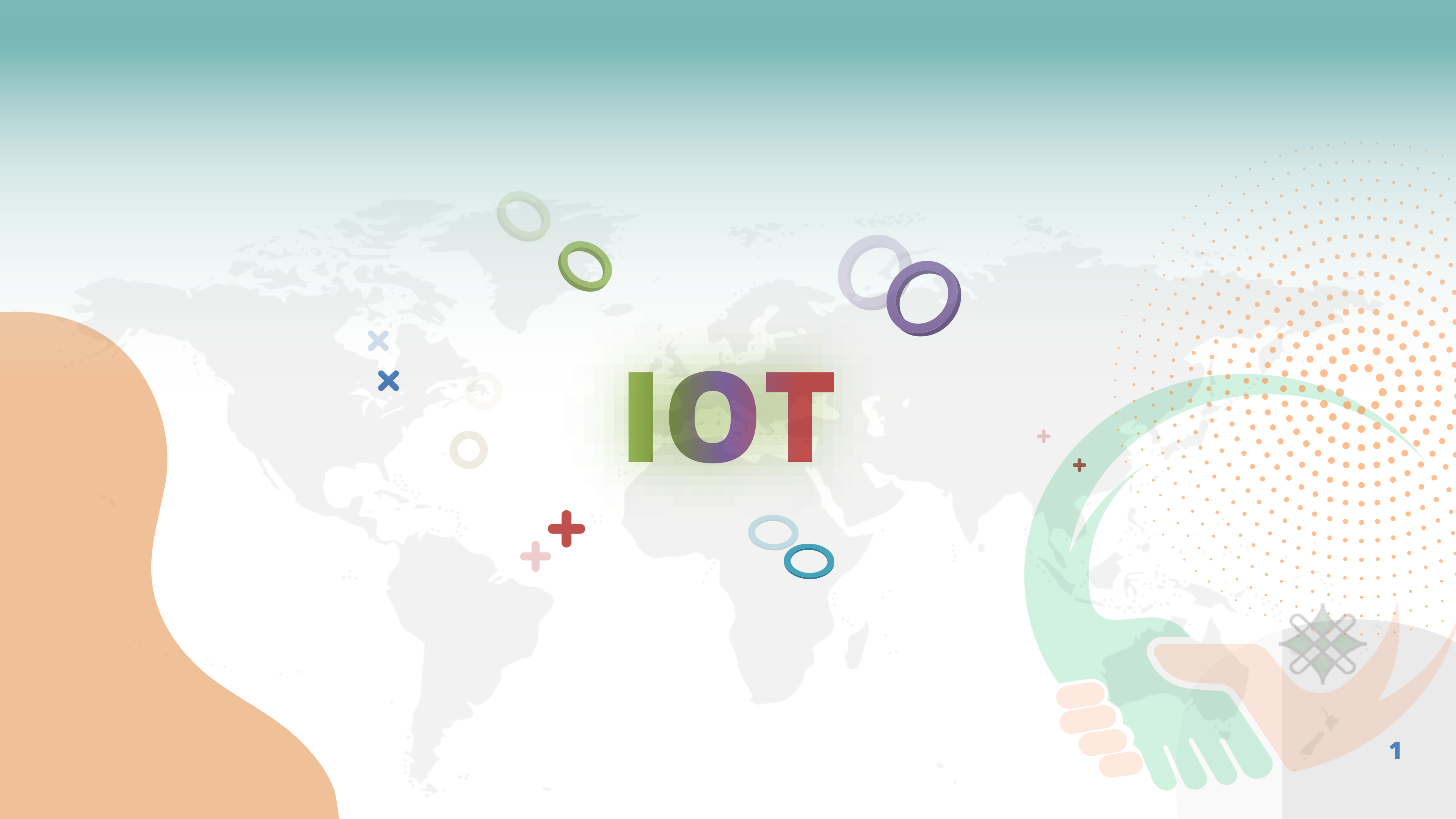
