Où va l'informatique ?

Gérard Berry

Professeur au Collège de France
Chaire Algorithmes, machines et langages
Académie des sciences, Académie des technologies

http://www.college-de-france.fr/site/gerard-berry

Cours n° 2 en 2 actes, 23/01/2019

COLLÈGE DE FRANCE
1530

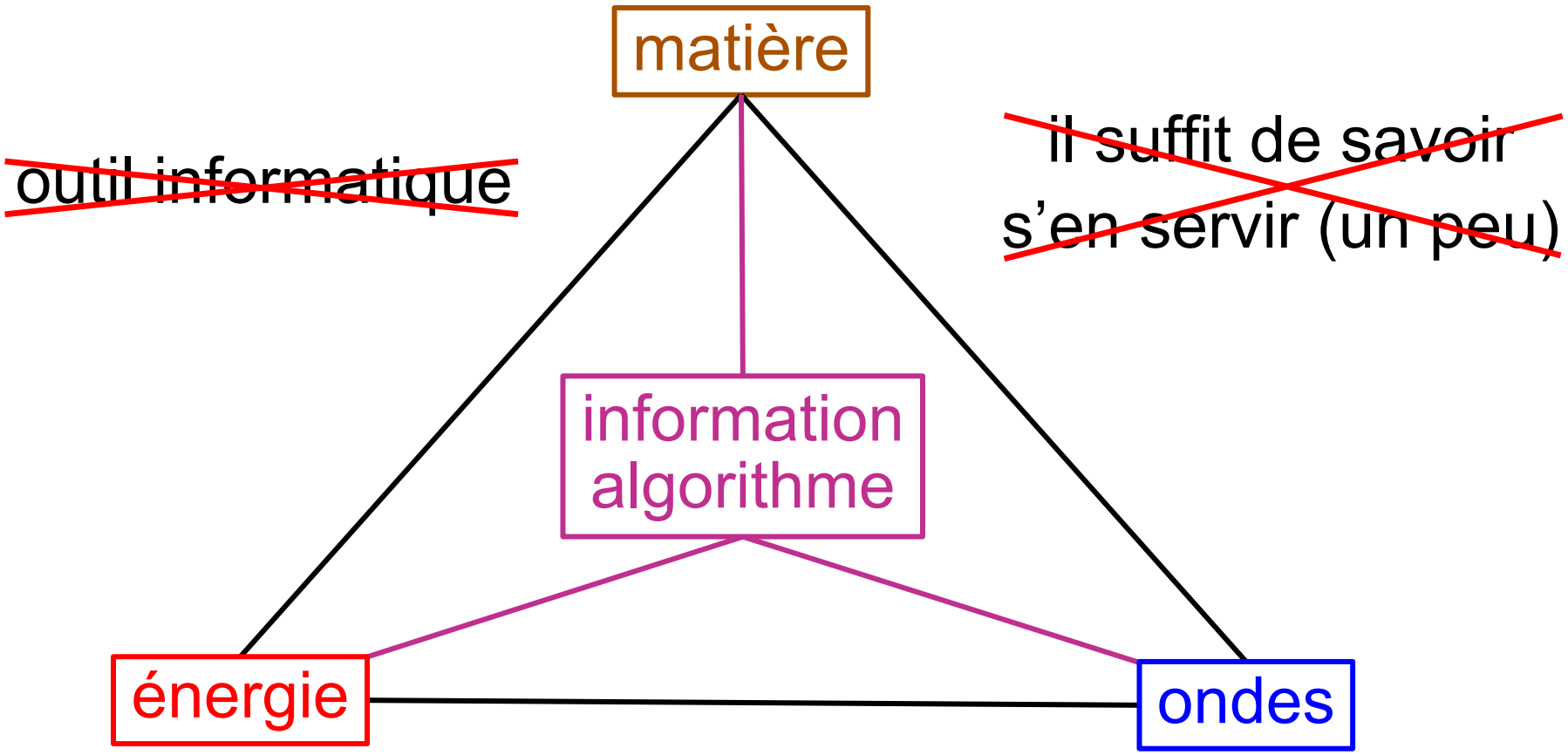
Acte 1 : de 2007 à 2019, quelles évolutions ?

1. L'hyperpuissance de l'informatique
2. L'infrastructure matérielle
3. L'infrastructure logicielle
4. Les applications
5. Le recentrage sur les données
6. Vers l'Internet des objets

Acte 1 : de 2007 à 2019 quelle évolution?

1. L'hyperpuissance de l'informatique
2. L'infrastructure matérielle
3. L'infrastructure logicielle
4. Les applications
5. Le recentrage sur les données
6. Vers l'Internet des objets

Sciences et techniques, du 20e au 21e siècle



L'informatique et ses algorithmes conduisent à une nouvelle façon de penser et de faire qui change le monde

Puissance et universalité de l'informatique

- L'information est la même partout
  - une seule notion d'information en médias, télécoms, physique biologie, neurologie, histoire, etc.
  - une seule notion d'algorithme pour tous les domaines
  - une machine universelle, unique dans l'histoire
- Le levier de l'information est hyper-efficace
  - textes, musiques, hôtels, voitures → information
  - posséder l'information > posséder l'hôtel ou la voiture
- Mais une difficulté mentale majeure
  - le raisonnement et l'action sur l'information sont très différents de ceux sur la matière ou l'énergie

Comprendre l'essence de l'informatique
est essentiel pour la plupart des activités de demain

Les inversions mentales de l'informatique

L'informatique est tellement puissante qu'elle provoque de véritables inversions mentales entre façons de faire et générations

Exemples d'inversions mentales

- Le téléphone portable

  Avant : zut, elle n'est pas chez elle…

  Maintenant : t'es où ?

  Papy, pourquoi t'as mis un antivol ?

- Maman, tu m'as dit que quand tu étais petite, tu n'avais pas d'ordinateur. Alors, comment faisais-tu pour aller sur Internet ?

- Papa, le voisin a un ordinateur incroyable ! Tu appuies sur les touches, et il imprime tout de suite !

Pour les enfants, l'ordinateur, le smartphone et Internet sont des parties de la nature, comme la mer, la montagne, le vélo ou le chat

Inversions mentales, pour adultes aussi

- La photographie :

  20e siècle : apporter la pellicule au labo
  le lendemain, envoyer les tirages dans une lettre

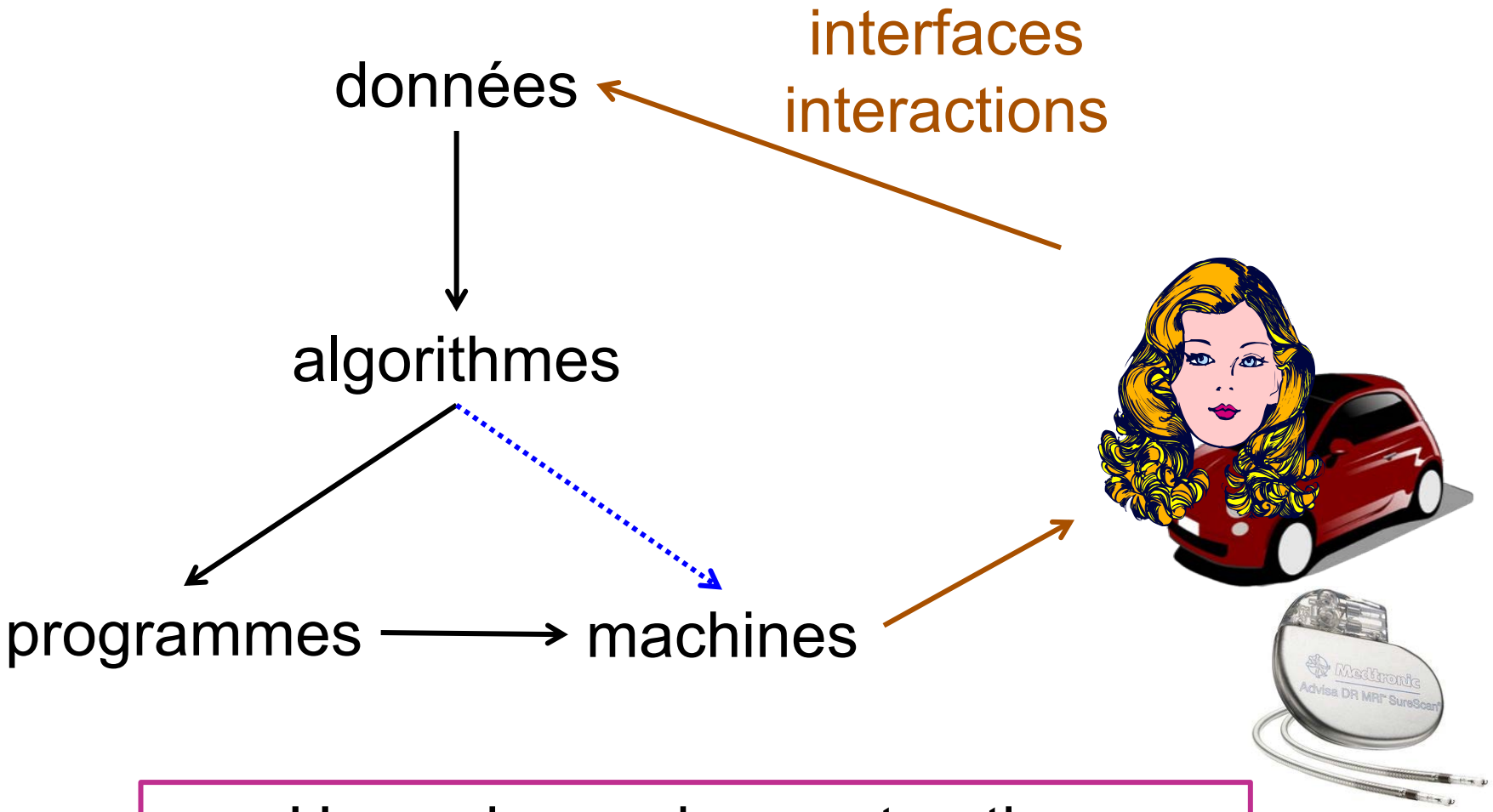
  21e siècle : aussitôt pris, aussitôt parti, aussitôt arrivé !

- S'orienter sur une carte :

  20e siècle : on achète la carte du lieu (à quelle échelle?)
  on cherche où on est, on cherche la destination

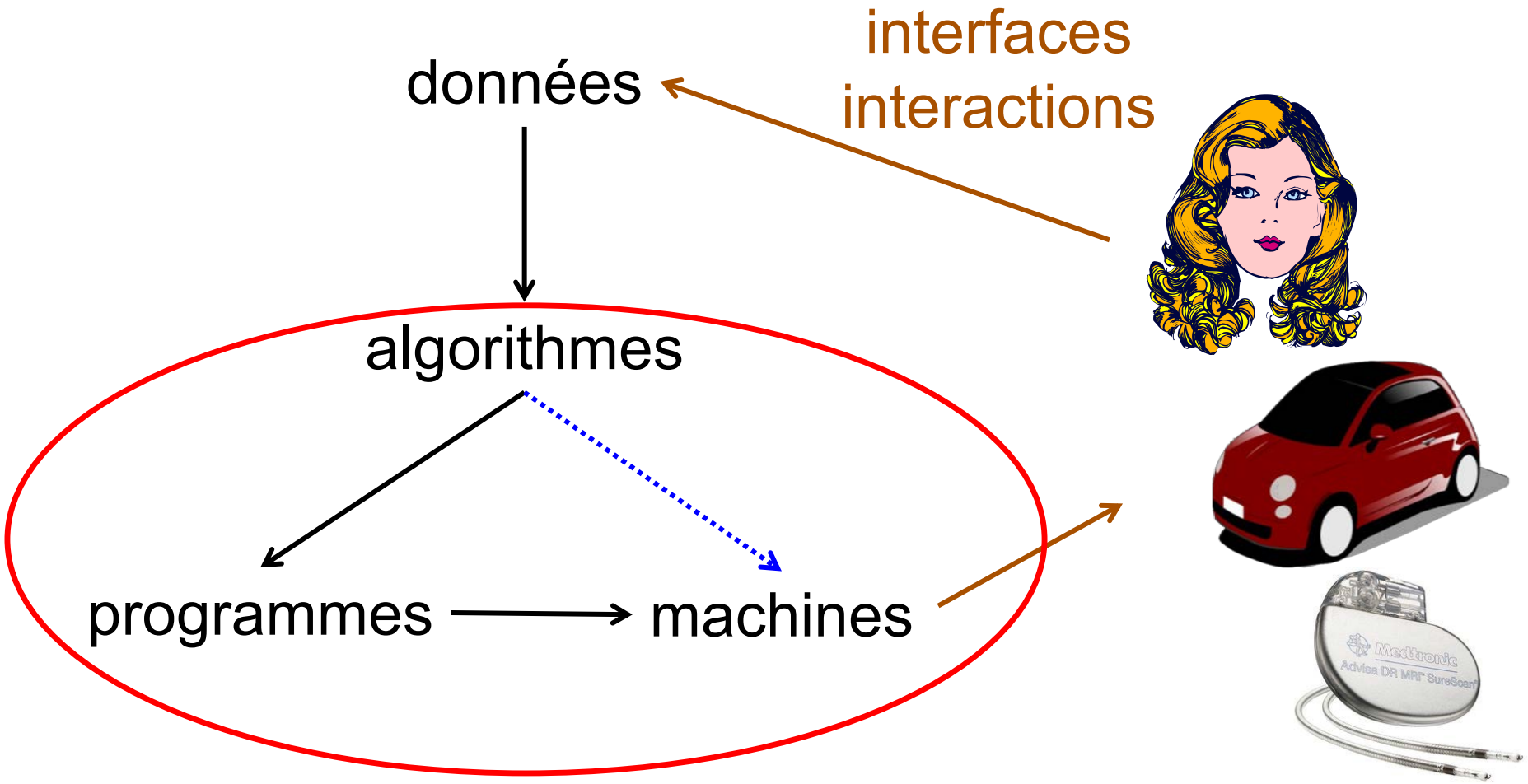
  21e siècle : on appelle la carte du monde (à toutes les échelles)
  elle nous dit où on est, on tape le nom de la destination, elle nous donne l'itinéraire

Les piliers de l'informatique



Une science de construction,
très différente des sciences naturelles

Les piliers de l'informatique – version 2007



Centrage sur le calcul + bases de données

Evolutions scientifiques (lentes par nature)

- Données : deviennent massives et partielles, voir plus loin
- Algorithmes :
  - deviennent probabilistes, cf. Claire Mathieu (2017-2018)
  - deviennent répartis, cf. Rachid Guerraoui (2018-2019)
- Langages de programmation
  - deux camps bien distincts, cf. cours des 04/11/2015 et 13/12/2018

langages typés
puissance d'expression
Caml, F#, Scala, …
grande rigueur
détection statique de bugs
investissement intellectuel

langages dynamiques
souplesse
Python, JavaScript, …
rigueur approximative
bugs au dernier moment
yaka s'y mettre !

- Machines : vers de nouvelles technologies et architectures ?

