop*



Réf. TRT-Fr/STI/LSEC/OG - 21/11/2023
Thales Research & Technology France
Template trtp version 8,0,0 / Template : 87204467-DOC-GRP-EN-002

THALES

Application to catenary monitoring

Catenaries

- Most likely failure on high-speed trains
- Physical tension is the key
- Geo-distributed

Real-time monitoring

- Using track-side sensors
- Exploited by a analytics server / datalake
- Can be geo-distributed

THALES

Application to catenary monitoring

Catenaries

- Most likely failure on high-speed trains
- Physical tension is the key
- Geo-distributed

Operational needs

- *Group connectivity*
- *Interoperability*

Real-time monitoring

- Using track-side sensors
- Exploited by a analytics server / datalake
- Can be geo-distributed

Security risks

- *Physically accessible devices*
- *Open-network access (internet)*

THALES

Industrial networks: OPC UA

OPC UA (2008)

Ambitions

- Unifying Industrial Ethernet
- Interoperability between field buses
- Introducing security

Open Platform Communications

- Only relies on open standards
- Evolving & customizable
- Focus on communications

Unified Architecture

- Information model for data definition
- Backed by a strong industrial consortium

Industrial networks & IIoT: OPC UA PubSub

Publish-subscribe OPC UA (PubSub)

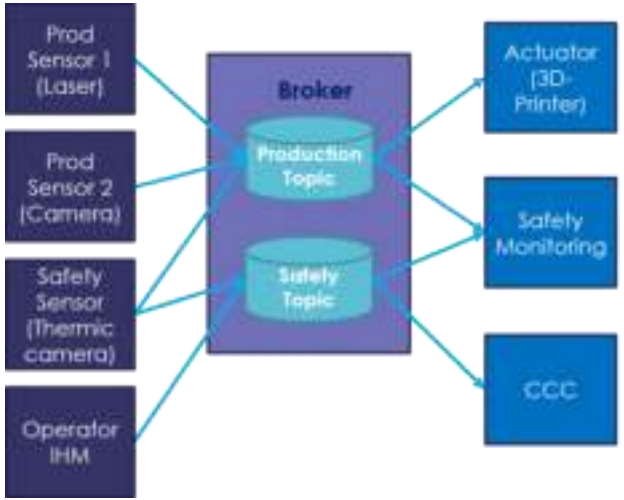
- Nodes are Publishers or Subscribers
- Topic-Based communications & rights

Scalable & Flexible

- Broker-based or brokerless
- Enable flexible topologies
- Reduce workload, low weight
- ***More adapted to dynamic systems***

Timing performances

- OPCUA/TSN 802.1Qbv (2018)
- 1 ms period with 40 ns jitter



Embeddability

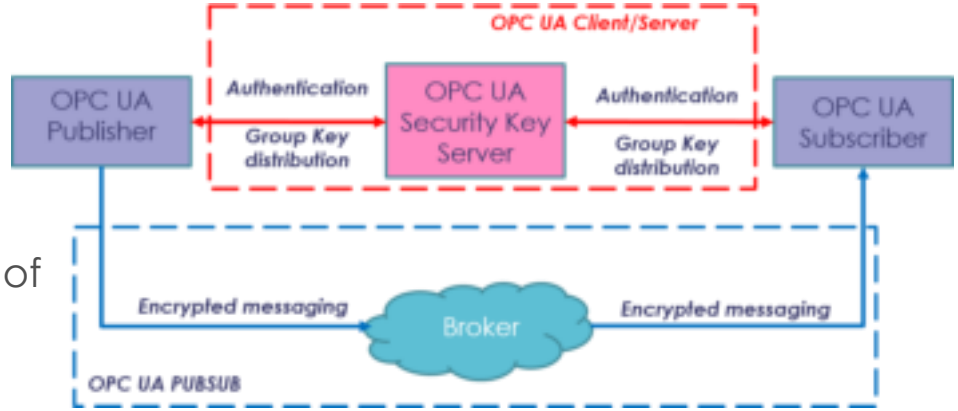
- Frame footprint: 17 B incl. UDP header
- Client footprint: 150 to 500 KB
- Small RTOS support

THALES

Industrial networks & IIoT: OPC UA PubSub security

Secure

- Topic-based key & security
- Separation of concern:
  - **Secure Key Service (SKS)** in charge of security
  - **Broker** in charge of performance (untrusted)



Security Key Service (SKS)

- Symmetric group key distribution
- Keys lifecycle management
- **Perform client authentication**

