"Logic Design Pathology and Space Flight Electronics"

Richard B. Katz
NASA Goddard Space Flight Center

Dr. Rod L. Barto
Spacecraft Digital Electronics

Ken Erickson
Jet Propulsion Laboratory

Introduction

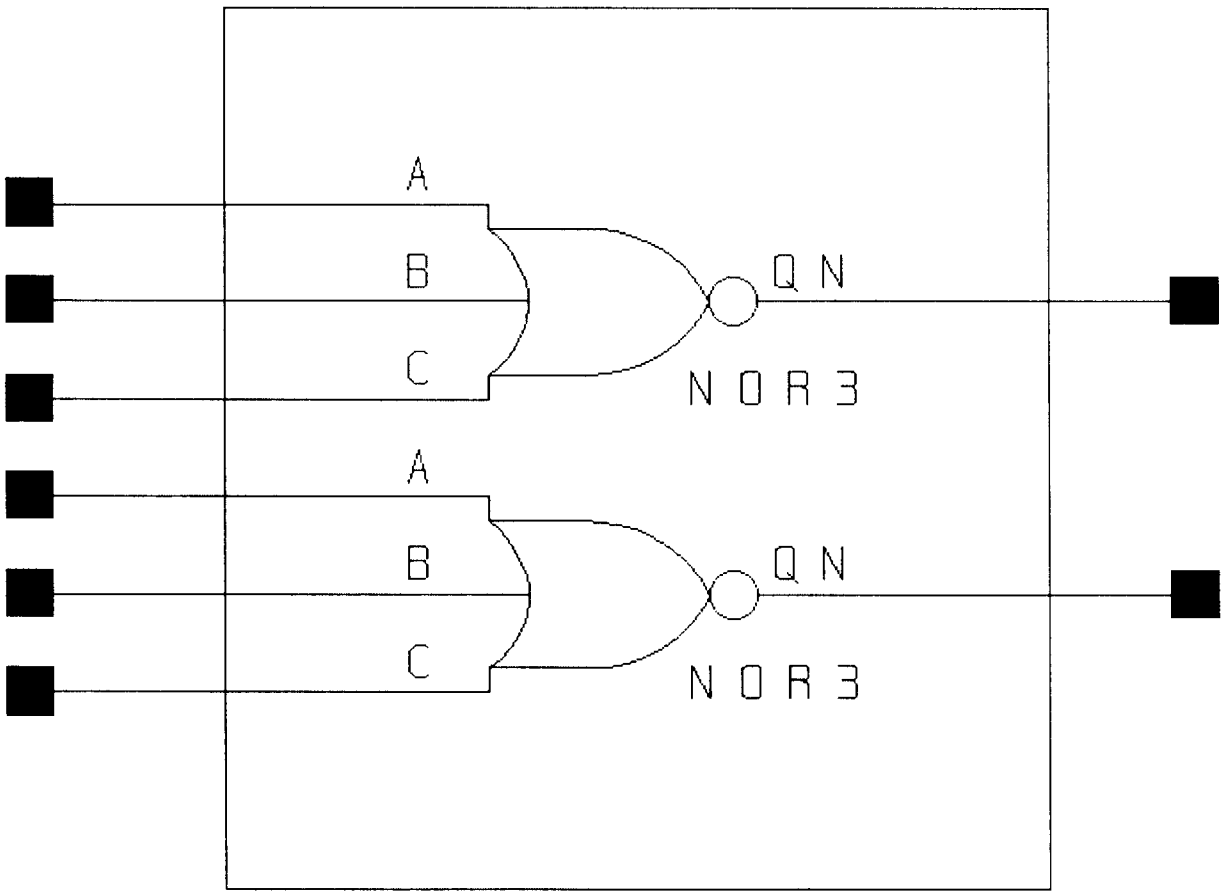
- Look at Logic Design from Early in the US Space Program
- Examine Faults in Recent Logic Designs
- Most Examples Are Based on Flight Hardware Failures
- Some Examples Are From an Analysis of New Tools and Techniques
- Sampling - Many More Examples in the Full Paper

Apollo Guidance Computer

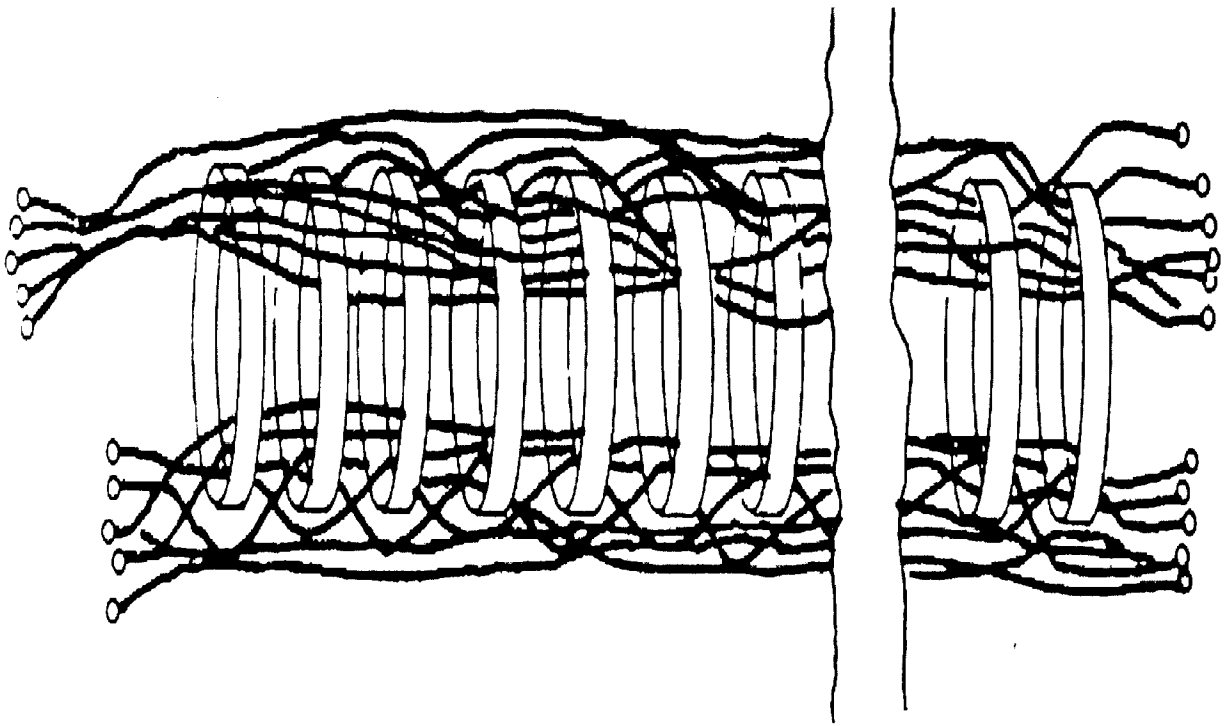
(AGC)