Une valeur ajoutée majeure

En couplant informatique et physique, on peut faire des choses inaccessibles à la physique seule

La photo numérique

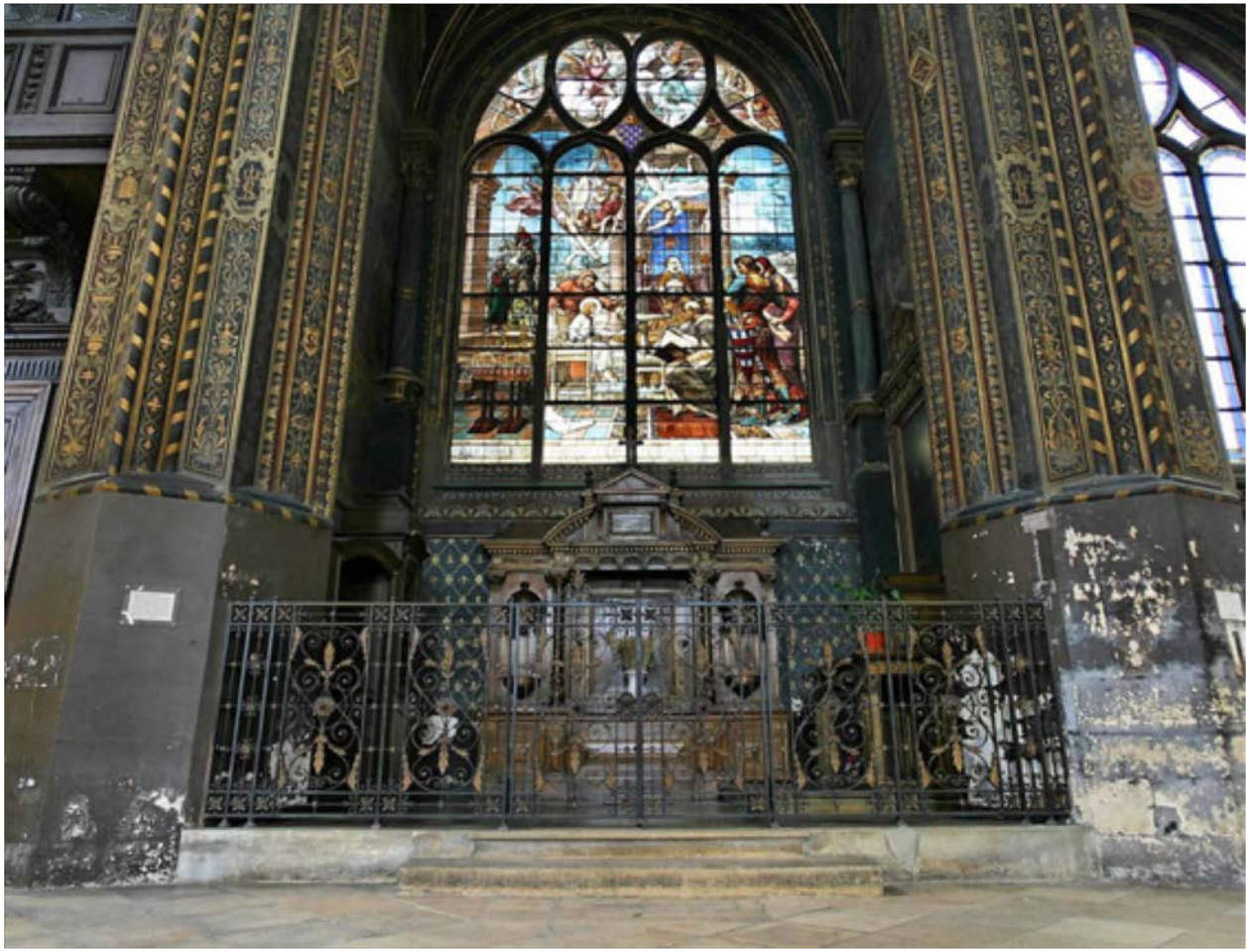
cf. séminaire 2008 de F. Guichard et cours du 31/01/2018

Photo argentique: clic, c'est fini → tirage

Photo numérique : clic ça commence → algorithmes !

La photo numérique

cf. séminaire 2008 de F. Guichard et cours du 31/01/2018



Inversion algorithmique des distorsions

Transformation algorithmique de la lumière : ~~Physique~~ ?

Et pour un clic de plus

Faisable avec la physique, mais pas simple

2019 : fusion d'images multiples

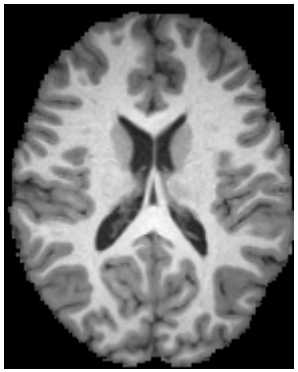
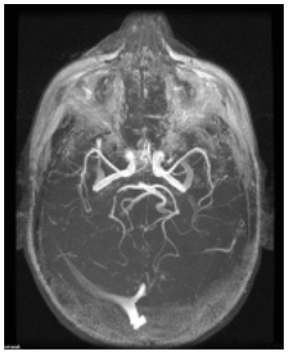
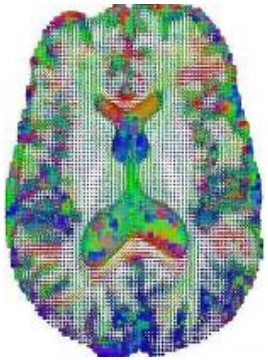
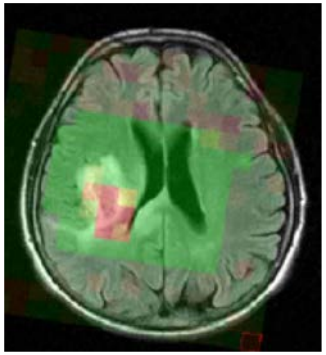
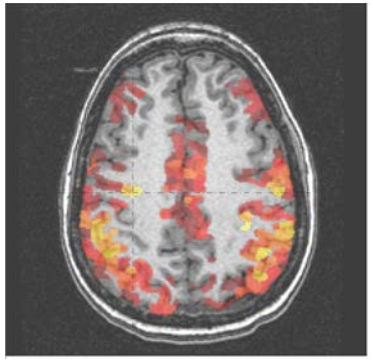
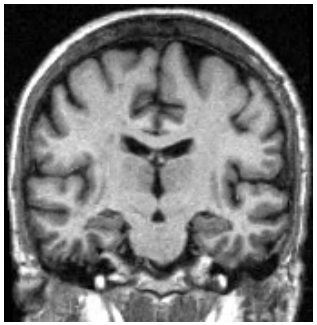
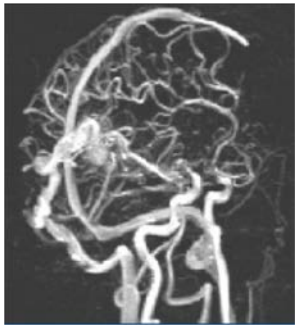
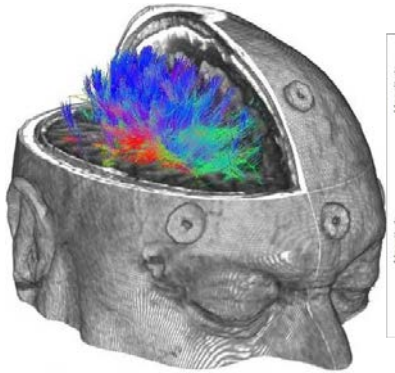
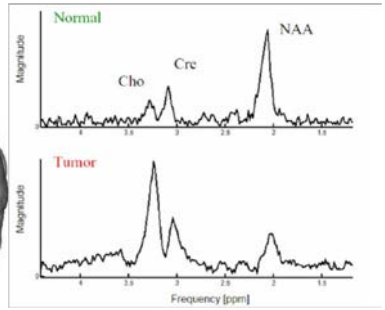
6 images sucessives
à mises au point décalées

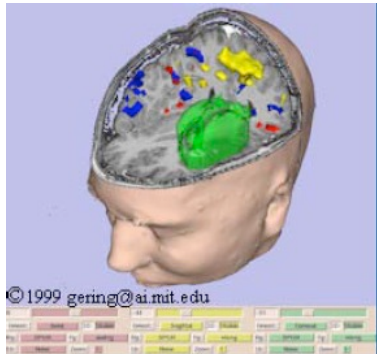
image finale

Infaisable par les seuls procédés physiques !

Fusion d'images multiples en médecine

anatomy angio diffusion spectro functional



Le Bihan, Le cerveau de cristal, 2013

Infaisable par les seuls procédés physiques !

L'informatisation des sciences

(voir cours du 28 janvier 2015)

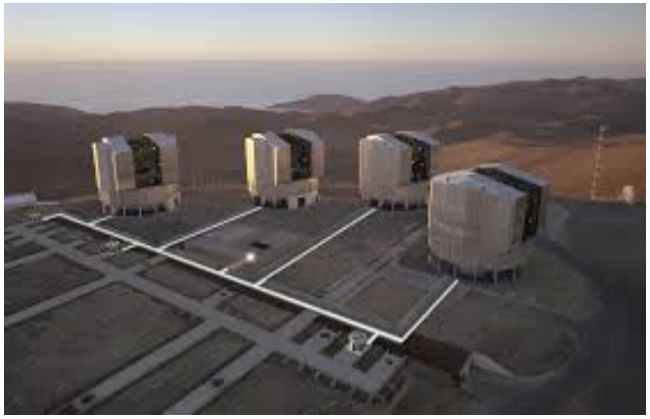
Modern high field clinical MRI scanner.

(3T Achieva, the product of Philips
at Best, the Netherlands.)

Séquenceur d'ADN

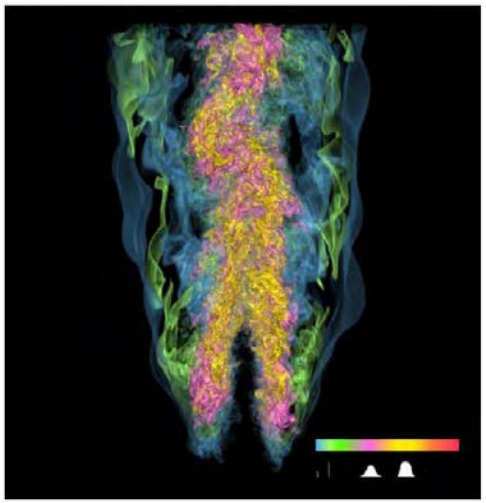
Par Flickr user jurvetson — Flickr, CC BY 2.0,
https://commons.wikimedia.org/w/index.php?curid=1552252

Curiosity (Mars)

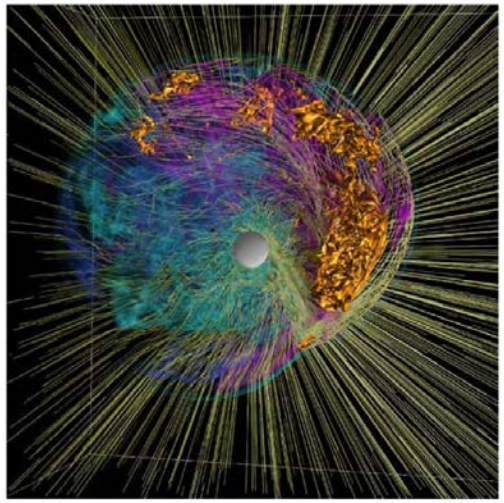


VLT (Chili)

