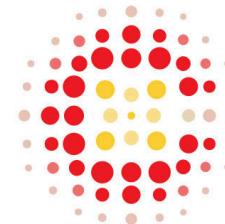


Implémentation de contremesures contre les attaques en température sur cible FPGA

Stage PFE au LCIS (février-juillet 2025)



LCIS

**Laboratoire de Conception
et d'Intégration des Systèmes**

GUERIN Enzo, BEROULLE Vincent, HELY David

Lundi 23 juin 2025

Table des matières

I.	Introduction	2
II.	Objectifs de mon travail	4
III.	Analyse théorique des modules	6
IV.	Implémentations et validations des modules	15
V.	Campagne expérimentale	27
VI.	Conclusion & perspectives	32
VII.	<u>Questions</u>	34

I. Introduction

Introduction

Contexte

Multiplication et diversification des attaques matérielles sur systèmes embarqués.
Focalisation ici sur les Power-Off Temperature Attack (POTA).
Besoin de détection pour protéger de ces dernières.

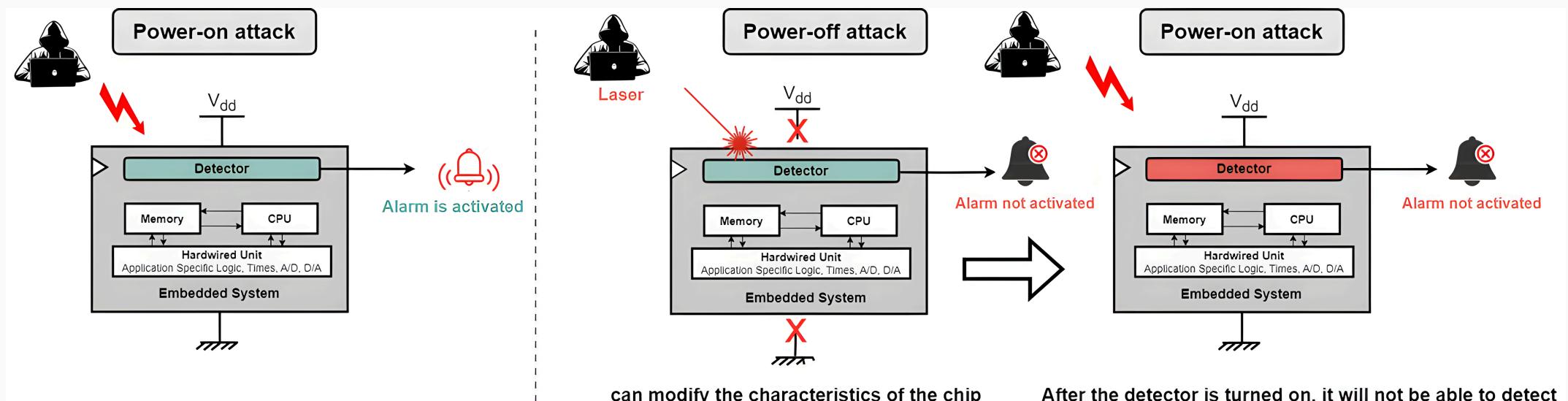


Fig. 1. – Représentation d'une attaque POTA sur le détecteur d'un système embarqué.

II. Objectifs de mon travail

Objectifs de mon travail

Objectifs

Détection des POTA sur un FPGA.

Mise en place d'un module d'auto-test (ATM) pour tester intégrité détecteur en permanence.
Implémentation et tests du détecteur et de l'ATM.

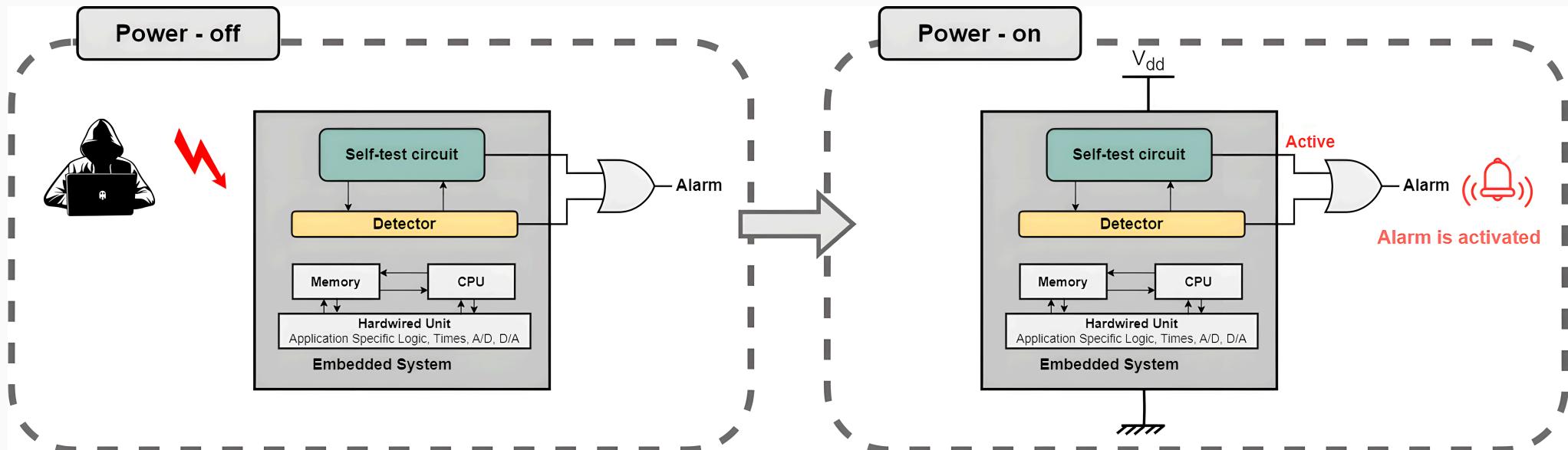


Fig. 2. – Représentation d'une attaque POTA avec un module d'auto-test implémenté.

III. Analyse théorique des modules

Fonctionnement du détecteur

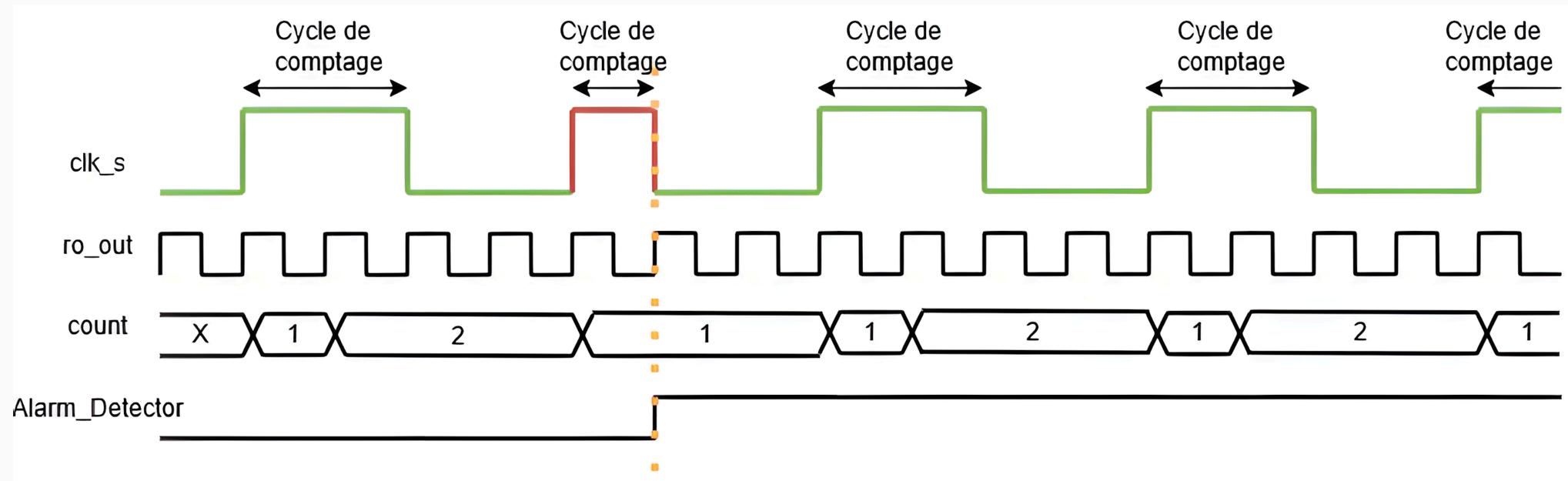


Fig. 3. – Chronogramme détaillant le fonctionnement du détecteur.

Rôle & hypothèse

- Le détecteur doit vérifier que **clk_s** ne subit pas de glitches.
- Le signal **ro_out** doit fonctionner dans les zones opérationnelles définies.

Fonctionnement de l'ATM

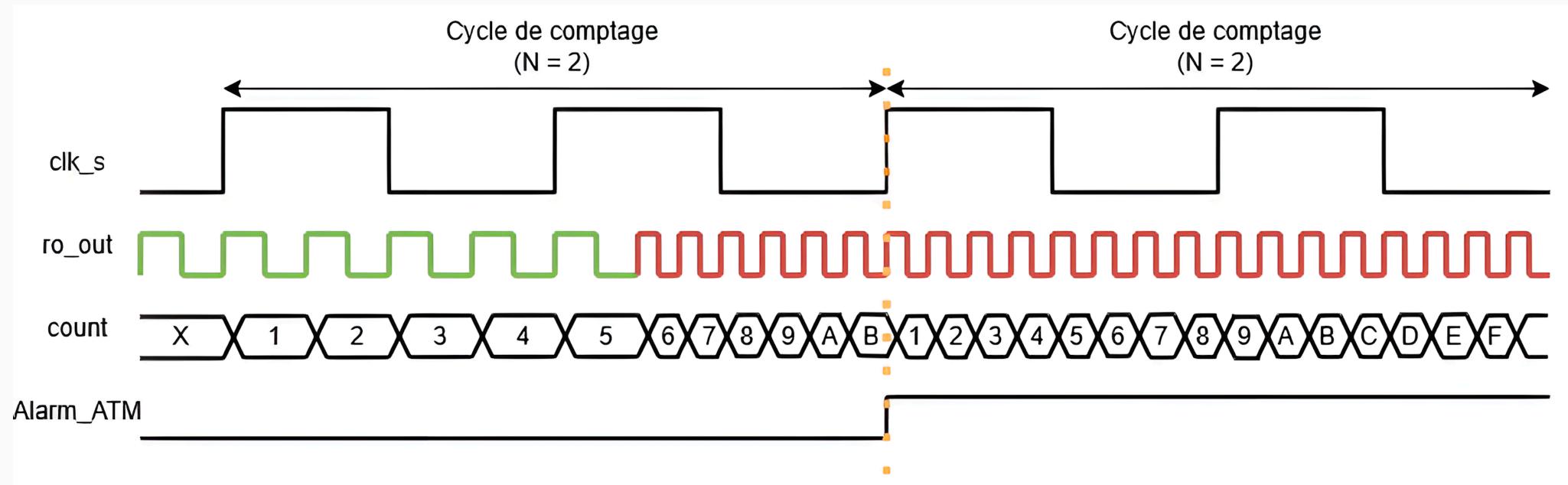


Fig. 4. – Chronogramme détaillant le fonctionnement de l'ATM.

