Sensing Nanosecond-scale Voltage Attacks and Natural Transients in FPGAs

Kenneth M. Zick, Meeta Srivastav, Wei Zhang, Matthew French

kzick@isi.edu, meeta@vt.edu, wz6pc@virginia.edu, mfrench@isi.edu

USC Information Sciences Institute, Arlington, VA

International Symposium on Field-Programmable Gate Arrays, Feb. 2013

USC

USC Viterbi
School of Engineering

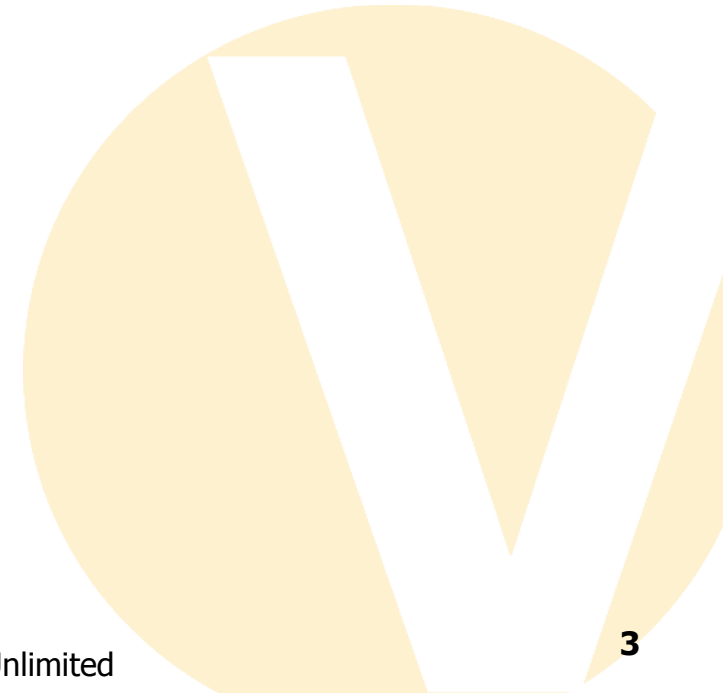
Motivation

- **The power supply voltages on a chip can fluctuate on fine timescales (nanoseconds). *Voltage transients.* Very hard to observe**
- **Malicious transients can be a security risk. Secret information can be obtained with *voltage glitch attacks***
- **Natural transients cause inefficiencies. Typically, supply voltages are kept high to compensate for droops. Burns extra power.**
- **Related work has not fully addressed problem. Built-in A/D converters are not quick enough for ns-scale effects. Ring oscillators also not quick enough.**
- **Need new methods of quickly detecting and reacting to voltage transients in FPGAs**