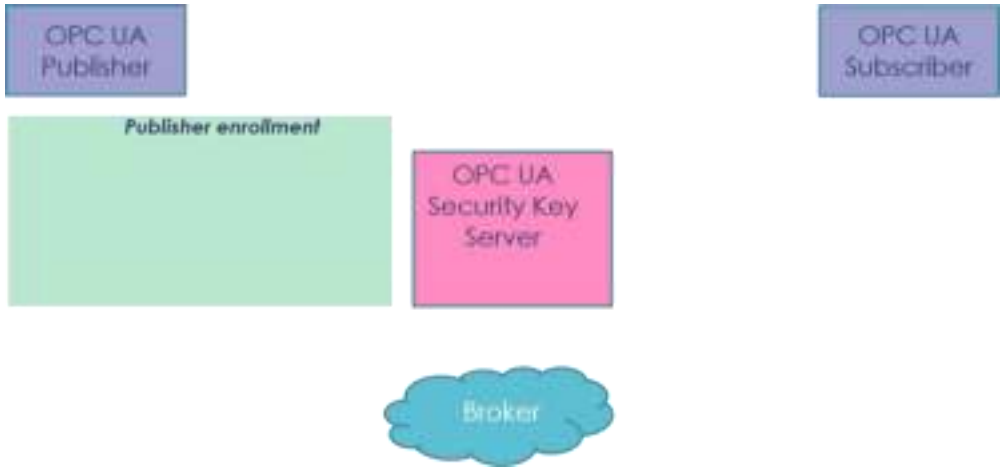
Clients (publishers/subscribers)

- Indirect connection through broker
- End-to-end, symmetric encryption (AES256)
- Initiate key renewal

THALES

OPC UA PubSub Security

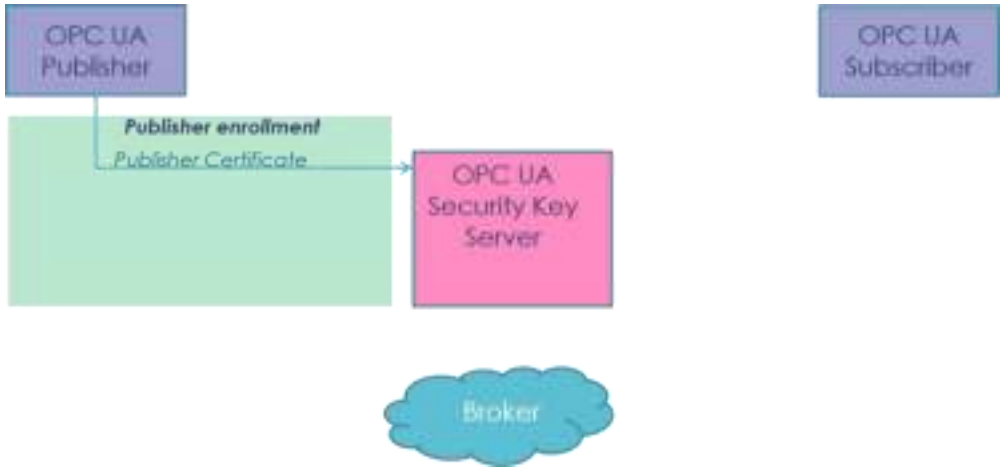
Client authentication by SKS



OPC UA PubSub Security

Client authentication by SKS

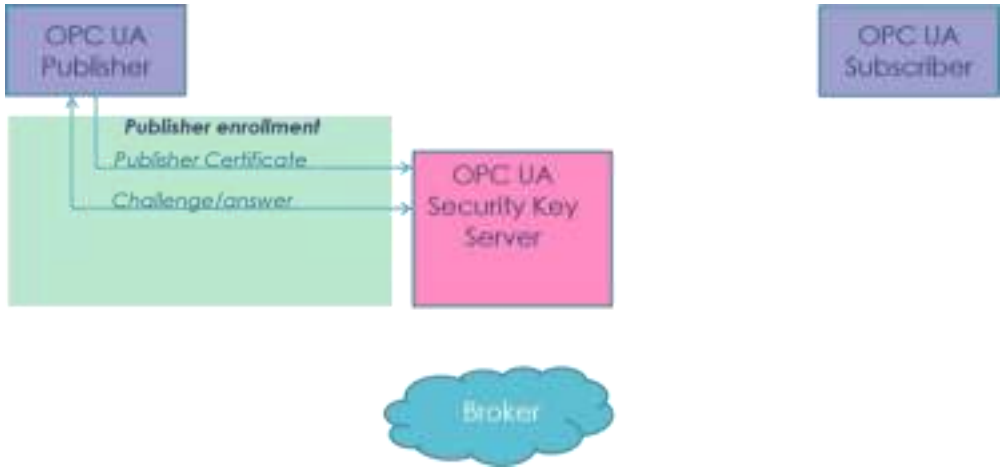
- Client send its certificate incl. public key