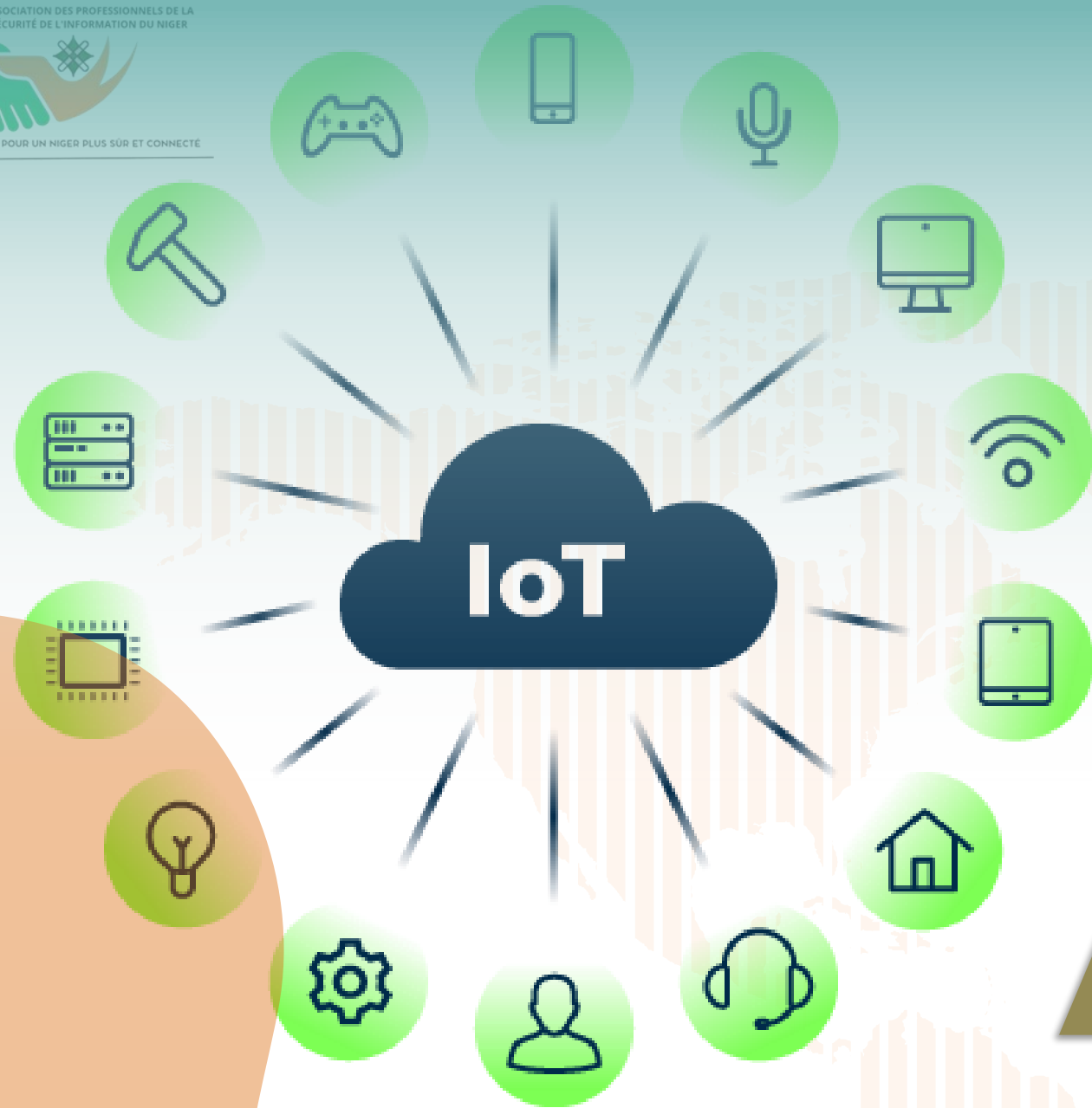




