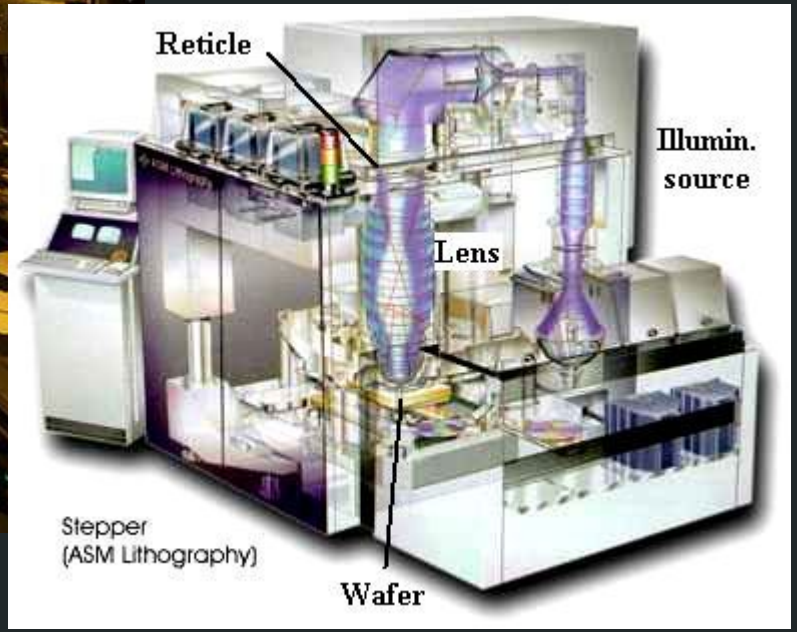
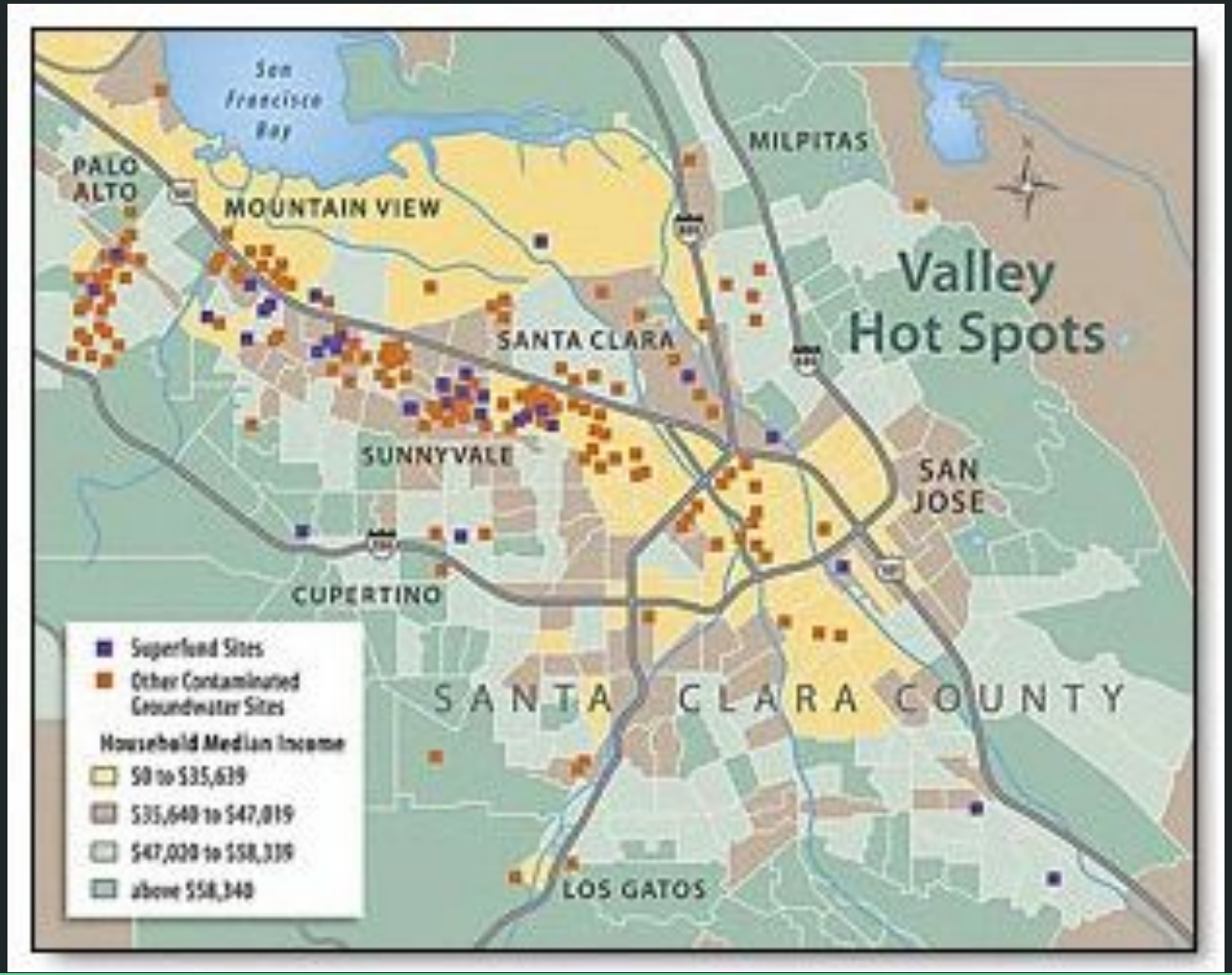
A2: Analog Malicious Hardware

Paper by:
Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, Dennis Sylvester
Department of Electrical Engineering and Computer Science
University of Michigan Ann Arbor, MI, USA