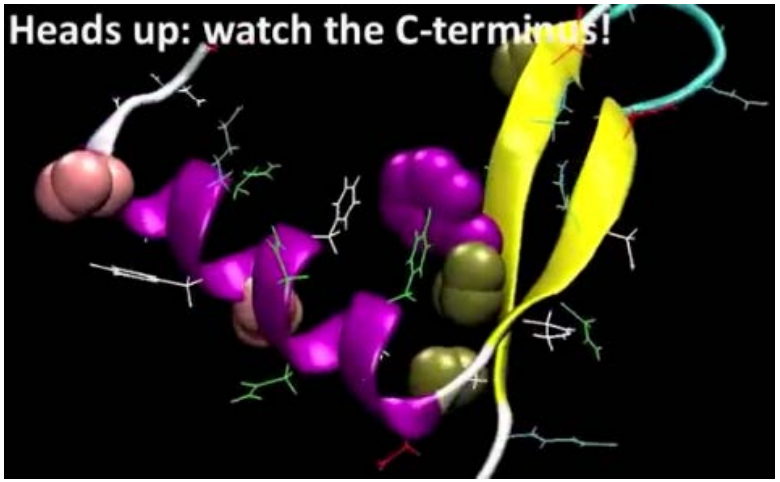
Modélisation et simulation numérique



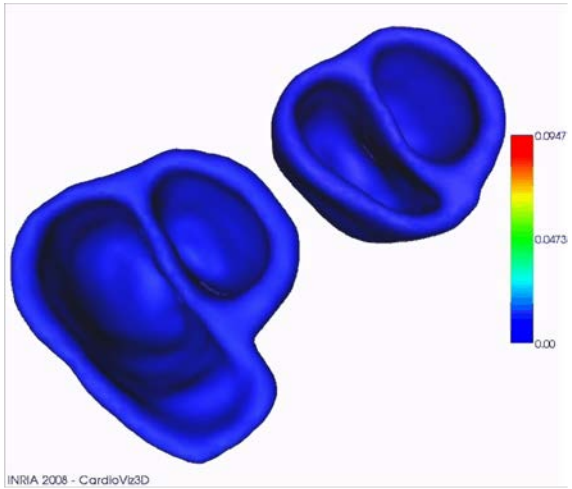
Ariane 5



Supernova

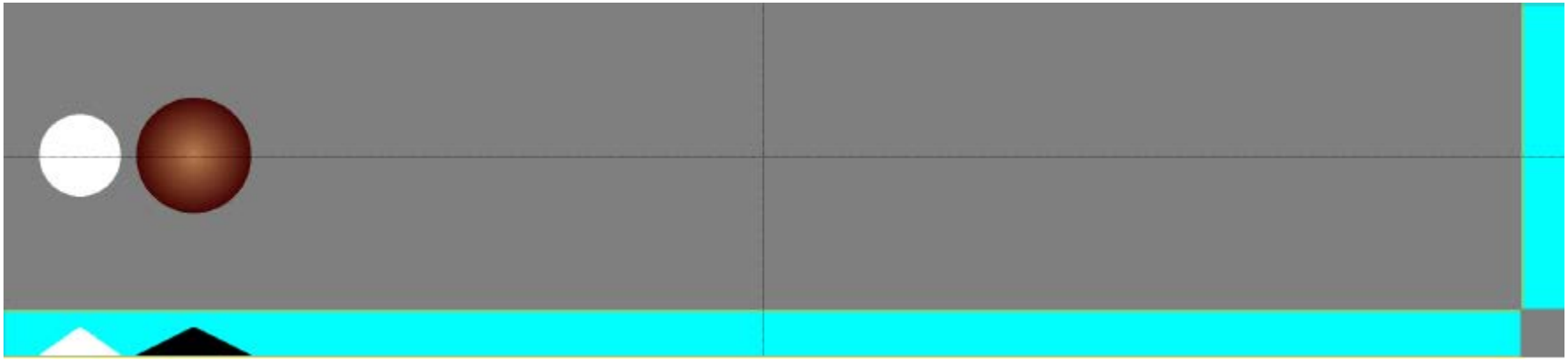


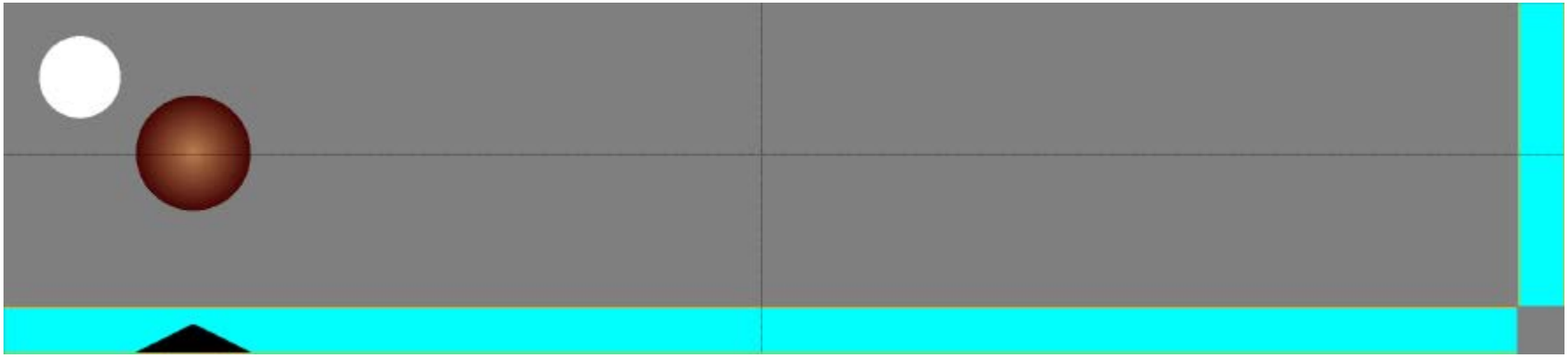
repliement de protéine



Préparation d'opération

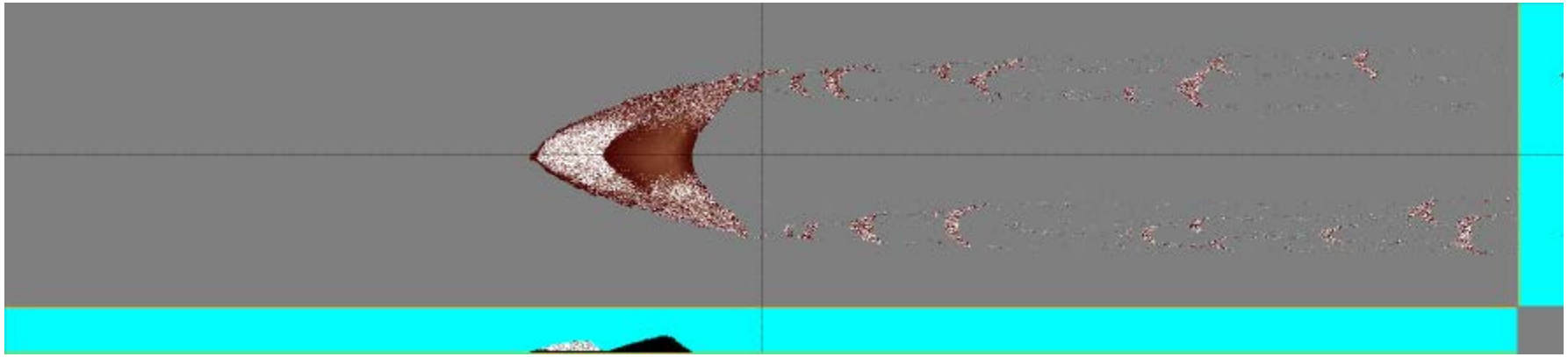
Simulation des dunes de sable

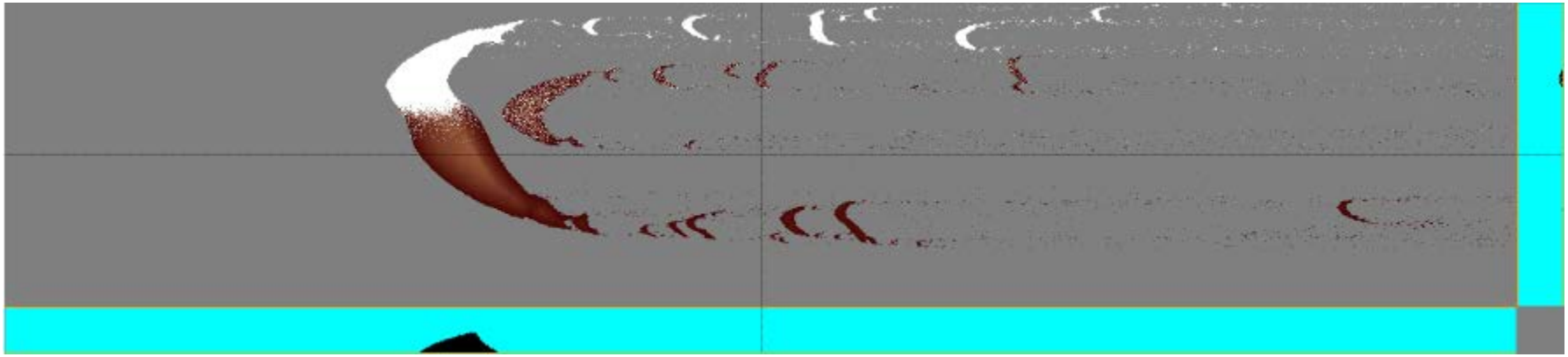




Voir Clément Narteau, « Structures éoliennes au sein des mers de sable »
Colloque « Sciences et arts, de nouveaux domaines pour l'informatique »
27 mai 2016

Simulation des dunes de sable





Voir Clément Narteau, « Structures éoliennes au sein des mers de sable »
Colloque « Sciences et arts, de nouveaux domaines pour l'informatique »
27 mai 2016

Qu'est ce que la simulation, au fond ?

- Remplacer matière et énergie par la seule information
- Remplacer les lois de la nature par leur équivalent algorithmique programmé sur ordinateur
- Remplacer le temps physique par le temps de calcul
  - ▹ simulation rapide de phénomènes lents
  - ▹ simulation lente de phénomènes rapides
  - ▹ simulation en temps réel

Il faut bien sûr de la matière et de l'énergie,
mais celles de l'informatique sont universelles
et sans rapport avec celles du phénomène simulé !

Limite : on ne trouve pas de pétrole en forant la carte !

Acte 1 : de 2007 à 2019 quelle évolution?

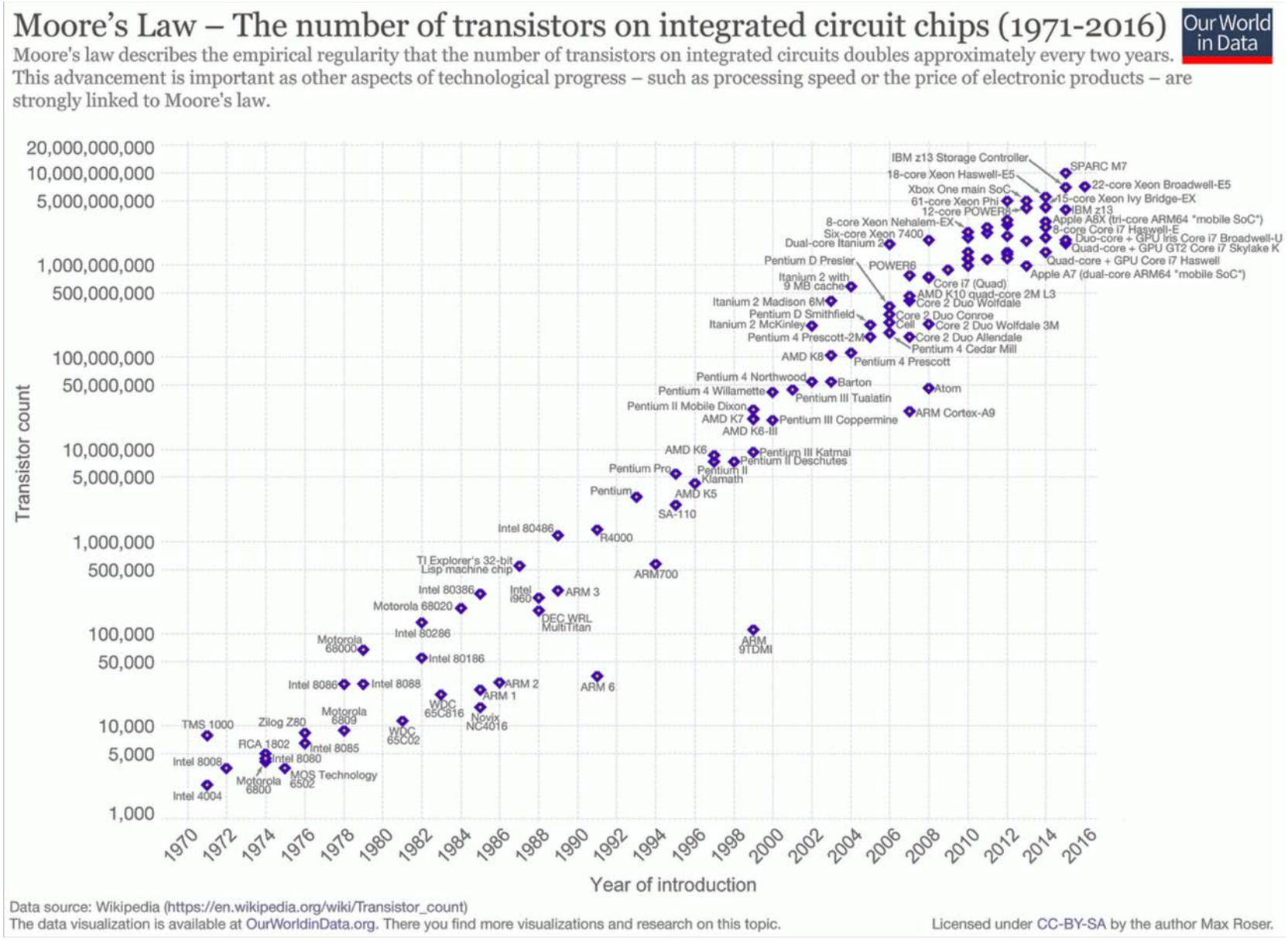
1. L'hyperpuissance de l'informatique ?
2. L'infrastructure matérielle
3. L'infrastructure logicielle
4. Les applications
5. Vers l'Internet des objets
6. Le recentrage sur les données

La « Loi » de Gordon Moore

~~La puissance des ordinateurs va doubler tous les 18 mois~~

Décision industrielle concertée :
Le nombre de composants électroniques par unité de surface double tous les 2 ans

La loi de Moore



source Wikipedia

L'arrêt de la loi de Moore, annoncé en permanence

Loi complémentaire : Le nombre de commentateurs « bien informés » prédisant la fin proche de la loi de Moore par atteinte des « limites de la physique » double tous les 2 ans

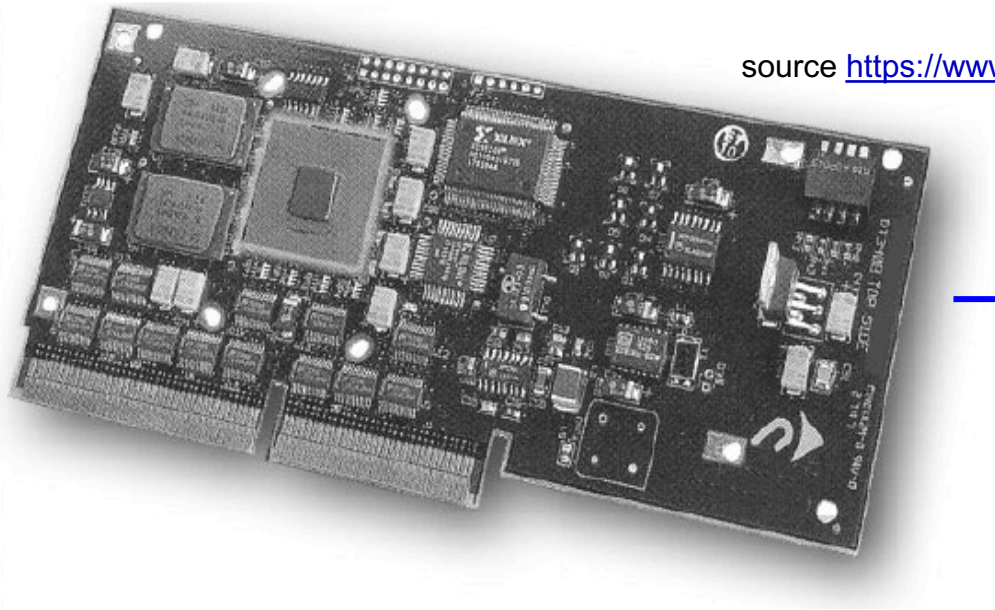
C'est sûr, « ils » toucheront la limite à
50 → 20 → 15 → 10 nm

Actuellement : 7-10 nm

en construction : 5-3 nm

Mais les gros problème arrivent maintenant…

Circuits → systèmes sur puce (SoCs)



source https://www.powershow.com/users/esElfakN6

- Construction par assemblage d'IPs (*Intellectual Properties*)
  - CPUs, GPU, vidéos, USB, radio, contrôle mémoire, etc.
- Avantages : taille, consommation,vitesse de développement, fabrication, prix, etc.

La grande variété des machines universelles

CERN, Par Hugovanmeijeren
Travail personnel, CC BY-SA 3.0,
https://commons.wikimedia.org/w/index.php?curid=10282772

fermes de données / calcul (20 MW)

https://commons.wikimedia.org/wiki/User:Raysonho
CC BY 3.0

Idem en conteneurs

L'incroyable essor du smartphone

source Wikipedia, Francis Flinch

moyen partout

excellent partout !

Philipe Geluk, *Le chat pète le feu*, Casterman, 2018

Le circuit fait les calculs, le logiciel décide quoi faire

L'incroyable essor du smartphone

source Wikipedia, Francis Flinch

moyen partout

excellent partout !

Philipe Geluk, *Le chat pète le feu*, Casterman, 2018

A utiliser avec modération, parents et enfants !

L'avancée continue toujours

- Apple / TSMC, iPhone A12 Z : 7 nm, 9 milliards de transistors (aussi Samsung, Huawei…)
- 2019 : 5 nm en production (Samsung)
- 2022 : 3 nm en chantier (TSMC)
- Plusieurs équipes ont construit des transistors à 1 atome (0,35 nm) !

Le problème majeur est la diminution de la consommation d'énergie…

La loi de Moore ralentit…

- Le mur de la chaleur : la fréquence n'aumente plus
  calcul + fuites électriques ⟹ chaleur excessive
- La difficulté croissante de la CAO électronique
- Le coût démesuré des nouvelles usines
  - Prévision : TSMC 3nm, 2022 → $ 20 Md
    Chine 3nm → $ 30 Md
- Réduction associée du nombre de fournisseurs
  - ST Microelectronics : ~~25 nm~~
  - Août 2018 : Global Foundries (ex. AMD) : ~~7nm~~

Quid de l'Europe ?
Un problème stratégique majeur…

- Leader des machines de fabrication : ASML (Hollande)
- Un des leaders du design : ARM (Angleterre)
- Presque plus de fabs, restées à 28nm : ST Micro
- Nouveau projet européen de calculateur Exascale (10^{18}) (ATOS + 23 participants)

ARM ? Ou RISC-V (*open source*) ? Ou nouveau ?

De toutes façons, même en maîtrisant son design l'Europe ne saura pas le fabriquer….
Mais ST Micro est très bon en SoCs applicatifs

Enfin de la place pour d'autres approches !

3D

spintronique, memristors, graphène,…

quantique ? machines neuromorphes ?

→ nouvelle recherche excitante

Le reste de l'équipement avance aussi vite !

- Le stockage
  - mémoires RAM : 32 KO → 512 MO → 16 GO
  - disques : 10 MO (1985) → 10 TO, x 1000 000 !
  - mémoires flash : 4 GO → 256 GO → 2 TO
- Les écrans
  - petits cathodiques → moyens LED → grands OLED
- Les imprimantes
  - jets d'encre (devenues excellentes en photo)
  - laser
- Les réseaux locaux
  - Ethernet : 10 Mb → 100 Mb → 1GB
  - Wifi, Bluetooth, etc.

Et les grands réseaux aussi !

- Le cuivre
  - ADSL : pas mal pour les villes
  - VDSL : super pour ceux qui sont près du central
- La fibre
  - en voie de généralisation, surtout dans les villes
- Sans fil :
  - 2G → 3G → 4G → 5G
  - mais couverture encore insuffisante hors des villes (plans d'amélioration en cours)

Belles affirmations, mais fausses ? (Quand les commentateurs se lâchent)

Grâce à Internet, l'accès aux réseaux et l'informatique distribuée sont devenus ubiquitaires

On sait que c'est faux dès qu'on habite à la campagne !

- téléphone en bout de ligne, ADSL 512 K, lignes non maintenues
- portable ne passant pas, ou trop cher pour Internet
- fibres optiques vite saturées par la TV sur Internet (en ville aussi)
- plans numériques répétés, mais peu d'effet (ARCEP → espoir)

Il faudra un investissement énorme et pas seulement urbain pour que ça devienne plus ou moins vrai

Le tout-fibre (FTTH) est-il vraiment la meilleure idée ?

Belles affirmations, mais fausses ? (quand les médias se lâchent)

L'ordinateur quantique sera
infiniment plus rapide que l'ordinateur classique,
et calculera beaucoup plus de choses

1. Pour les calculs classiques, au mieux exponentiellement meilleur (excellent), ou $\sqrt{n}$ meilleur (pas si mal)
2. Il calcule les même fonctions plus l'aléatoire, aussi greffable à l'ordinateur classique (générateurs quantiques)
3. Les problèmes technologiques restent considérables

Ceci ne vaut pas pour la simulation quantique
de phénomènes quantiques

Acte 1 : de 2007 à 2019 quelle évolution?

1. L'hyperpuissance de l'informatique ?
2. L'infrastructure matérielle
3. L'infrastructure logicielle
4. Les applications
5. Vers l'Internet des objets
6. Le recentrage sur les données

L'infrastructure logicielle

- Systèmes d'exploitation

très gros, complexes, pb. sécurité, mises à jour fréquentes, …

- Navigateurs

…

gros, complexes, pb. sécurité, mises à jour fréquentes, …
cachés dans les apps de téléphones

- Langages de programmation, bibliothèques, outils systèmes, outils pour le web, …
- Une notion clef : l'API (*Application Programming Interface*)

Internet et la connectivité

- Internet : 4,12 Md utilisateurs (54%, Europe 80%)
- Réseaux sociaux : 3,36 Md (44%, français 58%)
- Portables : plus d'abonnements que de personnes !
  - 2007 : 3,3 Mds, 2017 : 7,7 Mds (103,5%). Pays evd 98,7%, dév. 127,3%. France 93% dont 71% de smartphones
- Connexions interopérables : ADSL, fibre, 3G/4G, WiMax, etc.

