Independent Functional Testing of Commercial FPGA Devices

Matthew French, Neil Steiner, Jeffery Draper, Michael Bajura, and Wes Hansford

GOMACTech 2015

4676 Admiralty Way
Marina del Rey, CA

3811 N Fairfax Drive
Arlington, VA

Outline

- SURE Center Overview
- FPGA Functional Testing Problem
- Overview of IFT Tool

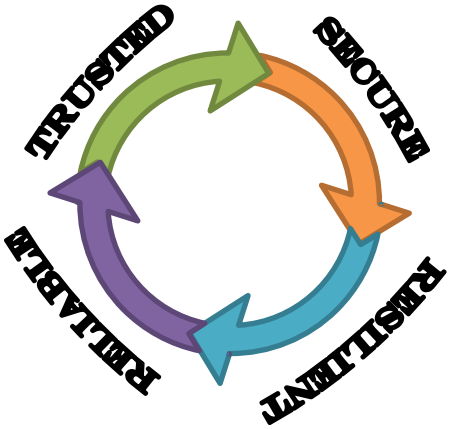
SecUre and Robust Electronics (SURE) Center Mission

- Raise societal and commercial awareness of the importance of Hardware Security and Robustness issues
- Contribute to advancing US leadership in Hardware Security and Robustness
- Advance the scale, pace, and impact of hardware robustness and security technology development

Establish a national center of excellence for Secure, Robust Electronics that advances national security and national capabilities

SURE Center Theme

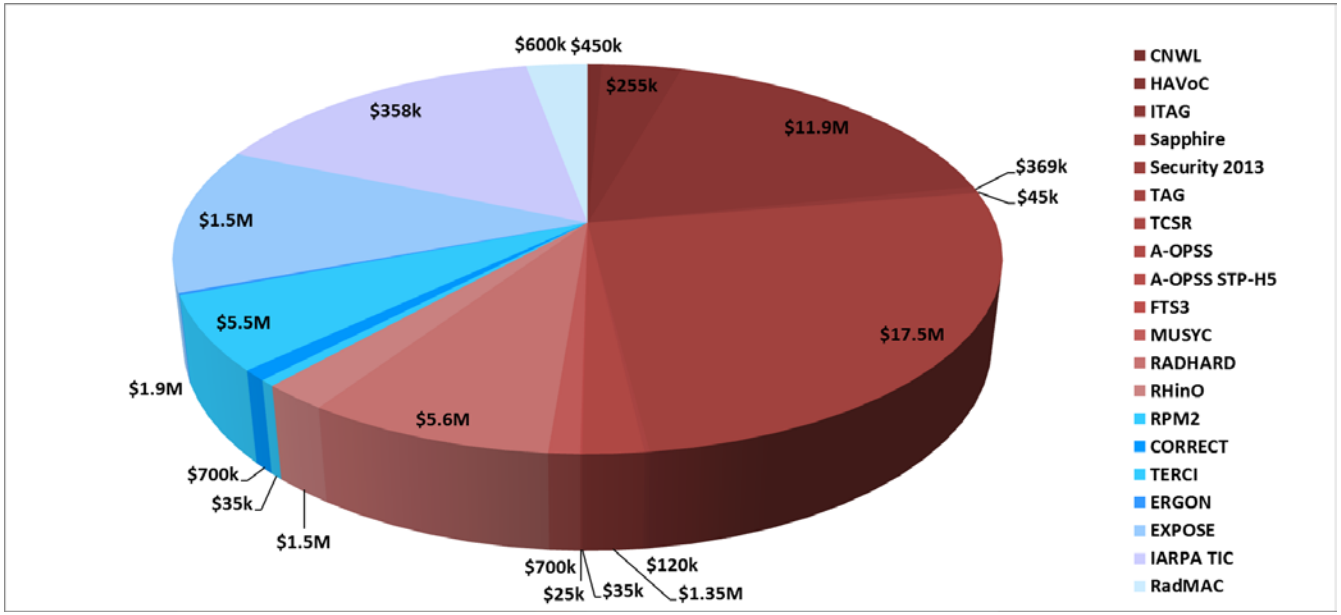
- **Effective hardware needs to be Trustable, Secure, Resilient, and Reliable**
  - "It just needs to work"
- **Trust: Does it work as expected?**
- **Security: Can it be hacked? Counterfeited?**
- **Resilience: Is it error tolerant?**
- **Reliability: Does it wear out prematurely?**