Rôle & hypothèse

- L'ATM doit vérifier que `ro_out` ne dérive pas en dehors des intervalles prédéfinis.
- Le signal `clk_s` doit fonctionner dans les zones opérationnelles définies.

Interdépendances des modules

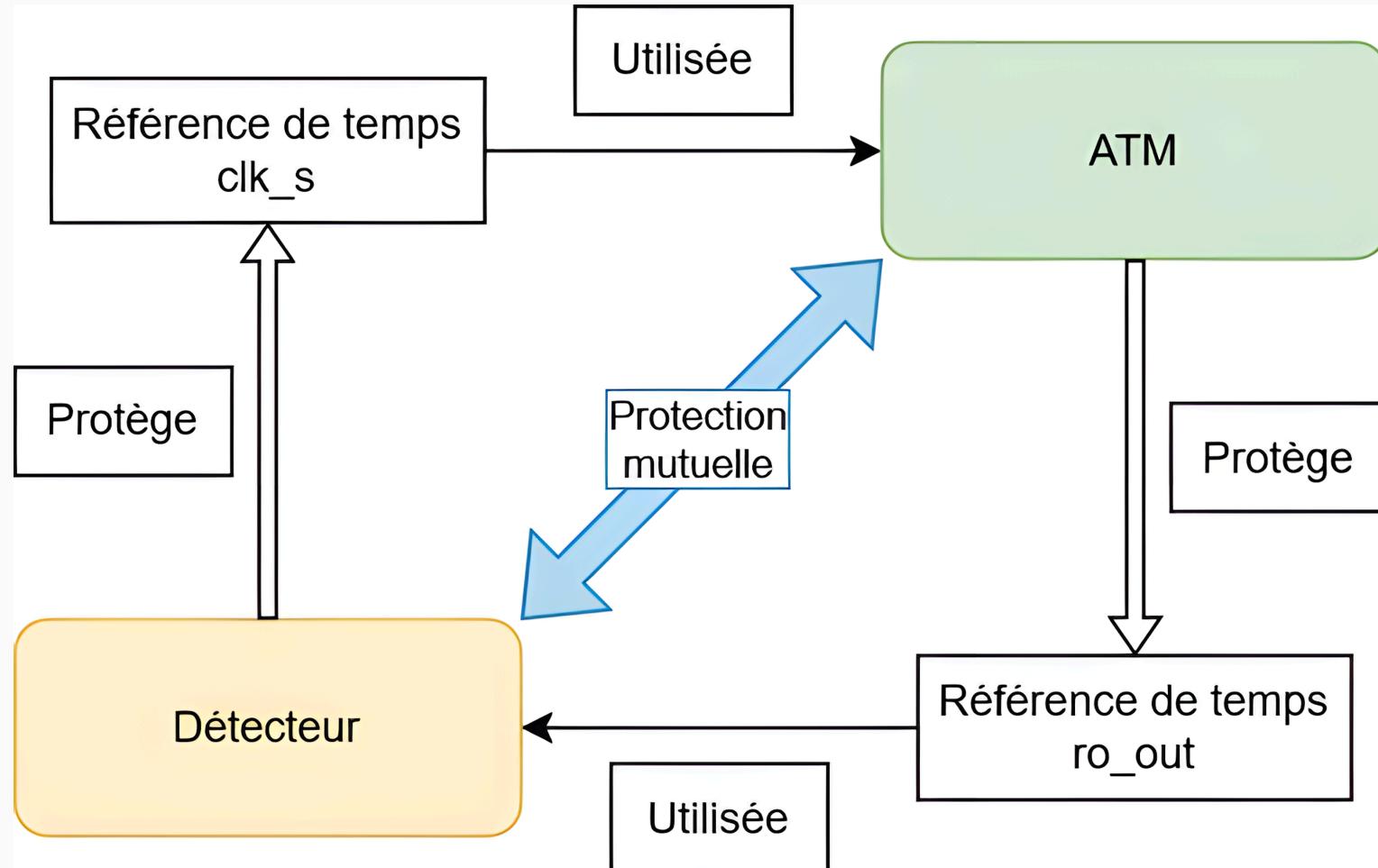


Fig. 5. – Représentation des interdépendances entre les modules et leurs paramètres.

Hypothèses

1. L'attaquant a un accès total au système embarqué.
2. Une POTA induit un vieillissement accéléré des composants, qui à terme, induira un décalage de fréquence de fonctionnement du RO.
3. L'attaquant ne contrôle pas précisément la fréquence du RO, étant un élément interne du circuit.
4. La présence de protections systèmes sur le système embarqué empêche à l'attaquant de lever autant d'alarmes qu'il désire.

Objectif et protocole

Objectif

Représenter les cas théoriques couverts par le détecteur et l'ATM.

Protocole

Balayer les valeurs de périodes pour `clk_s` et `ro_out` à partir de leurs valeurs nominales.

Dans la partie résultats, nous réaliserons une vérification expérimentale sous forme de carte thermique.

Introduction des paramètres utilisés

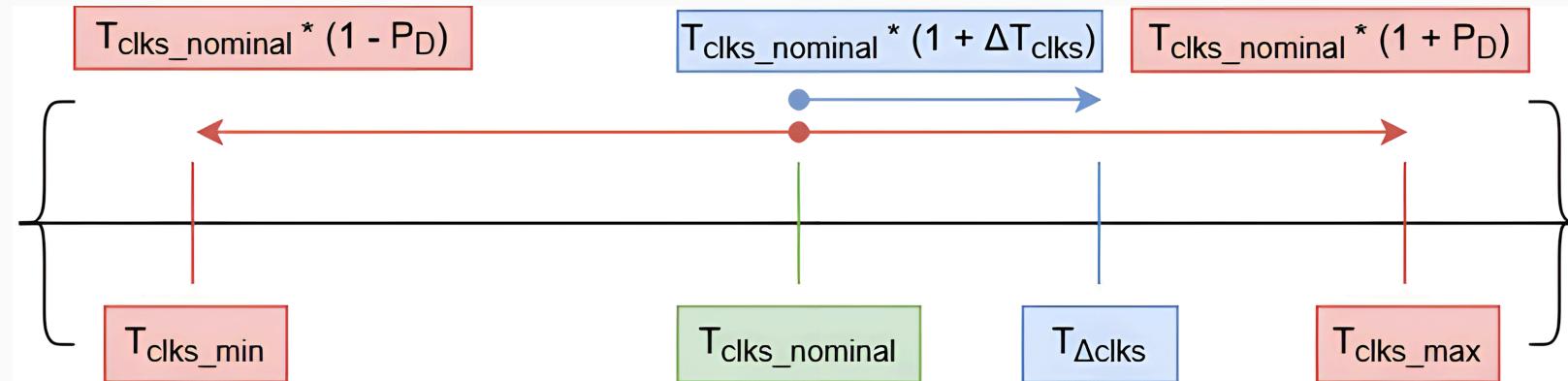


Fig. 6. – Schéma de l'intervalle des valeurs de T_{clk_s} pour le DéTECTEUR.

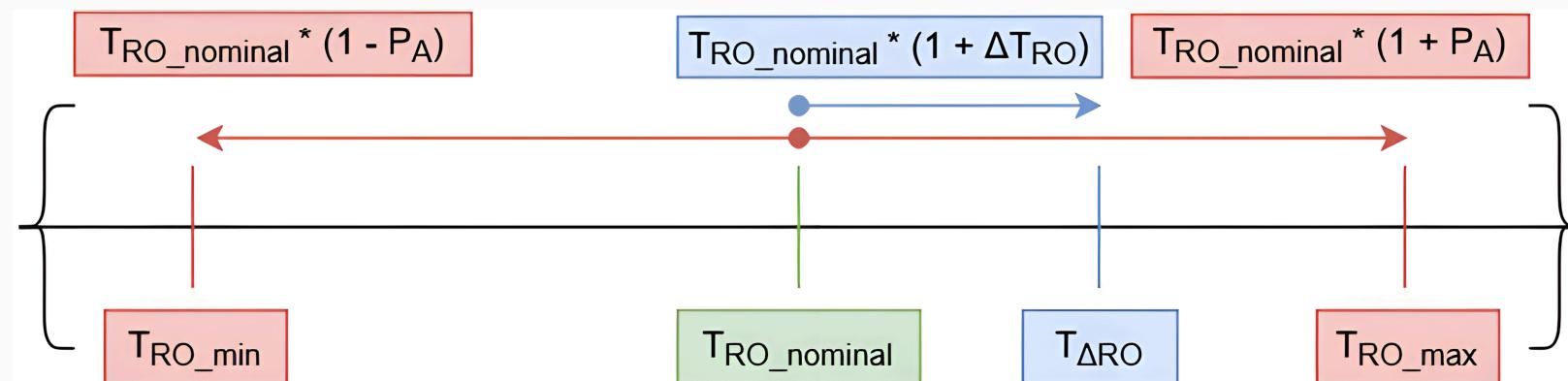


Fig. 7. – Schéma de l'intervalle des valeurs de T_{RO} pour l'ATM.

