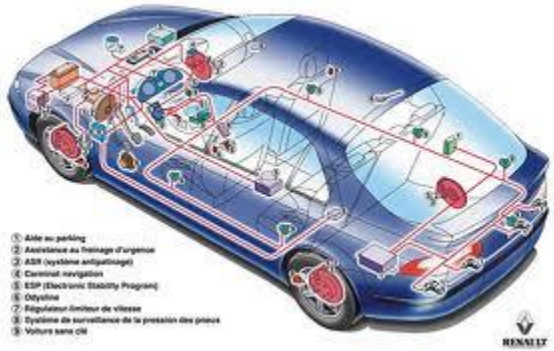
Pascal Cotret
UBS, Lorient
11 décembre 2012

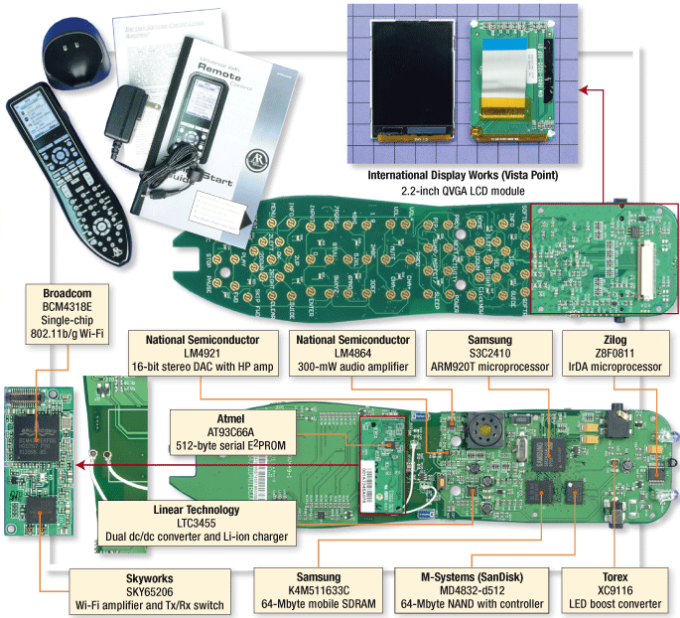
Protection des architectures hétérogènes multiprocesseurs dans les systèmes embarqués

Une approche décentralisée basée sur des pare-feux matériels

Systèmes embarqués et sécurité

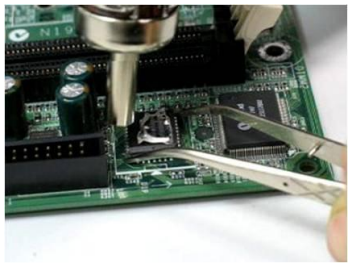
- Consommation.
- Performances.
- Coûts de développement.
- Circuits complexes.





Systèmes embarqués et sécurité

- Données confidentielles utilisateur.
- Configuration du système.

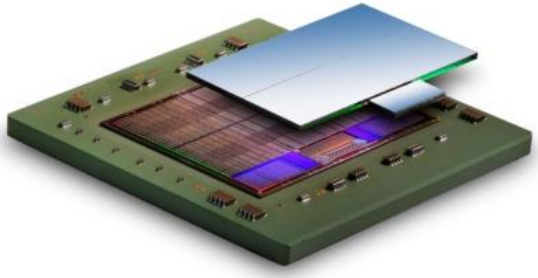


- Clonage ou contrefaçon de circuit.
- Extraction de données.

- Sécurité et systèmes embarqués :
  - Mobiles, budget dédié : 330M€ (2012) => 1450M€ (2017).
  - Académique : nombreuses conférences et publications.

ICT Procurement / ABI Research report, 2012.

La technologie FPGA



- Programmable et reprogrammable (contrairement aux circuits ASICs).
- Prototypage.
- Ressources limitées.

Projet ANR SecReSoC

- Partenaires académiques et industriels :

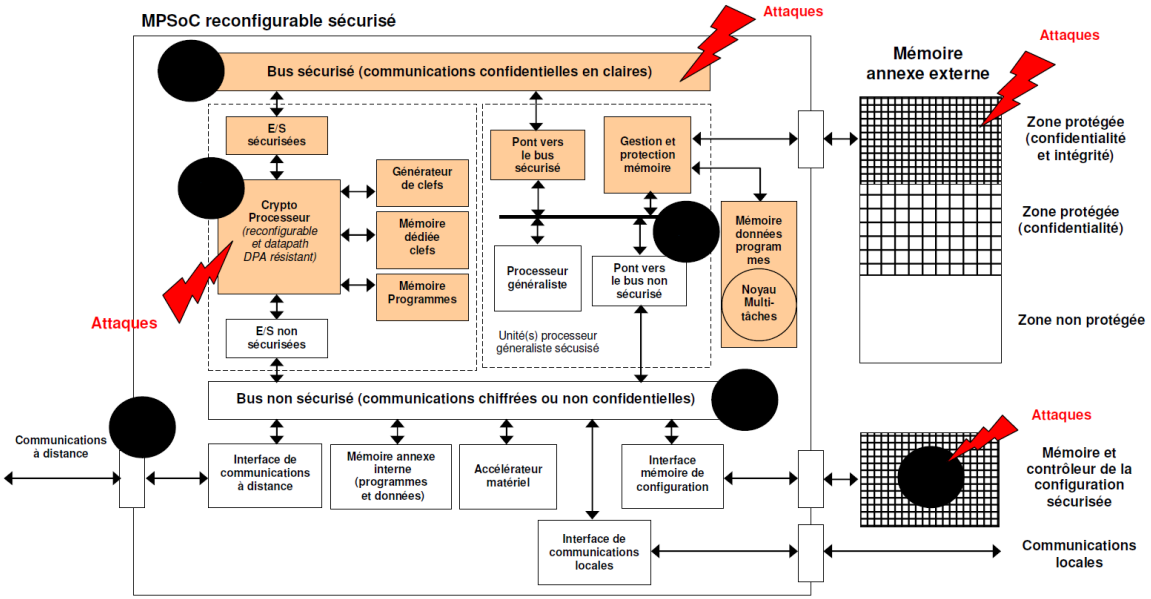
Lab-STICC

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM

LABORATOIRE Hubert CURIEN
UMR • CNRS • 5516 • ST-ETIENNE

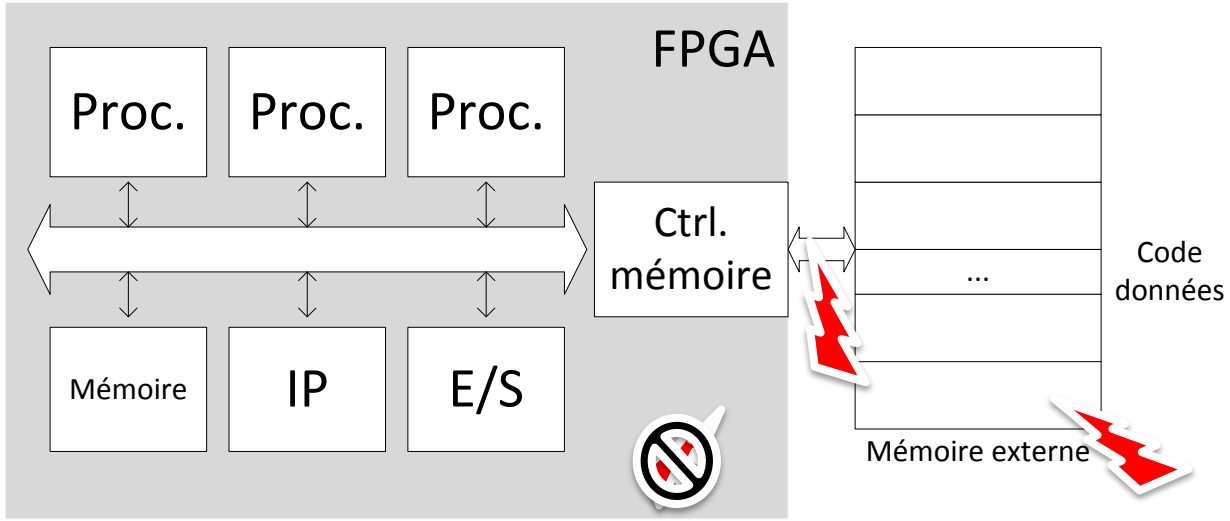
TELECOM ParisTech

Netheos
CONFIDENTIALITÉ & SÛRETÉ NUMÉRIQUE

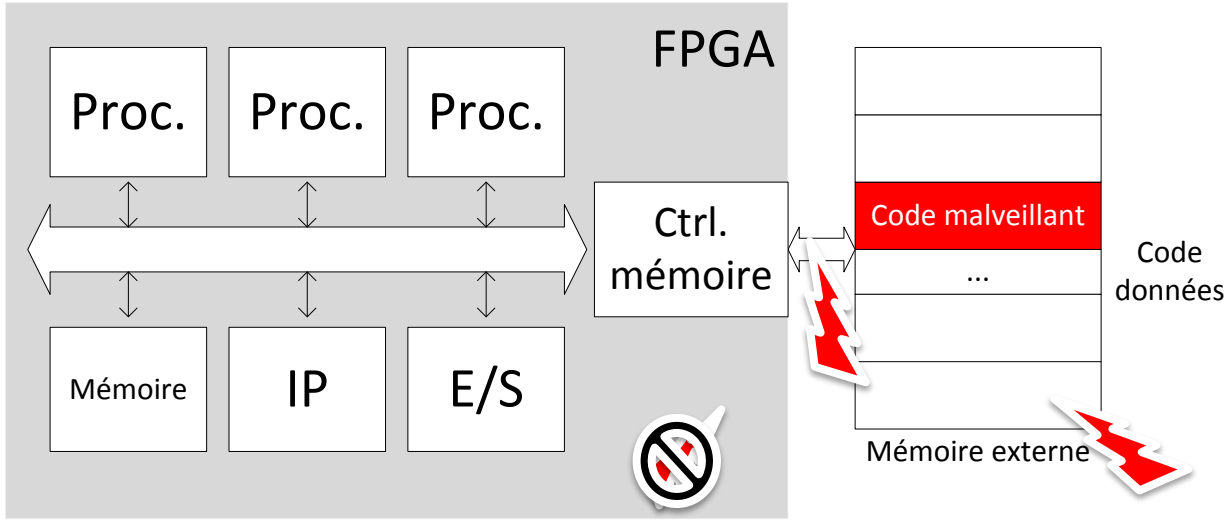


- Boot/Bitstream (LIRMM).
- Cryptoprocesseur (LaHC).
- Contre-mesures DPA (Télécom Paris).
- Protection comms & mémoires (Lab-STICC).

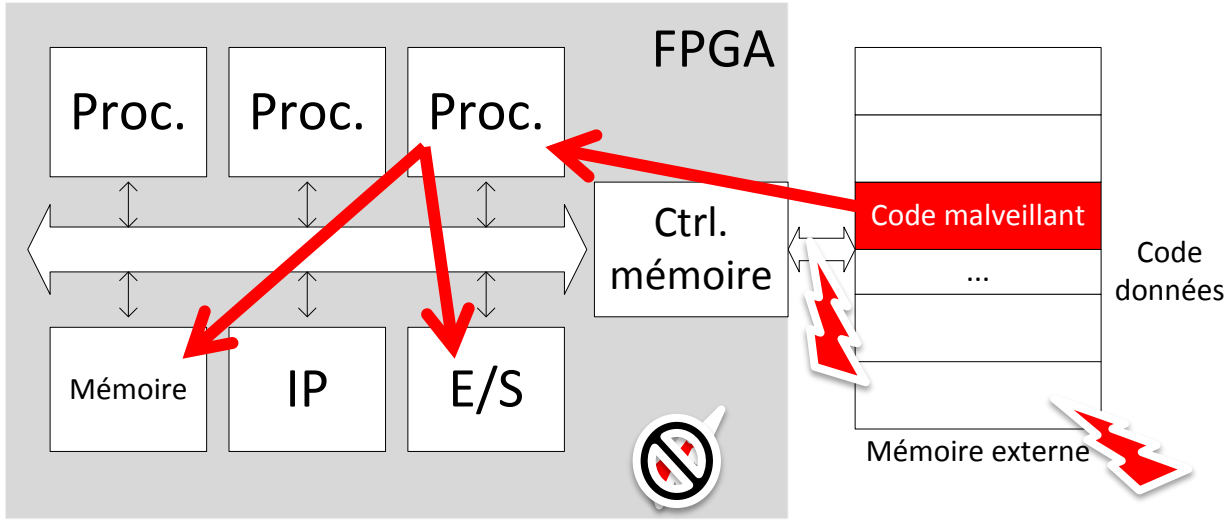
Les architectures multiprocesseurs



Les architectures multiprocesseurs



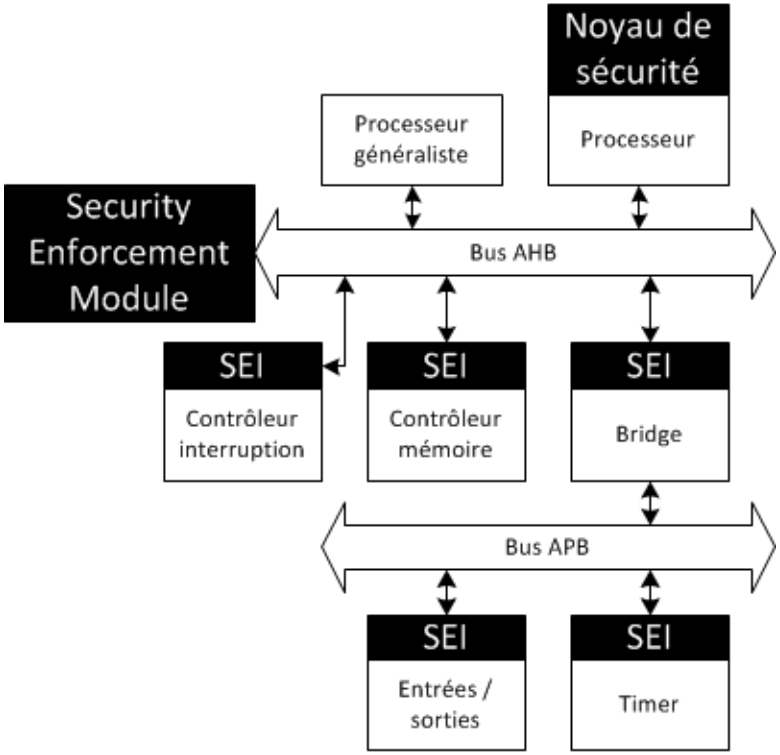
Les architectures multiprocesseurs



- Bus externe.
- Mémoire externe.
- Communications internes.