Proposed solution

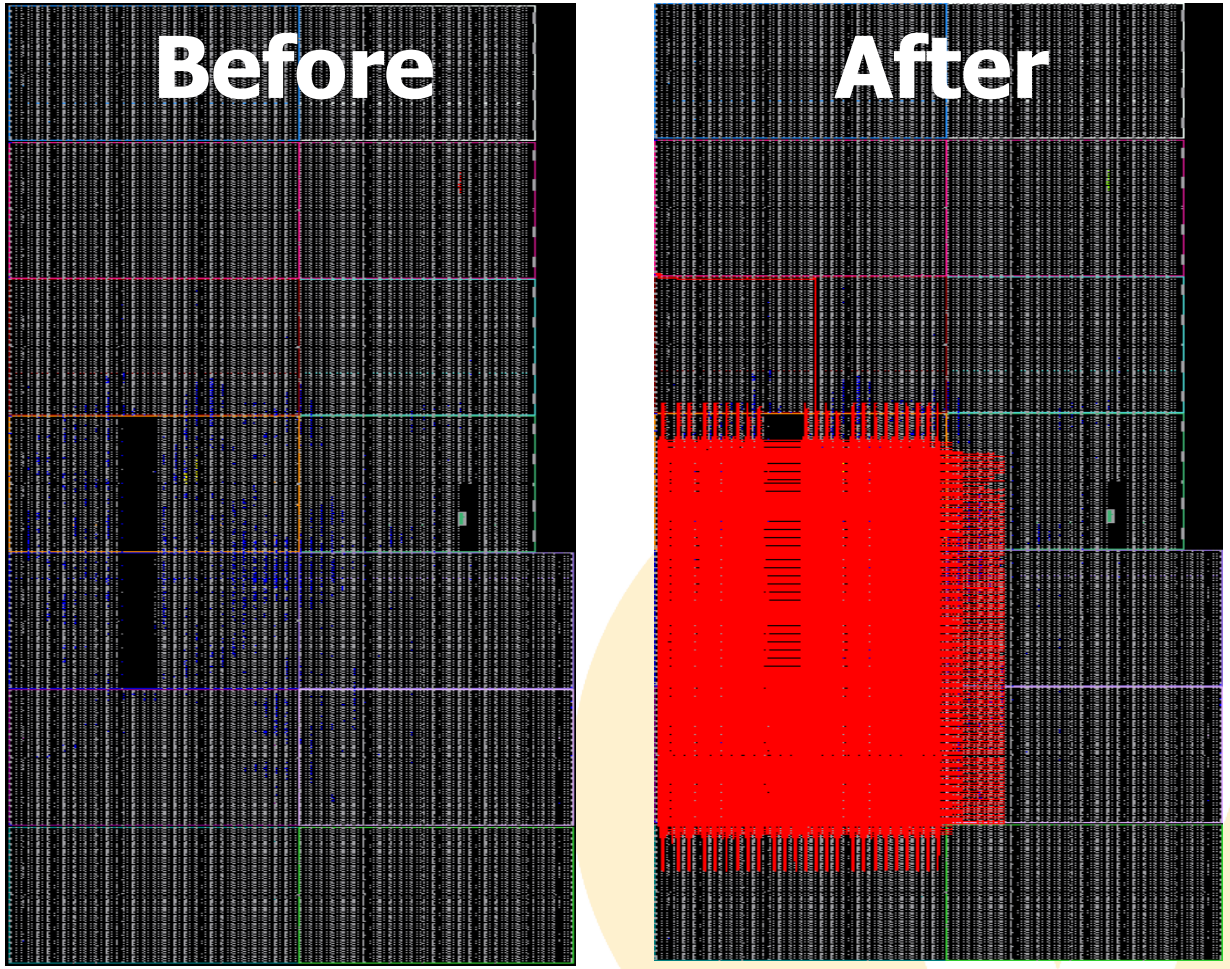
- **Deploy delay sensors with very high sample rates (500M samples/s) using digital logic in FPGA fabric. Pair a delay line with a time-to-digital converter.**

- **By measuring ns-scale changes in delays, ns-scale changes in voltage can be inferred**



