Rockwell Collins
Building trust every day

FPGAs: High Assurance through Model Based Design

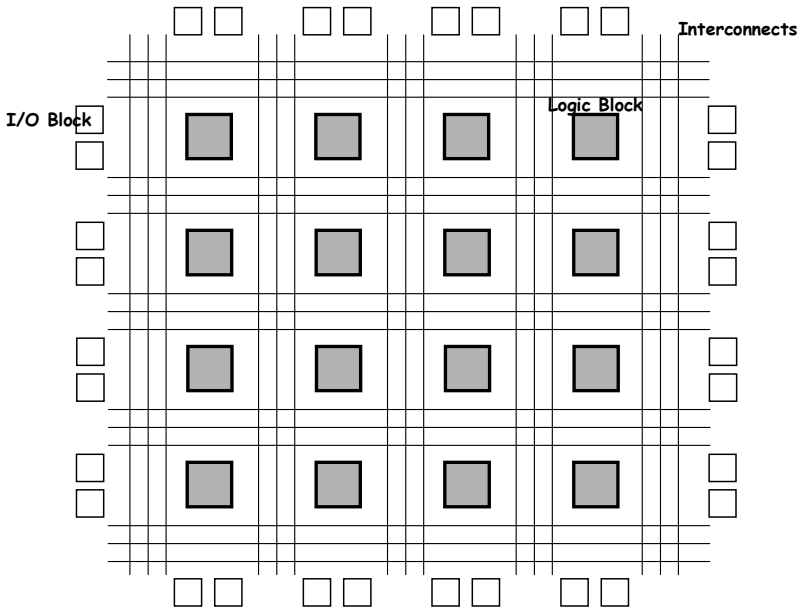
AADL Workshop
24 January 2007
9:30 – 10:00

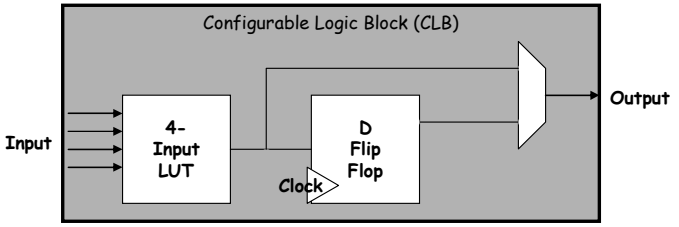
Yves LaCerte
Rockwell Collins
Advanced Technology Center
400 Collins Road N.E.
Cedar Rapids, IA 52498
ylacerte@rockwellcollins.cm

Rockwell Collins

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
        - » http://csrc.nist.gov/CryptoToolkit/aes/round2/conf3/papers/08-aelbirt.pdf

