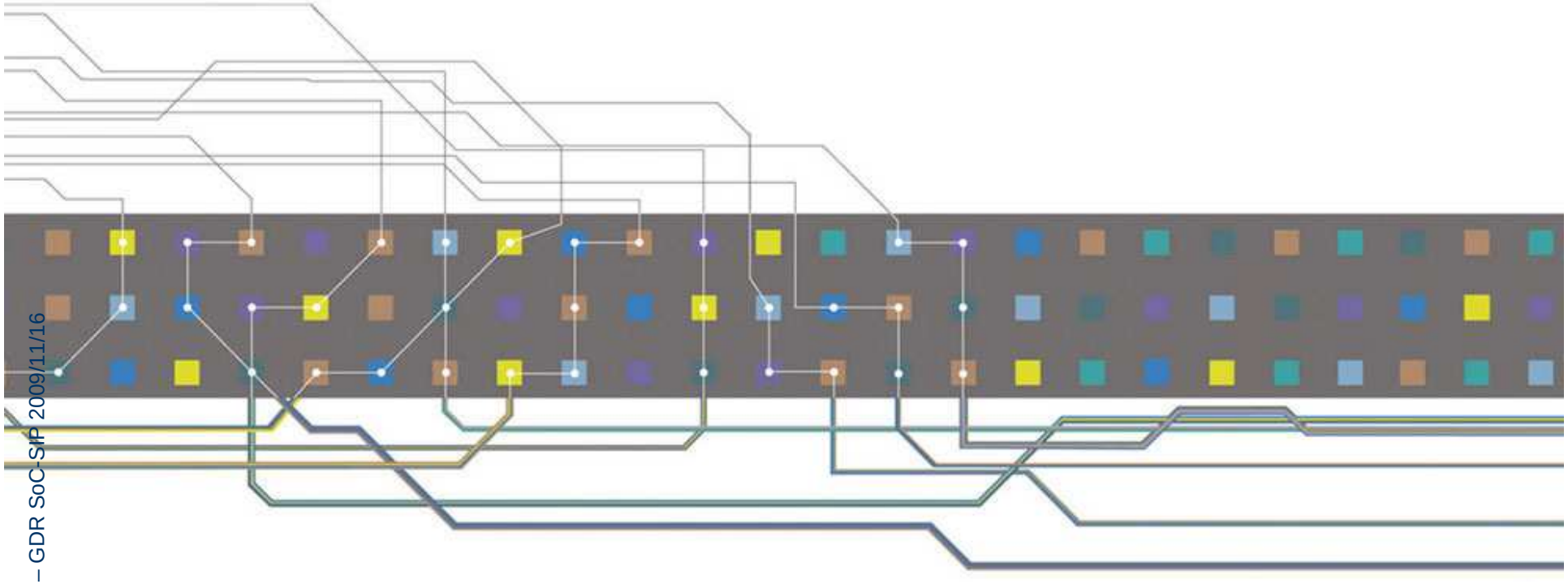
THALES



Sécurité côté “manufacturing”

Eric Saliba & Antoine Delautre

Journée Sécurité Numérique – GDR SoC-SiP 2009/11/16

Thales Systèmes Terre et Interarmées

- Recherche & développement représentant 30 % du chiffre d'affaires
- Plus de 10 000 ingénieurs, dont 4 200 chercheurs
- Plus de 1 500 brevets déposés
- Contrats de Recherche & Technologie dans plus de 15 pays
- Une stratégie collaborative avec le monde universitaire, l'industrie, les PME et la communauté des chercheurs, au niveau européen et international.
- Déploiement de technologies duales / COTS standard

Générer l'innovation, établir les standards du futur

Réponse SSI

Sécurité des réseaux

- IP
  - VPN sécurisé
  - Pare-feu
  - Passerelles
- Ethernet
- Voix
  - Voix
  - Signalisation
- Messagerie