OPC UA PubSub Security

Client authentication by SKS

- Client send its certificate incl. public key
- SKS use public key to build a challenge
- Client uses its private key to answer
- RSA2048



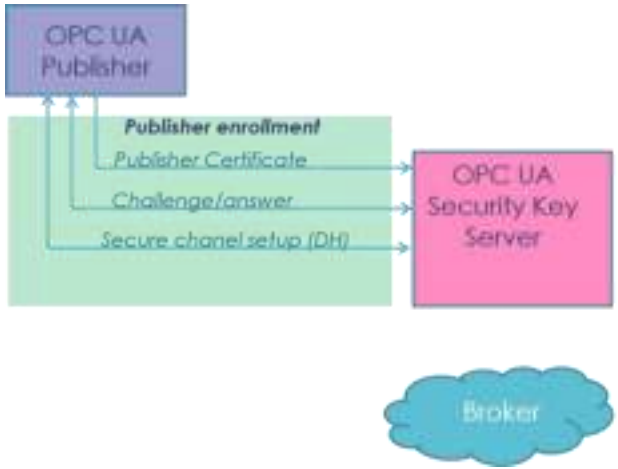
OPC UA PubSub Security

Client authentication by SKS

- Client send its certificate incl. public key
- SKS use public key to build a challenge
- Client uses its private key to answer
- RSA2048

Key distribution by SKS

- SKS and client build a secure channel
- Diffie Hellman



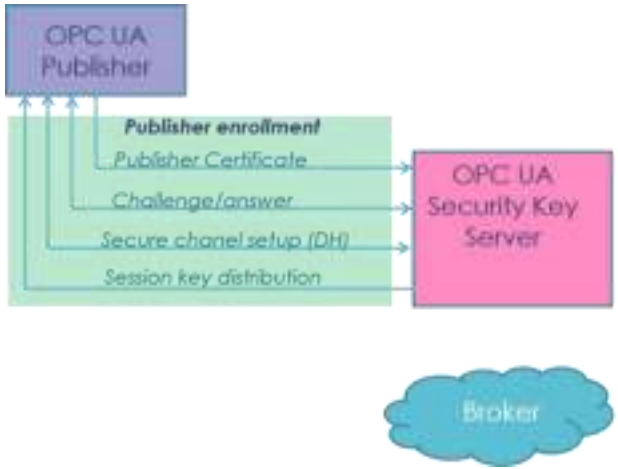
OPC UA PubSub Security

Client authentication by SKS

- Client send its certificate incl. public key
- SKS use public key to build a challenge
- Client uses its private key to answer
- RSA2048

Key distribution by SKS

- SKS and client build a secure channel
- Diffie Hellman
- SKS send the session keys to client



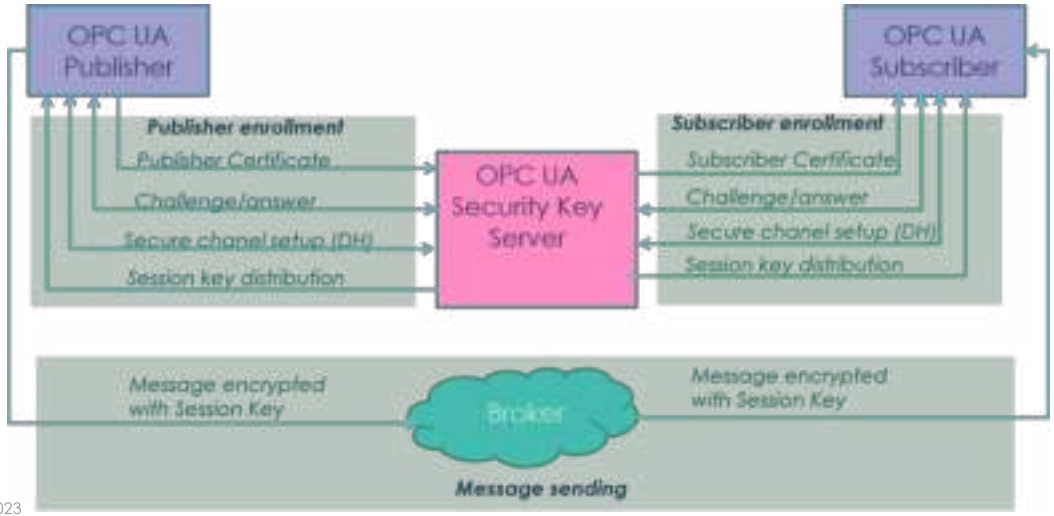
OPC UA PubSub Security

Client authentication by SKS

- Client send its certificate incl. public key
- SKS use public key to build a challenge
- Client uses its private key to answer
- RSA2048