Reticle
Illumin. source
Lens
Stepper
(ASM Lithography)
Wafer

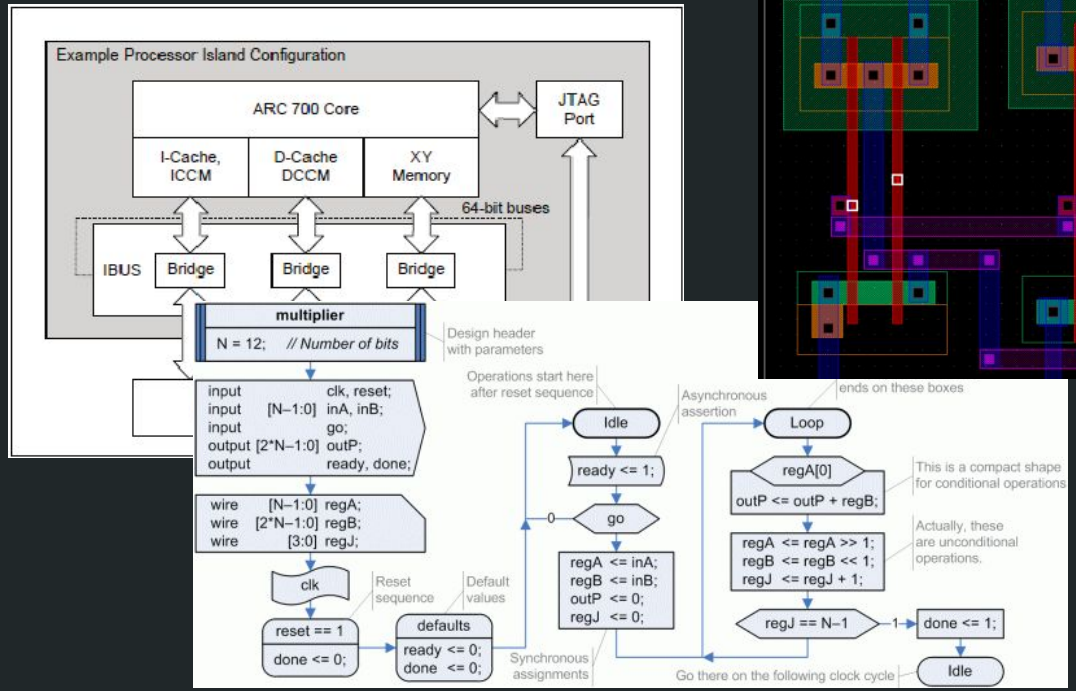

San Francisco Bay
PALO ALTO
MOUNTAIN VIEW
MILPITAS
Valley Hot Spots
SANTA CLARA
SUNNYVALE
SAN JOSE
CUPERTINO
SANTA CLARA COUNTY
LOS GATOS
Superfund Sites
Other Contaminated Groundwater Sites
Household Median Income
$0 to $35,639
$35,640 to $47,019
$47,020 to $58,339
above $58,340

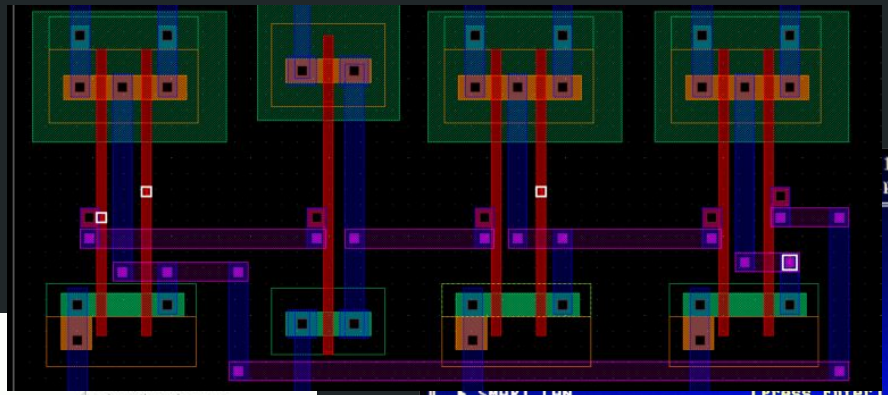
TSMC - biggest non-affiliated fabricator, Taiwan

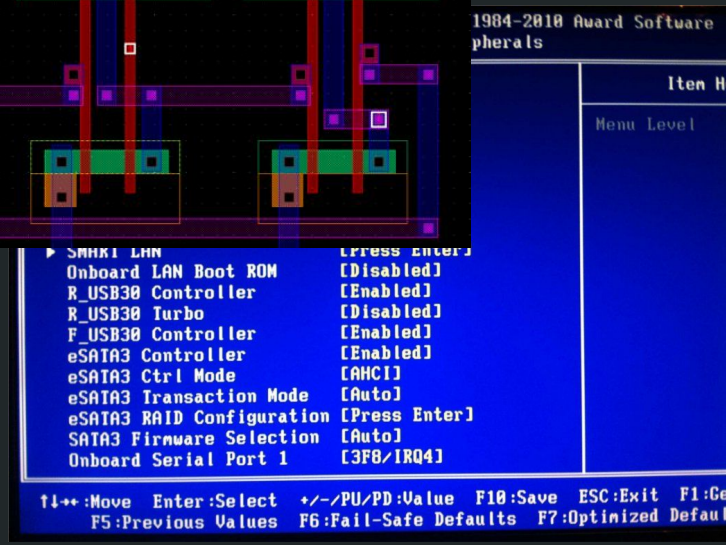
GlobalFoundries - spun off of AMD, Singapore