Quelle différence entre Internet et un réseau téléphonique ?
la gestion de la communication est faite par les utilisateurs,
et le système est auto-adaptatif aux changements !

Calcul dans le nuage (Cloud Computing)

Puissance de calcul / stockage énorme mais fixe
+ portables mobiles mais limités par la batterie
+ réseaux efficaces
+ algorithmes distribués (cf. cours R. Guerraoui)
= décentraliser les calculs et stockages coûteux
partager le calcul entre le local et le distant

- Grandes bases de données
- Calcul scientifique, analyse de données
- Moteurs de recherche, réseaux sociaux
- Reconnaissance de la parole, traduction automatique
- Streaming audio / vidéo
- …

Acte 1 : de 2007 à 2019 quelle évolution?

1. L'hyperpuissance de l'informatique ?
2. L'infrastructure matérielle
3. L'infrastructure logicielle
4. Les applications
5. Vers l'Internet des objets
6. Le recentrage sur les données

Logiciels → Applications

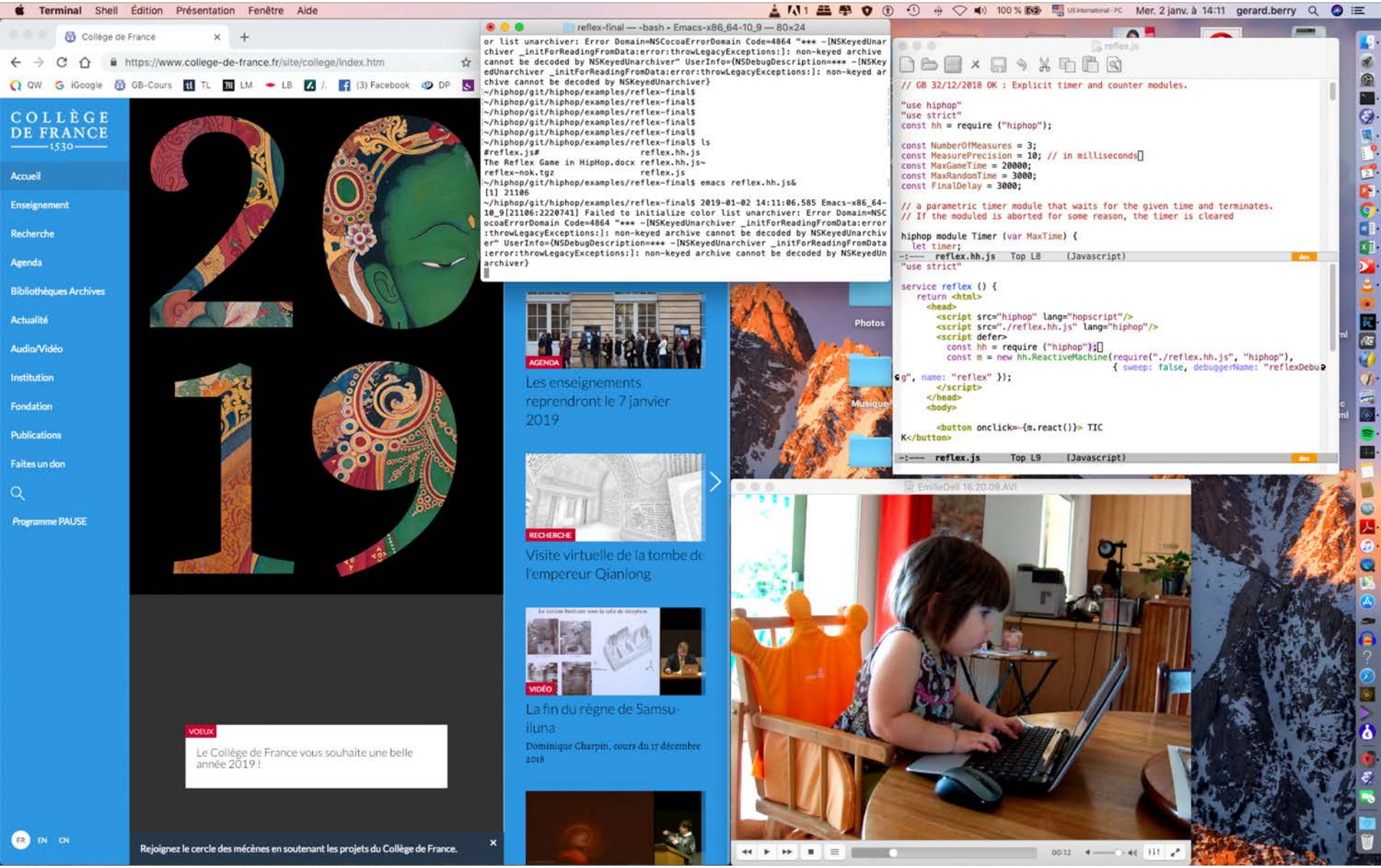
- Programmeur → Développeur

  ~~Programmateur~~
- Très grande variété, mais beaucoup de redondance
- Mises à jour systématiques, fonctionnalités et sécurité

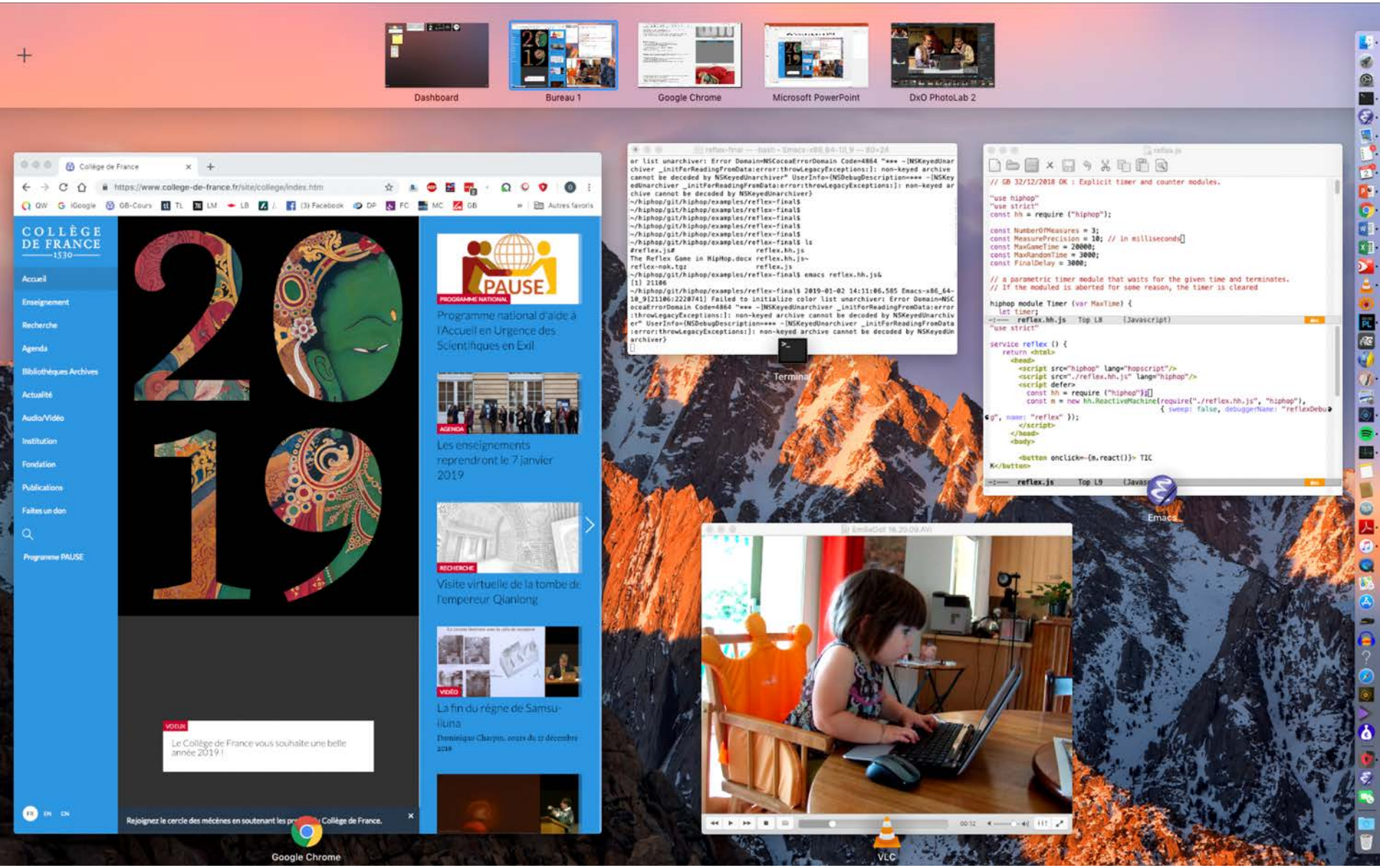
  « amélioration de l'expérience utilisateur et correction de bugs »

  ⇔ c'est pas encore ça…
- Profond changement de style et d'IHM
  - 2007 : ordinateur, multifenêtrage, applications génériques
  - 2019 : smartphone / tablette, mono(bi-)-fenêtrage, toucher
    applications très spécialisées

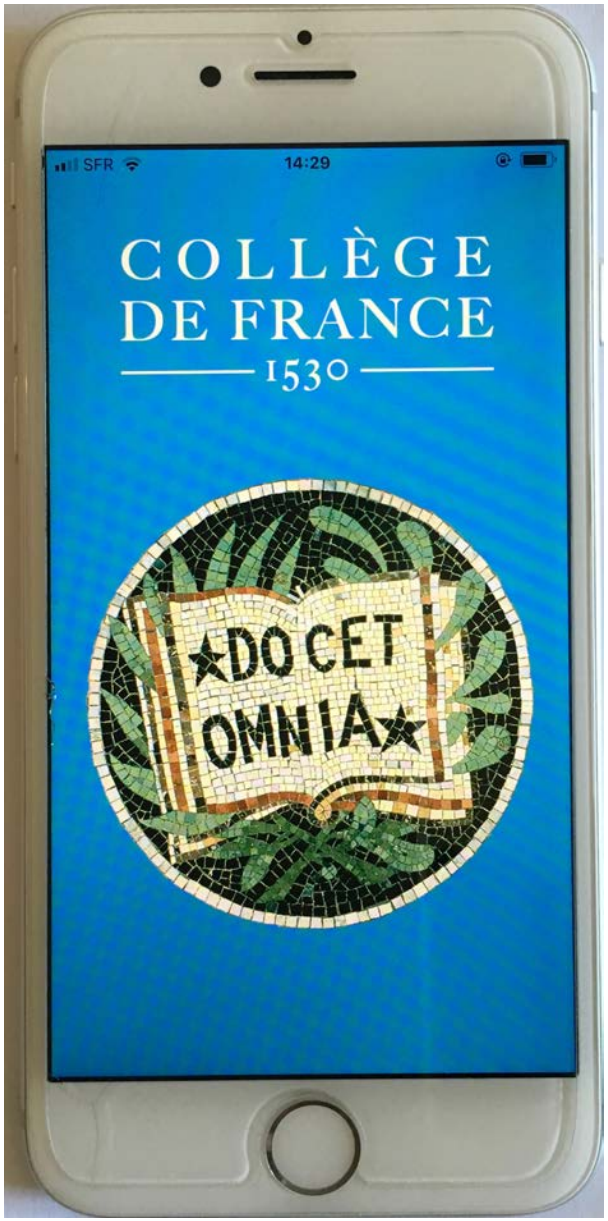
Multifenêtrage + souris (toujours en 2019)

