RA2 - Mise en œuvre du Cortex-A9

Ce cours couvre les CPU ARM haut de gamme Cortex-A9, en versions mono-cœur et multicœur

Objectifs

- Ce cours se décompose en 3 parties importantes :
  - l'architecture du Cortex-A9(MP)
  - la mise en œuvre logicielle et le débogage du Cortex-A9(MP)
  - la mise en œuvre matérielle du Cortex-A9(MP)
- Le fonctionnement de la MMU sous Linux est décrit.
- La mise en œuvre d'un spin-lock dans un système multicœur est également détaillée
- L'interaction entre les caches de niveau 1, le cache de niveau 2 et la mémoire principale est étudiée au travers de séquences.
- Le mécanisme d'exception est expliqué, en indiquant comment la virtualisation permet la prise en charge de plusieurs systèmes d'exploitation.
- Une présentation de la spécification CoreSight est donnée avant la description des unités liées au débogage.
- Le cours décrit également la mise en œuvre matérielle et fournit des recommandations pour concevoir un SoC à base de Cortex-A9.
- La cohérence de cache est détaillée, y compris les miroirs de tags de cache, l'intérêt de connecter les canaux DMA à l'ACP et les séquences à utiliser pour modifier un descripteur de page.

Prérequis et cours associés

- Connaissance des ARM7/9 ou avoir suivi notre cours Fondamentaux ARM.
- Ce cours ne comporte pas de chapitres sur la programmation bas niveau.
- Cours associés :
  - Programmation VFP, cours RC0 - VFP programming
  - Programmation NEON, cours RC1 - Programmation NEON-v7

    .

Environnement du cours

- Cours théorique
  - Support PDF (en anglais), imprimé en présentiel ; à distance via Teams.
  - Assistance du formateur tout au long de la formation.
- Chaque session débute par un point avec les stagiaires.

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

Plan du cours

Premier jour

Introduction au Cortex-A9

- Variantes du Cortex-A9
- Nouveaux registres mappés en mémoire dans le MPCore
- Les 3 jeux d'instructions
- Options configurables

Bases de l'architecture ARM

- États et modes
- Intérêt du banking des registres
- Mécanisme d'exception
- Jeux d'instructions

Pipeline d'instructions

- Fonctionnement du pipeline superscalaire
- Mécanisme de prédiction de branchement
- Return stack
- Instructions prédites et non prédites

TrustZone

- Transitions autorisées de secure vers non secure
- Indicateurs d'état secure des L1 et L2, partitionnement de la mémoire
- Gestion des interruptions en présence de sources d'interruption à la fois secure et non-secure
- Séquence de démarrage

Introduction aux systèmes multicœurs

- AMP et SMP
- Séquence de démarrage
- Moniteur d'accès exclusif
- Mise en œuvre d'un spin-lock
- Utilisation des événements
- Concepts de base des RTOS supportant l'architecture SMP de l'A9

Deuxième jour

Thumb-2 instruction set (V7-A)

- Généralités sur la syntaxe
- Instructions de branchement et de contrôle de flux
- Instructions d'accès mémoire
- Instructions générant des exceptions
- Blocs conditionnels If&then
- Interworking entre les états ARM et Thumb
- Démonstration de séquences en assembleur destinées à comprendre ce nouveau jeu d'instructions

Unité de gestion mémoire

- Permissions d'accès aux pages, domaines et protection des pages
- Attributs de page, types de mémoire
- Utilisation des instructions de memory barrier
- Format de la table externe de descripteurs de pages
- Verrouillage du TLB
- Exception abort, mécanisme de pagination à la demande
- Opérations de maintenance de la MMU
- Utilisation d'une table de descripteurs de pages commune dans une plateforme SMP, maintien de la cohérence entre plusieurs TLB

Système mémoire de niveau 1

- Indexation virtuelle, tagging physique pour le cache d'instructions
- Opérations de maintenance supportées
- Allocation de cache write-back write allocate
- Instructions de memory hint PLD, PLI, PLDW, préchargement des données
- Description des transactions transitoires liées au cache : line fills et line eviction
- Store buffer 64 bits à 4 entrées avec fusion

Cohérence matérielle

- Principes de base du snooping : requêtes de snoop CLEAN, CLEAN & INVALIDATE et INVALIDATE
- Snoop Control Unit : transferts de cache à cache
- Machine d'états MOESI
- Compréhension, au travers de séquences, du maintien de la cohérence des données entre la mémoire L2 et les caches L1
- Accelerator Coherency Port

AMBA 3

- AXI
  - Topologie : connexion directe, multi-maître, multi-couche
  - Interconnect AXI PL301
  - Séparation des phases d'adresse/contrôle et de données
  - Canaux AXI, handshake de canal
  - Ordonnancement des transactions
  - Chronogrammes des bursts de lecture et d'écriture
  - Interface mémoire externe du Cortex-A9, codage des ID
- APB 3

Mise en œuvre matérielle

- Domaines d'horloge
- Domaines de reset
- Architecture Wait For Interrupt
- Attributs de l'interface maître AXI
- Cache L2 exclusif
- Informations sideband AXI

PL310 level 2 cache

- Caractéristiques de l'interface AXI
- Fonctionnement en mode exclusif
- Compréhension, au travers de séquences, de la copie des informations cacheables depuis la mémoire vers les caches de niveau 1 et de niveau 2

- Support de TrustZone
- Gestion de l'énergie
- Surveillance des événements du cache
- Description de chaque opération de maintenance
- Verrouillage du cache
- Gestion des interruptions

Moniteur de performance

- Comptage d'événements
- Choix de l'événement à compter pour les 6 compteurs
- Débogage d'un système multi-cœur à l'aide du PMU

Quatrième jour

Contrôleur d'interruptions

- Gestion des exceptions du Cortex-A9
- Virtualisation des interruptions
- Unité timer et watchdog intégrée dans le MPCore
- Groupes d'interruptions : STI, PPI, SPI, LSPI
- Mode legacy
- Priorisation des sources d'interruption
- Distribution des interruptions vers les cœurs Cortex-A9
- Détail de la séquence d'interruption
- Interruption parasite

Modes basse consommation

- Domaines de tension
- Contrôle de la consommation du Cortex-A9
- Communication avec le contrôleur de gestion d'énergie
- Registre SCU power status

CoreSight debug units

- Débogage invasif, débogage non invasif
- Interface de débogage APBv3
- Connexion au Debug Access Port
- Breakpoint et watchpoint liés au processus
- Échantillonnage du program counter
- Event catching
- Debug Communication Channel
- Interface PTM, connexion au funnel
- Description des registres de débogage
- Cross-Trigger Interface, débogage d'un SoC multi-cœur