SELF-RECONFIGURABLE SECURITY-ENHANCED COMMUNICATIONS IN FPGA-BASED MPSOCS

Pascal Cotret, Guy Gogniat, Jean-Philippe Diguet, Jeremie Crenne

Nowadays, security is a key constraint in MPSoC development lifecycle as many critical and secret information can be stored and manipulated in these systems. Monitoring and controlling communications is a method to protect an embedded system from classic attacks such as malicious accesses to restricted components. This work proposes security enhancements based on Block RAMs and AES-GCM ciphering to provide the designer an AXI-compliant design where no user intervention is required for reconfiguration of security services. A Virtex-6 FPGA implementation (with a set of miBench and custom applications) demonstrates a reduction up to 33% in terms latency overhead compared to an unprotected multiprocessor architecture and an area overhead around 10% for the reconfiguration logic.