RA4 - Mise en œuvre du Cortex-A7

Ce cours couvre le CPU ARM Cortex-A7

OBJECTIFS

- Ce cours se décompose en 3 parties importantes :
  - l'architecture du Cortex-A7(MP)
  - la mise en œuvre logicielle et le débogage du Cortex-A7(MP)
  - la mise en œuvre matérielle du Cortex-A7(MP).
- Une introduction au nouveau mode privilégié Hypervisor est donnée au début de ce cours.
- Les conséquences sur la traduction d'adresse sont ensuite expliquées, avec l'introduction de la traduction en 2 étapes.
- Le découplage de l'OS invité et du matériel à l'aide de déroutements vers l'Hypervisor est étudié.
- Le cours détaille également les nouvelles fonctions du Generic Interrupt Controller v2, en expliquant comment les requêtes d'interruption physiques peuvent être virtualisées.
- Le cours détaille la nouvelle approche concernant les timers / compteurs intégrés.
- Les nouvelles possibilités de l'AXI v4 sont mises en évidence par rapport à l'AXI v3.
- Au travers de séquences impliquant un Cortex-A15MP et un Cortex-A7MP, la cohérence matérielle est étudiée, en expliquant comment les requêtes de snoop peuvent être relayées par l'interconnect CCI-400.
- La mise en œuvre de l'I/O MMU-400 est également couverte.

PRÉREQUIS ET COURS ASSOCIÉS

- Plus de 12 bonnes réponses au questionnaire de prérequis Cortex-A.
- Cours associés :
  - Programmation avec l'IDE RVDS, référence cours RV0 - Programming with RVDS IDE
  - Programmation VFP, référence cours RC0 - VFP programming
  - Programmation NEON, référence 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

Présentation du Cortex-A7MP

- Architecture du Cortex-A7
- Organisation d'un SoC à base de Cortex-A7MP
- Possibilités de l'interconnect cohérent AMBA4
- I/O MMU
- Ligne de cache de 64 octets, cache L2 intégré
- VFPv4 et SIMDv2
- Jeux d'instructions supportés
- Mise en évidence des différences entre le Cortex-A9 et le Cortex-A7

Pipeline d'instructions

- Organisation globale, capacité de dual issue
- Étages fetch / decode / issue / writeback
- Unité de traitement de données
- Accélérateurs de branchement

Introduction à l'état hyperviseur

- Machine d'états des niveaux de privilège du processeur : user, OS invité, hypervisor
- Détail des différents modes de fonctionnement (Bare-Metal, noyau et tâche utilisateur de l'Hypervisor, Hypervisor avec partition invitée)
- Objectif de l'Hypervisor
- Support de l'imbrication des interruptions en mode Hypervisor
- Détection de l'utilisation de VFP/NEON par une partition invitée

Mécanisme d'exception

- Table des vecteurs de l'Hypervisor
- Utilisation du vecteur n°5 pour dérouter les événements d'une partition invitée
- Contrôle des bits Virtual Interrupt et Abort, contrôle du routage des IRQ, FIQ et external abort
- Prise d'exceptions en mode Hypervisor

GENERIC INTERRUPT CONTROLLER (GICv2)

- Intégration dans un SoC à base de Cortex-A15MP et de Cortex-A7MP
- Mise en évidence des nouvelles fonctions par rapport au Cortex-A9MP
- Aiguillage des interruptions vers l'OS invité ou l'Hypervisor
- Interface CPU virtuelle
- Fonctionnalité Split EOI
- Désactivation d'une source d'interruption depuis l'interface CPU virtuelle

Deuxième jour

Extensions de virtualisation

- Nouvelle Intermediate Physical Address, traduction d'adresse en 2 étapes
- Système de traduction mémoire
- Gestion de la mémoire en mode hypervisor

- Exposition de la MMU aux autres maîtres, IO MMU
- Support de l'émulation, déroutement des load et store et exécution en état Hypervisor
- Fonctions de sécurité supplémentaires

Large physical address extensions specification (lpae)

- Nouveau système à 3 niveaux
- Traduction d'adresse au niveau hypervisor
- Format des descripteurs de table de niveau 1
- Format des descripteurs de table de niveau 2
- Champs Attribute et Permission dans les tables de traduction
- Gestion de l'ASID dans le LPAE
- Nouvelles opérations de maintenance du cache et du TLB

Mise en œuvre de la MMU

- Organisation du TLB, L1-TLB, L2-TLB
- Table walk cohérent
- Fonctionnement du tablewalk cache et de l'IPA cache
- Détermination de la cause exacte des aborts au travers des registres d'état
- Comportement lorsque la MMU est désactivée
- Opérations de maintenance du TLB

OS support synchronization overview

- Interruptions inter-processeurs
- Barrières
- Cluster ID
- Moniteur d'accès exclusif, mise en œuvre de sémaphores booléens
- Moniteur global
- Mise en œuvre d'un spin-lock
- Utilisation des événements

Troisième jour

Sous-système de niveau 1

- Organisation du cache, cache d'instructions 2-way, cache de données 4-way
- Accès spéculatifs
- Hit Under Miss, Miss under Miss
- Mode read allocate
- Récupération du contenu des caches L1 au travers de registres CP15 dédiés
- États MOESI d'une ligne de cache de données
- Détail des opérations de maintenance du cache

Sous-système de niveau 2

- Cache L2 optionnel
- Mode read allocate
- Interface maître ACE
- Au moyen de séquences impliquant un Cortex-A7 multi-cœur et des maîtres externes, compréhension de l'utilisation des requêtes de snoop pour maintenir la cohérence des données entre les caches et la mémoire
- Primitives de synchronisation, les 3 niveaux de moniteurs

Generic timer

- Timers génériques ARM 64 bits pour chaque processeur

- Temps virtuel et temps physique
- Rôle de l'event stream
- Génération de l'event stream par le noyau
- Génération de l'event stream par l'Hypervisor

Extensions de virtualisation du moniteur de performance

- Surveillance des performances de l'Hypervisor
- Surveillance des performances de l'OS invité
- Réduction du nombre de compteurs disponibles pour un OS invité
- Virtualisation complète des registres d'identification du PMU

Quatrième jour

AMBA4

- AXI-4
- Protocole AXI-4 stream
- AXI-4 lite
- AXI Coherency Extension (ACE)
- Barrières exportées

Mise en œuvre matérielle

- Domaines d'horloge
- Resets, chronogramme du power-on reset
- Domaines d'alimentation
- Séquence de power-on reset, séquence de soft reset
- Gestion de l'énergie, WFI / WFE, mode dormant fondé sur la mémoire L2
- Interface avec la Power Management Unit
- Mise hors tension d'un CPU
- Débogage externe pendant la mise hors tension

CCI-400 cache coherent interconnect

- Transport des requêtes de snoop AMBA 4
- Connectivité et contrôle du snoop
- Interface maître ACE
- Connexion de 2 CPU au travers du CCI, gestion des domaines de cohérence
- Exemple d'un Cortex-A7 double cœur et d'un Cortex-A15 double cœur

CoreSight debug

- Program Trace Macrocell
- Cross Trigger Interface et Cross Trigger Matrix pour le débogage multi-processeur
- Ajout du Virtual Machine ID dans le critère utilisé pour poser un breakpoint / watchpoint