Cyber sécurité pour l'IoT

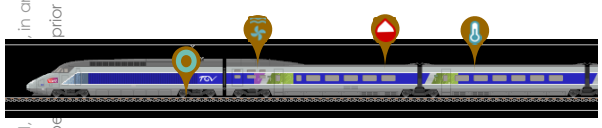
quels risques et quelles solutions ?

BILAN ET RISQUES ACTUELS POUR LE FERROVIAIRE

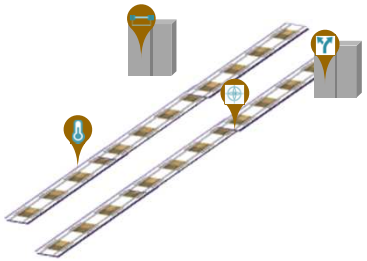
THALES

Etat de la cyber sécurité dans l'Internet des objets (IoT) de transport

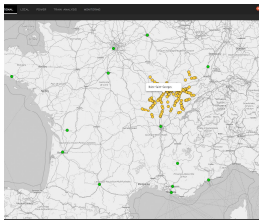
Trains connectés



Voies connectées



Smart Stations, SCADA, & télé-localisation des trains



- **Manque de contrôle d'accès sur les capteurs-**

Vulnerabilité, pas de rôles filtrant les usages

Nimporte quel hacker peut simuler un mainteneur

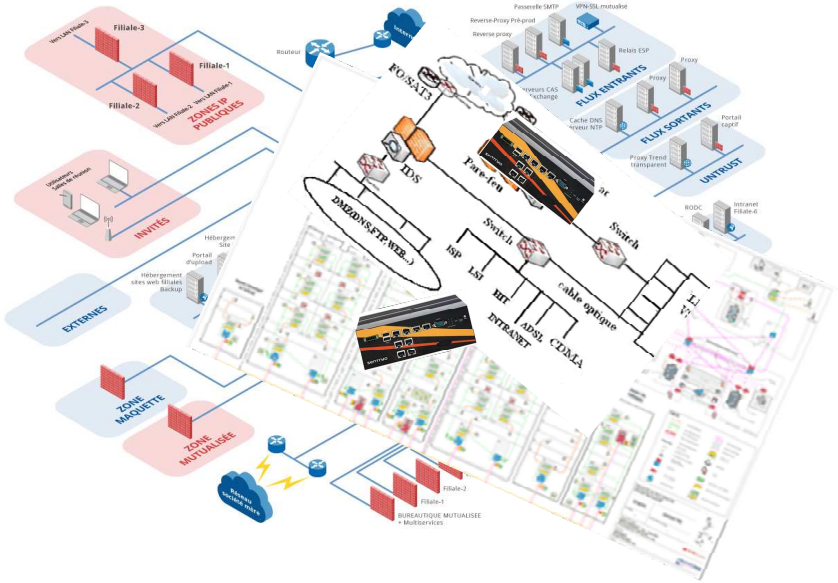
- **L' IoT et les SCADA déployés sont un patchwork multi-vendeurs**

Nombreux protocoles de réseau

THALES

Etat de la cyber sécurité dans l'Internet des objets (IoT) de transport

« Les cyberattaques profitant de la vulnérabilité des objets connectés représentent un pourcentage croissant des attaques , avec encore +50% d'augmentation en 2019 par rapport à 2018 » *



