Institut
Mines-Télécom

Principe des Architectures Numériques

Introduction et logique combinatoire

Jean-Luc Danger

Objectifs du module ELEC 203

- Connaître les bases des architectures des circuits nuémriques
- Comprendre les fonctions de base de l'électronique numérique
- Comprendre la logique combinatoire et synchrone
- Comprendre comment concevoir un circuit numérique
- Application à un algorithme cryptographique
- Etude des phénomènes physiques des circuits
- Initiation aux attaques par canaux cachés des architectures cryptographiques

Informations utiles

Site pédagogique

- `http://sen.enst.fr/elec203`

Plan

Principe des architectures

De l'algorithme au circuit

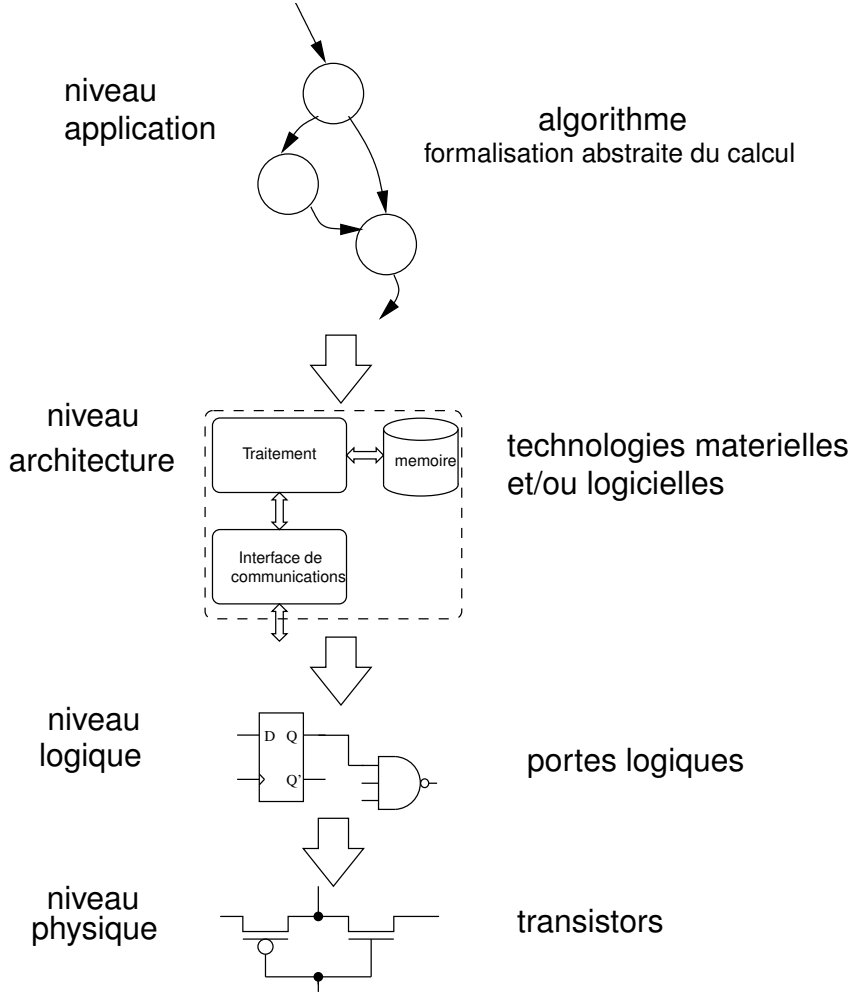


FIGURE : Niveaux hierarchiques

Implantation d'un algorithme

Règles de base au niveau architecture

- la technologie **matérielle** est indispensable
- la technologie **logicielle** offre une grande flexibilité
- le calcul matériel est synchrone $\Rightarrow$ signal d'**Horloge**
- le calcul matériel doit être initialisé $\Rightarrow$ signal de **Reset**

