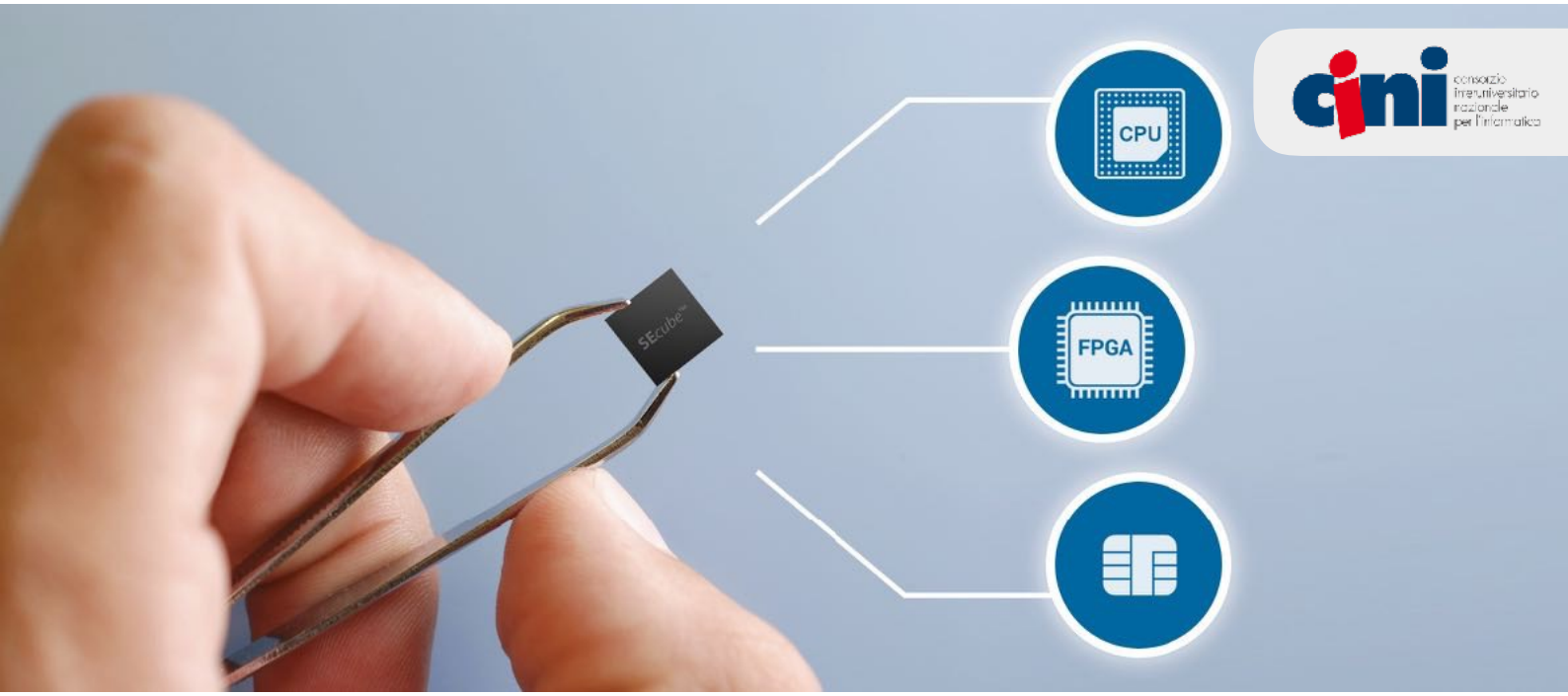
Case Study

SEcube™

Future-proof reconfigurable silicon



Background

Since 1960, reconfigurable architectures have evolved and there is a wide consensus that they are a promising solution to bridge the gap between ASIC performance and processing flexibility. The electronic industry, from traditional markets (smartphones and PCs) to innovative fields of application (automotive, industrial, IoT, AI, Machine Learning and Data Mining) has been the driving force behind new semiconductor technologies. Catering for advanced functionalities they require improved computational performance and flexibility. Reconfigurable hardware based on FPGA empowers developers and system integrators to address the complexity of today smarter devices by developing programmable solutions based on fixed hardware.

Challenge

As levels of integration grow, PCBs become more complex in terms of number of components and multi-layer boards, hence the higher the probability of incorrect connections. Besides, successful designing and testing of a working system are coming under increasing time pressure.
Attempts were made by manufacturers to design hybrid FPGA+CPU chips in a single chip, however all the communication interfaces and memories, would still be on the main PCB board. Crafting new ways to combine hard CPU cores with programmable logic while addressing security is the future.

Industry

Electronic Manufacturing Services (EMS)
Joint Design Manufacturing (JDM)
Outsourced Design Manufacturing (ODM)

Challenges

- Pressure to develop systems to meet evolving standards
- Extended designers' freedom to system alterations after production without hardware redesign

Goals

- Empowering application designers to run execution codes safely and efficiently
- Provide equipment designers with the flexibility to increase functionalities or integrate custom elements to their designs without requiring the use of multiple devices

Solution

- SEcube™ is a System-on-Chip embedding 3 main cores: a highly powerful processor, a EAL5+ Common Criteria certified security controller and a high-performance FPGA

Solution

Many equipment developers face the challenge that design requirements may change or there is a need to reuse an existing semiconductor device in a new design. These circumstances often require the use of additional semiconductor devices in order to meet the equipment design goals.
Growing design complexity and cost has forced designers to build programmability into System-on-Chip (SoC) designs to reduce the number of costly chip re-spins, and amortise chip development costs. Programmability in the form of field programmable gate array (FPGA) is an answer to meet these challenges. FPGAs can be focused on a particular task and run it more efficiently than a same task defined in software, running on a general-purpose processor. With FPGAs developers are given full freedom to define runtime the architecture, which best suits their application.
While addressing the above issues, Blu5 is going far beyond offering a System-on-Chip combining a powerful microprocessor, including a wide number of peripherals and embedded memories, with tightly coupled FPGA fabric and a EAL5+ Common Criteria certified Security Controller on a single and compact (9x9mm) BGA device: SEcube™.
Implementation of SEcube™ is particularly ideal for complex and computationally intensive tasks as well as demanding security applications. Adaptive and configurable platform, SEcube™ allows developers to add application-specific functions that normally would require spinning custom ASICs.

Benefits

- Increased hardware design flexibility
- Fast prototyping
- Rapid application development
- High reliability
- Low power
- Efficient parallel programming
- Tamper protections
- Established development environment
- Open-source

> “A programmable hardware resource within a tamper-resistant chip makes SEcube a leader solution for flexibility, efficiency and security all-in-one”
>
> Prof. Paolo Prinetto,
> President of CINI

CINI coordinates research and training activities in the field of Information Security on a national and international scale with the ultimate objective to support the National Italian Authorities to thwart cyber threats, making it a more resilient Country. CINI is committed to improving the protection measures of the Public Administration and Enterprises from cyberattacks and is actively involved in the definition of the National standards and methodologies. https://www.consorzio-cini.it

Blu5 Group
info@blu5group.com
www.blu5group.com