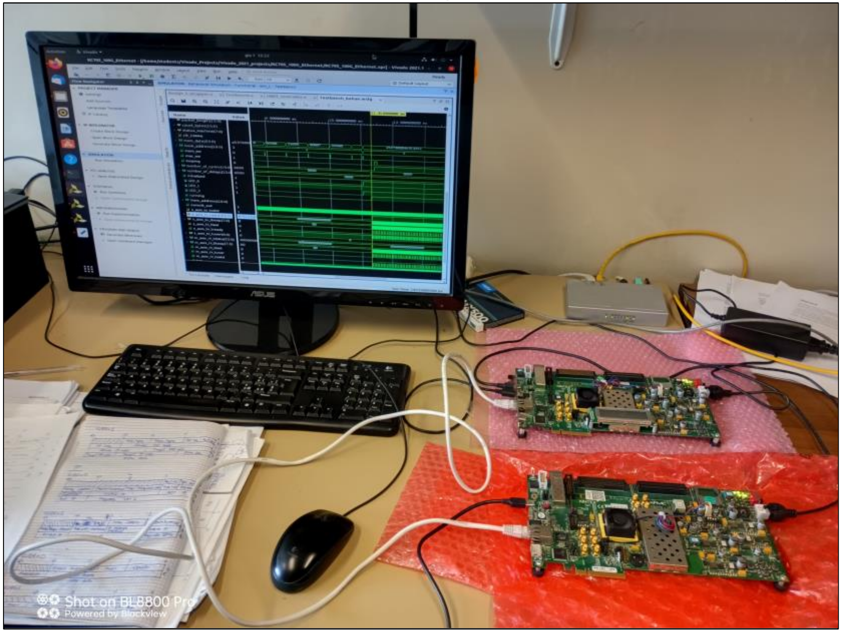
16th Topical Seminar on Innovative Particle and Radiation Detectors (IPRD23) 25-29 Sep. 2023 Siena, Italy
Topic: **Outreach**
Title: **Protecting experimental data using custom-designed Firewall Hardware**

Authors: *A. Gabrielli*[1,2], F. Alfonsi[2], M. Grossi[1,2], M. Prandini[3]
1) Physics and Astronomy Department – University of Bologna
2) INFN – Bologna
3) Department of Computer Science and Engineering – University of Bologna

Abstract: As can be seen from the document PNR 2021-27, points 2.4 and 4.6 (Accompanying the development f a new generation of researchers, technologists, and knowledge transfer professionals), the training of young researchers with high scientific skills it is a relevant point. In fact, the proposal for a development of **FireWall Hardware** also has the objective of training young researchers with high technological skills who can be absorbed in a local and international market. For this reason, the project incorporates the skills acquired in years of research by the Department of Physics and Astronomy in the field of data acquisition electronics on large experiments in high energy physics at CERN. In particular, the project develops and uses design skills of latest generation commercial programmable devices, such as FPGAs with characteristics compatible with the specifications and standards of modern communications and telematic transmissions. These topics perfectly complement the topics of information security against external intrusions, covered within the framework of this project. Furthermore, the skills and experience of the authors in the field of cryptography and computer security, complementary to the electronic skills, complete the knowledge useful for the development of a project of excellence. The creation of a **FireWall Hardware** prototype, with possible engineering and marketing through a commercial partner, could therefore guarantee future industrial development as suggested by the PNR. The project aims at the use of latest generation FPGA devices, such as the components of Xilinx, UltraScale+ family, which can manage a throughput of tens of TB/s since they are precisely oriented towards modern telecommunications. It is evident how a **FireWall Hardware** device, dynamic in that it can be programmed at all firmware levels, can constitute not only an information security element for an intelligent network system, but also an element of symbiotic exchange of skills between universities, industry, and research centers. In fact, for research institutions (CNAF-CERN) that need huge data exchange between remote machines (mirrors), the possibility of increasing security from intrusions and attacks also coming from the Internet is today of increasingly fundamental importance.



Summary: A **FireWall Hardware**, working in sniffer mode, has been designing in Verilog and implemented using the KC705 development board that integrates the Xilinx XC7K325T-2FFG900C FPGA, see the figure. Two KC705 boards have been used: one to design the **FireWall Hardware**, capable to analyse the frames present at the Ethernet port, and the other to design a frame generator, capable to generate Ethernet frames of different lengths and types. We are using programmable inter-frame delay and a maximum data rate of 1 Gb/s to test the system performance. The **FireWall Hardware** is aimed at providing statistics of the Ethernet frames present at the input of the Ethernet port (length, protocol type, presence of corrupted data) and to discriminate the Ethernet traffic according to rules based on IP addresses, source and destination ports and level 4 protocol. All the communications between the FPGA boards and a PC used for data visualization and are realized using the UART communication protocol and handled by software designed by LabVIEW (National Instruments). The **FireWall Hardware** is tested with a set of Ethernet frames and the results have shown it can perform the required operations efficiently and reliably.