Architecture d'une application numérique

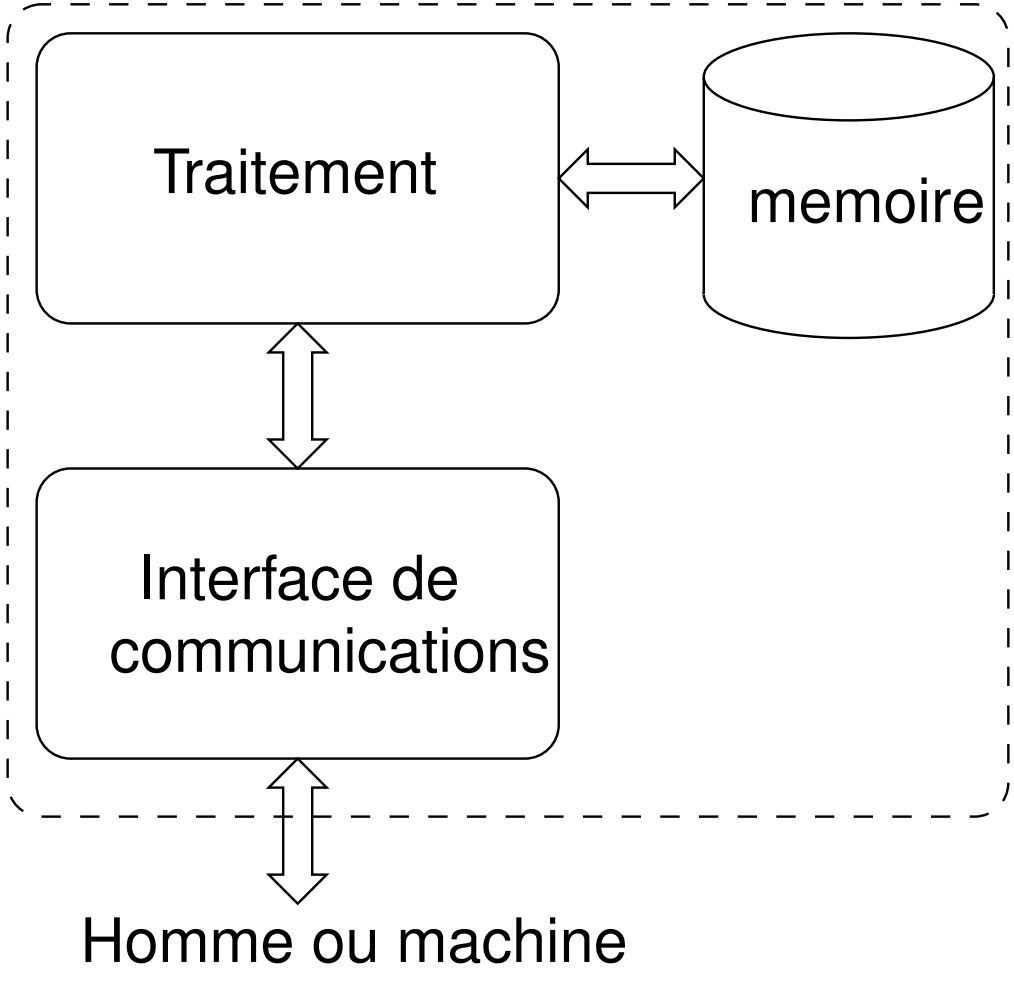


FIGURE : Architecture générale d'un système numérique

Des mathématiques à la physique 1/2

Des contraintes physiques importantes à considérer

- **Complexité** faible de l'architecture
- **Vitesse de calcul** élevée
- **Consommation** faible

Nécessité d'un Système mixte

- La technologie 100% matérielle délivre l'optimalité mais n'est pas flexible
- pour un grande flexibilité : mélange Matériel/Logiciel

Des mathématiques à la physique 2/2

Autres contraintes importantes

- **Testabilité** : facilité pour vérifier l'intégrité du système
- **Fiabilité** : le bon fonctionnement doit durer le plus de temps possible
- **Sécurité** : Certaines données doivent être secrètes
- **Compatibilité** : conformité avec l'environnement