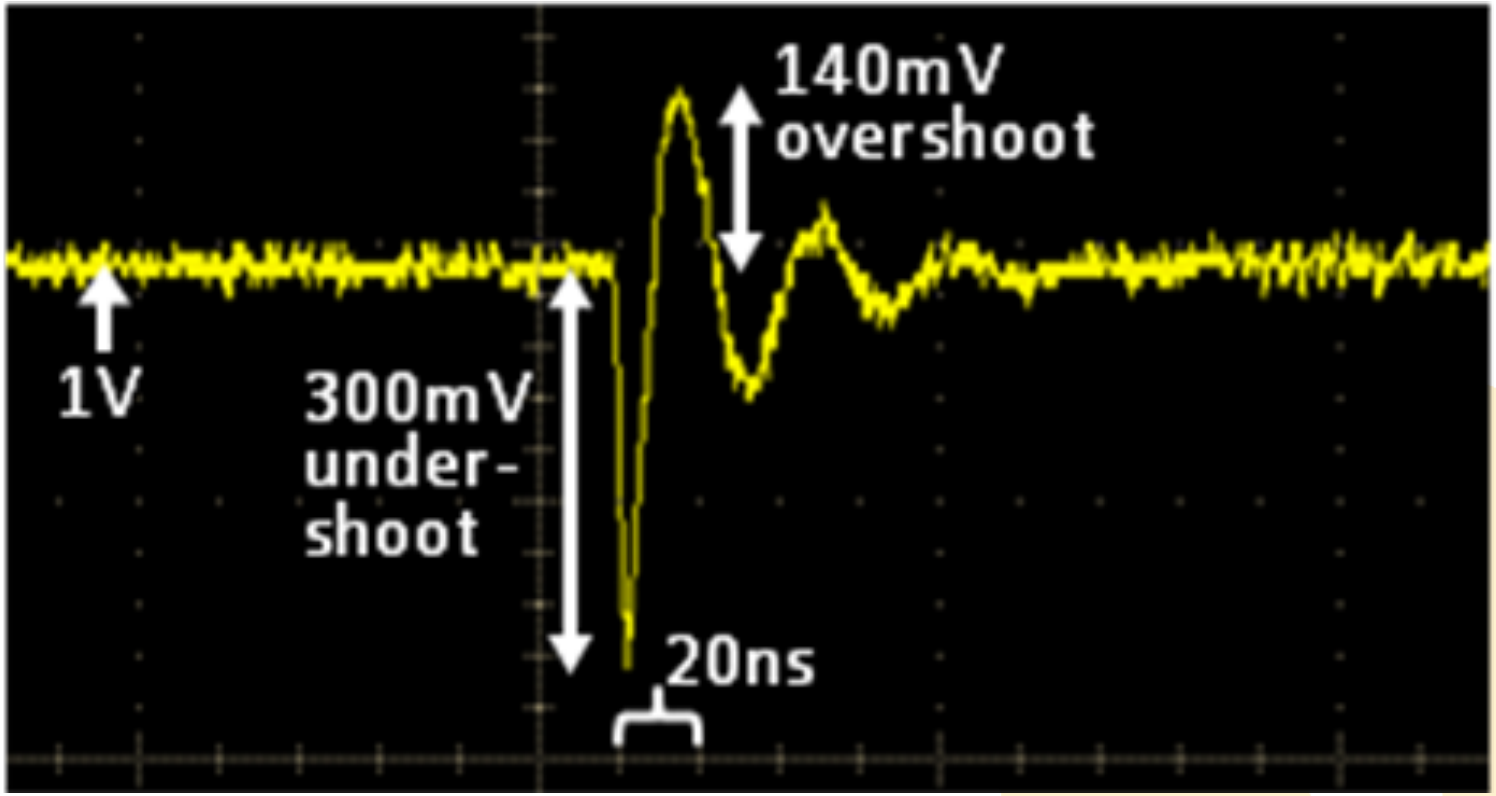
Methodology for generating ns-scale voltage transients

- To test the sensing approach, generate transients with novel technique: simultaneous switching of interconnect
- Connect all unused interconnect resources within a region to the same signal. Switching causes transient. Sizing of region allows for sizing of events.
- Enabled by the Torc tools [Steiner, FPGA'11]