Représentation des résultats théoriques

On pose les conditions nécessaires pour ne pas lever d'alarmes :

$$\begin{cases} D_{\min} \leq D(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}}) \leq D_{\max} \\ A_{\min} \leq A(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}}) \leq A_{\max} \end{cases}$$

⋮

On obtient alors à l'issue de la démonstration les inéquations suivantes :

$$\boxed{\begin{cases} (1 - P_D) \cdot \Delta T_{\text{RO}} - P_D \leq \Delta T_{\text{clk}_s} \leq (1 + P_D) \cdot \Delta T_{\text{RO}} + P_D \\ (1 - P_A) \cdot \Delta T_{\text{RO}} - P_A \leq \Delta T_{\text{clk}_s} \leq (1 + P_A) \cdot \Delta T_{\text{RO}} + P_A \end{cases}}$$

Représentation des résultats théoriques

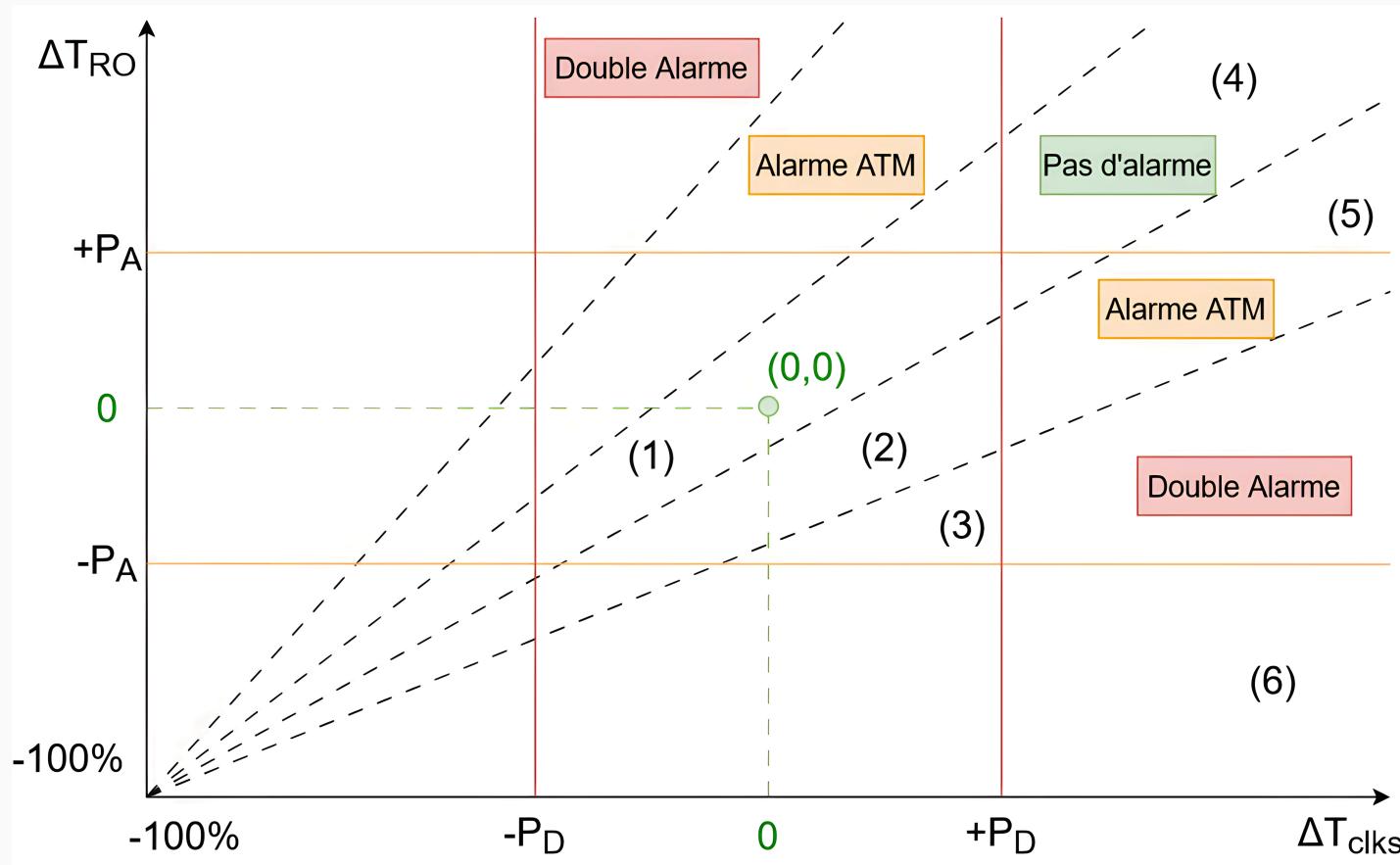


Fig. 8. – Schéma de couvertures des alarmes en fonction des déviations de régime de `clk_s` et `ro_out` selon la théorie : (1)/(4) Pas d'alarme, (2)/(5) Alarme ATM, (3)/(6) Double Alarme

IV. Implémentations et validations des modules

Implémentation du détecteur

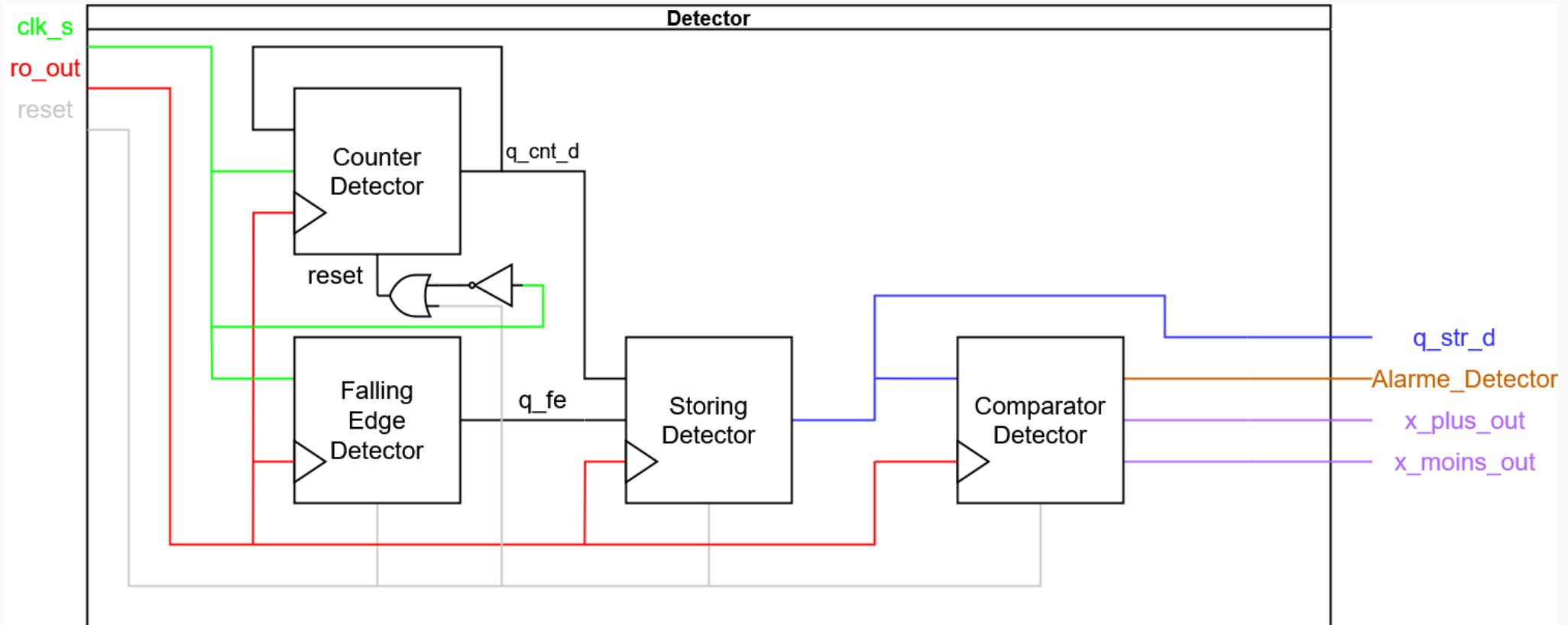


Fig. 9. – Schéma d'implémentation du détecteur.

Validation en simulation du détecteur

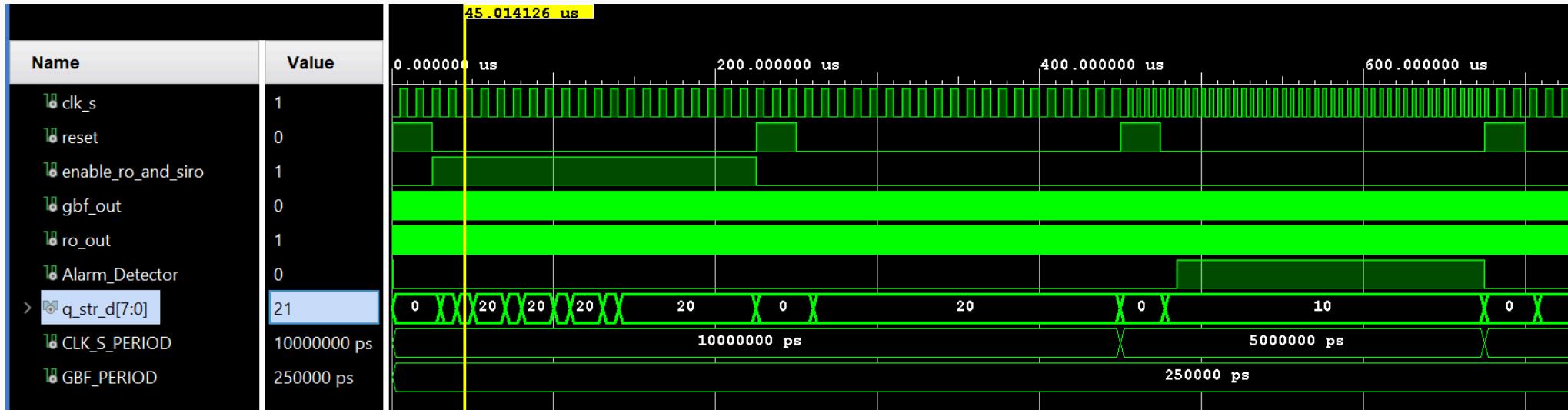


Fig. 10. – Chronogramme d'un test réalisé sur le détecteur.

Test & conclusion

RO interne puis simulé. T_{clk_s} de $10\mu s$ puis $5\mu s$, supposée lever l'alarme ($10 \notin [18, 22]$). Le détecteur est fonctionnel en simulation post placement et routage.

