Secure Boot based on PQC

Auteurs : LUCAS Arpad – SLEZAK Arthur– REYNAUD Anthéo

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.

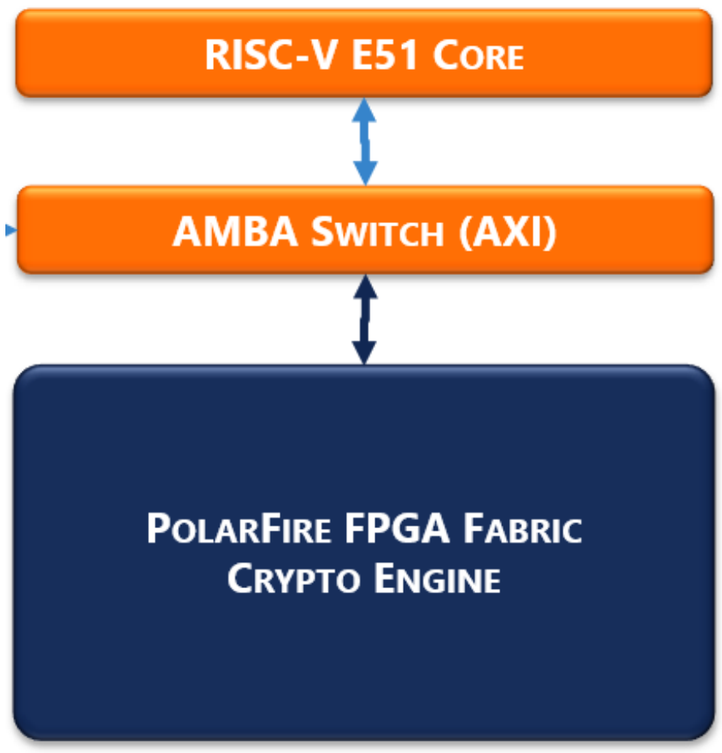
Safran E&D a besoin de certifier que tout firmware démarrant sur une plateforme RISC-V multicœur a été vérifié en intégrité et authenticité.

Lever un verrou technologique majeur : Intégrer des algorithmes de cryptographie post-quantique (NIST FIPS 205) dans le processus de démarrage sécurisé (Secure Boot), tout en garantissant un temps de démarrage minimum.

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 machine à états finis qui permet le cryptage et décryptage de clés et signatures

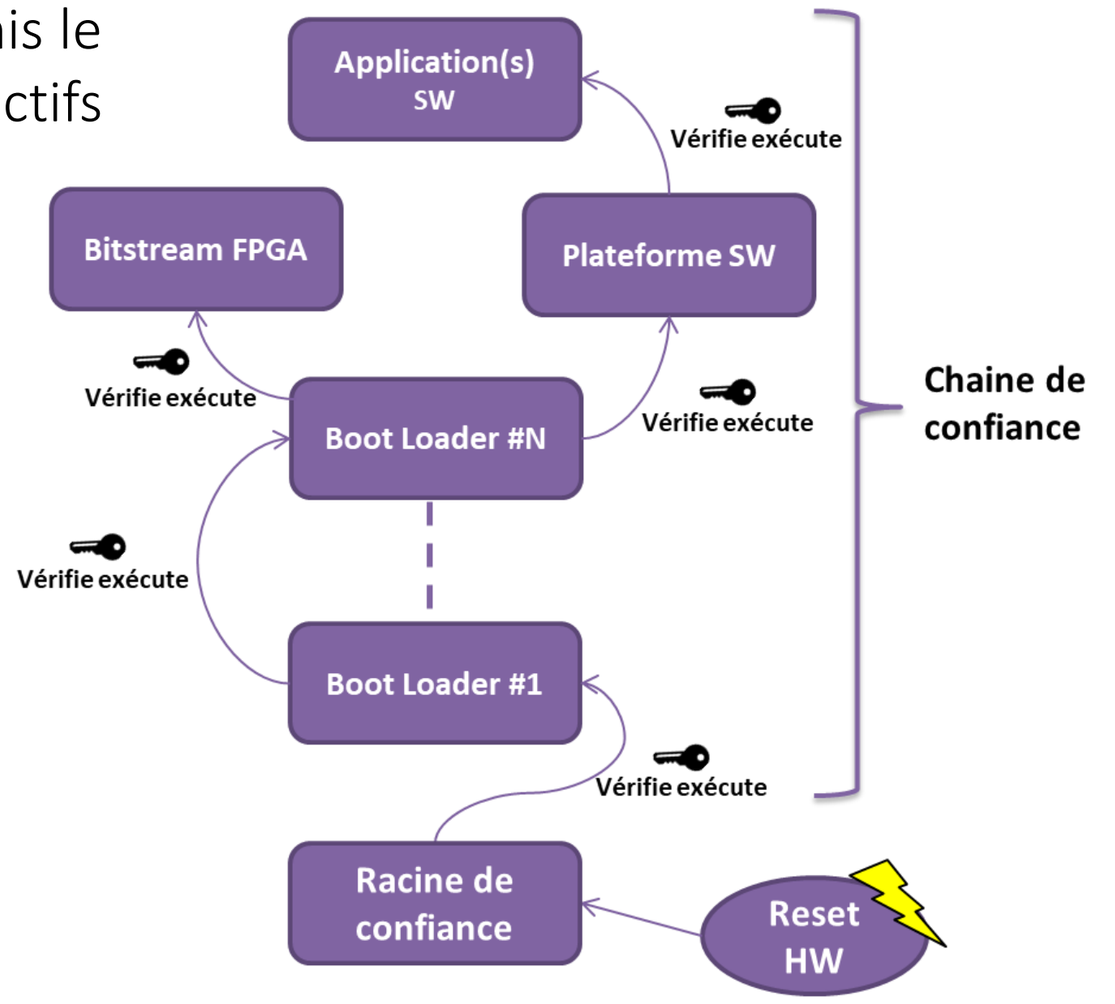
Le développement s'est fait en et en VHDL avec un versioning git .



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

RÉSULTATS ET CONCLUSION

La chaîne de confiance post-quantique, accélérée matériellement par le FPGA, garantit que tout firmware critique démarrant sur le calculateur est strictement intègre et authentique. Cette architecture hybride prévient toute exécution malicieuse face aux futures menaces quantiques, tout en respectant la contrainte de démarrage d'une seconde.



MOTS-CLÉS : RISC-V, Sécurité Embarquée , Secure Boot, Cryptographie post-Quantique VHDL