Technology

Apollo Guidance Computer
Logic Element - Microcircuit



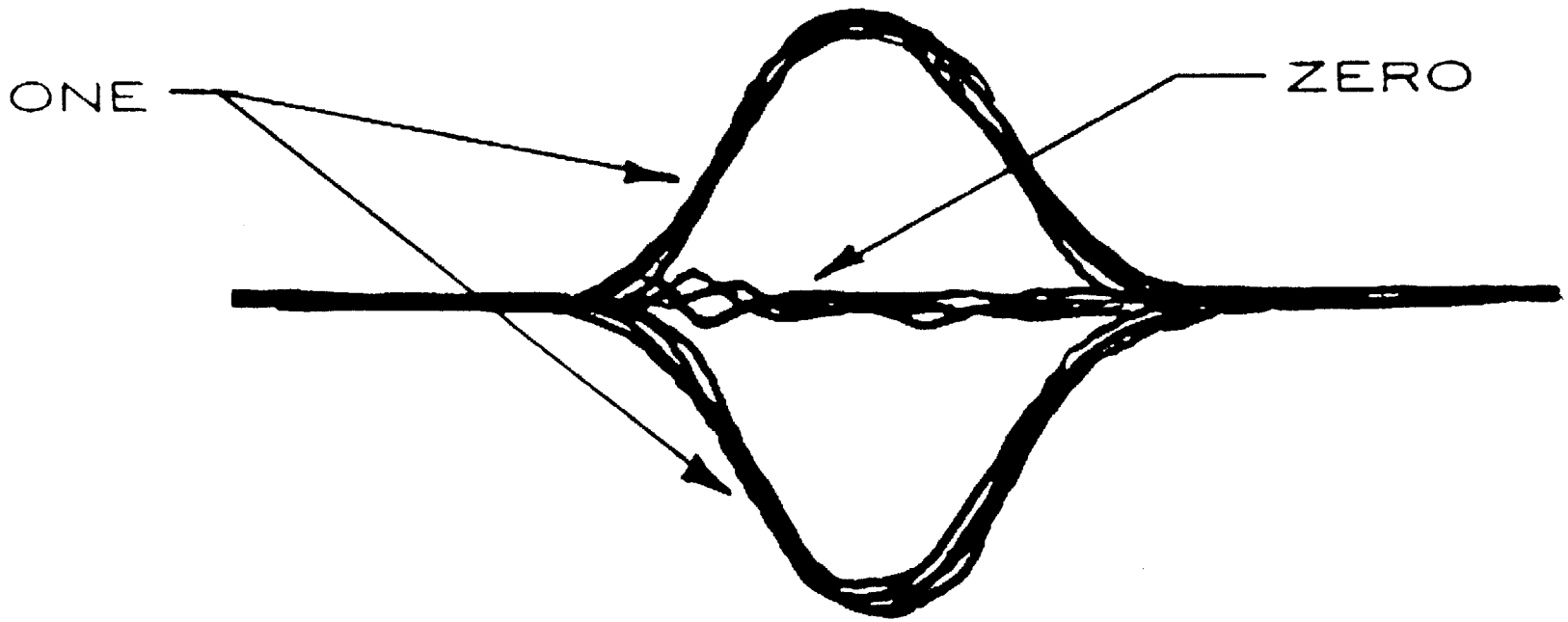
Inihibit and Sense Lines Through a "Rope Memory"



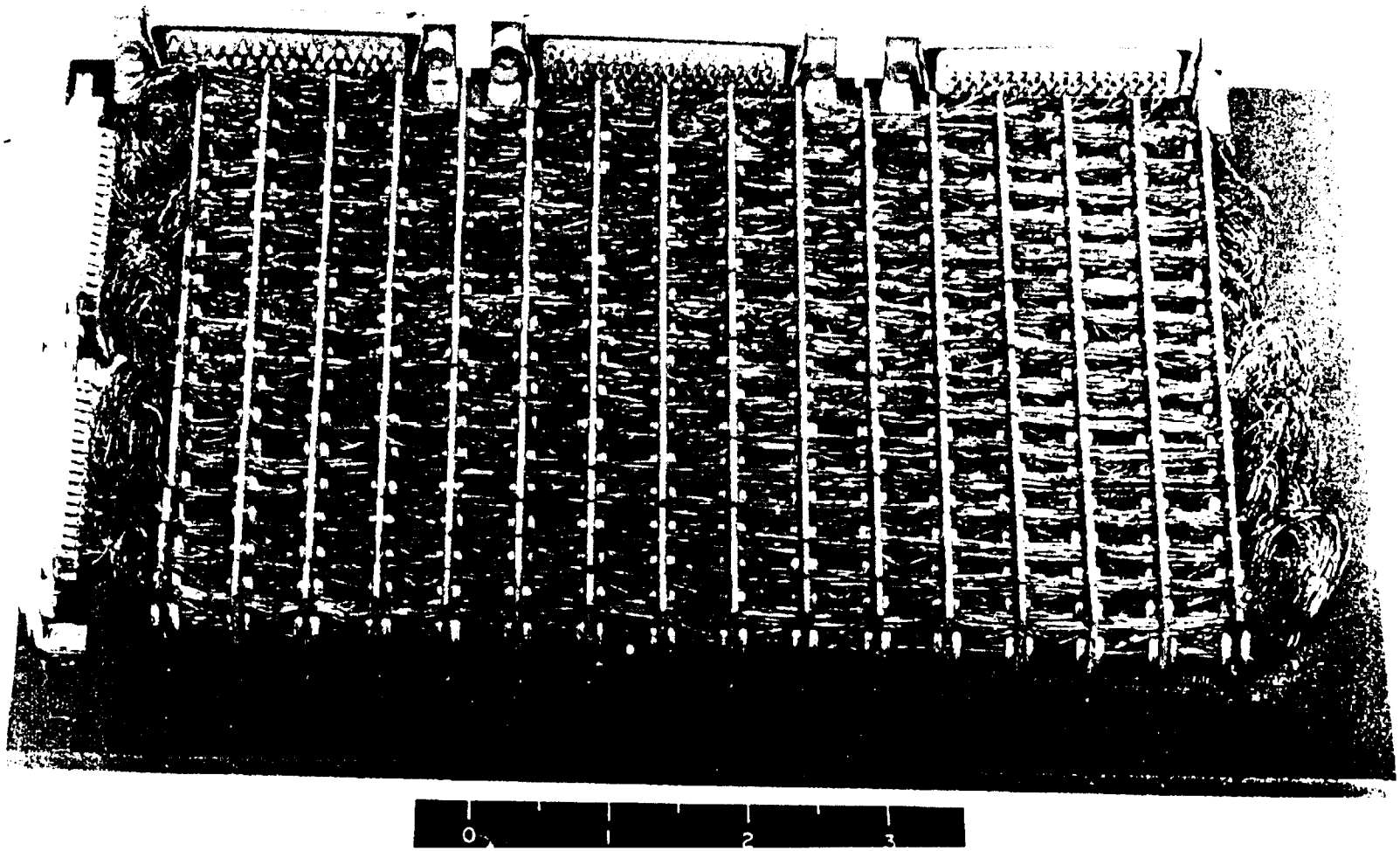
Sense Lines
(Information)

Inhibit Lines
(Core Selection)

