SAND2016-7628C

Exceptional service in the national interest

Sandia National Laboratories

Authenticating Treaty Processor Systems: An Evaluation Framework

Presented at INMM 57th Annual Meeting
July 27, 2016

Jay Brotz[1]
Ross Hymel[1]
Neil Grant[2]
Neil Evans[2]

[1]Sandia National Laboratories, Albuquerque, NM
[2]Atomic Weapons Establishment, Aldermaston, UK

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Problem Statement

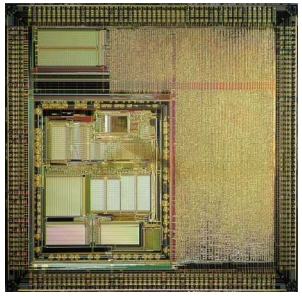
Sandia National Laboratories

- Cooperative treaty verification and monitoring equipment has a unique challenge:
  - Both parties to a treaty need to trust the measurements and data collected
  - If the host provides the equipment, the inspector needs to authenticate it
- Inspector authentication of equipment is more difficult for complex components
- Processing elements are likely to be the most complex components, and thus the most difficult to verify

Processing Options

Sandia National Laboratories

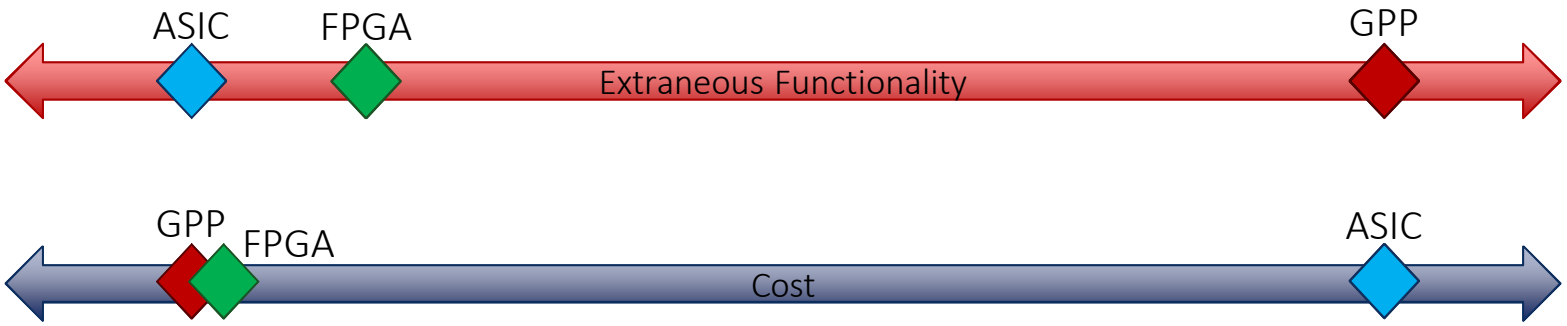
ASIC



FPGA

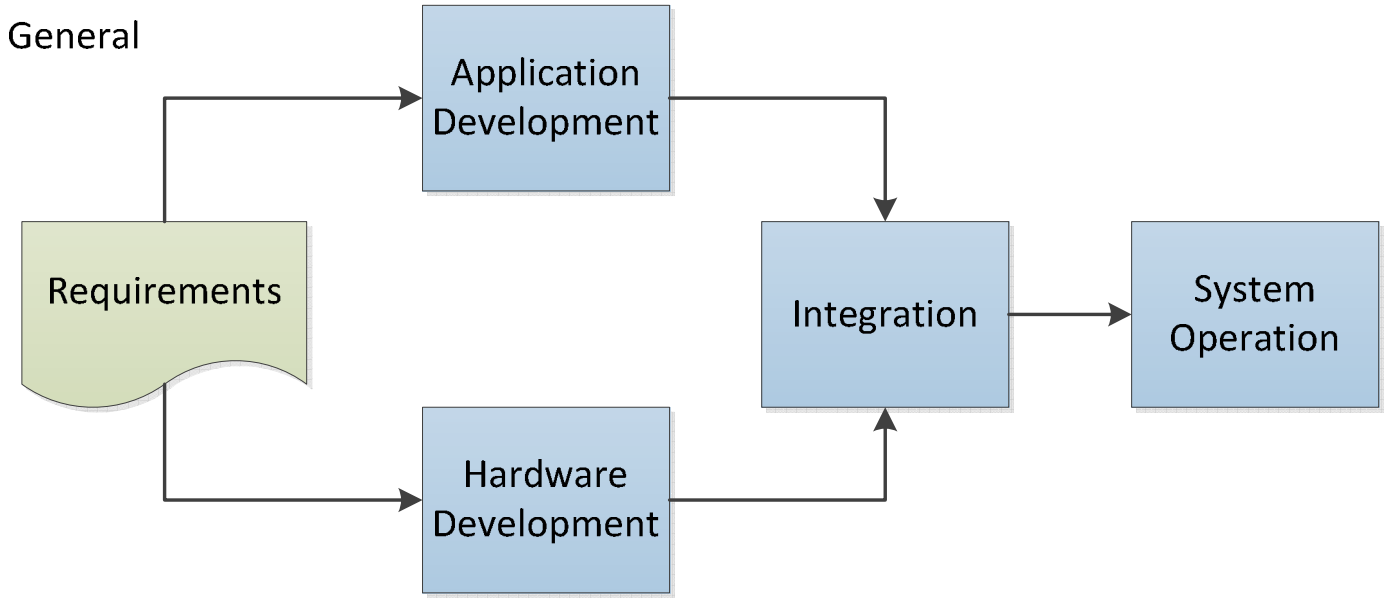
General Purpose Processor (GPP)

```c
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <arpa/inet.h>

void serveur1(portServ ports)
{
    int sockServ1, sockServ2, sockClient;
    struct sockaddr_in monAddr, addrClient, addrServ2;
    socklen_t lenAddrClient;

    if ((sockServ1 = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
    perror("Erreur socket");
    exit(1);
    }
    if ((sockServ2 = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
    perror("Erreur socket");
    exit(1);
    }

    bzero(&monAddr, sizeof(monAddr));
    monAddr.sin_family = AF_INET;
    monAddr.sin_port = htons(ports.port1);
    monAddr.sin_addr.s_addr = INADDR_ANY;
    bzero(&addrServ2, sizeof(addrServ2));
```