Protections des communications

Communications par un système de bus :

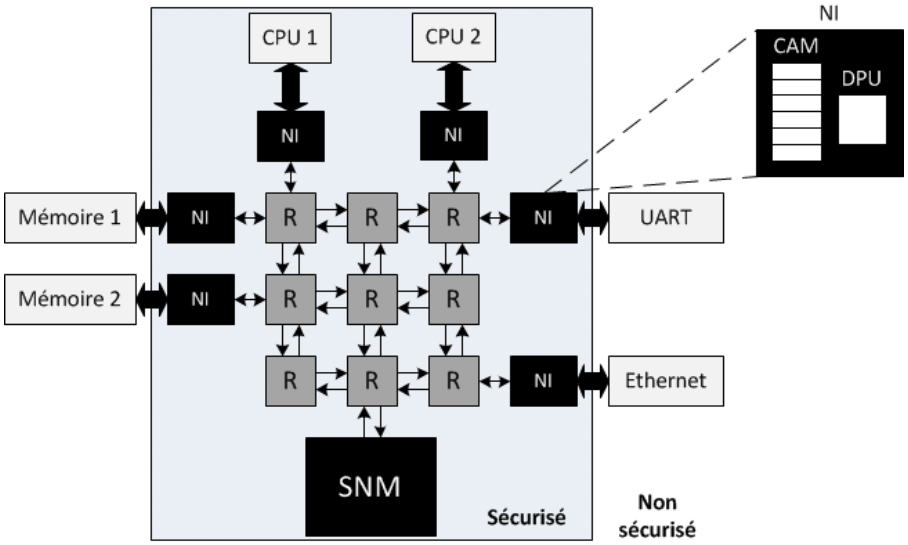


- Modèle de menace.
  - Accès aux bus internes du circuit.
- Contrôles.
  - Centralisés dans le SEM.
- Mise à jour.
  - Noyau de sécurité fixe.
- Fonctions cryptographiques.
  - Pas de chiffrement proposé.

[Coburn 2005] J. Coburn, S. Ravi, A. Raghunathan et S. Chakradhar. *SECA : Security-Enhanced Communication Architecture*. CASES 2005.

Protections des communications

Communications par un réseau sur puce :



- Modèle de menace.
  - Mémoire externe et bus externe.
- Contrôles.
  - Distribué.
- Mise à jour.
  - Modification des CAM.
- Fonctions cryptographiques.
  - Pas de chiffrement proposé.

[Fiorin 2008] L. Fiorin, G. Palermo, C. Silvano. *A security monitoring for NoCs*. CODES+ISSS 2008.

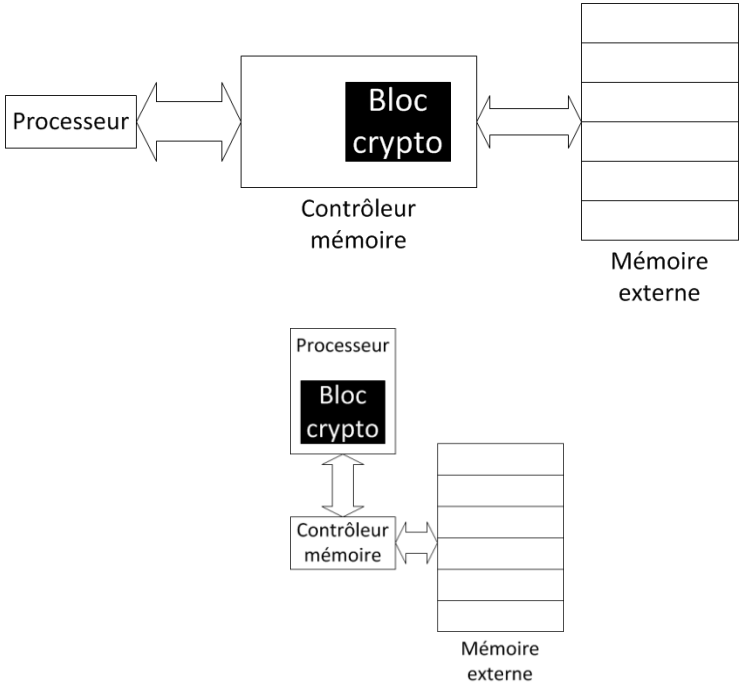
Protection des communications

	[Coburn 2005]	[Fiorin 2008]	Notre solution
Paramètres quantitatifs			
Surface	6,6 %	21 %	
Latence	< 1%	N/A	Objectif principal
Occupation mémoire	N/A	N/A	N/A
Paramètres qualitatifs			
Protocole communication	Bus (AHB-APB)	NoC	Bus (AXI-4)
Granularité	IP	IP	IP (extensible tâche)
Modèle de menaces	Bus	Mémoire + bus ext.	Mémoire + bus ext.
Mise à jour	Non	Oui	Oui
Fonctions cryptographiques	Non	Non	Oui

Protection des mémoires externes

Utilisation de primitives cryptographiques.

- Modification du contrôleur mémoire :
  - XOM (eXecute-Only Memory [Lie 2003]).
  - PE-ICE (Parallel Encryption-Integrity Checking Engine [Elbaz 2006]).
  - AES-TAC (Time Address Cipher [Vaslin 2008]).
  - HSC (Hardware Security Core [Crenne 2011]).
- Intégration d'un processeur dédié :
  - AEGIS (A Single-Chip Secure Processor [Suh 2005]).



[Lie 2003] D. Lie, C. Thekkath, M. Horowitz. *Implementing an untrusted operating system on trusted hardware*. SOSP 2003.

[Elbaz 2006] R. Elbaz, L. Torres, G. Sassatelli, P. Guillemelin, M. Bardouillet, A. Martinez. *A parallelized way to provide data encryption and integrity checking on a processor-memory bus*. DAC 2006.

[Vaslin 2008] R. Vaslin, G. Gogniat, J-P. Diguet, R. Tessier, D. Unnikrishan, K. Gaj. *Memory security management for reconfigurable embedded systems*. FPT 2008.

[Crenne 2011] J. Crenne. *Sécurité haut-débit pour les systèmes embarqués*. Thèse 2011.

[Suh 2005] G.E. Suh. *AEGIS : A single-Chip Secure Processor*. Information Security Technical Report 2005.

Cahier des charges de la solution

- Compromis des solutions existantes.
- Faible latence <= objectif principal
  - Communications en ordre (pas de perturbations).

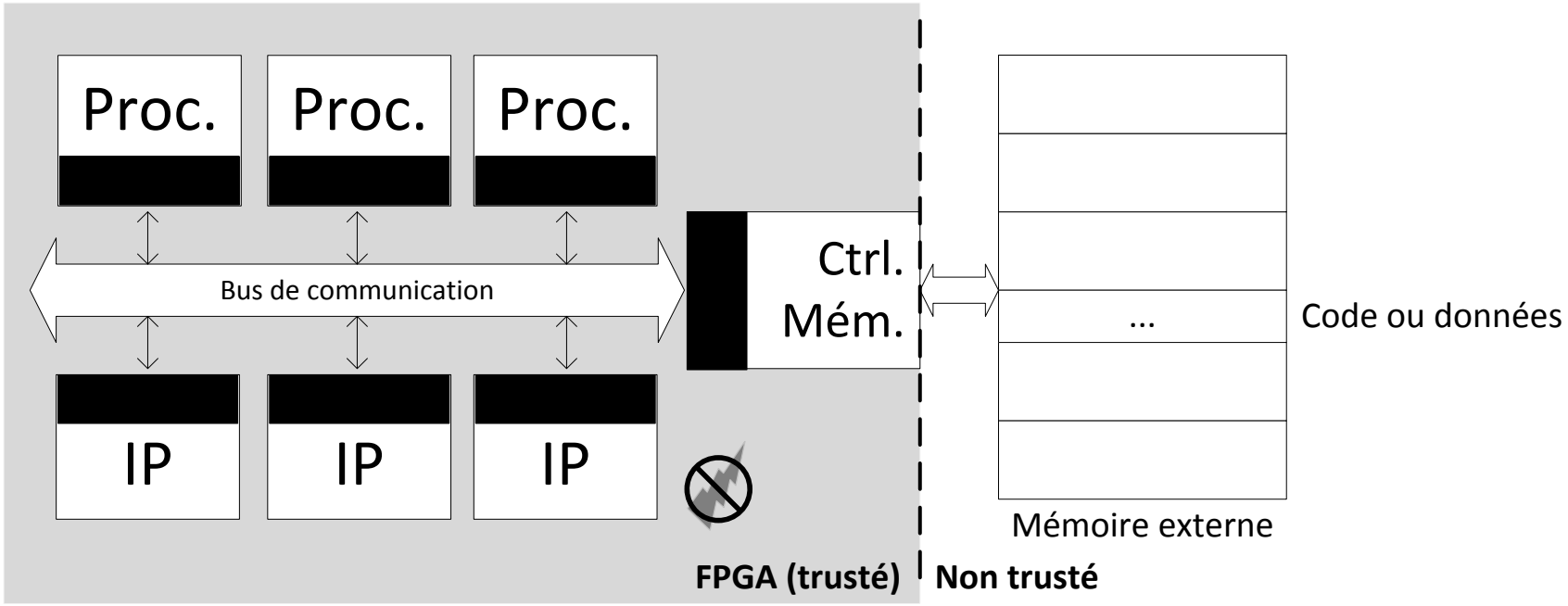
- Impact ressources du FPGA.
- Adaptivité, « reconfiguration » :
  - Mise à jour des services de sécurité.
  - Pas de fuites de données malveillantes.

Plan

- Solution de sécurité statique
- Mise à jour en temps réel
- Conclusion
- Perspectives

Solution de sécurité statique

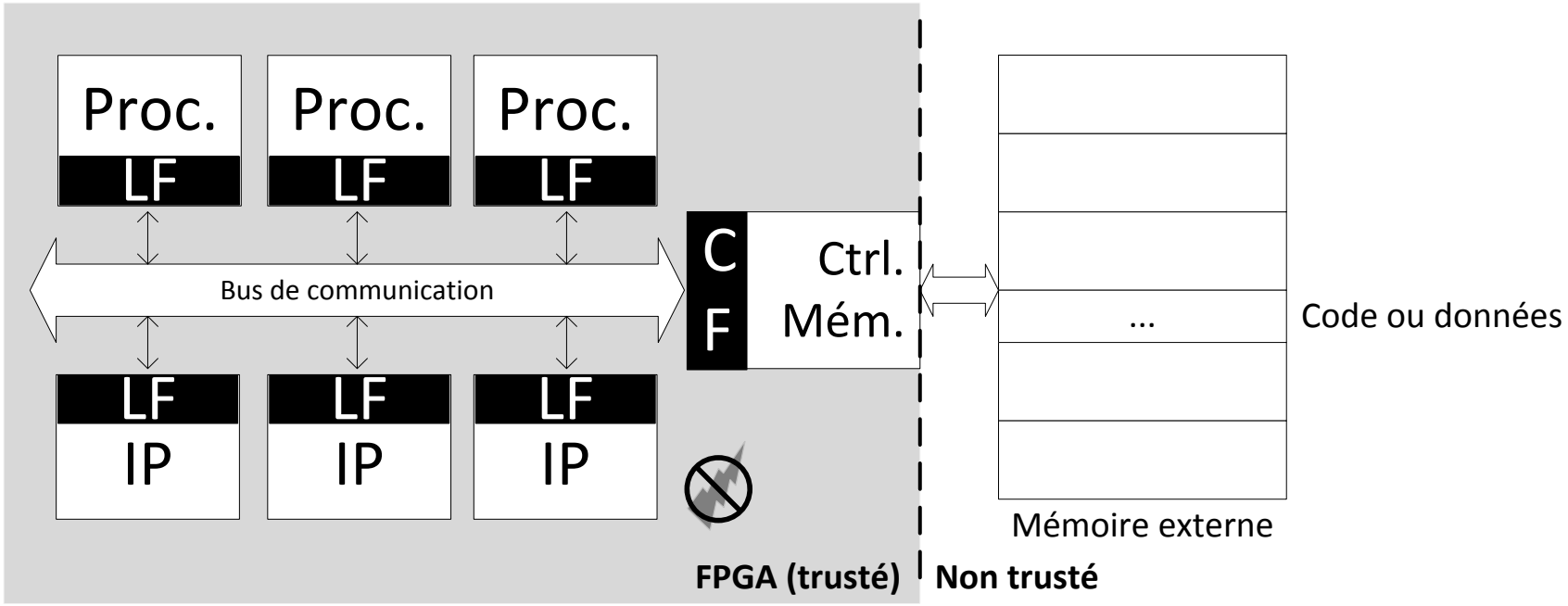
Pare-feux matériels



- Mécanismes de sécurité => pare-feux (ou « firewalls »).
- Protection contre le modèle de menace.
- Faible latence des mécanismes.
- Mise à jour des règles.

Solution de sécurité statique

Pare-feux matériels



- Local Firewalls (LF) :
  - Protection des zones mémoires en clair.
- Cryptographic Firewall (CF) :
  - Fonctions cryptographiques associées à la mémoire externe.

Solution de sécurité statique

Les différents types de menaces

Pas d'accès illégaux

Protection données
Interdiction modification
Contenus illisibles

Solution de sécurité statique

Les différents types de menaces

Pas d'accès illégaux

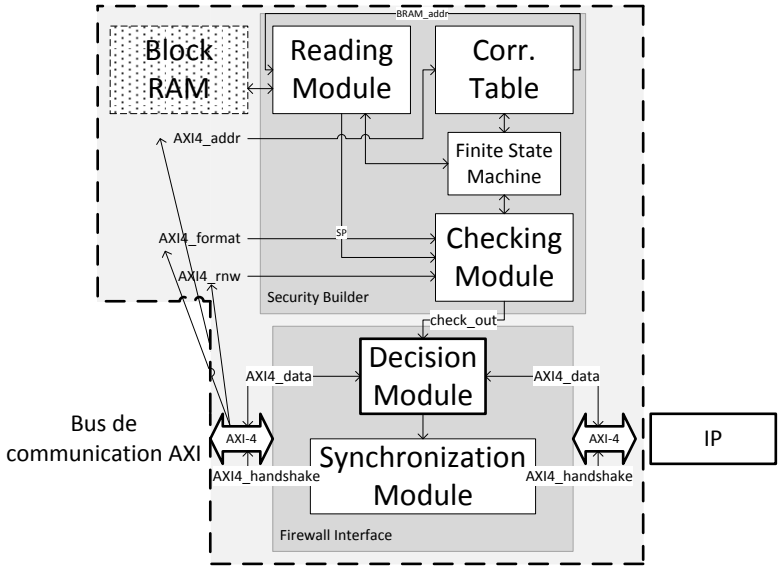
- Droits lecture-écriture.
- Filtrage espaces d'adresses.
- Format des données.

Protection données
Interdiction modification
Contenus illisibles

- Confidentialité.
- Intégrité.