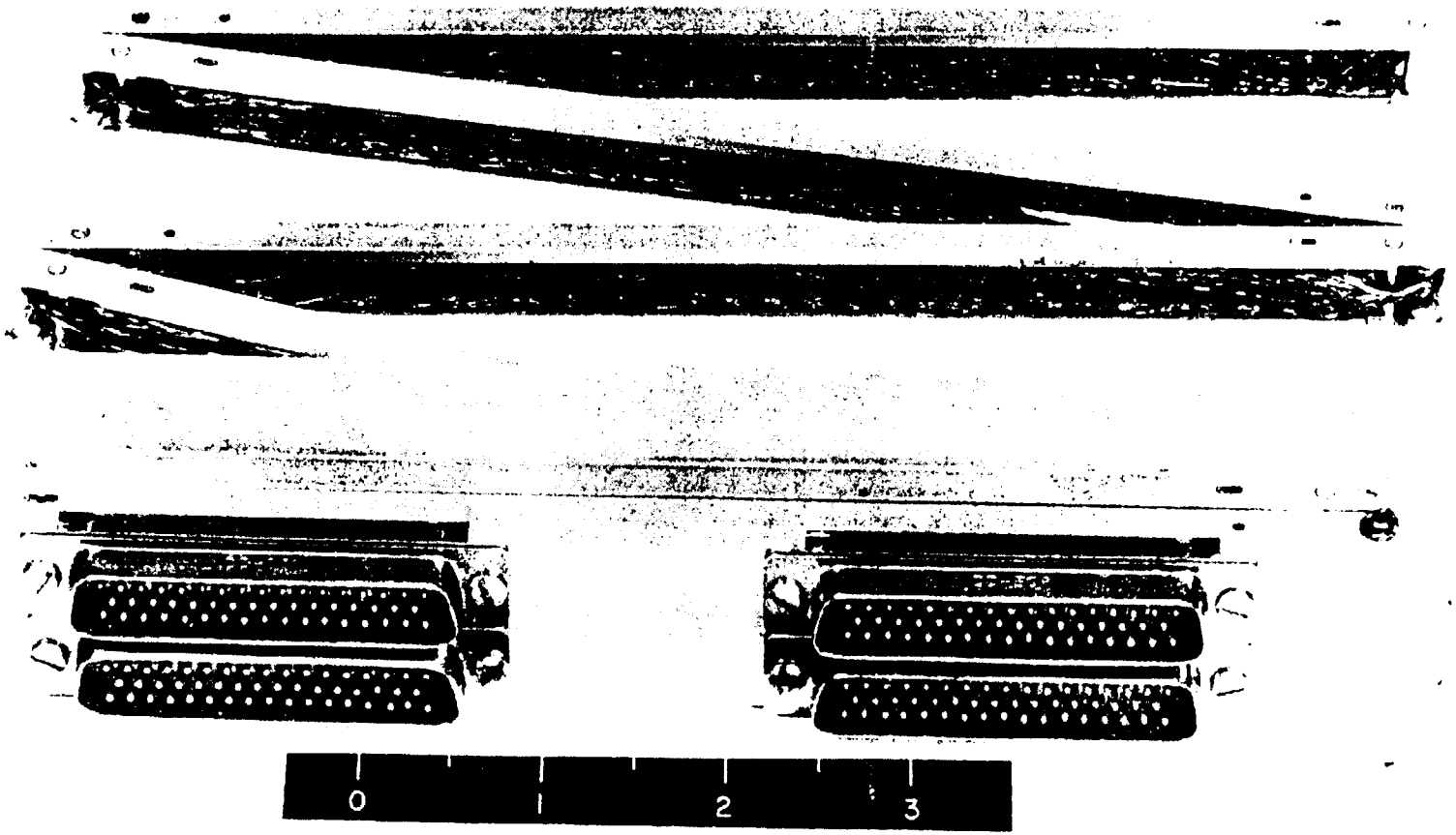
Sequential Output Envelope of a 256 Core Rope Memory



