Comparaison des Approches de Lockstep pour la Tolérance aux Fautes des FPGAs Utilisés en Milieu Radiatif

Hugo Closquinet, Florent Miller, Patrick Girard, Thibault Vayssade, Arnaud Virazel

Comparaison des Approches de Lockstep pour la Tolérance aux Fautes des FPGAs Utilisés en Milieu Radiatif

H. Closquinet[1] F. Miller[1] Y. Helen[2] P. Girard[3] T. Vayssade[3] A. Virazel[3]

[1] Nuclétudes
Les Ulis, France
hclosquinet@lirmm.fr, fmiller@lirmm.fr

[2] Direction Générale de l'Armement
Rennes, France
youri.helen@intradef.gouv.fr

[3] LIRMM – Univ. of Montpellier / CNRS
Montpellier, France
patrick.girard@lirmm.fr, thibault.vayssade@lirmm.fr, arnaud.virazel@lirmm.fr

***Abstract*—Ce papier présente une analyse d'une technique de protection, le Lockstep, appliquée à un système s'exécutant sur un composant complexe, et cela afin d'assurer la tolérance aux fautes de ce système lorqu'il est utilisé dans des environnements radiatifs sévères. En effet, les systèmes électroniques sont sujets à des défaillances en raison du nombre élevé d'erreurs pouvant survenir de manière aléatoire dans ces environnements, soulignant ainsi la nécessité de mettre en place une solution de protection efficace. Ce papier décrit le processus de déploiement du Lockstep et examine son impact sur une cible FPGA. Cette technique est initialement implémentée sur FPGA en vue d'une adaptation sur SoC-FPGA.**

Mots Clés—Tolérance aux fautes, FPGA, Lockstep, SoC-FPGA, laser, faisceau de particules

I. Introduction

Dans les applications critiques telles que l'aéronautique ou le spatial, la tolérance aux fautes est essentielle pour garantir le bon fonctionnement des systèmes électroniques soumis à des environnements radiatifs sévères. Les composants et technologies utilisés n'ont pas été conçus spécifiquement pour résister dans des environnements très contraints, la plupart d'entre eux visant des applications grand public. Le choix de composants et architectures numériques pour la plupart issus de filières COTS (Commercial Off-The-Shelf) est porté avec un intérêt grandissant pour les composants reprogrammables de type FPGA en raison de la modularité qu'ils offrent. Sans mécanisme de protection, les contraintes radiatives sont telles que les taux d'erreurs et de pannes dans ces architectures ne seraient pas acceptables.

Les environnements radiatifs imposent des défis importants pour la fiabilité des sytèmes électroniques, et se divisent en deux catégories : l'environnement spatial et l'environnement atmosphérique. L'environnement spatial est composé de protons, d'électrons et d'ions lourd provenant de rayons cosmiques, de vents solaires et d'éruptions solaires [1]. L'environnement atmosphérique est plutôt composé de neutrons, de protons, d'électrons, de muons, de pions et de photons issus de collisions atomiques atmosphériques. Heureusement, une partie de ces particules provenant de l'environnement spatial se retrouvent piégées par les champs magnétiques terrestres, formant les ceintures de Van Allen.

En fonction de l'environnement dans lequel l'électronique est exposée, les effets qui peuvent en résulter se divisent en trois catégories. Ces trois catégories sont les SEE - Single Event Effects, les effets de dose et les effets de déplacement. Les effets de dose et les effets de déplacement sont dus à des effets sur le long terme, ou cumulés, de l'impact de plusieurs particules, alors que les SEE sont des effets singuliers qui sont obtenus après l'impact d'une seule particule. Ce travail se concentre sur les SEE et donc sur les différents évènements qui peuvent découler de cet effet. Parmi les principaux types d'évènements singuliers, on retrouve les SEU - Single Event Upset (changement d'état d'un élément mémoire), les SET – Single Event Transient (pic de courant indésirable), les SEFI – Single Event Functional Interrupt (arrêt ou dysfonctionnement du système), et les SEL – Single Event Latch-up (pic de courant entraînant un court-circuit). L'enjeu réside donc dans la nécessité de contrer efficacement les évènements singuliers à l'aide de techniques de protection.

Ce papier présente le Lockstep, une technique de protection utilisant la redondance pour détecter les erreurs. Une première approche sur FPGA a été réalisée, incluant une analyse préliminaire. L'objectif principal est désormais d'évaluer la tolérance aux fautes de cette méthode en utilisant l'injection de fautes par laser et par faisceau de particules afin de déterminer si elle offre un bon taux de couverture. Ensuite, l'adaptation sur SoC-FPGA sera envisagée afin de déterminer si cette nouvelle approche constitue une solution plus efficace que les solutions utilisées jusqu'à présent.