Validation en situation réelle du détecteur

Implémentation réelle

- $F_{clk_s} = 300 \text{ kHz}$ et $F_{ro_out} = 12 \text{ MHz}$.
- Intervalles Détecteur = {18, 22} avec précision de 10%
 1. Choisir les fréquences nominales posées précédemment à l'aide d'un GBF.
 2. Diminuer clk_s à moins de 270 kHz.
 3. Augmenter clk_s au dessus de 330 kHz.

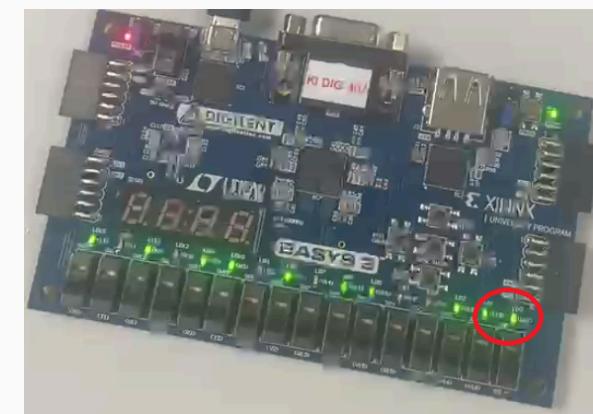
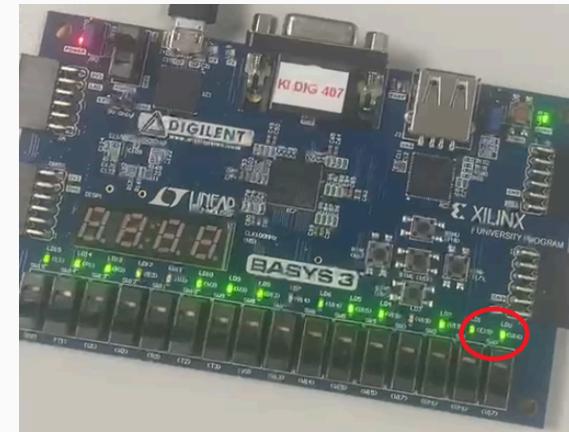
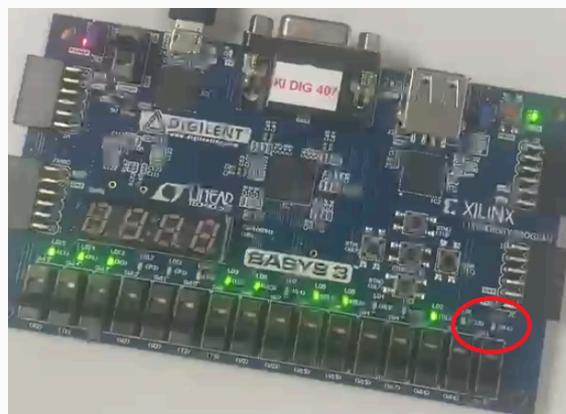


Fig. 11. – FPGA en situation : Initiale, d'alarme (inférieure), d'alarme (supérieure)

Implémentation de l'ATM

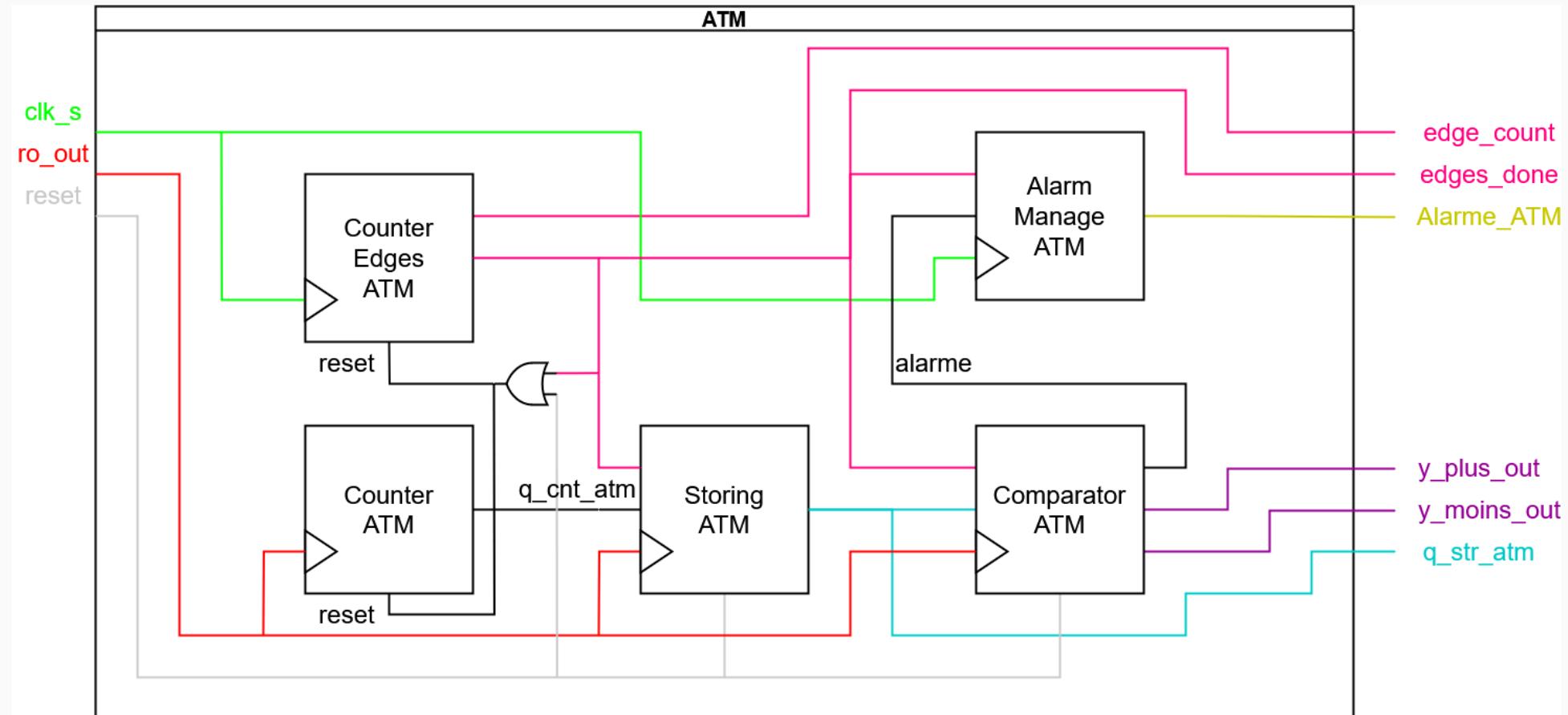


Fig. 15. – Schéma d'implémentation de l'ATM.

Validation en simulation de l'ATM

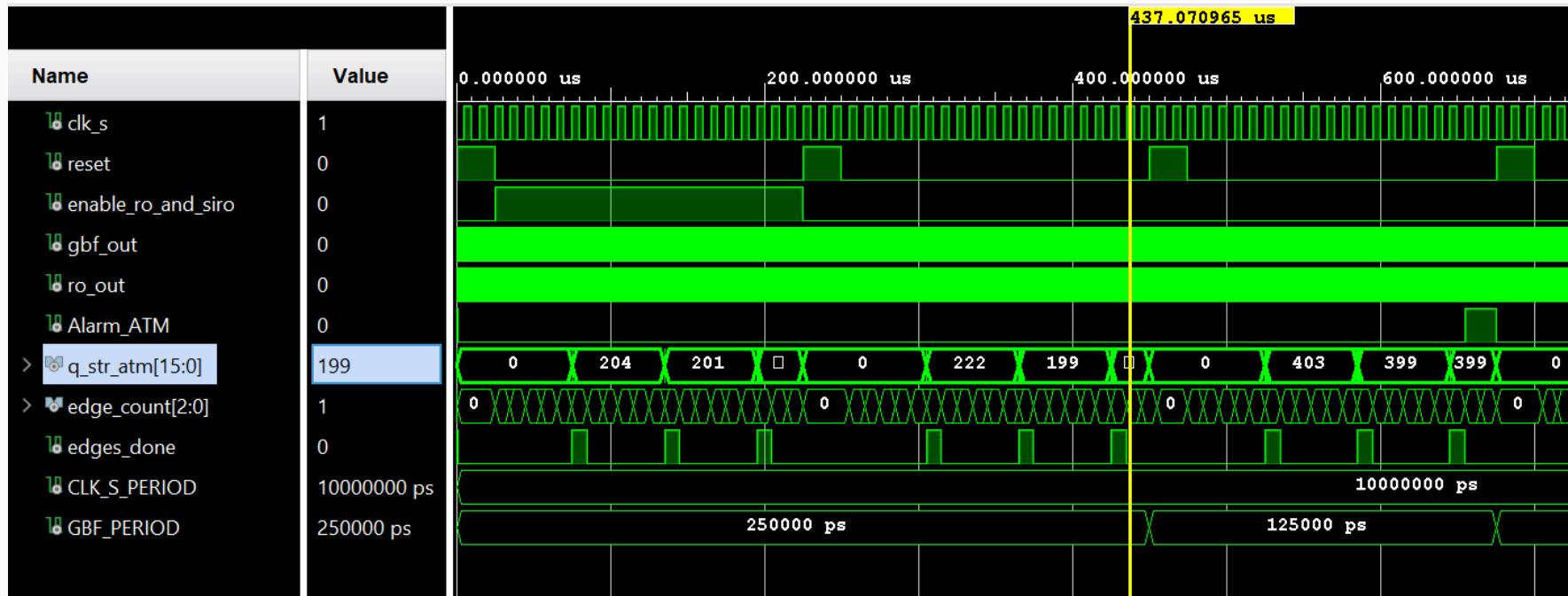


Fig. 16. – Chronogramme d'un test réalisé sur l'ATM.

Test & conclusion

RO interne puis simulé. T_{RO} de 250ns puis 125ns, supposée lever l'alarme ($399 \notin [190, 210]$). L'ATM est fonctionnel en simulation post placement et routage.

