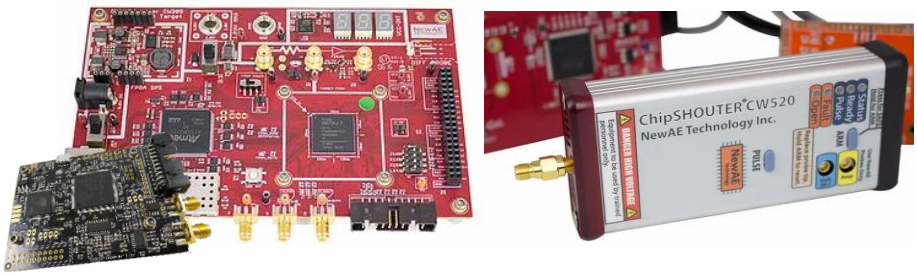
Fault Injection platform for Safety and Security Analyses on RISC-V (FISSA5)

Plate-forme d'Injection de Fautes pour Analyses de Sûreté et Sécurité pour RISC-V (IFASS5)

The RISC-V consortium has defined an open instruction set for a high-performance processor architecture adaptable to different usage scenarios. Today, there is a very large ecosystem that includes both proprietary and open-source solutions: in recent years, the platform has gained even more popularity, and several satellite projects and initiatives, both academic and industrial, have emerged. The adaptability of the RISC-V system is also confirmed by the fact that several major players are choosing it as a key element for Systems-on-Chips, 5G architectures, and automotive, where safety and security properties are critical and need to be assured.

This project concerns the implementation of a complete hardware platform for fault injection (clock, power supply, EM pulses), with a particular focus on RISC-V architectures. Dedicated boards allow easy and simple, though accurate, fault injection attacks on microcontrollers or FPGA chips, thanks to a development environment able to control glitches on global clock or power supply inputs. Additional equipment based on a pulse generator and a table bench is used to perform electromagnetic (EM) fault injections. EM attacks can be used effectively for safety and security evaluations, thanks to a high level of controllability (spatial position, power, timing, duration) that brings them closer to the performance obtained through laser injections, but without the same cost and complexity of implementation.



The platform will allow to:

(1) Analyze the fault models specific to the RISC-V architecture;
(2) Study the threats and vulnerabilities to safety and security of RISC-V based systems;
(3) Evaluate the different solutions addressing the system robustness and the state-of-the-art countermeasures (both hardware and software)
(4) Propose appropriate innovative solutions.

This platform completes the solution currently available on side channel analysis of power consumption and electromagnetic emissions.

This project is partially funded by the *Institut des sciences de l'information et de leurs interactions* of the *Centre National de la Recherche Scientifique* (CNRS-INS2I/AAP-SP-FEI-2021) and *IRT Nanoelec* (IRT40-CYBERSECURITE-2020)