Università della Svizzera italiana | Faculty of Informatics | Advanced Learning and Research Institute

Reconfigurable Architectures Workshop - RAW 2010

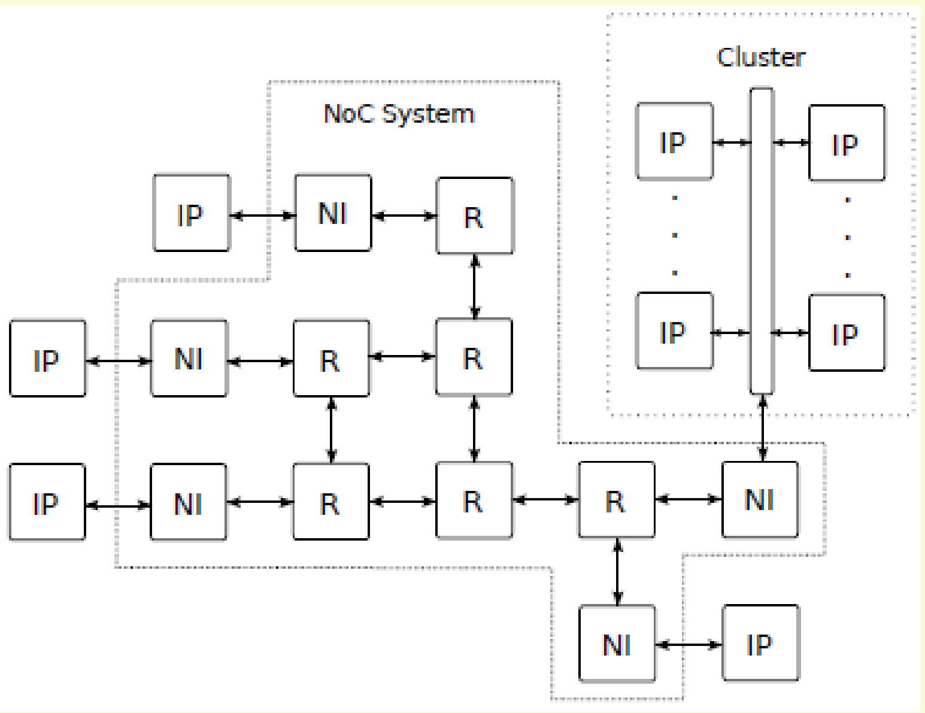
Stack Protection Unit as a step towards securing MPSoCs

Slobodan Lukovic, Paolo Pezzino, Leandro Fiorin
{lukovics, pezzinop, fiorin} @ alari.ch
Faculty of Informatics/ALaRI
University of Lugano
Lugano/Switzerland

Abstract

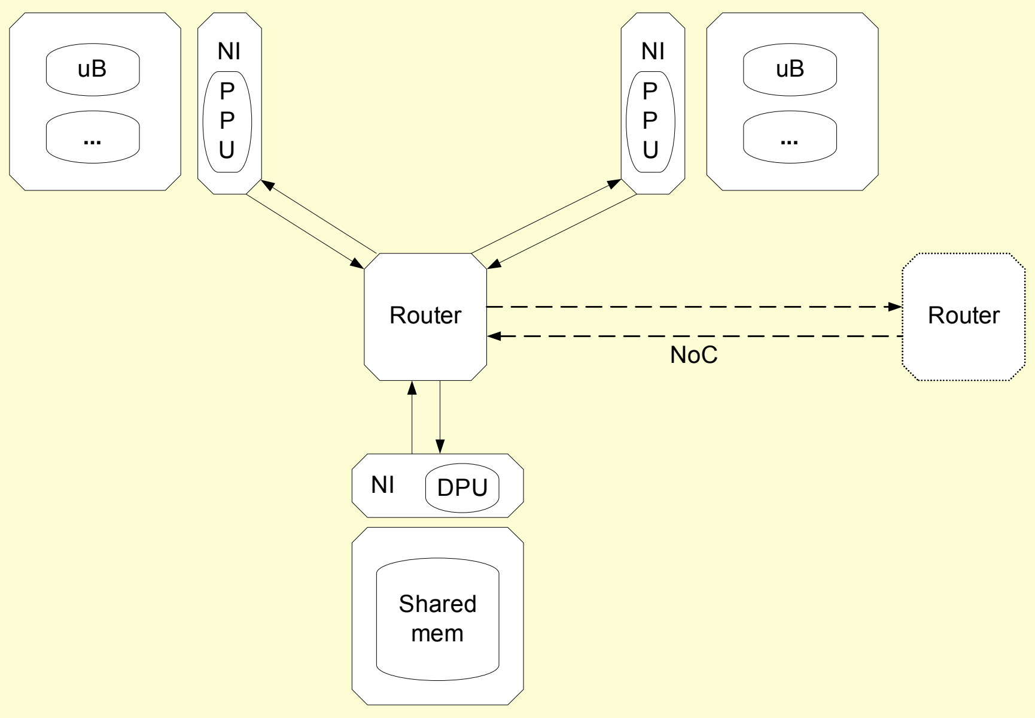
Multi-Processor System-on-Chip (MPSoC) architectures, in particular Network-on-Chip (NoC) based ones, have emerged as a design concept to cope with increased complexity of modern applications. However, the increasing heterogeneity, coupled with possibility of reconfiguration, makes security become one of major concerns in MPSoC design. The protection strategies must consider security at both - component and system level. This work present one possible approach to these issues