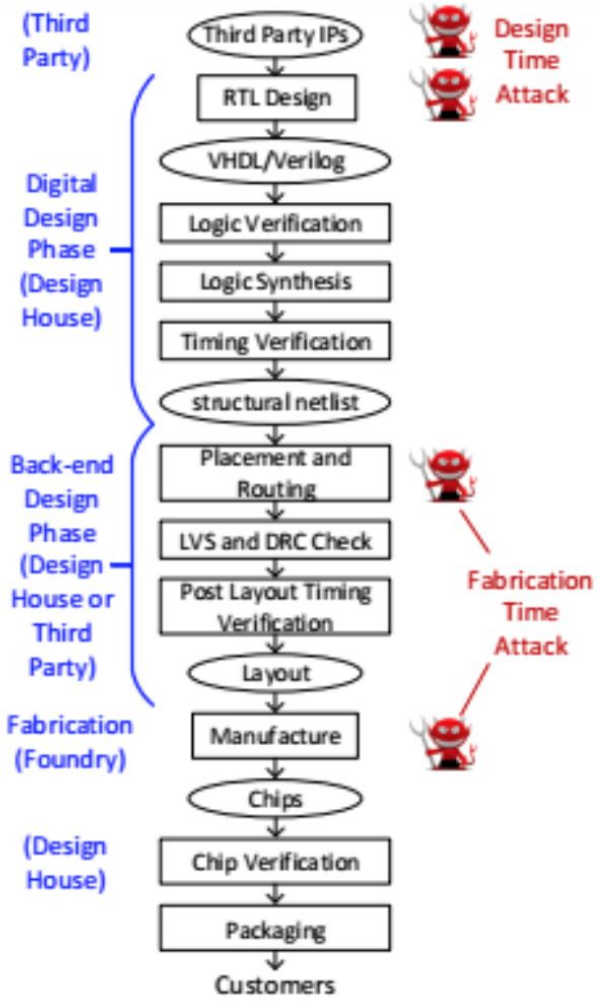
SMIC - major Chinese player

Architecture -> RTL/VHDL/timing -> Fabrication -> Drivers/verification

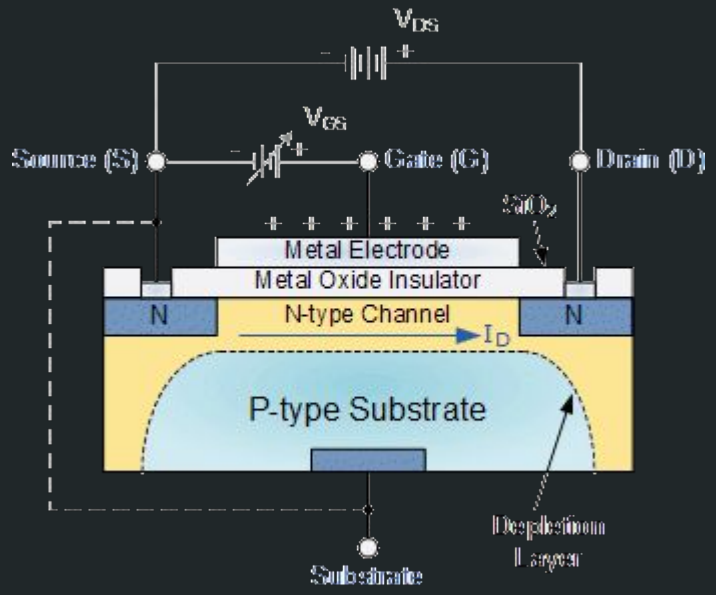


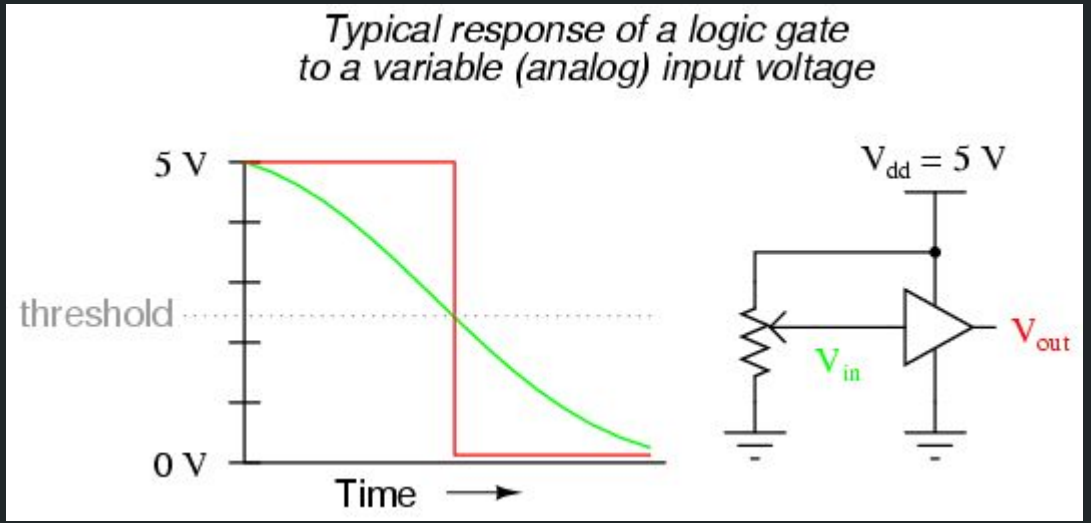


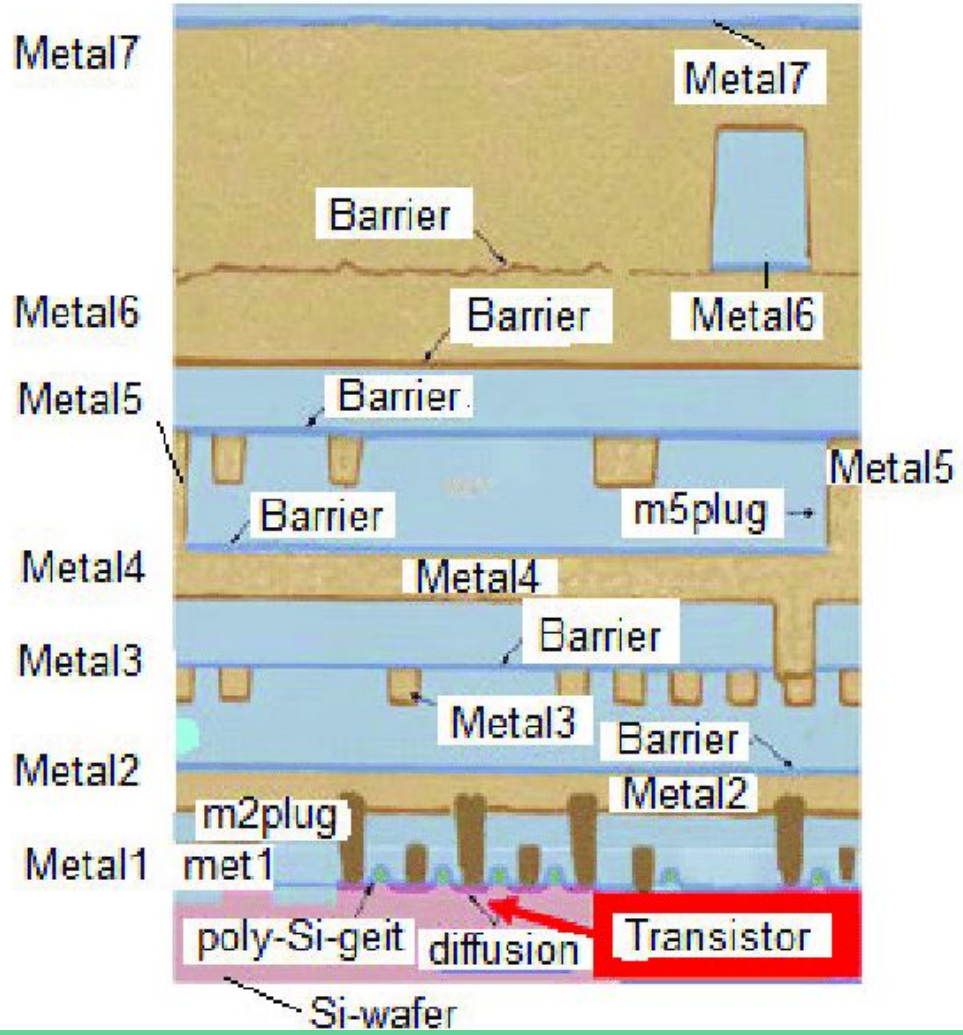


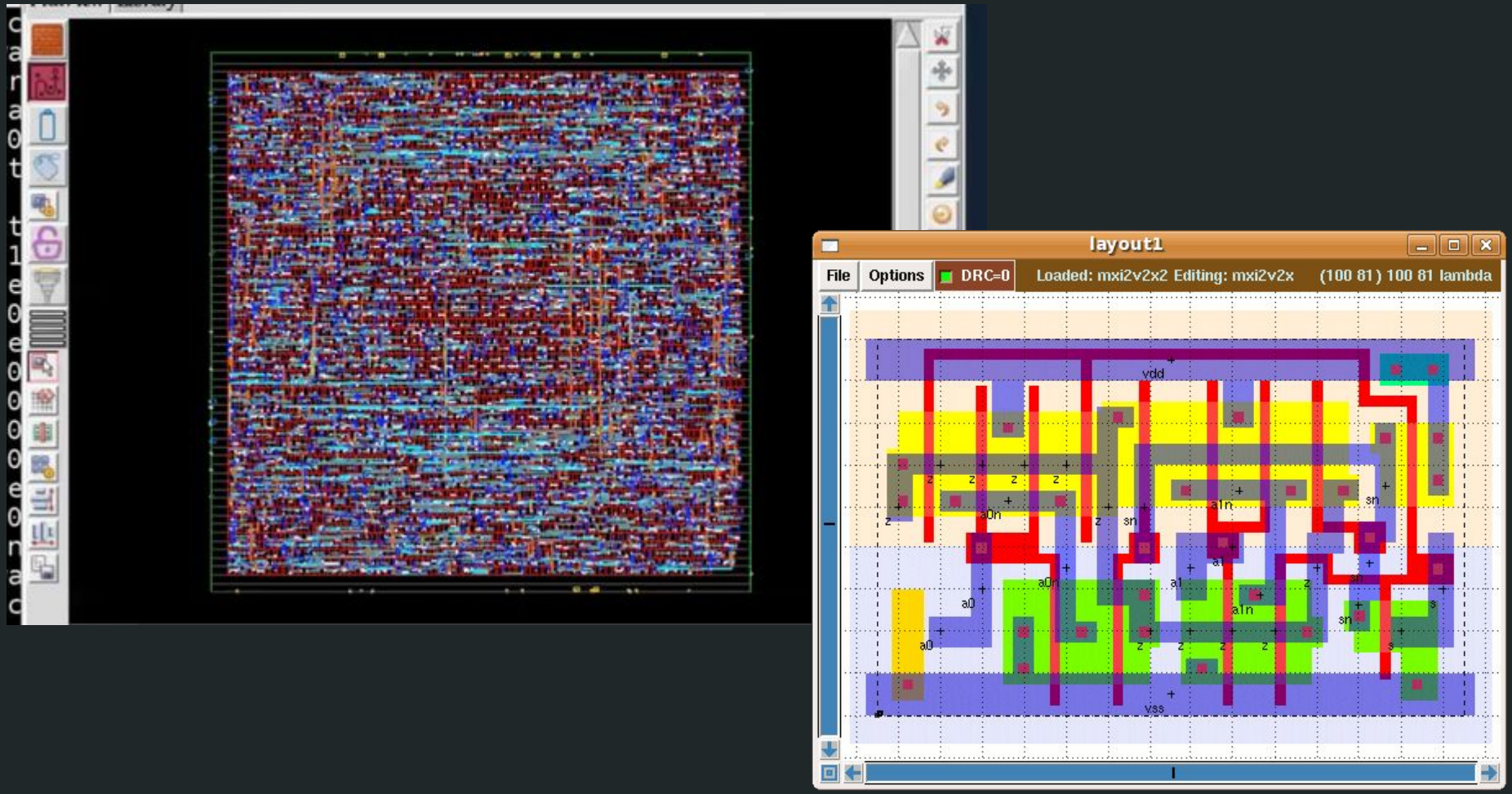

(Third Party)
Third Party IPs
RTL Design
VHDL/Verilog
Logic Verification
Logic Synthesis
Timing Verification
structural netlist
Placement and Routing