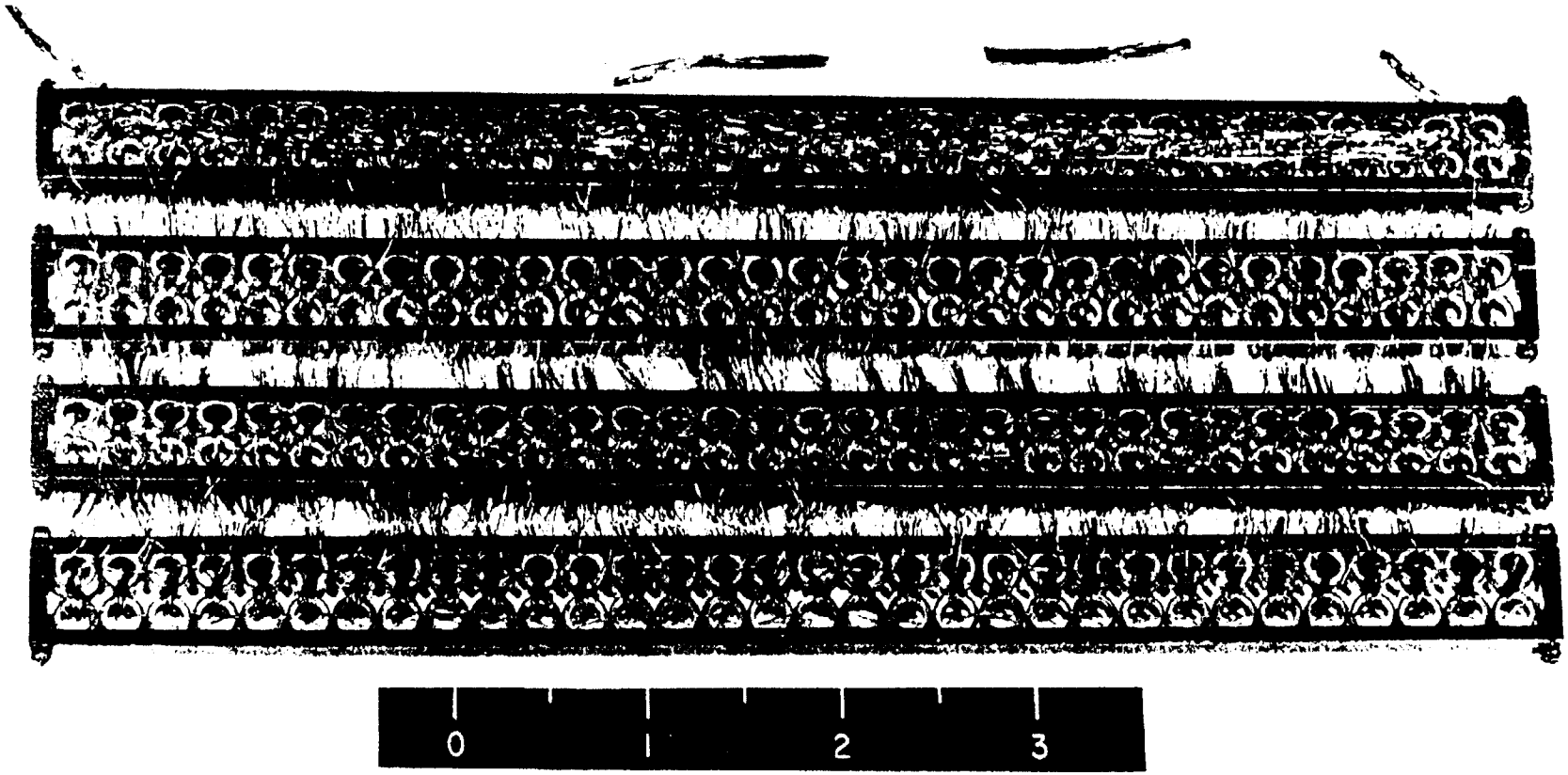
Core Rope Memory
Burroughs Corporation



Core Rope Memory
Sippican Corporation



Core Rope Memory
Raytheon Corporation

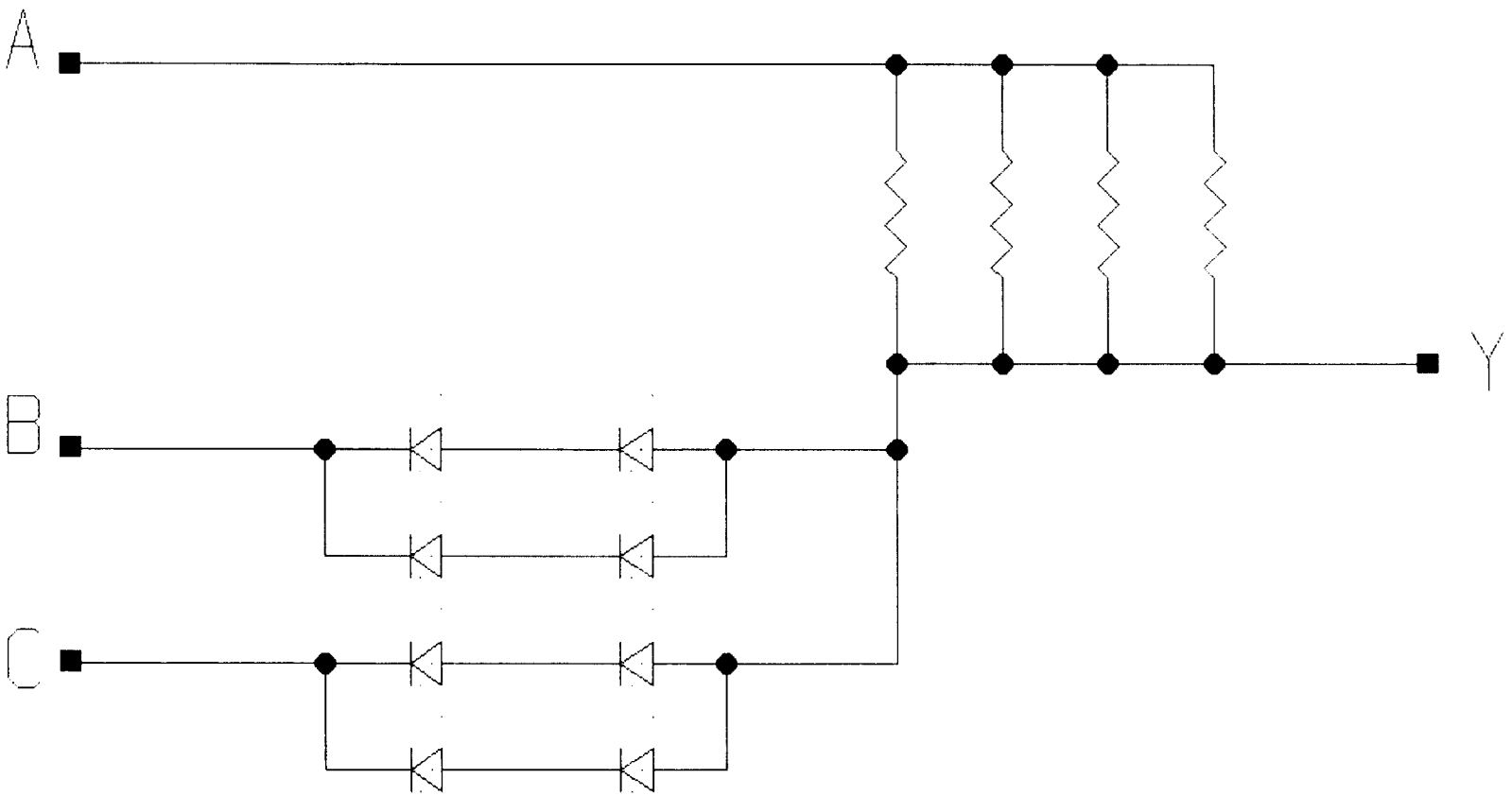


Orbiting Astronomical Observatory

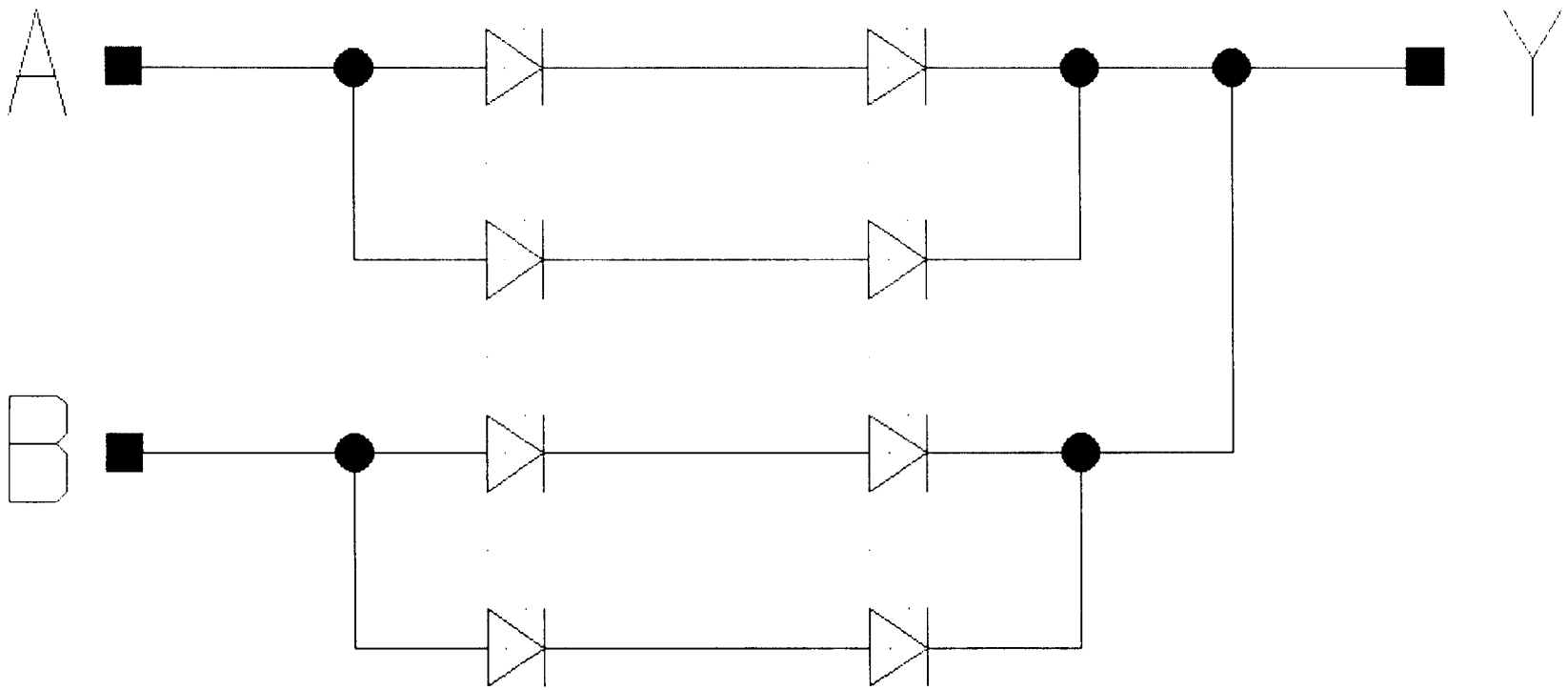
(OAO)

Technology

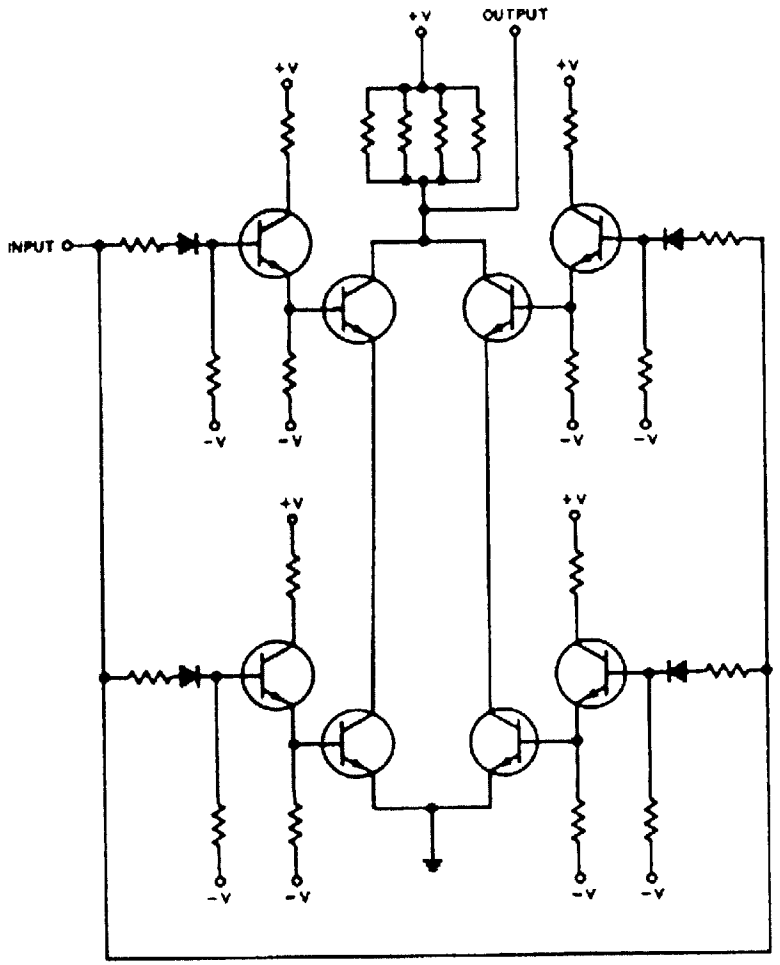
Quad Redundant AND Gate Orbiting Astronomical Observatory