IOT



CYBERSÉCURITÉ DES OBJETS CONNECTÉS (IOT) & DES SYSTÈMES INDUSTRIELS.

Présentation :

- Abdoul Karim MAMANI MALAM GOGA
- Maliki SOUMANA HAMIDOU
- Harouna CHAIBOU ADAMOU

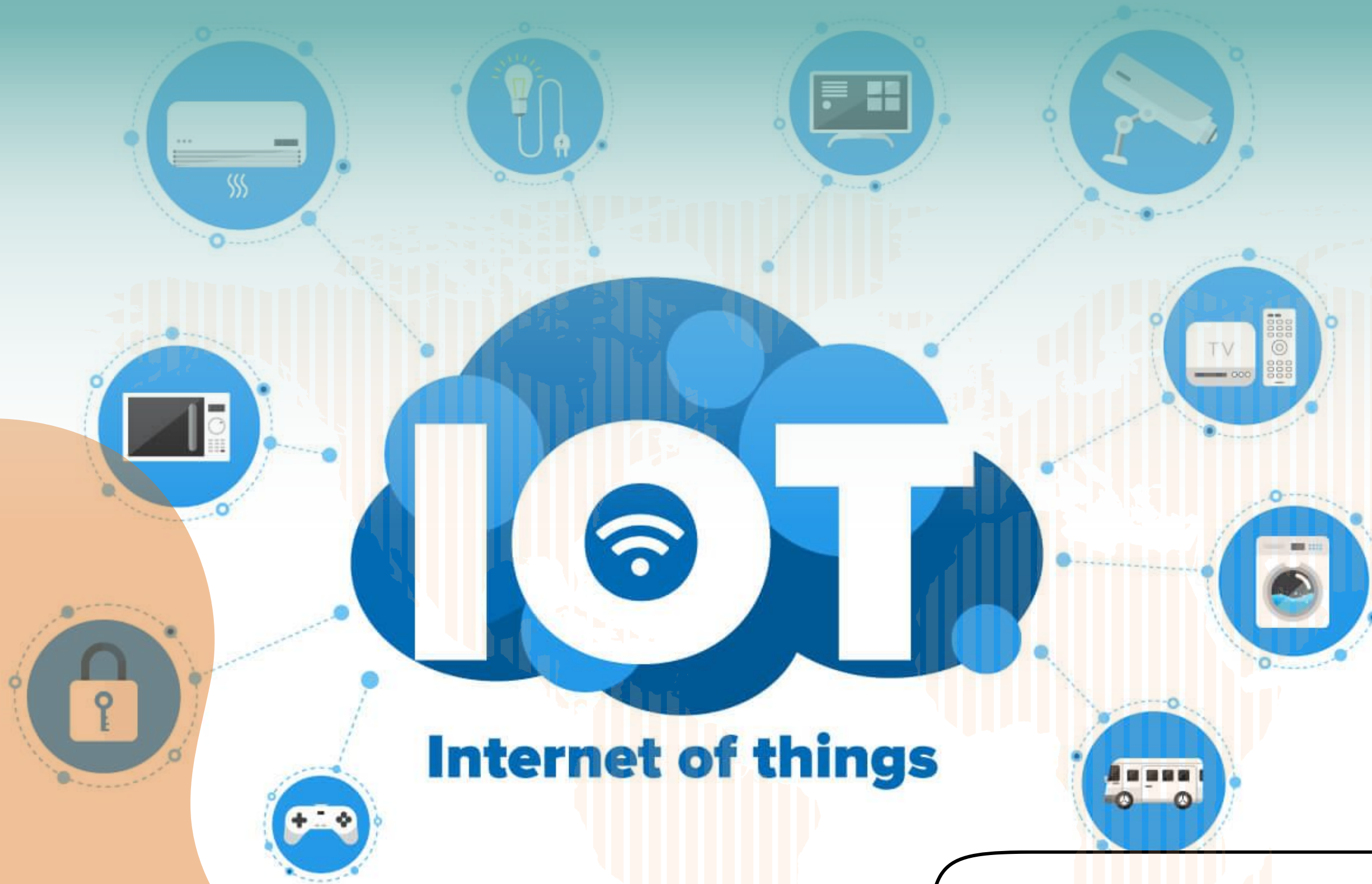
**Introduction
Générale**

**Menaces majeures
dans l'IoT et ICS**

**Qu'est-ce que
l'IoT**



**Prochaine
Session**



INTRODUCTION GÉNÉRALE

OBJECTIF DU MENTORAT

Comprendre les Technologies IoT, ICS et IIoT :

- Découvrir les concepts clés.
- Analyser les cas d'usage dans différents secteurs.

Comprendre leur importance:

- Explorer l'impact de des technologies.
- Voir les bénéfices liés à l'adoption de ces technologies.

Identifier leurs vulnérabilités et comment les sécuriser :

- Détecter les principaux risques.
- Apprendre les meilleures pratiques de cybersécurité.

CONTEXTE GLOBAL

L'Internet des Objets (IoT)

- redéfinit notre société moderne en connectant des milliards d'objets à travers le monde : Maison, Véhicules, Équipements Industriels, Agriculture, Ville etc.

Les Systèmes de Contrôle Industriels (ICS)

- jouent un rôle essentiel dans la gestion automatisée des infrastructures critiques telles que les réseaux électriques, les usines de fabrication, les systèmes de distribution d'eau, etc.

Intégrés à l'IoT, les ICS

- jouent un rôle clé dans l'optimisation du contrôle et le renforcement de la supervision des opérations industrielles. Cette convergence donne naissance à l'Internet Industriel des Objets (IIoT), qui permet une gestion intelligente et sécurisée des infrastructures critiques.

