Présentation du travail sur le sujet proposé par THALES

Dmitriy Slutskiy, Daria Stépanova, Simon Stuker

8 Juin 2012

Introduction

- Les puces électroniques sont partout !
- Leur production coûte cher.

Conséquence : RD en France, fabrication ailleurs.
Dangers :

- qualité de fabrication
- sécurité

Problème de vérification

- Comparer le modèle numérique avec l'échantillon
  - milliards de connections minuscules à vérifier
  - milliers de photos à haute résolution (cher et lent).

Exemple

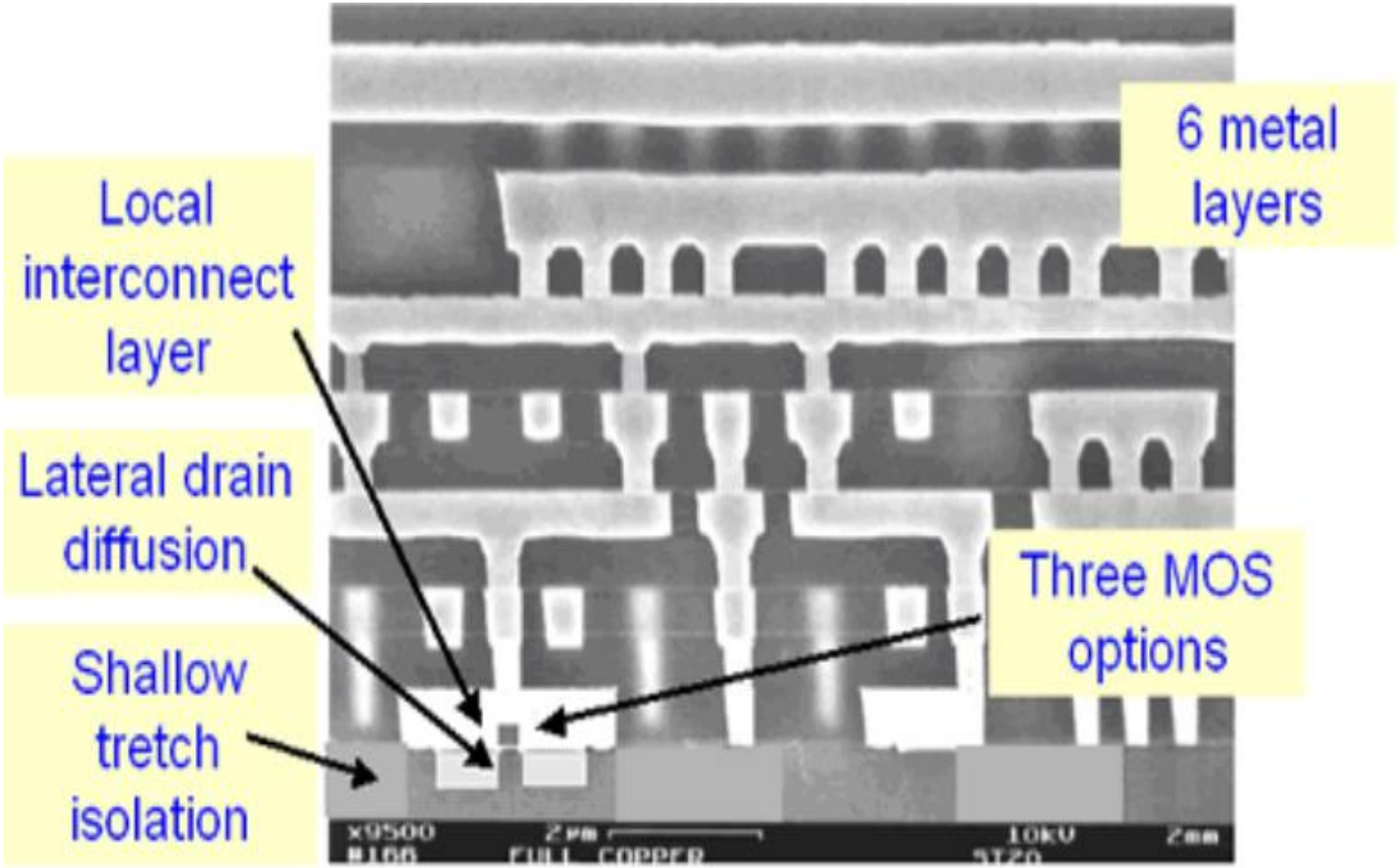
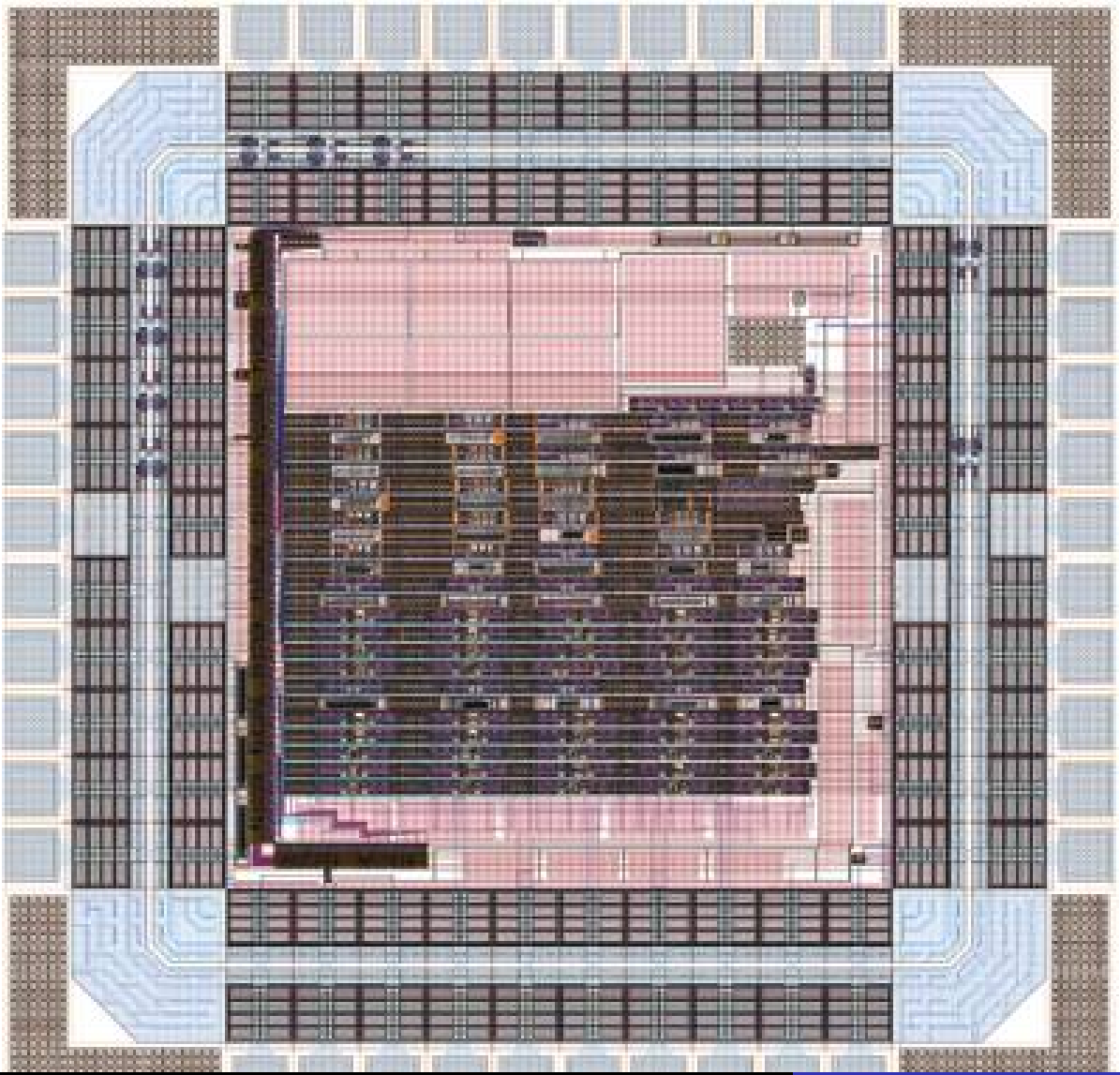

Local interconnect layer
Lateral drain diffusion
Shallow tretch isolation
6 metal layers
Three MOS options

Image par rétroingénierie



La tache

Déterminer les zones les plus importantes sur la puce à vérifier

- densité de graphe logique (composantes connexes, densité de connections)
- densité géographique (physique) du circuit électrique dans le circuit intégré.