Quad Redundant AND Gate Orbiting Astronomical Observatory



Quad Redundant Inverter
Orbiting Astronomical Observatory



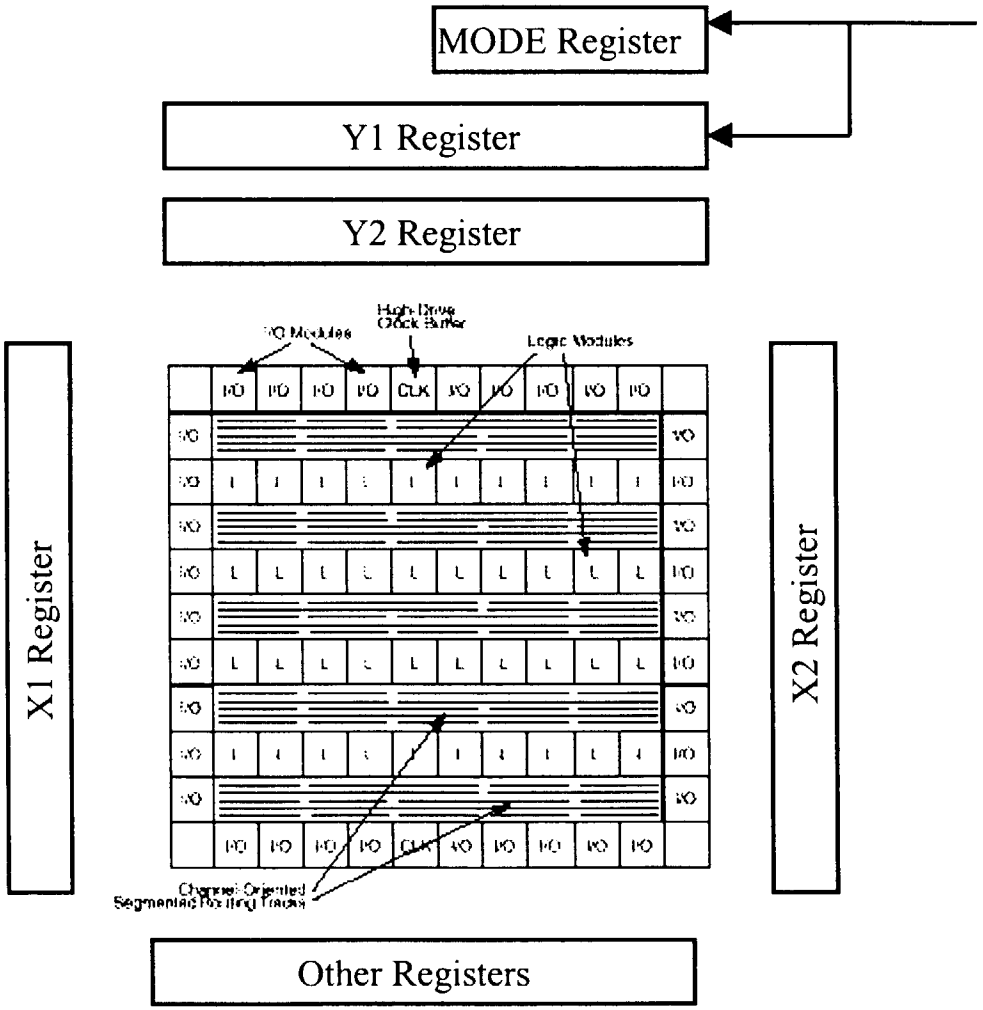
Termination of Special Pins

- MODE pin (test program mode).
- V_{PP} pin (programming voltage).
- TRST* (Reset to JTAG TAP controller)
- TCLK (provides clock to TAP controller)
- SDI, DCLK (varies for each device type)
- Others

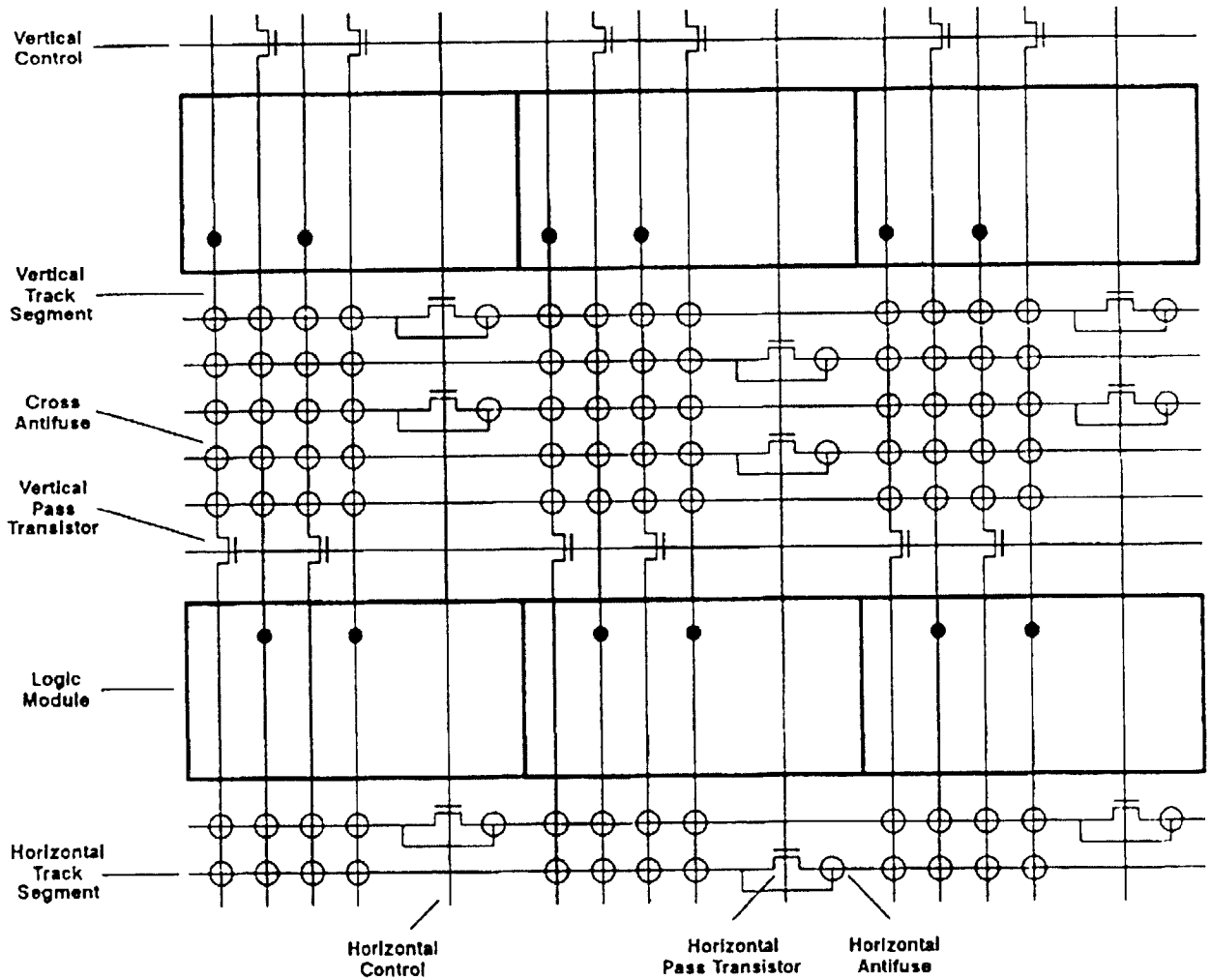
MODE Pin

- Left Floating
  - Device can be non-functional
  - High currents
  - Uncontrolled I/O
- Tied High During Test
  - Working device stopped functioning
  - Power supply rise time key