Key distribution by SKS

- SKS and client build a secure channel
- Diffie Hellman
- SKS send the session keys to client



Solution architecture overview

Gateway

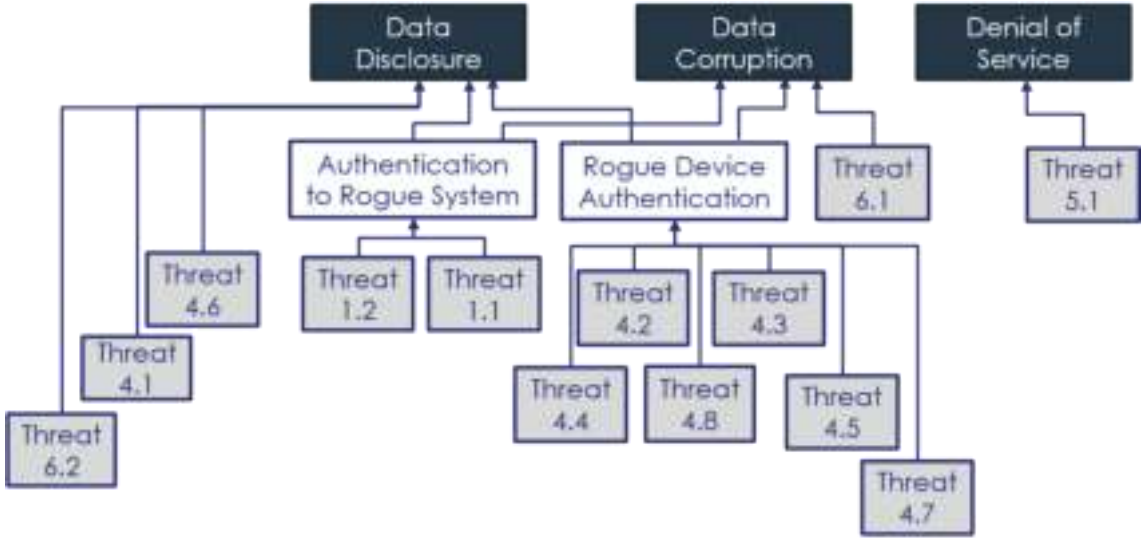
- Connected to sensor through LoRaWAN
- Connected to analytics through LTE + public network

