Les activités, quizz et la frise chronologique du chapitre sont disponibles sur frederic-junier.org.

1 Systèmes embarqués

1.1 Architecture

Définition 1

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 traités par un **processeur** et selon le programme du système des actions physiques peuvent être déclenchées avec des **actionneurs**.

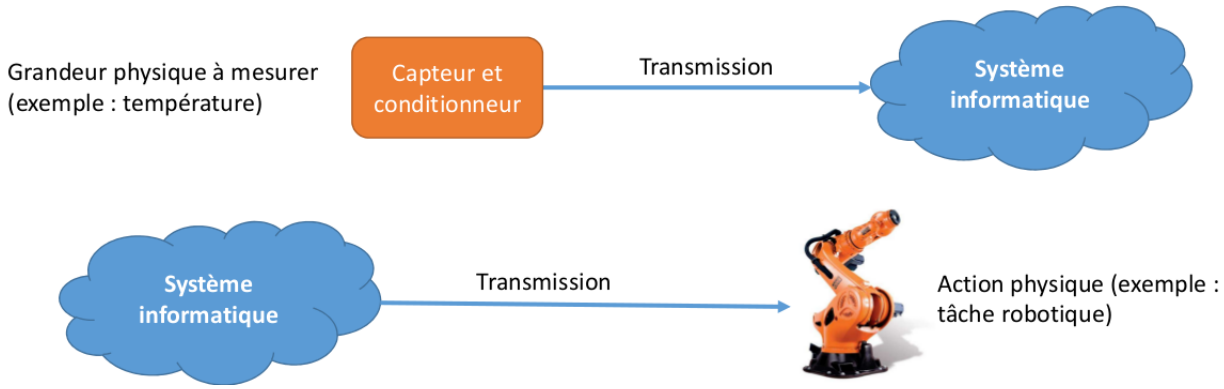
Les signaux capturés sont **analogiques** analogues au phénomène : par exemple la rotation de l'axe d'un anémomètre qui mesure la vitesse du vent sur une station météo. Pour être traités par le processeur, ils sont numérisés c'est-à-dire transformés en un nombre fini d'informations codées par des 0 et des 1 par **échantillonnage** (nombre fini de relevés) 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.

Les systèmes informatiques embarqués sont utilisés dans tous les domaines : l'industrie (robots), le transport (avionique, automobile, métro ...), la médecine (pacemakers, imagerie ...), la maison (domotique, appareils ménagers ...), les télécommunications (téléphonie ...), le monde du travail (contrôle d'accès ...), les loisirs (vélo électrique ...).

On parle d'**informatique ubiquitaire** pour désigner cette omniprésence de l'informatique dans notre environnement.

1.2 Programmation



Source : Yassine Haddab Université de Montpellier

Méthode

Un algorithme de contrôle fréquent sur un système informatique embarqué consiste en une boucle infinie où s'enchaînent capture d'événements par les émetteurs, traitement puis action par les actionneurs.

```
Initialiser les actionneurs à leur position de départ
Tant que Vrai
    Lire les informations des capteurs
    Traiter ces informations
    Calculer des informations sur les actionneurs
    Transmettre ces informations aux actionneurs
```

1.3 Interface Homme Machine

Définition 2

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.

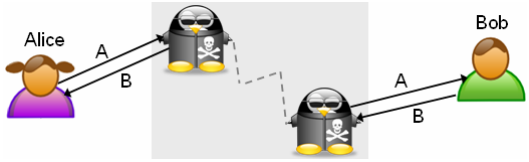
1.4 Fiabilité et sécurité

- La **sûreté** est la garantie qu'un système fait ce qu'il doit faire et ne fait pas ce qu'il ne doit pas faire. Les programmes des systèmes embarqués doivent parfois s'exécuter avec des contraintes fortes (manque de ressource, temps de réaction très rapide) et ils ne sont pas toujours développés avec la rigueur nécessaire. Les bugs sont donc fréquents. Parfois bénins (une mauvaise gestion des années bissextiles a provoqué l'arrêt du lecteur MP3 Zune de Microsoft le 31/12/2008, ils peuvent avoir a des conséquences dramatiques : les bugs du Therac 25 (appareil de radiographie) ou du contrôle moteur sur les Toyota Camry ont provoqué plusieurs morts.

- La **confidentialité** est une problématique majeure des systèmes embarqués qui collectent des données personnelles sur leurs utilisateurs, comme par exemple les cartes électroniques de transport comme le pass Navigoo ou la carte Técély.

- La **sécurité** est souvent un point faible des systèmes embarqués, qui manquent de ressources matérielles, ont des cycles de vie long sans mise à jour et mettent en jeu des modes de communication sans contact particulièrement vulnérables.

  Par exemple, une voiture ne peut démarrer que si la carte de démarrage se trouve à proximité car la carte et la voiture partagent un secret commun permettant de déverrouiller le système antidémarrage. L'attaque par relais permet de déjouer ce protocole en relayant la communication : un pirate se trouve près de la voiture et l'autre près de la carte et par un leurre technologique ils font croire aux deux parties qu'elles sont à proximité. Tous les systèmes embarqués qui communiquent sans contact (carte bancaire, carte d'accès ...) sont vulnérables à cette attaque.



Source : Image : Martial Régereau [CC BY-SA 3.0], via Wikimedia Commons

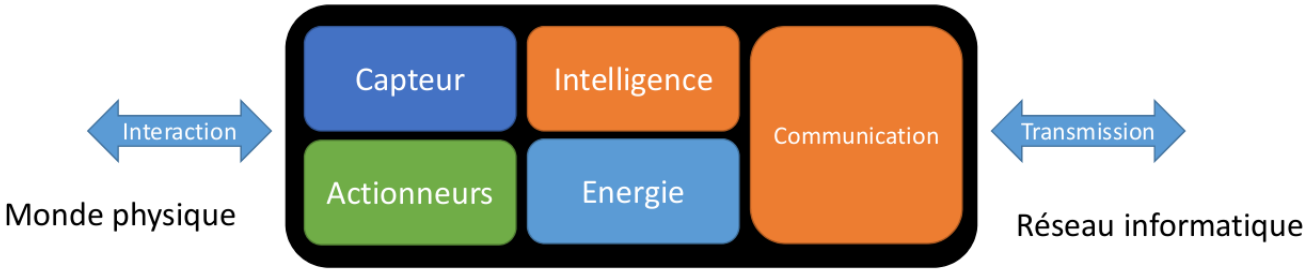
2 Objets connectés

2.1 Internet des objets

Définition 3

Un **objet connecté** est un système informatique embarqué disposant d'une connexion à un réseau local ou à L'Internet.

Les Interfaces Homme Machine des objets connectés sont souvent des applications Web disponibles sur Smartphone.



Source : Yassine Haddab Université de Montpellier

Avec la baisse des coûts des microcontrôleurs et des puces Wifi, les objets connectés se multiplient. On peut en fabriquer facilement à partir de cartes Arduino, de Raspberry Pi ou de cartes Wifi ESP8266. Actuellement, il existe plus d'objets que d'humains connectés à Internet et leur nombre va augmenter fortement dans les prochaines années avec la baisse de coût des . On parle d'`IOT` pour Internet Of Things pour désigner l'ensemble des objets connectés à l'Internet.

On estime à 50 milliards le nombre d'objets connectés en 2020.

2.2 Fiabilité et sécurité

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.