Validation en situation réelle de l'ATM

Implémentation réelle

- $F_{clk_s} = 300 \text{ kHz}$ et $F_{ro_out} = 12 \text{ MHz}$.
- Intervalles ATM = {190, 210} avec précision de 5%
 1. Choisir les fréquences nominales posées précédemment à l'aide d'un GBF.
 2. Diminuer ro_out à moins de 11.4 MHz.
 3. Augmenter ro_out au dessus de 12.6 MHz.

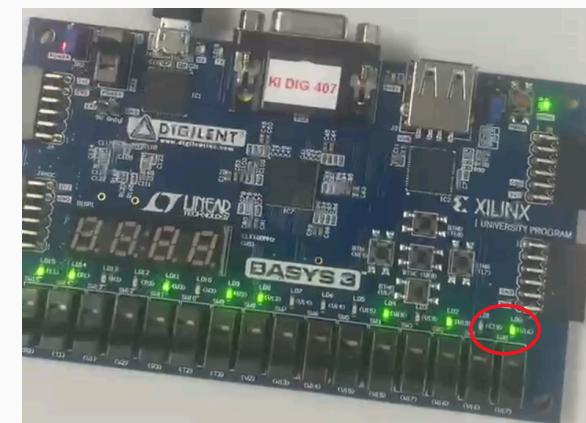
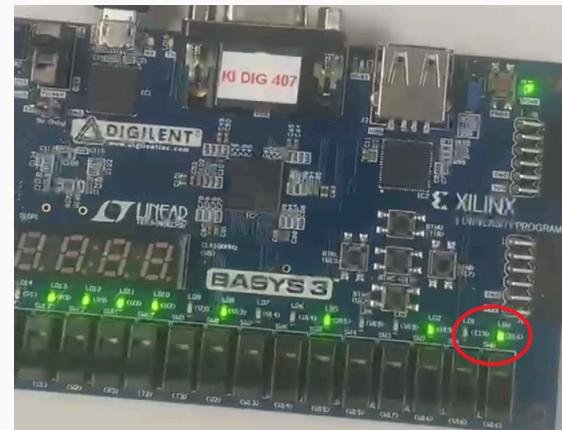
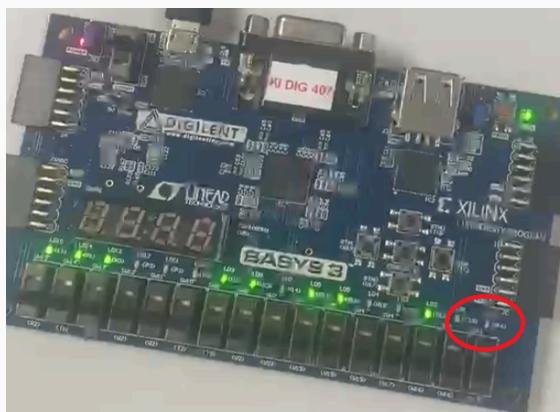


Fig. 17. – FPGA en situation : Initiale, d'alarme (inférieure), d'alarme (supérieure)

Implémentation du MTR

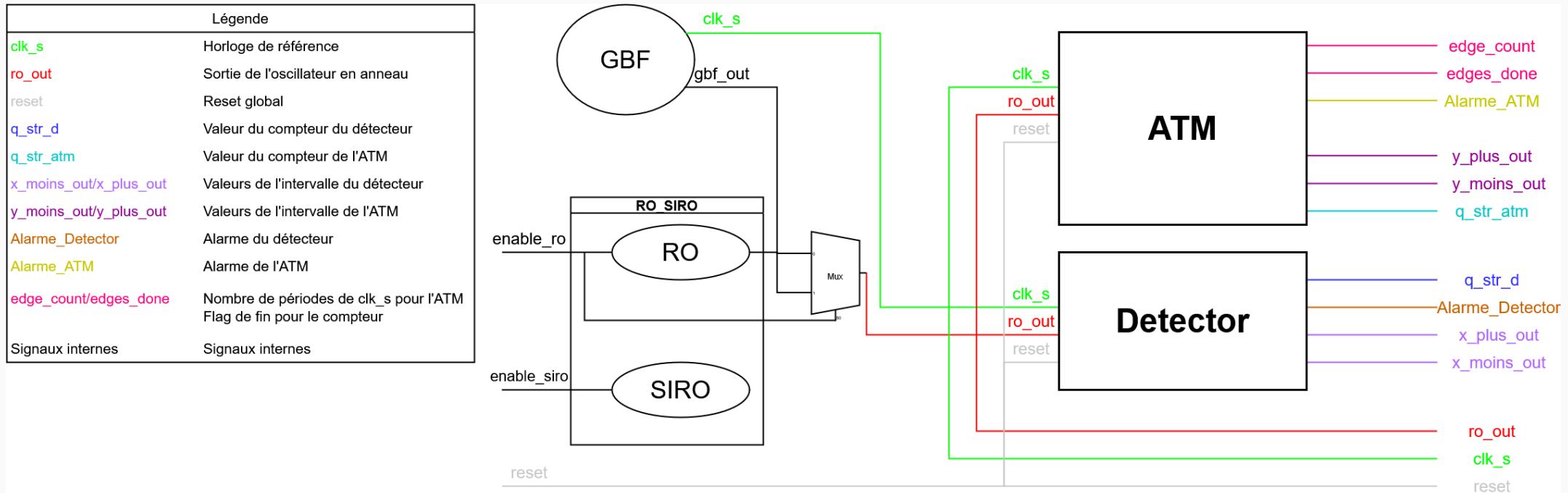


Fig. 21. – Schéma d'implémentation du MTR.

Validation en simulation du MTR

Protocole de validation en simulation du MTR

Balayer tout les cas possibles de changements de périodes pour clk_s et ro_out .

On passe du cas nominal à anormal en divisant par deux la période de clk_s ou ro_out .

Notre hypothèse actuelle sur le MTR est que les alarmes ne seront pas levées si le ratio nominal entre T_{clk_s} et T_{RO} est conservé (cas 0 et 2 ici).

Cas	T_{clk_s}	T_{RO}
0	$10\mu s$	250ns
1	$5\mu s$	250ns
2	$5\mu s$	125ns
3	$10\mu s$	125ns

Tableau 1. – Tableau recensant les cas et valeurs des périodes pour le protocole de validation en simulation du MTR.

Validation en simulation du MTR

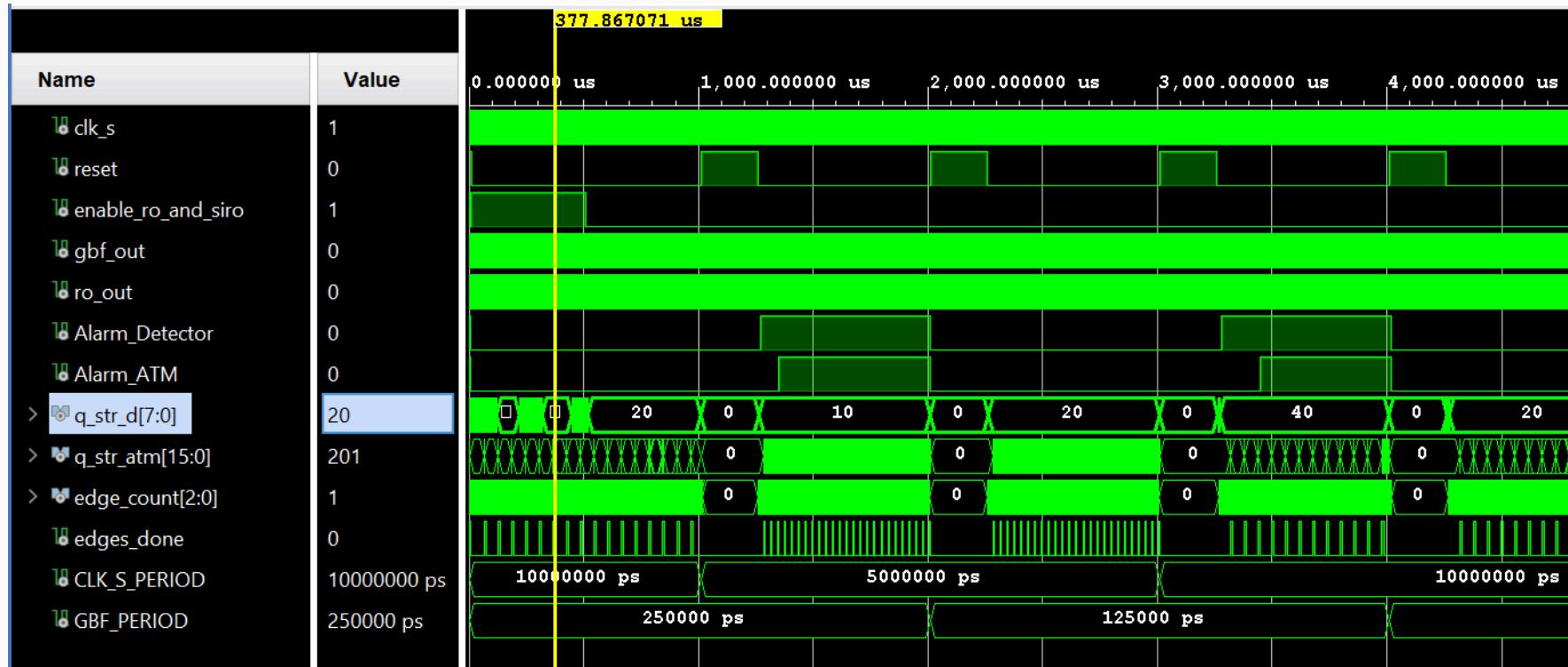


Fig. 22. – Chronogramme d'un test réalisé sur le MTR.

Conclusion

Le MTR est fonctionnel en simulation post placement et routage.

Implémentation réelle

- $F_{clk_s} = 300 \text{ kHz}$ et $F_{ro_out} = 12 \text{ MHz}$.
- Intervalles détecteur = {18, 22} avec précision de 10%
- Intervalles ATM = {190, 210} avec précision de 5%
 1. Se positionner aux fréquences nominales posées précédemment à l'aide d'un GBF.
 2. Diminuer clk_s à moins de 270 kHz.
 3. Augmenter clk_s au dessus de 330 kHz.
 - Alarmes levées correctement.
 4. Diminuer ro_out à moins de 11.4 MHz.
 5. Augmenter ro_out au dessus de 12.6 MHz.
 - Alarmes levées correctement.