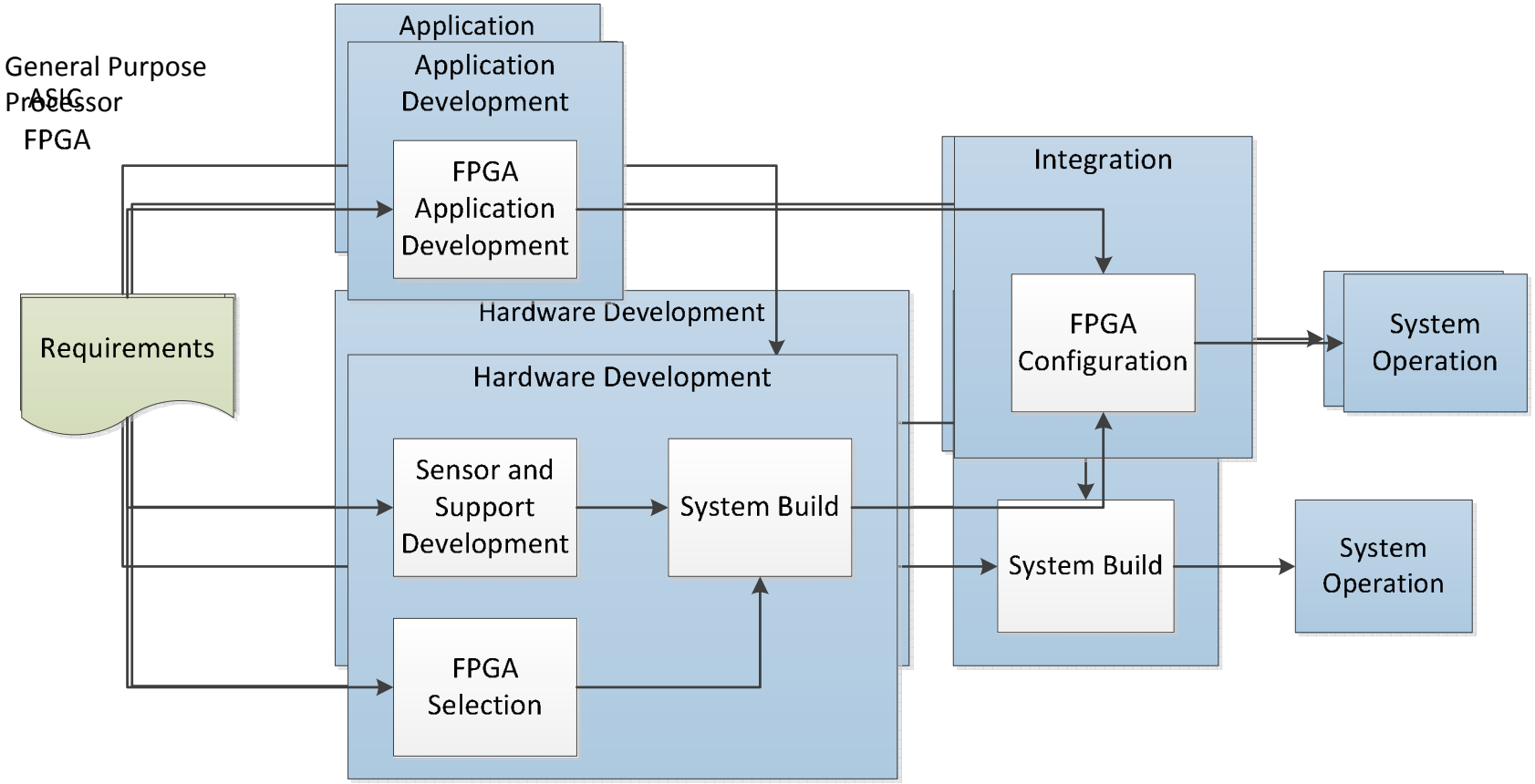


ASIC = application specific integrated circuit
FPGA = field-programmable gate array