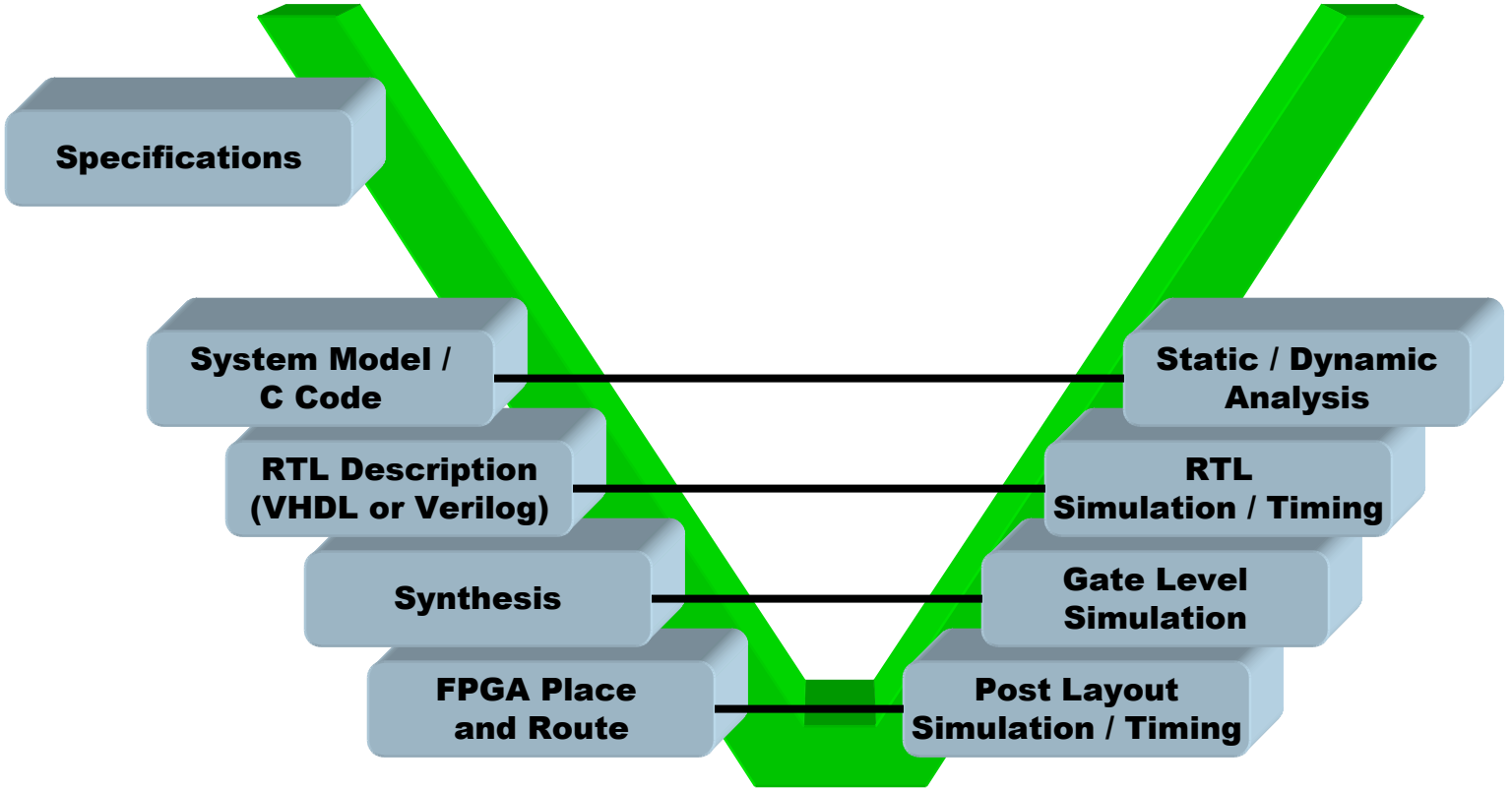
Rockwell Collins

Performance Characteristics

Performance Characteristics	Values
Target FPGA device	
Maximum master clock frequency	__ MHz
Throughput	__ Gbit/s
Area [CLB slices]	__ CLB slices
Area [percentage of the target device resources]	__ % of CLB slices
Area [Block RAMs]	__ Block RAMs
Area [percentage of the target device resources]	__ % of Block RAMs
Power consumption	

Rockwell Collins

Typical Development Process



Rockwell Collins

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 ≈ 5,000 lines of code
    - Provably partitioned from the rest of the FPGA
    - Total application over 50,000 lines of code