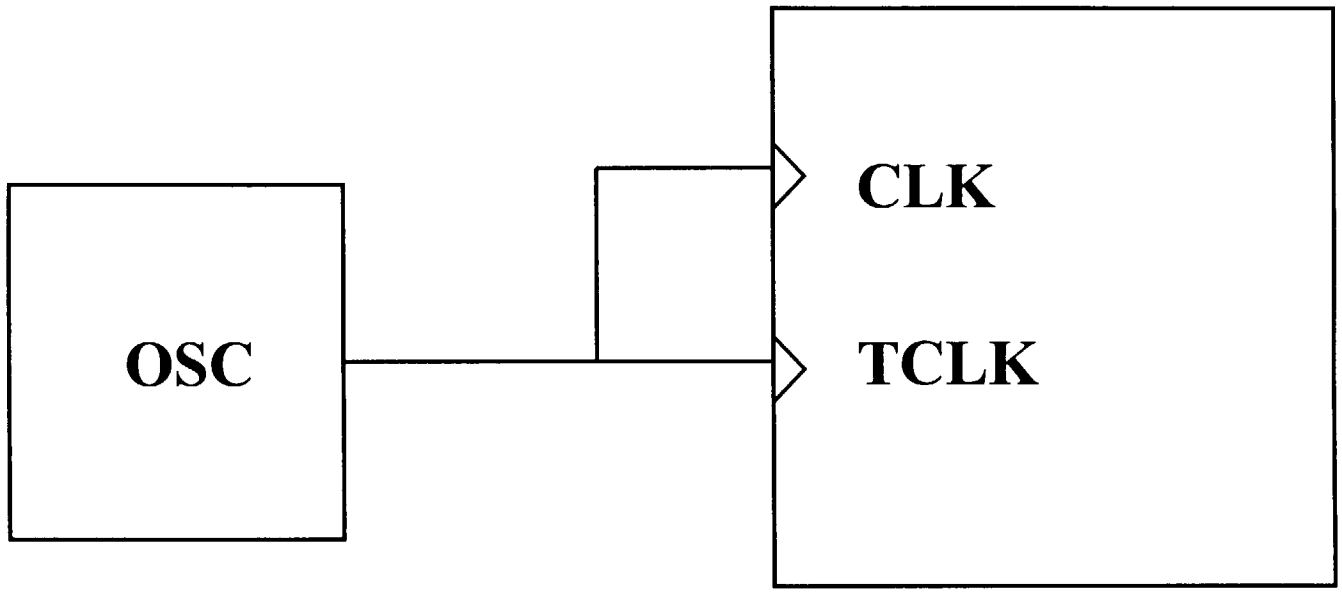
MODE Pin - Test, Debug and Programming Control