LES BÉNÉFICES MAJEURS DE L'IOT ET DES ICS

■ Surveillance en Temps Réel :

- Santé Connectée
- Sécurité Publique
- Gestion des Infrastructures Critiques

■ Collecte et Analyse de Données Massives (Big Data) :

- Business Intelligence
- Machine Learning et IA

■ Réduction des Coûts :

- Maintenance Prédicative
- Bâtiments Intelligents
- Agriculture Intelligente

Inconvénients de l'IOT



Sécurité

Facilité pour les pirates de s'introduire dans les appareils.
Peut conduire à des systèmes dangereux.



Vie privée

Collecte de nombreuses informations personnelles.
Peut suivre les personnes à leur insu



Coûts

L'installation et l'achat d'appareils sont coûteux.
Nécessite des corrections et des mises à jour régulières, qui coûtent de l'argent.



Connectivité et dépendance excessive

L'IOT a besoin d'un internet stable pour fonctionner, et les perturbations peuvent provoquer des pannes.
Avec le temps, les gens risquent de trop se fier aux appareils, ce qui réduit leur capacité à résoudre les problèmes manuellement.

Nombre d'objets connectés :

Lorem 18,8 Milliards fin 2024 et 40 Milliards d'ici 2030 (Source : IoT Analytics, State of IoT Summer 2024)
is simply dummy text of the printing and typesetting.

Impact économique de l'IoT :

L'IoT pourrait générer entre 3 900 et 11 100 Milliards USD de valeur économique d'ici fin 2025 (Source : McKinsey Global Institute)

N

S

I

A

STATISTIQUE
S CLÉS SUR
L'IOT

Sécurité des objets connectés :

70 % des objets connectés présentent des vulnérabilités sérieuses de sécurité (Source : HP Security Research, rapporté par la FTC)

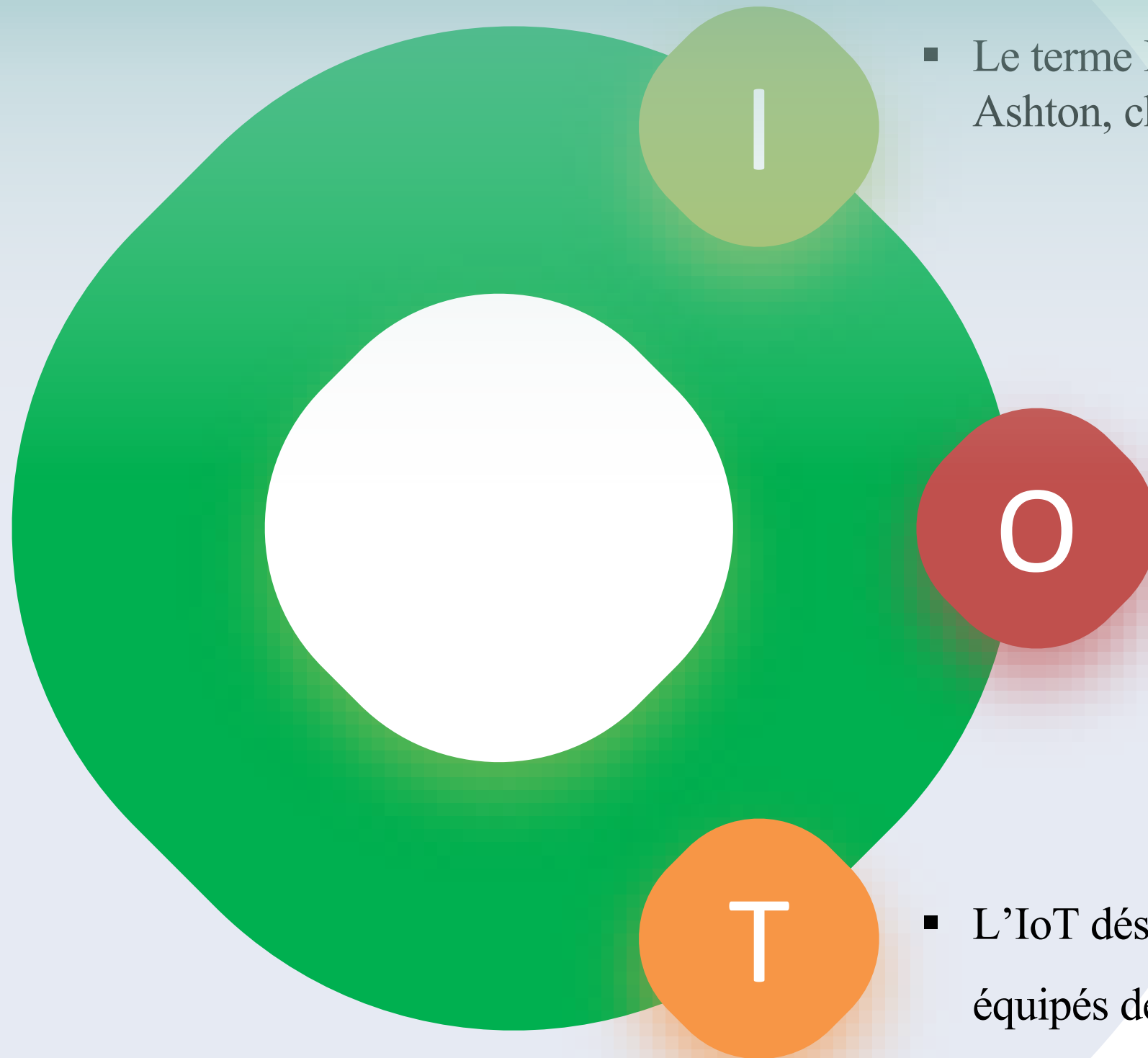
Adoption de l'IoT par les entreprises :

