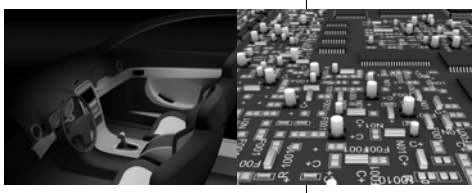
Mécanismes de protection dans AUTOSAR OS

Nicolas Navet, RTaW
Hervé Perrault, PSA Peugeot Citroën



Conférence à RTS'09
le 31/03/2009

PSA PEUGEOT CITROËN

RTaW
RealTime-at-Work

Plan

1. Code ECU : besoin de ré-utilisabilité et multi-source
2. Concepts de base de la protection OS
3. Mécanismes de protection mémoire et implication sur l'ordonnancement ECU
4. Mécanismes de protection temporelle
5. Mécanismes de protection du service
6. Possibilités, limites et perspectives

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Objectif central de AUTOSAR : code multi-source ré-utilisable

- Situation typique pré-AUTOSAR: l'intégrateur fournit 100% du code d'un ECU …
- Difficultés pour l'OEM:
  - Intégrer du code « maison » ou du code tiers
  - Ré-utiliser du code applicatif et ses paramètres de (pré-) calibration
  - Faire jouer la concurrence sur le meilleur ratio perf / qualité / cout sur des modules ciblés
  - Engagement en responsabilité délicat si code multi-source..
  - …

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Mécanismes de protection OS: services de partitionnement mémoire / temporel

- Bénéfices:
  - Non interférence des applications entre elles et confinement des erreurs
  - Phase mise au point et véhicule série
  - Sécurise l'intégrateur et facilite le partage des responsabilités
  - Ré-utilisabilité et multi-source ⇨ ↘ coûts et ↗ qualité par effet levier de la transversalité des modules
  - Services standardisés (hors champ compétitif):
    - référentiel commun
    - économie d'échelle et qualité des implémentations grâce au partage entre OEMs (notamment BSW)

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Ré-utilisabilité du code…

- ☺ L'unicité des exigences, notamment en conception « Model based », permet également de réutiliser des paramètres de (pré)calibration
- ☺ Les composants logiciels conservent leur certification ASIL
- ☹ Difficile si architectures fonctionnelles très dissemblables (☺ WP10.x AUTOSAR)
- ☹ Nécessité de « contrats » sur la disponibilité des ressources ?!

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Peu de choses avant AUTOSAR …

- OSEK/OS : « OSEK OS does not provide sufficient support for isolating multi-source components at runtime »
- OSEKTime et HIS : « immature specifications that contain concepts necessary for AUTOSAR »
- AUTOSAR OS = OSEK/VDX +
  - tables d'ordonnancement statiques « switchables »
  - mécanismes de protection
  - concept de code / OS-application « trusted/non-trusted »
  - …

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

La réponse AUTOSAR

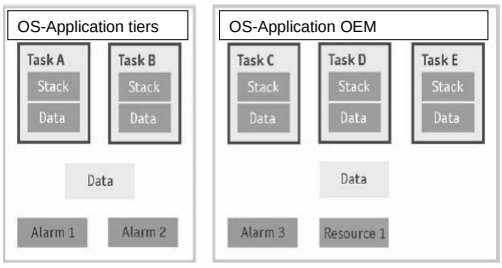
- Problèmes potentiels : confiscation de ressources (CPU, ressources partagées, mémoire, drivers monopolisé), accès/appels non autorisés
- 5 types de mécanismes
  - protection mémoire
  - protection temporelle
  - protection des services OS
  - protection des ressources matérielles
  - code trusted / non-trusted
- Déclinés en 4 classes de « scalabilité »

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection OS: exécuter des applications multi-sources sur un même ECU

OS-applications: unités fonctionnelles composées d'objet-OS (tâches, tables d'ordonnancement, etc)

Portée de la protection:
✓ OS-applications ⇨ oui
✓ tâches OS ⇨ oui
✓ runnables ⇨ non
✓ ISR 1 ⇨ non
✓ ISR 2 ⇨ oui



PSA PEUGEOT CITROËN RTaW RealTime-at-Work

OS-applications trusted vs non-trusted

- Besoin? Modules dont on veut limiter les capacités d'accès aux ressources – pour d'autres impossible
- Trusted OS-applications:
  - Exécution sans mécanismes de monitoring / protection possible et en mode CPU superviseur
  - Accès complet à la mémoire et à l'API de l'OS
  - Possibilité d'exporter des « trusted functions » exécutées en mode superviseur
- Non-trusted OS-applications:
  - Protection / monitoring imposés
  - Pas d'exécution en mode superviseur
  - Possibilité d'accéder à des objets distants « non-trusted » si spécifié à la configuration

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Comportement en situation d'erreur

