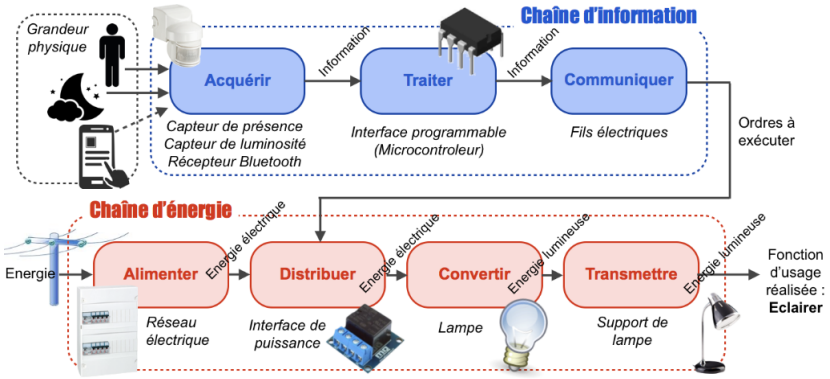
Un **système informatique embarqué** est un système de traitement de l'information autonome ne possédant pas d'entrée et sortie standard comme le clavier et l'écran. Les informations sont reçues de l'extérieur par le biais de capteurs, elles sont traitées par un processeur et selon le programme du système, des actions physiques peuvent être déclenchées avec des actionneurs.



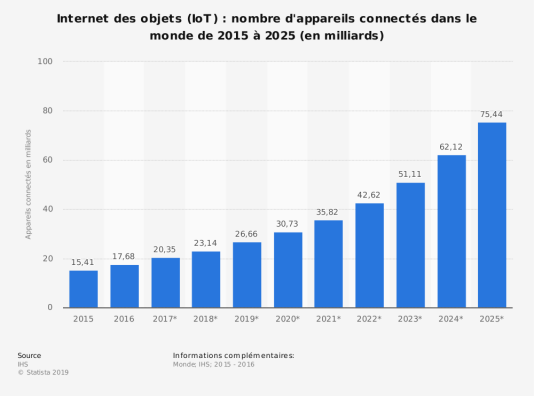
Les signaux capturés sont analogiques analogues au phénomène : par exemple la rotation de l'axe d'un anémomètre qui mesure la vitesse du vent sur une station météo. Pour être traités par le processeur, ils sont numérisés, c'est-à-dire transformés en un nombre fini d'informations codées par des zéro et des uns par échantillonnage (nombre fini de relever) et quantification (nombre fini de valeurs possibles). Les ordinateurs miniatures des systèmes embarqués s'appellent des microcontrôleurs : ils ont un mémoire, un processeur, des entrées-sorties comme un ordinateur, mais se caractérisent par une miniaturisation accrue, une plus faible consommation électrique et des performances moindres, mais suffisantes pour des applications toujours plus nombreuses avec les progrès techniques.

Visionnez les deux petites vidéos suivantes :

- https://youtu.be/DOECi_ZKaYI
- https://youtu.be/H9iKiqeivg0

Une **Interface Homme Machine** est un ensemble de moyens physiques (boutons, manettes) ou logiciels (interface graphique) qui permettent à un humain d'échanger des informations avec une machine. Douglas Engelbart est un des pionniers des IHM en informatique avec son système NLS qui introduit la première souris.

Les objets connectés permettent d'ajouter de l'intelligence dans notre environnement à tous les niveaux : le corps (mes indicateurs de santé, ma nourriture), la maison (appareils, système de chauffage), les réseaux (électrique, de circulation), les transports (véhicules autonomes), la prévention des risques (incendies). . . De plus, la collaboration entre objets connectés, leur connexion à des bases de données en ligne, augmente considérablement leur puissance, même si chaque objet a des ressources matérielles limitées.



Néanmoins, les vulnérabilités des systèmes embarqués sont amplifiées s'ils sont connectés. La cyberattaque d'un serveur DNS majeur par des milliers de caméras de surveillance, transformées en bots, a gravement perturbé Internet en octobre 2016. La prise de contrôle à distance par des hackers de la Jeep Cherokee en 2015 ou des failles détectées dans des pacemakers sont des exemples parmi bien d'autres illustrant le fait que la révolution de l'internet des objets ne pourra se faire sans des progrès sur le plan de leur sécurité. Enfin, la moisson de données personnelles que peuvent collecter des objets connectés comme les assistants personnels proposés par les Gafa doit absolument être contrôlée.

Faire le test suivant : https://frederic-junier.org/wp/?page_id=1435