80 % des entreprises ont déjà intégré l'IoT dans leurs opérations pour optimiser les processus (Source : Forbes, cité par G2 Learn)



QU'EST-CE QUE L'IOT

DÉFINITION DE L'IoT



- Le terme Internet des Objets (IoT) a été introduit en 1999 par Kevin Ashton, chercheur au MIT, dans le contexte d'un suivi logistique (RFID).
- L'IoT permet une intégration entre le monde **physique** et les **systèmes numériques**.
- L'IoT désigne un **réseau d'objets physiques** connectés à **Internet**, équipés de **capteurs**, d'**actionneurs**, de **logiciels** et de **technologies de communication**, leur permettant de **collecter**, **échanger**, **analyser** des données et **d'agir**.

CAS D'USAGE DE L'IoT

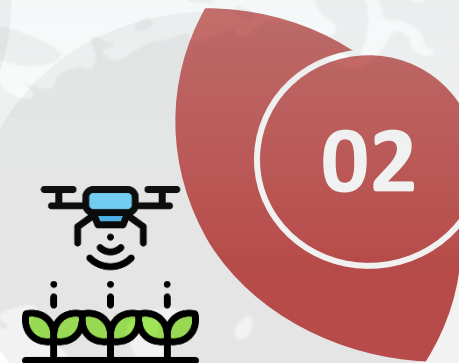
SMART HOME



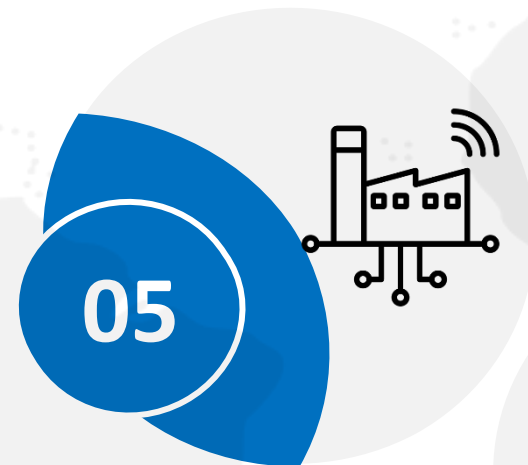
SMART HEALTHCARE



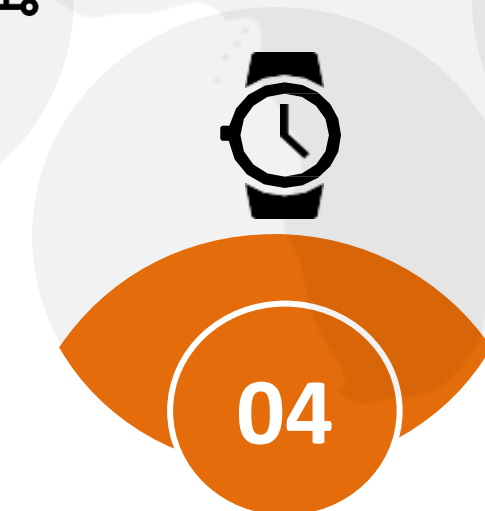
SMART AGRICULTURE



INDUSTRY 4.0

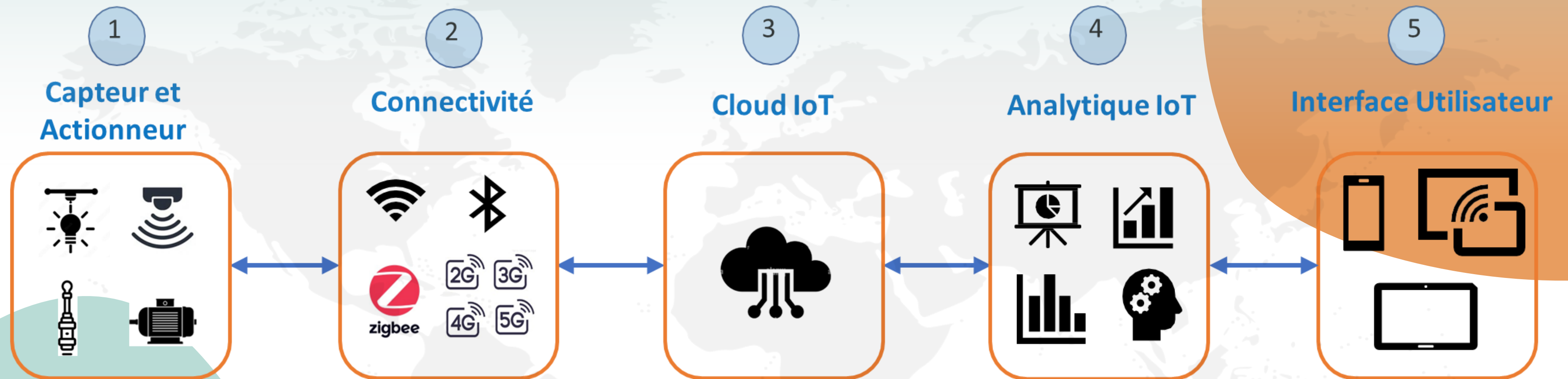


SMART CITY

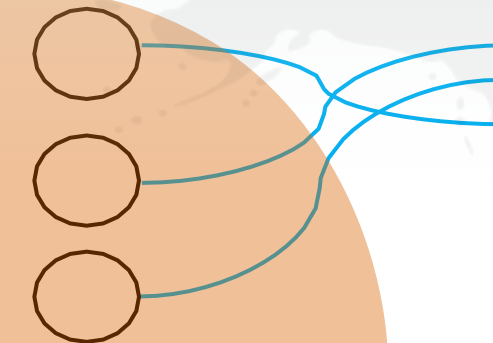
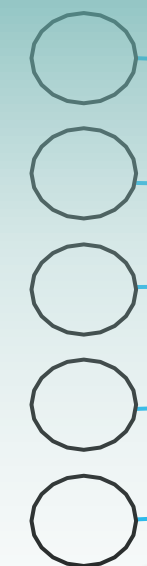


WEARABLES

LES COMPOSANTS DE L'IOT



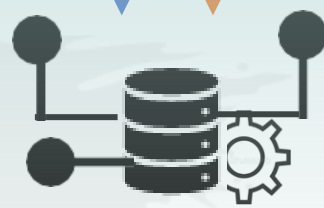
Sensors, Actuators
& Smart Devices



Sensors, Actuators
& Smart Devices



Cloud
Gateway