Effective Hardware: Trustable, Secure, Resilient, and Reliable

- **Problem: Inherent complexities within state of the art electronics have significantly compromised <u>all four areas</u>**

$70M, One Decade of Investment

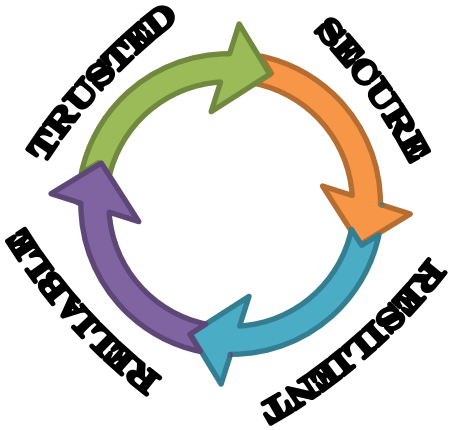


$70M to date since 2004, robust across CS&T and DE divisions

- DARPA Expose – First program to investigate developing 3D chip inspection techniques using high resolution xray tomography
- DARPA TAG – Trust in Integrated circuit program Black Hat team which developed Benchmark hardware trojans and analysis of white hat capabilities
- AFRL SPAoA – Consulted with AFRL on the development of a level 5 Secure Processor
- DARPA TERCI - Investigating novel methods for efficient detection of reliability tampering with ICs
- DARPA ITAG - Black hat team for DARPA IRIS program which developed integrity and reliability hardware trojans; Also researching FPGA functional discovery techniques
- IARPA TIC – Investigating use of foreign SOA Fabs to develop "secure" Ics via the paradigm of "split-manufacturing"
- IARPA SAFIRE – Investigating novel anti-tamper methods for FPGA devices
- AFRL CNWL – Investigating control of EM emissions from commercial devices
- DARPA HAVoC – Adversarial Challenge team for FPGA firmware security vetting
- NASA RHINO, FTS-3, and A-OPSS – Investigating Radiation Hardening by Software techniques for FPGAs, including hard IP
- DTRA RadMAC - Application of residue coding theory for low overhead error detection & correction

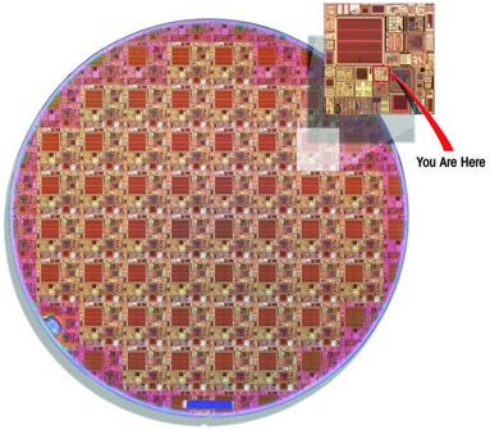
SURE and MOSIS

SURE Center



Technology Transition

The MOSIS Service



Trusted Development Flow

Design → Broker → Aggregation

- Performs research and development in hardware Trust, Security, Reliability, and Resiliency
- Operates as a designated center within ISI

- Provides low cost access to modern foundry nodes through shared mask, wafer, and foundry and packager interface
- Operates as a non-profit service center within ISI