- **Sondes réseau absentes, ou mises à un niveau très global (exemple : gare)**

➡ **Faiblesse dans la détection**

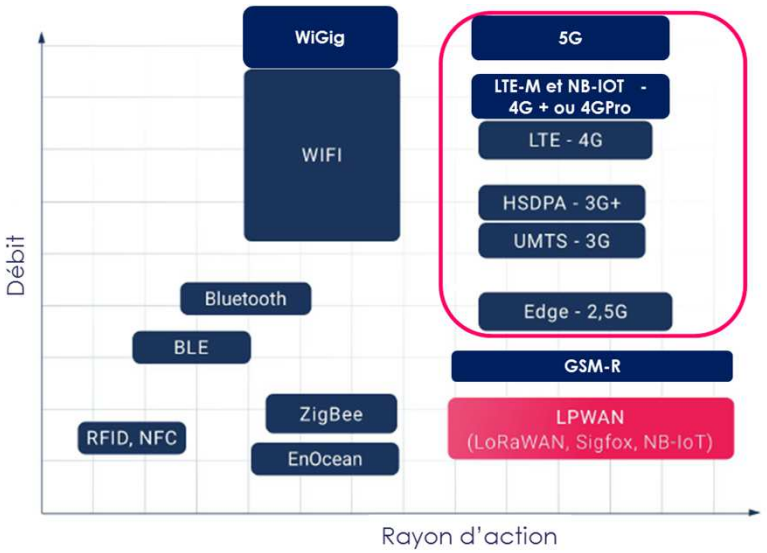
- **Réseaux et règles de pare-feu complexes**

➡ **Faiblesse dans l'évaluation**

*** Source Veritas – taskforce Cybersécurité**

THALES

Etat de la cyber sécurité dans l'Internet des objets (IoT) de transport



- **Héritage : réseaux informatiques câblés**
  Pas de sécurisation sous le principe de la protection périmétrique (emprise locale)

  Au mieux séparation des réseaux IS / IoT

- **Nouvel IoT : usage de la 3G/4G et de LoraWan**

⇨ **Pas de chiffrement privé**

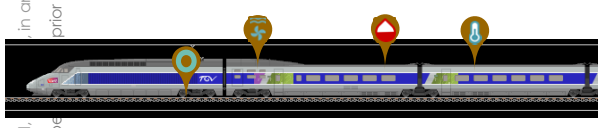
⇨ **Hackers très à l'aise en 3G/4G**

Le risque principal est sur les points non-GSM-R et sans fibre optique ferroviaire

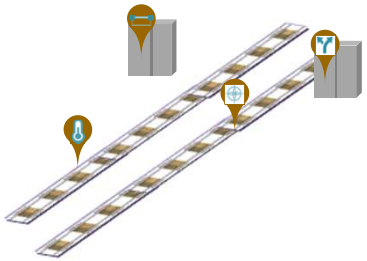
THALES

Quelles conséquences Cyber pour l'IoT ferroviaire

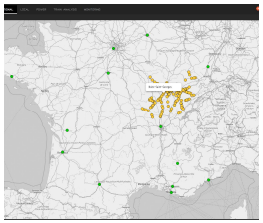
Trains connectés



Voies connectées



Smart Stations, SCADA, & télé-localisation des trains



- Que peut faire un hacker avec l'IoT ferroviaire ou les SCADA?
  - Déplacement de mainteneurs inutile
  - Camouflage d'un sabotage réel
  - Atteinte à l'image de marque / publicité sur la compromission.
  - Changement de tous les logiciels et seuils