On peut extraire cette information du modèle numérique de la puce.

Lecture d'un fichier .cif

CIF (Caltech Intermediate Format) format utilisé pour la description des schémas integrés.

- formes géométriques simples (2D) sur les différentes couches d'une puce ;
- description hierarchique ;
- format textuel ;
- géométrie à très grande échelle (VLSI)

Géométrie

- LAYER (L) passage entre couches ;
- BOX (B) mettre un rectangle ;
- WIRE (W) mettre un chemin ;
- ROUNDFLASH (R) mettre un cercle ;
- POLYGON (P) mettre une figure arbitraire ;
- CALL (C) mettre un symbole contenant d'autres déclarations géométriques

Contrôle

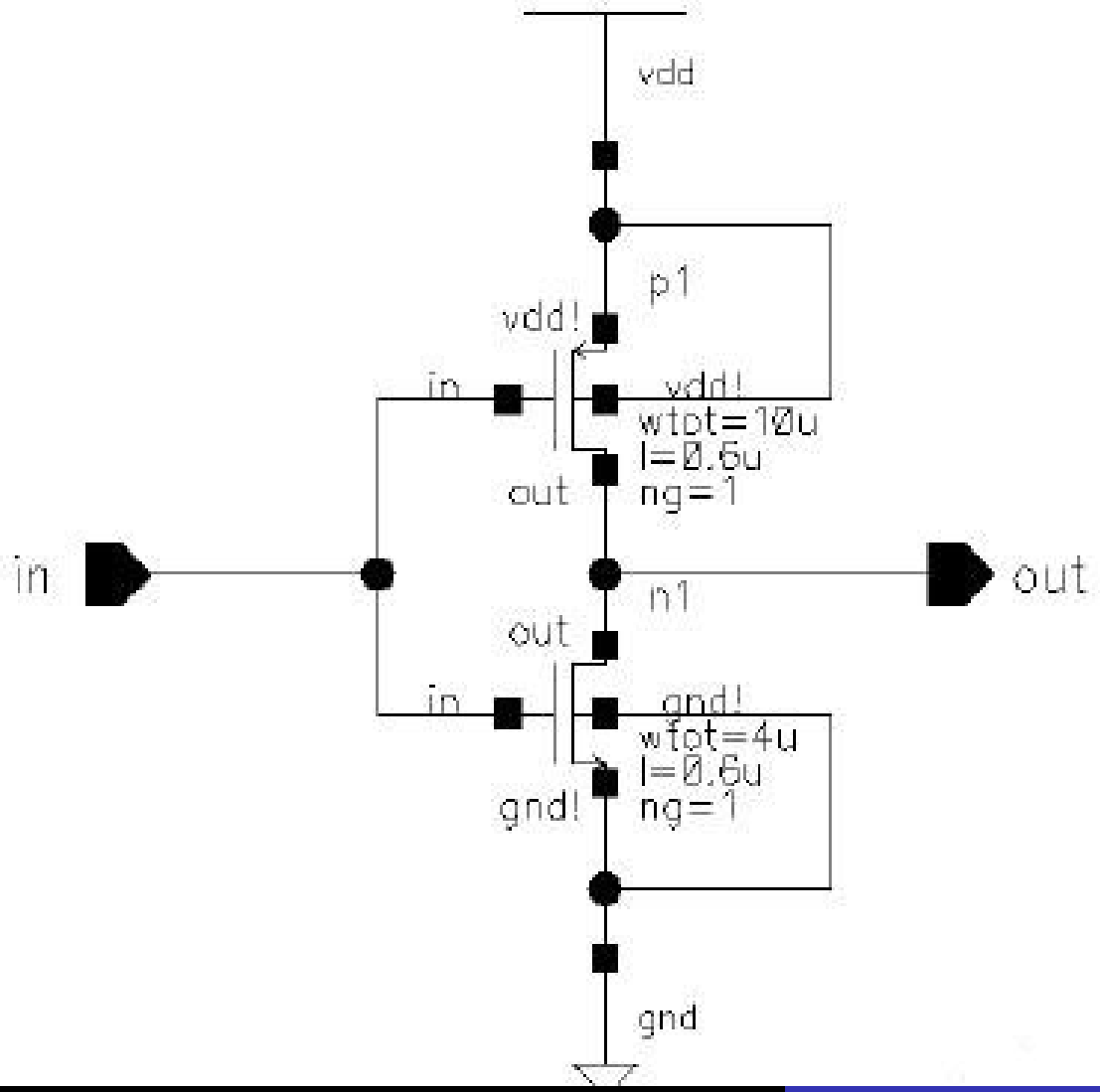
- DS début de la définition d'un symbole ;
- DF fin de la définition d'un symbole ;
- supprimer la définition de sousroutages ;
- 0 à 9 pour inclure une information supplémentaire ;
- END (E) pour terminer un fichier CIF