SATCOM

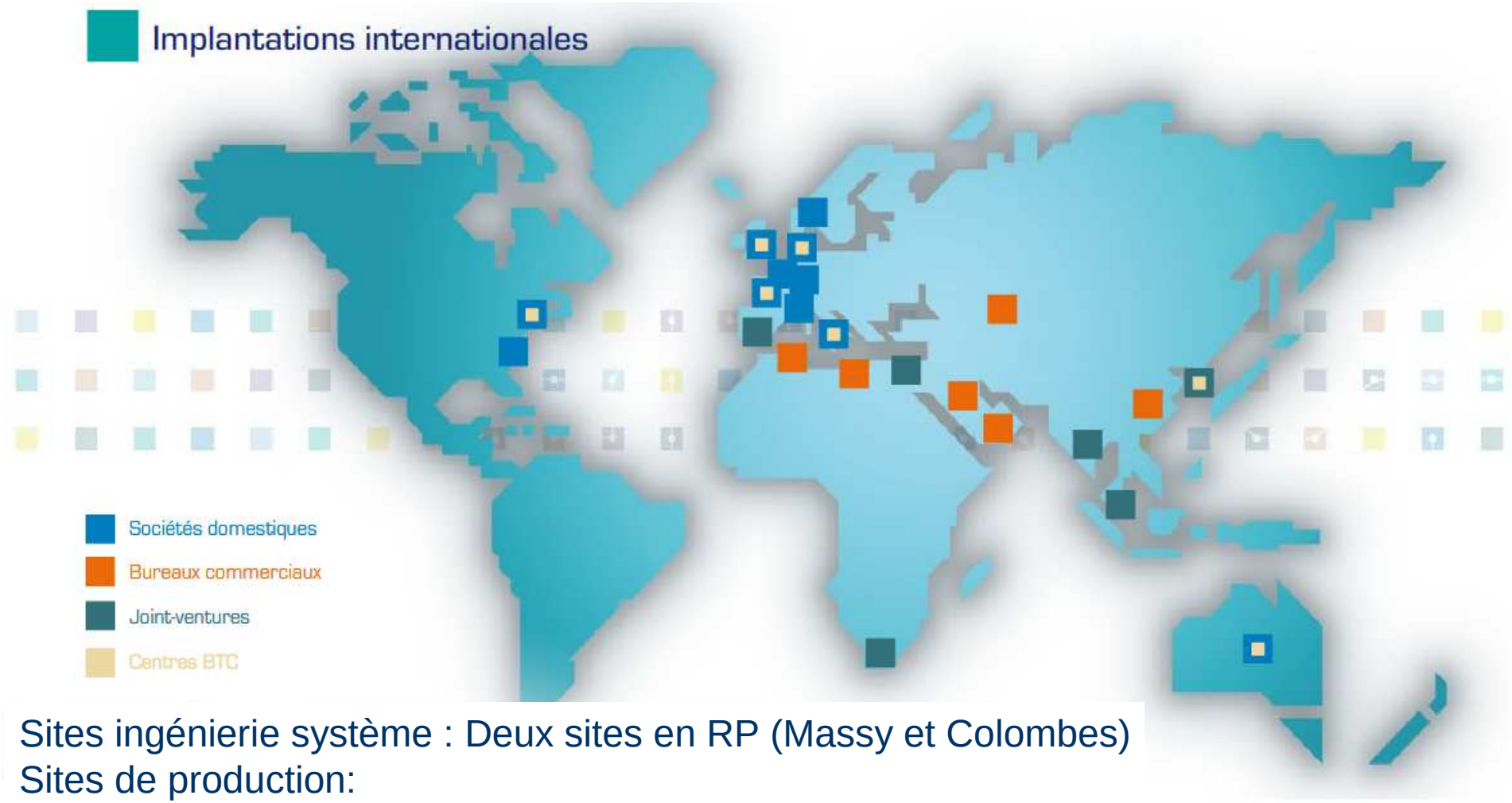
Processus et Certification

- Méthode EBIOS
- Accréditation
  - France
  - NATO
- Certification CC (EAL5+)

Système – Equipements - Composants

- SELTIC
- MUSE
- CNG mobile
- Composants Crypto Générique

Partenaire local fiable / des capacités mondiales



Sites ingénierie système : Deux sites en RP (Massy et Colombes)
Sites de production:
- Laval (aéro)
- Cholet (tactique / sécurité) : Conception équipements (dont SSI)