Security

- Gateway-to-backend server encryption

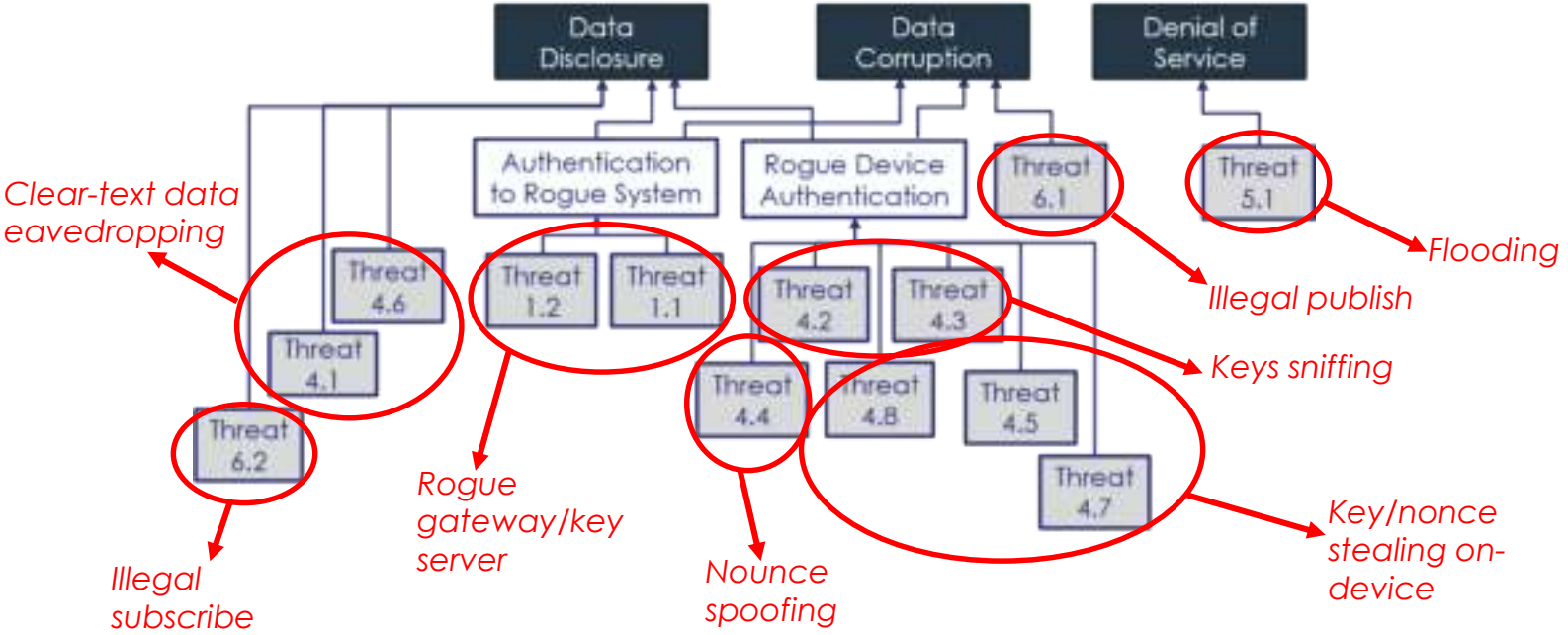
THALES

Threats



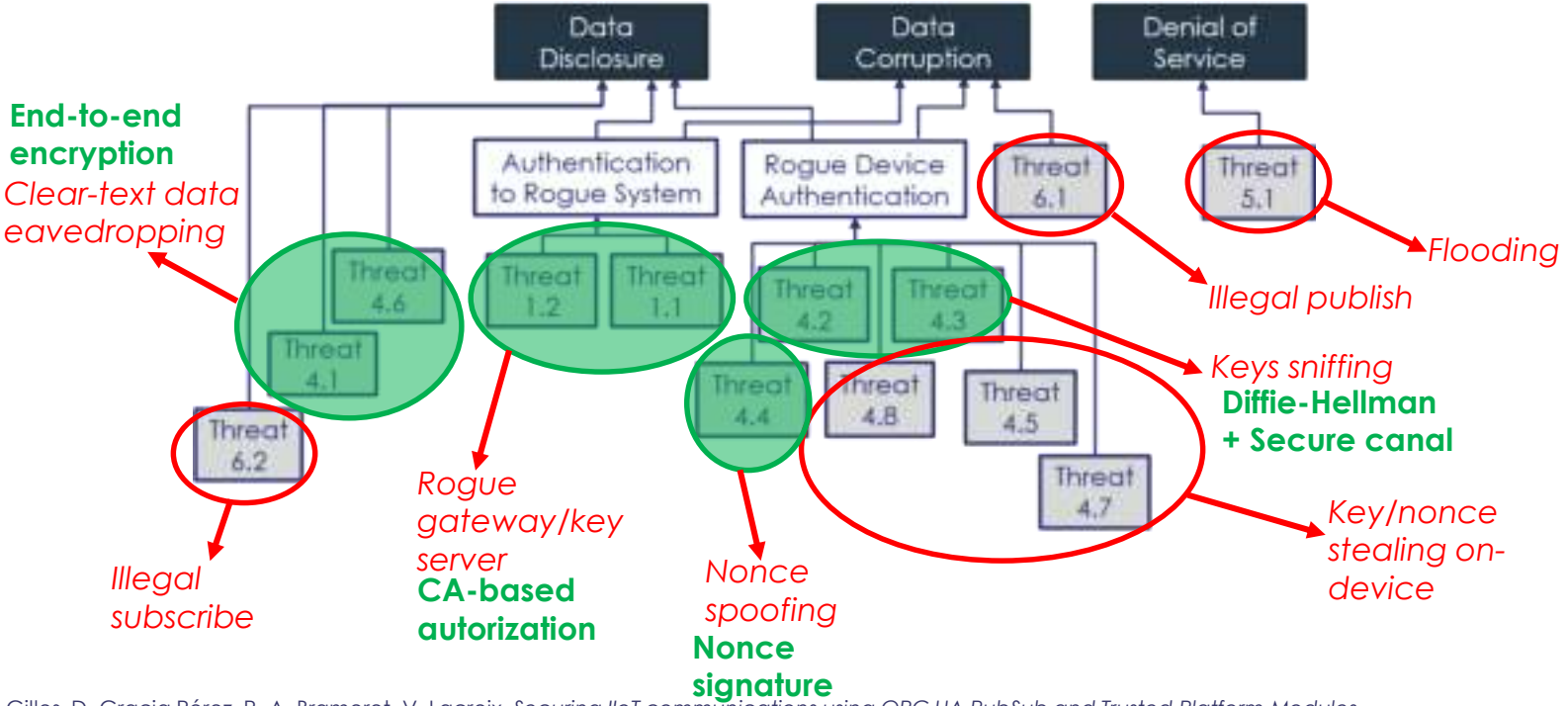
[1] O. Gilles, D. Gracia Pérez, P.-A. Brameret, V. Lacroix, *Securing IIoT communications using OPC UA PubSub and Trusted Platform Modules*, Journal of Systems Architecture, 2023.

