Racine de confiance et démarrage sécurisé sur plateforme RISC-V

Auteurs : Antonin Marion – Louis Bilheux – Tahar Herri

CONTEXTE ET OBJECTIF

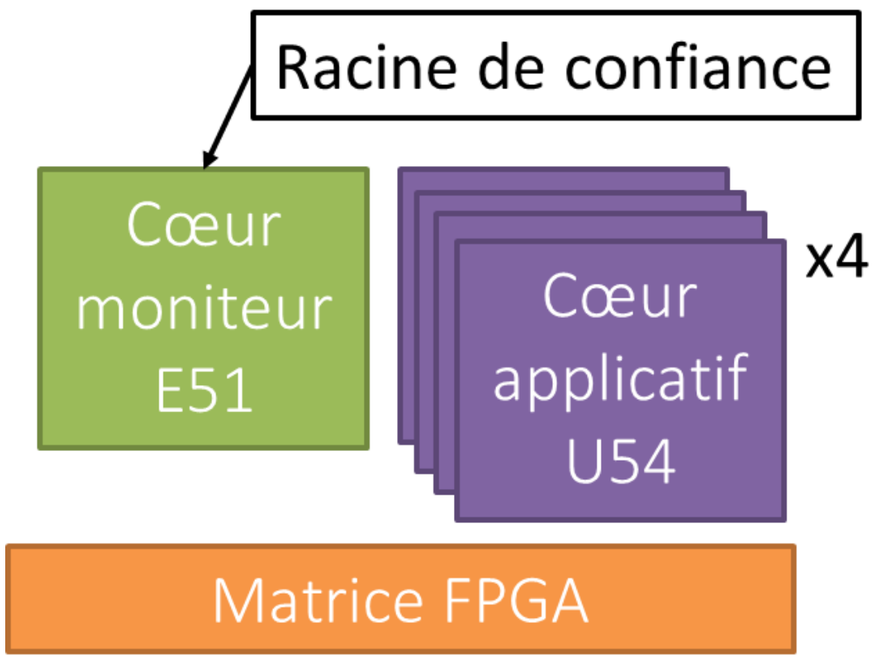
Safran Electronics & Defense est l'une des dix entités du groupe international Safran, plus ancien groupe industriel aéronautique au monde, opérant également dans les domaines de l'espace et de la défense.

Safran E&D a besoin de certifier que tout firmware démarrant sur une plateforme RISC-V multicœur a été vérifié en intégrité et authenticité.

Développement d'une racine de confiance qui, en utilisant des fonctions cryptographiques, vérifiera l'authenticité et l'intégrité de tout firmware démarrant sur l'appareil. Développement d'un outil de mise en forme de chaine de confiance compatible avec notre racine.

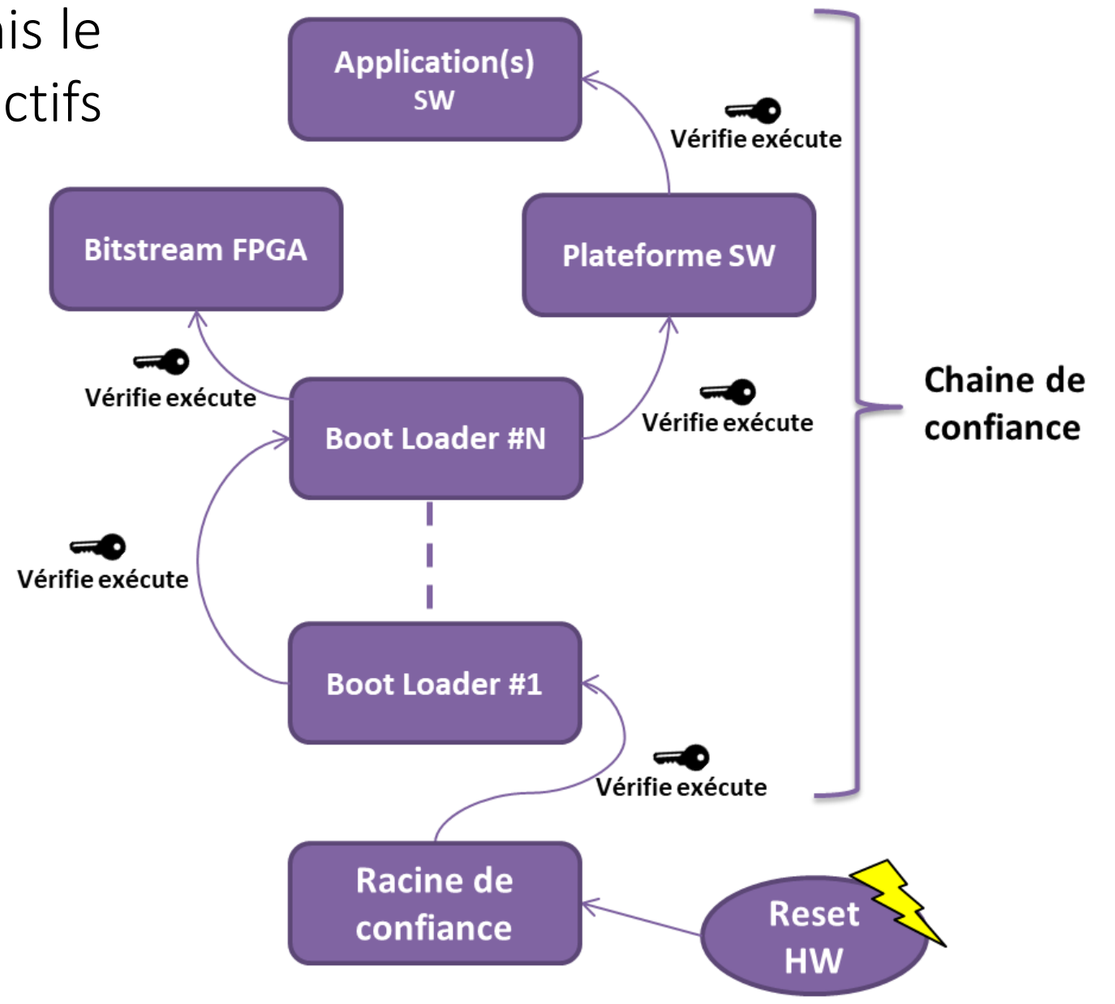
MÉTHODES ET DÉVELOPPEMENTS

L'état de l'art, l'évaluation des kits de développement ainsi que la rédaction des spécifications fonctionnelles et technique ont permis de concevoir une chaine de confiance flexible selon le besoin du client reposant sur une racine de confiance immuable.



Le développement s'est fait en et en ASM avec un versioning git .

Des points d'avancement hebdomadaires ont permis le suivi du projet ainsi que la validation des objectifs intermédiaires.



RÉSULTATS ET CONCLUSION

La chaine de confiance s'appuyant sur la racine de confiance permet de s'assurer que tout ce qui démarre sur le matériel quelque soit sa nature (application bare metal, OS, application OS) est bien intègre et authentique afin d'éviter toute exécution malicieuse.

MOTS-CLÉS : RISC-V, Sécurité Embarquée , Secure Boot, Racine de Confiance, Chaine de Confiance, Cryptographie appliquée