THALES

Sécurité et cycle de vie

Objectif : Fabriquer un équipement / système de confiance

- Une sécurité définie pour un contexte d'emploi OPE dont le niveau d'efficacité requis est déterminé en fonction du risque opérationnel
- Un niveau d'assurance de sécurité sur la réalisation des mesures de sécurité

L'efficacité n'est garantie que sous réserve d'un niveau d'assurance suffisant

- Sécurité des processus de développements et de production
- Sécurité du processus de maintenance
- Sécurité des opérations de reconfiguration

Les risques spécifiques

Compatibilité des processus de fabrication retenus avec le niveau d'assurance de sécurité requis

- Maintenir un haut niveau de protection sur l'intégrité des éléments fabriqués
  - Détérioration de l'efficacité des mécanismes de sécurité
  - Piégeage des éléments produits (logiciel / matériel)

- Maintenir un haut niveau de protection du savoir faire et des risques de collusion
  - Identification des failles inhérentes à l'implémentation
  - Besoin d'en connaître

Objectif : Garantir la confiance sur les processus de fabrication

Confiance et processus de fabrication

Maintenir un niveau de confiance sur la fabrication

- Identifier les risques spécifiques à la fabrication qui impacteront à terme l'efficacité de la sécurité opérationnelle
- Introduire des mesures couvrant les risques

Maîtrise des processus de fabrication

- L'externalisation d'activités de développement, de production et de fabrication est une réalité nécessaire pour une maîtrise des coûts et des choix technologiques standards
- Ces activités sont maitrisées au niveau des affaires pour le respect notamment des engagements client

La maîtrise industrielle de la fabrication est nécessaire mais non suffisante au maintien de la confiance sur la sécurité

THALES

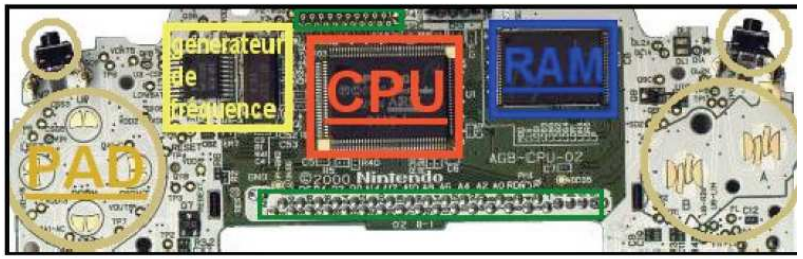
Maintenir le niveau de confiance

Des mesures spécifiques sont définies pour garantir la sécurité des processus de fabrication

- Mesures organisationnelles internes sont « étendues » vers les sous-traitants
- Le niveau de maîtrise des contrôles de sécurité doit toutefois être formalisé et contractualisé
- Les moyens de contrôle doivent être en cohérence avec le niveau de confiance recherché
- Le choix d'un sous-traitant est instruit en fonction du risque portant sur l'élément externalisé

Introduire des mesures permettant le contrôle de la sécurité des processus de fabrication

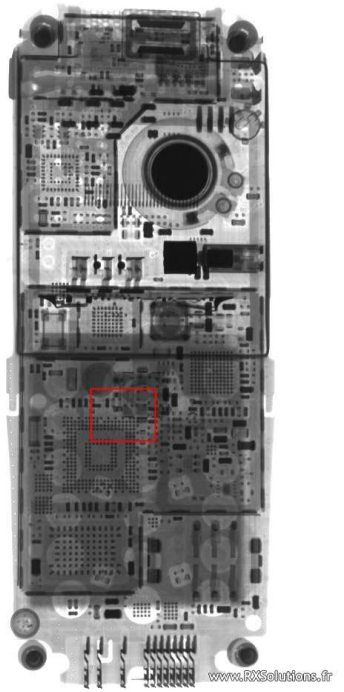
Exemple de moyens de contrôle



Source internet

Contrôle du matériel

- Inspection visuelle des circuits électroniques,
- Identification des composants pour en vérifier leur intégration,
- Analyser la continuité des pistes sur les cartes électroniques
- Application de signaux précis / anomalies à des endroits précis afin d'observer le comportement du système