NoC based MPSoCs



MPSoCs consist of computational, memory and communicational elements.

Our approach considers securing each of these components but also the system as a whole.

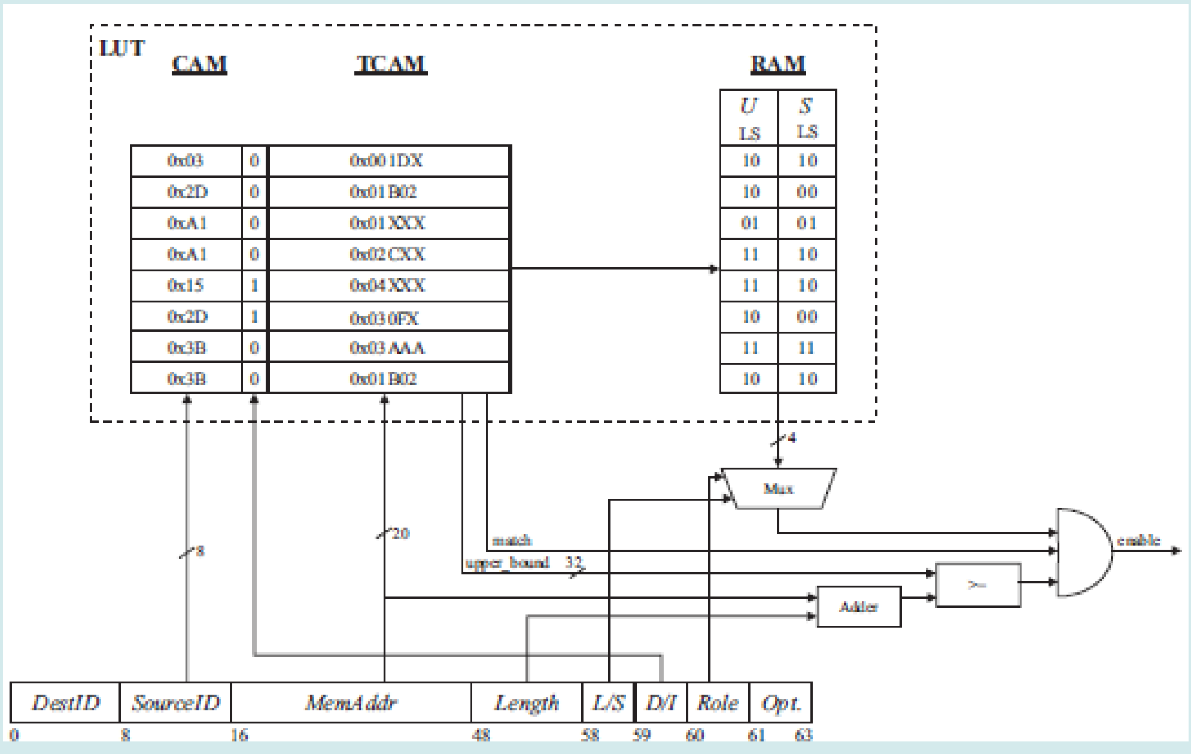


Network-on-Chip (NoC) comprises Network Interfaces (NIs) and Routers.