Exemple (CIF file for Inverter cell)

```
DS 1 1 1;
9 Inverter;
L NWELL;
B 760 1360 380,1680;
L PPLUS;
B 480 200 400,250; B 420 1080 410,1680;
L DIFF;
B 400 540 400,460; B 540 1000 310,1680;
L NPLUS;
B 480 420 400,560; B 200 1080 100,1680;
L POLY1;
B 520 60 400,550;B 140 140 70,560; B 140 140 360,1050;B 60 1120 400,1680;
L CONTACT;
B 60 60 280,260;B 60 60 400,260;
B 60 60 520,260;B 60 60 280,440; B 60 60 400,440;B 60 60 520,440;
B 60 60 280,660;B 60 60 400,660; B 60 60 520,660;B 60 60 110,2100;
B 60 60 110,1980;B 60 60 110,1860; B 60 60 110,1740;B 60 60 110,1620;
B 60 60 110,1500;B 60 60 110,1380; B 60 60 110,1260;B 60 60 290,2100;
B 60 60 290,1980;B 60 60 290,1860; B 60 60 290,1740;B 60 60 290,1620;
B 60 60 290,1500;B 60 60 290,1380; B 60 60 290,1260;B 60 60 510,2100;
B 60 60 510,1980;B 60 60 510,1860; B 60 60 510,1740;B 60 60 510,1620;
B 60 60 510,1500;B 60 60 510,1380; B 60 60 510,1260;B 60 60 360,1050; B 60 60 70,560;
L METAL1;
B 360 120 400,660;B 120 120 70,560;B 120 120 360,1050;B 120 960 510,1680;
B 300 960 200,1680; B 300 130 200,2225;B 760 200 380,2390;B 110 120 635,660;
B 120 1440 630,1440;B 120 370 70,805; B 360 300 400,350;B 300 120 150,1050; B 760 200 380,100;
DF;

C 1;E
```

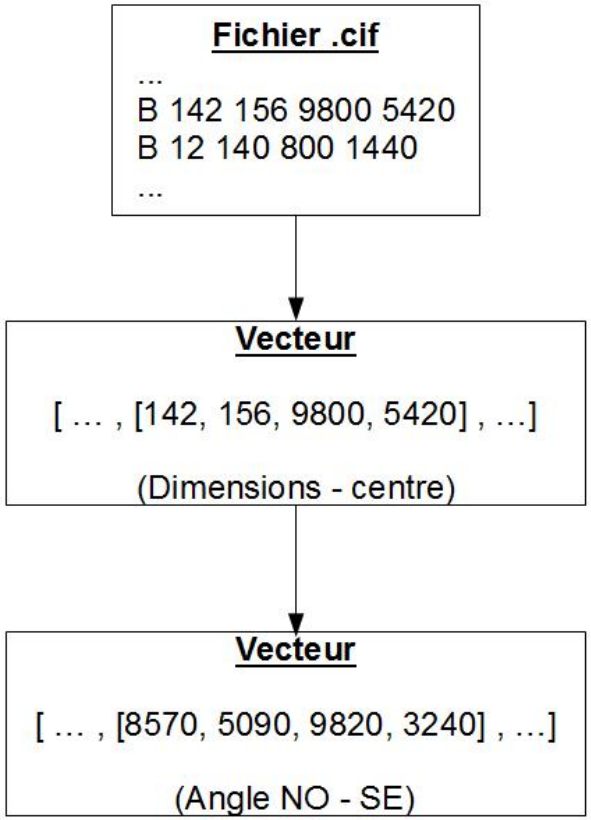
Inverseur


vdd
p1
vdd!
in
vdd!
wtot=10u
l=0.6u
out
ng=1
in
out
n1
out
in
gnd!
wtot=4u
l=0.6u
gnd!
ng=1
gnd