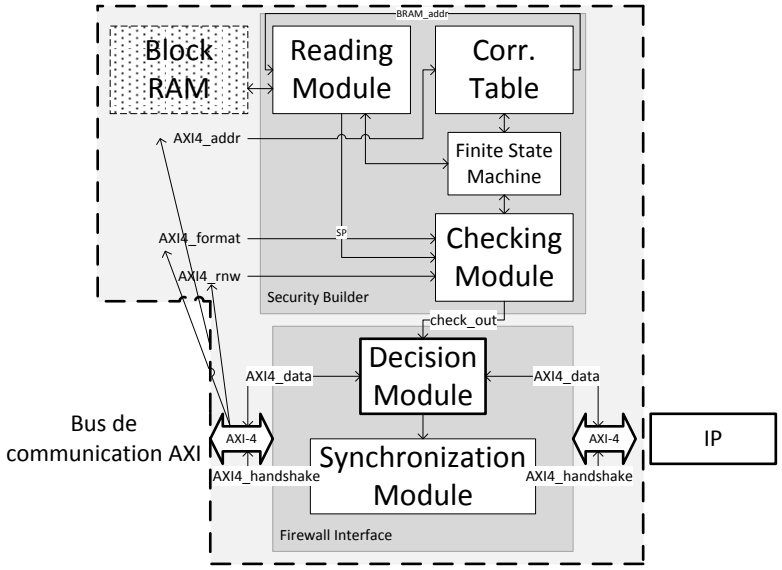
Solution de sécurité statique

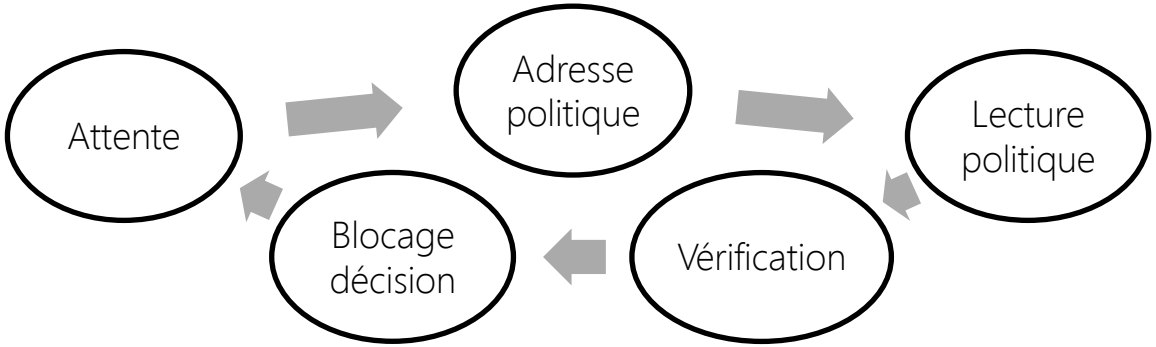
Local Firewall



Solution de sécurité statique

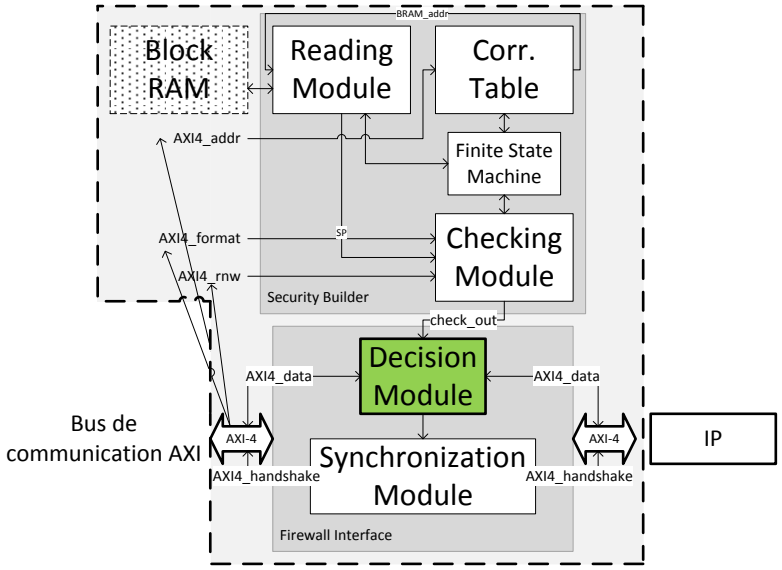
Local Firewall

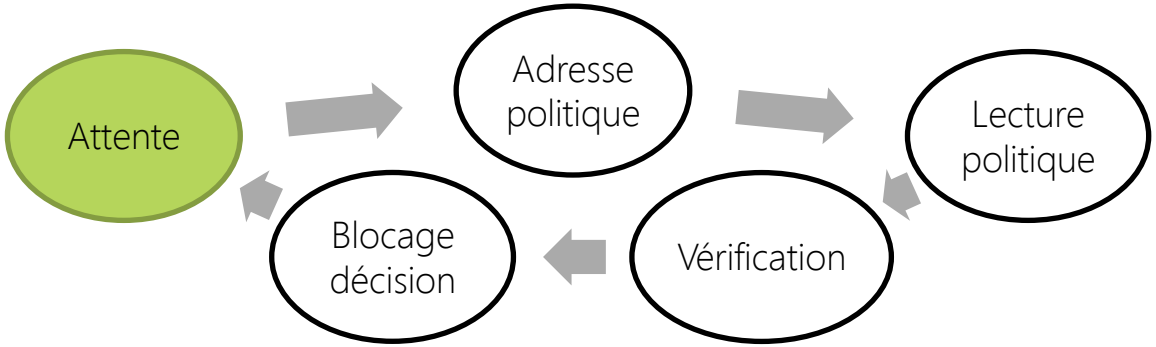




Solution de sécurité statique

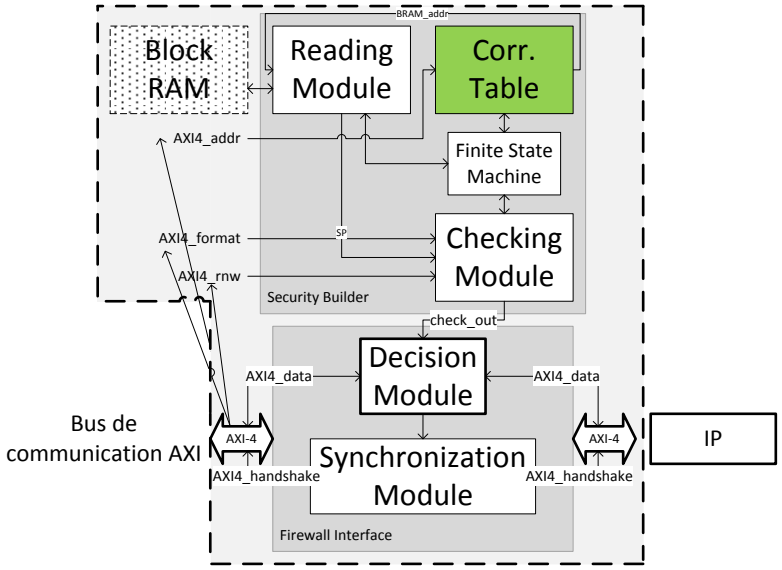
Local Firewall

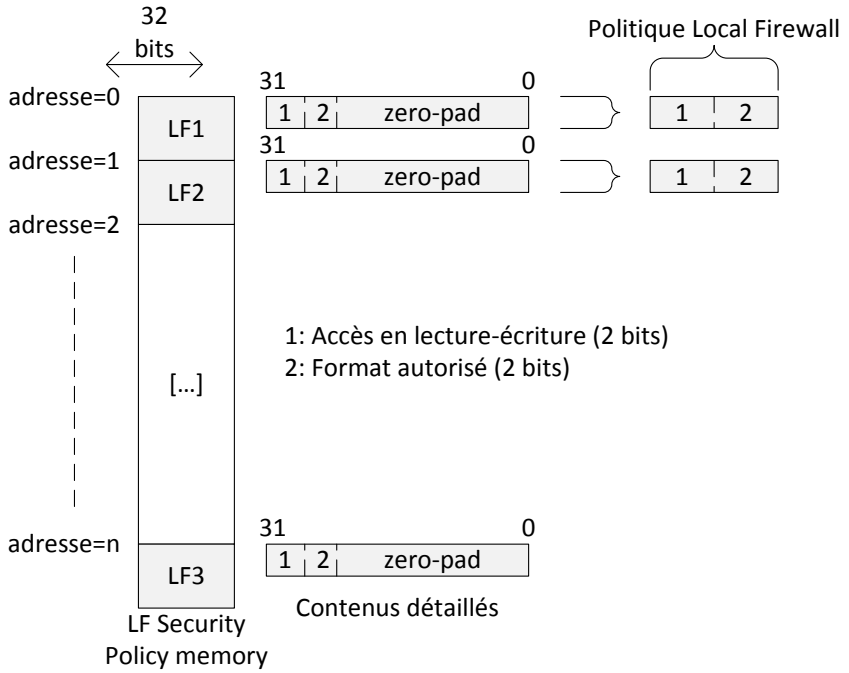


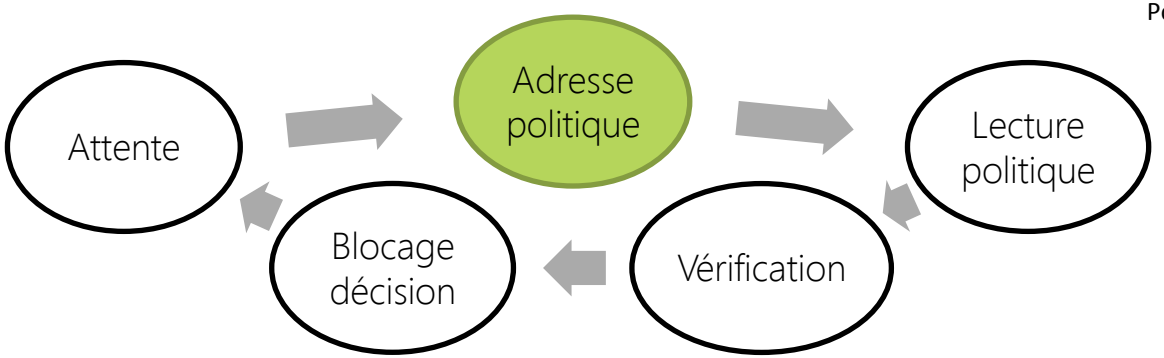


Solution de sécurité statique

Local Firewall

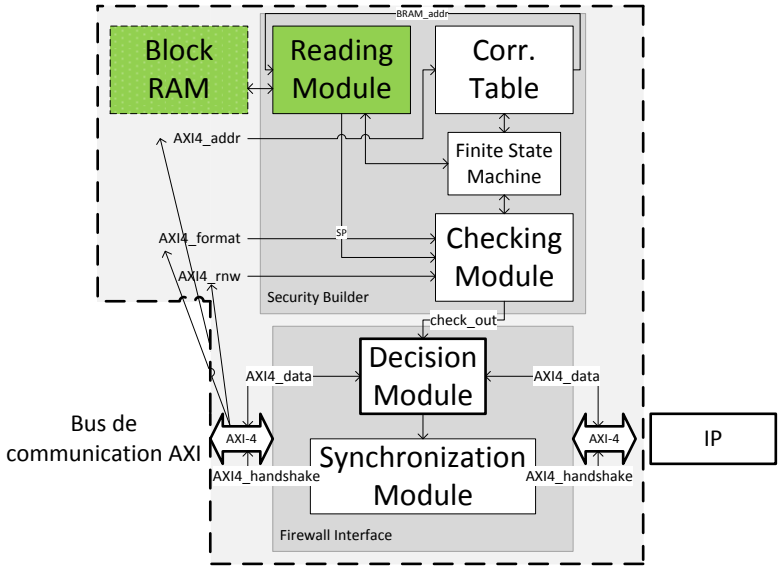


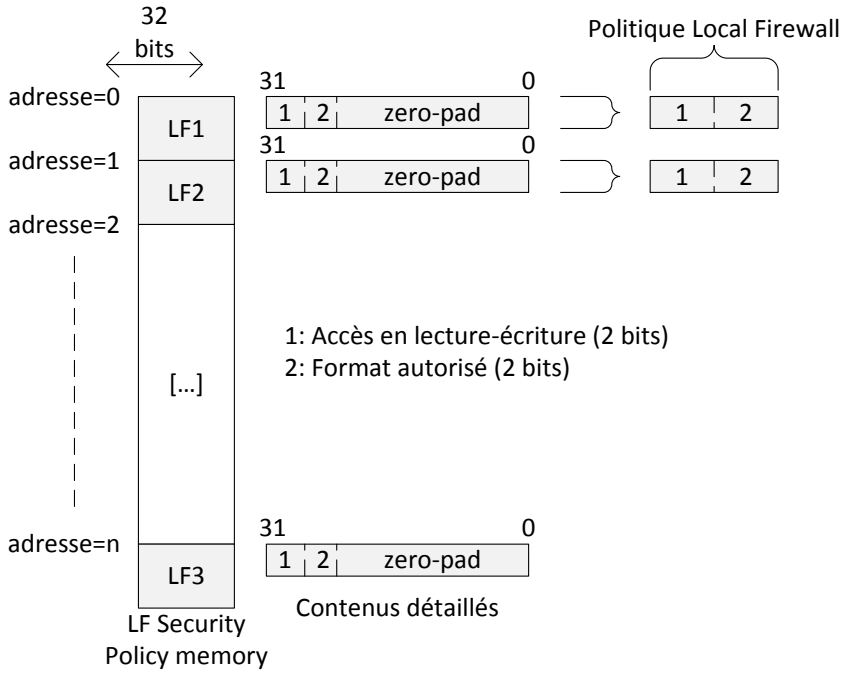


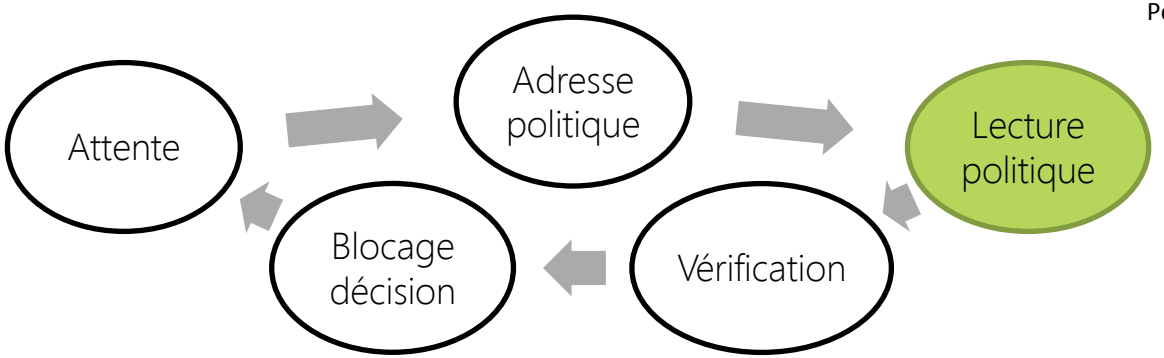


Solution de sécurité statique

Local Firewall

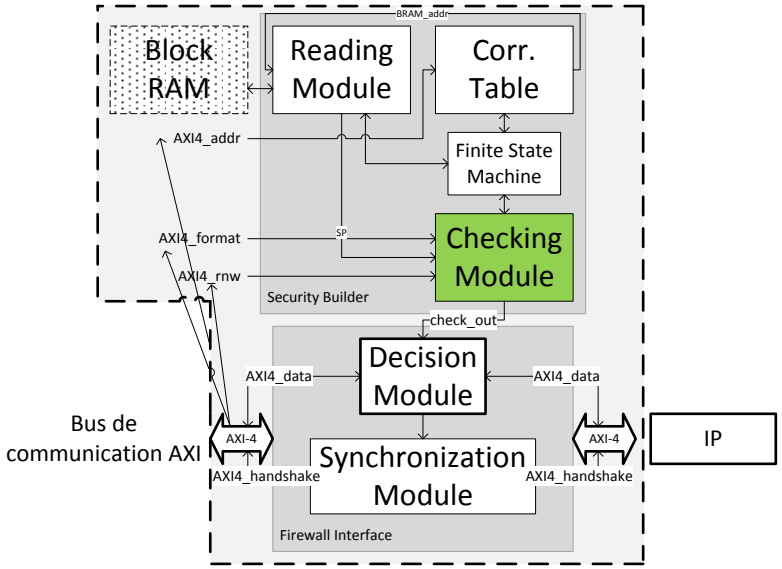


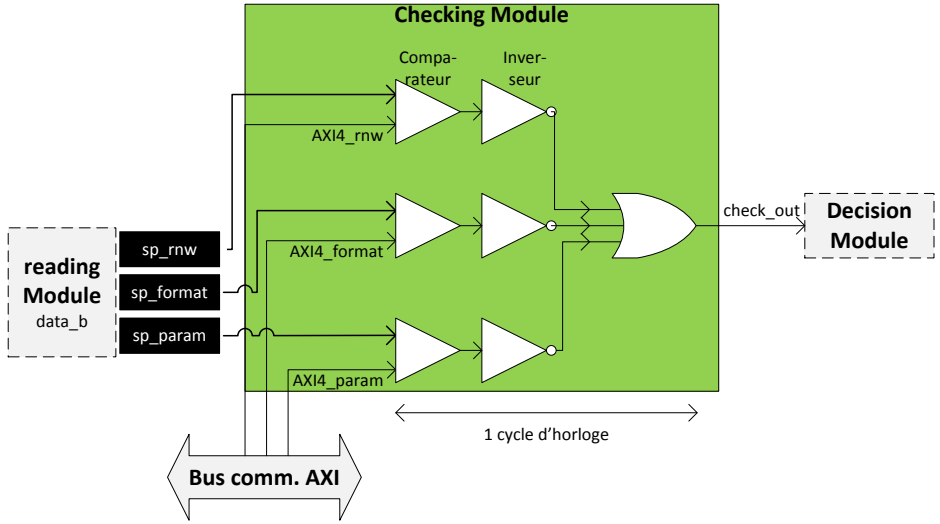


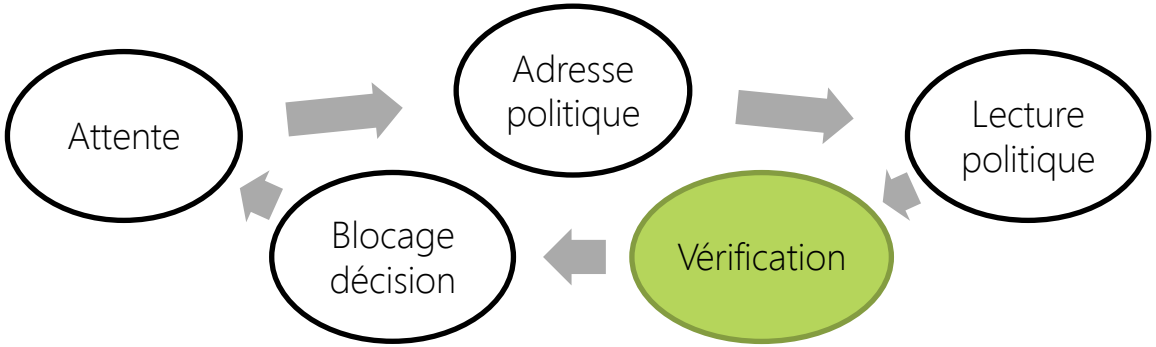


Solution de sécurité statique

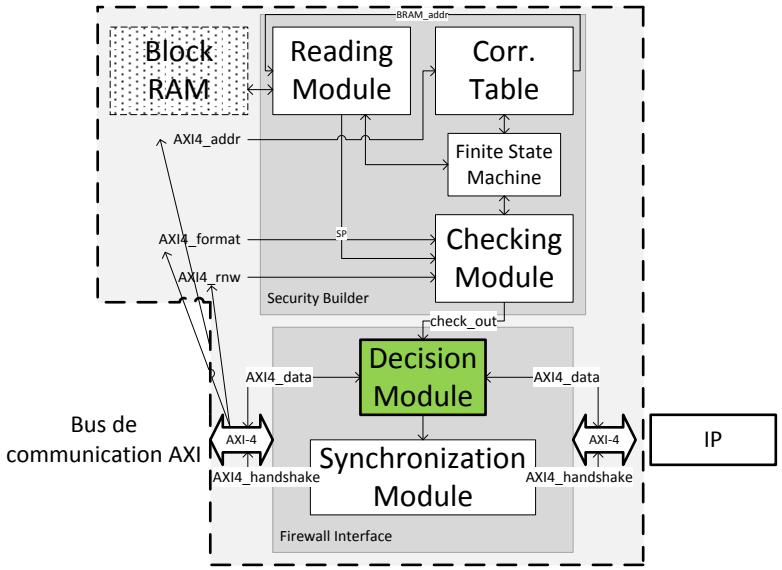
Local Firewall

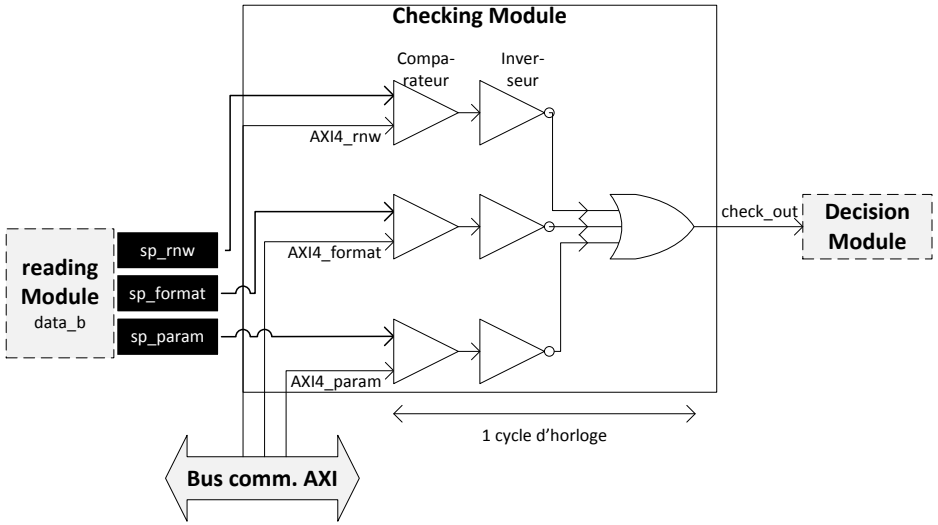