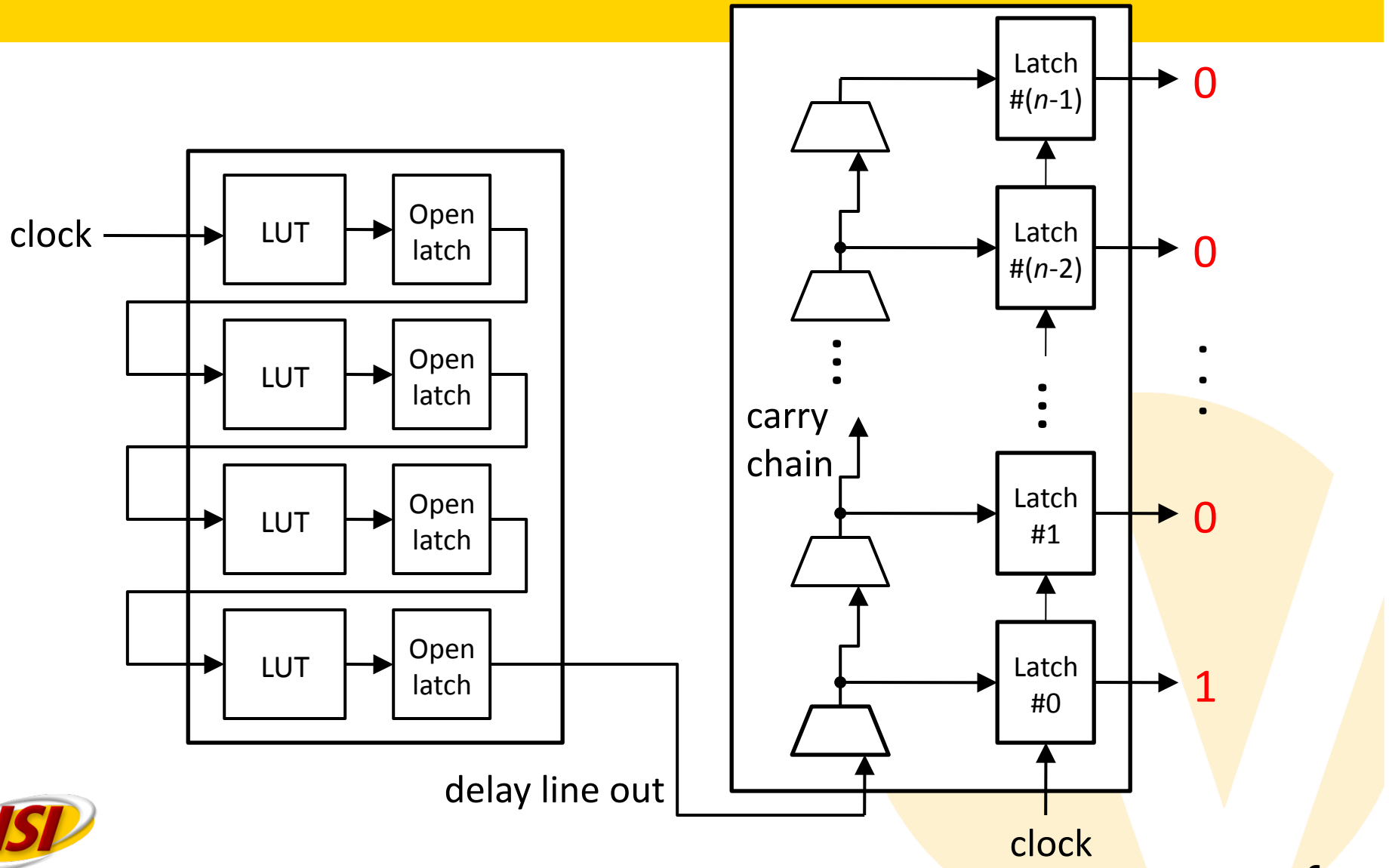


FPGA Editor views for a design mapped to Xilinx Kintex-7

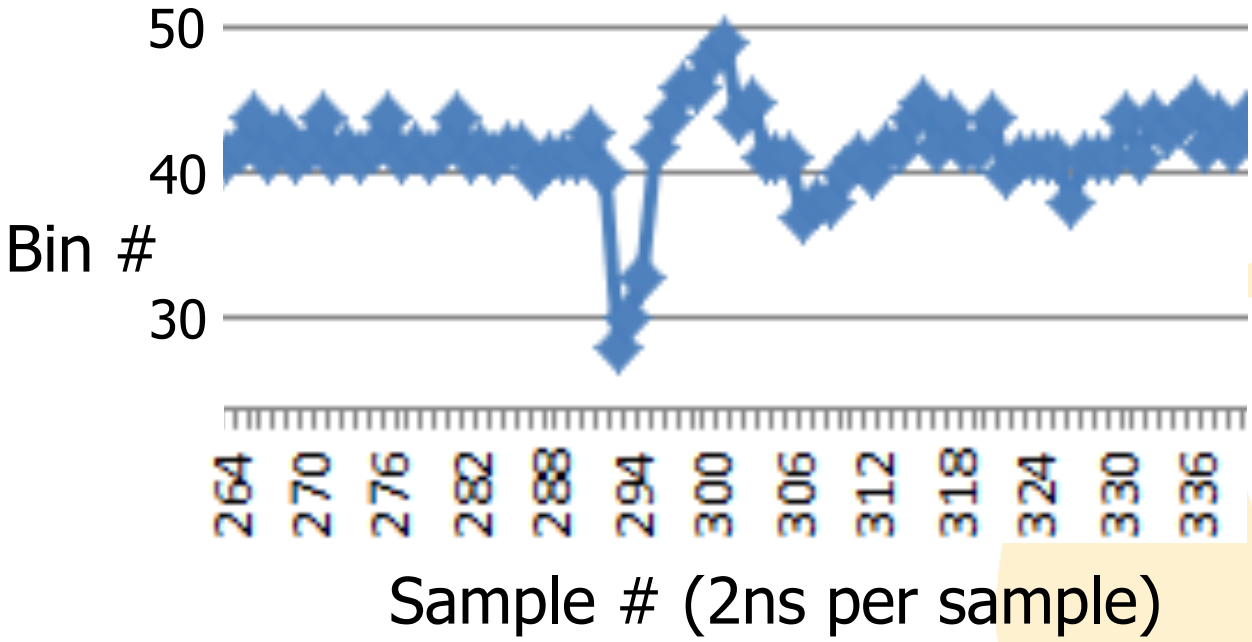
Voltage transients caused by extreme activity in fabric



Sensor basics



Results: example sensor data sequence



Conclusions

- Voltage transients can be very quick: initial droop in ~2ns. Not detectable by existing methods in FPGAs.
- In extreme cases, undershoot can be huge: >30% of VCC