NIs implement security interaction with cores

The system is realized on FPGA (Virtex-II Pro board)

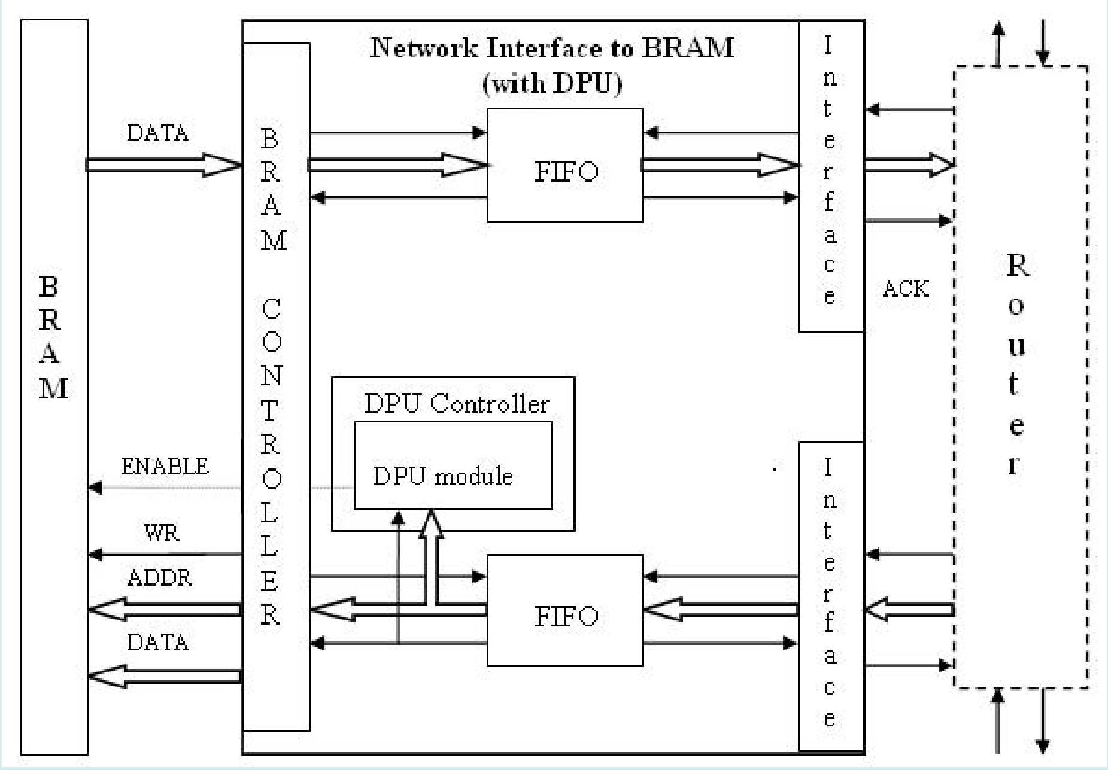
Securing memory elements



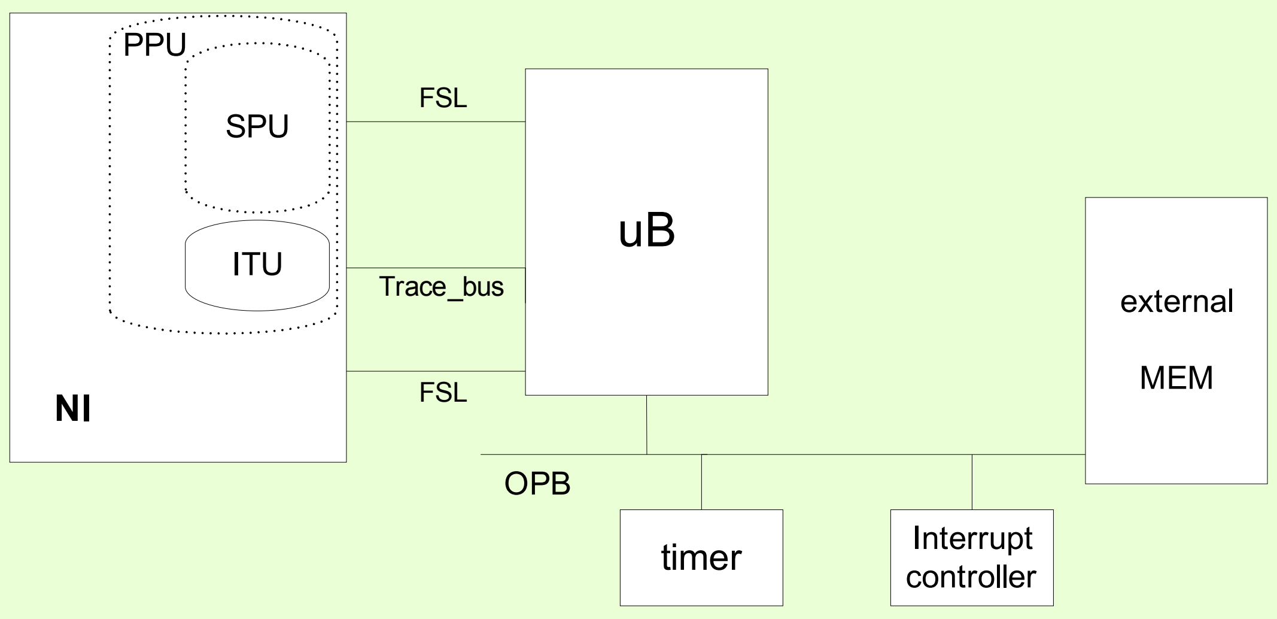
Data Protection Unit (DPU) has been developed as a module embedded into NI attached to shared memory elements to filter access to these cores.

It is a look-up table based

The cost (i.e. occupied area) of the implementation is around one quarter of the microBlaze.



