FPGAs: High Assurance through Model Based Design

AADL Workshop
24 January 2007
9:30 - 10:00

Yves LaCerte
Rockwell Collins
Advanced Technology Center
400 Collins Road N.E.
Cedar Rapids, IA 52498
ylacerte@rockwellcollins.cm
FPGA

- FPGAs comprise an array of configurable logic blocks and interconnect resources
  - 200,000+ logic blocks
  - 1,000 I/O pins

- Look-up table (LUT)
  - small one bit wide memory array
Typical Application

- Advanced Encryption Standard (AES)
  - more physically secure in hardware
    - cannot easily be read or modified by an outside attacker
  - easily achieve Gigabit encryption rates and at least one order of magnitude faster than the best reported software
    - parallelization (pipelining and sub-pipelining) of the loop structure
    - wide operand processing (e.g., 128 bits in one clock cycle)

- An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists
  » AJ Elbirt, W Yip, B Chetwynd, C Paar
## Performance Characteristics

<table>
<thead>
<tr>
<th>Performance Characteristics</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target FPGA device</td>
<td></td>
</tr>
<tr>
<td>Maximum master clock frequency</td>
<td>__ MHz</td>
</tr>
<tr>
<td>Throughput</td>
<td>__ Gbit/s</td>
</tr>
<tr>
<td>Area [CLB slices]</td>
<td>__ CLB slices</td>
</tr>
<tr>
<td>Area [percentage of the target device resources]</td>
<td>__ % of CLB slices</td>
</tr>
<tr>
<td>Area [Block RAMs]</td>
<td>__ Block RAMs</td>
</tr>
<tr>
<td>Area [percentage of the target device resources]</td>
<td>__ % of Block RAMs</td>
</tr>
<tr>
<td>Power consumption</td>
<td></td>
</tr>
</tbody>
</table>
Typical Development Process

- Specifications
- System Model / C Code
- RTL Description (VHDL or Verilog)
- Synthesis
- FPGA Place and Route
- RTL Simulation / Timing
- Gate Level Simulation
- Post Layout Simulation / Timing
- Static / Dynamic Analysis
The Challenge

- Transform system specification into a system model suitable for FPGAs
  - E.g. Impulse C
    - Commercial version of Streams-C (Los Alamos National Lab)

- Add significant complexity
  - E.g. High Assurance MILS I/O application
    - Provably correct \( \approx 5,000 \) lines of code
    - Provably partitioned from the rest of the FPGA
    - Total application over 50,000 lines of code
Implications

• Build a system model in Impulse C
  - Highly parallelized implementation of system specs
  - When is there enough parallelization?

• Architecture elements
  - Processes, streams, signals, memory
  - Clocking strategies

• High Assurance
  - Prove correctness of security properties
  - Prove MILS spatial partitioning
Ease The Burden

• Provably correct model transformations

• Helps High Assurance certification

• Model and analyze early
  - Analysis performed at design time, before detailed simulation of completed code

• Use architecture description language
Automated Transformations

• Model transformation
  - Transform a model into another model
    • From system specification to Impulse C ...
    • From processes and streams into standardized, error free code

• Modeling blurs the distinction between HW and SW engineers

Shift toward application domain expertise
Reduce Intellectual Gap

Specifications

System Model / C Code

RTL Description (VHDL or Verilog)

Synthesis

FPGA Place and Route

Static / Dynamic Analysis

RTL Simulation / Timing

Gate Level Simulation

Post Layout Simulation / Timing

?
Enhanced Process

Specifications

Architecture Model

System Model / C Code

RTL Description (VHDL or Verilog)

Synthesis

FPGA Place and Route

Architecture Analysis

Static / Dynamic Analysis

RTL Simulation / Timing

Gate Level Simulation

Post Layout Simulation / Timing

Transform

Transform
Transformations

Transform

Architecture Model

Platform Independent Model

Transform Rules

Platform Specific Model

System Model / C Code

Transform

Architecture Analysis

Transform

Clock Strategy

Process B

Memory

Process E

Process G

Low Bandwidth
Asynchronous

High Bandwidth
Synchronous

Process C

Process F

Deployment

Process D

Execution

Port Depth

Process A

Process C

24 January 2007

© Copyright 2006 Rockwell Collins, Inc. All right reserved.
Transform to System Model

From code-oriented to model-oriented production techniques

Clear separation of the fundamental logic of the specification from the particular implementation
Architecture Model

Building blocks for FPGA hardware and computational models using Streams C language

Processes, Ports, and Connections

Memory utilization

Deployment and execution constraints
Architecture Analysis

Architecture Analysis and Design Language (AADL)
Architecture description language
SAE standard AS5506

Models structure and high-level constraints of embedded computer systems

Abstract specifications with general system design concepts
Components, interconnections, hierarchy, data flow, etc.

Concrete Specifications
Properties (custom name/value pairs)
Annexes (non-standard language embedded in AADL specifications)
## AADL / FPGA Concepts

<table>
<thead>
<tr>
<th>Impulse C concept</th>
<th>AADL concept</th>
<th>Adaptation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process (or thread)</td>
<td>Process</td>
<td>Fixed execution rate. Possibly depends on a global clock. If using thread, one per process.</td>
</tr>
<tr>
<td>Streams</td>
<td>Data Port</td>
<td>Ports have depth and width.</td>
</tr>
<tr>
<td>Signal</td>
<td>Event Port</td>
<td>Occasional communication. Typically for synchronization.</td>
</tr>
<tr>
<td>Memory</td>
<td>Memory</td>
<td>Many FPGA implementations possible.</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Defines the payload of a stream.</td>
</tr>
<tr>
<td>Connections</td>
<td>Connectors</td>
<td>AADL Bus and information flow</td>
</tr>
</tbody>
</table>
Example – MILS I/O

- Multiple independent levels of security (MILS)
  - Provides multi level enforcement by strict separation (the I in MILS)
  - A given separation (or partition) may hold a single level of classification, or multiple single level (MSL)

- AADL experience with modeling MILS OS

- MILS applied to FPGA
  - Separation of logic and pins
Example - MILS I/O

High Assurance Component

Trusted App on trusted OS makes high assurance I/O decision

Trusted FPGA makes high assurance I/O decision

Sensor Feed
Example – MILS I/O

Specifications
Architecture Model
System Model / C Code
RTL Description (VHDL or Verilog)
Synthesis
FPGA Place and Route

Transform

Architecture Analysis
Static / Dynamic Analysis
RTL Simulation / Timing
Gate Level Simulation
Verification tool

AADL model and analysis artifacts

MILS FPGA implementation and verification
Conclusions

• FPGAs are important computational devices
  - Traditionally the domain of hardware engineers
  - Moving toward complex systems

• FPGAs have many “shared resource” issues of traditional computational devices
  - Performance parameters are somewhat different
Conclusions

• FPGA algorithm implementations
  - High quality through model transformations
  - Rapid through analyses of models

• Models and analyses are necessarily coarse grained

• Notions extensible to any FPGA and any code base

• FPGAs can be High Assurance
  - MILS partitions proven through Verification Tool (logic and pins)