LVS and DRC Check
Post Layout Timing Verification
Layout
Manufacture
Chips
Chip Verification
Packaging
Customers
Digital Design Phase (Design House)
Back-end Design Phase (Design House or Third Party)
Fabrication (Foundry)
(Design House)
Design Time Attack
Fabrication Time Attack

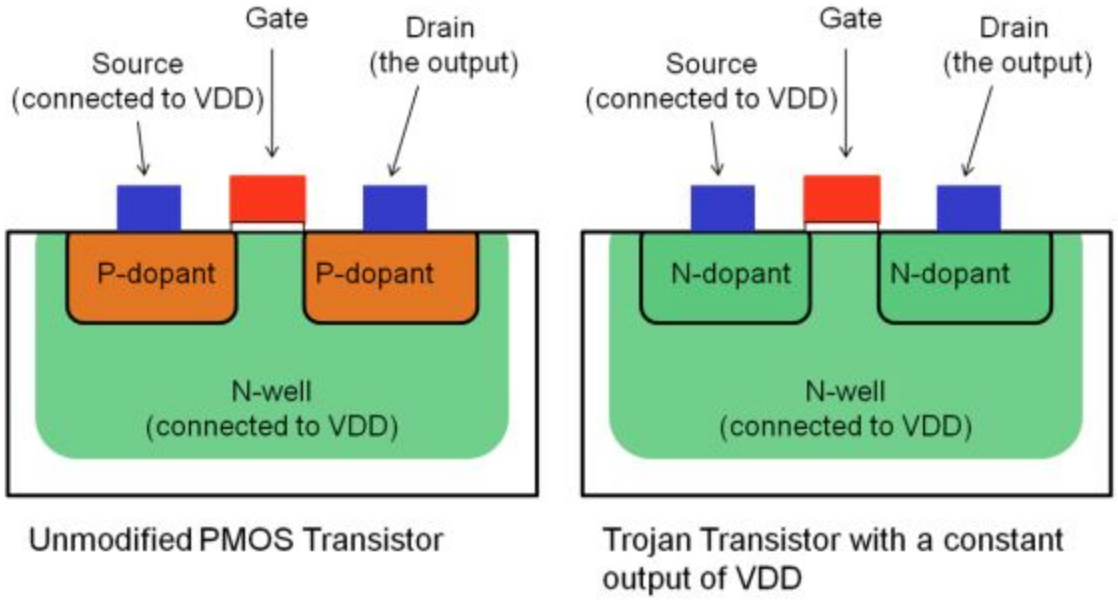
MOSFET:


Source (S)
Gate (G)
Drain (D)
Metal Electrode
Metal Oxide Insulator
N
N-type Channel
N
P-type Substrate
Substrate