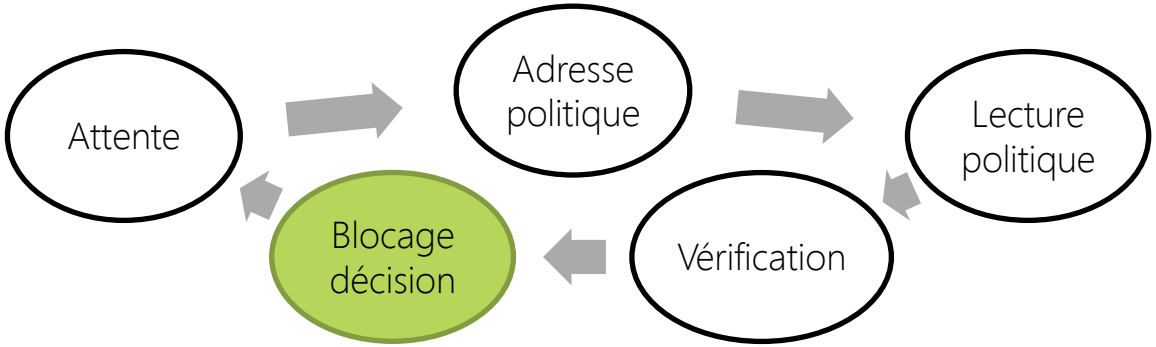




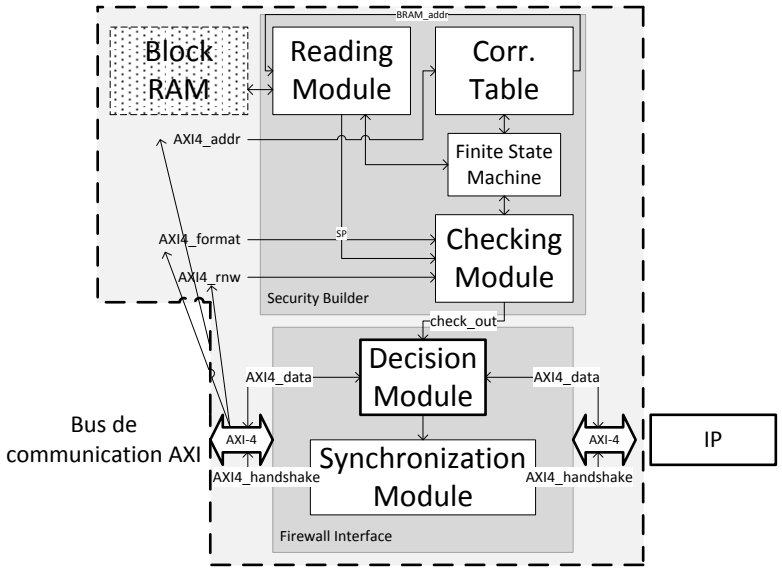
Solution de sécurité statique



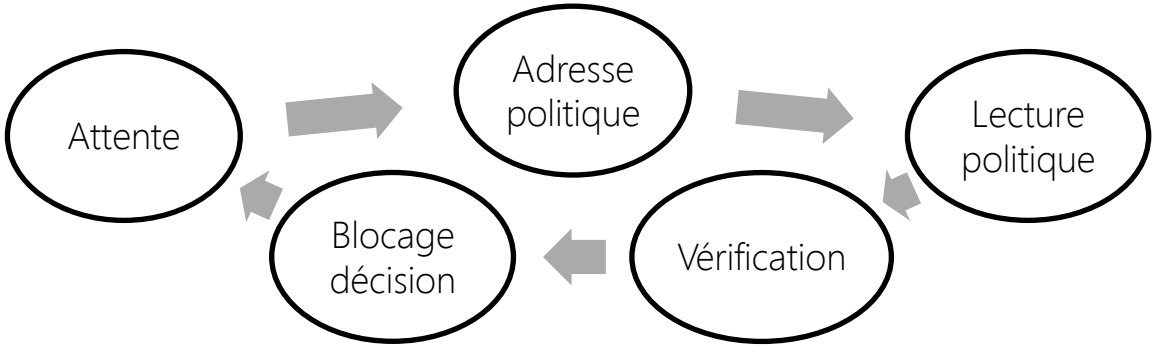




Solution de sécurité statique

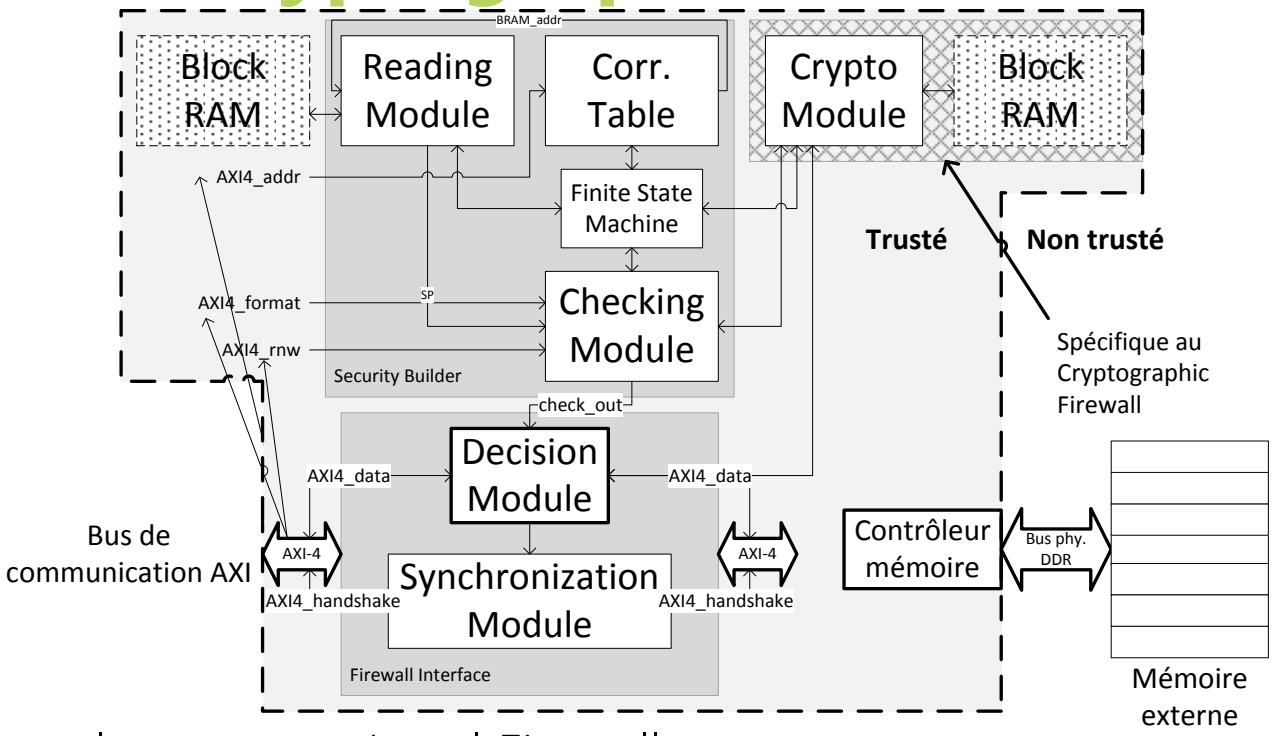


- Stockage en Block RAM.
  - Zone de confiance + mémoire à accès rapide.
- Contrôles :
  - Espaces d'adresse.
  - Droits d'accès en lecture-écriture.
  - Format des données autorisées pour la transaction courante.



Solution de sécurité statique

Cryptographic Firewall



- Propriétés analogues au « Local Firewall ».
- Dédié aux transaction externes.
- Fonctions cryptographiques.
- Protection « flexible ».

Solution de sécurité statique

Choix de l'algorithme cryptographique

- Confidentialité + intégrité.
- Possibilité de réaliser les deux fonctions séparément.
  - Cahier des charges utilisateur.
- Faible latence globale des opérations cryptographiques.
  - Latence de traitement.
  - Débit.