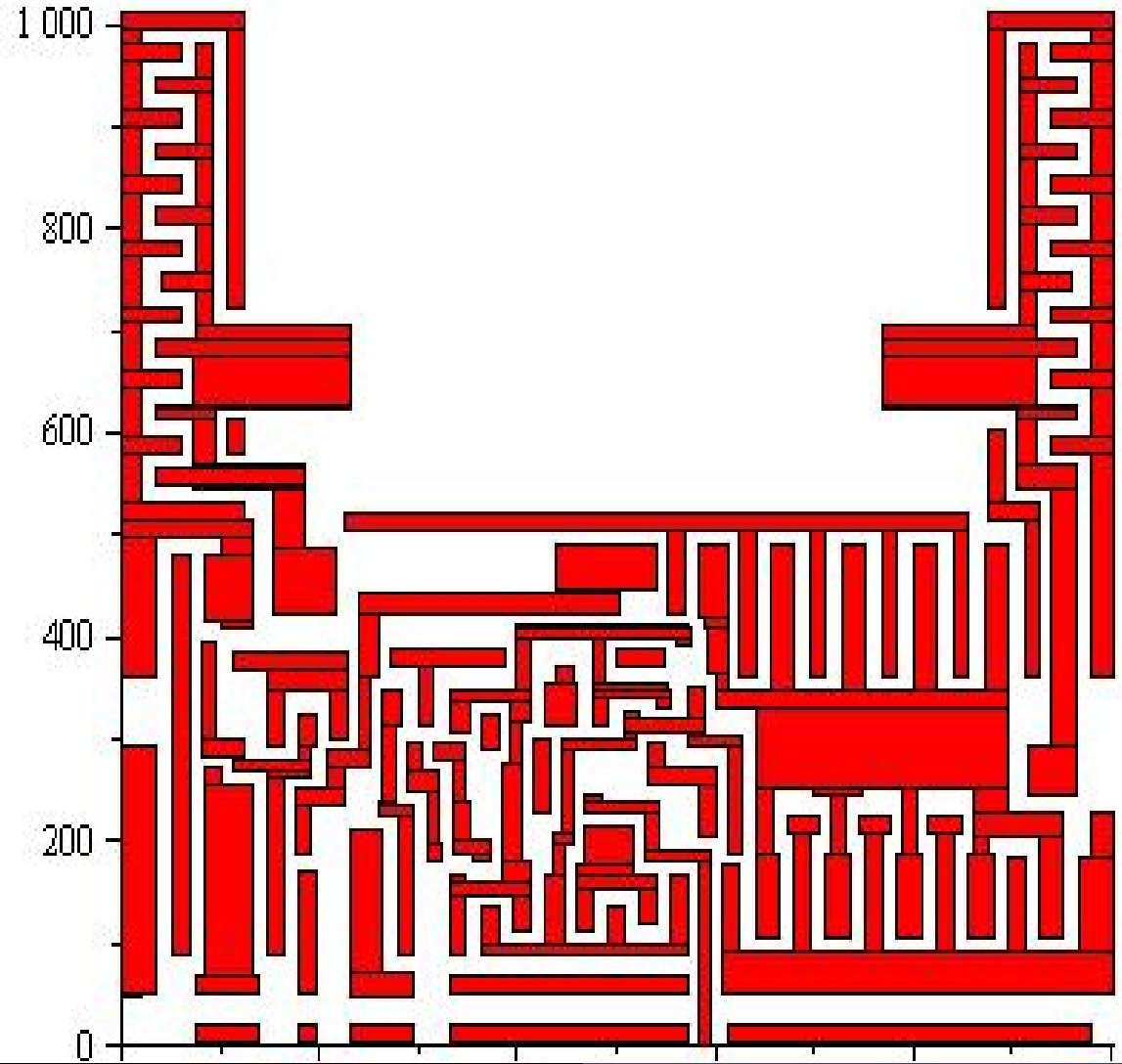
Adaptation pour le traitement mathématique

- Extraction de couches et leur prétraitement :
  - éditeur de texte ;
  - scripts pour extractions de données nécessaires et leur reorganisation
- mise en format lisible par les logiciels de calcul :
  - adaptation du langage pour MAPLE (Mathlab, Matematica, pari gp etc)
  - optimisation du format par les logiciels