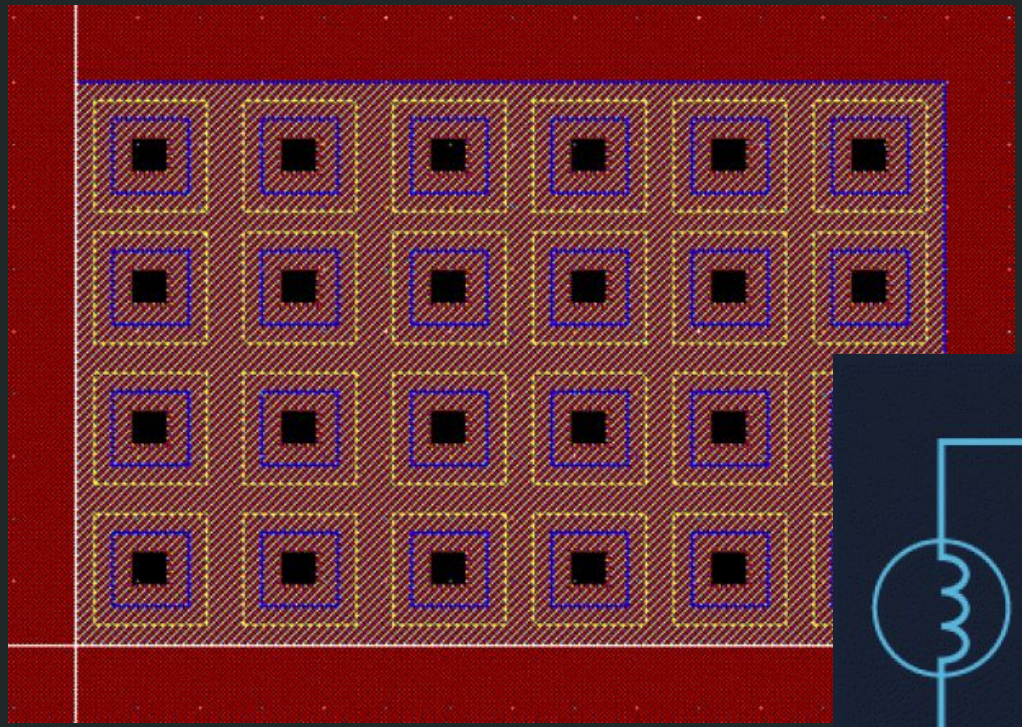

Typical response of a logic gate
to a variable (analog) input voltage
5 V
threshold
0 V
Time
V_{dd} = 5 V
V_{in}
V_{out}

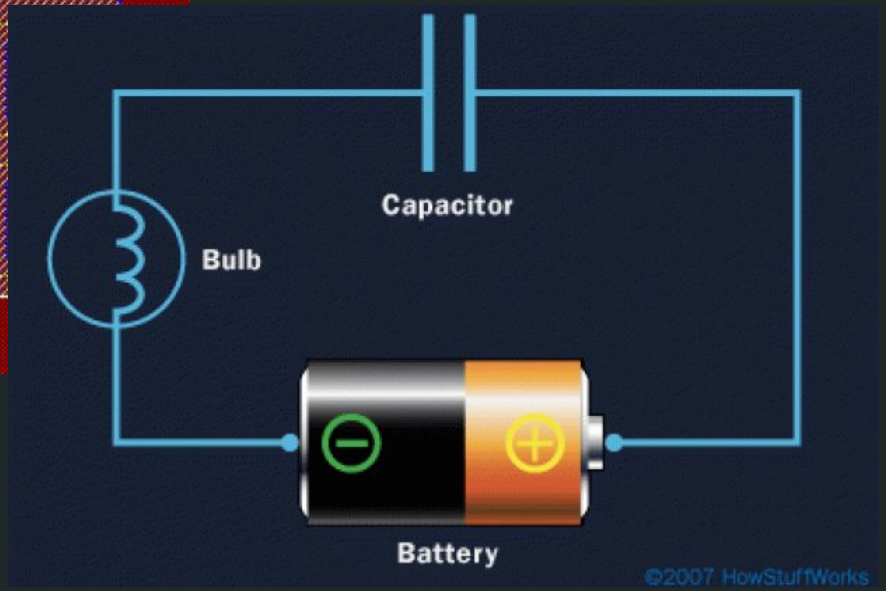

Metal7
Metal7
Barrier
Metal6
Barrier
Metal6
Metal5
Barrier
Metal5
Barrier
m5plug
Metal4
Metal4
Barrier
Metal3
Metal3
Barrier
Metal2
Metal2
m2plug
Metal1
met1
poly-Si-geit
diffusion
Transistor
Si-wafer


layout1
File
Options
DRC=0
Loaded: mxi2v2x2 Editing: mxi2v2x
(100 81) 100 81 lambda
vdd
vss
a0
a0n
a1
a1n
sn
z