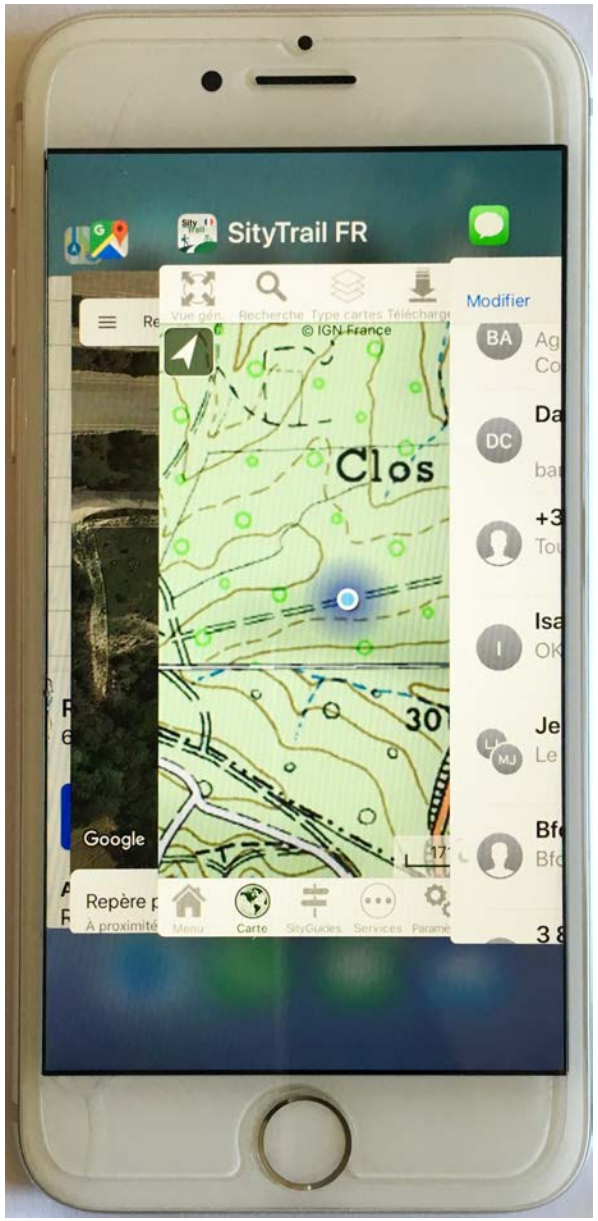


Multibureaux

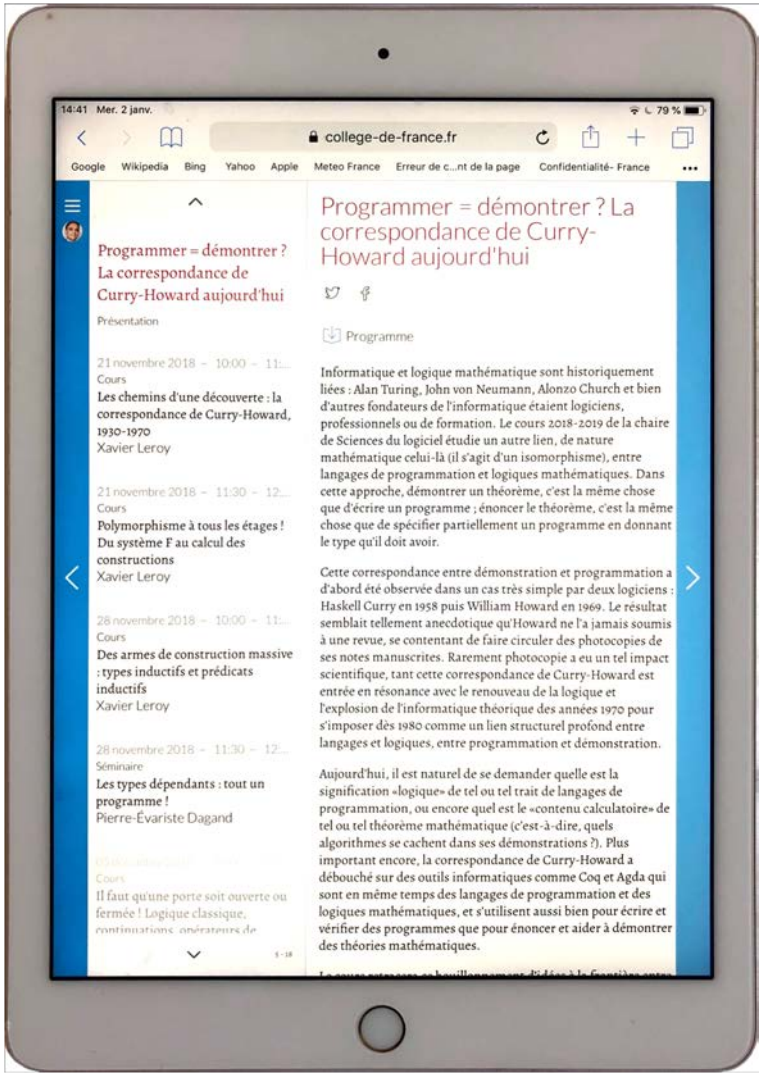


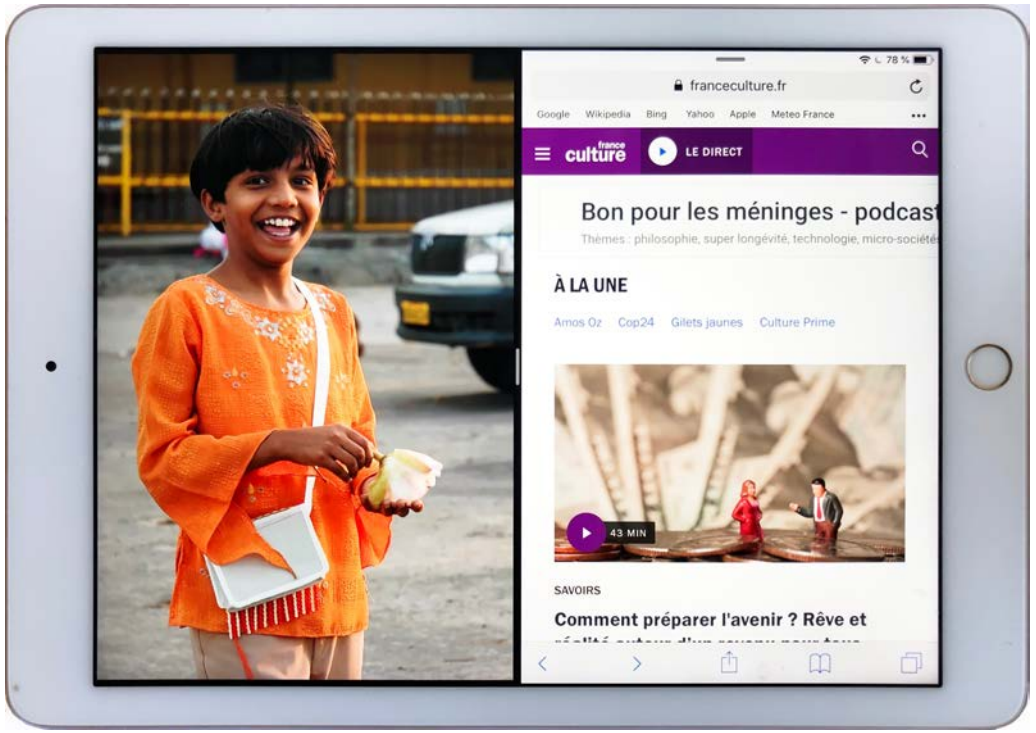
Téléphone : « form factor » petit + tactile





Tablette : « form factor » moyen



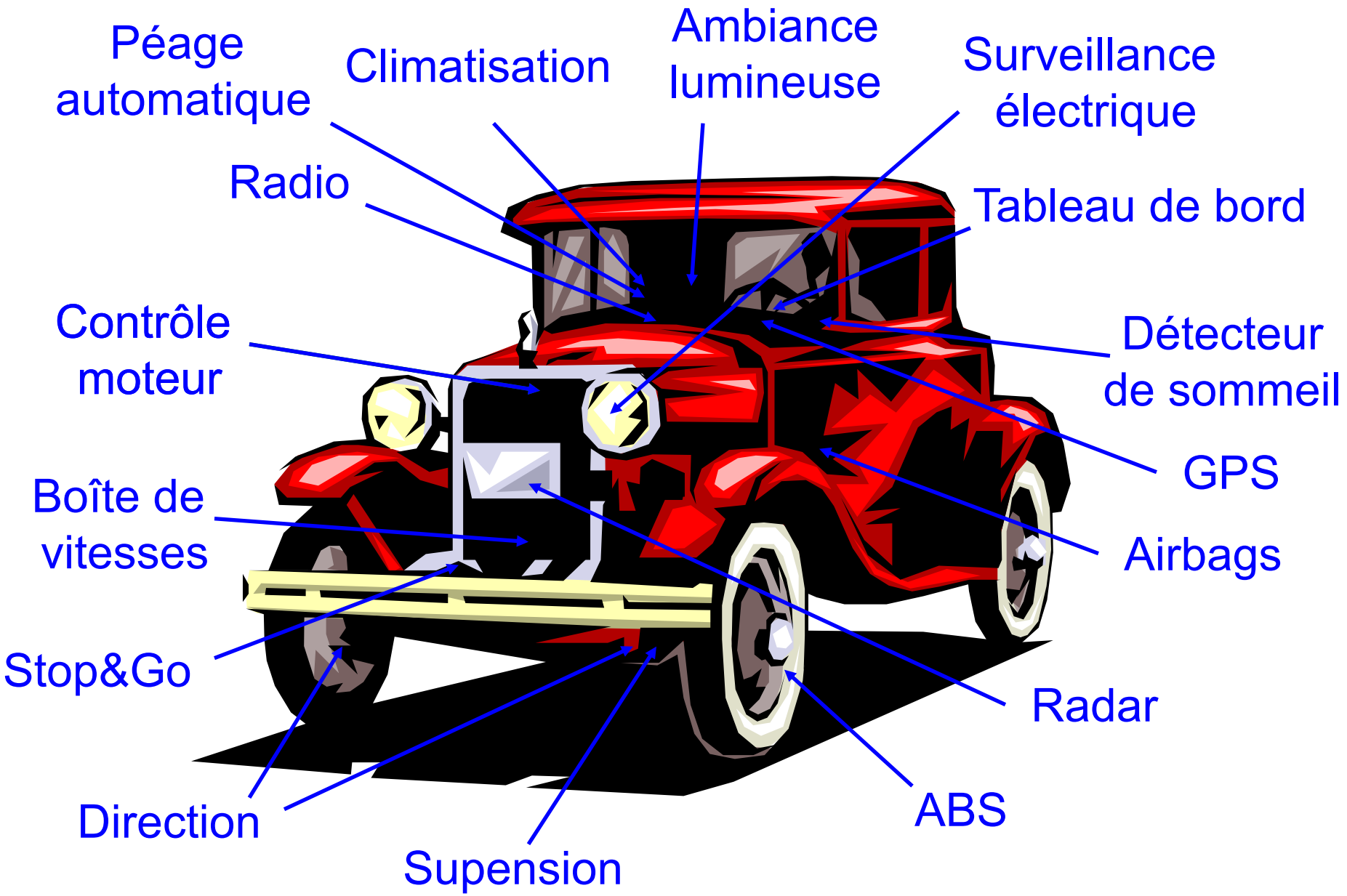


Acte 1 : de 2007 à 2019 quelle évolution?

1. L'hyperpuissance de l'informatique ?
2. L'infrastructure matérielle
3. L'infrastructure logicielle
4. Les applications
5. Vers l'Internet des objets
6. Le recentrage sur les données

Les objets se numérisent et se connectent

Infestation massive par Systems on Chips & logiciels
Pas seulement les montres, assistants vocaux, etc.
Surtout les objets de tous les jours (20e siècle) !

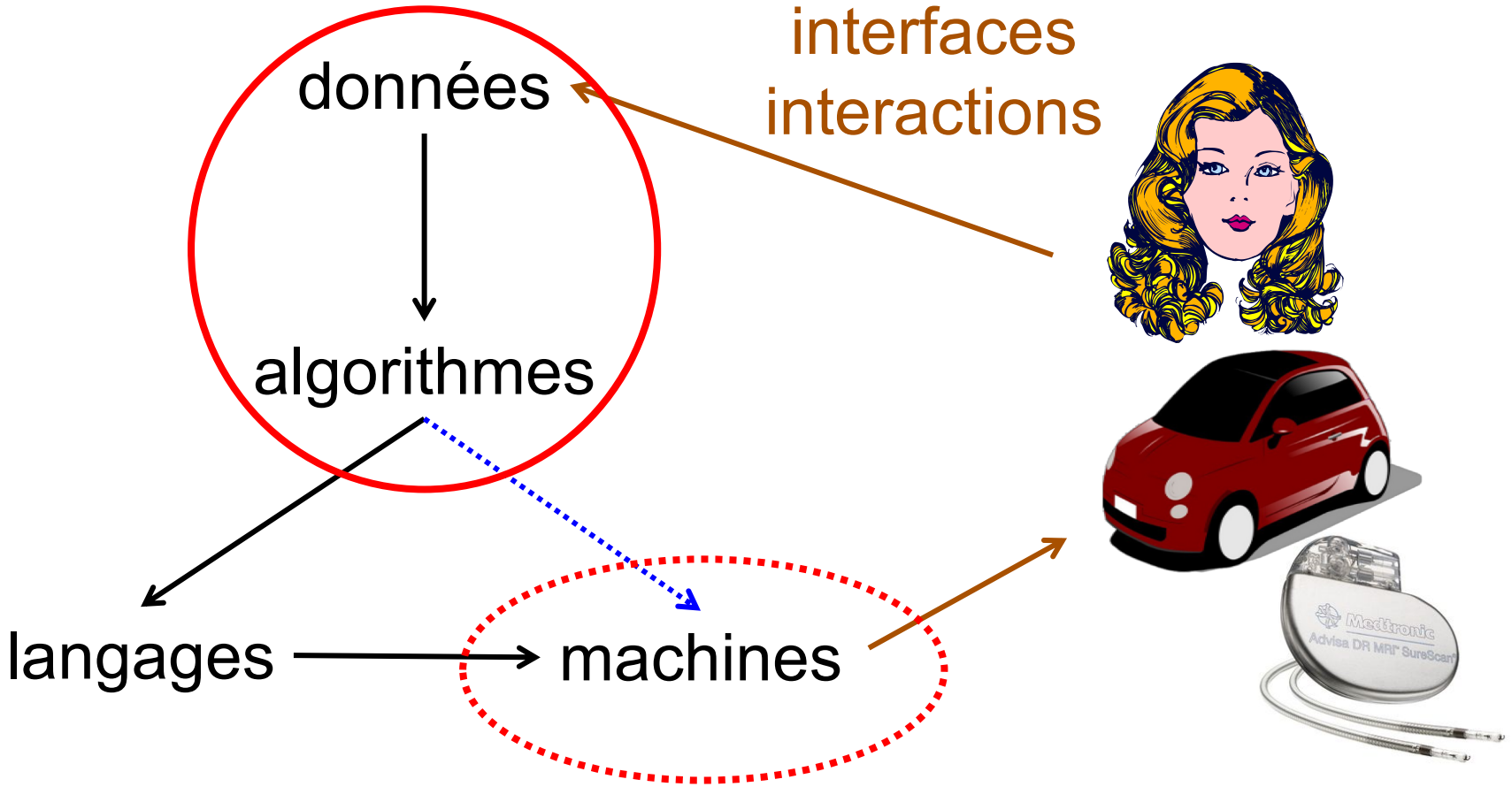


A venir : autonomie, coordination avec la route et les autres voitures

Acte 1 : de 2007 à 2019 quelle évolution?

1. L'hyperpuissance de l'informatique ?
2. L'infrastructure matérielle
3. L'infrastructure logicielle
4. Les applications
5. Vers l'Internet des objets
6. Le recentrage sur les données

Les piliers de l'informatique – version 2019



Recentrage sur les données, devenues massives
analyse statistique, apprentissage profond, etc.
Cf. cours de Stéphane Mallat

Reconnaissance d'objets dans les images

Mask-RCNN Results on COCO dataset, 2017 (Merci à Yann Le Cun)

Autres grands succès

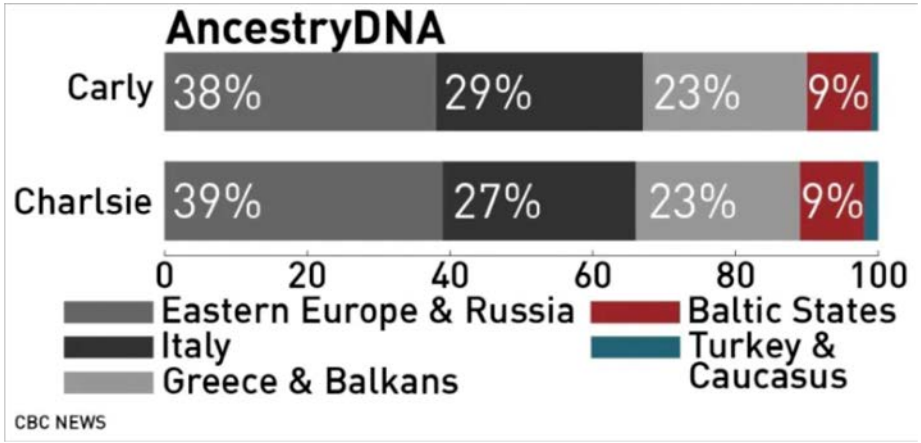
- Analyse de vidéos : du 2D au 3D de image + temps
- Reconnaissance de la parole
- Traduction automatique multilingue
- Etude de comportements
- Détection de tumeurs, santé
  voir colloque du 23 avril 2019
- Robotique
- …

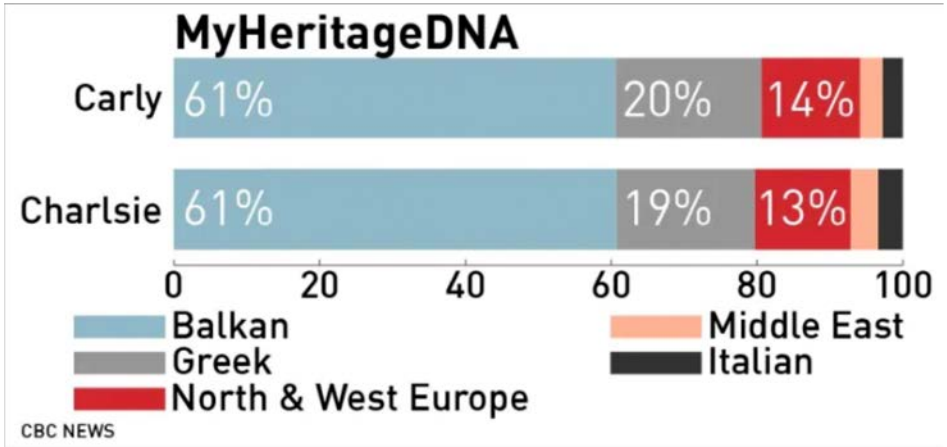
Développement de circuits spécialisés
exemple : TPU (Tensor Programming Unit) de Google

Se méfier des imitations !

Deux jumelles à l'ADN *schokingly identical* selon un prof de Yale font analyser leur ADN par 5 sociétés pour voir leurs origines :

5 résultats bien différents ! soupçon : les algorithmes…





https://www.cbc.ca/news/technology/dna-ancestry-kits-twins-marketplace-1.4980976

Trois sortes d'analyses prédictives (Yann Le Cun)

- Renforcement pur (jeu de Go)
  - la machine prédit un petit nombre de bits (victoire / défaite)
  - elle reçoit peu de feedback (fin de partie)
  - demande énormément d'entraînement !
- Apprentissage par supervision
  - la machine prévoit un petit nombre de bits (type d'objet)
  - elle reçoit un feedback à chaque essai
  - demande beaucoup d'entraînement par exemples annotés
- Apprentissage auto-supervisé (nous?)
  - peu de supervision, mais énormément de feeback de l'expérimentation spontanée
  - exemple : le bébé et la gravité, la tache aveugle de l'œil

Inférence du contenu d'une zone aveugle

Apprentissage de modèles par prédiction

Merci à Yann Le Cun pour ces exemples

L'orang-outan est la magie

Dan Zaleski, https://www.youtube.com/watch?v=FIxYCDbRGJc

Entracte

« De l'autre côté du rideau », Compagnie plein feux d'Aubagne

Acte 2 : évolutions en cours et futures (?)

1. La numérisation progressive de la société
2. Exemples de succès et d'échecs
3. Les problèmes de sécurité deviennent majeurs
4. Un exemple : l'informatisation de la médecine

Acte 2 : évolutions en cours et futures (?)