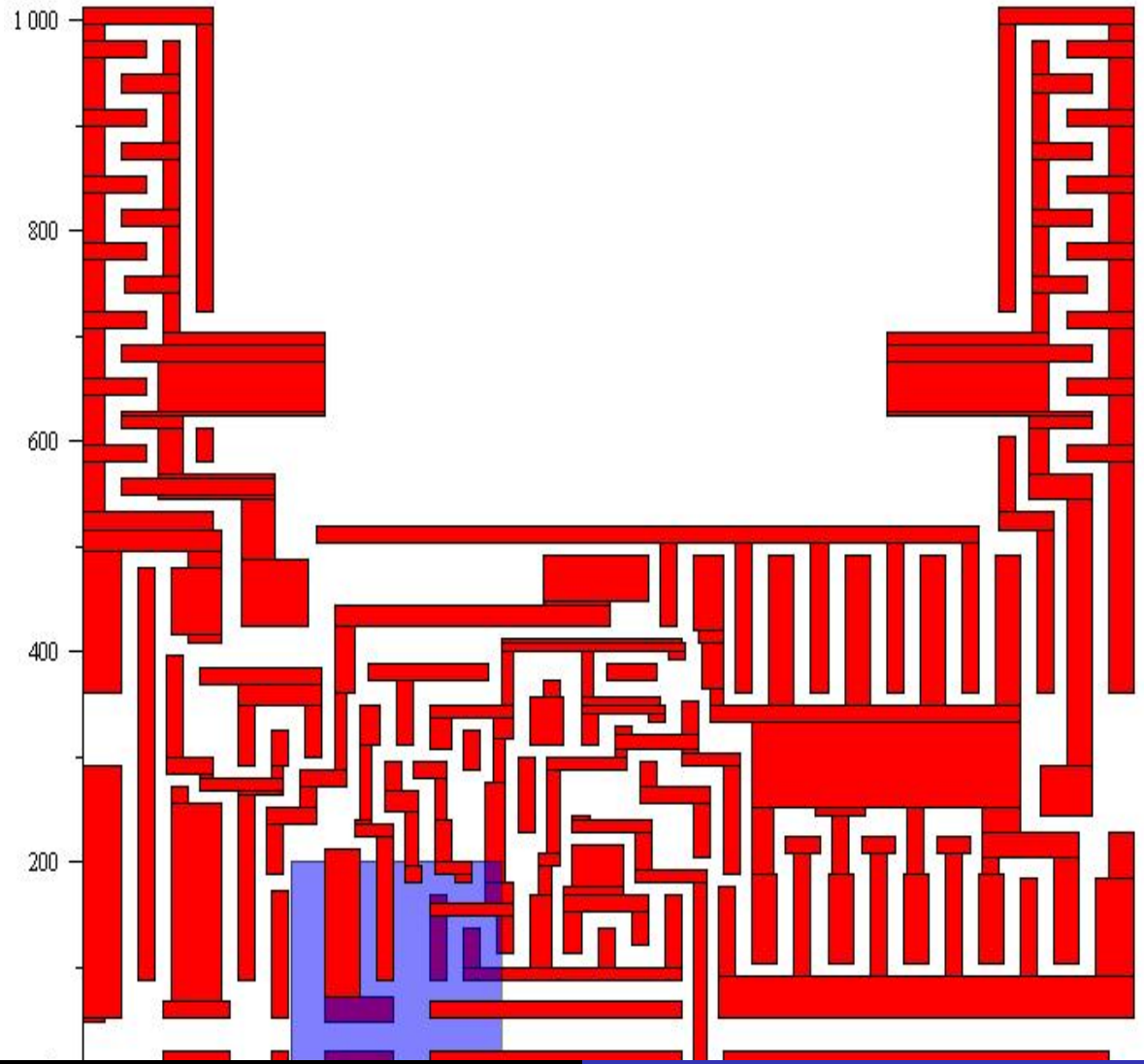
Prétraitement



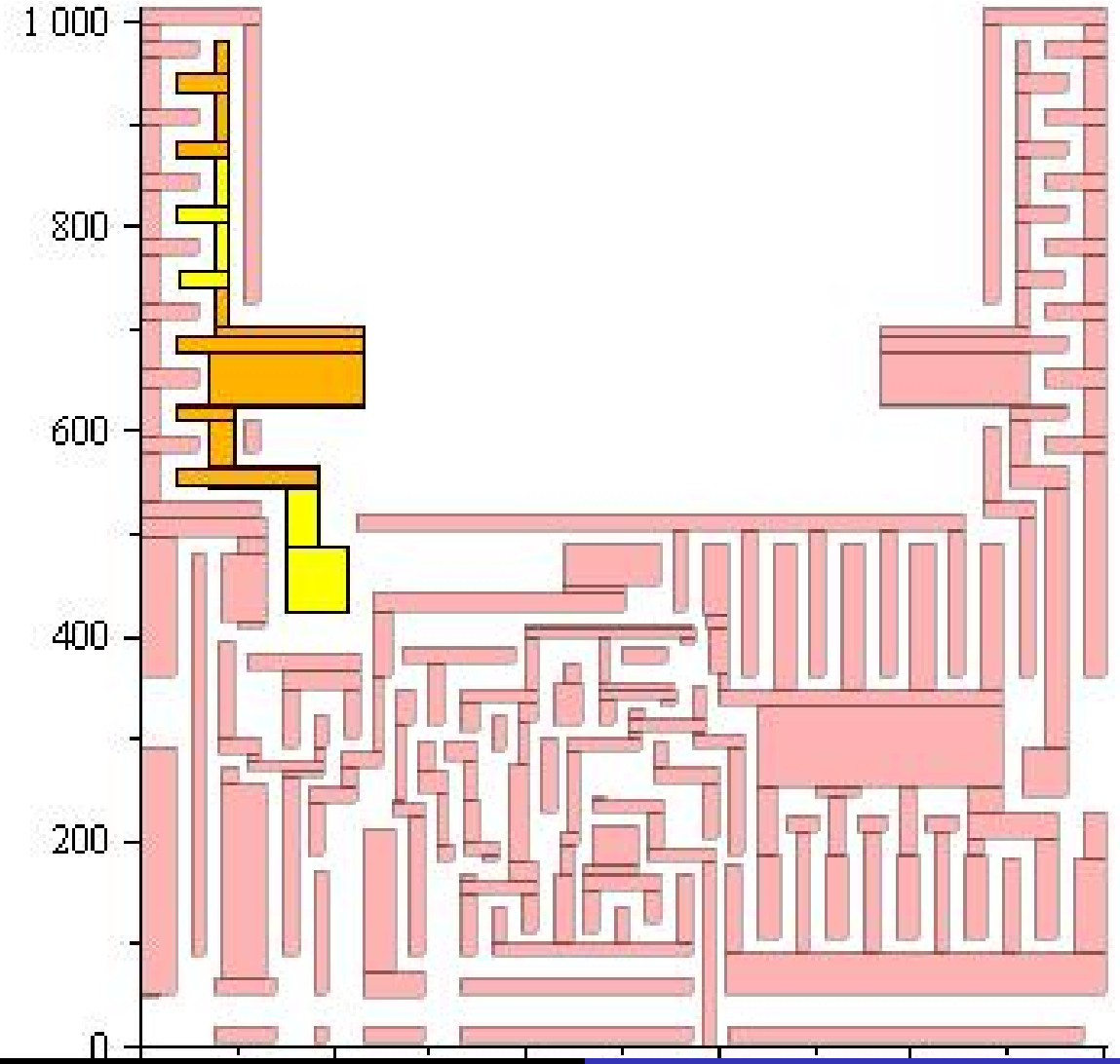
Affichage/vérification



Densité d'une zone



Adjacence et composantes connexes



Détermination des zones à risque.

Contraintes du producteur malveillant :

- **Spatiales :** Trouver une zone de...
- **Logiques :** Connexion à l'horloge, à l'alimentation...

Deux types de topologies à étudier/rapprocher :