- Appel à protectionHook() définie globalement par l'intégrateur – possibilités:
  - ✓ terminer la tâche
  - ✓ terminer l'OS-application (restart optionnel)
  - ✓ rebooter l'ECU
  - ✓ ne rien faire
- protectionHook() peut appeler errorHook() spécifique à l'OS-application:
  - ✓ traçabilité
  - ✓ traitement de l'erreur spécifique

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection mémoire
Protection de la pile
Protection SC3 et SC4
Protection temporelle
Protection du service

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection mémoire – surveillance de la pile

- Détection d'un usage « excessif » de la pile par une tâche,
- Mécanisme « best-effort » sans nécessité d'une MPU,
- Uniquement lors des changements de contexte ⇨ détection peu « fiable » et différée (post-erreur)
- Intérêt pour SC1 & SC2 – pb détecté par « stack overflow » pour SC3 & SC4

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection mémoire – SC3 & SC4

- Principe:
  - protection en écriture imposée – lecture et exécution optionnelle
  - ne concerne que les OS-applications non-trusted
- Pile : propriété d'une tâche ou OS-application
- Données : propriétés d'une tâche ou OS-application
- Code : propriété d'une OS-application ou partagé (attention si bug dans une librairie partagée!)
- Périphériques : propriétés d'une OS-application

Protection mémoire – support hardware pour SC3 & SC4

- CPU : mode superviseur et user
- Memory Protection Unit (MPU) : partition de l'espace d'adressage avec attributs de protection individuels
- Disponibilités : SX12E, MPC5510 (Freescale), XC3200 (Infineon), MB91460 (Fujitsu), V850 (NEC), …
- Problème : mécanismes OS génériques, nivellement par le bas ..

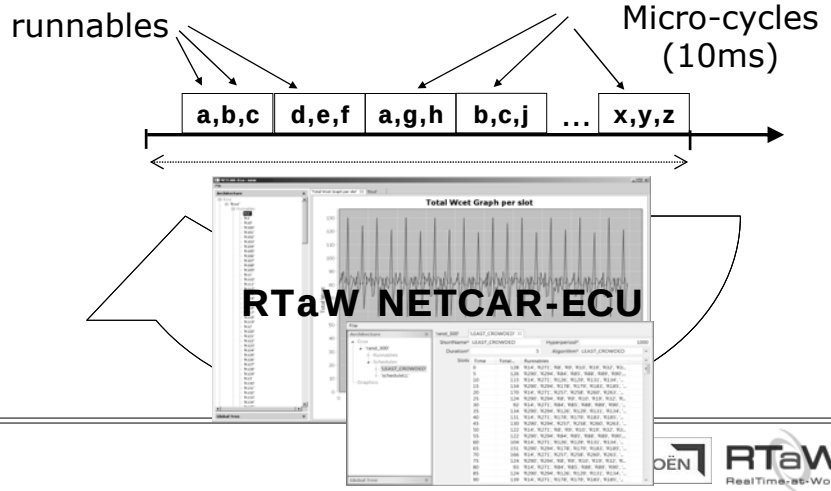
Protection mémoire – bénéfices attendus

- Cloisonnement de modules applicatifs distincts :
  1. dans des OS-applications ≠ mais seulement 2 OS-applications requis par le standard ☹
  2. dans des tâches ≠ mais peu de protection sur les OS-objets de l'OS-application (ex. alarmes, tables d'ordonnancement, compteurs, ressources)
- Mise au point (puis portage sur SC1 ou SC2 ?)

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection mémoire – exemple d'impact sur l'ordonnancement (1/2)

- Exemple typique sans protection, tous les runnables applicatifs ordonnancés dans une même tâche OS



RTaW RealTime-at-Work

Protection mémoire – Exemple d'impact sur l'ordonnancement (2/2)

- Protection mémoire ⇨ tâches distinctes
- Questions:
  1. comment regrouper les runnables en ≠ tâches?
  2. comment prioriser les tâches?
- Contraintes:
  - ✓ nombre de tâches limité (8, 16)
  - ✓ runnables dans des tâches != avec contraintes de temps fortes
  - ✓ les priorités sont fixes

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection mémoire
Protection temporelle
Protection du service

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection temporelle vue d'ensemble

- Dépassement d'échéances dues:
  - ✓ Temps d'exécution trop élevés ⇨ execution time budget
  - ✓ Temps de blocage ⇨ locking time protection
  - ✓ Inter-arrivées trop fréquentes ⇨ inter-arrival time protection
- Mais …
  - ✓ SC4 uniquement / obligatoire mais peut-être « bypassée »
  - ✓ Pas de deadline monitoring

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection temporelle contrôle des temps de blocage

- Temps max. de possession des interruptions / ressources
- Individualisable par tâche et par ressource
- Mais ..
  - pas de contrôle sur le nombre de fois où la ressource est prise …

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection temporelle
contrôle du temps d'exécution

- Pire temps d'exécution (WCET) défini statiquement à la conception
- Remise à zéro du compteur :
  - Passage dans l'état « suspended »
  - Passage dans l'état « waiting » (ECCx)

➢ Question : applicabilité dans le cas où une attente est nécessaire dans le corps de la tâche ?

