

# Parcours pré-thèse et début de thèse

**Nicolas Gaudin**

Projet SCRATCHS

Lab-STICC, Lorient



# Pré-thèse

- DUT GEII, IUT Montpellier



- Ingénieur Microélectronique et Automatique, Polytech Montpellier
  - Spé Microélectronique
  - VHDL, C, microcontrôleur, architecture des processeurs
  - 5A en alternance chez STMicroelectronics



# STMicroelectronics



Site de Rousset



Fabrication



Test



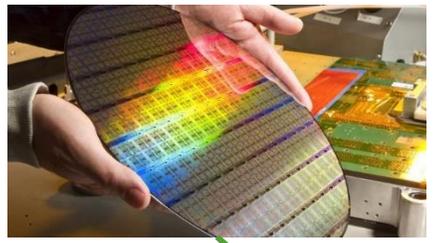
Divisions

Microcontroller Division

- Design
- Marketing
- Quality
- **Test & product Engineering**
- ...

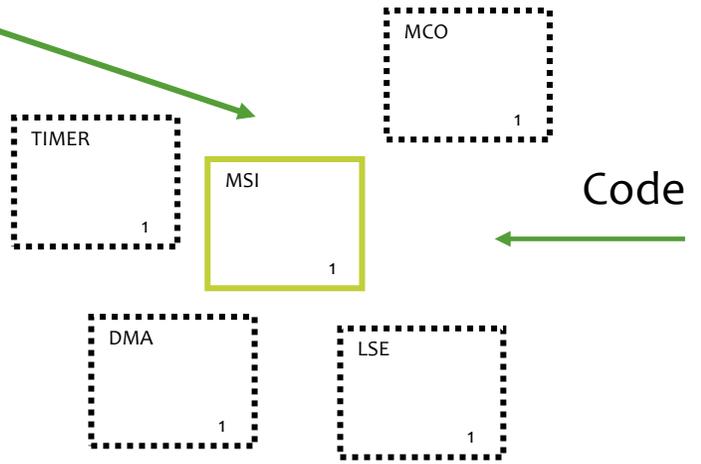
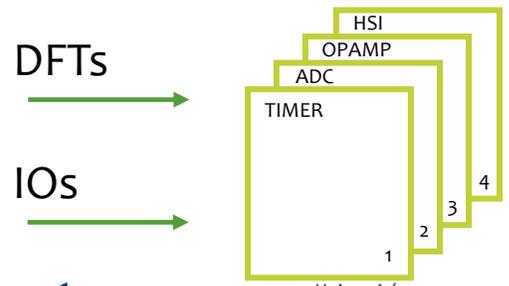


# Tests des STM32



Standalone

SoftBIST

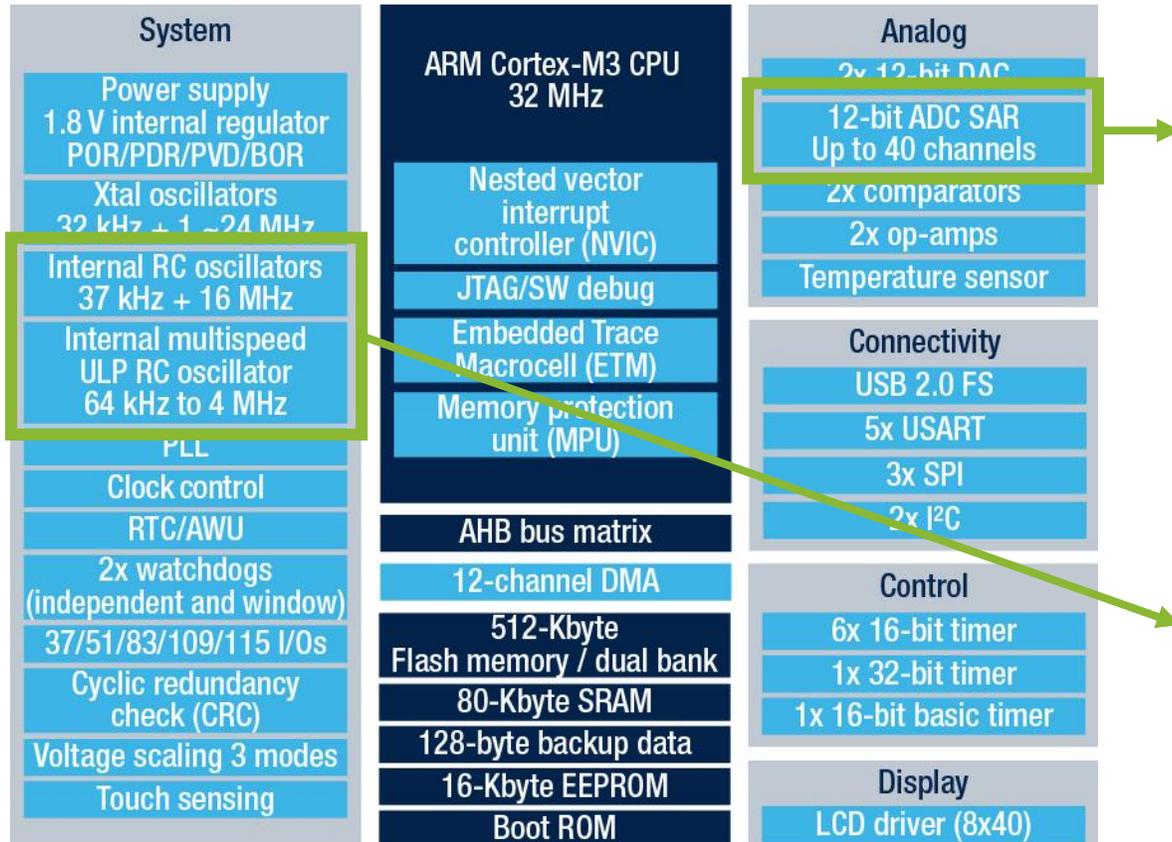


- Contraintes de coût → temps
- Fiabilité des tests



# Définition des projets

## Périphériques de la STM32



## Génération de signaux analogiques

- Test des ADCs
  - Précision de signal (*ENOB*)
  - Temps de génération
  - Coût matériel
  - Portabilité

## Calibration des horloges internes

- Donner la valeur d'étalonnage
  - Fiabilité
  - Temps de test
  - Généricité
  - Portabilité

# Formations

- RISC-V
  - Introduction à la toolchain
  - Cible: Basys3 (Artix-7)
- Objectif : Manipuler les parties des processeurs CV32.. en les modifiant pour avoir plus d'aisance lors des futurs manipulations

# Lectures

- Surveys :
  - Attaques de temps sur les microarchitectures
  - Sécurité sur RISC-V
- Mémoires caches
  - Fonctionnement, hiérarchisation, interaction processeur/cache/mémoire, ...
  - Article sur l'évaluation de caches aléatoires

# Lectures

- RISC-V
  - Article sur un ISA sans aucunes dépendances
- Attaques par canaux auxiliaires/cachés
  - Articles sur différentes méthodologies permettant d'attaquer les caches
    - ciblés sur la crypto, les caches et d'autres organes des processeurs (prefetcher, TLB ...)