II. Etat de l'art sur le Lockstep

De nombreuses études ont montré que les contraintes radiatives entraînent des erreurs inacceptables en l'absence de mécanismes de protection pour les applications critiques. Dans le domaine des techniques de protection, de nombreuses stratégies ont été étudiées et sont largement documentées [2]. Parmi ces approches, on retrouve des méthodes telles que la redondance, la détection et la correction d'erreurs, les mécanismes de récupération, ainsi que l'utilisation de codes correcteurs d'erreurs [1]. Ces techniques visent toutes à renforcer la fiabilité des sytèmes électroniques. Cependant, le Lockstep suscite un intérêt particulier en raison de sa proposition d'un meilleur compromis entre l'utilisation des ressources et l'impact sur les performances [3]. Contrairement à d'autres méthodes plus traditionnelles de redondance, le Lockstep exploite une redondance où les opérations sont effectuées en parallèle et sur des unités de traitement indépendantes. Ces unités peuvent se composer de trois types différents, comme illustré sur la Figure 1. Il peut s'agir a) d'une redondance des cœurs processeurs, b) d'une redondance des cœurs avec leur cache, ou encore une version c) de redondance avec une mémoire distincte pour chaque cœurs.

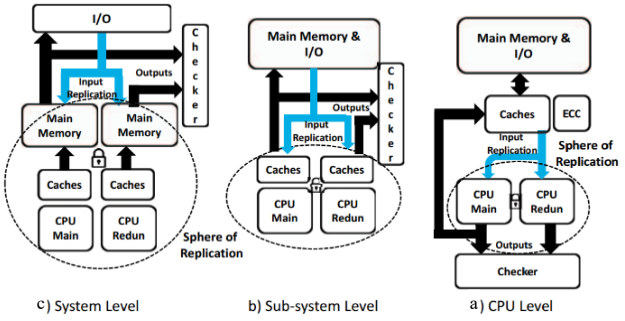

Figure 1 : Types de blocs fonctionnels redondants en Lockstep [4]

Le Lockstep comprend plusieurs variantes, notamment la DCLS (Dual-Core Lockstep), la TCLS (Triple-Core Lockstep) et la DCLS avec diversité. Ces variantes se différencient par la manière dont elles utilisent la redondance et par leurs fonctionnalités. La DCLS implique deux cœurs de processeur identiques exécutant le même processus d'un système. Une comparaison se fait à chaque étape pour détecter toute erreur potentielle entre leurs signaux de sortie et/ou résultats. La TCLS étend le concept du DCLS en utilisant trois cœurs de processeur pour exécuter les mêmes tâches. La redondance supplémentaire offre une meilleure capacité de détection et de correction [5]. Et la DCLS avec diversité reprend le concept de DCLS avec des cœurs de processeur différents [4]. Le tout en ajoutant une couche de protection supplémentaire, en introduisant la diversité qui rend moins probable la simultanéité des erreurs sur l'ensemble des cœurs.

III. Deploiement progressif du Lockstep sur FPGA vers des SoC-FPGA

Dans un objectif de mise en place du Lockstep, un premier travail a consisté à évaluer la faisabilité et la flexibilité de cette technique. Une implémentation du Lockstep en DCLS sur FPGA a été réalisée en utilisant deux soft processeurs RISC-V et fonctionnant avec un décalage de deux cycles d'horloge. En introduisant une latence de deux cycles entre les processeurs, cela permet d'éviter que les deux processeurs captent la même faute en cas d'occurrence. De plus, le module de Lockstep a été implémenté sur un bus de communication AMBA AHB entre les deux cœurs RISC-V et la mémoire du système. Le choix de placement au niveau du bus de communication ajoute une certaine versatilité afin de pouvoir facilement modifier le type de processeur sans avoir à modifier toute l'architecture. Sachant que l'ensemble des activités du système va circuler sur ce bus, implémenter une protection par Lockstep sur celui-ci semble donc être un choix cohérent pour capter un maximum d'erreurs. La technique de protection par Lockstep a ensuite été validée et des travaux d'évaluation de l'impact sur les performances ont ensuite été menés. Ils ont démontré que les taux d'exécution obtenus étaient trop élevés en raison de l'incapacité des processeurs à communiquer simultanément sur le bus de communication. Une optimisation est en cours pour résoudre ce problème.