Exemple de tomographie 3D au rayons X (scan d'un GSM) – source internet

THALES

« éclatement » de la problématique

Les processus de fabrication d'un équipement sont répartis auprès de différents partenaires, dont notamment

- Constructeurs des plates-formes matérielles
- Fournisseurs des éléments de (re)configuration (ex. FPGA)
- Fournisseurs des briques logicielles

L'équipement est le résultat de l'assemblage de ces différents éléments

- La problématique de confiance est répartie auprès des différents partenaires
- Maîtrise distribuée / confiance répartie

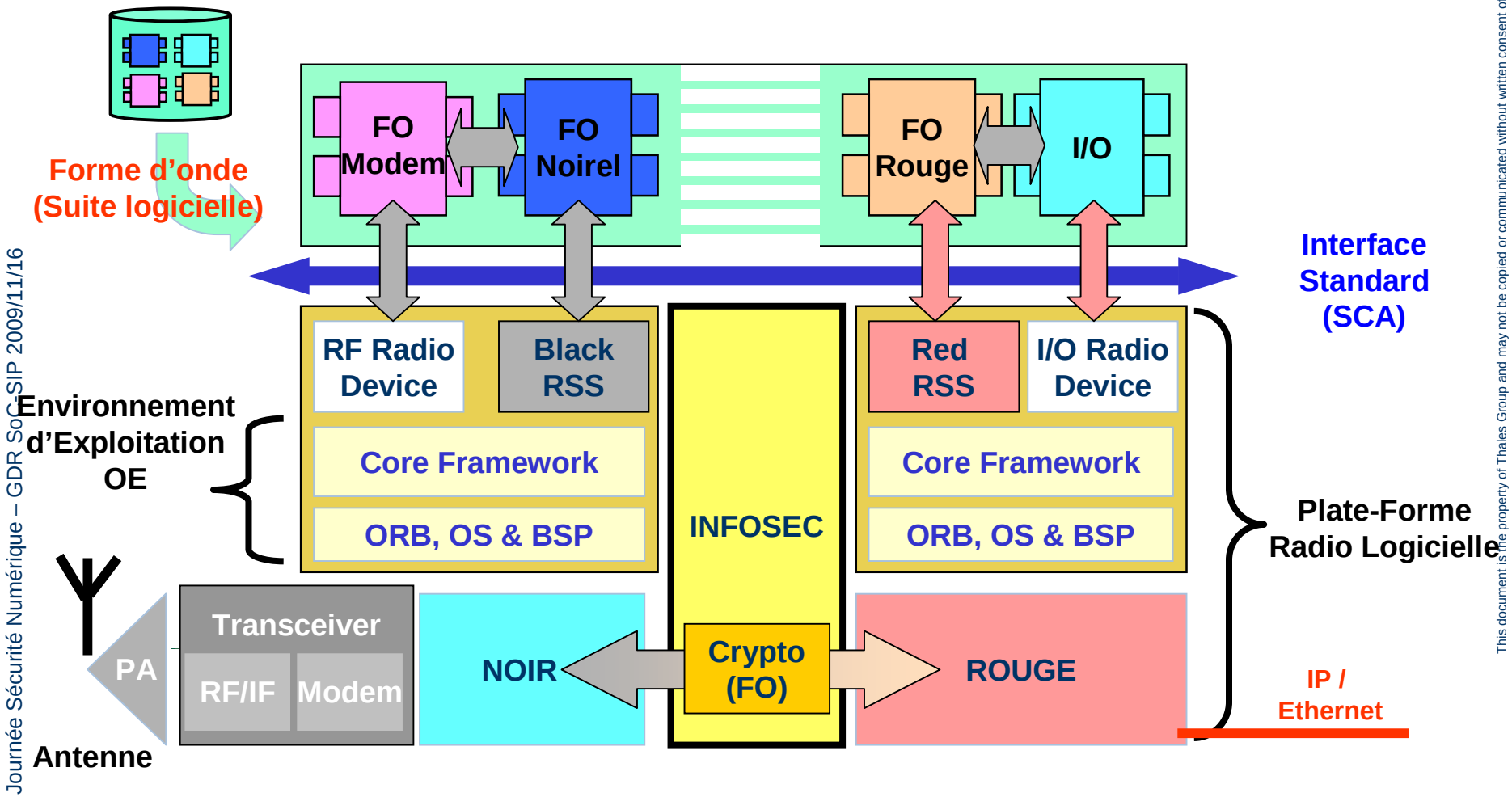
Exemple : La radio logicielle

Plate-forme matérielle sur laquelle des éléments de configuration viennent « finaliser » le produit avant emploi opérationnel

- Une plate-forme peut accueillir différents éléments de configuration pour donner plusieurs produits
- Les fournisseurs des éléments de configuration s'appuient sur la plate-forme pour réaliser les services attendus (dont la sécurité)

Confiance mutuelle entre la plate-forme et les éléments de configuration

Schéma de la radio logicielle



THALES

Mécanismes permettant de garantir le maintien du niveau de confiance visé

- La maîtrise forte des éléments pouvant être chargés sur la plate-forme
- La maîtrise forte du chargement des éléments sur une plate-forme cible authentique

Maîtrise forte

- Basée sur des caractéristiques spécifiques à la plate-forme (non clonables)
- Basée sur des moyens cryptographiques

Alternative PUF

L'exploitation des PUF est une alternative candidate au besoin

Caractéristiques liées à la plate-forme

- Primitive qui transforme des défis Di en réponses Ri
  - Ri fortement tributaire des propriétés physiques de la plate-forme dans laquelle le PUF est embarqué

Mise en œuvre de solutions cryptographiques

- Exploiter les réponses Ri pour générer des clés cryptographiques
  - La clé générée est directement liée aux caractéristiques physiques de la plate-forme
  - Pas de stockage de clés mais génération à l'emploi