Threats



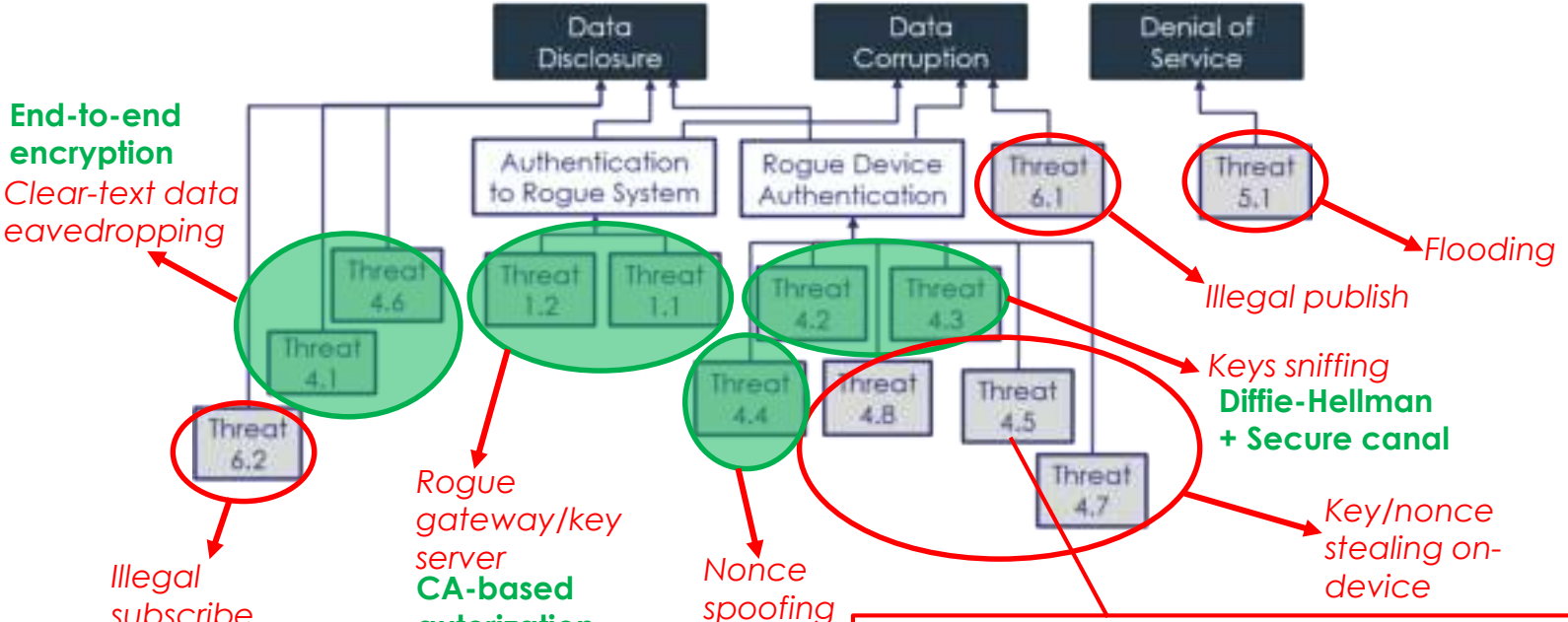
[1] O. Gilles, D. Gracia Pérez, P.-A. Brameret, V. Lacroix, *Securing IIoT communications using OPC UA PubSub and Trusted Platform Modules*, Journal of Systems Architecture, 2023.