MODE Pin - Test, Debug and Programming Control

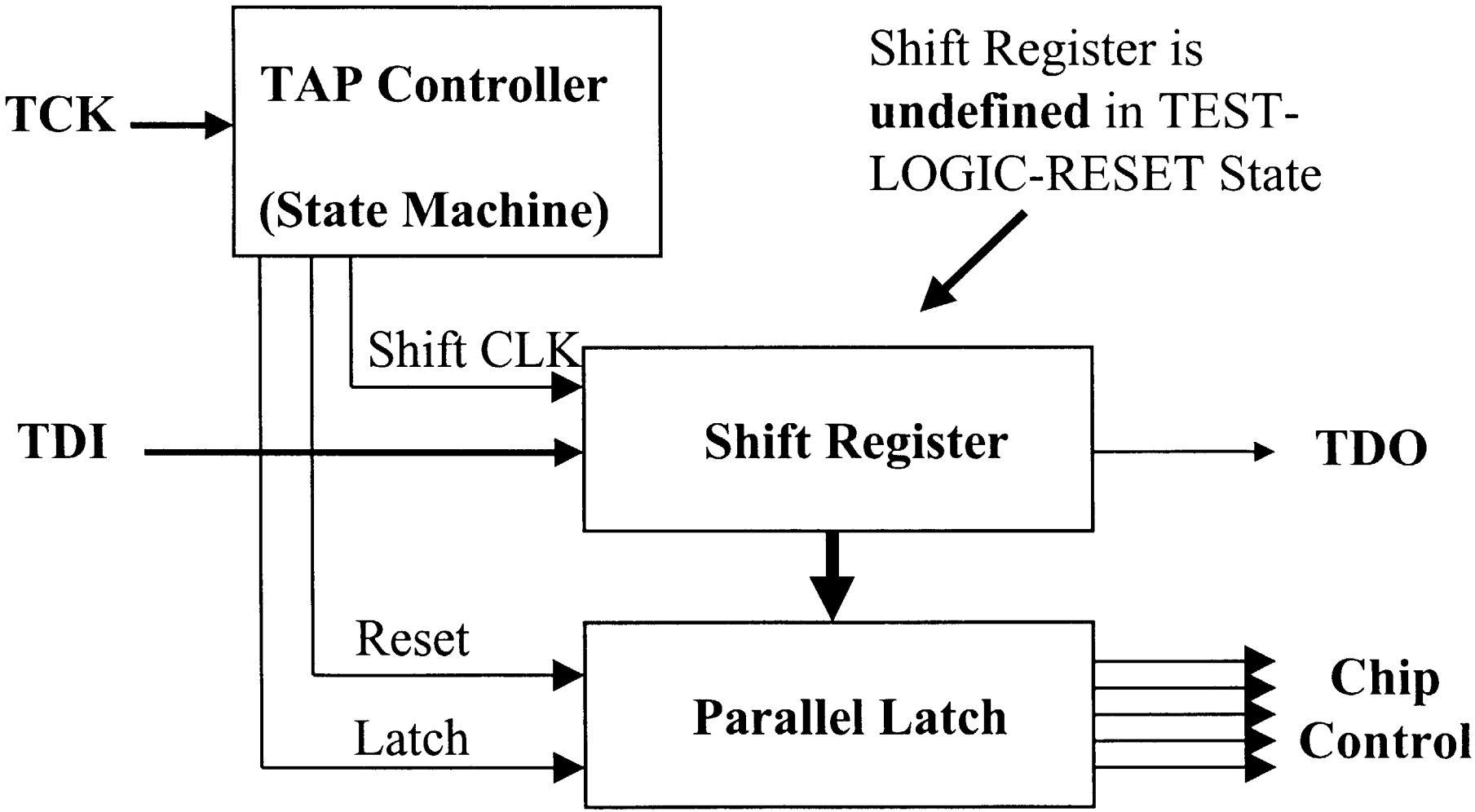


IEEE JTAG 1149.1 TCLK

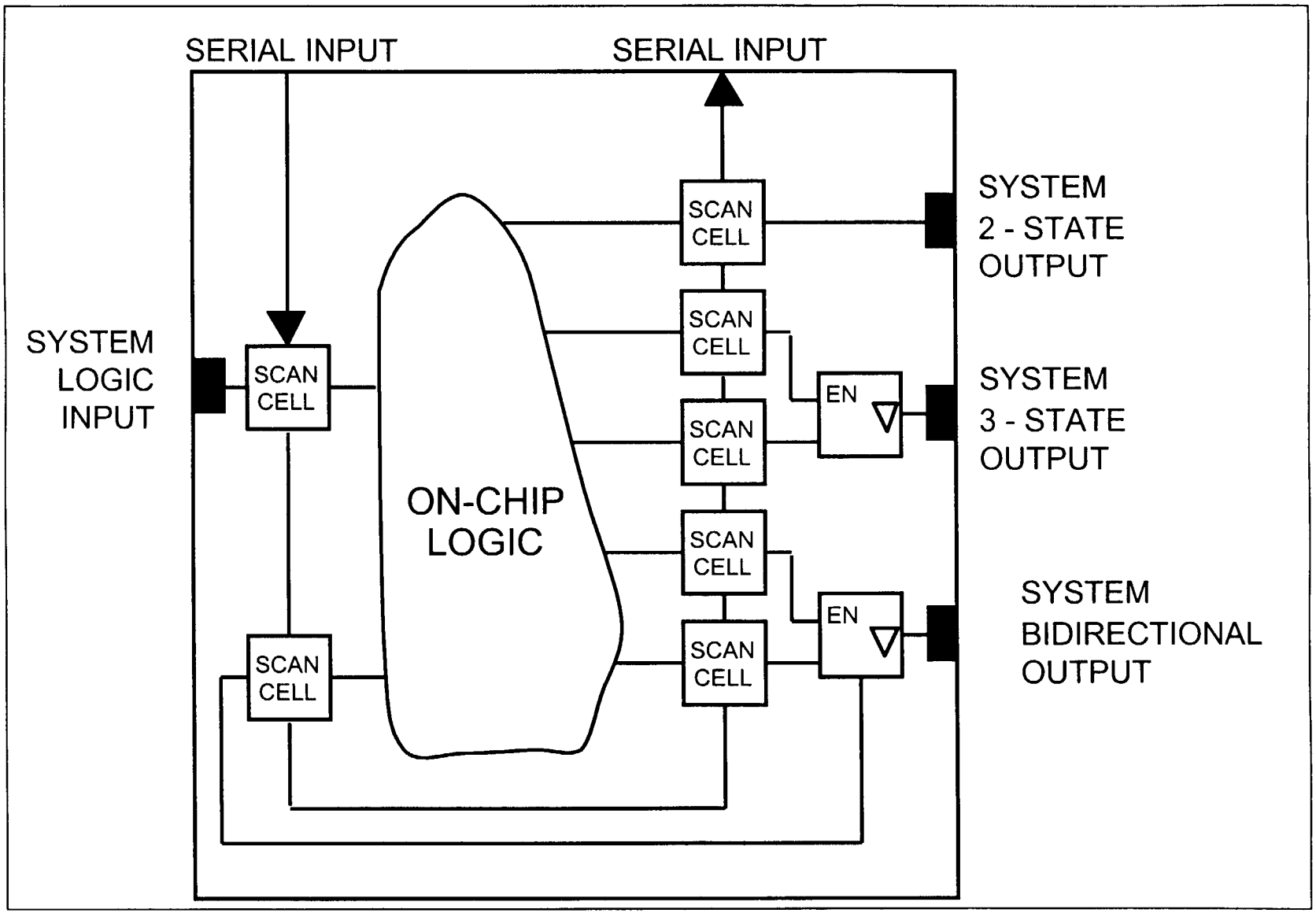


The CLK pin may turn into an output driving low, clamping the oscillator's output at a logic '0'. The TAP controller can not reset and restore I/O operation. Most FPGAs do not have the optional TRST* pin. Note TRST*, when present, has a pull-up.

