RA9 - Mise en œuvre du CORTEX-A73, architecture ARM V8

Ce cours couvre le Cortex-A73 et AARCH64

Objectifs

- Ce cours a pour but de mettre en évidence les nouvelles fonctionnalités offertes par l'architecture V8.
- Il a été conçu pour les ingénieurs développant du logiciel bas niveau et pour les ingénieurs chargés du hardening d'IP.
- Une présentation du Cortex-A73 est d'abord donnée, afin de mettre en évidence les différences entre une plateforme matérielle Cortex-A15/Cortex-A7 fondée sur le CCI-400 et une plateforme matérielle Cortex-A73/Cortex-A53 fondée sur le CCN-504.
- Le nouveau mécanisme d'exception est décrit.
- Les améliorations concernant le LPAE sont détaillées.
- Les nouvelles instructions assembleur A64 sont expliquées au travers d'exemples pratiques.
- L'AAPCS64 est également couvert.
- Le cours détaille aussi les nouvelles fonctions de débogage de l'ARM V8.
- La mise en œuvre matérielle du Cortex-A73 est expliquée, en particulier les états de basse consommation.

Prérequis et cours associés

- La connaissance d'un CPU ARM 32 bits est recommandée
- Voir également cours RI0 - AXI3 / AXI4 INTERCONNECTet cours RC1 - Programmation NEON-v7qui décrit l'architecture et le jeu d'instructions advanced SIMD (NEON)

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-A73

- Architecture du Cortex-A73
- Cohérence de cache intra-cluster
- Cohérence de cache inter-cluster via AXI4 ACE
- Port ACP
- Programmer’s model

Introduction à l'architecture ARM V8

- Améliorations par rapport à l'AArchv7
- Correspondance des registres entre A32/T32 et A64

- Correspondance entre les registres système AArch64 et les registres système AArch32

Exceptions ARMv8

- Quatre exception levels
- Exception Link Registers
- Banking des registres par exception level, fondé sur un nouveau modèle d'exception
- Imbrication au sein d'un même exception level
- Type d'exception et origine de l'exception
- Registres de syndrome fournissant une information d'état au gestionnaire d'exception
- Instruction de retour d'exception

Le modèle de sécurité de l'ARMV8-A

- Modèle de sécurité lorsque l'EL3 utilise AArch64
- Déroutement vers l'EL3 en AArch64

Interprocessing

- Gestion de deux types de processus, 64 bits et 32 bits, avec bascule lors d'une exception
- Organisation de l'espace non secure

Deuxième jour

Virtualisation

- Nouveau niveau de privilège hyperviseur côté non-secure
- Mode réentrant
- Gestion des exceptions de l'hyperviseur, déroutement
- Routage et contrôle des exceptions asynchrones

Pipeline d'instructions

- Fonctionnement superscalaire
- Instructions prédites et non prédites
- Accélérateurs de branchement
- Invalidation et changements de contexte
- Mise en évidence des différences avec le Cortex-A57

Multicore

- Synchronisation et sémaphores
- Attributs mémoire de shareability
- Fonctionnement du moniteur global
- Paire d'instructions Load acquire / Store release
- Utilisation des instructions WFE et SEV par les spin-locks
- Signalisation de requête et d'acquittement CLREXMON

Accès mémoire

- Support du mixed-endian
- Alignement du program counter et du stack pointer
- Contraintes d'ordonnancement
- Attributs de page : Normal ou Device
- Shareability et limitations d'accès sur les opérations de data barrier
- Memory barriers

Support de la MMU ARMv8

- Améliorations du LPAE pour s'adapter à AArch64
- Support de VA jusqu'à 48 bits par TTBR
- Vérification des permissions d'accès
- Support d'espaces IPA et PA jusqu'à 48 bits
- Système de traduction d'adresse VMSAv8-64
- Taille de granule de traduction mémoire
- Organisation de la table de descripteurs de pages, format des descripteurs
- Contrôle hiérarchique des accès mémoire Secure ou Non-secure
- Instructions de préchargement du TLB
- Instructions de maintenance du TLB en A64
- Mise en œuvre du TLB du Cortex-A73

Troisième jour

Caches

- Hiérarchie de caches, Point of Unification, Point of Coherency
- Instruction Load non temporal
- Instructions de maintenance des caches d'instructions et de données en A64
- Système mémoire L1 et L2 du Cortex-A73
- Vidage matériel du cache L2
- Choix de l'algorithme de remplacement du L2

Nouveau jeu d'instructions A64

- Langage d'assemblage A64, structure d'encodage binaire régulière
- Alias d'instructions
- Branchements, appel et retour de fonction
- Instructions de sélection conditionnelle, pour éviter les branchements
- Instructions Load Store, modes d'adressage
- Instructions arithmétiques et logiques, instructions de calcul de CRC
- Instructions d'accès aux registres de l'environnement d'exécution AArch32

ARM Architecture Procedure Call Standard 64-bit

- Convention générale d'utilisation des registres
- Stack pointer et frame pointer
- Convention d'utilisation des registres NEON / VFP

Unités NEON, VFP et cryptographiques

- Nouveau banking des registres pour NEON et VFP
- Correspondance des registres SIMD et flottants entre les états d'exécution
- Formats de vecteurs en état AArch64
- Nouvelles instructions SIMD
- Support logiciel de la cryptographie par une nouvelle famille d'instructions

GICv4

- Registres de l'interface CPU du Generic Interrupt Controller
- Virtualisation des interruptions
- Traitement des interruptions permettant l'imbrication

Quatrième jour

Generic Timer

- Fréquence d'horloge du system counter
- Registres de comptage des timers physique et virtuel
- Registres de comparaison en comptage, de valeur de décomptage et de contrôle du timer physique
- Registres de comparaison en comptage, de valeur de décomptage et de contrôle du timer virtuel

États de basse consommation

- Wait for Interrupt et Wait for Event
- Modes basse consommation du Cortex-A73
- L2 Wait for Interrupt
- Rétention dynamique du processeur
- Support de la gestion d'énergie avec plusieurs domaines d'alimentation
- Mode dormant
- Rétention dynamique du processeur
- Rétention dynamique des RAM du L2
- Interface Q-channel du cœur

Débogage ARMv8

- Débogage self-hosted
- Instructions de l'état de débogage
- Comparaisons chaînées pour la génération d'exceptions Breakpoint/Watchpoint
- Exceptions Software Step
- Routage des exceptions de débogage
- Débogage externe, cross-triggering
- Architecture Embedded Trace Macrocell

Performance Monitor

- Surveillance des performances par fonction au niveau EL0
- Effet de l'EL3 et de l'EL2 sur le Performance Monitor
- Filtrage des événements

Mise en œuvre matérielle du Cortex-A73

- Horloges
- Resets