Threats: applying OPC UA security



[1] O. Gilles, D. Gracia Pérez, P.-A. Brameret, V. Lacroix, *Securing IIoT communications using OPC UA PubSub and Trusted Platform Modules*, Journal of Systems Architecture, 2023.

Threats: residual risk management



An attacker may extract a legit private key in order to set up a rogue gateway with legitimate credentials

Avoiding residual risk: leveraging on Secure Element

Private key protected by Secure Element

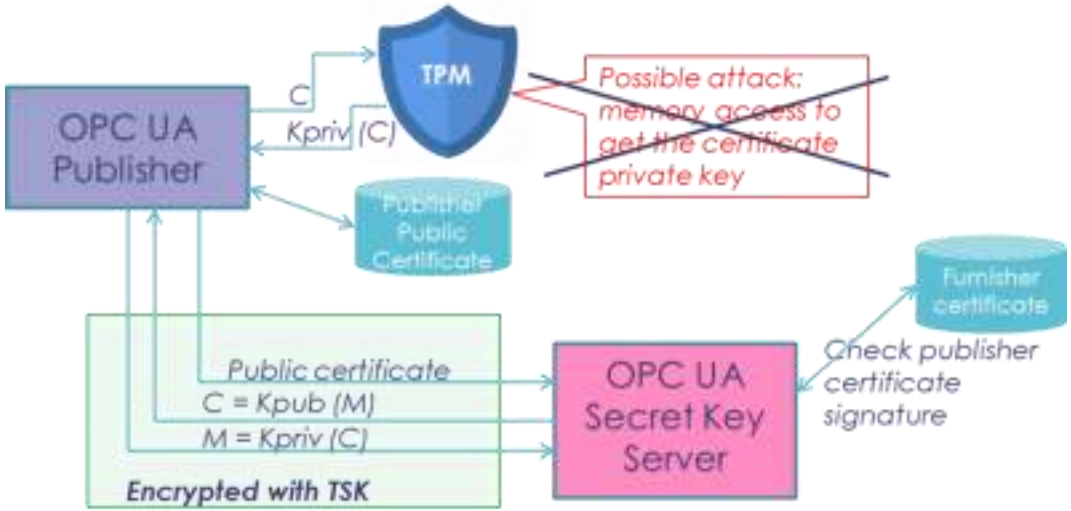
- During generation
- At rest
- While using

Needed SE features

- Asymmetric key generation
- Secure storage
- Limited cryptography

Implementation

- ST33 TPM2



TRUSTed gateway

Integration into STIMIO RAILNET

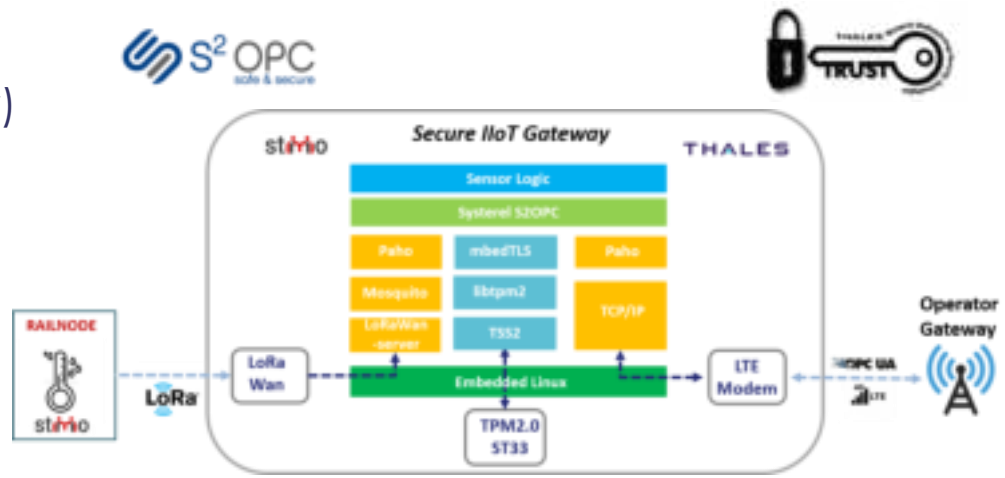
- Mature industrial gateway (railway)
- LoRA + LTE
- STM TPM integrated

OPC UA PubSub ensures

- Interoperability
- Flexible topology
- Reasonnable HW requirements
- End-to-end encryption

Security improvement

- Protection against attacker with physical access



THALES

Going further

From continuous computing to continuous security

- Crossing networks with **data integrity** and **mutual authentication**
- Limited rights (*besoin d'en connaitre*)
- Early rejection of faulty messages
- A new node type is needed (*OPC UA proxy*)

Redundancy with security

- Ensuring « *loose synchronization* » of SKS
- Captured equipment cannot leak keys
- Patent ongoing

Questions ?