THALES

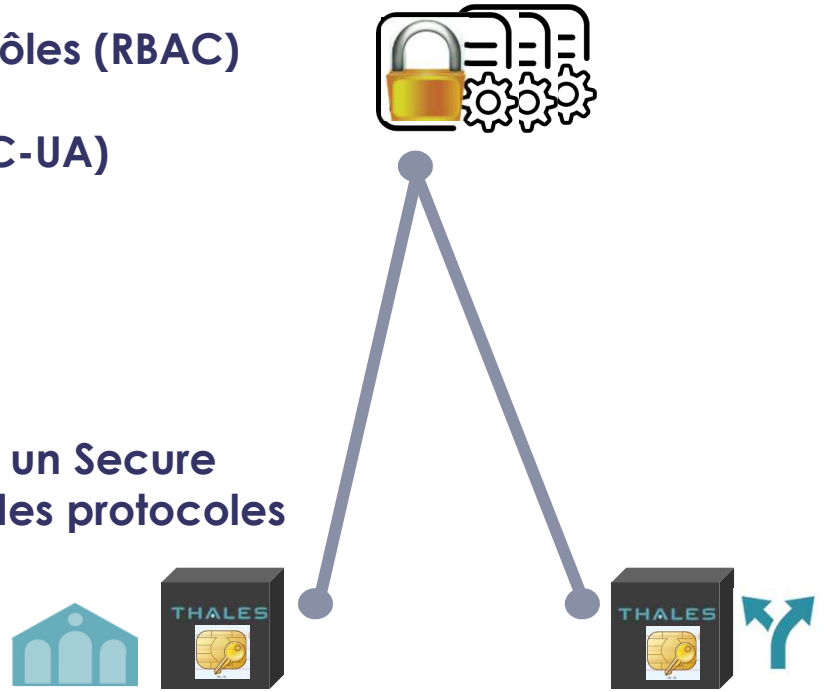
QUELLE ARCHITECTURE CYBER EN 2019 POUR l' IOT ?

THALES

Thales propose une nouvelle approche pour sécuriser l'IoT

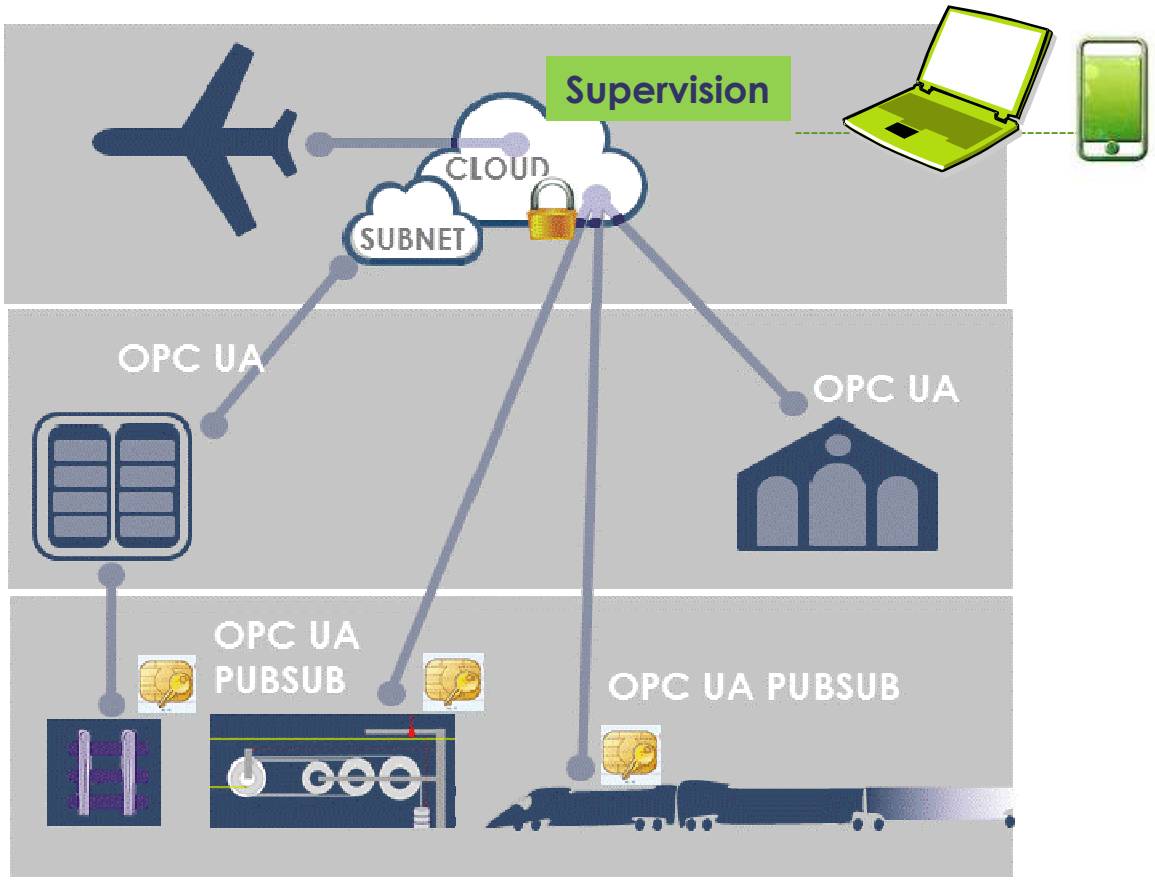
Partant d'une étude de risque conforme à IIEC - 62443 nous proposons:

- **Un Contrôle d'Accès centralisé basé sur des rôles (RBAC)**
- **Des profiles de sécurité de bout en bout (OPC-UA)**
- **Un équiment autonome à l'Edge comprenant un Secure Element HW. Cette Edge box est agnostique des protocoles et OS des capteurs ou PLC qu'elle sécurise.**
- **Un enrôlement industriel des équipements distribuant les clés en confiance.**



THALES

Utilisation d' OPC-UA PubSub



THALES

Utilisation de l'expérience télécom de Thales DIS (ex GEMALTO) : la Edge box

- Module 3G/4G Thales DIS, qui deviendra Module 5G
  - Cœur à venir du remplacement GSM-R(FRMCS)

- Secure Element / TPM portant la solution Thales DIS pour la protection des clés
- Co-processor du modem Thales avec le stack OPC-UA PubSub & plus (AI ready)
- Enrôlement Thales utilisant des clés « 2020 » et un identifiant d'accès.

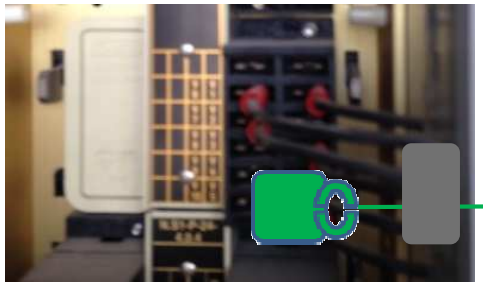
THALES

CAS D'USAGE TYPIQUES

THALES

Supervision d'équipements de signalisation en guérite par exemple

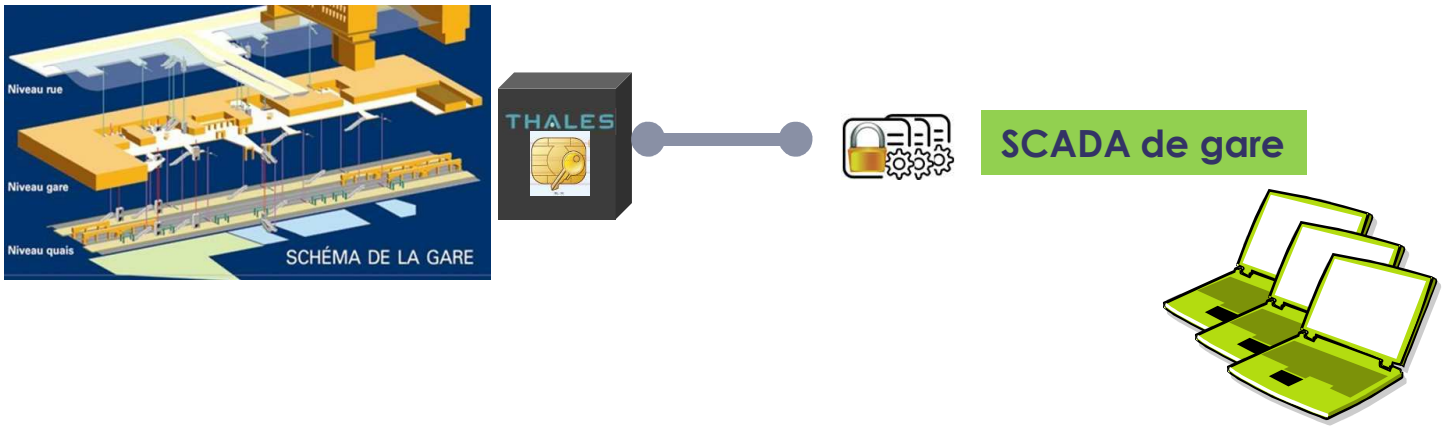
- **Micro – capteur non intrusif**



- **Profil SC3 après étude de risque IEC443 SC3 (chiffrement des données)**