(a) p-MOS Transistor




Capacitor
Bulb
Battery
©2007 HowStuffWorks

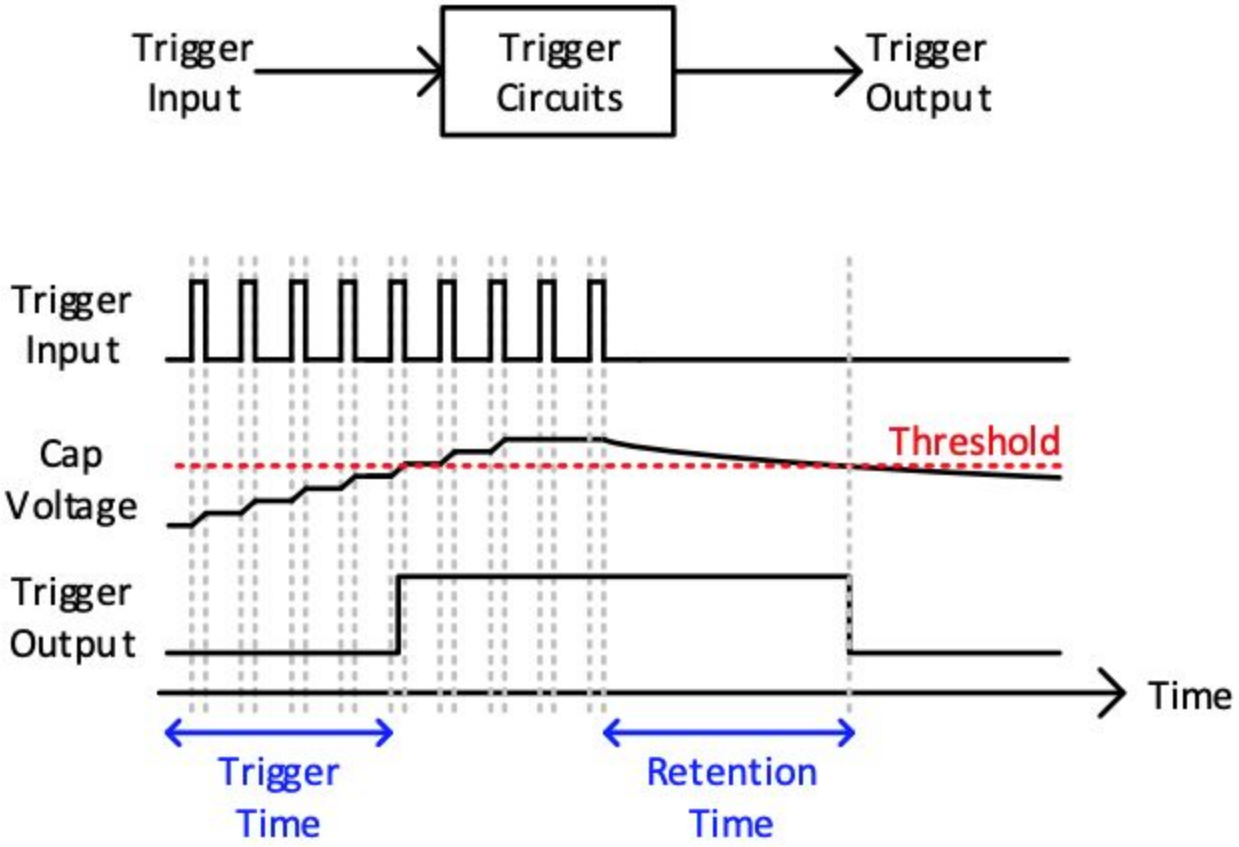
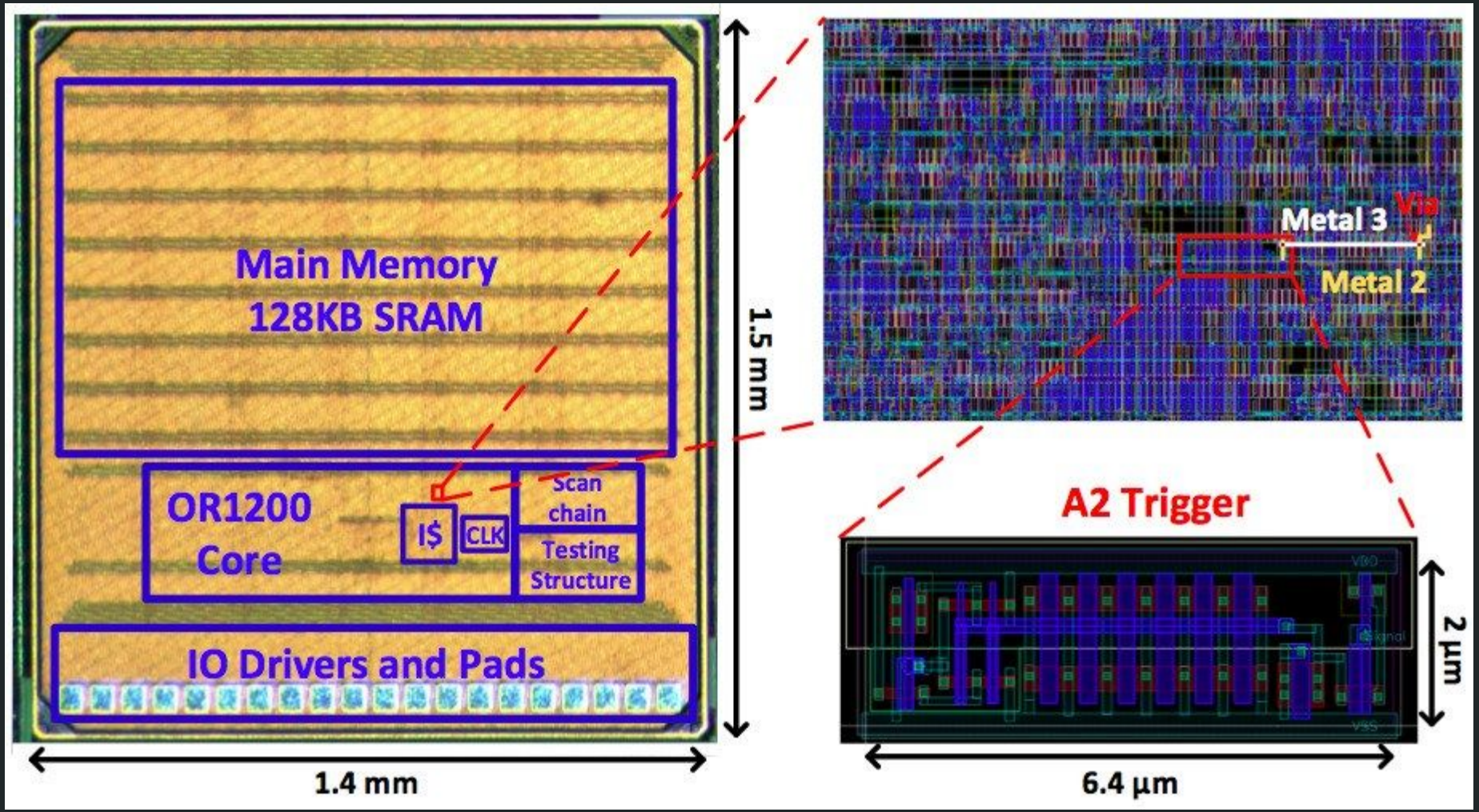
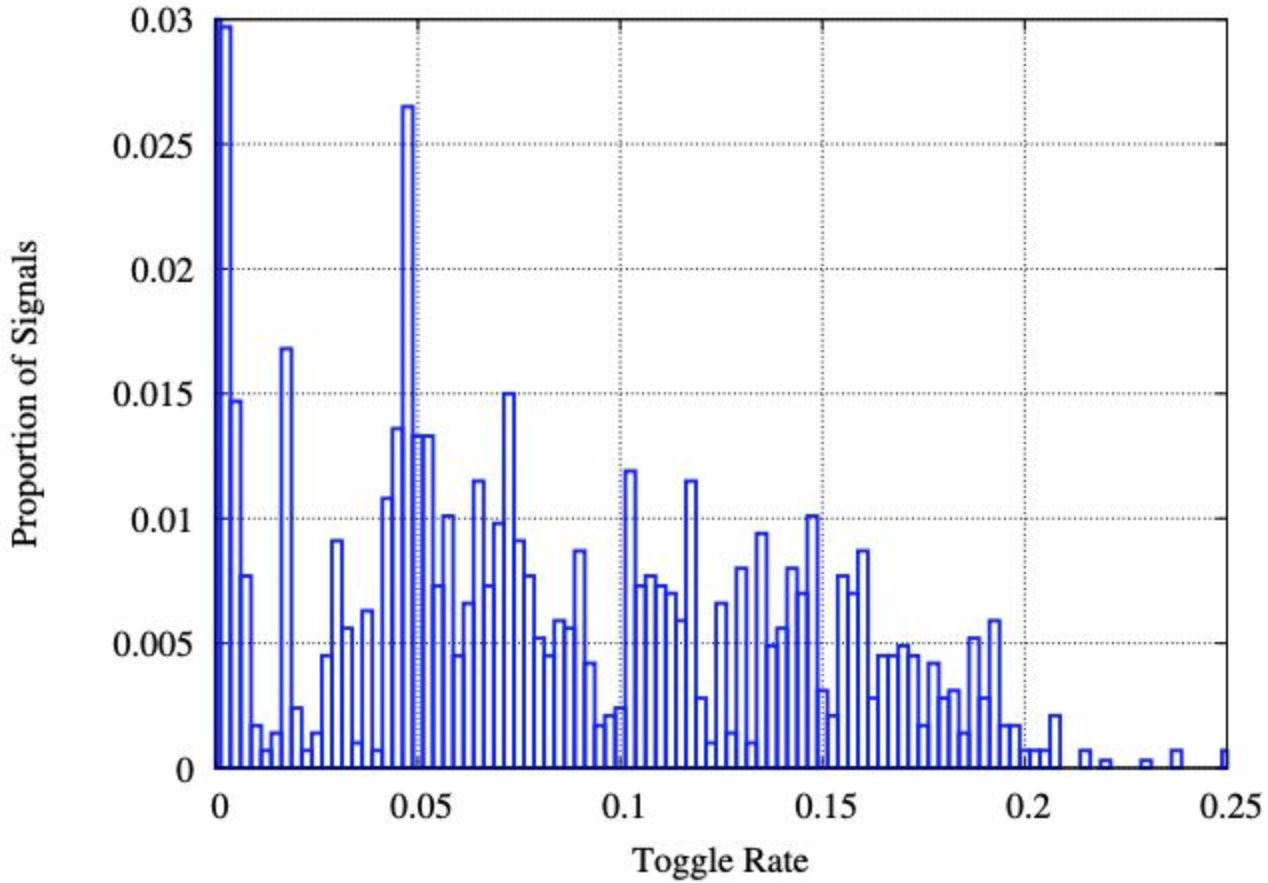
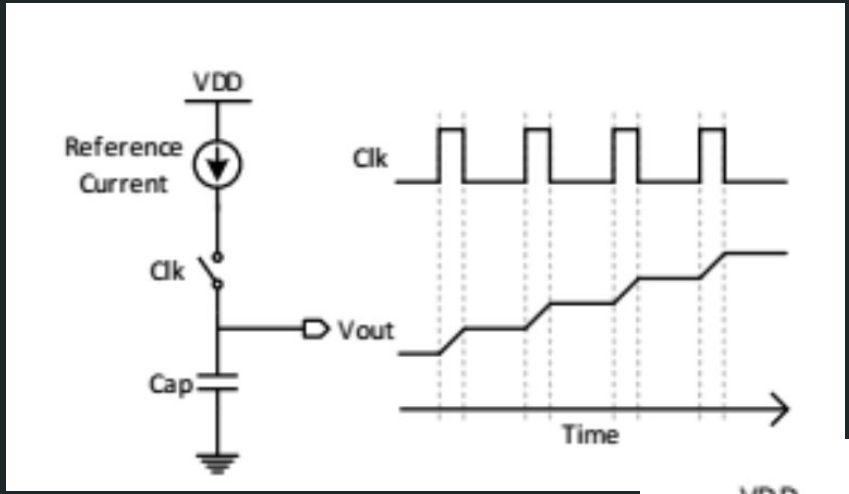
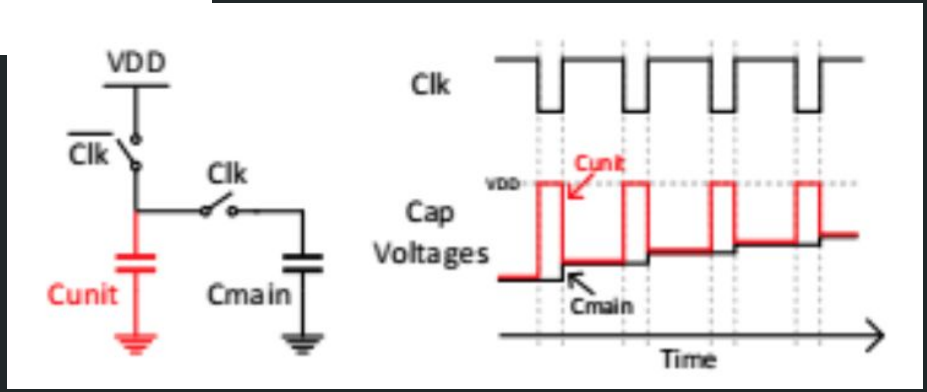


