# Secure protocol implementation for remote bitstream update preventing replay attacks on FPGA (Abstract)

Florian Devic
SAS NETHEOS &
LIRMM UMR - CNRS 5506
University of Montpellier 2
Montpellier, FRANCE
Email: f.devic@netheos.net

Lionel Torres
LIRMM UMR - CNRS 5506
University of Montpellier 2
Montpellier, FRANCE
Email: lionel.torres@lirmm.fr

Benoît Badrignans
SAS NETHEOS
Montpellier, FRANCE
Email: b.badrignans@netheos.net

**Abstract**

Nowadays, there is lot of applications where remote update for hardware systems is an essential service. Indeed, in high volume sale products or Space-based systems it is too expansive to retrieve the system in order to update it. Field Programmable Gate Arrays (FPGAs) are able to perform that with success. However, this feature may give rise to security flaw like spoofing and replay attacks. These attacks consist in tampering the update of the hardware configuration or in replaying an old bitstream to downgrade the system. Such an attack can be performed over a network when the FPGA-based system is remotely updated. Several security schemes providing encryption and integrity checking of the bitstream have been proposed in the literature. However, they do not detect the replay of old FPGA configurations; hence they provide adversaries with the opportunity to downgrade the system.

We focus on spoofing and replay attacks and propose a new protocol that both guarantees bitstream confidentiality, integrity and prevents old bitstreams replay. This work is the improvement and the implementation of previous presented ideas in order to achieve more flexibility. That is why we insist on the way to manage bitstream versions and to evaluate the area and performance overhead of this architecture.