Carte thermique expérimentale

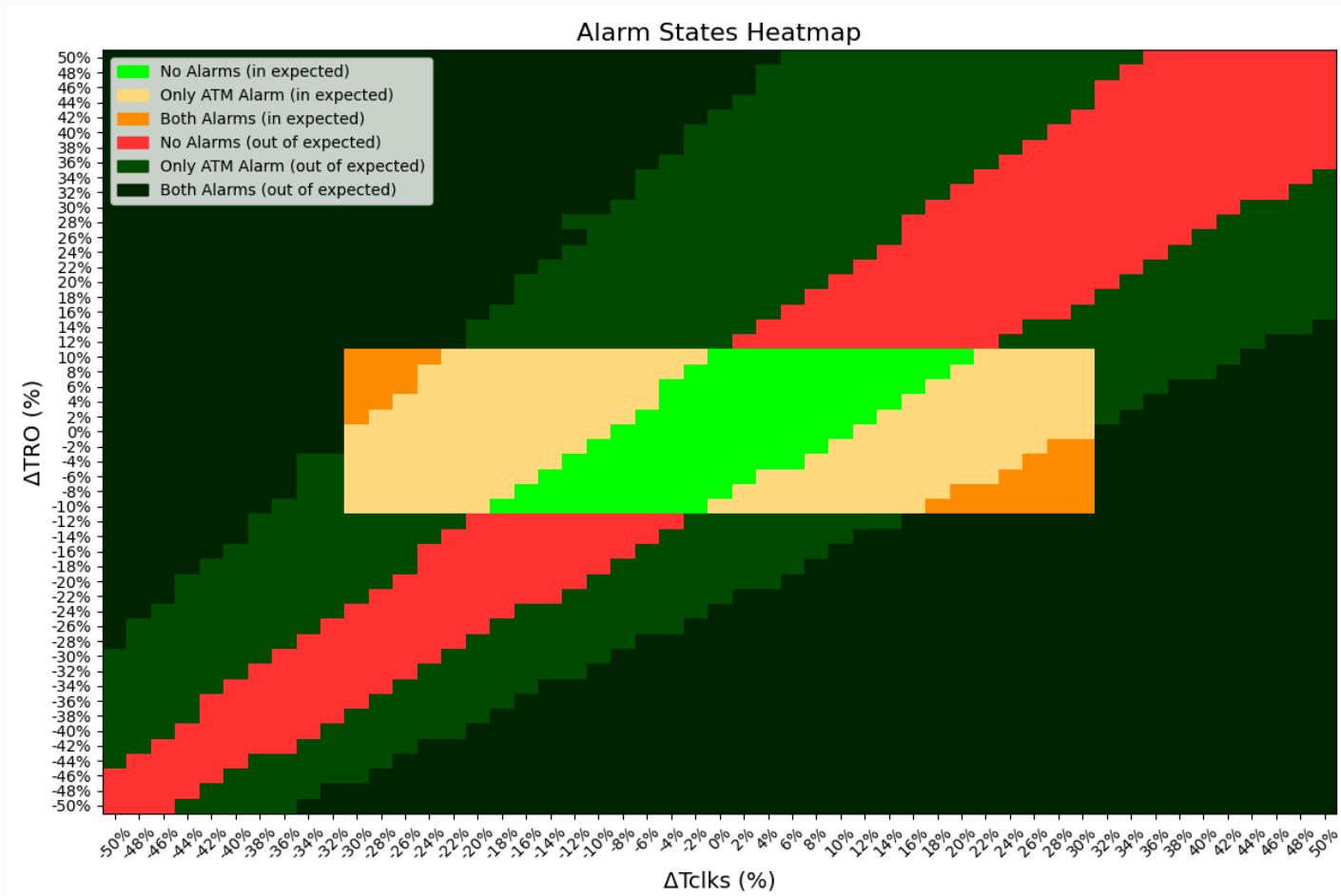


Fig. 23. – Carte thermique représentant l'évolution des états des alarmes en fonction des déviations des périodes nominales de `clk_s` et `ro_out`.

V. Campagne expérimentale

Objectif et protocole

Objectif

Réaliser des attaques thermique sur FPGA pour démontrer la robustesse du module d'auto-test.

Protocole

Appliquer des quantités de chauffage progressives sur les FPGA (40-100°C) à l'aide de SIROs (Single Input Ring Oscillators).

Après chaque jour d'expérimentation, laisser les FPGA refroidir jusqu'à température ambiante.

Mesurer `ro_out` et vérifier la robustesse du module d'auto-test pour chaque FPGA.

Effets des SIROs

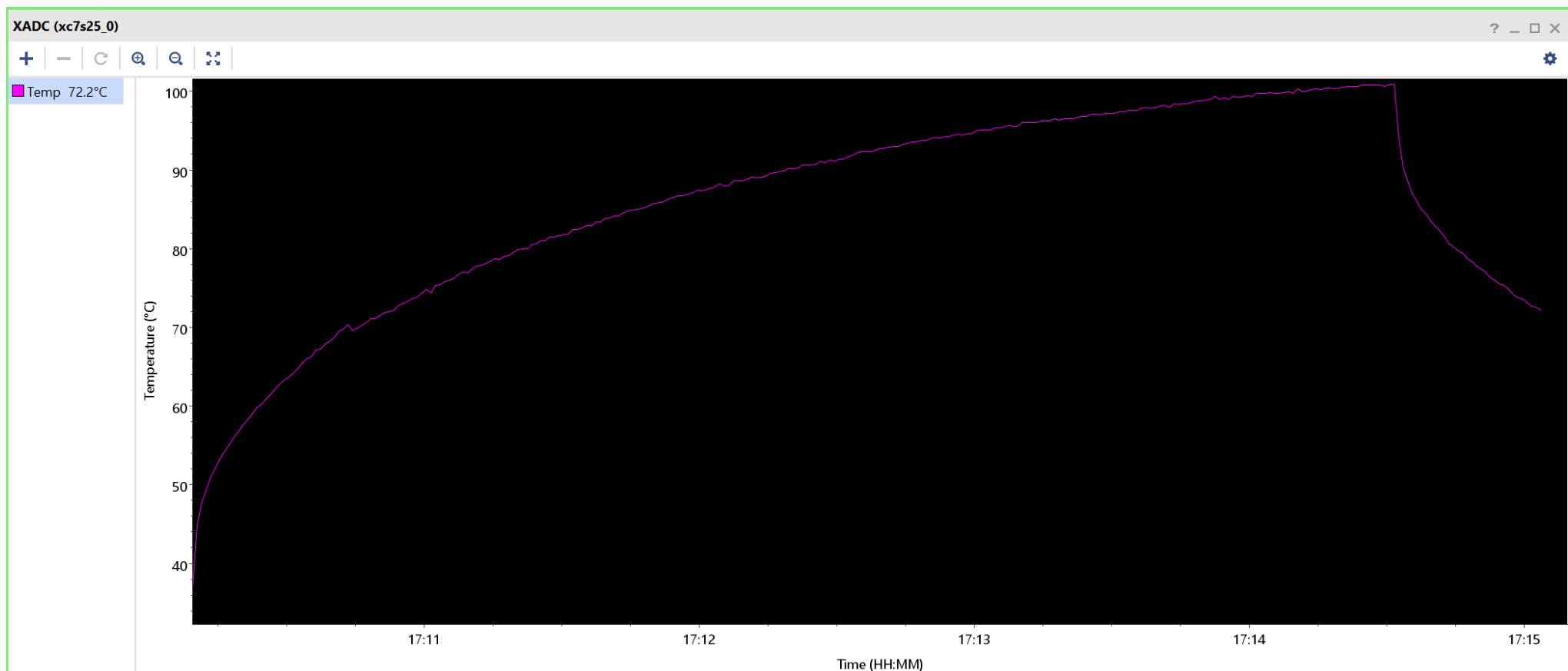


Fig. 24. – Relevé de température par capteur de température sur FPGA avec 7000 SIROs.

Schéma de principe

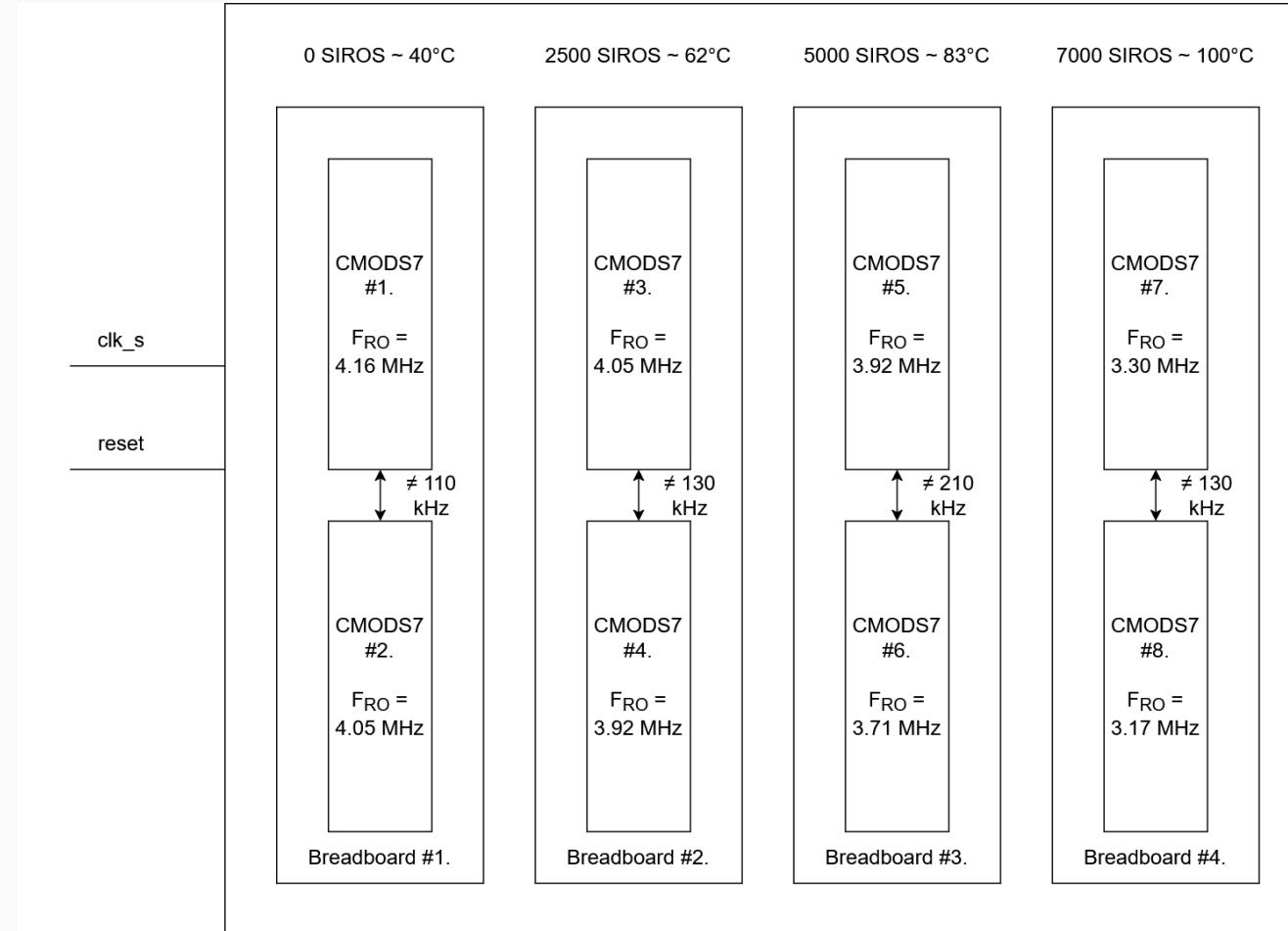


Fig. 25. – Schéma de principe du montage utilisé dans la première campagne.

