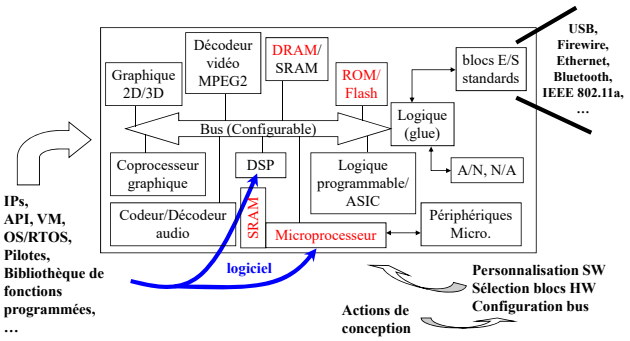
Architectures de processeurs et sécurité matérielle

Régis Leveugle
Grenoble INP – Phelma / TIMA
Regis.Leveugle@univ-grenoble-alpes.fr

Système électronique (intégré) moderne



Plan du cours – Partie 1 (Micro)processeurs

Méthodes de conception "avancées" - optimisation des "performances"

- "Performances" : définition, évaluation, principes généraux d'amélioration (systèmes numériques synchrones, mono-coeur)
  - Directions d'optimisation (puissance de calcul)
  - Principe de base d'une architecture pipeline
- Microprocesseurs et micro-parallélisme
  - Modèles d'exécution et évolution des architectures
  - Architectures RISC, Superscalaire, VLIW …
  - Parallélisme niveau processus/tâche (MT, SMT, …)
- Mémorisations et hiérarchie mémoire (Caches), MMU
- Macro-parallélisme (architectures multi-cœurs)
- Nouveau paradigme : calcul en mémoire

Lien architecture/logiciel de base : montré en filigrane …

Ouvrages de référence – Partie 1

- J. Hennessy, D. Patterson
  Computer architecture: a quantitative approach
  Morgan Kaufmann, 1996 (2nd edition) K01-HEN
- Idem, 5th edition, 2012
  Idem, 6th edition, 2019 - => cloud, réseaux de neurones ("machine/deep learning") …
- D. Patterson, J. Hennessy
  Organisation et conception des ordinateurs : l'interface matériel/logiciel
  Dunod, 1994 (version française) K01-PAT
- D. Patterson, J. Hennessy
  Computer organization and design: the hardware/software interface – RISC-V edition
  Morgan Kaufmann, 2018 K04-PAT
- Et autres … ex. H. Lilen, "Microprocesseurs : du CISC au RISC", Dunod, 1995 (K04-LIL)

Plan du cours – Partie 2 Sécurité - sensibilisation

Sécurité "matérielle" : menaces, évaluation – (Micro)processeurs, mais aussi ASIC, FPGA …

- Attaques matérielles : contexte général et évolutions, domaines concernés
- Circuits sécurisés : certification, critères communs
- Panorama des attaques matérielles usuelles
- Modélisation/Caractérisation des erreurs
- Autres types d'attaques
- Influence du style de conception

Défenses ("contre-mesures") : pistes montrées en filigrane …

Contenu global : 3 parties

- Architecture des (micro)processeurs (CM+TD)
- Sécurité matérielle – sensibilisation (CM)

  QCM (connaissances, synthèse, problème) + qq. réponses rédigées
  Page de notes personnelle manuscrite

  → DS 70%

- Travail en groupes
  (si 41 => 6 groupes de 6 + 1 groupe de 5 …)
  - Conception / optimisation d'un processeur RISC V
  - Différent de l'existant - approche recherche/innovation …

  → Rapport 30%

- Evaluation du cours : attention
  - Note DS : rattrapable en session 2
  - Note rapport pour travail en groupes : non rattrapable en session 2, modulée individuellement par les relevés de présence et la contribution personnelle (participation constructive – apport personnel dans le groupe)

Fonctionnement général

- CTD ou TD dédoublés ???? => CTD … (ne pas se fier à ADE)
- A vous de savoir être responsables et travailler régulièrement
- Les conseils généraux …
  - Arriver à l'heure
  - Ecouter / prendre des notes (le "poly" est un support, notamment pour les figures et éléments clé, pas un livre de cours exhaustif)
  - Travailler les notes (et les TD) entre deux cours consécutifs
  - Poser des questions sur les points restés flous (après avoir retravaillé …)

Travail en groupe : sujet global

- Conception et/ou optimisation d'un processeur RISC V : mise en pratique concrète des éléments abordés dans le cours + compléments ciblés sur la base d'une recherche bibliographique
- Possibilité de mettre l'accent sur l'architecture générale, ou sur une optimisation plus poussée de certains sous blocs
- Définition précise des objectifs par le groupe (proposition + discussion avec l'enseignant)

Notation + évaluation de 2 compétences (niveau 2 ?)

- Travail en groupes (organisation, gestion de projet, contribution personnelle …)
  Groupes au choix, mélanger les origines (inter-culturalité)
- Recherche et innovation
  - Etat de l'art – bibliographie
  - Réflexion / propositions - optimisation multi-critères : complexité, puissance de calcul, énergie (électronique durable), sécurité … => compromis et cibles des optimisations à choisir
  - Schéma d'architecture original (inspiration, oui – copier/coller, non)
  - Description détaillée des mécanismes implantés pour le jeu d'instructions visé dont gestion des aléas, accès mémoire …
  - Analyse / évaluations selon les différents critères – comparaison avec l'existant dans l'état de l'art (sans description RTL / synthèse vu le temps imparti)

Laissez parler votre imagination !
Et parlez en avec votre enseignant …

Travail en groupe : fonctionnement global

- Mise en œuvre d'un outil de gestion de projet ? Nomination d'un chef ou une cheffe de projet ? Dans tous les cas, planning avec répartition des tâches …
- Travail en séances (dont échanges) + participation en dehors
- Réparti sur les séances en fonction de l'avancement global (non planifié dans ADE)

  ⚠ Présence obligatoire, pénalité si absence non justifiée
- Rapport concis mais précis et argumenté reprenant toutes les étapes depuis l'analyse de l'état de l'art – évalué sur la pertinence, la justification des choix et l'originalité
  A rendre au plus tard au moment du DS (le rendre plus tôt est autorisé)
  + Evaluation individuelle des compétences acquises/démontrées
- 2022-2023 : 2 semaines entre la dernière séance et les DS

Evaluation des compétences (pas de note)

- Se référer aux présentations Phelma sur les preuves de compétences et la rédaction d'un rapport de preuves
- Points fondamentaux
  - Aller à l'essentiel (1/2 page à une page convaincante et personnelle par membre du groupe) ; les "traces" (conception, méthodologie, résultats) peuvent être partagées dans le groupe pour éviter les répétitions
  - Faire ressortir et argumenter l'exploitation (et/ou la recherche de complément) de vos connaissances, la justification des choix, ce qui a été mis en place pour contourner les difficultés (et ce qui a été facile à réaliser)
  - Analyser de manière critique la méthodologie et les résultats sur l'exemple particulier de l'étude et identifier ce qui est généralisable
  - Prise de recul : que feriez vous différemment sur les différents aspects si c'était à refaire (et pourquoi) ?

Entrainement (et base partielle) pour la preuve finale en 3A