General Development Model



Development Models

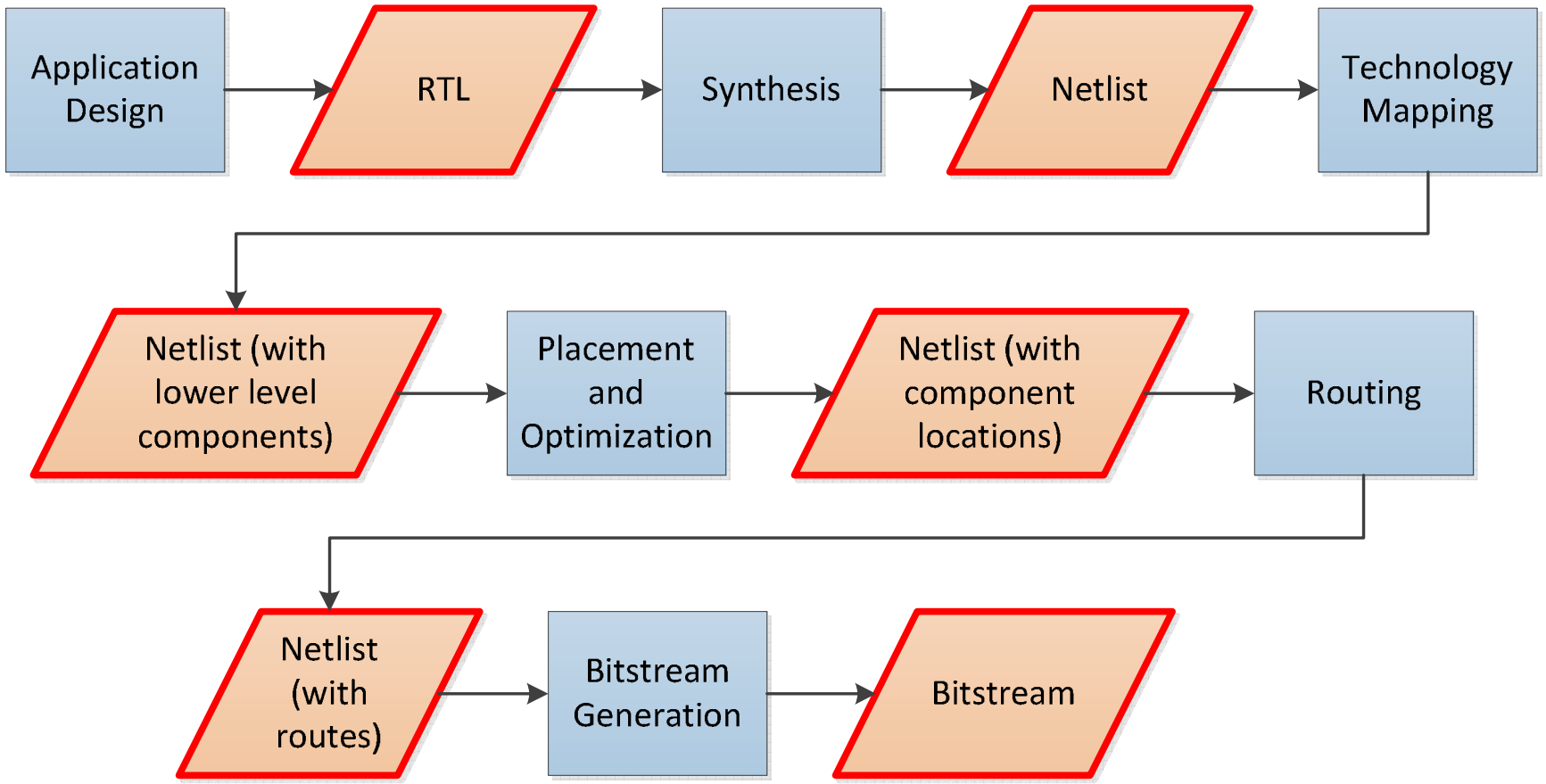


Authentication Objectives

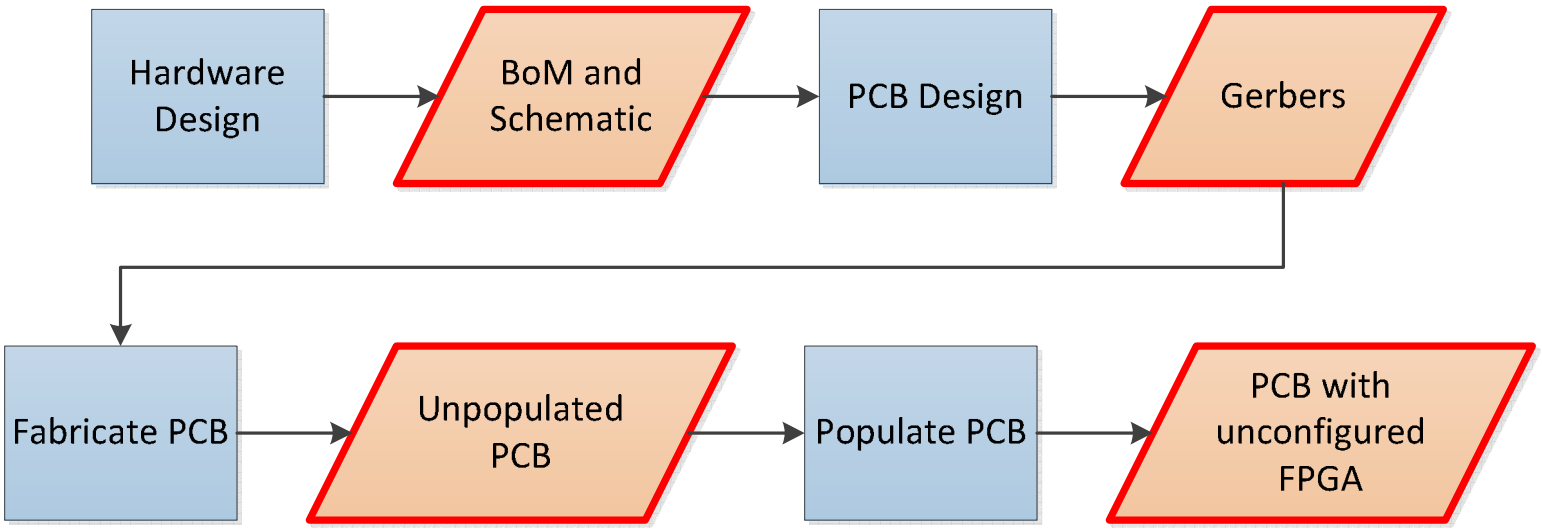
Sandia National Laboratories

- The inspecting party wants to ensure that:
  - The application development outputs and the hardware development outputs (designs) meet the functionality captured in the requirements and do not exhibit any other functionality;
  - Any intermediate outputs within the application development or hardware development phases have not injected unwanted functionality (and are therefore functionally equivalent to the initial design);
  - The built system is completely functionally equivalent to the verified design; and