Définition des protocoles « d'enrôlement » et « de contrôle » mis en œuvre dans le cadre des processus de fabrication

Contraintes

Choix du PUF

- Dépendant du matériel dans lequel il est embarqué (ASIC, FPGA, mémoire…)

Blocs complémentaires au PUF

- Définition d'un ensemble de primitives permettant la génération de clés cryptographiques sur la base d'une Ri
  - Tolérance au bruit
  - Extraction d'aléas
- Compatibilité avec le design
  - Evolution des composants du design (changement de fournisseur ou de gamme) ?
  - Surcoût en ressources physiques (dans les composants)?
  - Surcoût budget (consommation) ?
  - Intégration dans le flow de conception ?

Travaux complémentaires

Travaux « Académiques »

- Quelle modélisation mathématique ?
- Quelle complexité du modèle physique ?
- Quel effort de clonage ?

Travaux d'industrialisation

- Tenue en environnement d'emploi comme le tactique ou l'aéronautique (température et vibrations)
- Compatibilité à la durée de service de l'équipement
- Reproductibilité de la génération d'aléa (Identifier la sensibilité de l'élément physique aux variations de son environnement)

Synthèse des pistes d'étude

Adéquation du PUF avec une fonction d'authentification

- Génération du secret lors du processus de fabrication
- Processus de fabrication intégré à l'objet
- Pas de source d'énergie spécifique nécessaire
- Réduction du besoin d'architecture cryptographique à mettre en place (ex. IGC)
- Indépendance de l'équipement cible

Utilisation de la propriété de résistance physique d'une PUF à la modification

- Modification de l'environnement (ex. température)
- Modification de la structure (ex. introduction d'une sonde)
- Modification de l'intégrité (ex. modification de circuit électronique)

Le caractère aléatoire de la variable physique est mis à profit pour générer un aléa

- Contribution à la procédure de génération d'aléa
- Personnalisation implicite, simplification de l'introduction du secret initial
- Suppression du stockage numérique de l'information

