# Supporting security and safety in open hardware platforms

September 24, 2023

## 1 Abstract

Open hardware reached impressive maturity. In the last decade, the research community proposed several methodologies, tools, and IPs providing a solid base for the development of open-hardware System-on-Chip. Multiple open platforms have been proposed. These ease the development of full System-on-Chips entirely made of open-source components and provide base platforms for the integration of commercial third-party IP components. Most mature open hardware platforms provide a complete and flexible workflow for the deployment of complete System-on-Chips. However, most of such platforms have not been completely developed with the main aim of security and safety. In modern SoCs, security and safety threats have been demonstrated to be possibly arising from multiple sources, either at the IP level or at the system level. Moreover, it has been demonstrated how a single IP module can have different methodologies to create safety and security issues able to compromise the whole system execution. To make a couple of examples, we have recently demonstrated that in modern SoCs dangerous conditions ranging from bandwidth stealing among modules to complete denial-of-service of shared resources can be triggered by a single compromised IP. Moreover, the access control system, a fundamental component for keeping the confidentiality and integrity of the system data, has been demonstrated to lead to major weaknesses if not properly deployed and verified. This is also witnessed by the MITRE consortium: out of 12 top hardware weaknesses published by MITRE, 6 of them are related to access control. Such security and safety issues have been mainly attributed to: (i) lack of specification in the communications standard for modern SoCs, which are mainly defined for flexibility and high performance, rather than safety and security; (ii) the specific implementation of the on-chip communication backbone; (iii) limited support for providing safety and security mechanism; and/or (iv) missing or superficial security verification. Nevertheless, the fully available codebase of mature open platforms provides an unprecedented opportunity for developing and testing innovative mechanisms and tools aimed at improving the safety and security of the system.

This talk introduces the work we are conducting to enhance the safety and security of open hardware platforms. Among all of the proposed open platforms, we mainly focus on the PULP platform from ETH Zurich and the ESP platform from Columbia University, as two of the most mature platforms currently available. We will cover different aspects of projects we are leading or to which we are directly collaborating related to: (i) development and verification of secure access control systems, (ii) mathematical timing analysis of open-hardware platforms to support time-critical operation in mission-critical systems (iii) secure and safe on-chip communication infrastructures based on the most common standard for on-chip communication in SoCs, (iv) security verification at the IP level and system level, and (v) an ad-hoc PULP-based platform integrating advanced safety and security mechanisms for mixed-critical systems. We are conducting our research projects in joint efforts with multiple academic and industrial partners, and we always welcome interested collaborators to join our efforts.

*Francesco Restuccia* is a postdoctoral researcher at the University of California, San Diego. He received his Ph.D. in Computer Engineering (cum laude) from Scuola Superiore Sant'Anna Pisa, Italy, in 2021. He authored and co-authored multiple research articles regarding hardware security, on-chip communications, timing and performance analysis of heterogeneous platforms, cyber-physical systems, and time-predictable hardware acceleration of DNN algorithms on heterogeneous platforms. He was program co-chair of the 2nd Real-time And intelliGent Edge computing (RAGE) workshop, held in conjunction with CPS-IoT week 2023, and co-founder and general chair of the Safety and Security in Heterogeneous Open System-on-Chip Platforms workshop (SSH-SoC) workshop, held in conjunction with DAC 2023.