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection temporelle
Inter-arrival time protection

- Pour une tâche : paramètre *Time Frame* spécifie une borne inf. entre deux transitions vers l'état *ready*
- Pour un ISR : temps minimum entre deux appels

➢ Adapté pour des tâches périodiques / sporadiques simples

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection mémoire
Protection temporelle
Protection du service

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection du service

- Bloquer les appels systèmes incorrects:
  - Arguments invalides
  - Services appelés dans un contexte invalide (ex: *terminateTask()* dans ISR)
  - Insuffisance de droits pour un service (ex: *shutdownOS()*)
  - Insuffisance de droits pour une ressource

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

La réponse AUTOSAR en résumé ..

	Classe de scalabilité 1 (SC1)	Classe de scalabilité 2 (SC2)	Classe de scalabilité 3 (SC3)	Classe de scalabilité 4 (SC4)
Protection temporelle				✓
Protection mémoire			✓	✓
Stack monitoring	✓	✓	✓	✓
Protection hook		✓	✓	✓
OS-applications			✓	✓
Protection des services			✓	✓
Appel de functions « trusted »			✓	✓

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection dans AUTOSAR OS conclusions (1/2)

- Mécanismes puissants pour:
  - Contrôle mémoire
  - Éviter utilisation excessive CPU
  - Garantir intégrité du système
- Il est souvent possible de contourner les protections
- Aucune protection contre des défaillances hardware
- Quid des ISR1 ?

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Protection dans AUTOSAR OS conclusions (2/2)

- Limites:
  - seulement 2 OS-applications
  - pas de bibliothèques de fonctions « non-trusted » (?)
  - protection temporelle pour les tâches étendues
  - Autres composants AUTOSAR en retrait (ex: RTE 3.1)
- Perspectives consortium: extension au multi-processeur / multi-core
- Perspectives fondeurs : standardiser les mécanismes on-chip ou la façon de les utiliser
- Perspectives OEM :
  - modification importante de la façon d'acheter/produire du logiciel (logiciel transversaux)
  - Diminution de l'effort nécessaire pour arriver à l'inocuité ..
- Perspectives fournisseurs de code : faciliter la mise au point et la prise de responsabilité.

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Bibliographie (1/2)

[1] AUTOSAR Consortium, "Specification of Operating System", V3.0.3, R3.1 Rev 0001, 2008.

[2] AUTOSAR Consortium, "Requirements on Operating System", V2.0.5, R3.1 Rev 0001, 2008.

[3] AUTOSAR Consortium, "Specification of RTE", V2.0.1, R3.1 Rev 0001, 2008.

[4] D. Lohmann, J. Streicher, W. Hofer, O. Spinczyk, W. Shröder-Preikschat, "Configurable memory protection by aspects", Proceedings of the 4th workshop on Programming languages and operating systems, 2007.

[5] Fujitsu,"AUTOSAR Package for Fujitsu automotive microcontrollers – description of the MB91460 Series (32-bit)", Février 2007.

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

Bibliographie (2/2)

[6] "Infineon rolls Autosar compliant microcontroller family", EETimes Europe, http://eetimes.eu/germany/197800861, Juillet 2007.

[7] Martin Markert (Freescale), "Multiple applications in control units - AUTOSAR-OS allows multiple applications to run on one microcontroller by the use of memory protection", http://www.elektroniknet.de, 2008.

[8] Peter Liebscher (Vector Informatik), "Timing, memory protection and error detection in OSEK Systems", Embedded Control Europe, pp 41-44, June 2006.

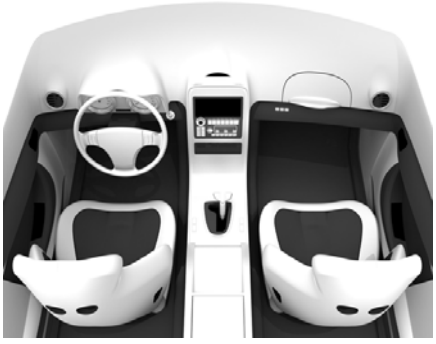
[9] DaimlerChrysler AG, "OSEK OS Extensions for Protected Applications", Juillet 2003. Available at http://www.automotive-his.de/

[10] OSEK/VDX, "Time-Triggered Operating System - Specification 1.0", Juillet 2001.

PSA PEUGEOT CITROËN RTaW RealTime-at-Work

nicolas.navet@realtimeatwork.com

http://www.realtimeatwork.com



STAND A7

PSA PEUGEOT CITROËN RTaW RealTime-at-Work