Conception équipement

L'analyse de sécurité doit être menée lors de la définition de l'équipement en incluant le processus de fabrication envisagé

L'architecture de l'équipement doit intégrer les contraintes de sécurité liées à sa fabrication

Dans le périmètre direct des développements

- Sous-traitants
- Approvisionnement et fournisseurs

Dans le périmètre affaire

- Co-traitants et partenariat

Recherche d'équilibrage

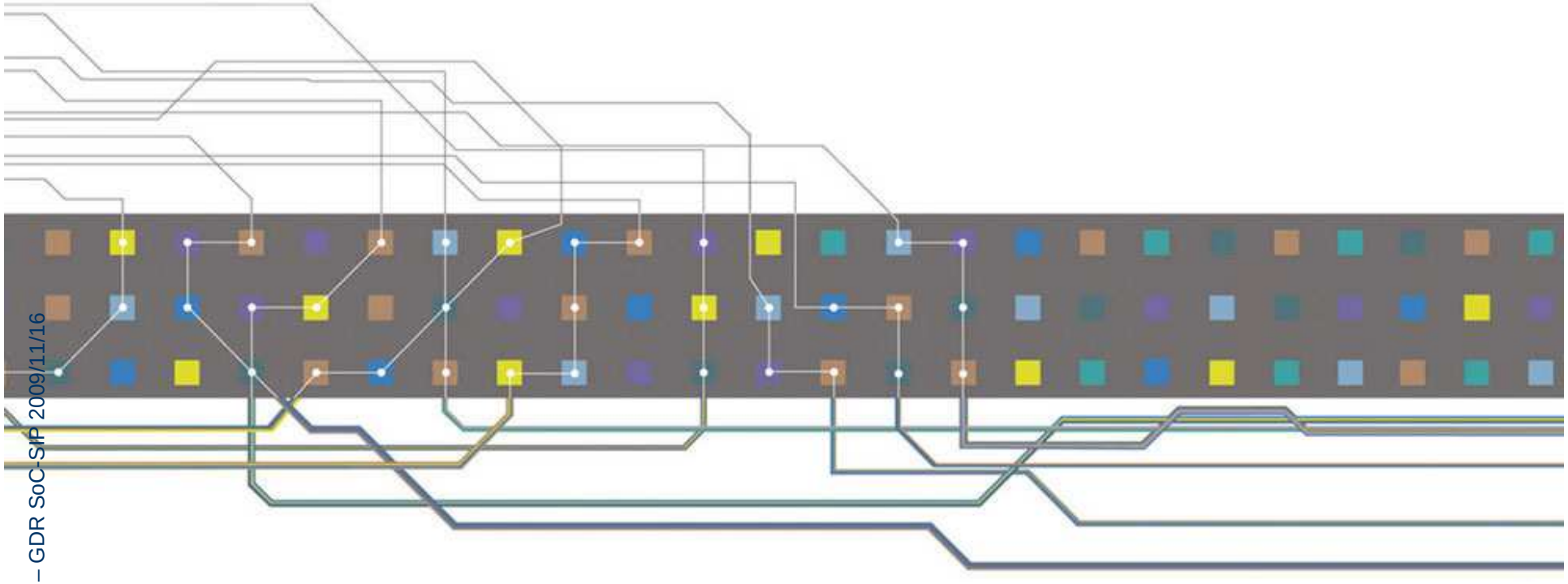
Les menaces identifiées sur le périmètre du processus de fabrication doivent être ramenées sur le périmètre du risque opérationnel

La capacité de nuisance d'éléments malveillants introduits en fabrication reste à démontrer en terme de réalisation ou mise en œuvre au regard des risques inhérents au contexte d'emploi

Les mesures retenues pour la sécurisation du processus de fabrication doivent être mises en rapport des coûts et délais de fabrication

Les approches retenues dans le domaine de la sureté de fonctionnement sont des alternatives complémentaires permettant de réduire les risques sur l'approvisionnement d'éléments non maitrisés

THALES



Eric.Saliba@fr.thalesgroup.com
Antoine.Delautre@fr.thalesgroup.com