

Sécurité des circuits analogiques

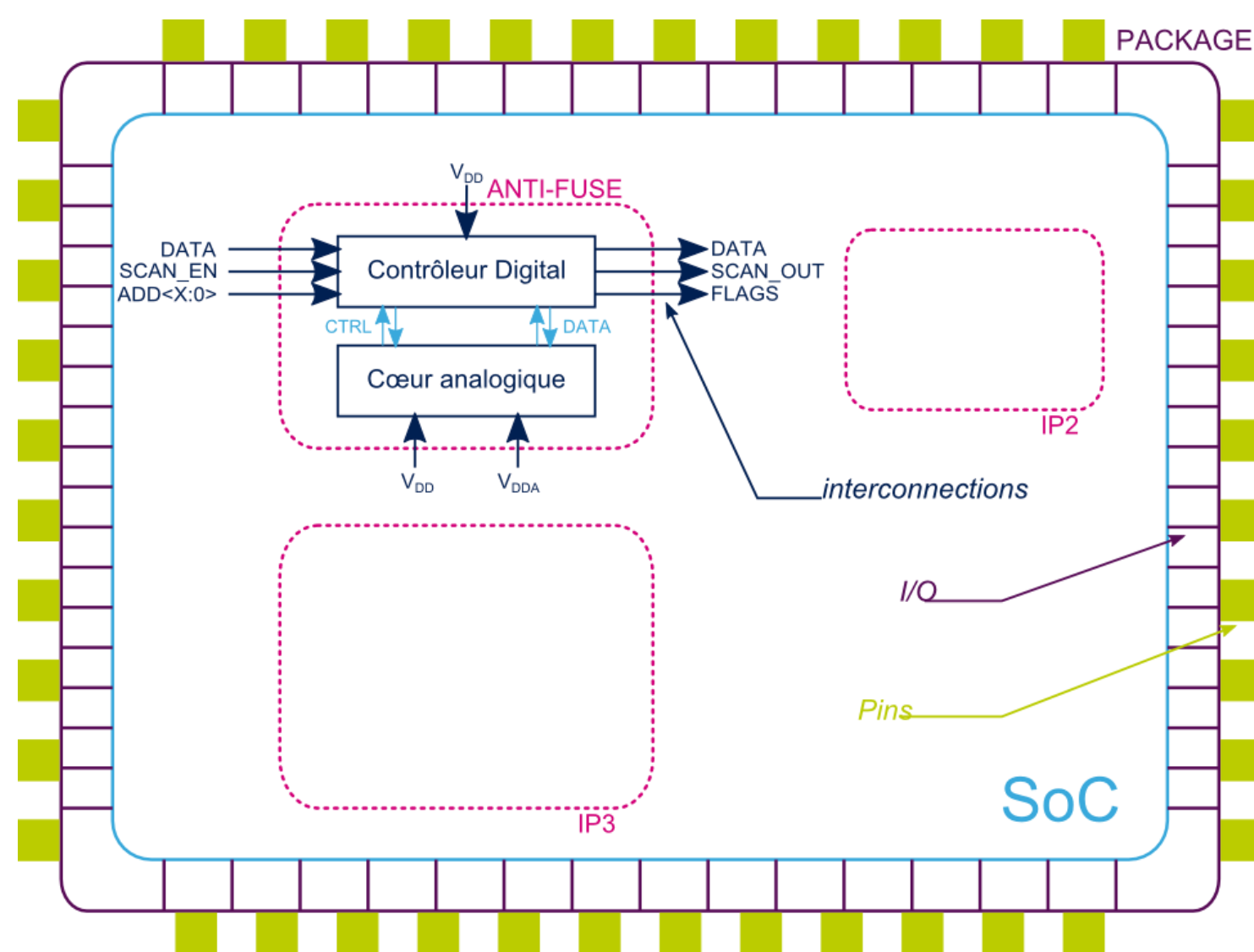
Application aux mémoires non-volatiles

Noémie Boher^{1,2}, Vincent Beroulle¹, David Hély¹, Joël Damiens², Philippe Candelier²

¹: Grenoble INP LCIS, Valence ; ²: STMicroelectronics, Crolles

Contact : prenom.nom@lcis.grenoble-inp.fr, prenom.nom@st.com

Problématique: La **sécurité des circuits analogiques** est peu abordée par la littérature. Pourtant, que ce soit d'un point de vue attaques par canaux auxiliaires ou d'un point de vue attaques par injections de fautes, ces circuits jouent un rôle important dans la sécurité des SoCs. Ainsi, ces travaux aborderont cette problématique afin de sécuriser le cœur analogique de circuits de mémoires non-volatiles (NVM), programmables une fois (OTP) et de type **Anti fusible**.



Intégration d'un circuit de mémoire anti-fusible dans un SoC

Spécificités de la sécurité des circuits analogiques

- Complexité et **interdépendances** des blocs analogiques
- Seuils de tolérance sur les signaux
- Effets des **fautes paramétriques** non négligeables et difficiles à analyser
- Effet des attaques fortement dépendants des **conditions de fonctionnement** et de fabrication du circuit

Les mémoires anti fusibles:

- Non-volatiles** et **programmables une fois électriquement**
- Utilisées pour stocker des **petites quantités d'information** (clés de cryptographie, clés d'activation de services, ...)
- Basées sur le phénomène physique de **claquage d'oxyde** (la cellule est programmée quand l'oxyde est claqué.)
- Ne demandent **pas de masque supplémentaire**