Installation expérimentale

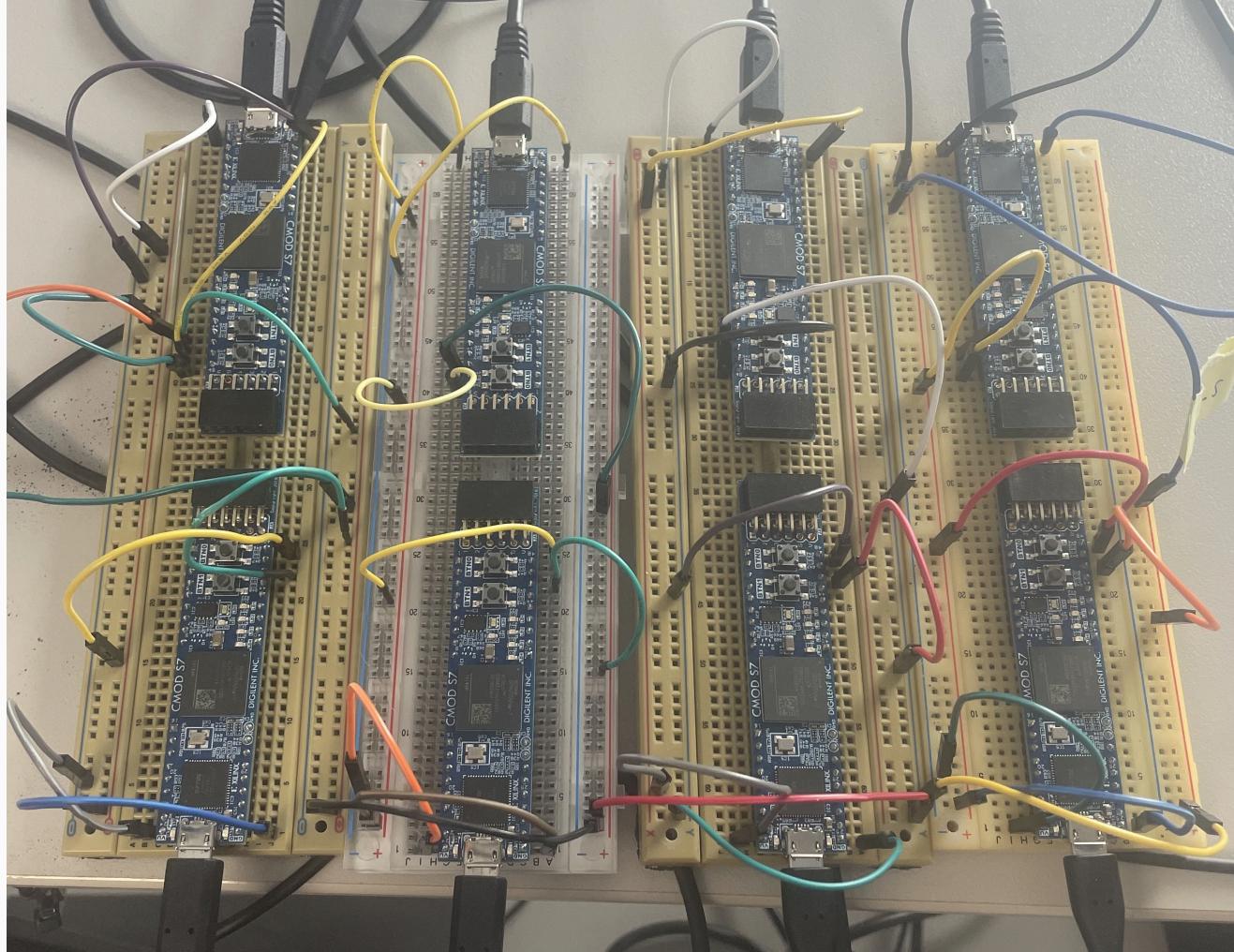


Fig. 26. – Installation expérimentale utilisée dans la première campagne.

VI. Conclusion & perspectives

Conclusion & perspectives

Conclusion

- Validation du détecteur en simulation et implémentation.
- Validation de l'ATM en simulation et implémentation.
- Validation du MTR en simulation et implémentation.
- Analyse théorique des modules et de leurs limites.
- Mise en place d'un protocole expérimental pour la campagne d'expérimentation.

Perspectives

Lancer d'autres campagnes d'expérimentation avec pour objectifs :

- Court terme : Durées plus longues
- Moyen terme : Plus de détecteurs, de fréquences et de FPGA différent(e)s
- Long terme : Autres types de détecteurs ou d'attaques

VII. Questions

Détail des équations

On pose les fréquences de `clk_s` et `ro_out` :

$$\begin{cases} F_{\text{clk}_s} = \frac{1}{T_{\text{clk}_s}} = \frac{1}{T_{\text{clk}_{s\text{nominal}}} \cdot (1 + \Delta T_{\text{clk}_s})} \\ F_{\text{RO}} = \frac{1}{T_{\text{RO}}} = \frac{1}{T_{\text{RO}_{\text{nominal}}} \cdot (1 + \Delta T_{\text{RO}})} \end{cases}$$

On définit ainsi le rapport de fréquence :

$$R = \frac{F_{\text{RO}}}{F_{\text{clk}_s}} = \frac{T_{\text{clk}_s}}{T_{\text{RO}}} = \frac{T_{\text{clk}_{s\text{nominal}}} \cdot (1 + \Delta T_{\text{clk}_s})}{T_{\text{RO}_{\text{nominal}}} \cdot (1 + \Delta T_{\text{RO}})} = R_{\text{nominal}} \cdot \frac{1 + \Delta T_{\text{clk}_s}}{1 + \Delta T_{\text{RO}}}$$

Les valeurs de fronts montants de `ro_out` pour DéTECTeur seront nommées $D(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}})$, et $A(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}})$ pour l'ATM, définis comme suit :

Détail des équations

$$D(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}}) = \frac{\frac{1}{2} \cdot \frac{1}{F_{\text{clk}_s}}}{\frac{1}{F_{\text{RO}}}} = \frac{T_{\text{clk}_s}}{2 \cdot T_{\text{RO}}} = \frac{1}{2} R = \frac{1}{2} \cdot R_{\text{nominal}} \cdot \frac{1 + \Delta T_{\text{clk}_s}}{1 + \Delta T_{\text{RO}}}$$

L'intervalle des valeurs de fronts montants de `ro_out` pour le module DéTECTeur se calcule de la manière suivante :

$$D_{\min / \max} = D_{\text{nominal}} \cdot (1 \pm P_D) = \frac{T_{\text{clk}_{s_{\text{nominal}}}}}{2 \cdot T_{\text{RO}_{\text{nominal}}}} \cdot (1 \pm P_D) = \frac{1}{2} R_{\text{nominal}} \cdot (1 \pm P_D)$$

Ainsi, on définit :

$$\begin{cases} D_{\min} = \frac{1}{2} R_{\text{nominal}} \cdot (1 - P_D) \\ D_{\max} = \frac{1}{2} R_{\text{nominal}} \cdot (1 + P_D) \end{cases}$$

Détail des équations

Le nombre de fronts montants de `ro_out` sur N périodes de `clk_s` (ATM) est nommé $A(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}})$, et est défini comme suit :

$$A(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}}) = \frac{N \cdot \frac{1}{F_{\text{clk}_s}}}{\frac{1}{F_{\text{RO}}}} = \frac{N \cdot T_{\text{clk}_s}}{T_{\text{RO}}} = N \cdot R = N \cdot R_{\text{nominal}} \cdot \frac{1 + \Delta T_{\text{clk}_s}}{1 + \Delta T_{\text{RO}}}$$

Les intervalles des valeurs de fronts montants de `ro_out` pour le module de l'ATM se calculent de la manière suivante :

$$A_{\min / \max} = A_{\text{nominal}} \cdot (1 \pm P_A) = \frac{N \cdot T_{\text{clk}_s_{\text{nominal}}}}{T_{\text{RO}_{\text{nominal}}}} \cdot (1 \pm P_A) = N \cdot R_{\text{nominal}} \cdot (1 \pm P_A)$$

Ainsi, on définit :

$$\begin{cases} A_{\min} = N \cdot R_{\text{nominal}} \cdot (1 - P_A) \\ A_{\max} = N \cdot R_{\text{nominal}} \cdot (1 + P_A) \end{cases}$$

Détail des équations

Détaillons à présent les conditions de levées d'alarmes pour le DéTECTeur et l'ATM :

$$D_{\min} \leq D(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}}) \leq D_{\max}$$