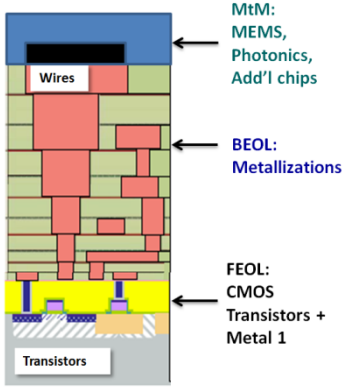
Tech Transition Pipeline

Split Fabrication

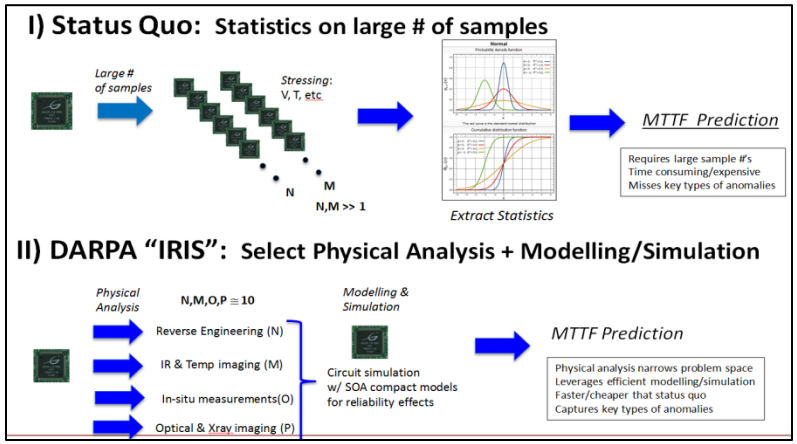
IARPA Trusted Integrated Chips (TIC) Program

Approach:
- The IARPA TIC program was established to access the best world-class semiconductor manufacturing capabilities through a concept know as split-manufacturing whereby CMOS transistors are produced at an off-shore (FEOL) foundry followed by the deposition of backend metallization layers (BEOL) in a US manufacturing facility.

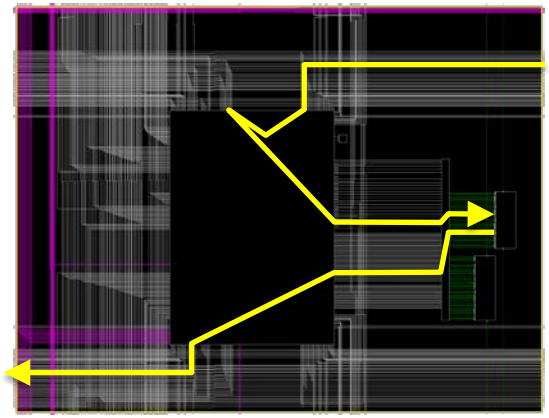
Challenges:
- Engaging foundries as a low volume potential customer
- Merging PDKs from different foundries
- Heterogeneous integration ("More-than-Moore")



Reliability Assessment



Independent 3rd Party Functional Test of FPGAs

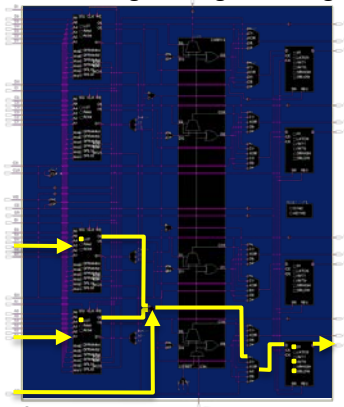


Interconnect Testing

Custom massively replicatable paths to exercise PIPs: one signal exiting to left and another signal arriving from right, passing through PIPs