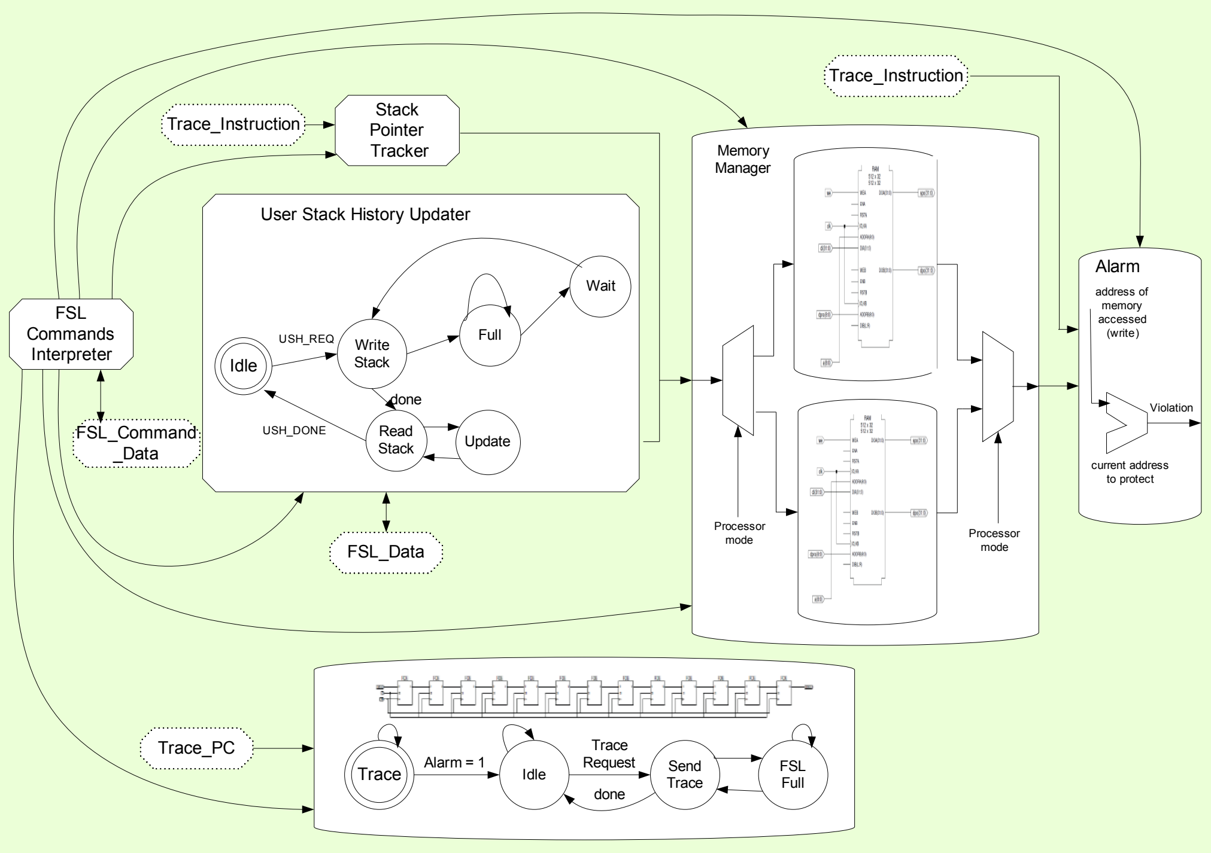
Securing processing elements



Stack Protection Unit (SPU) replicates functions' return addresses and verifies them on each context switch .

It prevents from buffer overflow type of the attack

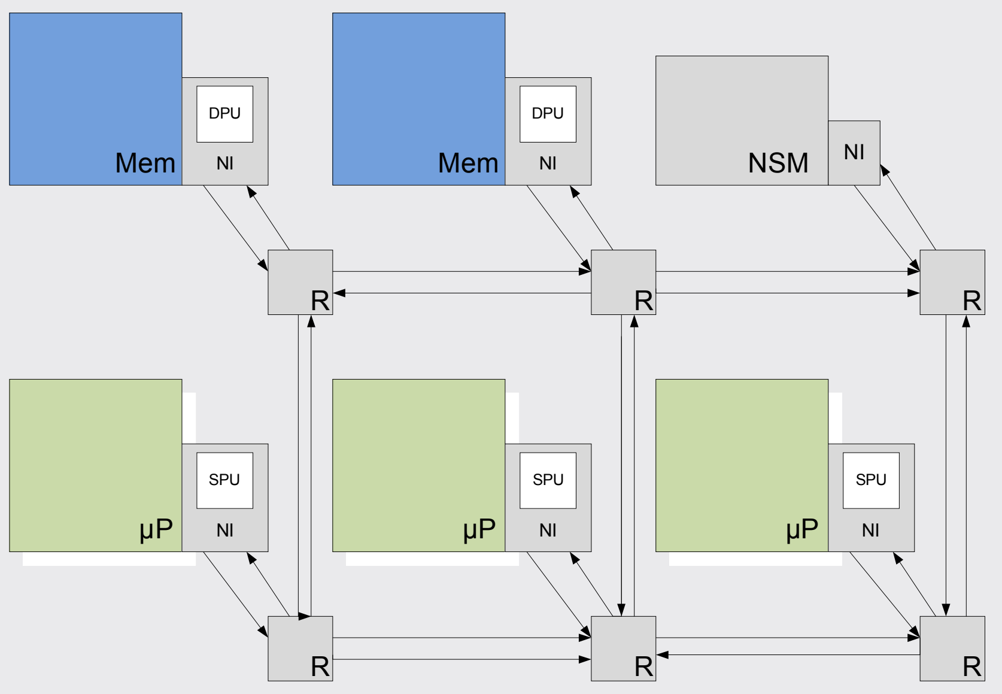
The cost of the implementation is around one fifth of the area occupied by a microBlzaze



System level security

Network Security Manager (NSM) implements centralized security policies. It monitors system behavior based on interaction with protection modules implemented in NIs.

The communication of security related messages is performed over autonomous 'security' NoC



Conclusions and ongoing work

Efficient security strategies for NoC based MPSoCs require hierarchical approach that considers protection of each system component as well as system as a whole. Presented work shows one approach to the problem. The proposed solutions are realized and verified in FPGA on Virtex-II board. Ongoing work considers integrated full protection solution that would be able to monitor the system and act autonomously

ALaRI Institute, Faculty of Informatics, University of Lugano