Rockwell Collins
Building trust every day

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

Rockwell Collins

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

Rockwell Collins
Building trust every day

Automated Transformations

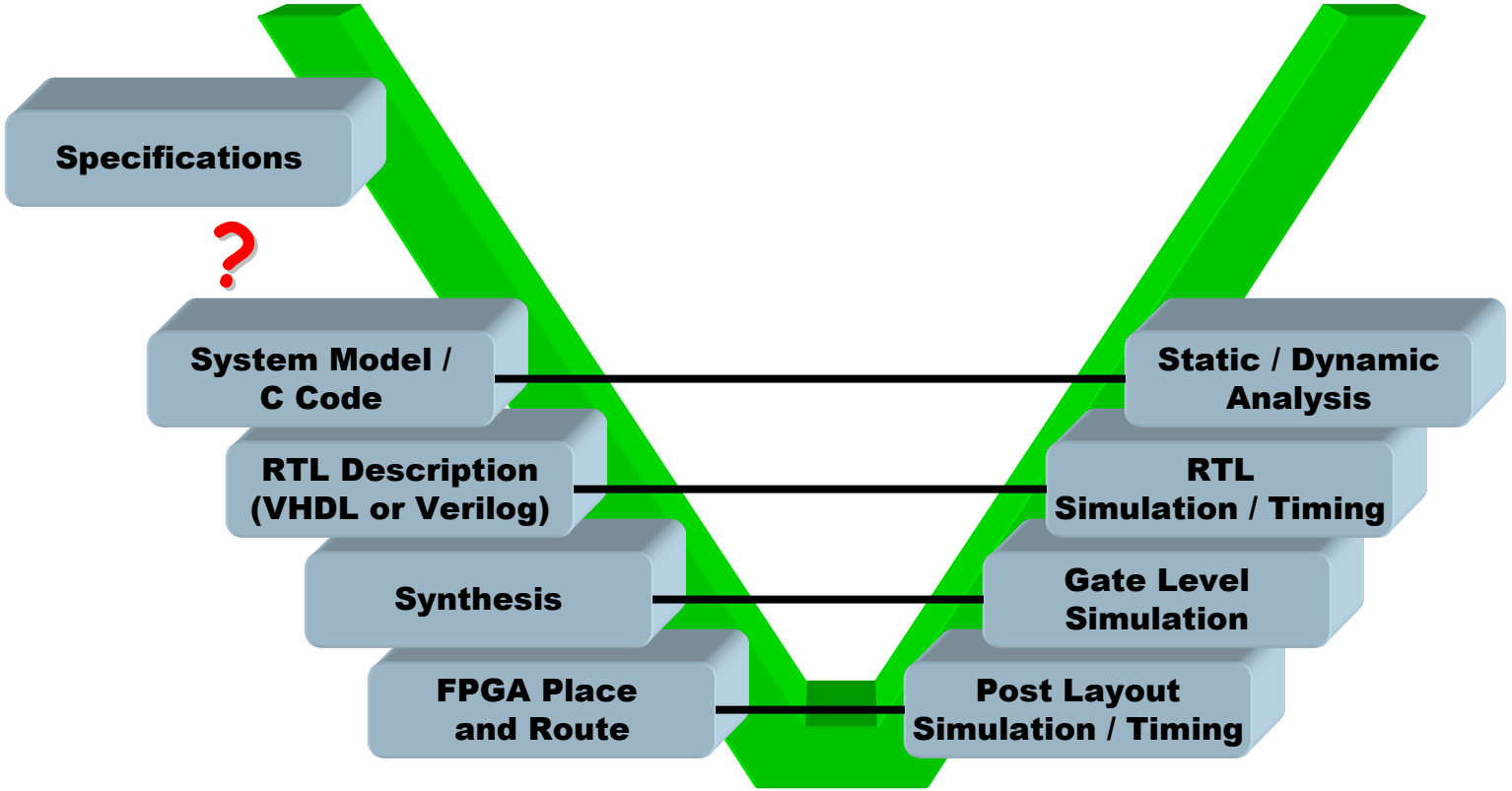
- Model transformation
  - Transform a model into another model
    - From system specification to Impulse C …
    - From processes and streams into standardized, error free code

