A Virtual FPGA for Secure Design Guarantees

Reusable Security Components for High Assurance Designs

This project investigates the use of FPGA overlay technology to provide secure-by-design guarantees to designs implemented in the overlay. An end-to-end toolchain allows designers to generate a custom FPGA overlay as a design target and synthesize their designs to it. The components of the generated architecture are intended to be pre-verified modules that can be mixed into an architecture as needed by a designer. Key benefits of this approach include:

1) a chain of trust that can extend down to the logic used to construct a hardware design running on an FPGA
2) a platform-independent approach wherein one architecture can be mapped to vendor parts using low-level place-and-route constraints

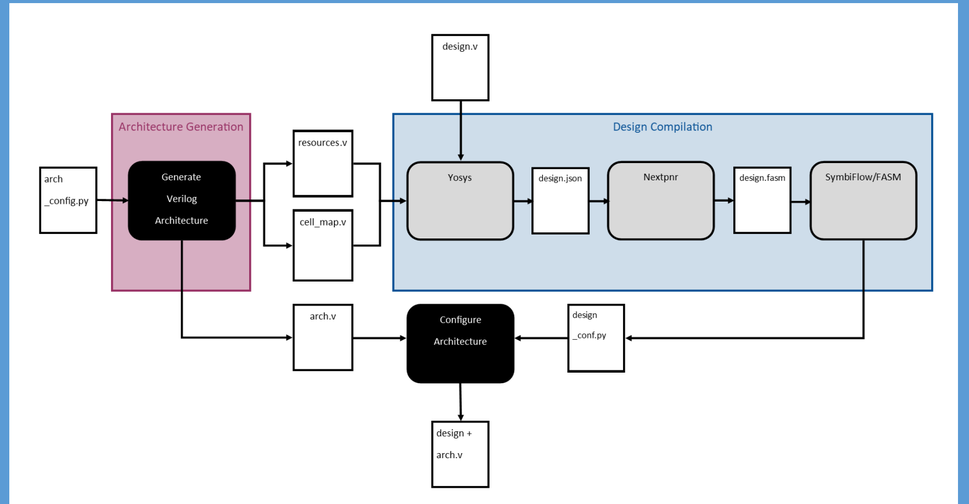

Figure 1. Flowchart showing components of the virtual FPGA toolchain.

High Assurance Design Requirements

Critical systems are those whose compromise would result in loss of life, loss of national security, or loss of valuable resources. To field such systems, security and trust considerations must be accounted for during the system's design. In recent years, FPGAs have become an important implementation platform for such critical systems due to their flexibility. However, ensuring proper system operation from functional conformance down to side channel emissions is no small feat. This work explores current techniques for high-assurance design and proposes a new method for achieving high assurance without depending entirely on vendor-specific tools.