- Overshoot also a problem: >14% of VCC
- Detection and characterization of transients is needed for optimization, hardware protection, privacy
- Presented approach can:
  1. Achieve sample rate of 500M samples/s
  2. Provide insight into voltage dynamics
  3. Help detect & react to anomalies within nanoseconds

Acknowledgments

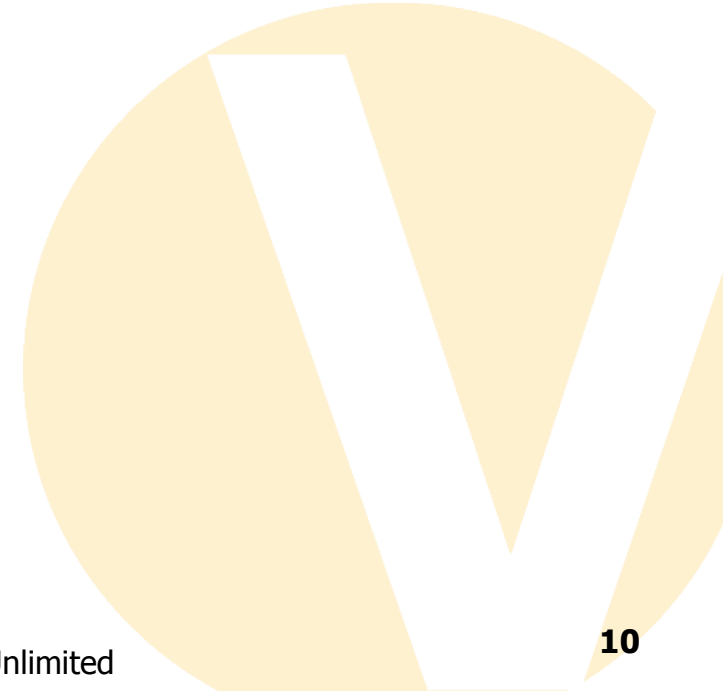
- Aaron Wood and Neil Steiner for providing tools and feedback