- Modeling blurs the distinction between HW and SW engineers

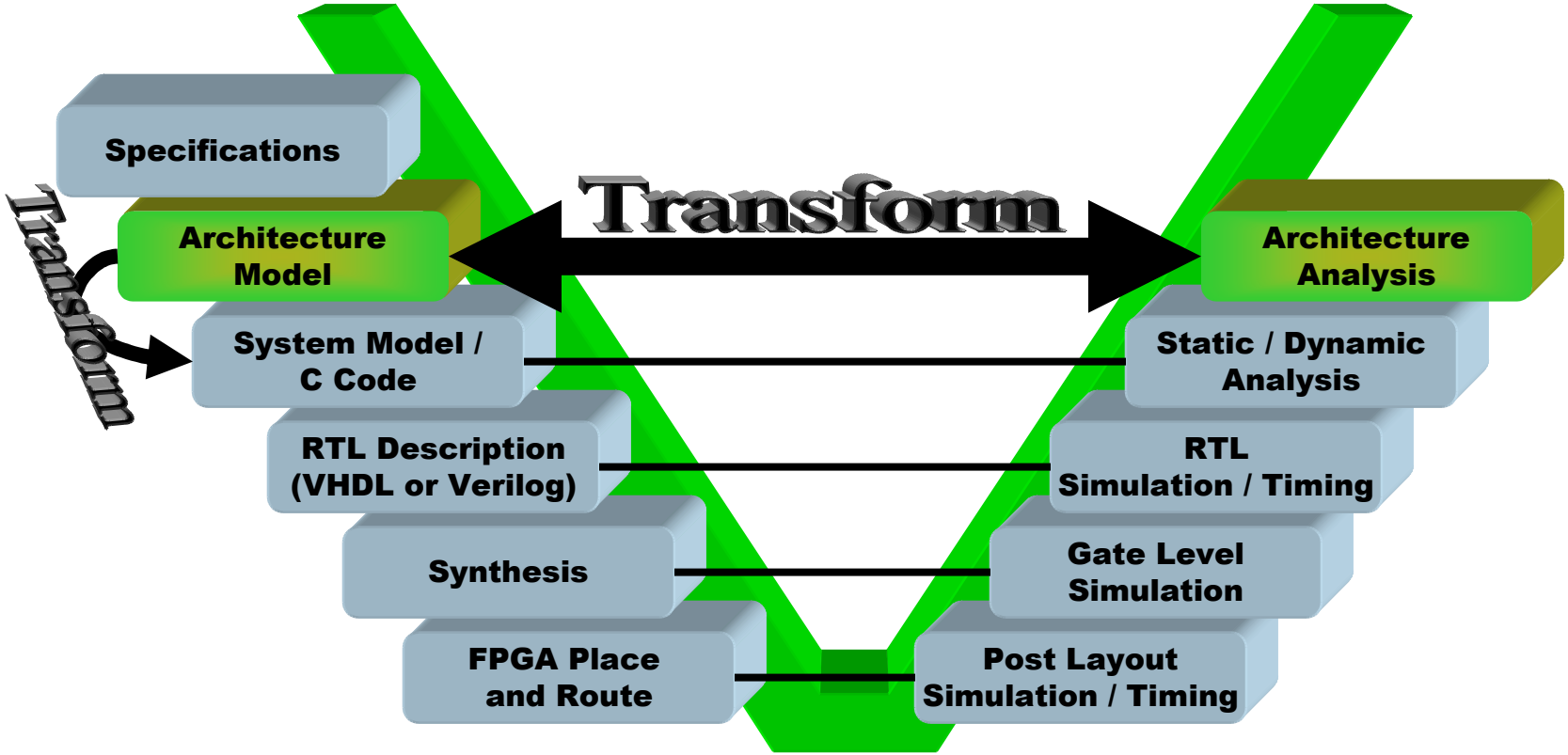
Shift toward application domain expertise