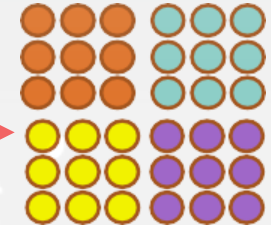
Streaming data
Processor



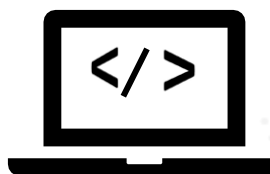
Sensor
Data



Data Lake



Big Data Warehouse



Web Application



Mobile Application



User Business Logic



Device
Administration



User
Administration



Security
Monitoring



Control
Data



Control
Applications



Models



Machine Learning



Data Analytics

CAPTEURS

■ **Un capteur** est un dispositif qui capte des informations physiques (température, pression, mouvement, lumière, etc.) et les convertit en signaux électriques exploitables (analogiques ou numériques). Ces données sont ensuite transmises aux systèmes embarqués (microcontrôleurs ou microprocesseurs) pour analyse et action.

■ **Exemples de Capteurs :**

○ **Smartphone :**

1. Accéléromètre
2. Capteur de lumière ambiante

○ **Montre connectée :**

1. Capteur de fréquence cardiaque
2. Capteur de température cutanée

○ **Véhicule connecté (eCall) :**

1. Capteur de choc
2. Capteur GPS
3. Capteur d'inclinaison

Position



SON



Flux



Température



Charge



Touché



Vitesse



Gaz



ACTIONNEURS

- Un **Actionneur** est un dispositif qui déclenche une action pour contrôler un dispositif, en réponse à un signal reçu d'un **Capteur**.