- This material is based upon work supported by the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR001-11-C-0041. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Defense Advanced Research Projects Agency (DARPA). Distribution Statement "A" (Approved for Public Release, Distribution Unlimited).

USC

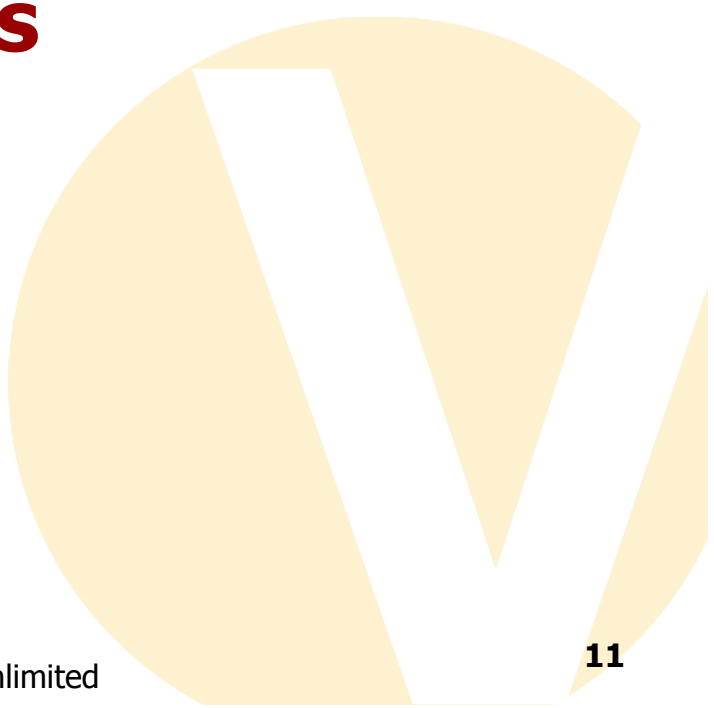
USC Viterbi
School of Engineering

Thank You

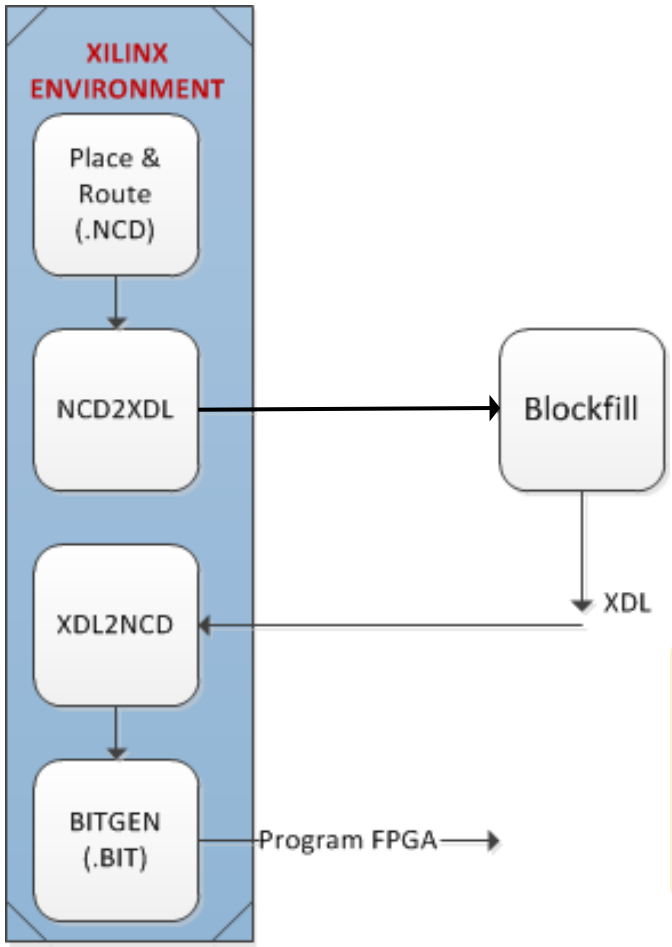