Par identification :

$$\frac{1}{2}R_{\text{nominal}} \cdot (1 - P_D) \leq \frac{1}{2}R_{\text{nominal}} \cdot \frac{1 + \Delta T_{\text{clk}_s}}{1 + \Delta T_{\text{RO}}} \leq \frac{1}{2}R_{\text{nominal}} \cdot (1 + P_D)$$

$$1 - P_D \leq \frac{1 + \Delta T_{\text{clk}_s}}{1 + \Delta T_{\text{RO}}} \leq 1 + P_D$$

$$(1 + \Delta T_{\text{RO}}) \cdot (1 - P_D) \leq 1 + \Delta T_{\text{clk}_s} \leq (1 + \Delta T_{\text{RO}}) \cdot (1 + P_D)$$

$$1 - P_D + \Delta T_{\text{RO}} - P_D \cdot \Delta T_{\text{RO}} \leq 1 + \Delta T_{\text{clk}_s} \leq 1 + P_D + \Delta T_{\text{RO}} + P_D \cdot \Delta T_{\text{RO}}$$

On obtient donc comme conditions de levée d'alarme pour le DéTECTeur :

$$(1 - P_D) \cdot \Delta T_{\text{RO}} - P_D \leq \Delta T_{\text{clk}_s} \leq (1 + P_D) \cdot \Delta T_{\text{RO}} + P_D$$

Détail des équations

$$A_{\min} \leq A(\Delta T_{\text{clk}_s}, \Delta T_{\text{RO}}) \leq A_{\max}$$

Par identification :

$$N \cdot R_{\text{nominal}} \cdot (1 - P_A) \leq N \cdot R_{\text{nominal}} \cdot \frac{1 + \Delta T_{\text{clk}_s}}{1 + \Delta T_{\text{RO}}} \leq N \cdot R_{\text{nominal}} \cdot (1 + P_A)$$

$$1 - P_A \leq \frac{1 + \Delta T_{\text{clk}_s}}{1 + \Delta T_{\text{RO}}} \leq 1 + P_A$$

$$(1 + \Delta T_{\text{RO}}) \cdot (1 - P_A) \leq 1 + \Delta T_{\text{clk}_s} \leq (1 + \Delta T_{\text{RO}}) \cdot (1 + P_A)$$

$$1 - P_A + \Delta T_{\text{RO}} - P_A \cdot \Delta T_{\text{RO}} \leq 1 + \Delta T_{\text{clk}_s} \leq 1 + P_A + \Delta T_{\text{RO}} + P_A \cdot \Delta T_{\text{RO}}$$

On obtient donc comme conditions de levée d'alarme pour l'ATM :

$$(1 - P_A) \cdot \Delta T_{\text{RO}} - P_A \leq \Delta T_{\text{clk}_s} \leq (1 + P_A) \cdot \Delta T_{\text{RO}} + P_A$$

Détail des équations

On peut ainsi définir les différentes possibilités couvertes par nos alarmes :

- Pas d'alarmes

$$\begin{cases} (1 - P_D) \cdot \Delta T_{\text{RO}} - P_D \leq \Delta T_{\text{clk}_s} \leq (1 + P_D) \cdot \Delta T_{\text{RO}} + P_D \\ (1 - P_A) \cdot \Delta T_{\text{RO}} - P_A \leq \Delta T_{\text{clk}_s} \leq (1 + P_A) \cdot \Delta T_{\text{RO}} + P_A \end{cases}$$

- Alarme de l'ATM

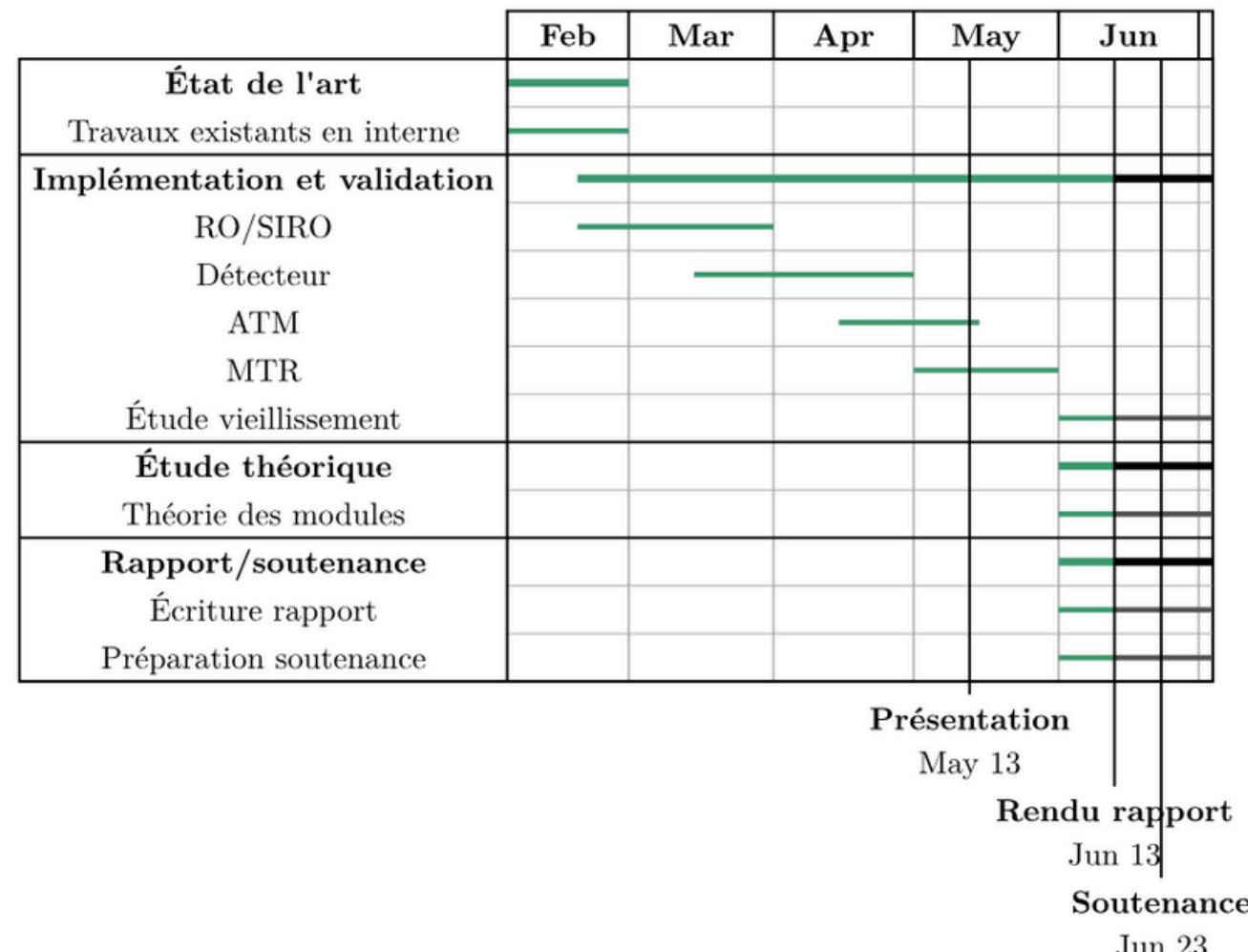
$$\begin{cases} (1 - P_D) \cdot \Delta T_{\text{RO}} - P_D \leq \Delta T_{\text{clk}_s} \leq (1 + P_D) \cdot \Delta T_{\text{RO}} + P_D \\ (1 - P_A) \cdot \Delta T_{\text{RO}} - P_A \not\leq \Delta T_{\text{clk}_s} \not\leq (1 + P_A) \cdot \Delta T_{\text{RO}} + P_A \end{cases}$$

Détail des équations

- Alarme du DéTECTEUR
 - N'arrivera pas car l'ATM est plus restrictif que le DéTECTEUR ($P_A < P_D$).
- Deux alarmes.

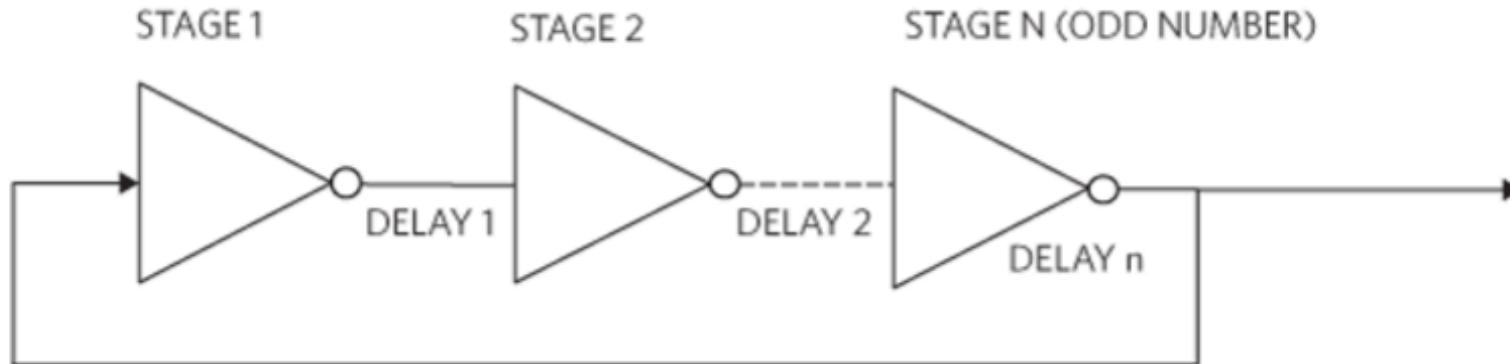
$$\begin{cases} (1 - P_D) \cdot \Delta T_{\text{RO}} - P_D \not\leq \Delta T_{\text{clk}_s} \not\leq (1 + P_D) \cdot \Delta T_{\text{RO}} + P_D \\ (1 - P_A) \cdot \Delta T_{\text{RO}} - P_A \not\leq \Delta T_{\text{clk}_s} \not\leq (1 + P_A) \cdot \Delta T_{\text{RO}} + P_A \end{cases}$$

Gantt du PFE



Oscillateur en anneau (RO)

SIMPLIFIED PUF ELEMENT – A RING OSCILLATOR



OUTPUT FREQUENCY = $1/(2 \times \text{STAGE DELAY} \times \text{NUMBER OF STAGES})$

$$\begin{cases} T_{\text{RO}} = 2 \cdot N \cdot t_d \\ F_{\text{RO}} = \frac{1}{2 \cdot N \cdot t_d} \end{cases}$$

où N correspond au nombre d'inverseurs
et t_d au délai moyen de propagation par inverseur