Annexes

Industrial networks: legacy and current protocols for M2M

Legacy: Fieldbuses

- Ex: ***MODBUS/RTU***, ***PROFIBUS-DP, CAN***
- Serial link or proprietary bus
- Deterministic
- Periodic, static slots booking
- **No security**

Industrial Ethernet

- Ex: *MODBUS TCP, EtherNet/IP, PROFINET*
- Leverage on Ethernet & IP availability
- On-demand bus booking
- Adapted lower layers
  - Impact on determinism mitigated
  - Support for hardened physical links
  - More than two nodes per link
- **Security**: **Point-to-Point (TLS, DTLS)**

OT/IT convergence

Cybersecurity

Industrial networks: OPC UA

Interoperable

- OS-Independant
- Data format + domain libraries
- Service-Oriented, **Client-Server** paradigm
- Communication-agnostic (Raw Ethernet, UDP, MQTT, HTTPS…)

Secure

- **Standardized, build-in security**
  - Authentication,
  - Encryption
  - Auditing
- Reviewed by BSI (Germany)

Increased connectivity

- Connect existing industrial networks
- Connect to open networks
- **IT/OT convergence**

Security

Residual risks

- **Threat 4.7**: An attacker may try to access to a group key (or multiple ones) on a legitimate gateway => ***accept***
- **Threat 4.8**: An attacker accesses to clear-text server nonce on a legitimate client gateway, and computes locally the session key to get access to the group keys in transit => ***accept***
- **Threat 6.1**: An already compromised subscriber (e.g. a monitoring client) publishes (writing) into its group data instead of reading them => ***accept***
- **Threat 6.2**: An already compromised publisher (e.g. a monitoring client) subscribes (reading) to its group data instead of writing them => ***accept***
- **Threat 5.1**: An attacker floods a SKS with connection requests in order to create a Denial of Service (DoS) for key distribution => ***ext. counter-measures***
- ***Threat 4.5**: An attacker may extract a gateway's private key in order to set up a rogue gateway with legitimate credentials => **avoid***

Embeddability : Bandwith

UDP / Binary

- Different kind of messages, **many optional fields**
- **Minimal overhead is 19 B (27 B over UDP)**
- MQTT/TCP: 22 B
- CoAP/UDP: 12 B (most of the time over IPv6, 20 B increase)
- Still have to add Link-level protocol (24 B for Ethernet)

Data profile	Frame size OPC-UA PUBSUB Heavy	Frame size OPC-UA PUBSUB Light	Ratio
Non-secure Short Message **(8 B)**	85 B	31 B	63%
Secure Short Message **(8 B + signing)**	117 B	67 B	42%
Secure Medium Message **(32 B + signing)**	149 B	91 B	39%
Secure Long Message **(1024 B + signing)**	1141 B	1083 B	5%

Embeddability: Memory footprint

Experimental

- Down to 10 KB (ROM)

Commercial : different server profile

- Systerel S2OPC : 160 KB (PUBSUB + Client/Server) + 4 KB/session + 16 KB/request
- Matrikon OPC UA SDK

FLASH and RAM

Table 2: Minimum Server Footprint		
Profile Configuration	**Flash (kB)***	**RAM (kB)**
Nano Embedded Device Server	461	48
Micro Embedded Device Server (4 Monitored items)	550	80
Embedded Server (including security and full address space and 10 Monitored Items)	675	208
Embedded Server (including security and full address space and 100 monitored items)	675	320

*Metrics obtained for ARM Thumb2 instruction set (Cortex-M4F), Atollic TrueSTUDIO 4.20, GCC -Os

OPC UA PubSub Stack: Safe & Secure OPC

Embeddability

- Down to 150 KB of RAM for a node
- Support Windows, Linux, FreeRTOS, Zephyr, VxWorks
- On-developpment TSN support

Business-ready

- Deployed by Schneider Electrics, Renault
- Open-source & Free

Safety & Security

- Formal proof of code with B method
- Deployed in EN50128 SIL2 environment
- Aims for EAL 4+ certification (ANSSI)
- **Integrating TRUST**

Systerel

- Developped by a french PME
- Long-term partnership with Thales
- Specialized in safety