Rockwell Collins

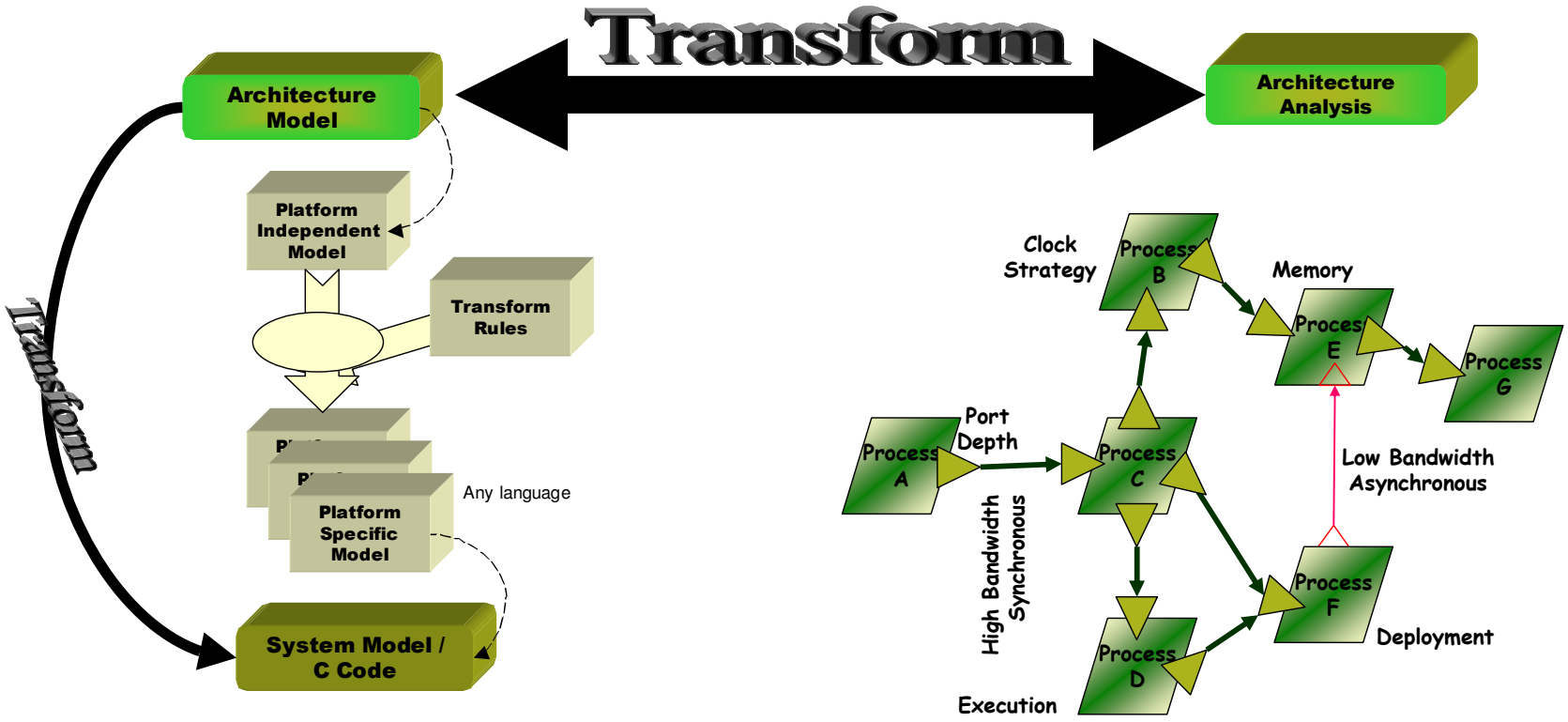
Reduce Intellectual Gap



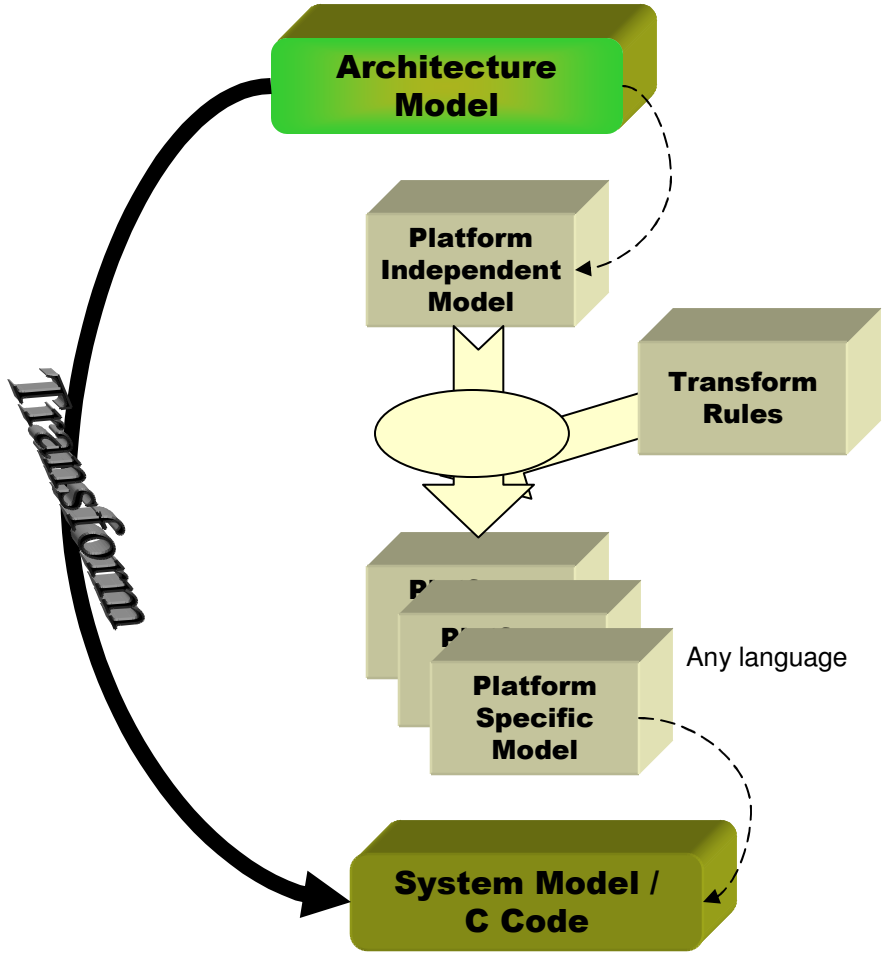
Enhanced Process



Transformations



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

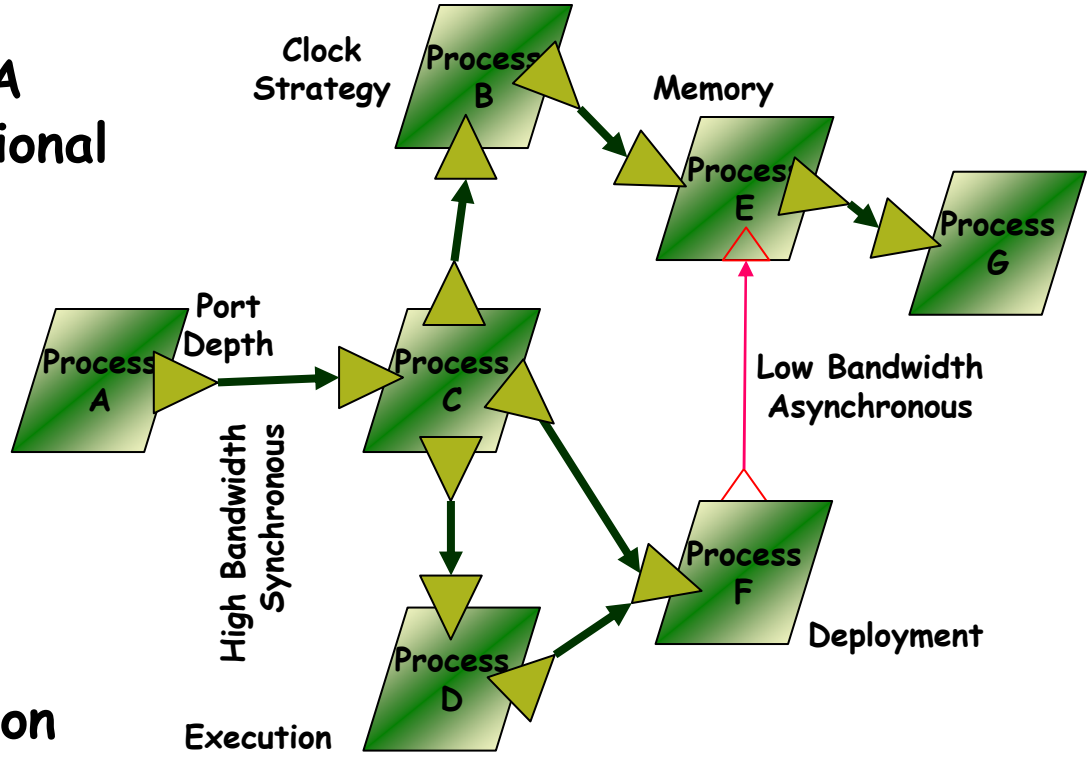
Architecture Model

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

Processes, Ports, and Connections

Memory utilization

Deployment and execution constraints

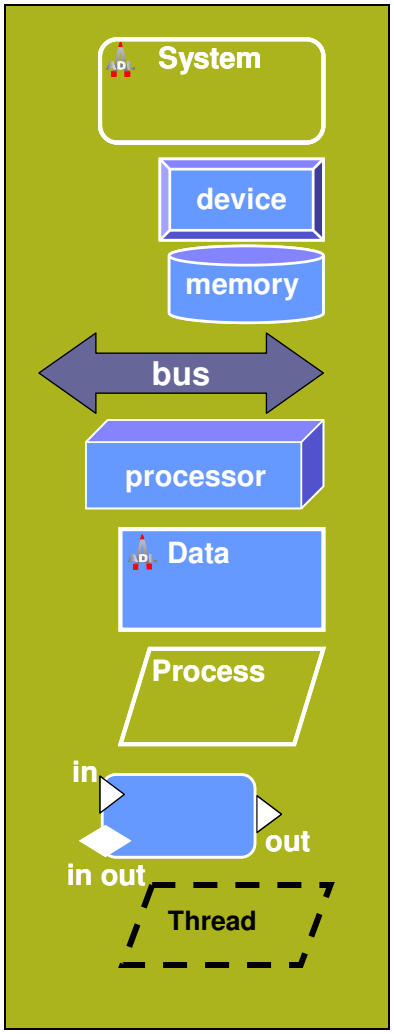