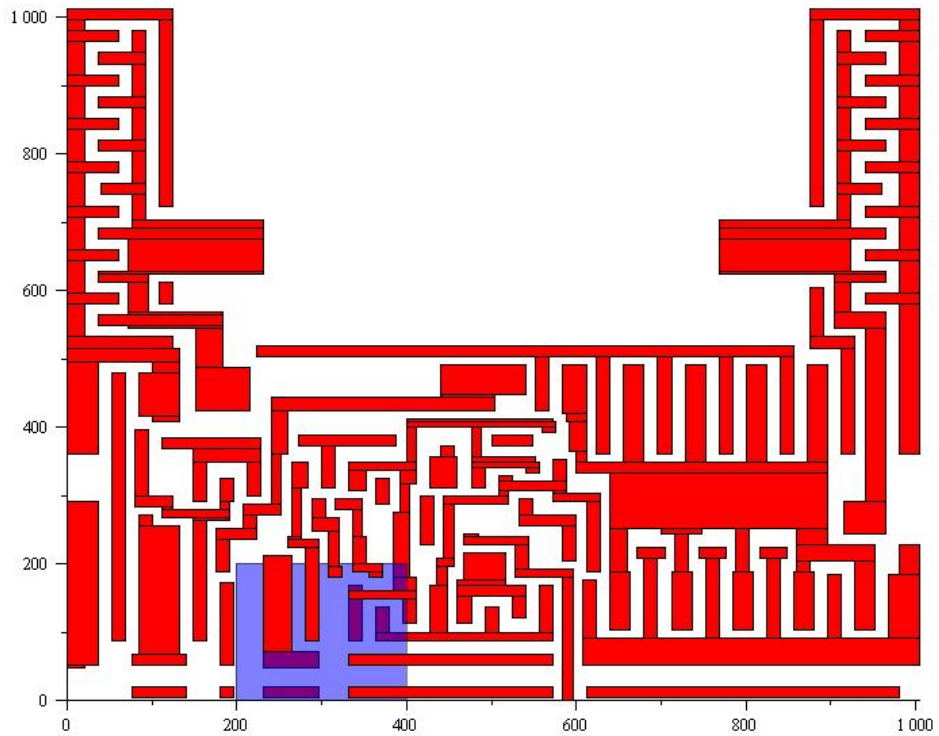
- La topologie géographique. (voisins dans l'espace)
- La topologie logique. (interconnectés)

Les zones à risque sont celles où ces deux topologies divergent :

- faible densité de cuivre
  ET
- forte connexité

Analyse spatiale.

Critère : quelles sont les zones suffisamment désertes pour pouvoir y implanter un composant supplémentaire en évitant l'isolement total ?



Analyse du graphe de connexion

Comment modéliser les connection par un graphe ?
Noeuds = vias , Arcs = connexions ou l'inverse ?
Les graphes auront des propriétés duales.
Pondération : par longueur, surface occupée ,... ! ?

Comment quantifier la sensibilité/richesse de la partie d'un graphe ?

- Fort degré (nombre d'arcs sortant d'un noeud), dégré moyen local.
- Diamètre / Longueur moyenne d'un chemin dans une zone.
- Partition du graphe en quelques parties faiblement interconnectées.

La sensibilité d'un noeud peut également être précisée par le concepteur. Entrées / sorties "utiles" à un cheval de Troie.

Analyse statistique

"Double" échantillonnage :

- Les composants sont détruits pendant la vérification. Limiter le nombre de composants testés sur un lot.
- On ne peut vérifier qu'une partie de chaque composante. Comment se prononcer sur ce qui n'a pas été vérifié ?

Le premier échantillonnage est classique :

n composants d'un lot de N adéquats $\Rightarrow$ la proportion de composants adéquats du lot est situé dans l'intervalle

$$[\frac{n}{N} - \frac{1}{\sqrt{N}}; \frac{n}{N} - \frac{1}{\sqrt{N}}]$$

avec une probabilité $\geq 95\%$.

(Si $n \geq 25$ et $0,2 \leq \frac{n}{N} \leq 0,8$)

Echantillonnage sur une plaquette.

Quelle confiance inspire l'adéquation d'une zone ?

- Simplement une proportion d'aire / connexions adéquates ?
- Quantifier le risque d'une zone ?

"La vérification d'une zone à gros risque assure l'adéquation à 90% du circuit."

Le risque est une fonction de :

- la densité de cuivre,
- connectique,
- dimensions du cheval de Troie recherché,
- ...

Pistes

- Appliquer les algorithmes proposés sur un exemple réaliste.
- Quantifier le rique d'une zone selon le composant malveilant recherché.
- Restreindre l'étude connectique à 3 niveaux successifs (via compris) pour réduire la complexité.

Difficultés prévisibles et lacunes éventuelles

- Complexité calculatoire qui explose. (Composante connexe)
- Impossibilité de calculer des invariants locaux du graphe, s'il est très étendu.
- Implanter un cheval de Troie est aussi difficile que d'implanter une nouvelle fonctionnalité. Des solutions existent peut-être déjà ?