ISI
Information Sciences Institute

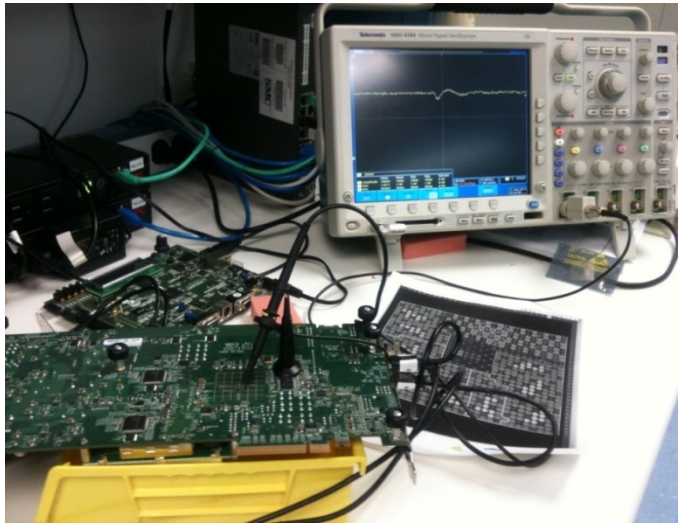
Backup slides

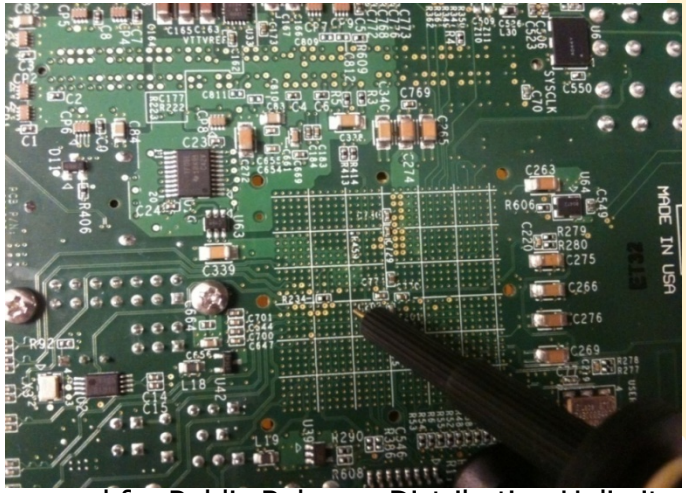


Methodology for generating ns-scale voltage transients

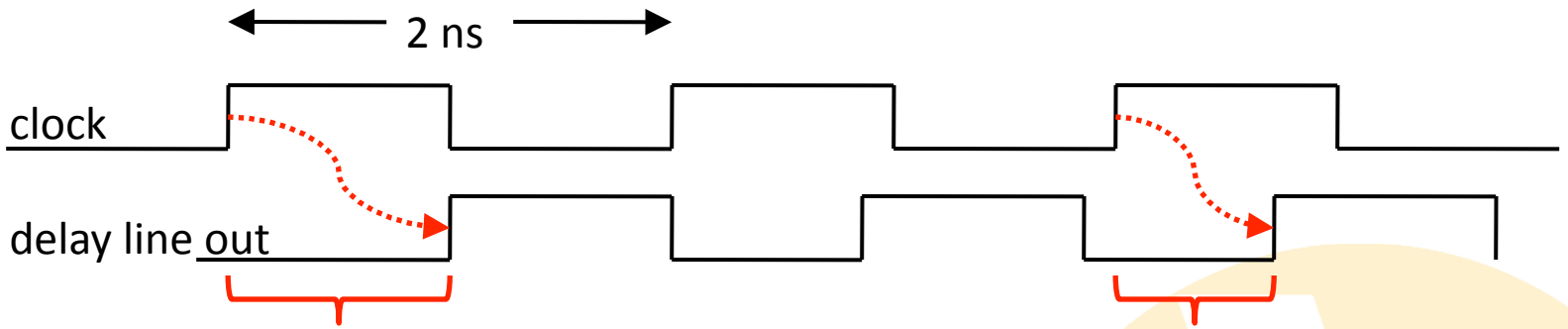


Lab setup



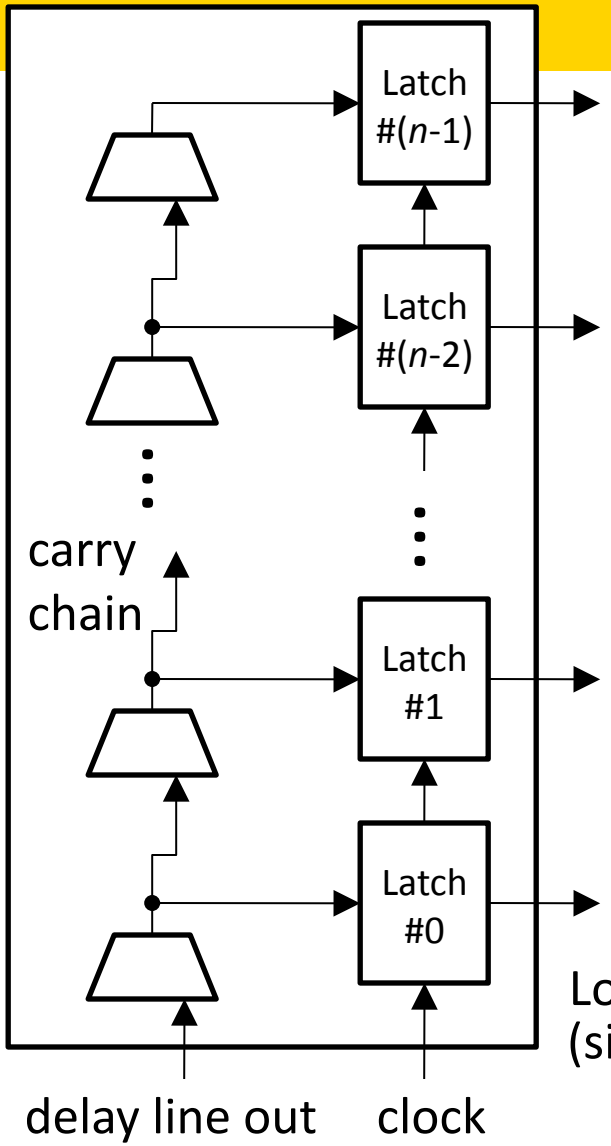


Timing diagram



Measured bin #	34	41	48

Time-to-digital converter



0	0	0
0		1
	0	
0	1	1
1	1	1
Lowest bin (signal was late)	Inter-mediate bin	Highest bin (signal was early)

Overhead of sensor

Resource (Xilinx 7 Series)	Utilization
Slices for delay line	1
Slices for TDC	16
Control register bits	32
Clocks	500MHz, 100MHz

Results: range of sensor values vs. size of event

Size of simultaneous switching events	Range of sensor values
0 (only nominal system activity)	11 bins
1% of K7 (100,000 PIPs)	15 bins
3% of K7 (300,000 PIPs)	22 bins