Pour la suite des travaux, une évaluation du taux de couverture de fautes du Lockstep est prévue. La planification d'injections de faute au laser [6] sera effectuée pour évaluer la méthode de protection. Un environnement de test sera établi pour effectuer ces injections de faute et cartographier l'ensemble du FPGA pour déterminer les surfaces sensibles à l'apparition d'erreurs. Par ailleurs, ces injections fourniront des données sur la capacité du module de Lockstep à détecter des fautes potentielles. Enfin, une évaluation sera menée dans un environnement réel, en allant sous faisceau de particules, pour obtenir des résultats plus représentatifs de conditions auxquelles les systèmes sont exposés. Ces ensembles de données de test fourniront des résultats pouvant établir une comparaison des niveaux de sensibilité entre le laser et un environnement radiatif.

Une fois les objectifs de faisabilité et d'évaluation atteints, il est prévu de complexifier cette architecture protégée par du Lockstep en augmentant le nombre de cœurs de processeur. Cette extension sera suivie de la même évaluation que celle présentée ci-dessus.

L'objectif final de ces travaux portera sur l'adaptation du Lockstep par la méthode DCLS avec diversité. Cette méthode sera réalisée sur SoC-FPGA. L'avènement des composants numériques complexes de type SoC-FPGA intégrant à la fois plusieurs cœurs de processeur et une partie programmable offre de nouvelles possibilités ainsi que la mise en place de diversité. L'enjeu associé sera d'identifier le bon niveau de granularité auquel se situer, de manière à optimiser le compromis entre efficacité de protection, impact sur les performances et portabilité.

Entre chacune de ces trois étapes, l'utilisation d'une plateforme virtuelle facilitera la validation de la preuve de concept et les tests sur les différentes architectures, réduisant ainsi les coûts de développement et facilitant la transition vers une implémentation sur cible matérielle une fois la solution optimisée. D'un point de vue général, ce travail aura pour objectif de mettre en lumière les avantages potentiels du Lockstep dans des environnements critiques en explorant les différentes étapes de son déploiement sur FPGA jusqu'à son intégration avec des SoC-FPGA.

IV. Conclusion et perspectives

En conclusion, l'étude approfondie de l'implémentation progressive du Lockstep sur SoC-FPGA permettra de confirmer son efficacité pour renforcer la fiabilité des systèmes électroniques exposés à des environnements radiatifs sévères. Les évaluations par faisceau de particules et injections de faute au laser permettront de démontrer la capacité du Lockstep à détecter et/ou corriger les fautes potentielles induites par radiations. Pour l'avenir, l'intégration du Lockstep avec des architectures à base de Network-On-Chip (NoC) ouvre des perspectives prometteuses pour le déploiement de systèmes embarqués plus complexes, capable de traiter des données massivement parallèles. Cette évolution vers des architectures NoC avec Lockstep peut représenter une avancée significative dans le domaine de la tolérance aux fautes. Il faudra donc étudier la robustesse et la fiabilité de celles-ci sous environnements radiatifs sévères.

References

[1] S. Houssany, "Méthodologie d'évaluation de la sensibilité des microprocesseurs vis à vis des rayonnements cosmiques," Thèse de Doctorat de l'Université de Grenoble, 2006.

[2] ESA-ESTEC, "Techniques for radiation effects mitigation in ASICs and FPGAs," ECSS-Q-HB-60-02A, Handbook of the European Cooperation for Space Standardization, Noordwijk, The Netherlands, 1 September 2016.

[3] E. W. Wächter, S. Kasap, X, Zhai, S, Ehsan and K. McDonald-Maier, "Survey of lockstep based mitigation techniques for soft errors in embedded systems," 11th Computer Science and Electronic Engineering (CEEC), Colchester, UK, pp. 124-127 , 2019.

[4] I. Marques, "A loosely-coupled Arm and RISC-V locksteping technology," Thèse de Master de l'Université de Minho, Portugal, 2020.

[5] S. Kasap, E. W. Wächter, X. Zhai, S. Ehsan and K. McDonald-Maier, "Novel lockstep-based approach with roll-back and roll-forward recovery to mitigate radiation-induced soft errors," IEEE Nordic Circuits and Systems Conference (NorCAS), Oslo, Norway, pp. 1-7, 2020.

[6] S. P. Buchner, F. Miller, V. Pouget and D. P. McMorrow, "Pulsed-laser testing for single-event effects investigations," IEEE Transactions on Nuclear Science, vol. 60, no. 3, pp. 1852-1875, June 2013.