Logic Testing

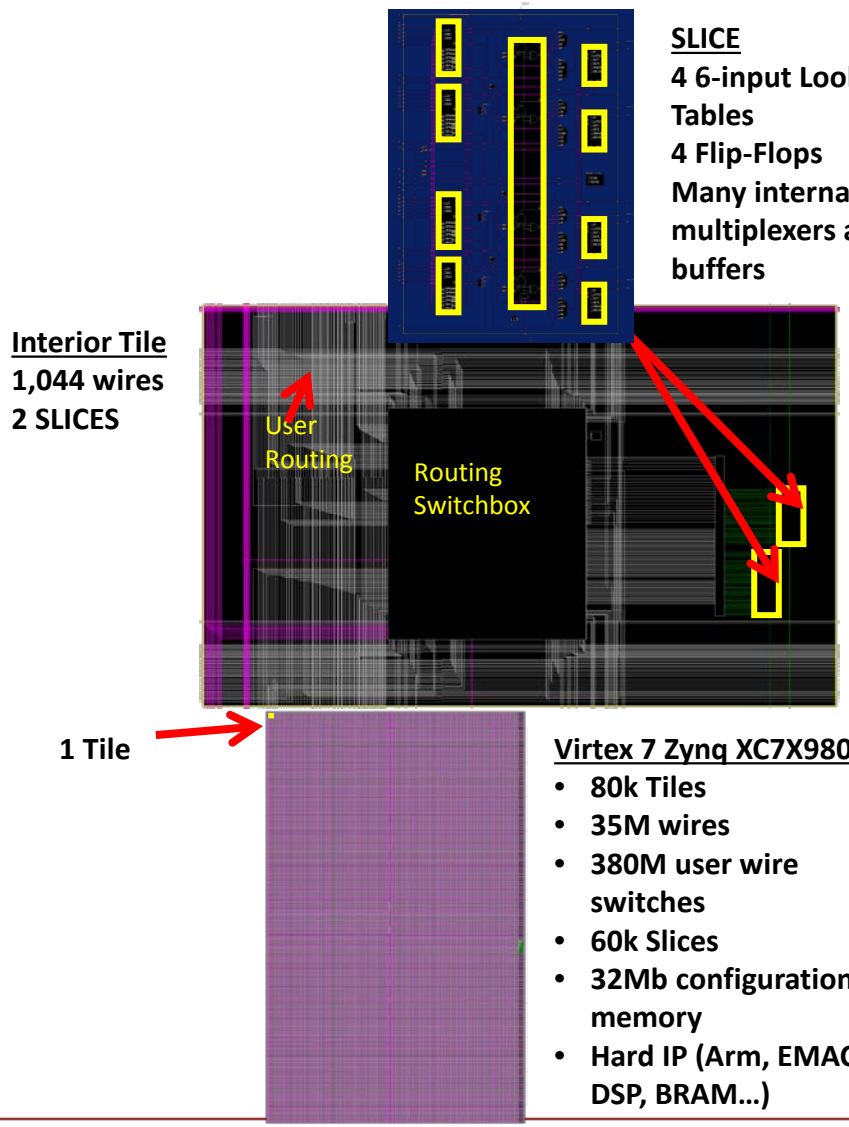
Paths through configurable logic



Flip-flop on right enables launch and capture of test signals through logic

FPGA Independent Test Overview

- **Why Independent test?**
  - FPGA vendors perform extensive functional testing during production
- **But what about**
  - Trusted supply chain verification
  - Devices acquired from deep storage
  - Determining health of fielded systems
- **Problem:**
  - FPGA architectures are large (~1 billion transistors), complex, and largely opaque to end users
  - **ATPG is intractable** – device size causes **state space explosion**