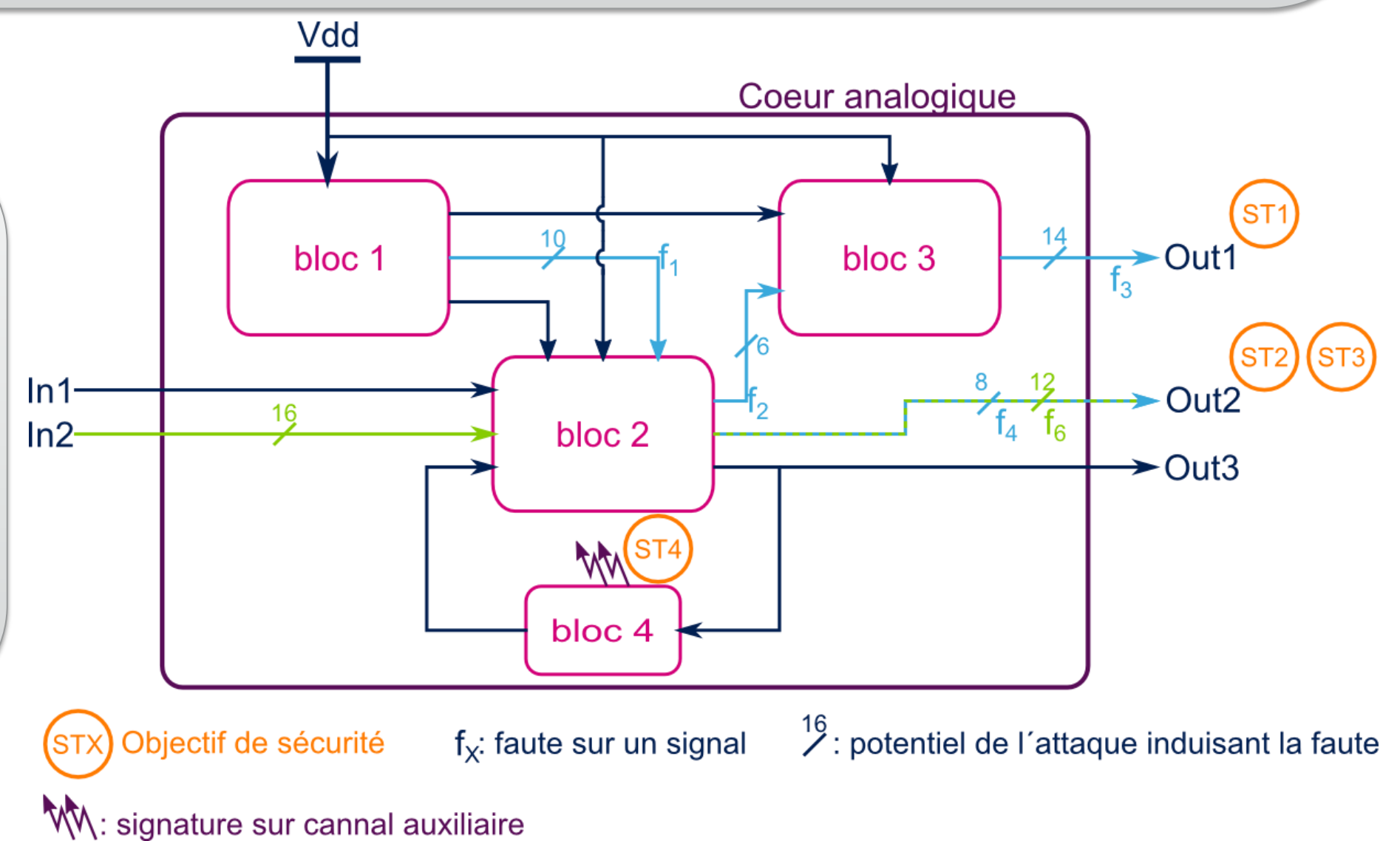


Illustration de l'analyse des vulnérabilités

Analyse des vulnérabilités des circuits analogiques

- Objectifs** : déterminer les failles d'un circuit afin d'envisager la sécurité dès la phase de spécifications et assurer le niveau de sécurité d'un circuit.
- Adaptation de la **Méthodologie Commune d'Évaluation** (CEM) proposée par les Critères Communs (CC) aux circuits analogiques
- Évaluation du **potentiel d'une attaque** afin d'identifier la **criticité des vulnérabilités**
- Travaux Publiés** : « Increasing the Security Level of Analog IPs by Using a Dedicated Vulnerability Analysis Methodology » IEEE ISQED 2013

Facteur	Ordre	Potentiel d'identification
Temps d'étude	< 0,5 heure	0
	< 1 jour	2
	< 1 mois	3
	> 1 mois	5
	Non applicable	*
Compétences	Débutant	0
	Compétant	2
	Expert	5
Connaissances de l'objet d'étude	Aucune	0
	Publique	2
	Spécialisée	5
Temps d'accès à l'objet	< 0,5 heure ou non détectable	0
	< 1 jour	2
	< 1 mois	3
	> 1 mois	4
	Non applicable	*
Équipement	Aucun	0
	Standard	1
	Spécialisé	3
	Sur mesure	5

Grille d'évaluation du potentiel d'une attaque

Perspectives :

- Classement** des attaques identifiées par niveau de criticité
- Développement de **nouvelles contre-mesures** augmentant encore le niveau de sécurité du cœur analogique de la mémoire
- Analyse des contre-mesures développées par simulations électriques et mesures sur **silicium**
- Modélisation** des principaux blocs analogiques du circuits afin de faciliter l'analyse du circuit et les effets d'une attaque