Architecture Analysis

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)**



Rockwell Collins

AADL / FPGA Concepts

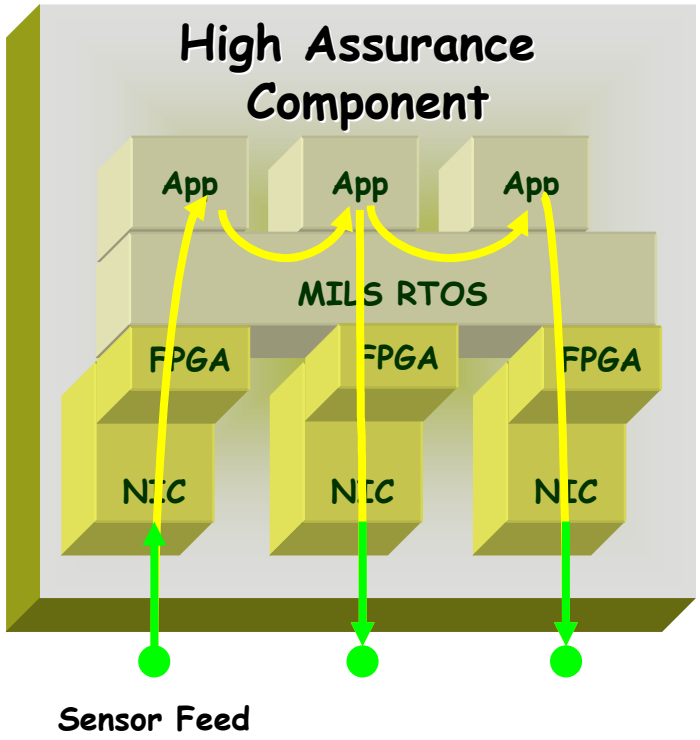
Impulse C concept	AADL concept	Adaptation
Process	Process (or thread)	Fixed execution rate. Possibly depends on a global clock. If using thread, one per process.
Streams	Data Port	Ports have depth and width.
Signal	Event Port	Occasional communication. Typically for synchronization.