Independent FPGA Functional Testing (IFT) Tool

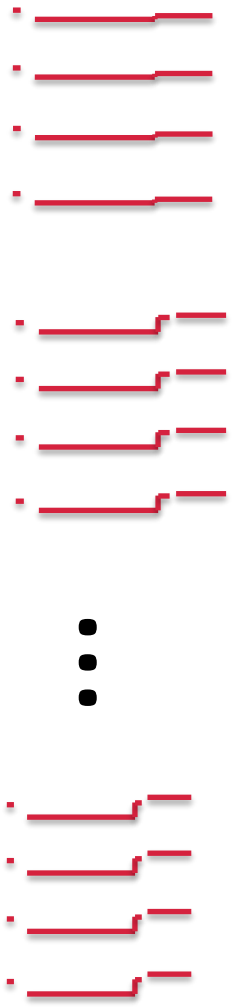
- **IFT Methodology:**
  - Combine ISI's **exhaustive knowledge** of FPGA device architecture with **internally developed APIs and tools which** exposes all configurable resources to **exhaustively quantify and test** all FPGA features
  - Leverages tools developed under DARPA Trust and IRIS programs
  - Provide coverage metrics
- **IFT queries and programs all elements on a device for testing**
  - FPGA may be mounted on PCB
  - Operates independently of
    - **FPGA I/O pin utilization**
    - **Clocks or resets**
  - Uses JTAG or SelectMAP for interface

IFT Approach

- **Simple stuck-at fault model utilized**
  - Easily extensible for other fault models
- **Testing approach by resource:**
  - **Configuration memory:** write and read entire configuration memory
  - **Logic:** slices fully covered by **19 configurations**
    - **Additional logic types can be added**
  - **Interconnect:** simultaneous launch and capture between pairs of logic sites for all tiles in clock region height
    - **200M mux / (50 mux/test) / (test/2.5µsec) ≈ 10 sec/device**
- **Real time execution**
  - IFT leverages algorithms which exploit regularity, parallelism, and partial reconfiguration to realize a tractable, scalable testing solution

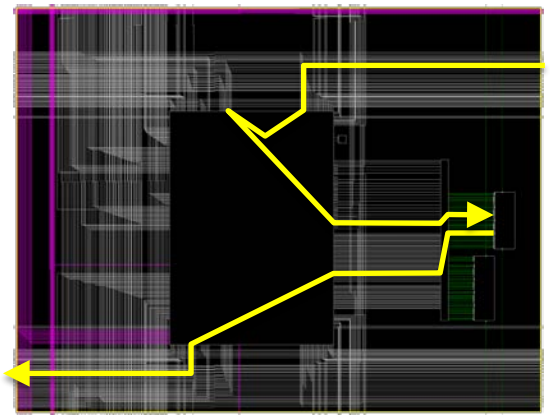
Logic: Slices

- **Coverage**
  - Every path and every element in SLICEL and SLICEM in entire device
    - **LUTs, flip-flops, carry chains, configurable muxes, single- and dual-ported RAM and ROM**
- **Groups**
  - LUTs
  - Combinational paths through AMUX/BMUX/CMUX/DMUX
  - Combinational paths through AF/BF/CF/DF muxes
  - SelectRAM (LUTs configured as RAM or ROM)
  - Shift registers
  - Vertical carry chains
- **Testing**
  1. Create paths that exercise every path in a SLICE
  2. Recursively connect four SLICE outputs to four inputs of next SLICE
  3. Chain through entire region under test (typically ½ – ¼ of device)
  4. Controller launches signal at beginning of chain and captures result at end of chain



Routing

- **Extends Slice launch and capture approach to routing wires**
- **Interconnect testing utilizes custom, massively replicatable paths to exercise user wires and routing multiplexers**
- **Up to 3,800 routing multiplexers verified in parallel**



Interconnect Testing
Custom massively replicatable paths to exercise PIPs: one signal exiting to left and another signal arriving from right, passing through PIPs

IFT Summary

- First known tools for **Independent FPGA Functional Testing** and **coverage metrics**
- Currently supports the **Xilinx 7-Series** architectures (Virtex7, Kintex7, Artix7, Zynq700).
  - Internal databases support all Virtex 1-7 devices. IFT can support other generations with one time port.
- **Coverage** on largest current Xilinx Virtex7 Zynq device (XC7X980T)
  - **100%** Configuration memory cells covered
  - **95+%** of wires (34,515,491) and routing multiplexers (378,563,268)
  - **100%** of logic Slices covered
  - Wire and slice coverage corresponds to **90%** of bitstream (3.7MB)
  - Test time << **2 hrs**
  - Coverage limitations not reached.
- **Future extensions**
  - Additional logic types (BRAMs, DSPs, DCMs, EMACs …)
  - Additional fault model types (bridging etc)