Solution de sécurité statique

Choix de l'algorithme cryptographique

Comparatif des différentes solutions

	Latence (cycles)	Débit
AES + MD5	90	Jusqu'à 725 Mbits/s
AES + SHA-2	74	Jusqu'à 1,8 Gbits/s
AES + SHA-3	25	Environ 30 Gbits/s
AES-GCM	22	30 Gbits/s

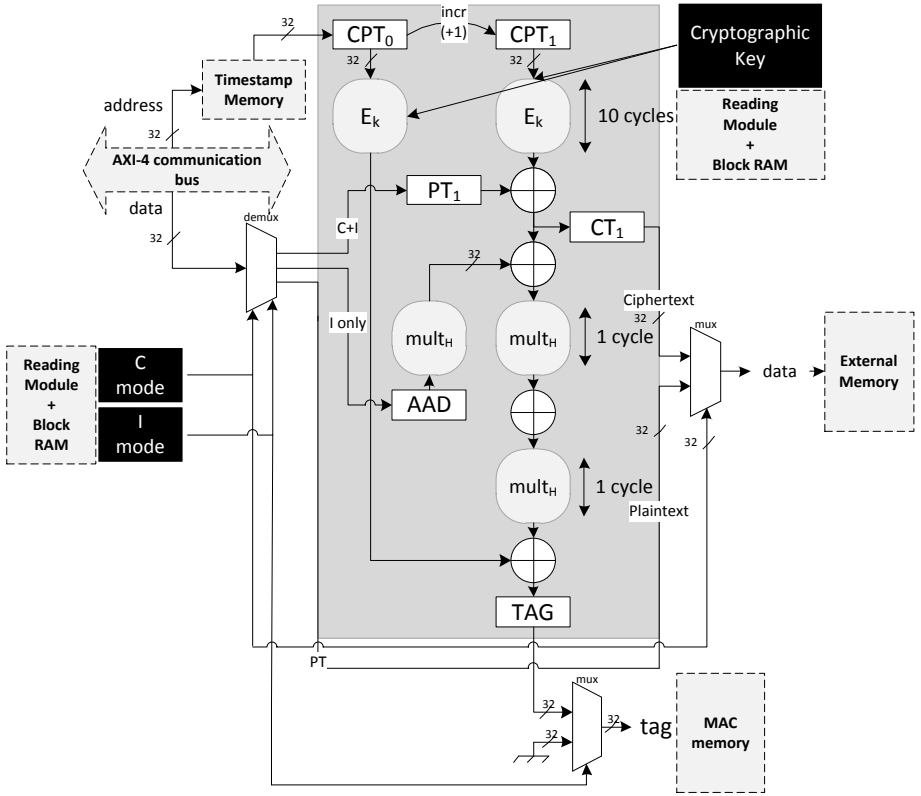
Solution de sécurité statique

Choix de l'algorithme cryptographique

Comparatif des différentes solutions

	Latence (cycles)	Débit
AES + MD5	90	Jusqu'à 725 Mbits/s
AES + SHA-2	74	Jusqu'à 1,8 Gbits/s
AES + SHA-3	25	Environ 30 Gbits/s
AES-GCM	22	30 Gbits/s

Algorithme AES-GCM



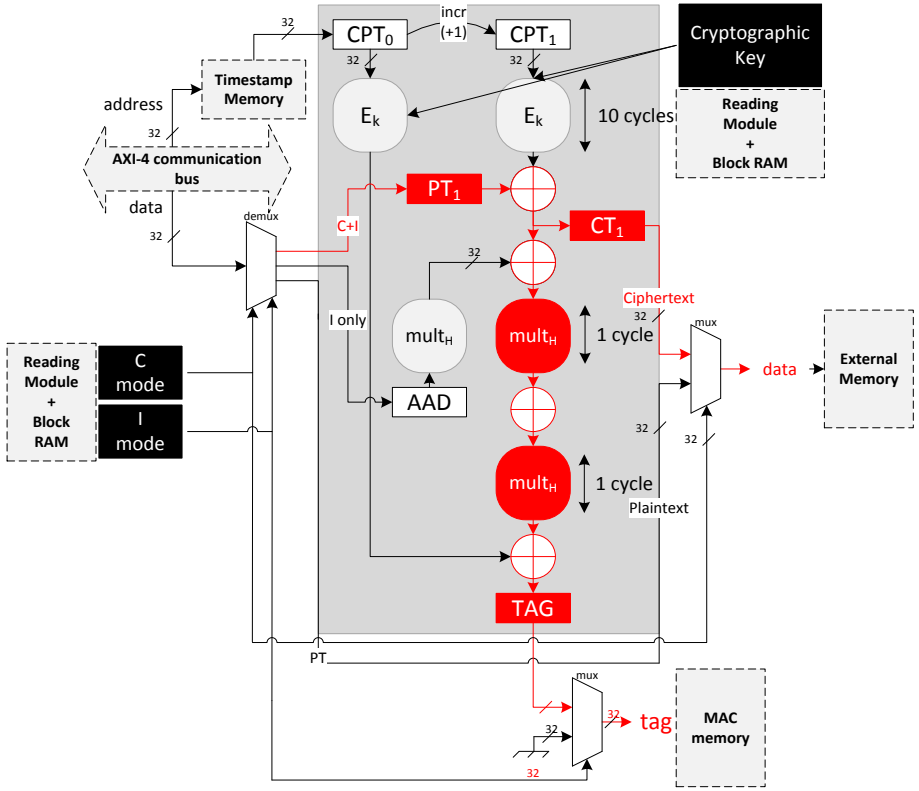
Solution de sécurité statique

Choix de l'algorithme cryptographique

Comparatif des différentes solutions

	Latence (cycles)	Débit
AES + MD5	90	Jusqu'à 725 Mbits/s
AES + SHA-2	74	Jusqu'à 1,8 Gbits/s
AES + SHA-3	25	Environ 30 Gbits/s
AES-GCM	22	30 Gbits/s

Algorithme AES-GCM



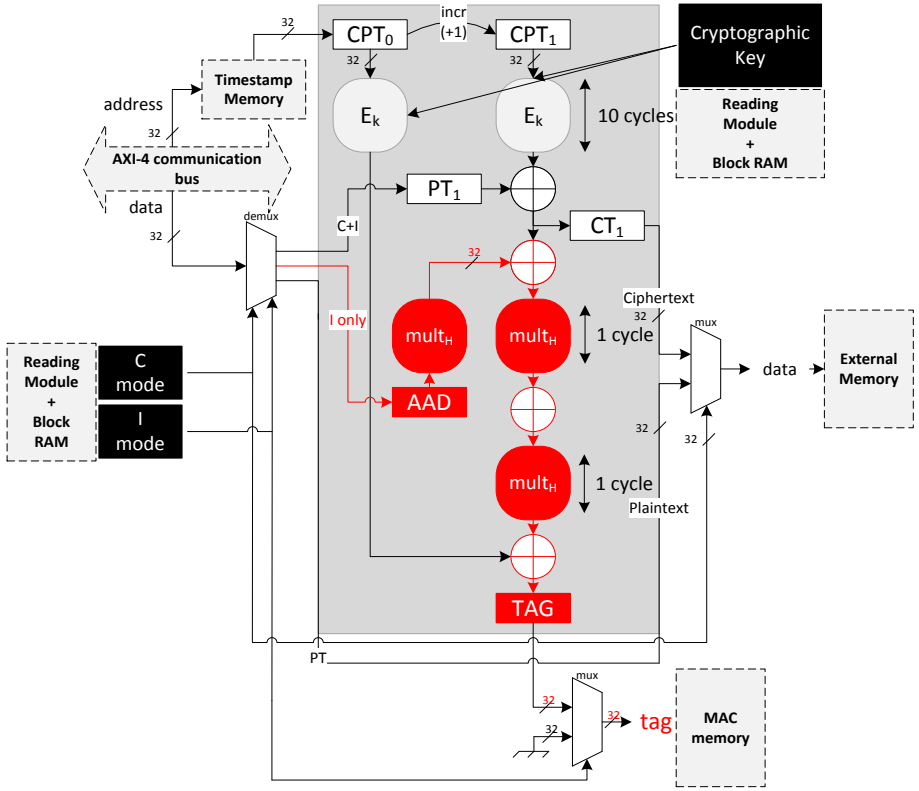
Solution de sécurité statique

Choix de l'algorithme cryptographique

Comparatif des différentes solutions

	Latence (cycles)	Débit
AES + MD5	90	Jusqu'à 725 Mbits/s
AES + SHA-2	74	Jusqu'à 1,8 Gbits/s
AES + SHA-3	25	Environ 30 Gbits/s
AES-GCM	22	30 Gbits/s

Algorithme AES-GCM



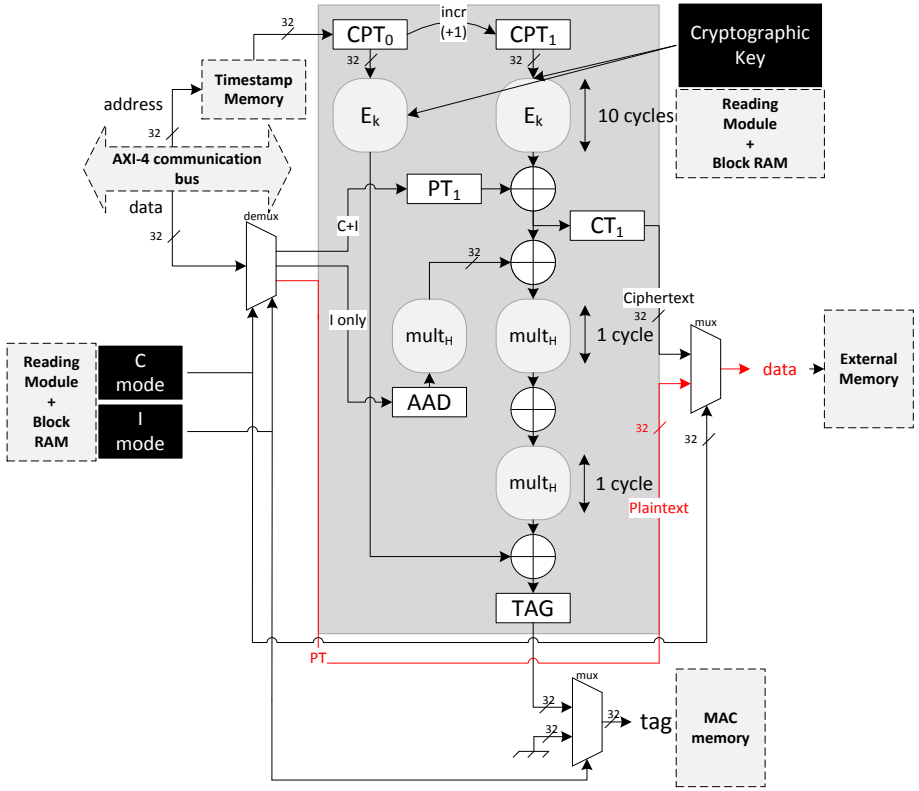
Solution de sécurité statique

Choix de l'algorithme cryptographique

Comparatif des différentes solutions

	Latence (cycles)	Débit
AES + MD5	90	Jusqu'à 725 Mbits/s
AES + SHA-2	74	Jusqu'à 1,8 Gbits/s
AES + SHA-3	25	Environ 30 Gbits/s
AES-GCM	22	30 Gbits/s

Algorithme AES-GCM



Solution de sécurité statique

Performances - Surface

		Slice	Registres	LUTs
Local Firewall	Total	99	123	293
Crypto Firewall	Total	1304	2161	2689
	Bloc crypto	1166 (89,42%)	2038 (94,31%)	2396 (89,10%)
Microblaze (référence)		1179	1298	1829

- Surface réduite des Local Firewalls.
- Impact du module de chiffrement (> 90%).

Solution de sécurité statique

Performances - Surface

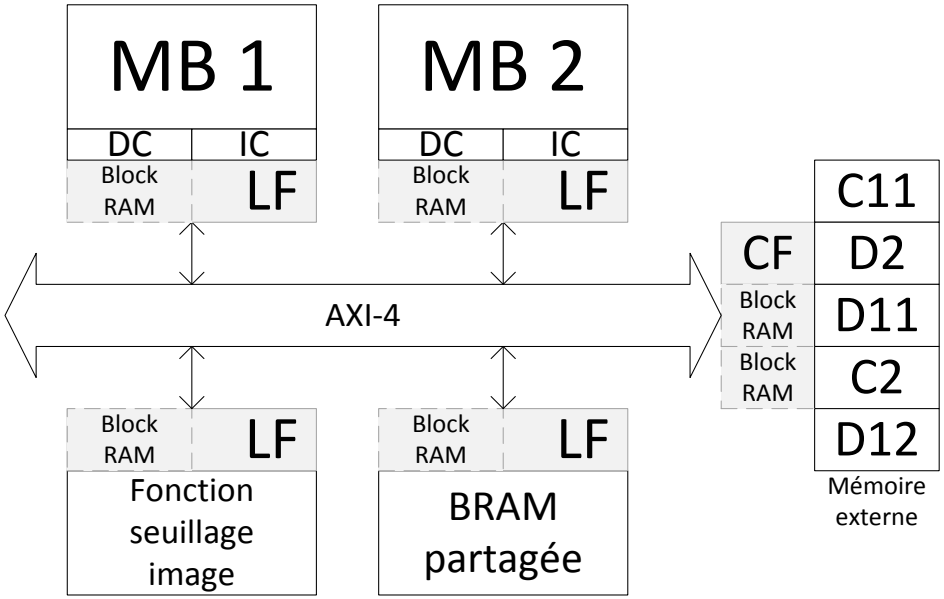
		Slice	Registres	LUTs
Local Firewall	Total	99	123	293
Crypto Firewall	Total	1304	2161	2689
	Bloc crypto	1166 (89,42%)	2038 (94,31%)	2396 (89,10%)
Microblaze (référence)		1179	1298	1829

- Surface réduite des Local Firewalls.
- Impact du module de chiffrement (> 90%).

Solution de sécurité statique

Performances – Cas d'étude

Xilinx ML605 + ISE 14.1

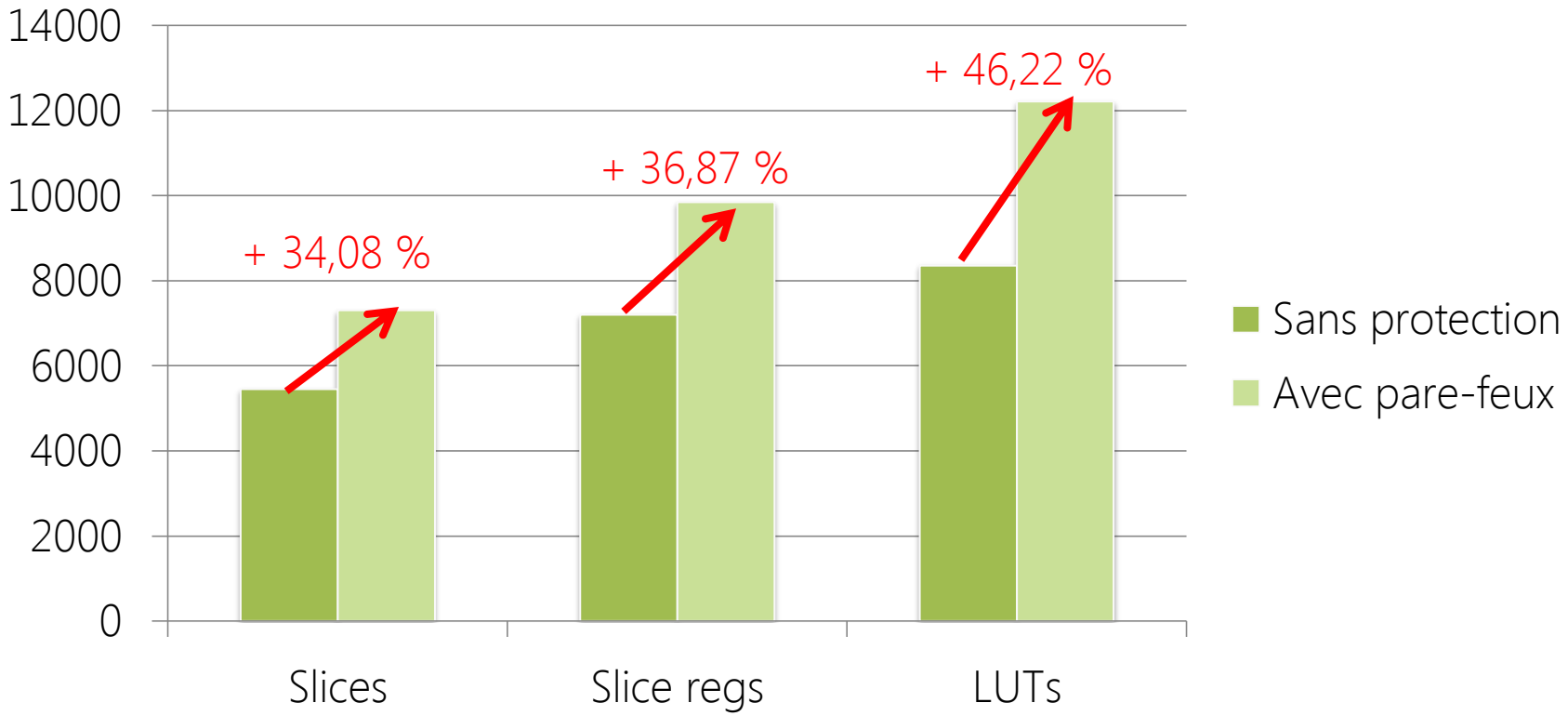


	Mode cryptographique
C11 – D11	Confidentialité – intégrité
D12	Intégrité seulement
C12	Texte clair