  - The built system in operation is not functionally altered at any point.

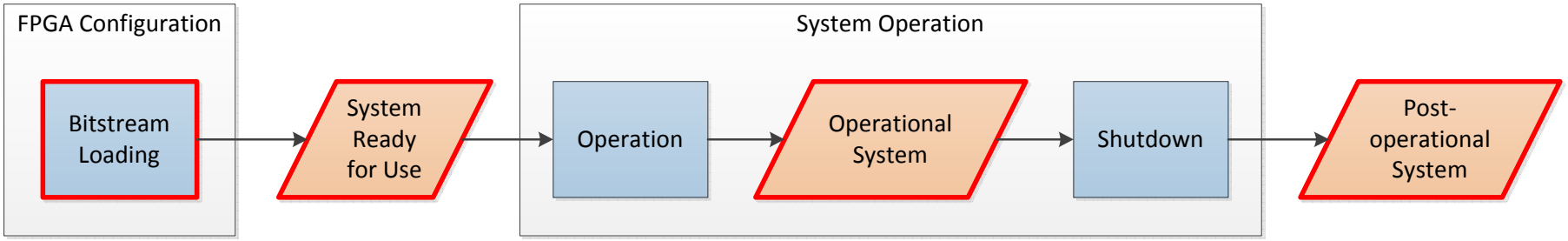
FPGA Example: Application Development



FPGA Example: Hardware Development



FPGA Example: Integration and System Operation



Conclusion

- Using the framework described:
  - authentication methods for the entire development cycle of processing design can be researched and evaluated,
  - different processor types or architectures could be analyzed for the ease of authentication, and
  - authentication evaluations can lead to better design for trust.

- The authors would like to acknowledge the National Nuclear Security Administration Office of Nuclear Verification and the UK Ministry of Defence for their generous support of this research.