1. La numérisation progressive de la société
2. Exemples de succès et d'échecs
3. Les problèmes de sécurité deviennent majeurs
4. Un exemple : l'informatisation de la médecine

La numérisation progressive de la société

- Commerce, banques en ligne
- Réservations : trains, avions, théâtres, cinémas, hôtels, …
- Echanges : produits d'occasion, partages de voiture, …
- Cartographie : localisation, itinéraires, agriculture, télédétection,..
- Culture : radios, TVs, podcasts, vidéos, films, concerts
- Information : journaux, blogs, réseaux sociaux (?)
- Echanges de savoir : cuisine, lecture, couture, décoration
- Etat, services publics : impôts, informations, données publiques
- …

Explosion de nouveaux acteurs privés

Moteurs de recherche

Réseaux sociaux

Commerce

Hôtellerie

Transports

Musique

Vidéo, cinéma

Non, ce n'est pas de la pub !

C'est pour insister sur le fait que ces sites sont imprégnés de la pensée informatique

et ont remplacé ceux qui ne l'étaient pas !

→ plus riche industrie mondiale

souvent effet *Winner Take All*

Des modèles économique simples

- Pour capter la valeur ajoutée de l'hôtellerie (du transport), est-il essentiel d'avoir des hôtels (des taxis) ?

  Non, ce qui compte c'est de savoir qui veut aller où et quand, de collecter ces données et les recommandations, etc. !

  Devise de XXX.com : *un pour tous, tous pour un, et mes 15% !*

- Pour la musique et la vidéo, qui sont de la pure information, pourquoi avoir encore des supports physiques ?

  Encore oui pour la qualité supérieure, mais ça change vite

  (mais les amoureux du vinyle existent aussi)

… accompagnés de problèmes sérieux

- L'invasion de la publicité
  - n'est-il pas aberrant de payer pour ne pas en avoir ?
- L'usage exagéré des écrans
  - déjà vrai pour la TV – problème d'enfants ou de parents ?
- Les dangers de la propagation trop rapide de l'info
  - infox (fake news) généralisées
- …

Aucun espoir d'améliorer la situation en faisant l'impasse sur la compréhension de ses causes réelles

Serons nous toujours en retard d'un métro ?

« Nous on fait, les Européens régulent »

… et aussi sites participatifs !

Encyclopédie

Cuisine

Cartographie

financement participatif

Voyages

L'importance des acteurs non commerciaux

- Wikipedia, la gigantesque encyclopédie
- Le logiciel libre, à développement collaboratif
  - Linux, NTP, langages de programmation, vérifieurs, …
- Internet Archive, sauvegarde du web (volontaire)
  - 15 pétaoctets, 330 10^9 pages, 2 10^6 livres, 10^7 textes
- Software Heritage, la grande mémoire du logiciel
  - 4,5 10^9 fichiers sources, 83 10^6 projets
- Les sciences ouvertes et collaboratives
  - physique, astronomie, sécurité informatique

Tout autant fondés sur la pensée informatique
Constituant une riche culture mondiale !

Etat et services publics

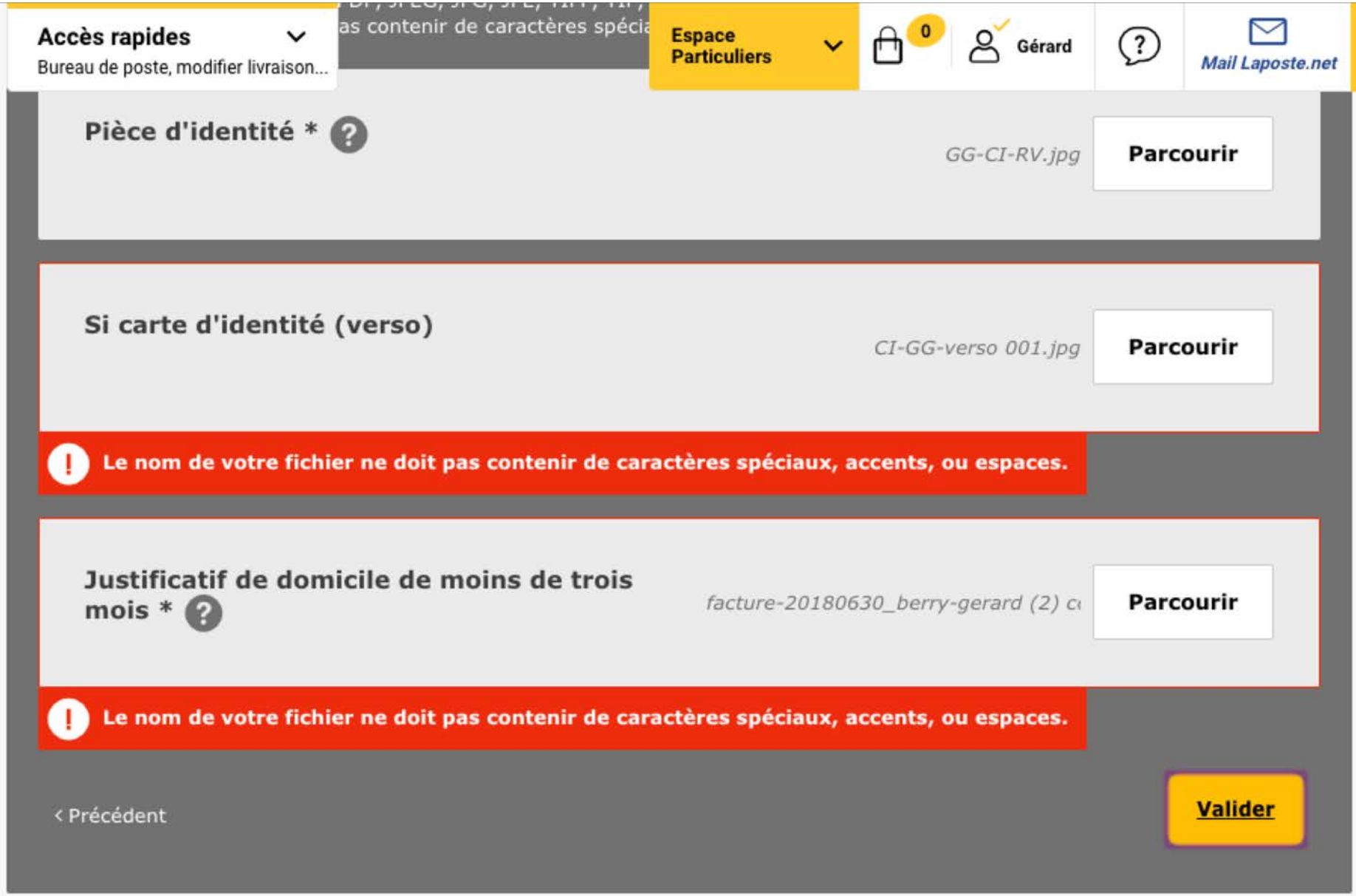
- Gros effort informatique, sites bien faits
  - impots.gouv.fr, service-public.fr
  - legifrance.gouv.fr, etalab.gouv.fr, data.gouv.fr gouvernement.fr, FranceConnect.fr
  - campagnol.fr pour les sites de mairies
- Mais encore bien trop de sites mal faits…
  - lauto-entrepreneur.fr, www.urrsaf.fr, net-entreprises.fr
  - https://digiposte.fr, demande de procuration
  - cartes grises

Amélioration continue

Quid de ceux qui n'ont pas ou n'aiment pas Internet ?

cf. défenseur des droits, janvier 2019

Les surprenantes lois de la poste



Acte 2 : évolutions en cours et futures

1. La numérisation progressive de la société
2. Exemples de succès et d'échecs
3. Les problèmes de sécurité deviennent majeurs
4. L'informatisation de la médecine

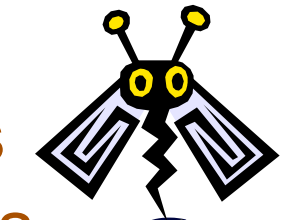
Exemples de succès

- L'informatisation des avions et métros
  - voir séminaires d'E. Ledinot, et de J-R. Abrial
- Les fonctions bien informatisées des voitures
  - freinage, moteur, etc. (pas toutes de ce niveau, hélas)
- La photo numérique, du reflex au smartphone
- L'imagerie médicale
  - une extraordinaire aventure physique et informatique
- Les appareils de physique et d'astronomie
  - mais encore de gros échecs (Ariane 501 → Schiaparelli)
- Le traitement algorithmique du génome
- Les prouesses de l'apprentissage automatique
- …

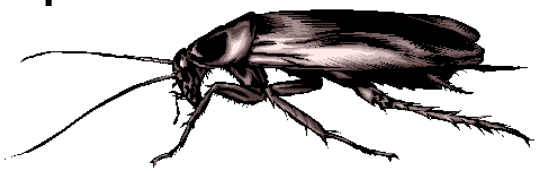
Echecs : bugs et trous de sécurité

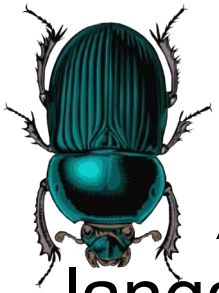
données

interfaces
interactions

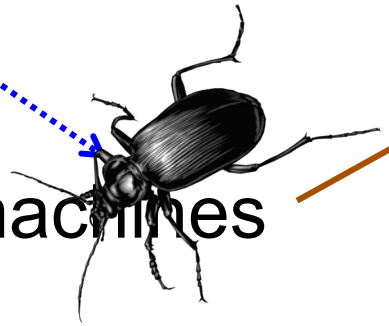


algo





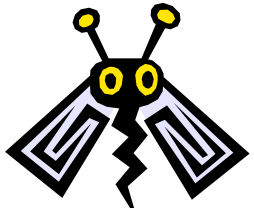
langages ⟶ machines



Sûreté : bon fonctionnement dans tous les cas
Sécurité : protection des données et des systèmes

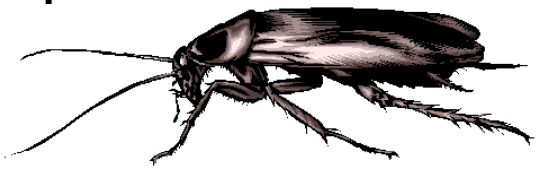
Echecs : bugs et trous de sécurité

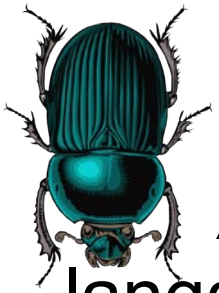
données



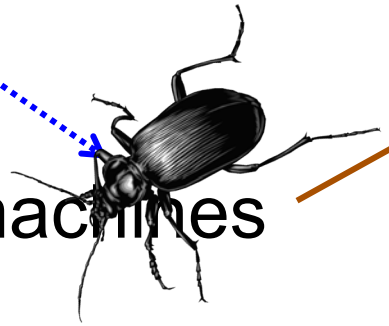
interfaces
interactions

algo





langages ⟶ machines



Deux dangers majeurs de l'informatique,
dont la puissance s'étend avec elle

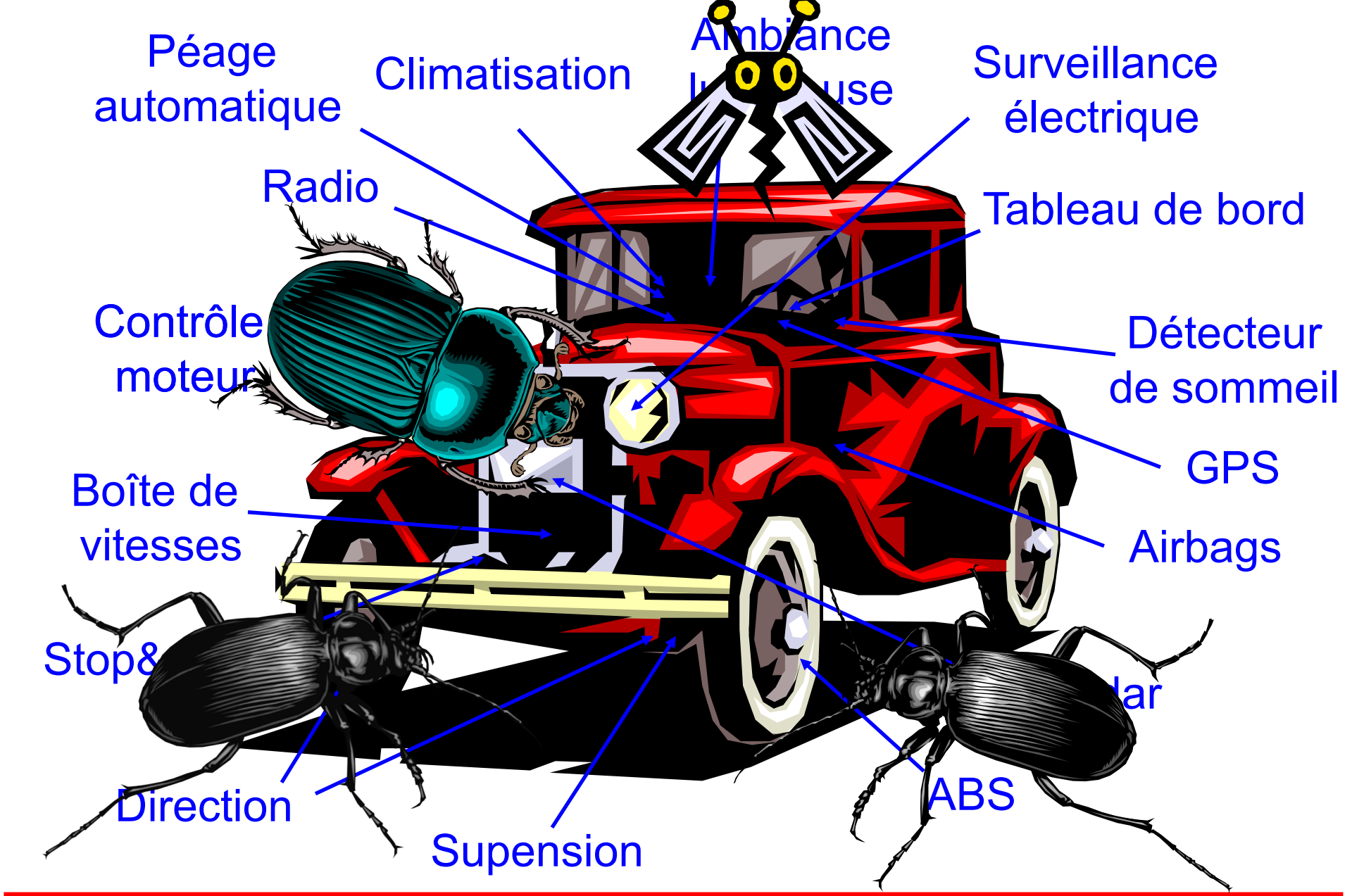
Exemples d'échecs

- Toujours des projets non convergents
  - Louvois, cartes grises, …
- Problèmes fréquents de qualité logicielle (bugs)
  - semi-gênants dans les apps de téléphones – drôles ?
  - inacceptables dans les logiciels contrôlant des processus dangereux : trains, voitures, internet des objets,…
- Sous-estimation persistante de l'interaction homme-machine
  - sites mal conçus, pleins de vide
  - sites nombreux et différents pour des fonctions reliées
- Problèmes croissants de sécurité informatique

Internet des objets : encore problématique

- Logiciels et IHM souvent frustres (⇒ frustrants)
  - IHM peu intuitives, documentations illisibles
  - qualité logicielle trop faible sans certification (ex. automobile)
  - la commande à distance est-elle vraiment avantageuse ?
- Gros problèmes de sûreté-sécurité sans certification
  - bugs de logiciels automobiles ⇒ accidents graves
  - domotique peu ou mal sécurisée
  - ouverture facile voire prises de contrôle des voitures (chères)
  - trous de sécurité dans les pacemakers et pompes à insuline