	BRAM	Seuillage image
MB1	Lecture seule	Lecture-écriture
MB2	Lecture-écriture	Ecriture seule

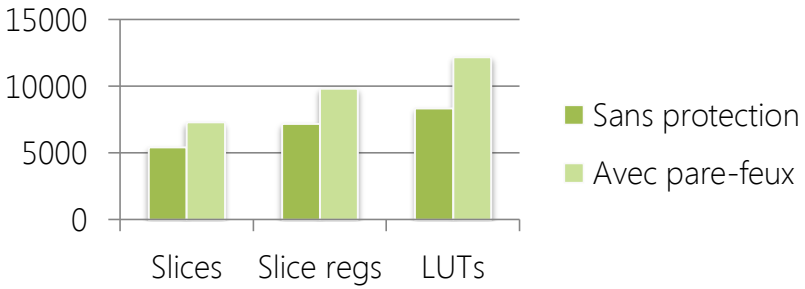
Solution de sécurité statique

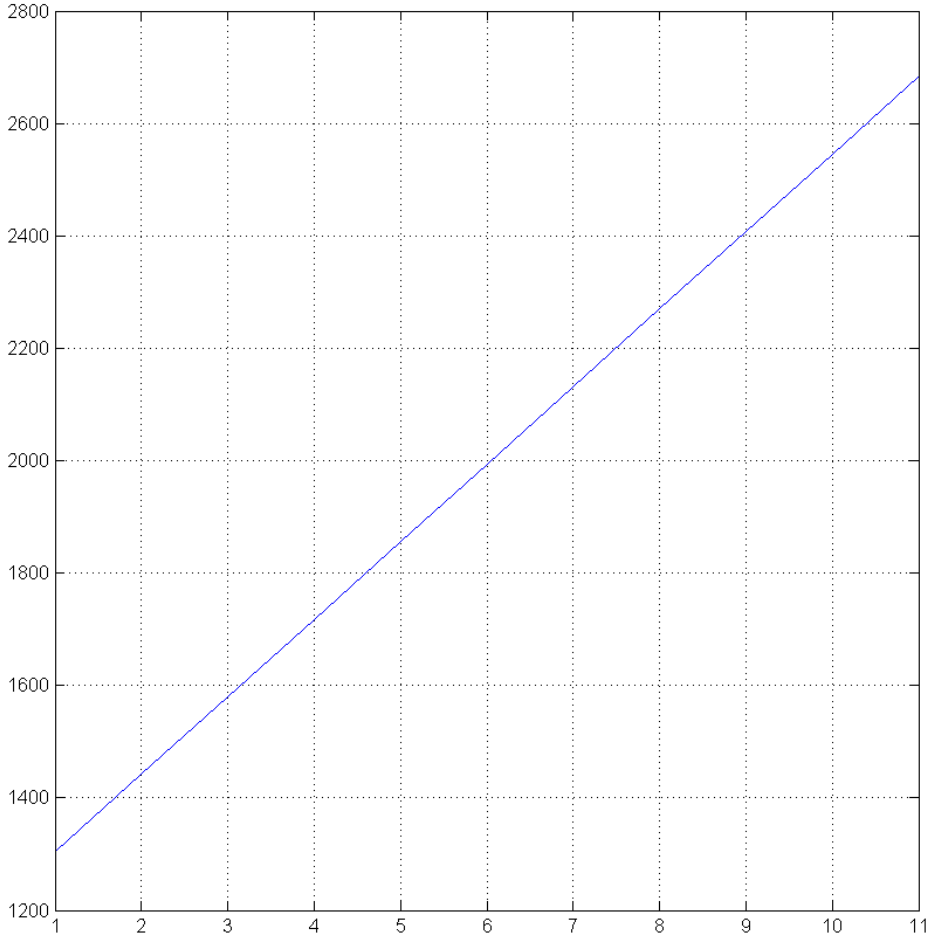
Performances - Surface



Solution de sécurité statique

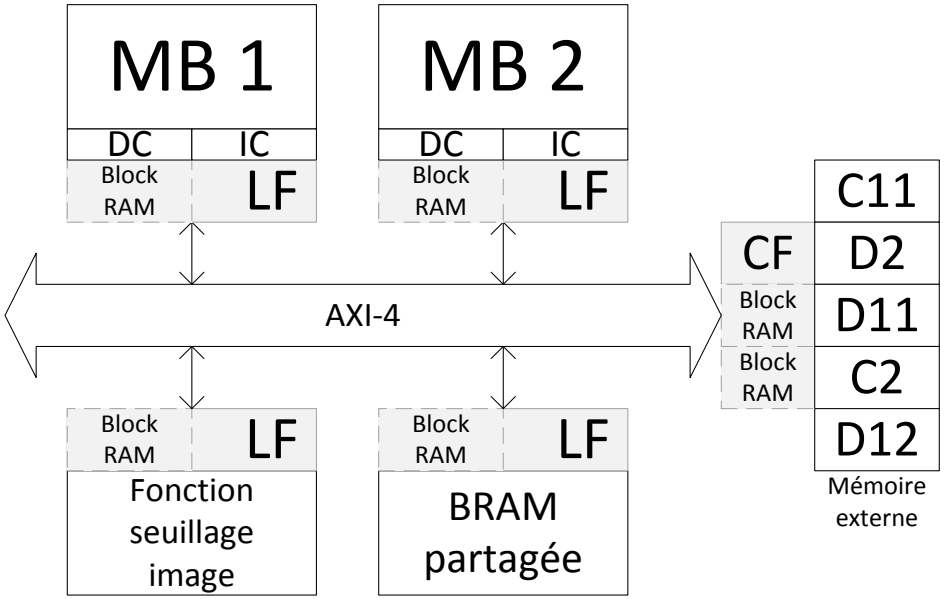
Performances - Surface

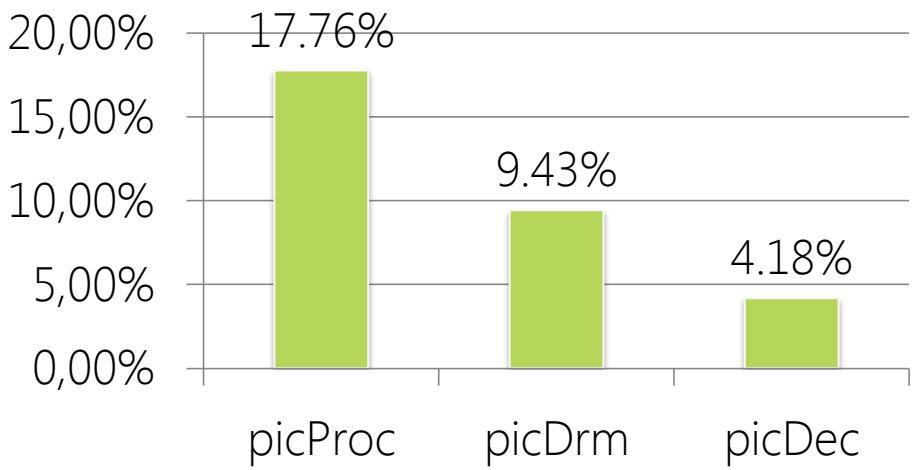




Solution de sécurité statique

Performances – Latence





Solution de sécurité statique

Problèmes liés…

- On bloque les attaques…

Solution de sécurité statique

Problèmes liés…

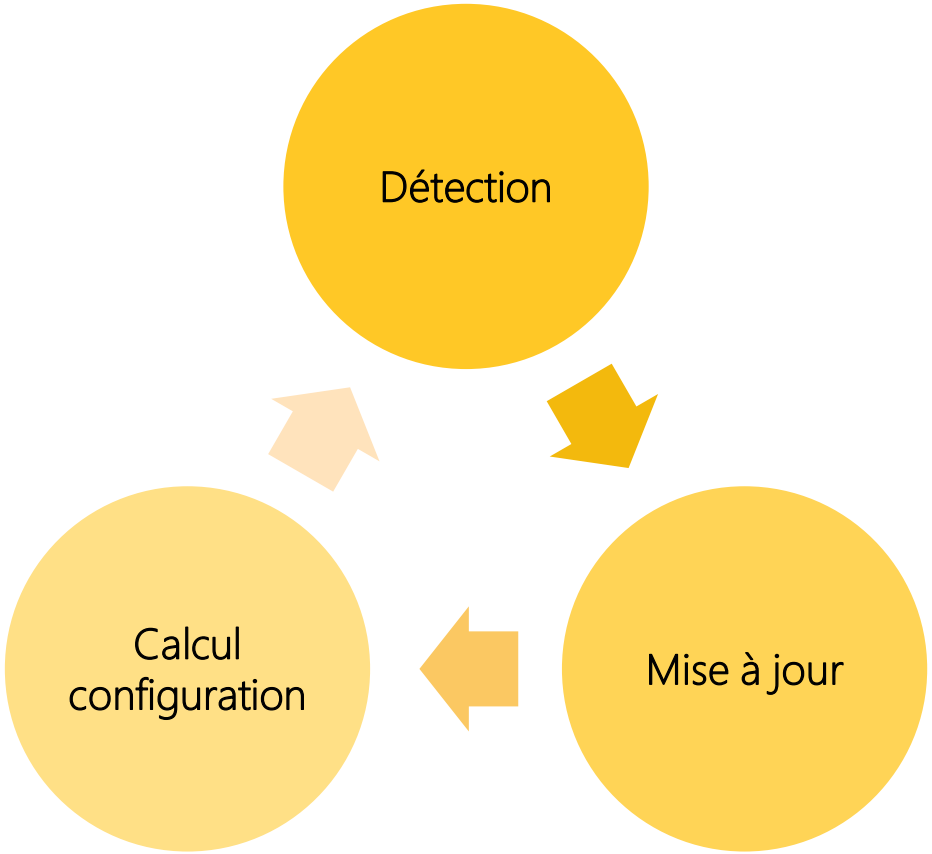
- On bloque les attaques…
- … mais on ne peut pas mettre à jour les pare-feux.
- … comment procéder à la mise à jour de manière fluide ? Sans fuites de données malveillantes ?

Plan

- Solution de sécurité statique
- Mise à jour en temps réel
- Conclusion
- Perspectives

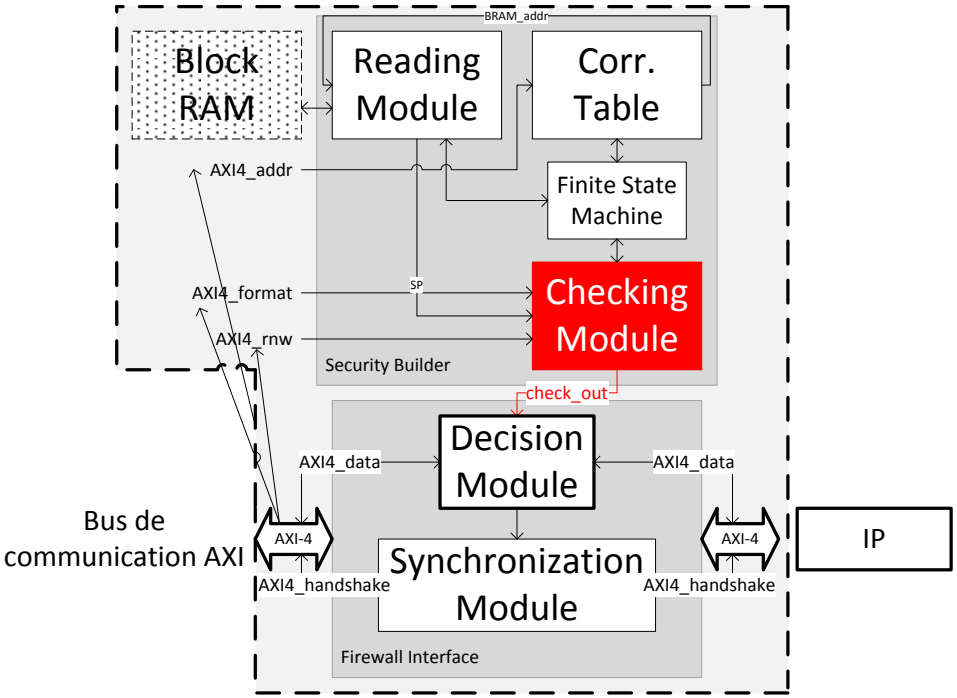
Mise à jour en temps réel

Schéma de principe



Mise à jour en temps réel

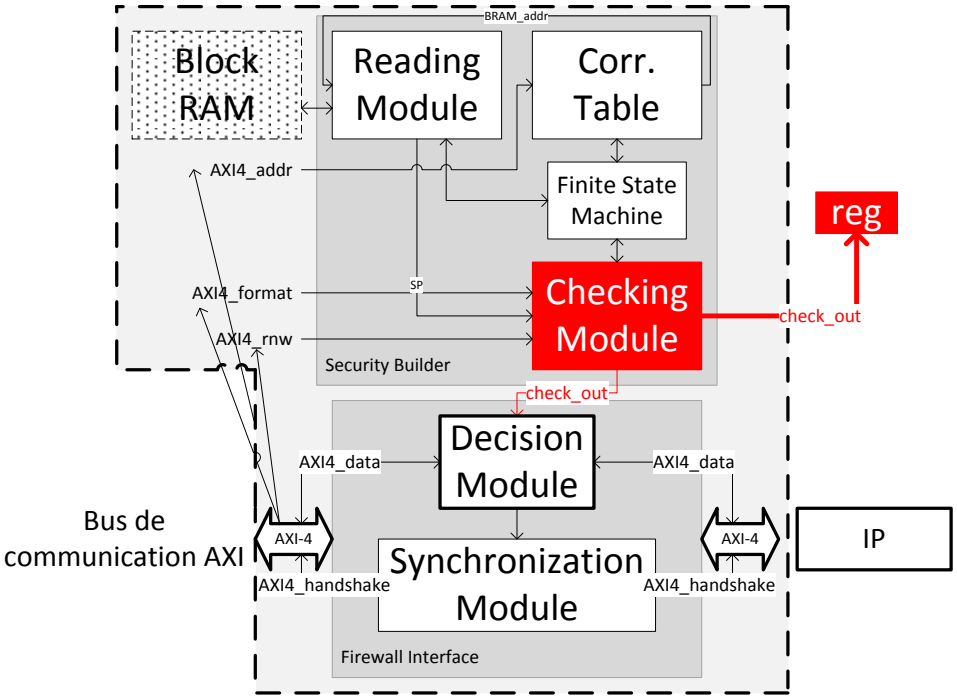
Détection d'une attaque



- Extraction du flag d'attaque check_out.

