RA3 - Mise en œuvre du Cortex-A15

Ce cours couvre le CPU ARM haut de gamme Cortex-A15

OBJECTIFS

- Ce cours se décompose en 3 parties importantes :
  - l'architecture du Cortex-A15
  - la mise en œuvre logicielle et le débogage du Cortex-A15
  - la mise en œuvre matérielle du Cortex-A15.
- 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-A15 et un Cortex-A7, 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

- Connaissance du Cortex-A9.
- 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-A15MP

- Architecture du Cortex-A15
- Organisation d'un SoC à base de Cortex-A15MP
- Possibilités de l'interconnect cohérent AMBA4
- Attribut Inner Shareable et Outer Shareable
- I/O MMU
- Ligne de cache de 64 octets, cache L2 intégré
- VFPv4 et SIMDv2
- Mise en évidence des différences entre le Cortex-A9 et le Cortex-A15

Pipeline d'instructions

- Organisation globale, capacité de triple issue
- Étages fetch / decode / rename / dispatch
- Mode loop
- Clusters d'exécution
- Exécution out-of-order, file de dispatch à 40 entrées
- 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)
- Approche asymétrique, pas de support de la virtualisation des fonctions de l'état Secure
- Instructions SVC, HVC et SMC
- Objectif de l'Hypervisor
- Instructions et registres liés à l'Hypervisor
- Liste des registres à sauvegarder / restaurer pour pouvoir suspendre / reprendre une partition invitée
- Accès aux registres bankés ou à tout mode Non-Secure depuis le mode Hypervisor

Mécanisme d'exception

- Table des vecteurs de l'Hypervisor
- Utilisation du vecteur n°5 pour dérouter les événements d'une partition invitée
- Appel système vers le mode Hypervisor
- Exceptions asynchrones
- Contrôle des bits Virtual Interrupt et Abort, contrôle du routage des IRQ, FIQ et external abort
- Retour d'exception de l'Hypervisor
- 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

- Interface front-end accédée par le noyau invité
- Interface back-end accédée par l'Hypervisor

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
- Identification de machine virtuelle
- Exposition de la MMU aux autres maîtres, IO MMU
- Support de l'émulation, déroutement des load et store et exécution en état Hypervisor
- Permissions et attributs d'accès de la seconde étape

Large physical address extensions specification (lpae)

- Nécessité d'introduire le support d'une seconde étape de traduction dans le cadre des Virtualization Extensions
- Nouvelle traduction à 3 niveaux
- 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
- Amélioration de la mise en cache des entrées de traduction par des hints de contiguïté
- ensemble complet des hints d'allocation de cache
- 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
- Processus de correspondance du TLB
- Table walk cohérent
- Détermination de la cause exacte des aborts au travers des registres d'état
- Comportement lorsque la MMU est désactivée

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
- Indication de l'effet du multi-cœur sur les interfaces de débogage

Troisième jour

Sous-système de niveau 1

- Caches Physically Indexed Physically Tagged
- Algorithme de remplacement LRU, mise en œuvre avec un cache 2-way
- Accès spéculatifs
- Hit Under Miss, Miss under Miss
- Définition du seuil de write streaming
- Récupération du contenu des caches L1 au travers de registres CP15 dédiés
- États MESI d'une ligne de cache de données

Sous-système de niveau 2

- Organisation du cache
- Propriété d'inclusion strictement imposée avec les caches de données L1, simplification du snooping
- Protection ECC / parité optionnelle
- Impact des register slices sur les performances
- Moteur de préchargement du L2
- Préchargement des accès de table walk
- Interface maître ACE
- Interface esclave ACP
- Au moyen de séquences impliquant un Cortex-A15 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

Generic timer

- Timers génériques ARM 64 bits pour chaque processeur
- Temps virtuel et temps physique
- Effet de la virtualisation sur ces timers
- Rôle de l'event stream
- Génération de l'event stream par le noyau
- Génération de l'event stream par l'Hypervisor
- Schéma de distribution du timer en code de Gray

Extensions de virtualisation du moniteur de performance

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

Quatrième jour

AMBA4

- AXI-4
  - Signalisation de Quality of Service
  - Nouvelle signification de Read Allocate et Write Allocate
  - Bufferisation des transactions
- Protocole AXI-4 stream
  - Types d'octets : data, position, null
  - Flux d'octets
  - Flux creux
  - Fusion, packing et conversion de largeur des données
- AXI-4 lite
  - Longueur de burst de 1
  - Pas de support des accès exclusifs
- AXI Coherency Extension (ACE)
  - Shareability domains
  - Modèle de cohérence, états du cache
  - Signaux de canaux supplémentaires
  - Nouveaux canaux : snoop address, snoop response, snoop data
  - Étude, au travers de séquences, du traitement d'une requête de load et d'une requête de store lorsqu'elles sont marquées comme outer shareable
  - Utilisation des requêtes ReadUnique, CleanUnique et MakeUnique
  - Distributed Virtual Memory (DVM)

    - Message de synchronisation DVM
    - Choix de la machine d'états de cohérence : MESI ou MOESI selon les possibilités de l'interconnect
    - Filtrage du snoop
- Barrières exportées
    - DMB / DSB inner shareable, outer shareable ou system

Mise en œuvre matérielle

- Domaines d'horloge
- Resets, chronogramme du power-on reset
- Combinaisons de reset valides
- Domaines d'alimentation
- Séquence de power-on reset, séquence de soft reset
- Gestion de l'énergie
- Maintien de la cohérence pendant que les CPU sont en état standby
- 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
- Au moyen de séquences impliquant un Cortex-A15 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
- 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 Criss Trigger Matrix pour le débogage multi-processeur
- Ajout du Virtual Machine ID dans le critère utilisé pour poser un breakpoint / watchpoint
- Suivi des changements de VMID dans la sortie de trace