Voir cours 2017 et
cours / séminaire sécurité du 13/02/2019



A venir : autonomie, coordination avec la route et les autres voitures

Contrôle moteur Toyota Camry : 89 morts

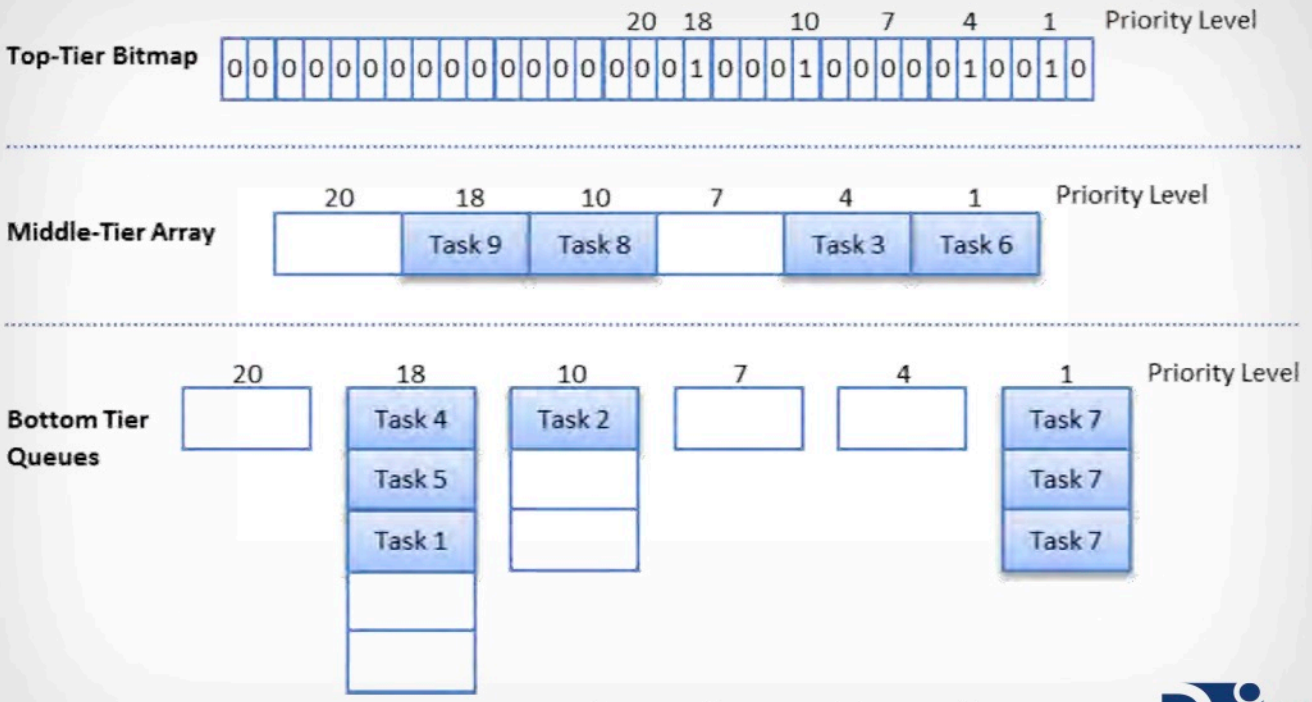
There are a large number of functions that are overly complex. By the standard industry metrics some of them are untestable, meaning that it is so complicated a recipe that there is no way to develop a reliable test suite or test methodology to test all the possible things that can happen in it. Some of them are even so complex that they are what is called unmaintainable, which means that if you go in to fix a bug or to make a change, you're likely to create a new bug in the process. Just because your car has the latest version of the firmware -- that is what we call embedded software -- doesn't mean it is safer necessarily than the older one….And that conclusion is that the failsafes are inadequate. The failsafes that they have contain defects or gaps. But on the whole, the safety architecture is a house of cards. It is possible for a large percentage of the failsafes to be disabled at the same time that the throttle control is lost.

Michael Barr, expert de la justice américaine

Rapport de plus de 750 pages, secret !

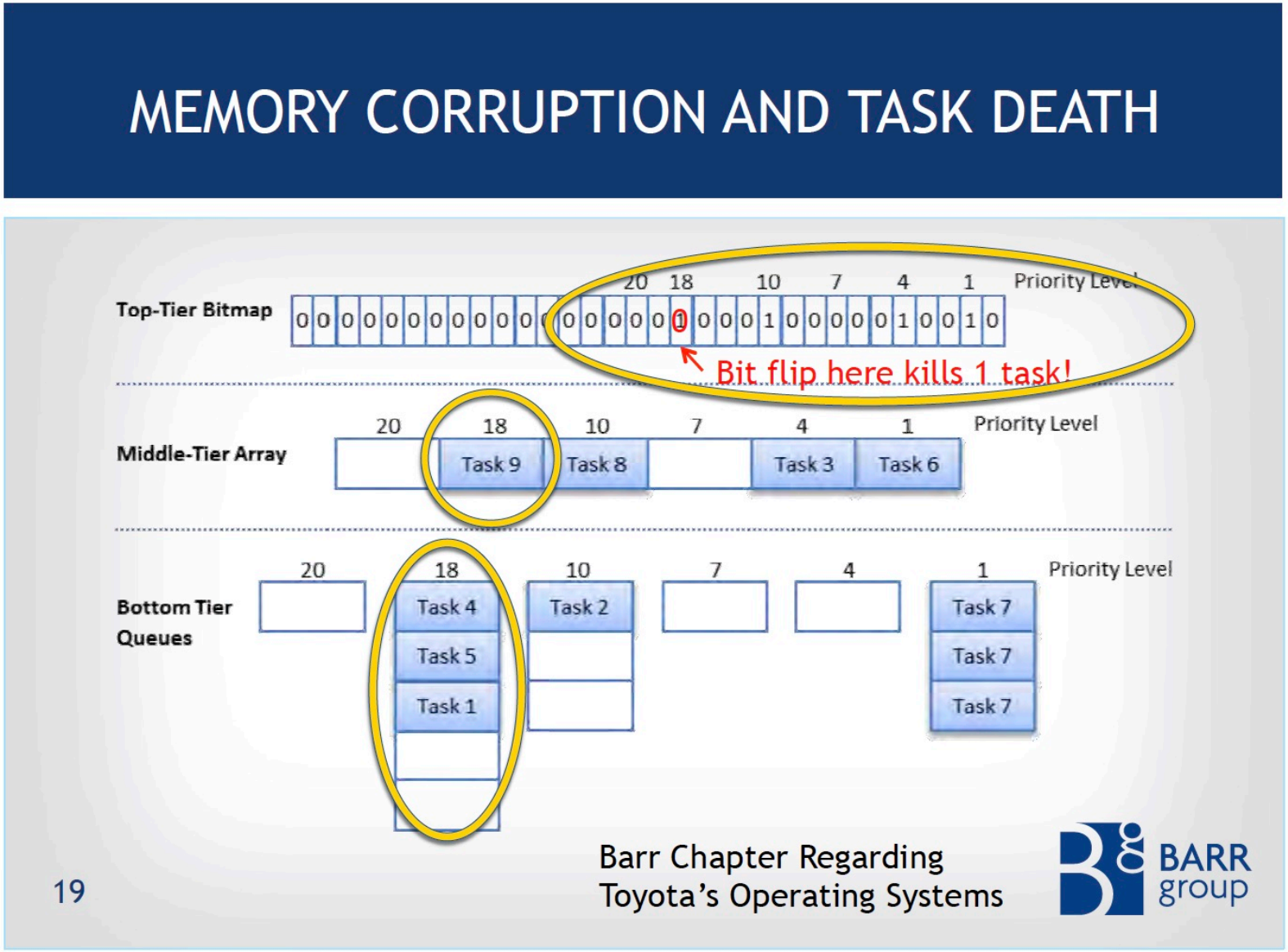
Gestion des tâches en OSEK

OSEK'S CRITICAL DATA STRUCTURES



http://www.safetyresearch.net/Library/BarrSlides_FINAL_SCRUBBED.pdf

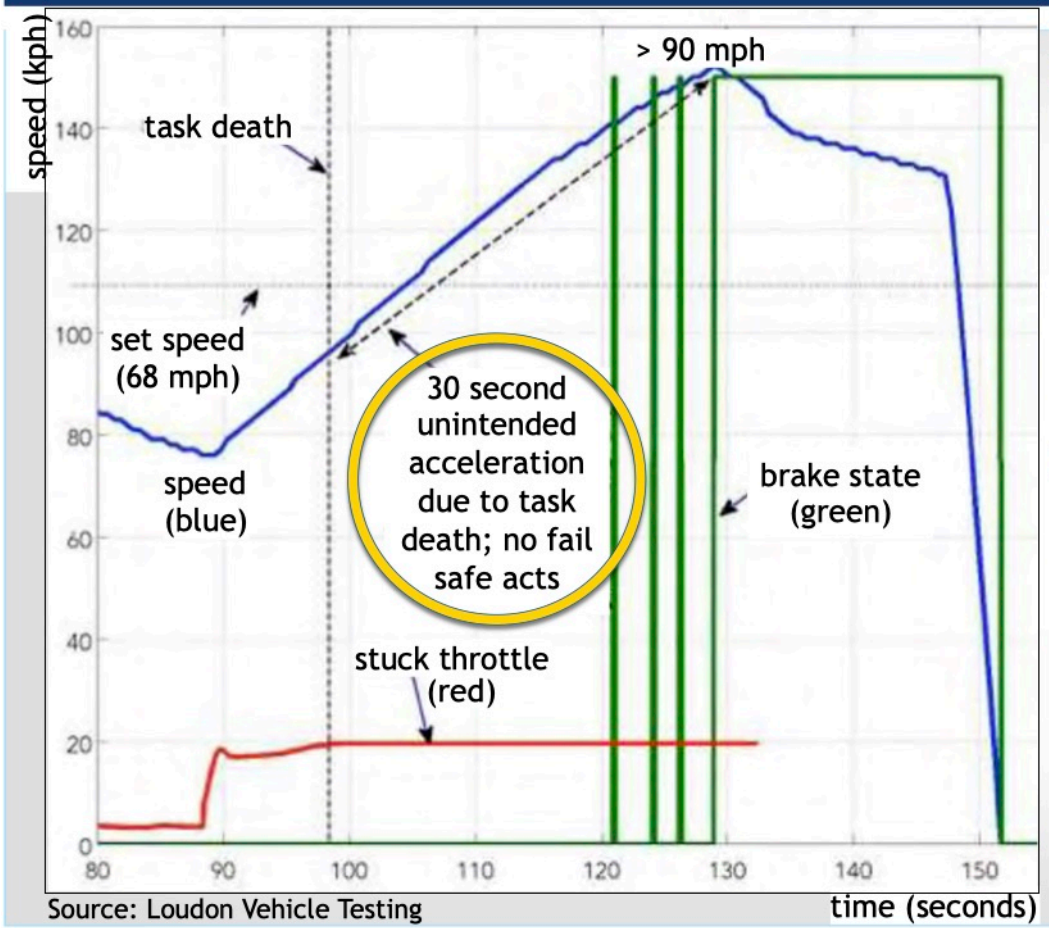
Corruption mémoire → mort d'une tâche critique



http://www.safetyresearch.net/Library/BarrSlides_FINAL_SCRUBBED.pdf

Exemple d'accélération spontanée

EXAMPLE OF UNINTENDED ACCELERATION



- Representative of task death in real-world
- Dead task also monitors accelerator pedal, so loss of throttle control
  - ✓ Confirmed in tests
- When this task's death begins with brake press (any amount), driver must fully remove foot from brake to end UA
  - ✓ Confirmed in tests

BARR group

http://www.safetyresearch.net/Library/BarrSlides_FINAL_SCRUBBED.pdf

Causes potentielles de corruption mémoire

SOFTWARE CAUSES OF MEMORY CORRUPTION

Type of Software Defect	Causes Memory Corruption?	Defect in 2005 Camry L4?
Buffer Overflow	Yes	Yes
Invalid Pointer Dereference/Arithmetic	Yes	Yes
Race Condition (a.k.a., "Task Interference")	Yes	Yes
Nested Scheduler Unlock	Yes	Yes
Unsafe Casting	Yes	Yes
Stack Overflow	Yes	Yes

21

Barr Chapter Regarding Toyota's Software Bugs

BARR group

http://www.safetyresearch.net/Library/BarrSlides_FINAL_SCRUBBED.pdf

Après un long déni, une déclaration étonnante

TOYOTA ADMITS ETCS HAS SOFTWARE BUGS

A: ***When it comes to software, there are going to be bugs, and [that] is the case not just with Toyota but with [any] software in the automotive industry and any software. So the issue is not whether or not there is a bug but rather is the bug an important material bug.***

- Ishii 5/24/12 Deposition, p. 91

Indeed there are bugs, including "important material bugs"

32

Barr Chapter Regarding
Toyota's Software Bugs

BARR group

NON !

http://www.safetyresearch.net/Library/BarrSlides_FINAL_SCRUBBED.pdf

Est-on condamné à ce genre de bugs ?

Non ! Tout ça est détectable avec les technologies actuelles d'analyse de programmes, utilisées dans les industries sérieuses

Méthodes B et Event B (Abrial) :
Métro Météor (ligne 14), …

Interprétation abstraite (P&R. Cousot) :
AbsInt → Airbus, Polyspace → automobile

SMT (Satisfaction modulo théories)
→ Preuve du programme général de Parcoursup

Voir aussi inaugurale et cours de Xavier Leroy

Compter le temps, c'est facile – non !

- 31 décembre 2008 : tous les lecteurs MP3 Zune de Microsoft vident leur pile en même temps (bissextile)
- 1er mars 2010 : les PS3 FAT de Sony perdent leur date, ne peuvent plus accéder au réseau, effacent les scores, etc.
- 2010 : au passage à l'heure d'hiver, tous les réveils des iPhone 4 aux USA sonnent une heure trop tard

- 11 février 2007 :
  - 12 F22 Raptor (330 M$ pièce) : Okinawa → Japon
  - au passage de la ligne de changement de date… leurs ordinateurs s'arrêtent et ne rebootent plus !

demi-tour et retour le nez sur les ravitailleurs…
heureusement qu'il faisait beau !

- 200x, Centre cardiologique du nord (F. Besse) :
  - le 29 février, la salle d'angiographie refuse de démarrer
  - corrigé par les néo-zélandais qui ont redémarré le 1er mars à 0h00 !

- Depuis le 1er janvier 2019
  - les sonnettes de nombreux lits d'hôpitaux suisses ne sonnent plus…

- Dharan, Irak, 25 févier 1991, bug des missiles Patriot
  - les arrondis dégradent rapidement la précision de l'heure
  - après 110h, l'erreur est de 0.34 s
  - le Patriot manque le Scud → 28 soldats morts, 98 blessés
  - fix officiel : rebooter toutes les quelques heures…

Pourquoi diable commet-on toujours les mêmes erreurs ?
Manque de professionnalisme !

Acte 2 : évolutions en cours et futures

1. La numérisation progressive de la société
2. Exemples de succès et d'échecs
3. Les problèmes de sécurité deviennent majeurs
4. Un exemple : l'informatisation de la médecine

2019, World Economic Forum

Classement des dangers économiques majeurs :

1. Evénements climatiques extrêmes
2. Désastres naturels
3. Attaques informatiques contre les infrastructures
4. Vols de données et de comptes

Janvier 2019 : 773 millions de paires adresse / mot de passe trouvées sur un site de hackers – dont 6 pour moi !

Fin 2016, 596 millions d'adresses,
avec plusieurs mots de passe pour chacune

D'où l'importance des mots de passe uniques et forts…

Sécurité informatique : le gros point faible

- Vol de données personnelles
  - Equifax, 2016, certification de crédits : 145 milllions
  - Marriott, 2014-18 (rachat de Starwood) : plus de 500 millions
- Attaques sur les réseaux et équipements informatiques
  - Attaque Mirai sur le serveur DNS Dyn par objets connectés
  - Virus Petya, NotPetya, Wannacry → hôpitaux, usines, …
- Attaques sur les objets connectés
  - voitures, pacemakers, pompes à insuline, (avions ?)
- Attaques sur les infrastructures
  - Estonie, réseau électrique Ukrainien

Qu'est-ce qu'une faille de sécurité ?

- Un mauvais comportement d'un utilisateur
  - mot de passe faible, clic d'hameçonnage, etc.
- Un chiffrement trop faible
  - cassé mais qu'on peut forcer pour une transaction car conservé pour parler à de vieux systèmes (HeartBleed)
- Une faille logique dans un protocole de sécurité pour l'établissement des échanges
  - votes, passeports, https, 5G, bluetooth,…
- Un micro-bug, ex. corruption mémoire
  - souvent sans impacts fonctionnels, donc non détecté au tests
- Un canal caché, même sur les systèmes corrects
  - mesure électrique ou même bruit → cassage de chiffrement (Shamir)
  - HW: optimisation des μ-procs → Meltdown, Spectre, BranchScope

Où sont les failles de sécurité ?