Mise à jour en temps réel

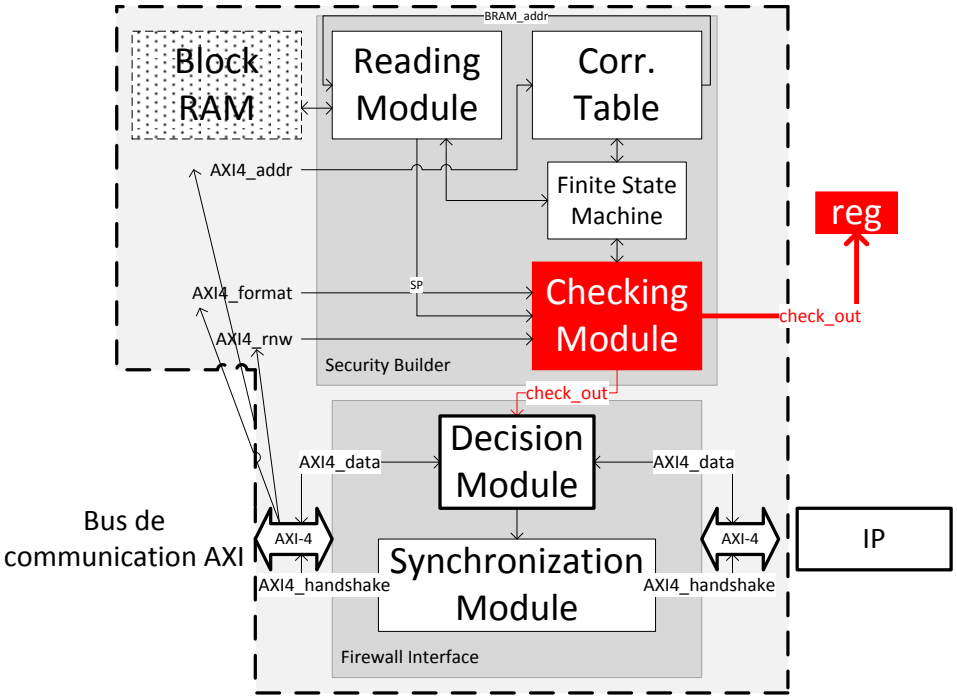
Détection d'une attaque

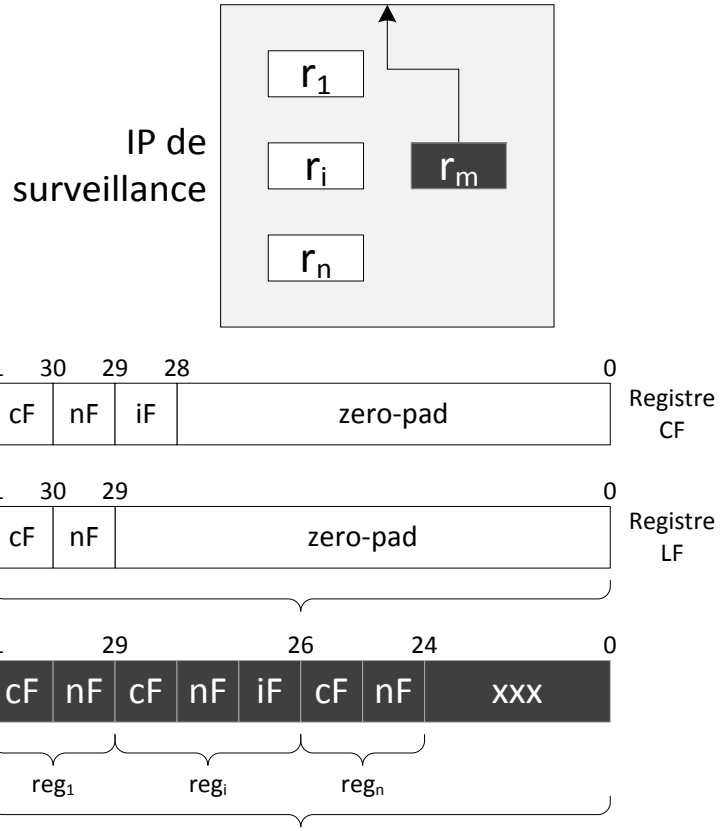


- Extraction du flag d'attaque check_out.

Mise à jour en temps réel

Détection d'une attaque

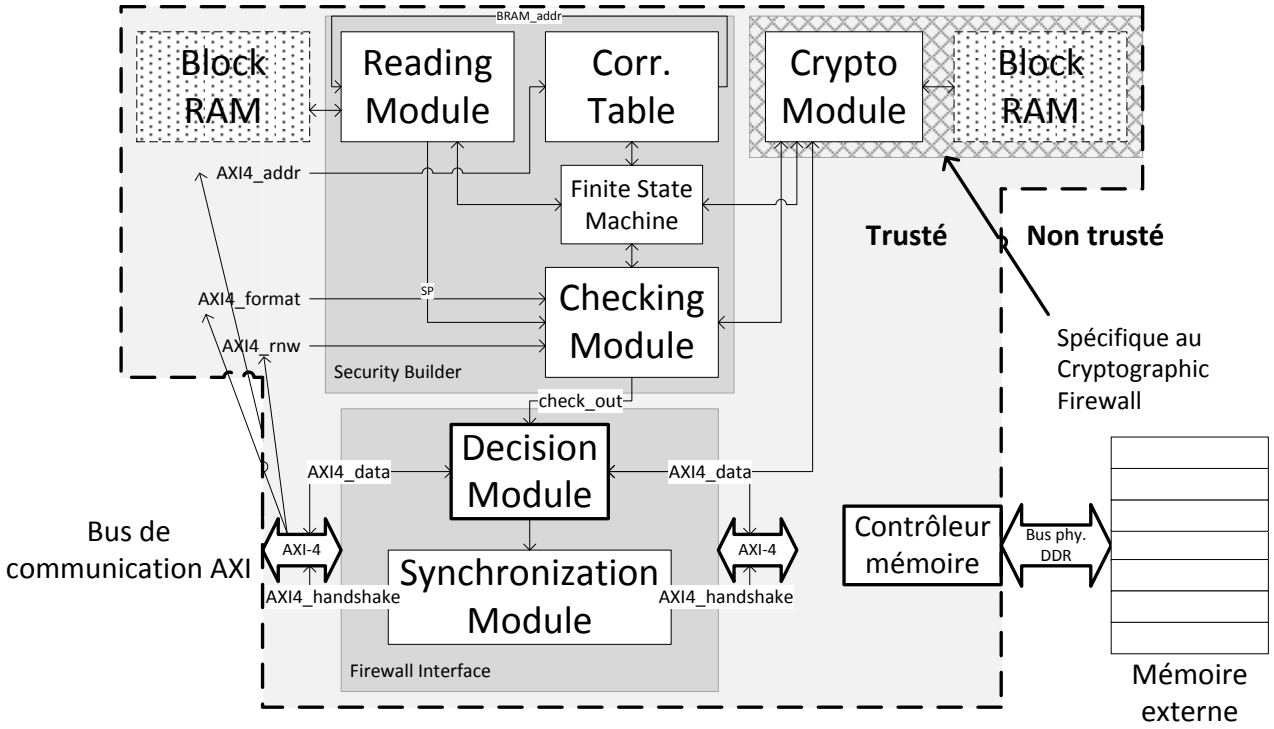




- Généralisation à N registres.

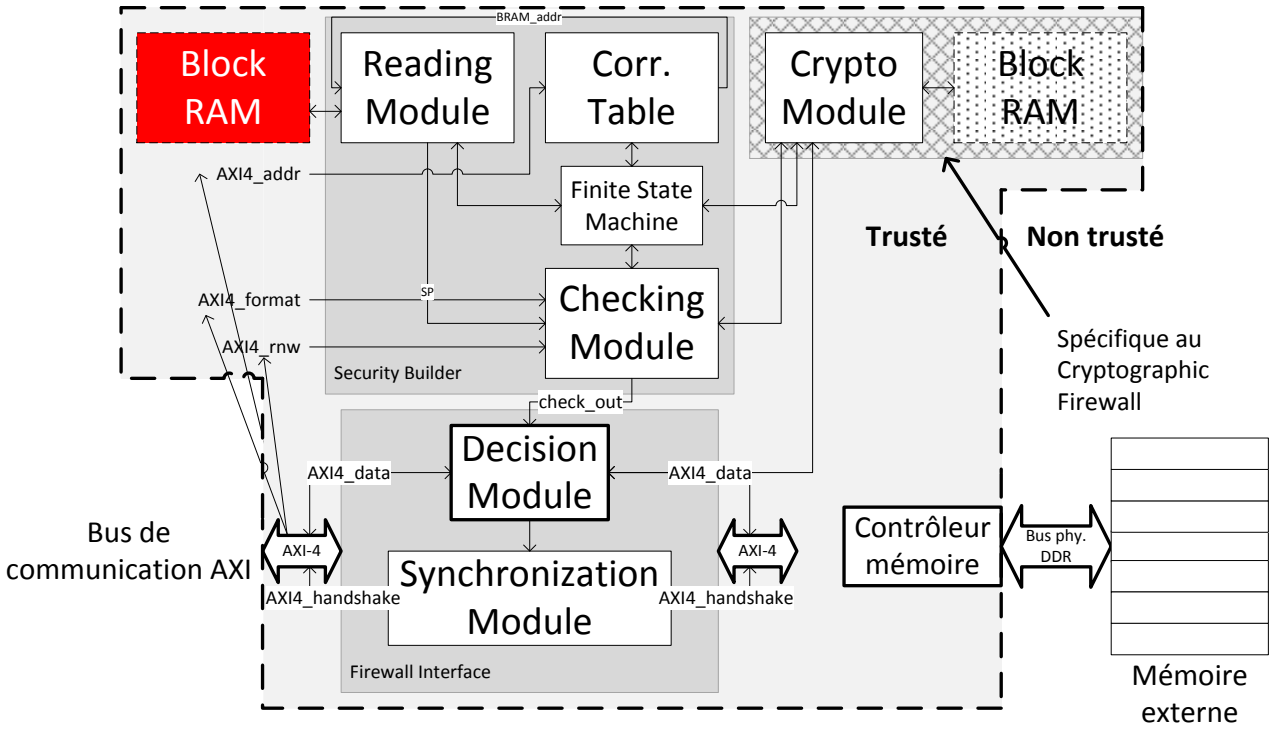
Mise à jour en temps réel

Eléments à modifier



Mise à jour en temps réel

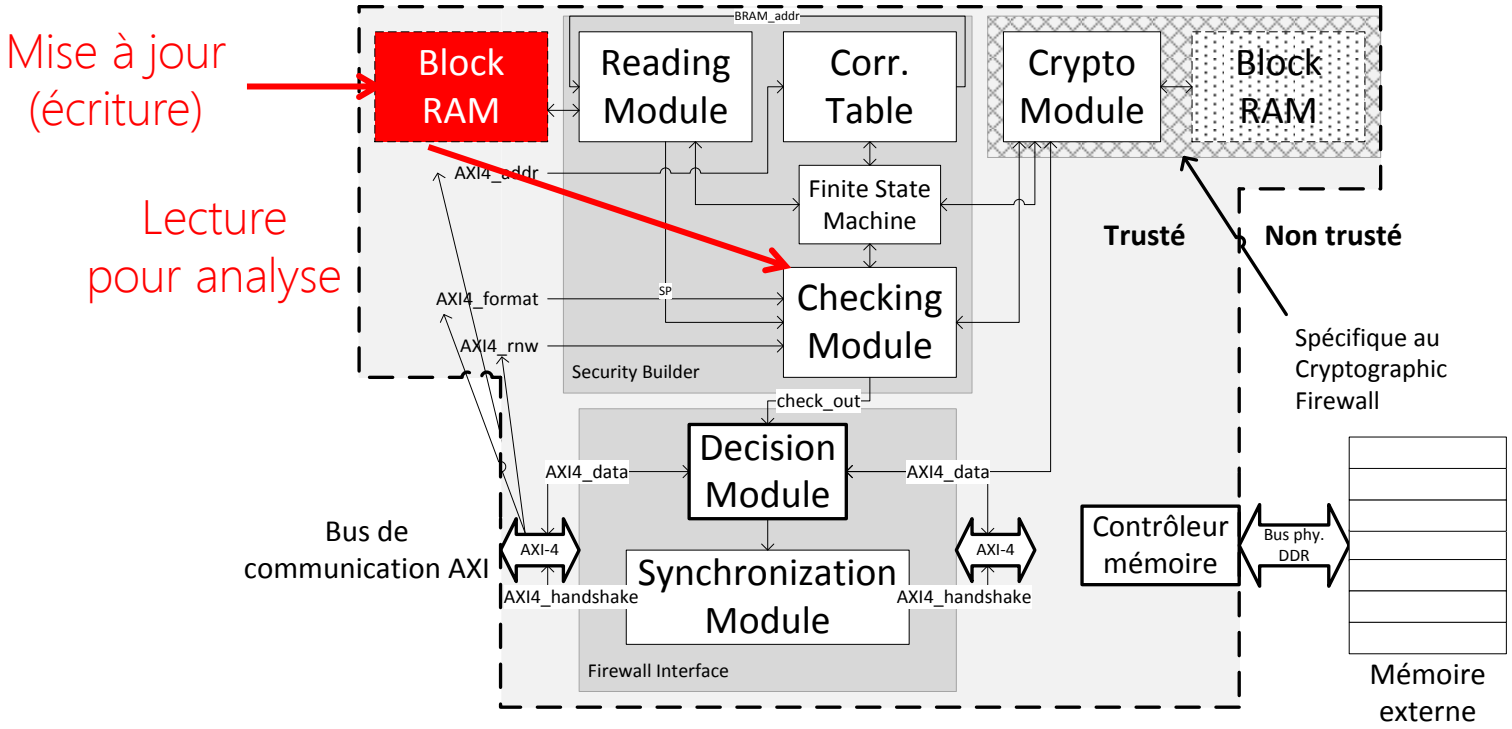
Eléments à modifier



- Paramètres des politiques de sécurité.
- Connexion supplémentaire.