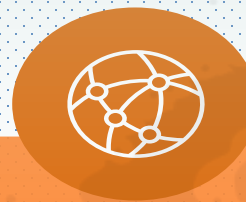


■ Serrure connectée :

- Moteur électrique
- Alarme sonore

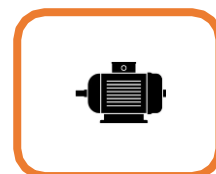


POMPE



■ Surveillance en Temps Système d'irrigation connecté:

- Capteur d'empreinte digitale



MOTEUR



HAUT-PARLEUR



■ Détecteur de gaz connecté :

- Vanne d'arrêt automatique
Intelligence



VANNE

M2M ET IOT

- **M2M (Machine-to-Machine)** représente la communication directe entre deux machines (capteurs, dispositifs industriels, etc.).
- **IoT (Internet of Things)** élargit le concept de M2M en intégrant une communication internet complète entre les objets.

Tableau Comparatif : M2M vs IoT

Critère	M2M (Machine-to-Machine)	IoT (Internet of Things)
Objectif	Communication directe entre machines pour un usage spécifique	Interconnexion d'objets à grande échelle avec communication Internet
Technologie réseau	Protocoles non-IP (GSM, CDMA, réseaux propriétaires)	Protocoles IP (IPv4, IPv6, MQTT, CoAP, HTTP)
Architecture	Point à point (P2P)	Multiniveaux (objets → passerelles → cloud → application)
Portée	Locale (industries, bâtiments)	Globale (Smart Cities, domotique, industrie 4.0)
Exemples	Compteurs intelligents, distributeurs automatiques	Caméras IP, capteurs domotiques, véhicules connectés
Interconnexion Internet	Rare, souvent isolé d'Internet	Intégration complète au Cloud, accès à distance
Mise à jour et sécurité	Limitées, souvent manuelles	Automatisées et gérées à distance

MODÈLE DE RÉFÉRENCE IOT SELON CISCO

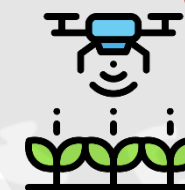
SMART HOME



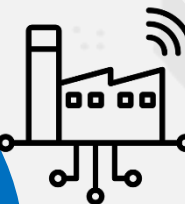
SMART HEALTHCARE



SMART AGRICULTURE



INDUSTRY 4.0



SMART CITY



WEARABLES

MODÈLE DE RÉFÉRENCE IOT SELON CISCO



Niveau 7

Collaboration et Processus (Intégration des utilisateurs et des processus métiers)
[Collaboration humaine et processus métiers centrés sur l'utilisateur]



Niveau 6

Application (Rapports, analyse et contrôle)
[Orientation principalement sur les applications logicielles et le contrôle des applications]



Niveau 5

Abstraction des données (Agrégation et accès aux données)
[Les données sont triées, agrégées et rendues plus accessibles et exploitables]



Niveau 4

Stockage des données collectées [Les données sont conservées localement ou sur le Cloud]



Niveau 3

Edge Computing (Analyse et transformation des éléments de données) [Traitement en temps réel, filtrage des données, réduction de la latence, et optimisation de la rapidité de réponse.]



Niveau 2

Connectivité (Communication et unités de traitement) [Bluetooth, Wi-Fi, Réseaux cellulaires, Passerelles (Gateways) et Routeurs]



Niveau 1

Dispositifs Physiques et Contrôleurs (L'objet physique dans l'IoT)
[Capteurs, machines, dispositifs, nœuds intelligents de différents types]

MODÈLES DE COMMUNICATION DANS L'IOT

Modèle	Portée	Latence	Protocole	Sécurité	Cas d'usage
Device-to-Device (D2D)	Local	Très faible	Zigbee, Bluetooth	Faible	Domotique, capteurs industriels
Device-to-Gateway (D2G)	Local → Cloud	Faible à moyenne	MQTT, CoAP	Moyenne	Bâtiments intelligents, IoT médicaux
Device-to-Cloud (D2C)	Global	Moyenne à élevée	MQTT, HTTP	Élevée	Vidéosurveillance, Smart City
Gateway-to-Cloud (G2C)	Local → Cloud	Moyenne	AMQP, MQTT, HTTP	Élevée	SCADA, systèmes industriels
Cloud-to-Cloud (C2C)	Global	Variable	REST API, GraphQL	Très élevée	Smart City, intégration cloud

MENACES MAJEURES DANS L'IOT ET ICS

VULNÉRABILITÉS LOGICIELLES

Les **IoT** et **ICS** reposent souvent sur des **firmwares** propriétaires et des logiciels embarqués qui ne sont pas toujours mis à jour régulièrement, laissant la porte ouverte à des vulnérabilités exploitables.