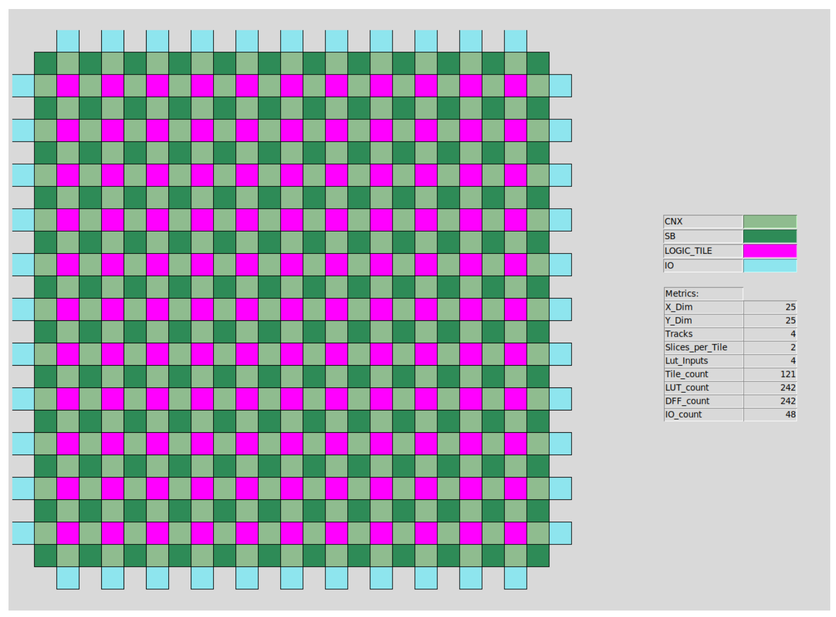

Figure 2. A generated FPGA architecture using logic tiles, I/O, and connection blocks. Future work will allow some of the logic tiles to contain dedicated security primitives.

Current High Assurance Design Process

The state-of-the-art process for assuring critical designs relies on inspecting a fully-implemented design using proprietary tools. For example, assured designs can be built on Xilinx' FPGA platforms. During the design phase, Xilinx-specific constraints are used to prevent sensitive logic from being placed too near to other logic. Then, during assurance, Xilinx' Isolation Verification Tool searches the entire design for violations where design elements are too close. This process, along with other proprietary Xilinx techniques, has been used to create FPGA designs that meet the NSA's Fail-Safe Design Assurance specification.

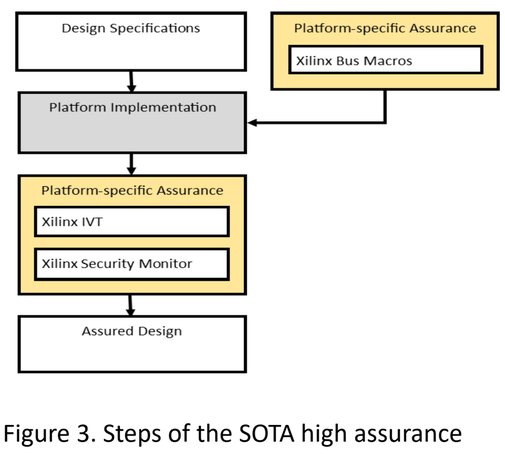

Figure 3. Steps of the SOTA high assurance design process.

Improved High Assurance Design Process

An alternative approach to design assurance makes use of pre-verified architectural components of an FPGA to construct an overlay architecture. The overlay inherits security properties from its components, allowing the overlay to securely run a user's design on any platform to which the architectural components can be properly mapped. Additionally, the user's design is implemented on the overlay using an open-source toolchain that provides greater introspection into the FPGA design compilation process. This project aims to improve upon the critical design assurance process by performing assurance before implementation.

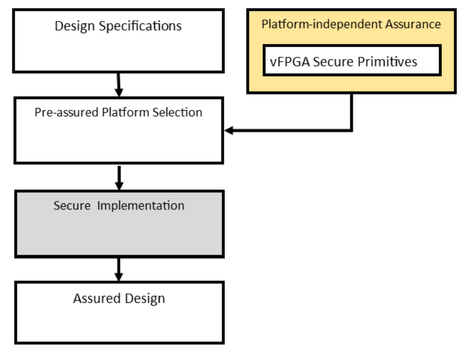

Figure 4. Steps of the proposed vendor-independent high assurance design process.

Project Goals and Milestones

- Create an FPGA architecture generator along with a supporting toolchain (in progress).
- Extend the architecture generator to include provably secure components such as a power-balanced look up table (future).
- Develop a constraint generator to seamlessly map the secure components' HDL to hardware from multiple vendors (future).

Funding Information

Thank you to the Georgia Tech Research Institute for providing the funding for this preliminary work.

References

[1] T. Huffman et al., "Managing Security in FPGA-Based Embedded Systems," in *IEEE Design & Test of Computers*, vol. 25, no. 6, pp. 590-598, Nov.-Dec. 2008.

[2] M. Mclean and J. Moore, "FPGA-Based single chip cryptographic solution," in *Military Embedded Systems*, pp. 34-37, 2007.

Jude Nifong | judea.nifong@gtri.gatech.edu

Abigail Cliche | abigail.cliche.stu@gtri.gatech.edu