Memory	Memory	Many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

Example – MILS I/O

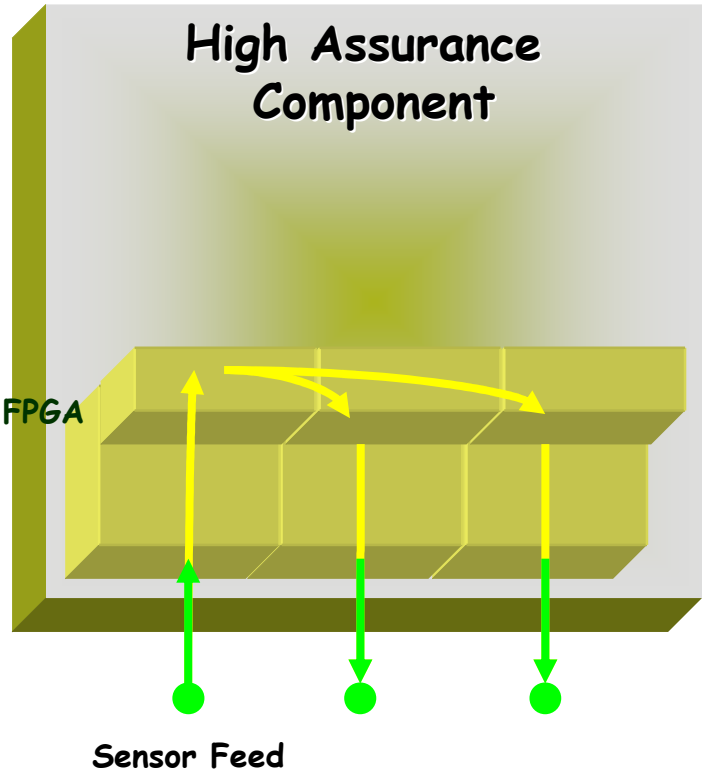
- Multiple independent levels of security (MILS)
  - Provides multi level enforcement by strict separation (the I in MILS)
  - A given separation (or partition) may hold a single level of classification, or multiple single level (MSL)
- AADL experience with modeling MILS OS
- MILS applied to FPGA
  - Separation of logic and pins