Mise à jour en temps réel

Eléments à modifier

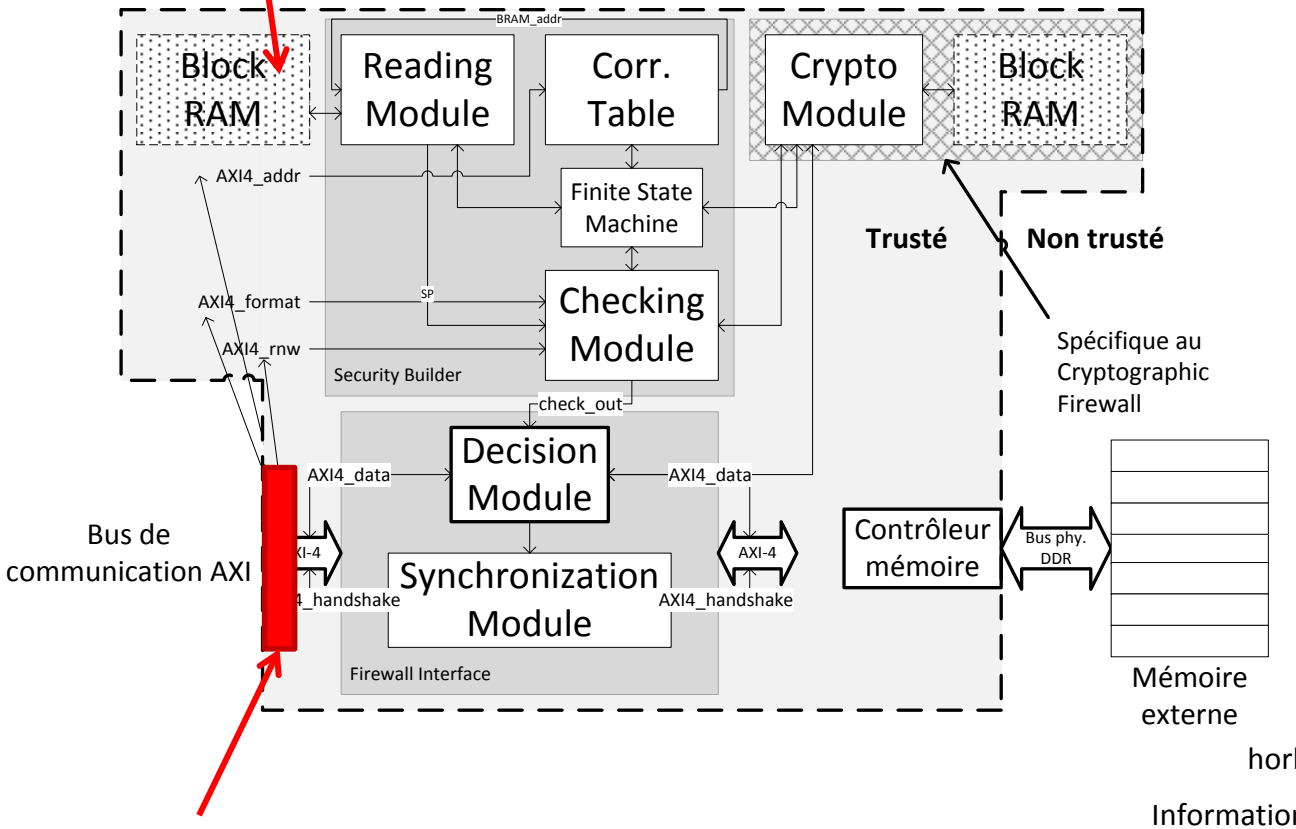


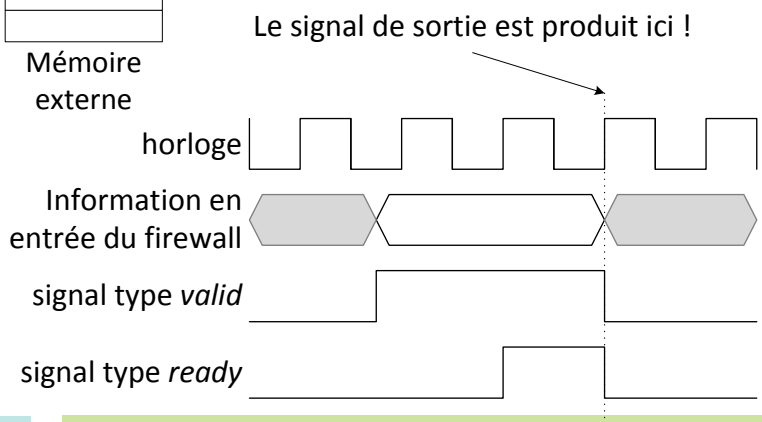
- Paramètres des politiques de sécurité.
- Connexion supplémentaire.

Mise à jour en temps réel

Mise à jour (écriture)

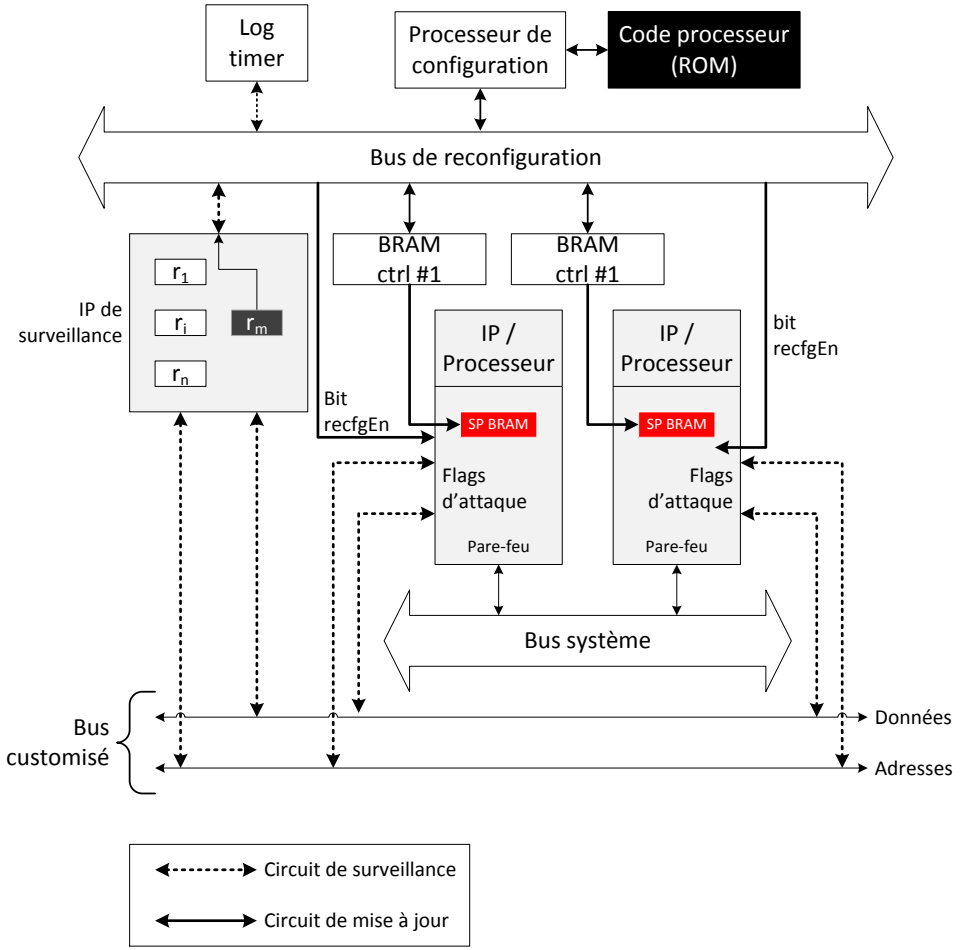
Eléments à modifier





Mise à jour en temps réel

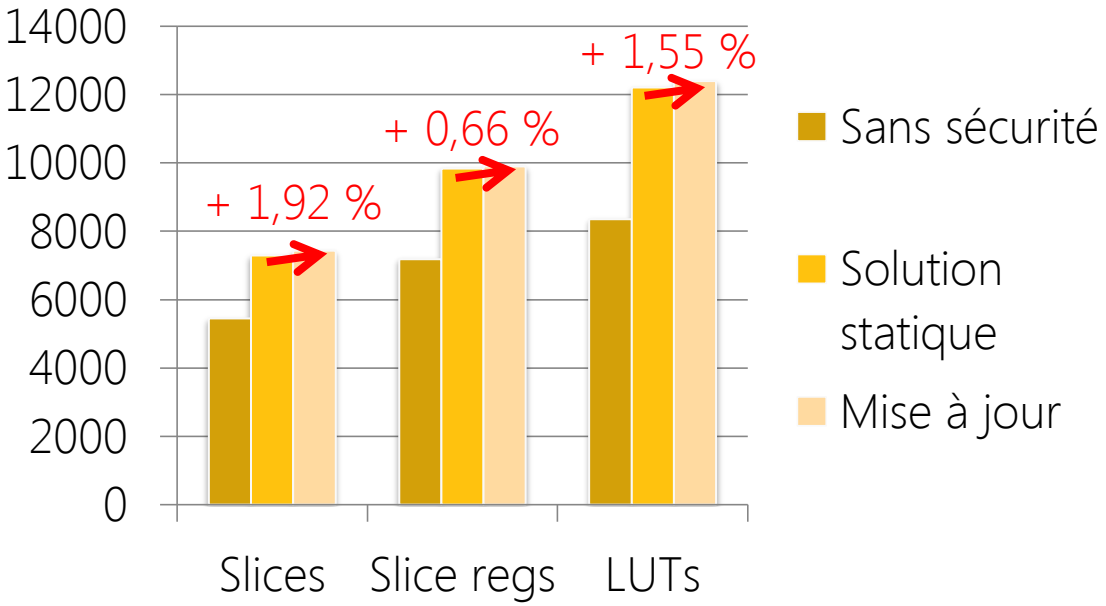
Architecture dédiée

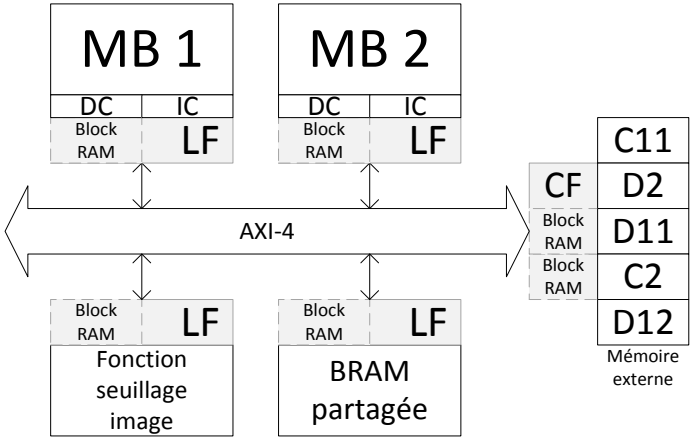


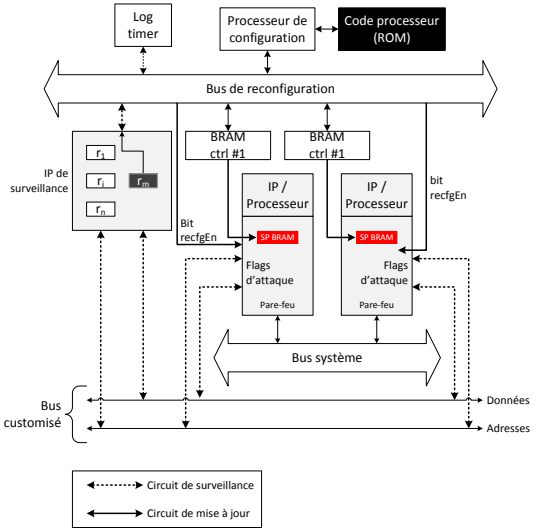
- Détection des attaques.
- Calcul de la nouvelle configuration.
- Mise à jour des Block RAM.

Mise à jour en temps réel

Performances surface et mémoire







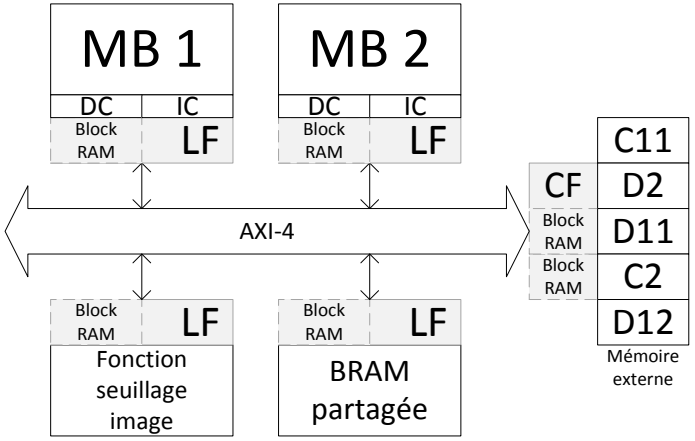
- Surface : impact négligeable.
- Mémoire : code du processeur de mise à jour (calcul configuration).

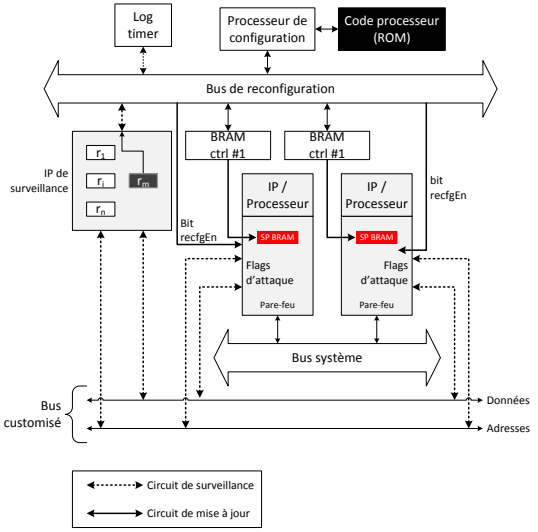
Mise à jour en temps réel

Performances latence

Opération	Nombre de cycles
Copie des flags	1
Routine d'interruption	2
Calcul nouvelle configuration	148
Ecriture nouvelle configuration	1
Réarmement application	1

Total minimum : 153 cycles





Mise à jour en temps réel

Performances - Comparatif

	[Coburn 2005]	[Fiorin 2008]	Notre solution
Paramètres quantitatifs			
Bloc de sécurité / Processeur	6,2 %	25 %	11,30%
Protocole de comm.	Bus	NoC	Bus
Mise à jour	Non	Oui	Oui
Crypto	Non	Non	Oui
Répartition sécurité	Centralisé	Distribué	Distribué

- [Fiorin 2008] L. Fiorin, G. Palermo, C. Silvano. *A security monitoring for NoCs*. CODES+ISSS 2008.
- [Coburn 2005] J. Coburn, S. Ravi, A. Raghunathan et S. Chakradhar. *SECA : Security-Enhanced Communication Architecture*. CASES 2005.

Plan

- Solution de sécurité statique
- Mise à jour en temps réel
- Conclusion
- Perspectives

Conclusion

- Protection des architectures multiprocesseurs (communications et mémoires).
- Contrôles de divers paramètres du trafic de données.
- Possibilité de mettre à jour la sécurité du système sans fuites de données.
- Cryptographie « flexible ».
- Compromis surface – latence.

Perspectives

- Filtrage au niveau logiciel :
  - Système multi-tâches.
  - Identification tâche.
  - Différenciation politiques selon identifiant.

- Tolérance aux fautes :
  - Détection des faux positifs.
  - Dysfonctionnement circuits.
  - Attaques détectées non valables.

Publications

Conférences internationales et workshops :

- Lightweight reconfiguration security services for AXI-based MPSoCs
  FPL 2012 - Oslo, Norvège – 29-31 août 2012
  Pascal Cotret, Guy Gogniat, Jean-Philippe Diguet, Jérémie Crenne
- Security enhancements for FPGA-based MPSoCs: a boot-to-runtime protection flow for an embedded Linux-based system
  ReCoSoC 2012 – York, Angleterre – 9-11 juillet 2012
  Pascal Cotret, Florian Devic, Guy Gogniat, Benoît Badrignans, Lionel Torres
- Bus-based MPSoC security through communication protection: A latency-efficient alternative
  FCCM 2012 - Toronto, Canada – 29 april, 1 mai 2012
  Pascal Cotret, Jérémie Crenne, Guy Gogniat, Jean-Philippe Diguet
- Efficient key-dependent message authentication in reconfigurable hardware
  FPT 2011 - New Delhi, Inde – 12-14 décembre 2011
  Jérémie Crenne, Pascal Cotret, Guy Gogniat, Russell Tessier, Jean-Philippe Diguet
- Distributed security for communications and memories in a multiprocessor architecture
  RAW 2011 - Anchorage, Etats-Unis – 16-17 mai 2011
  Pascal Cotret, Jérémie Crenne, Guy Gogniat, Jean-Philippe Diguet, Lubos Gaspar, Guillaume Duc
- HCrypt: a novel concept of crypto-processor with secured key management
  ReConFig 2010 - Cancùn, Mexique– 13-15 décembre 2010
  Lubos Gaspar, Viktor Fischer, Florent Bernard, Lilian Bossuet, Pascal Cotret

Conférence nationale :

- Sécurisation des communications dans une architecture multiprocesseur
  MajecSTIC 2010, Bordeaux, France – 13-15 octobre 2010
  Pascal Cotret, Jérémie Crenne, Guy Gogniat

pascalcotret.wordpress.com

Pascal Cotret
Lorient
11 décembre 2012

UNIVERSITÉ EUROPÉENNE DE BRETAGNE

UBS Université de Bretagne-Sud

Lab-STICC

Protection des architectures hétérogènes multiprocesseurs dans les systèmes embarqués

Une approche décentralisée basée sur des pare-feux matériels