Figure 2: Behavior model of proposed analog trigger circuit.


Main Memory
128KB SRAM
OR1200
Core
I$
CLK
Scan
chain
Testing
Structure
IO Drivers and Pads
1.5 mm
1.4 mm
Metal 3
Via
Metal 2
A2 Trigger
2 µm
6.4 µm


0.03
0.025
0.02
0.015
0.01
0.005
0
Proportion of Signals
0
0.05
0.1
0.15
0.2
0.25
Toggle Rate


VDD
Reference
Current
Clk
Clk
Vout
Cap
Time


VDD
Clk
Clk
Cunit
Cmain
Clk
Cunit
VDD
Cap
Voltages
Cmain
Time

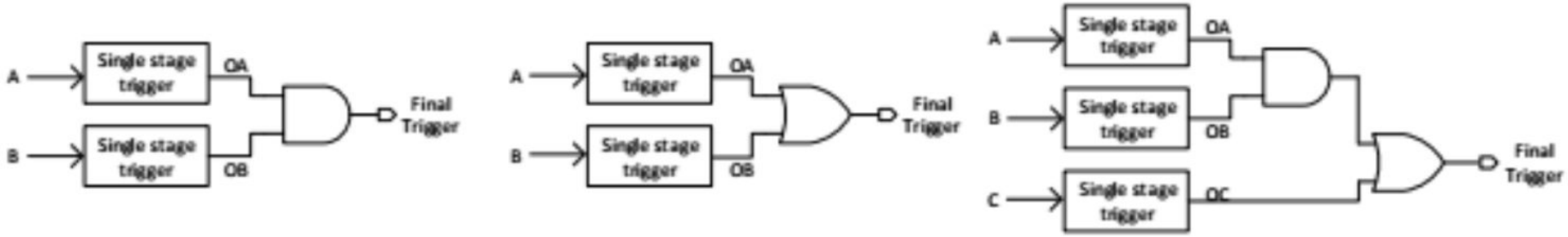


Figure 8: Basic ways of connecting single-stage triggers to form a multi-stage trigger.