- **Enrôlement industriel par smartphone – génération des clés**
- **OPC-UA Pubsub permet une sécurisation de bout en bout, quelquesoit le support télécom utilisé.**

THALES

Smart stations et Scadas

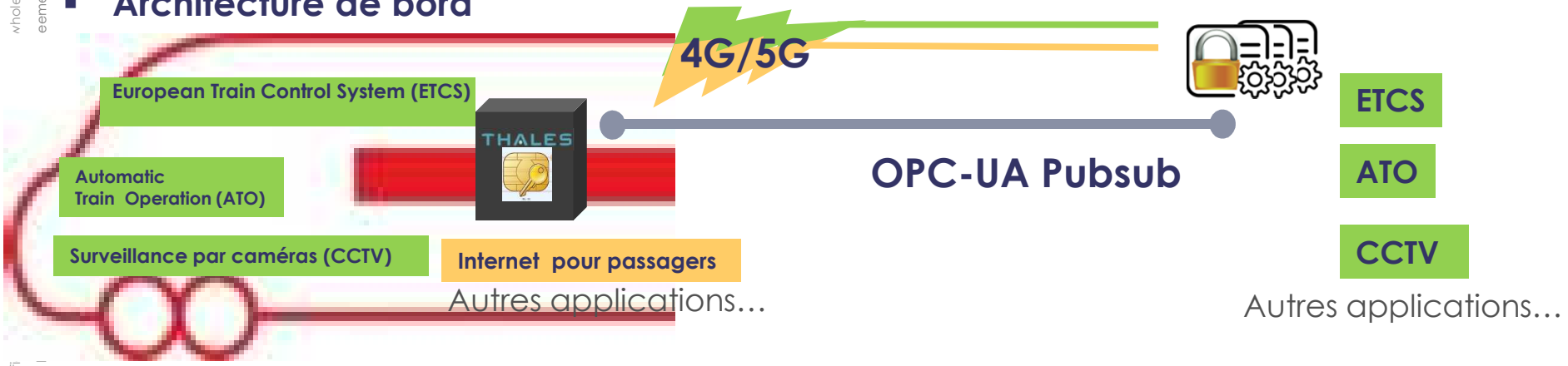


- **Profil SC3 d'une gare après étude de risque IEC443 SC3 (chiffrement des données)**
- **Echange des clés et vérification des droits d'accès (dialogue SKS - Edge box)**
- **Rôles des mainteneurs par métier et par géographie**
- **Mesures transmises par OPC-UA PubSub sur ligne mobile pour les petites gares n'ayant pas accès à la fibre, ou pour les grandes gares dans lesquelles la liaison mobile sert de sécurisation.**

THALES

Cyberprotection des Liaisons sol-bord.
Candidat cyber dans le Remplacement du GSM-R par le FRMCS

- **Architecture de bord**



- **Chiffrement des données nécessaire de bout en bout (applications critiques) à l'aide d'une clé privée, et distribution de clés par conversation pour chaque domaine applicatif.**

- **Essentiel sur les lignes où la liaison sol-bord utilise les Opérateurs mobiles publics.**

THALES