Architecture de traitement application numérique matérielle

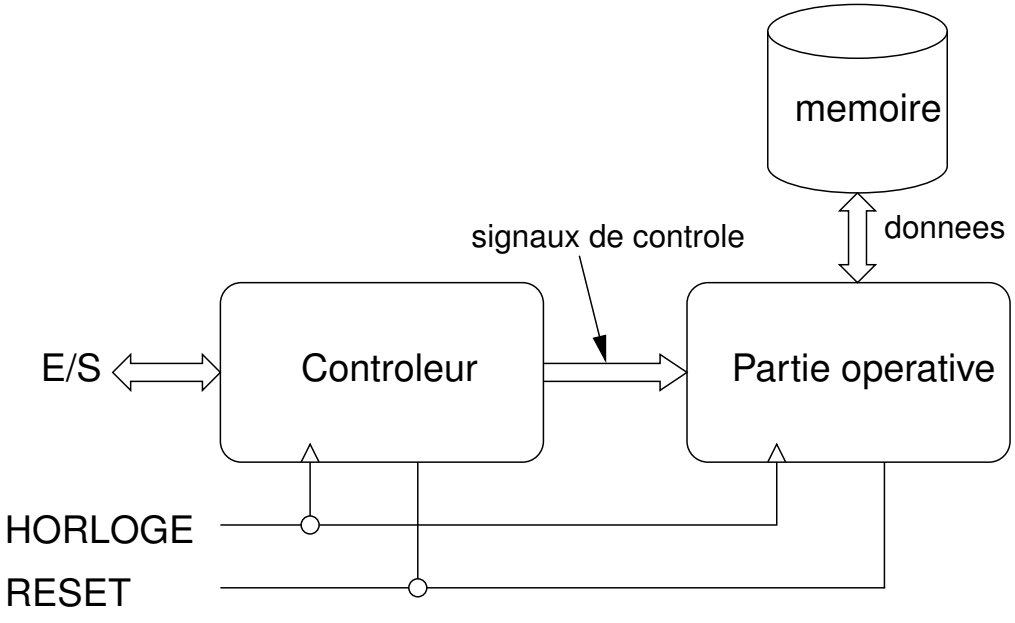


FIGURE : Architecture générale d'un traitement matériel

Architecture de traitement application numérique logicielle

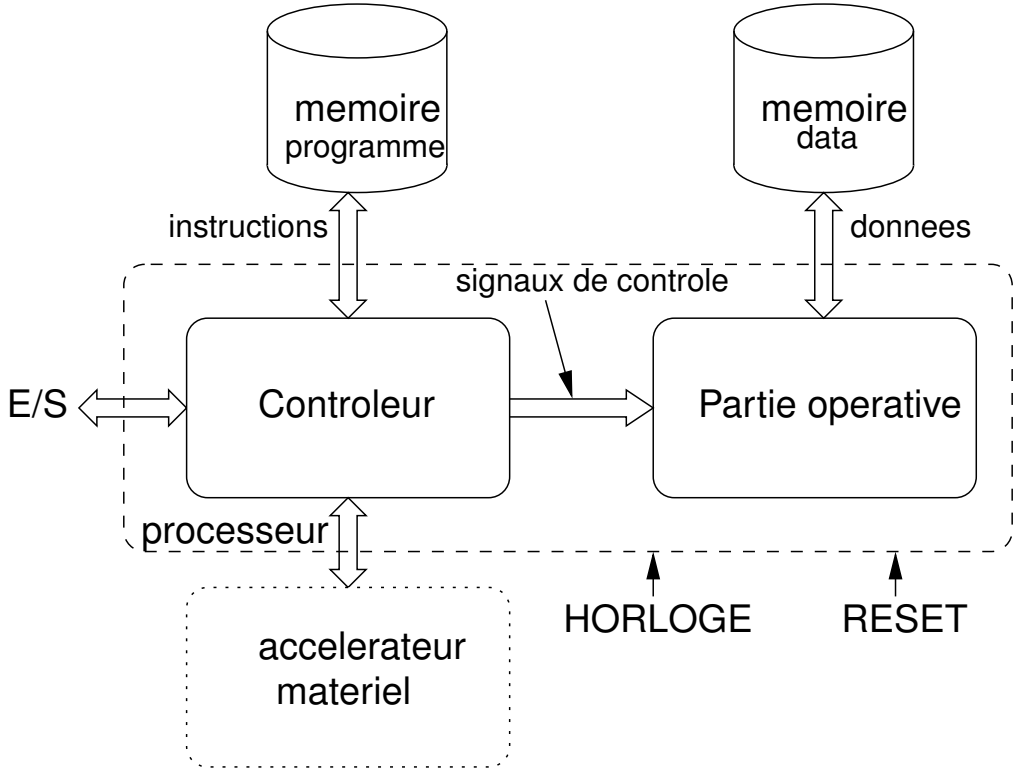
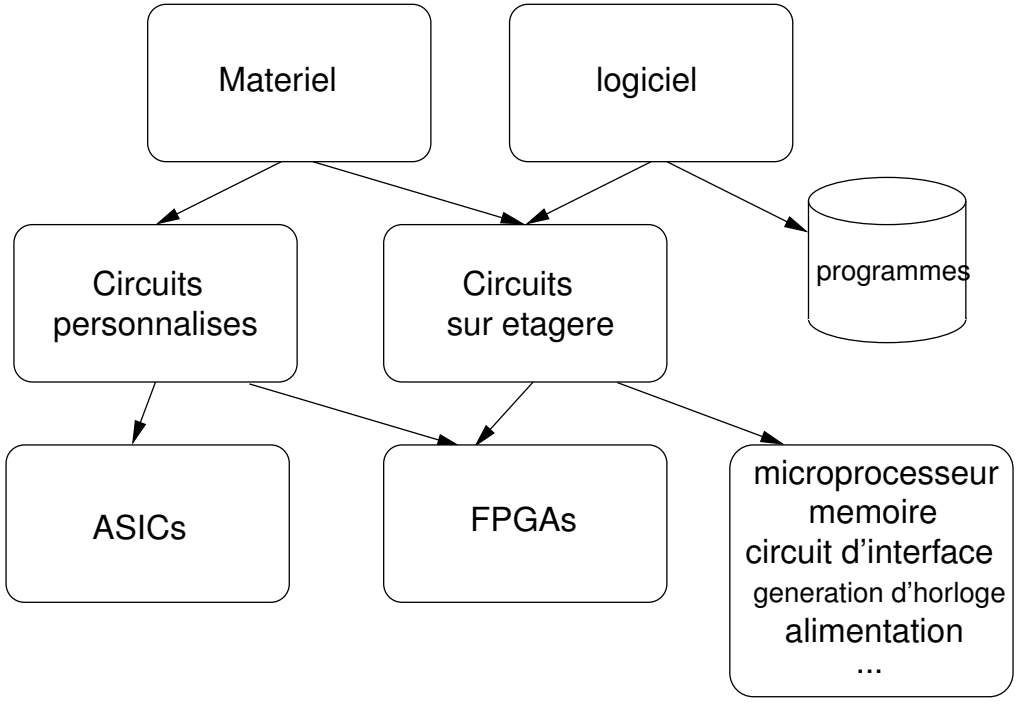


FIGURE : Architecture générale d'un traitement logiciel

Filières technologiques



...

FIGURE : Vue d'ensemble des filières

Choix des filières

	Logiciel	FPGA	ASIC
coût	celui du CPU	élevé	très faible si grand volume
tps dév.	très faible	faible	élevé
vitesse de calcul	faible	élevée	très élevée
consommation	élevée	moyenne	faible