📡 Module 1

Fondements et Enjeux de l'IoT

Intervenants : **Réda BOUREBABA** & **Sébastien Antonico**
Environnement : PlatformIO / Framework Arduino (C++)

📝 Changelog — V0.1.0

- Création du module Microcontrôleurs & IoT.
- Deck 1 : Histoire, domaines d'application, sécurité.

🌐 Qu'est-ce que l'IoT ?

> *L'Internet des Objets désigne l'extension du réseau Internet à des **objets du monde physique**.*

Ces objets collectent, traitent et transmettent des données de façon **autonome**, sans intervention humaine directe.

Exemples concrets :

- Un thermomètre qui envoie la température toutes les 5 minutes ☁️
- Une serrure déverrouillée par smartphone 🔑
- Un capteur vibratoire qui prédit une panne moteur avant qu'elle survienne ⚙️

⏳ Une histoire plus vieille qu'on ne le croit

- **1982** — Machine à soda à Carnegie Mellon : premier objet connecté via ARPANET
  (vérifie l'inventaire & la température des canettes à distance)
- **1990** — John Romkey : grille-pain connecté à Internet (1ère démo publique IoT)
- **1999** — Kevin Ashton (MIT/P&G) invente officiellement le terme **"Internet of Things"**

Le concept était là bien avant les smartphones !

📈 L'explosion des objets connectés

🏠 Le Nabaztag : l'IoT entre dans les foyers (2005)

Le **Nabaztag** est un lapin Wi-Fi communicant, véritable symbole de l'ère IoT grand public :

- Lit les e-mails à voix haute 🐰
- Bougent ses oreilles selon la météo
- Premier objet domotique réellement déployé à grande échelle

> *Un objet du quotidien, enrichi par la connectivité.*

M2M → IoT consommateur : la transition est lancée.

🏭 De l'industrie au grand public

Ère	Technologie	Exemple
Années 90	M2M (Machine to Machine)	SCADA industriel
2000s	RFID, capteurs sans fil	Suivi de palettes
2010s	Wi-Fi, BLE, smartphones	Thermostats Nest
2020s	LoRa, 5G, Edge AI	Villes intelligentes

L'IoT est **l'informatique qui sort des écrans** pour entrer dans le monde physique.

🌍 Domaines d'application

🏠 Domotique (Smart Home)

Le foyer connecté en pratique :

- **Thermostats intelligents** : apprentissage des habitudes, économies d'énergie
- **Éclairage adaptatif** : capteurs de luminosité, détecteurs de présence
- **Sécurité** : caméras IP, alarmes connectées, serrures numériques
- **Assistants vocaux** : Alexa, Google Home comme hub central

Protocoles typiques : Zigbee, Z-Wave, Matter, Wi-Fi, BLE

🌆 Smart City

La ville intelligente gère ses ressources en temps réel :

- **Éclairage public** adaptatif selon la circulation (économies 40-60%)
- **Gestion des déchets** : capteurs de remplissage pour optimiser les tournées
- **Trafic** : feux intelligents coordonnés, détection d'accidents
- **Eau** : surveillance des réseaux, détection de fuites

> *Exemple : Santander (Espagne) — 20 000 capteurs pour 180 000 habitants.*

🏥 Santé Connectée & Industrie 4.0

Santé (e-Health) :

- Suivi continu des constantes (glycémie, ECG, SpO_2)
- Détection automatique de chutes *(seniors)*
- Piluliers connectés, rappels médicaments

Industrie 4.0 :

- **Maintenance prédictive** : vibration + IA → panne prévue 3 semaines avant
- Robotique collaborative (cobots connectés)
- Jumeaux numériques (Digital Twins)

⚠️ L'IoT interagit avec le monde physique

L'informatique web : vol de données, ransomware → impact numérique
L'IoT : agit sur des **capteurs et des actionneurs** → impact physique

> *Un bug dans un thermostat peut geler une maison.*
> *Un pacemaker piraté peut tuer.*

Cela change radicalement le niveau de responsabilité du développeur embarqué.

🔒 Surface d'attaque IoT

Risques sur les capteurs

Les capteurs sont les **yeux** du système IoT :

Vecteur	Exemple d'attaque	Conséquence
Manipulation physique	Cache sur capteur CO_2	Pas d'alarme incendie
Injection de signal	Laser sur capteur image	Aveugler une caméra autonome
Spoofing GPS	Fausse position	Détournement de véhicule
Falsification thermique	Chauffage de thermomètre	Système de refroidissement désactivé

🔧 Risques sur les actionneurs

Les actionneurs sont les **muscles** du système IoT :

- **Pompes & vannes** : inondation volontaire, coupure d'eau
- **Moteurs** : sabotage de chaînes de production
- **Relais électriques** : déclenchement/coupure à distance
- **Portes & serrures** : intrusion physique

Cas réel 2021 : Station de traitement de l'eau d'Oldsmar (Floride) — un attaquant a tenté de modifier le taux de NaOH × 111.

🔐 Bonnes pratiques de sécurité IoT

1. **Chiffrement** : TLS/DTLS pour toutes les communications
2. **Authentification** : certificats ou tokens, jamais de mots de passe par défaut
3. **Firmware signé** : vérifier l'intégrité avant OTA update
4. **Segmentation réseau** : IoT sur VLAN séparé du réseau principal
5. **Surveillance** : logs d'anomalies, détection d'intrusion
6. **Principe du moindre privilège** : un capteur n'a accès qu'à son topic MQTT

> *La sécurité IoT n'est pas optionnelle — c'est une question de vie ou de mort.*

🎯 Synthèse du Module 1

Concept	Retenir
Définition IoT	Réseau étendu aux objets physiques
Histoire	1982 → 2005 → 30 milliards en 2025
Domaines	Domotique, Smart City, Santé, Industrie
Spécificité	Interaction avec le monde physique
Sécurité	Risques matériels, pas seulement numériques

Prochain module → Architecture Matérielle & Choix Technologiques

👨‍💻 Questions ?

Module 1 — Fondements IoT

Réda BOUREBABA & Sébastien Antonico