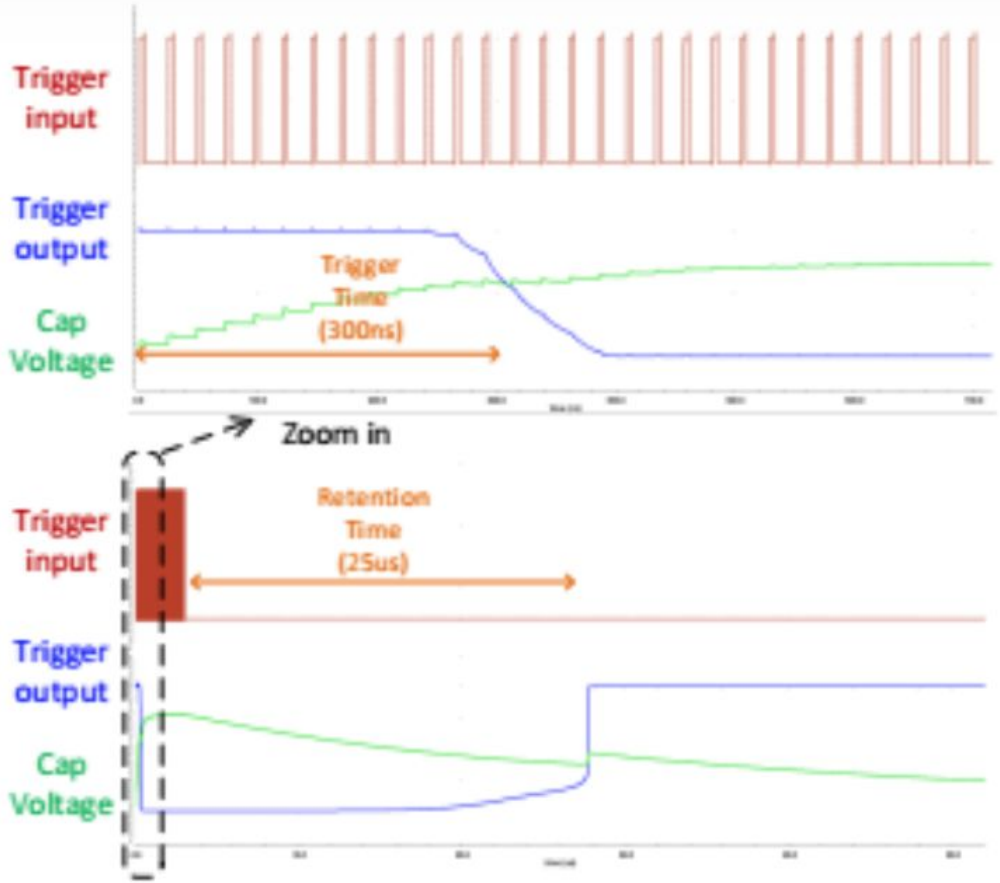
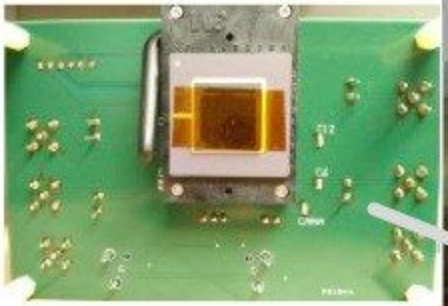


Figure 13: SPICE simulation waveform of analog trigger circuit using IO devices in 65nm CMOS.

Function	Drive Strength	Width†	AC Power†	Standby Power†
NAND2	X1	1	1	1
NAND2	X4	3	3.7	4.1
NAND2	X8	5.75	7.6	8.1
DFF with Async Set	X1	6.25	12.7	2.9
DFF with Async Set	X4	7.25	21.8	6.8
DFF with Async Reset	X1	6	12.7	2.6
DFF with Async Reset	X4	7.75	21.8	7.2
DFF with Async Set and Reset	X1	7.5	14.5	3.3
DFF with Async Set and Reset	X4	8.75	23.6	8.1
Trigger w/o IO device	**-**	**8**	**7.7**	**2.2**
Trigger w/ IO device	**-**	**13.5**	**0.08**	**0.08**

* DFF stands for D Flip Flop. † Normalized values

Packaged test chip



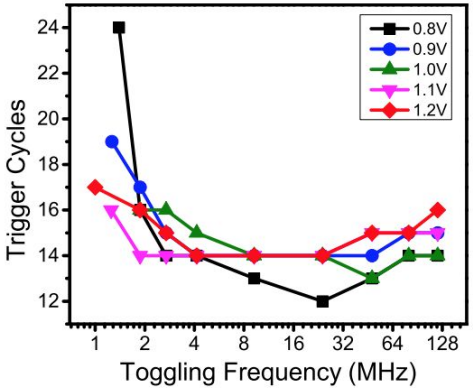
Testing PCB

Temperature Chamber

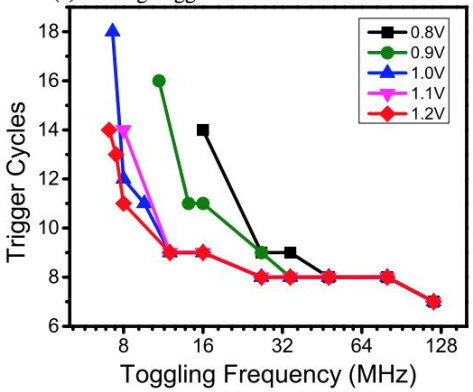
Labview

Power supply and source meter

Digital IO

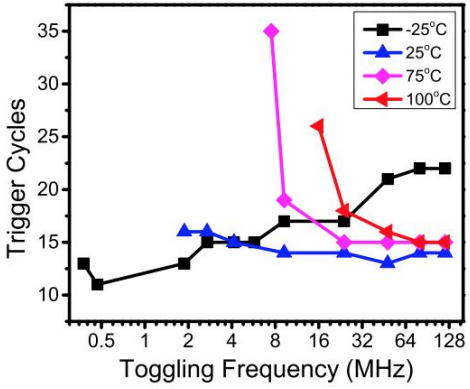


(a) Analog trigger circuit with IO device

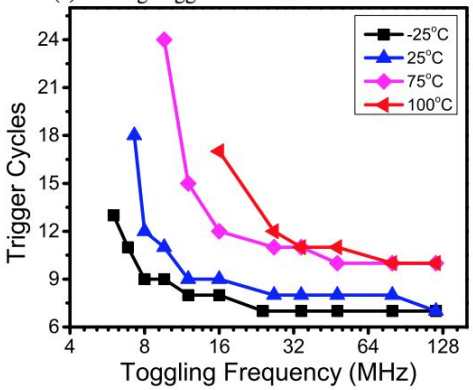


(b) Analog trigger circuit with only core device

Figure 18: Measured trigger cycles under different input frequency at different supply voltages.



(a) Analog trigger circuit with IO device



(b) Analog trigger circuit with only core device

Figure 19: Measured trigger cycles under different input frequency at different ambient temperatures.

Microprocessor transistor counts 1971-2011 & Moore's law