Exemples : Failles dans les protocoles de communication (Modbus, MQTT, Zigbee), logiciels obsolètes, absence de correctifs de sécurité.

Impact : Accès non autorisé, prise de contrôle à distance, vol de données, manipulation de systèmes critiques.

MANQUE DE SÉCURISATION DES COMMUNICATIONS

Les dispositifs IoT et ICS échangent des données en temps réel, souvent via des protocoles non sécurisés. L'absence de chiffrement et d'authentification forte expose les communications aux interceptions et manipulations.

Exemples : Attaques de type Man-in-the-Middle (MITM), écoute clandestine (eavesdropping), altération de messages.

Impact : Espionnage industriel, fuite d'informations sensibles, prise de contrôle à distance.

ATTAQUES DISTRIBUÉES PAR DÉNI DE SERVICE (DDOS)

Les objets connectés sont vulnérables aux attaques de type DDoS qui visent à saturer le réseau ou les ressources systèmes, rendant les services inaccessibles.

Exemple : L'attaque Mirai de 2016, exploitant des milliers de dispositifs IoT pour paralyser des services majeurs (Twitter, Netflix, Spotify).

Impact : Interruption de services critiques, pertes financières, dommages à la réputation.

PRISE DE CONTRÔLE À DISTANCE

Les dispositifs IoT exposés sur Internet sont une cible facile pour les cyberattaques.
L'exploitation de failles permet de prendre le contrôle à distance de l'équipement.

Exemples : Caméras IP piratées, serrures connectées manipulées, thermostats IoT reprogrammés.

Impact : Atteinte à la vie privée, sabotage, vol d'informations

ESCALADE DE PRIVILÈGES

Une fois un appareil compromis, un attaquant peut chercher à obtenir des droits supérieurs pour accéder à d'autres systèmes connectés.

Exemples : Exploitation des interfaces web mal sécurisées, contournement de droits d'administrateur.

Impact : Accès illimité aux données, manipulation des systèmes critiques, mouvements latéraux dans le réseau.

FAILLES DES INTERFACES WEB

Les interfaces de gestion web utilisées pour le contrôle à distance des dispositifs IoT sont souvent vulnérables aux attaques de type *Cross-Site Scripting (XSS)* ou *Injection SQL*.

Exemples : Interface de gestion d'une caméra IP accessible depuis Internet avec des failles SQL.

Impact : Exfiltration de données, modification des configurations, suppression de logs.

MAUVAISE GESTION DES IDENTIFIANTS

L'utilisation de mots de passe par défaut ou faibles est une faille critique dans les systèmes IoT et ICS.

Exemples : Routeurs avec le mot de passe "admin/admin", systèmes SCADA accessibles avec un mot de passe par défaut.

Impact : Accès non autorisé, manipulation des équipements, compromission totale du réseau.

Recommandations



Améliorer la sécurité :

Utiliser le cryptage, les mises à jour et les protocoles sécurisés pour prévenir les cyberattaques.

01

02

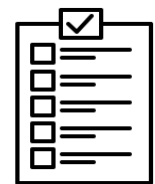
Protéger la vie privée :



Assurez la transparence des données, le consentement et suivez les réglementations telles que le GDPR.

03

04



Normaliser les dispositifs :

Rendre les appareils IoT compatibles pour améliorer l'efficacité et réduire les défaillances.

Être durable



Concevoir des appareils économes en énergie et recyclables afin de réduire les déchets électroniques.



PROCHAINE SESSION

OBJECTIF DU MENTORAT

❶ Technologies IoT :

1. L'anatomie d'un Objet Connecté.
2. La passerelle (Gateway).
3. Les protocoles de communication.
4. Le Cloud Computing.

❷ Cybersécurité de l'IoT :

1. Problèmes et Défis de sécurité liés à l'IoT.
2. Éléments de la sécurité IoT
3. Tomographie IoT
4. Défis de la sécurité IoT
5. Modèle d'attaque par couche
6. Architecture de sécurité IoT
7. Tendances émergentes en sécurité IoT

❸ Les applications de l'IoT:

1. Arduino et Raspberry Pi dans l'IoT
3. Maison intelligente (Smart Home)
4. Ville intelligente (Smart City)
5. Applications militaires
6. Santé (Health Care)
8. Agriculture
9. Industrie

❹ Pratiques sur Raspberry Pi :

1. Créer une sonde réseau à partir d'un Raspberry Pi
2. Collecter l'ensemble des échanges au sein d'un réseau local
2. Transmettre ces informations dans le cloud d'une manière sécurisée.

Q & R