Independent testing for when we don't trust the supply chain, parts are of unknown origin/condition, or fielded parts become faulty

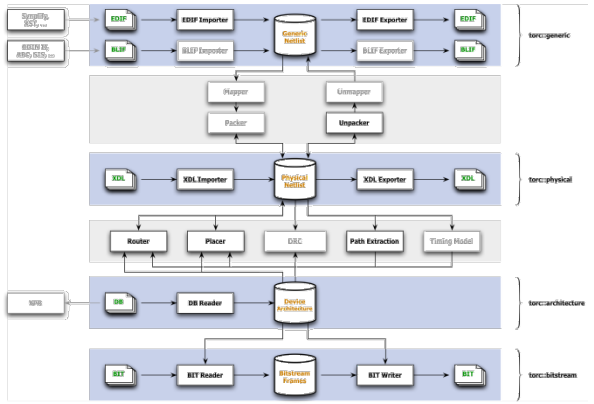
Tools for Open Reconfigurable Computing

- **What is it?**
  - **Open-source C++ framework** for reconfigurable computing
  - Strategic capability for ISI, **resource** for research community
  - **Complements ISE** – replaces/augments/constrains as needed
- **What does it offer?**
  - Complete **EDIF**, **XDL**, **XDLRC** (device architecture) support
  - Extensive **bitstream** support
  - Includes **routing**, **placing**, et cetera, in **REAL** devices
- **Is it legal?**
  - Built upon **non-proprietary**, publicly available information
  - Supports bitstream frames but **not** frame contents
- **Who cares?**
  - Researchers with **special requirements** unsupported by ISE
  - Researchers developing **CAD algorithms** for **REAL** devices

TORC

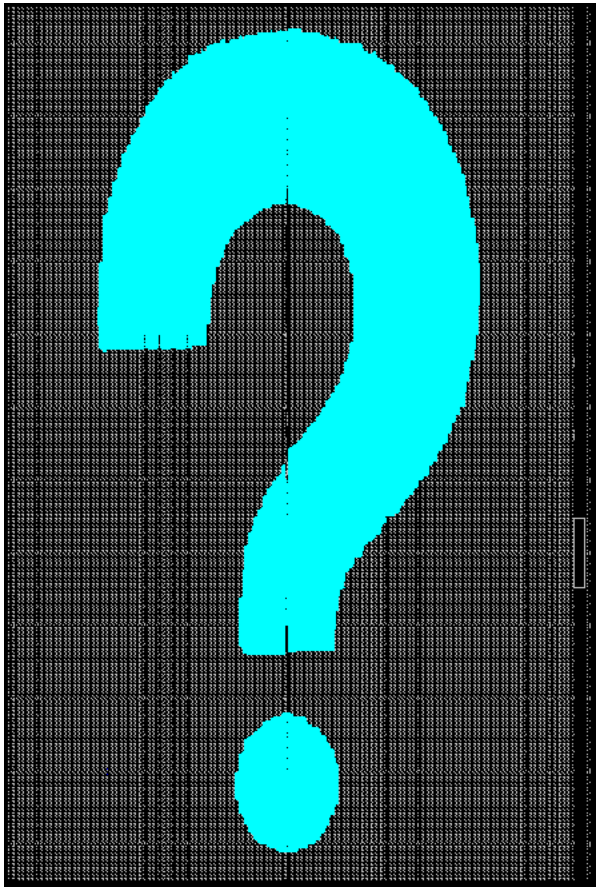
TOOLS FOR OPEN RECONFIGURABLE COMPUTING

http://torc.isi.edu



TORC Architecture

Questions



Thank You!