Example – MILS I/O

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

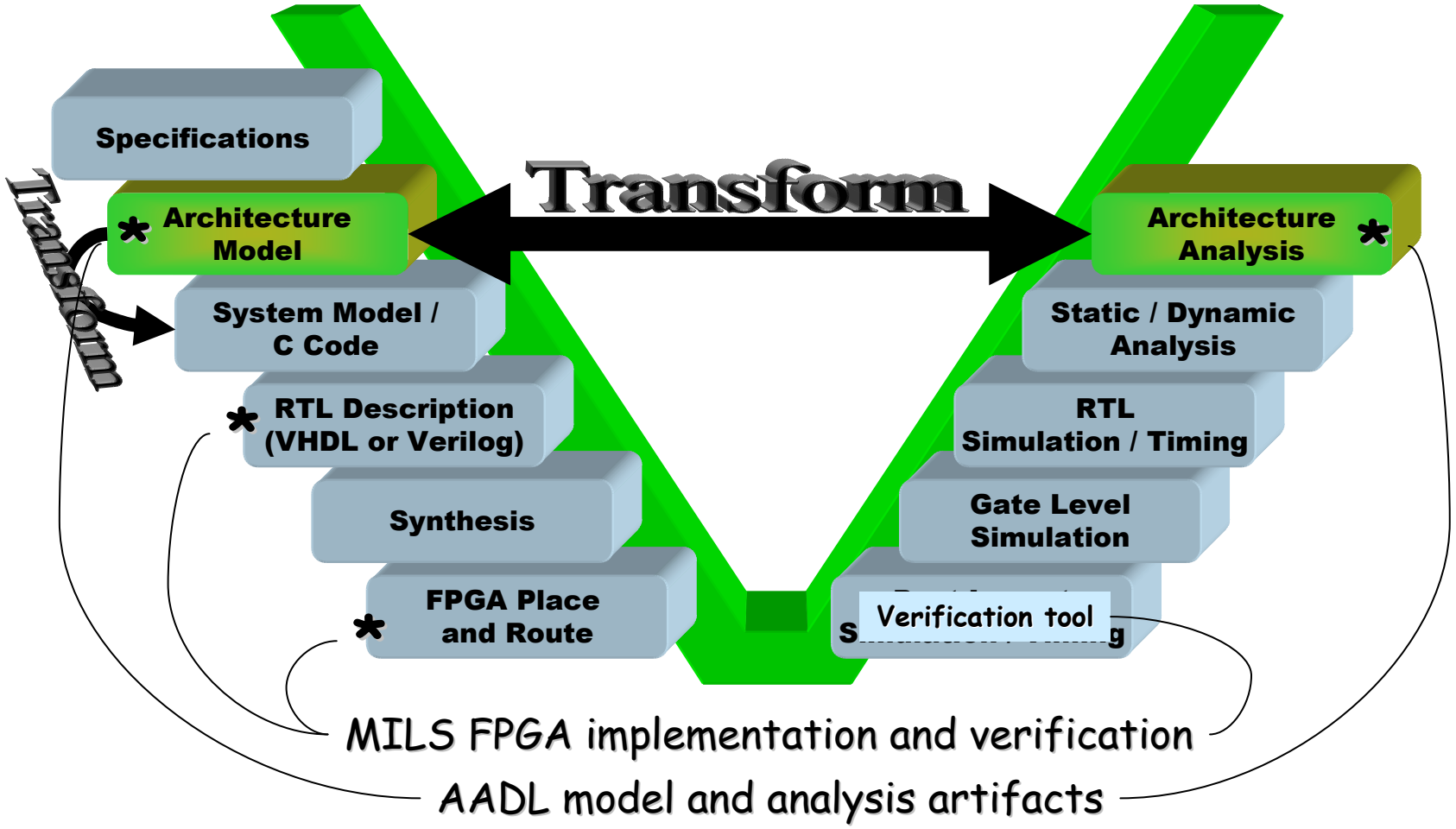


Trusted FPGA
makes high assurance I/O decision



Rockwell Collins
Building trust every day

Example – MILS I/O



Rockwell Collins

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)