- Chez les utilisateurs : mots de passe faibles, hameçonnage
- Dans les OS : Windows, Linux, macosx, iOS, Android, SCADA
  - 2018 : SMS de 1 caractère → crash des iPhone !
- Dans l'infrastructure logicielle et les bibliothèques
  - Adobe Reader, Java, navigateurs, …
  - domotique : Samsung Smart Things
- Dans les applications
  - Smartphones : bien des applications transmettent trop d'informations..
- Trouvées par les chercheurs avant d'être exploitées (?)
  - US Postal : 60 millions de comptes exposés pendant 1 an
  - vulnérabilité trouvée récemment dans la 5G (pourtant très sérieuse)
  - HeartBleed, Logjam : attaques sur https, sur les « votes électroniques »
  - failles internes des microprocesseurs : Meltdown, Spectre, BranchScope

Venez au cours et séminaire du 13 février 2019 !

Prise de contrôle à distance de Jeep Cherokee

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Leur code est un cauchemar : un logiciel qui laisse les hackers envoyer des commandes par l'autoradio de la Jeep vers son moteur, son tableau de bord, sa direction, ses freins, sa transmission, tout ça depuis un PC quelconque qui peut être à l'autre bout du pays…

Acte 2 : évolutions en cours et futures

1. La numérisation progressive de la société
2. Exemples de succès et d'échecs
3. Les problèmes de sécurité deviennent majeurs
4. Un exemple : l'informatisation de la médecine

Venez au colloque du 23 avril 2019

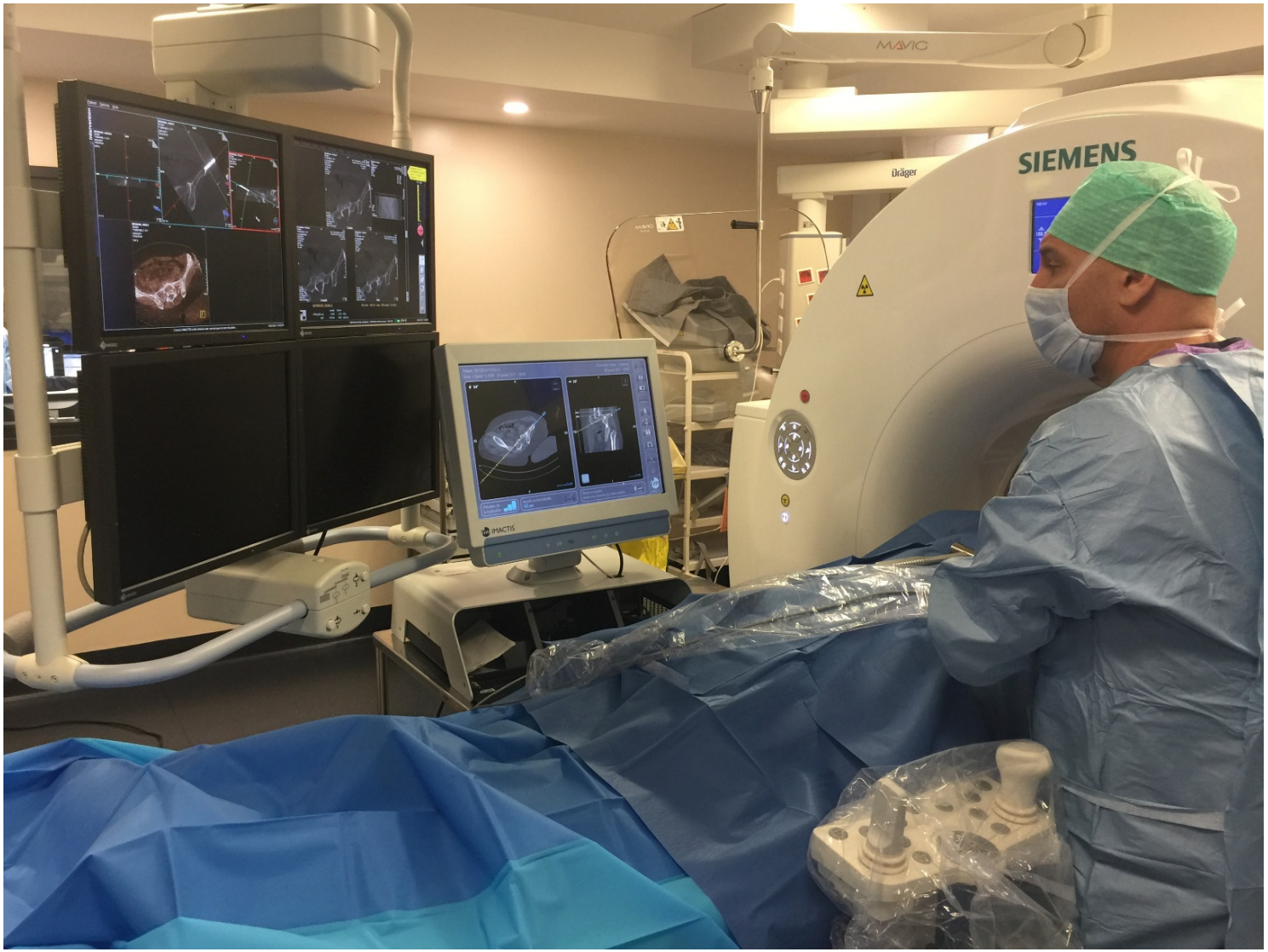
L'imagerie médicale à l'heure de l'IA : défis et opportunités

https://www.college-de-france.fr/site/gerard-berry/symposium-2018-2019.htm

Où intervient l'informatique en médecine ?

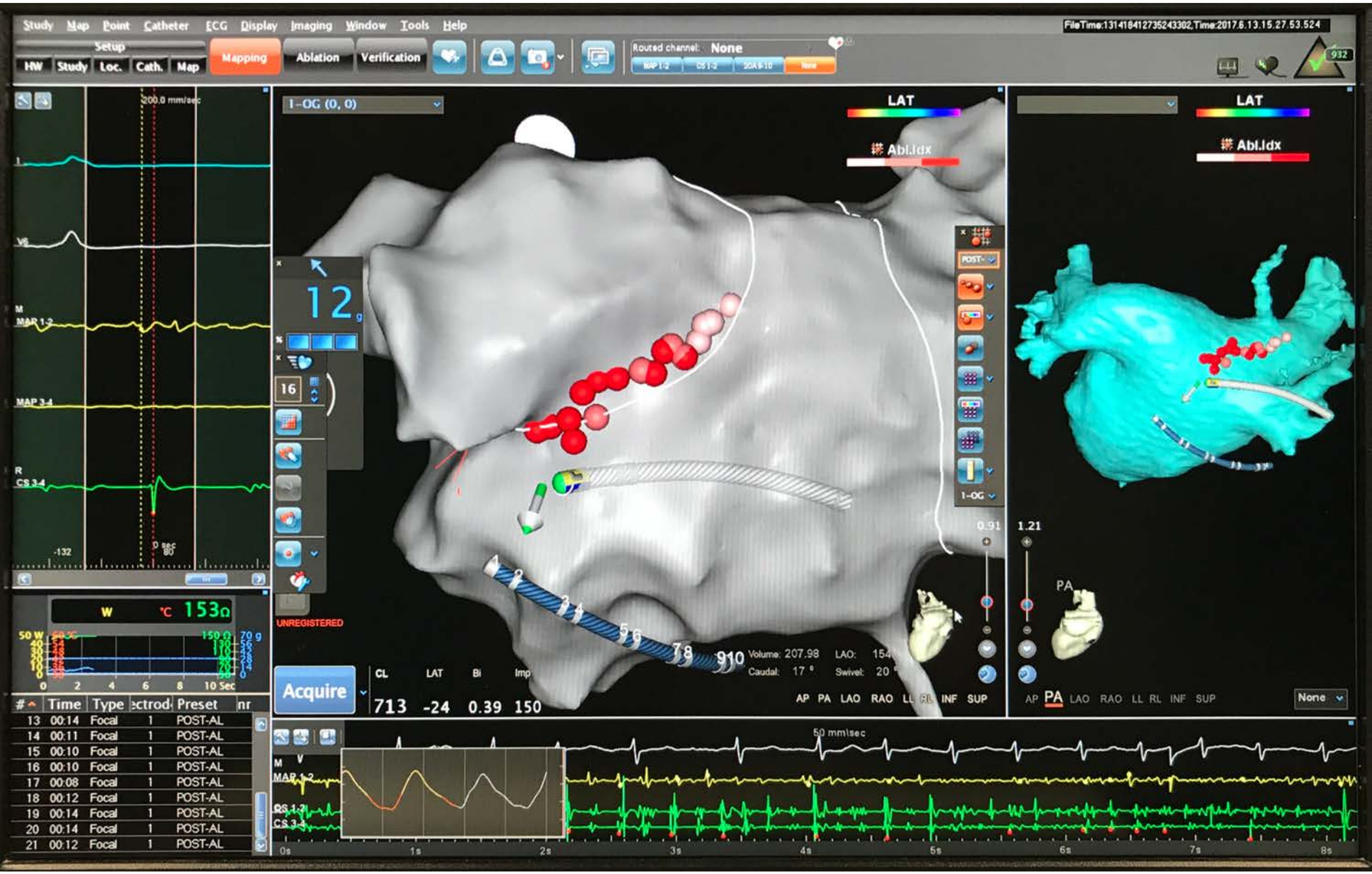
- Imagerie 2D/3D/4D, analyse d'images, instrumentation
- Radiologie interventionnelle
- Modélisation et simulation d'organes (cf. cours Ayache)
- Chirurgie :
  - robots, réalité virtuelle, simulation, …
- Appareillage :
  - pacemakers, pompes à insuline, audition, vision, …
- Protocoles de soin
- Collecte et analyse de données massives
  - diagnostic par apprentissage (tumeurs, mélanomes, etc.)
- Internet :
  - contact médecin / malade, réseaux de patients, informations médicales, …

Radiologie interventionnelle



Source F. Besse, Centre de Cardiologie du Nord

Multimodalité et réalité augmentée



Source F. Besse, Centre de Cardiologie du Nord

Sûreté et sécurité en médeine

- Sûreté : absence de bugs logiciels
  - Therac 25 : surirradiations massives
- Sécurité : protection des données et appareils
  - virus Wannacry (XP) ➤ 81 hôpitaux anglais
  - pacemakers (2017) : milliers de trous de sécurité
  - pompes à insuline : idem

Alors que les médicaments son hyper-testés,
rien n'est fait pour les logiciels
Avertissement du ministère US de la santé à la FDA

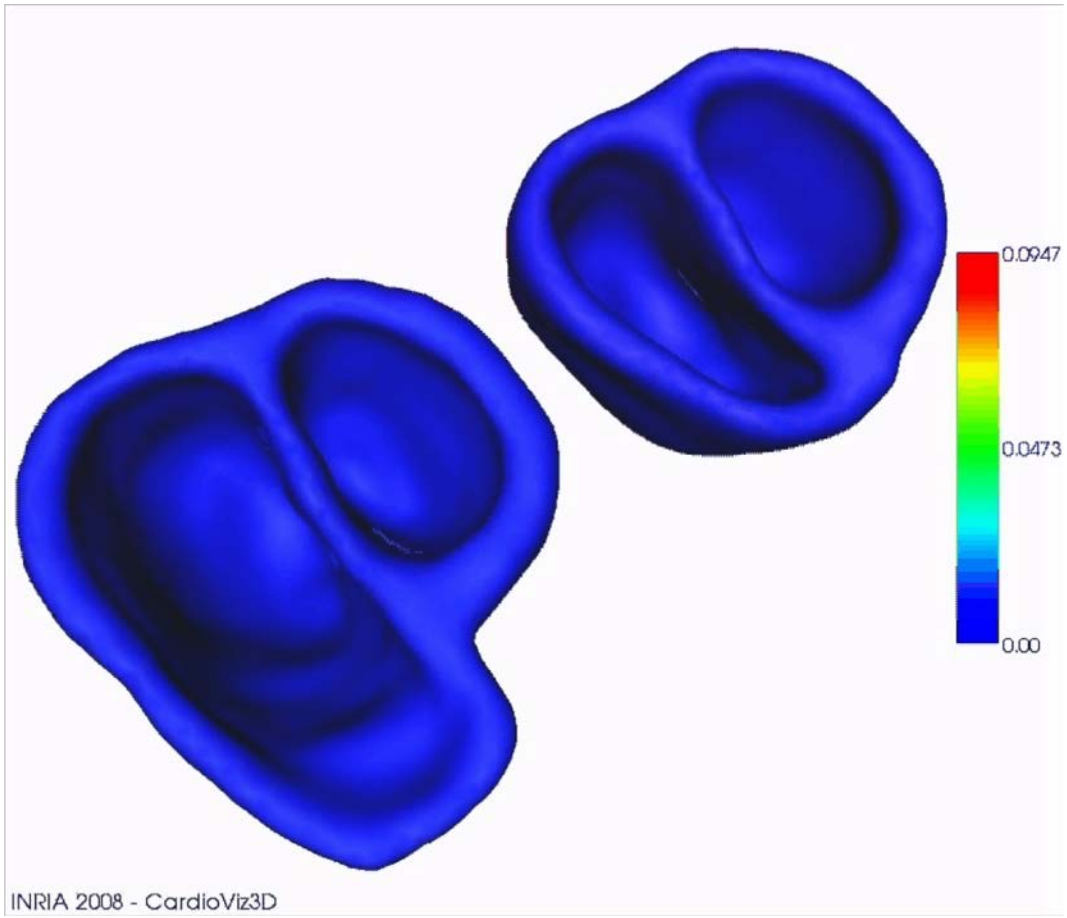
Le corps médical est-il vraiment au courant ?

Analyse de données ou modélisation ?

- Analyse de données massives
  - *deep learning* : grands succès, mais pas encore de compréhension ni d'explicabilité – problème ou pas ?
  - corrélation n'est ni explication ni causalité
  - risque : le renforcement des biais
- Modélisation
  - par lois mathématiques ou algorithmiques, ex. cœur
  - force d'explication, de simulation et de prédiction
  - mais le modèle doit être validé par l'expérience

A venir : couplage modèles / apprentissage ?

Modéliser et simuler une opération



Simuler, c'est remplacer matière, énergie et ondes par l'information et l'algorithme

Amélioration des protocoles médicaux

- Les protocoles hospitaliers sont complexes
  - nombreuses mesures et prescriptions temporellement liées
  - nombreux choix au cours du temps en fonction des résultats des mesures
- Leur description est souvent trop plate et difficile à comprendre et à tracer par la variété des acteurs
  ⇒ nombreux accidents médicaux (USA : + 400 000 / an)

Une solution possible : utiliser Esterel / HipHop pour leur spécification rigoureuse et traçable (avec Northwestern University Hospital, Chigago)

Le médecin face à l'algorithme

- Peut-on faire confiance à un algorithme qui se sait pas expliquer ses décisions ?

  Qui sera responsable en cas d'erreur de diagnostic ?

  Mais un médecin sait-il toujours expliquer ses décisions ?

- Les algorithmes seront disponibles sur Internet

  Que fera le médecin si le patient lui donne un diagnostic différent du sien ?

- Les capteurs connectés du patient pourront envoyer de l'information en temps-réel au médecin

  Comment et quand le médecin y accédera-t-il ?
  Comment saura-t-il quoi dire au malade à distance ?

  Consultation par téléphone → chat ou visioconférence ?

Le patient face à l'algorithme

- Pourra-t-on envoyer des courriel ou des SMS au médecin ?
  Ou le voir en vidéo comme pour le reste de la population ?

- Croira-t-on un médecin qui conteste les diagnostics qu'on a payés de sa poche sur Internet ?

- Les capteurs connectés envoient de l'information au médecin

  A-t-on vraiment besoin d'un médecin si un site Internet suffit ?

  Mais le médecin soigne un humain, pas un diagnostic !

Bien des questions à discuter
avant qu'il ne soit trop tard…

Conclusion

- L'hyperpuissance de l'informatique n'est pas un vain mot
- Bien faite, elle rend des services inestimables.
  Mal faite, elle peut conduire à des désastres
- Les moyens de mal faire sont connus
  Les moyens de bien faire aussi (mais plus durs)
- Le grand système développé dans les 10 dernières années va se consolider, avec toujours des avancées inattendues
- Les problèmes de sûreté et de sécurité sont durs et vont limiter l'expansion, en particulier pour l'Internet des objets
- Un grand problème reste l'ignorance du public général

D'où l'importance de l'éducation, trop longtemps en jachère
Voir le prochain cours du 6 février 2019 !