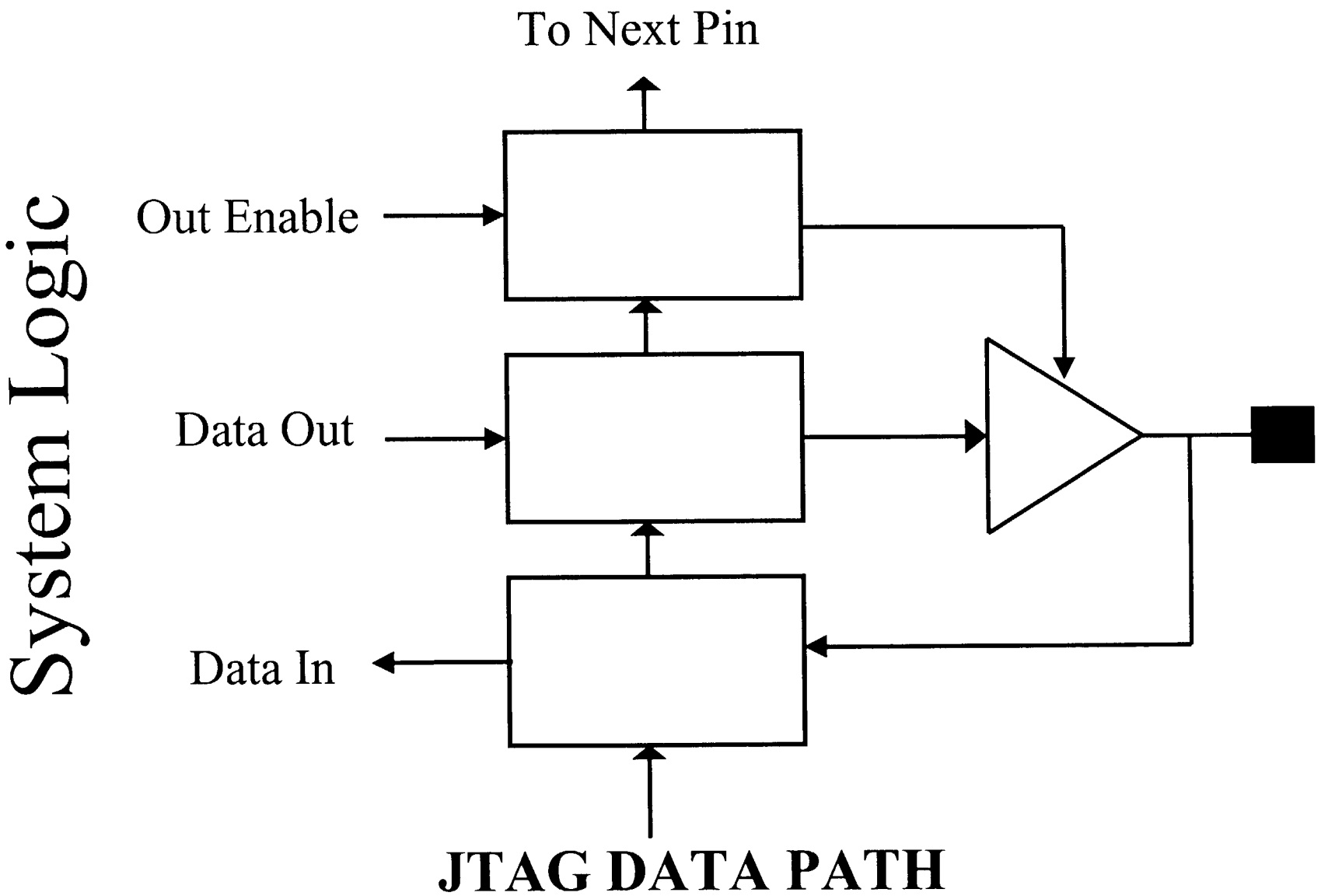
IEEE JTAG 1149.1 TCLK



IEEE JTAG 1149.1 - Scan Path



IEEE JTAG 1149.1 - Scan I/O Cell

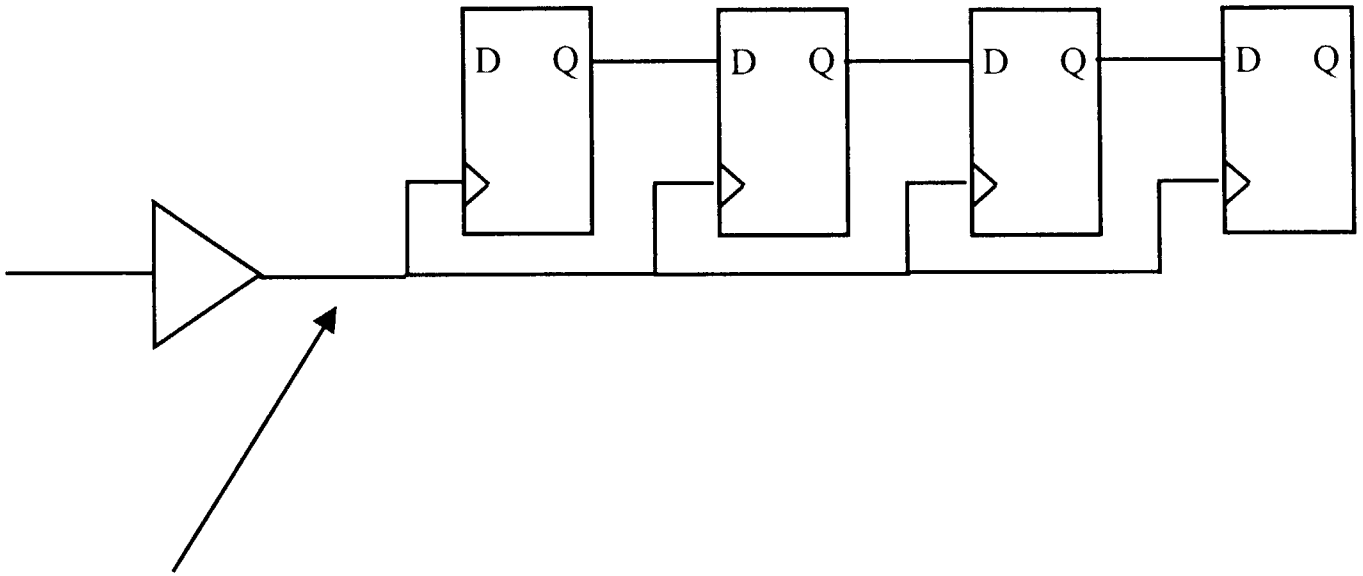


VHDL "Interface"

```
Library IEEE;
  Use IEEE.Std_Logic_1164.All;
Entity Bool Is
  Port ( X   : In  Std_Logic;
         Y   : In  Std_Logic;
         Z   : Out Boolean    );
End Bool;

Library IEEE;
  Use IEEE.Std_Logic_1164.All;
Architecture Bool_Test of Bool Is
Begin
  P: Process ( X, Y )
     Begin
       If ( X = Y )
         Then Z <= True;
         Else Z <= False;
         End If;
     End Process P;
End Bool_Test;
```

- Boolean signal was mapped to different logical values in different versions of the same VHDL logic synthesizer

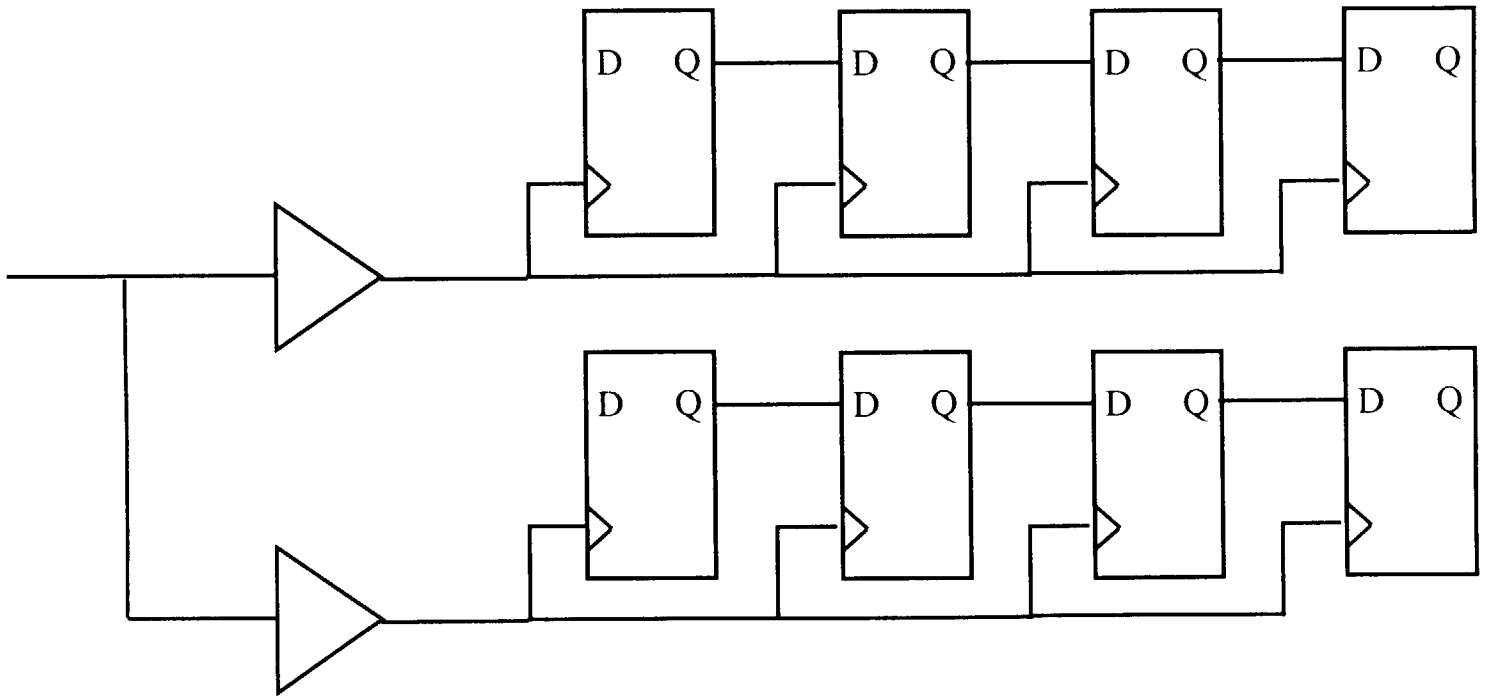
Clock Skew



Normal Routing Resource

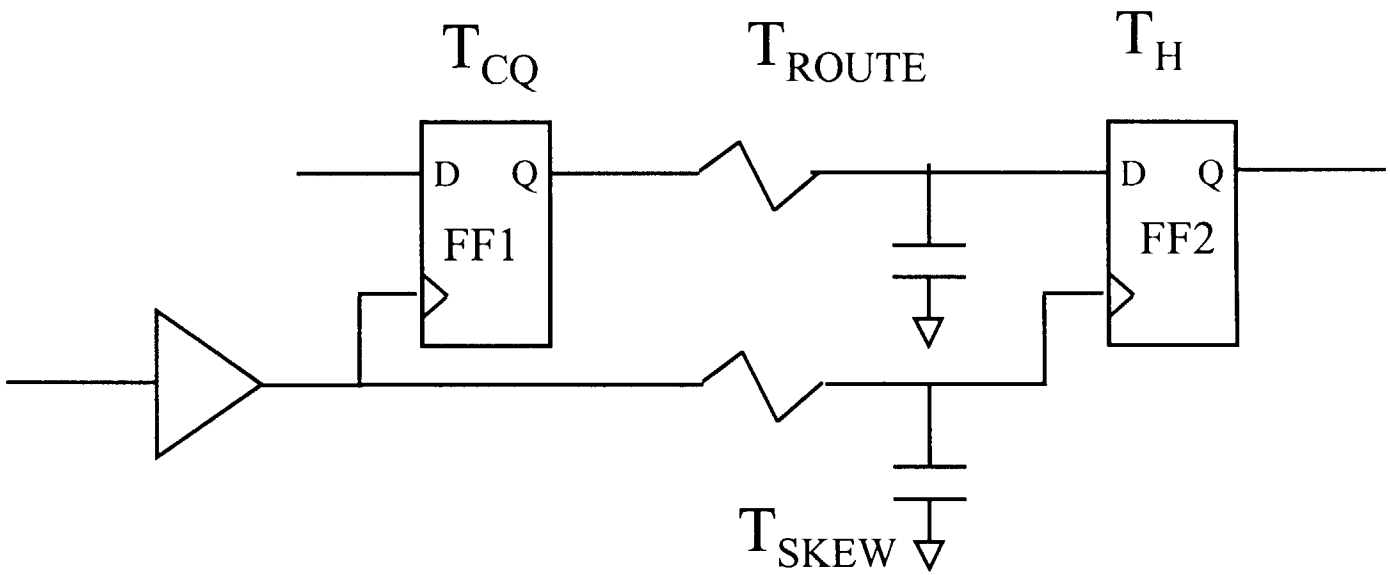
Shift register is given as an example. Also seen in counters and other logic structures.

Clock Skew



- Clock trees are made to increase fanout.
- Not placing buffers and flip-flops on the same row
  - Can increase skew problem.

Clock Skew - Timing Model



- Hold time at FF2 is the concern.
  - Worst-case
  - Low V_{IH} FF1
  - Hi V_{IH} FF2
  - Fast T_{CQ}, T_{Route}
  - High T_{SKEW}
- $T_{CQ} + T_{ROUTE} + T_H > T_{SKEW}$

Clock Skew - Timing Analysis

Most static timing analyzers give bounded numbers for min, max.

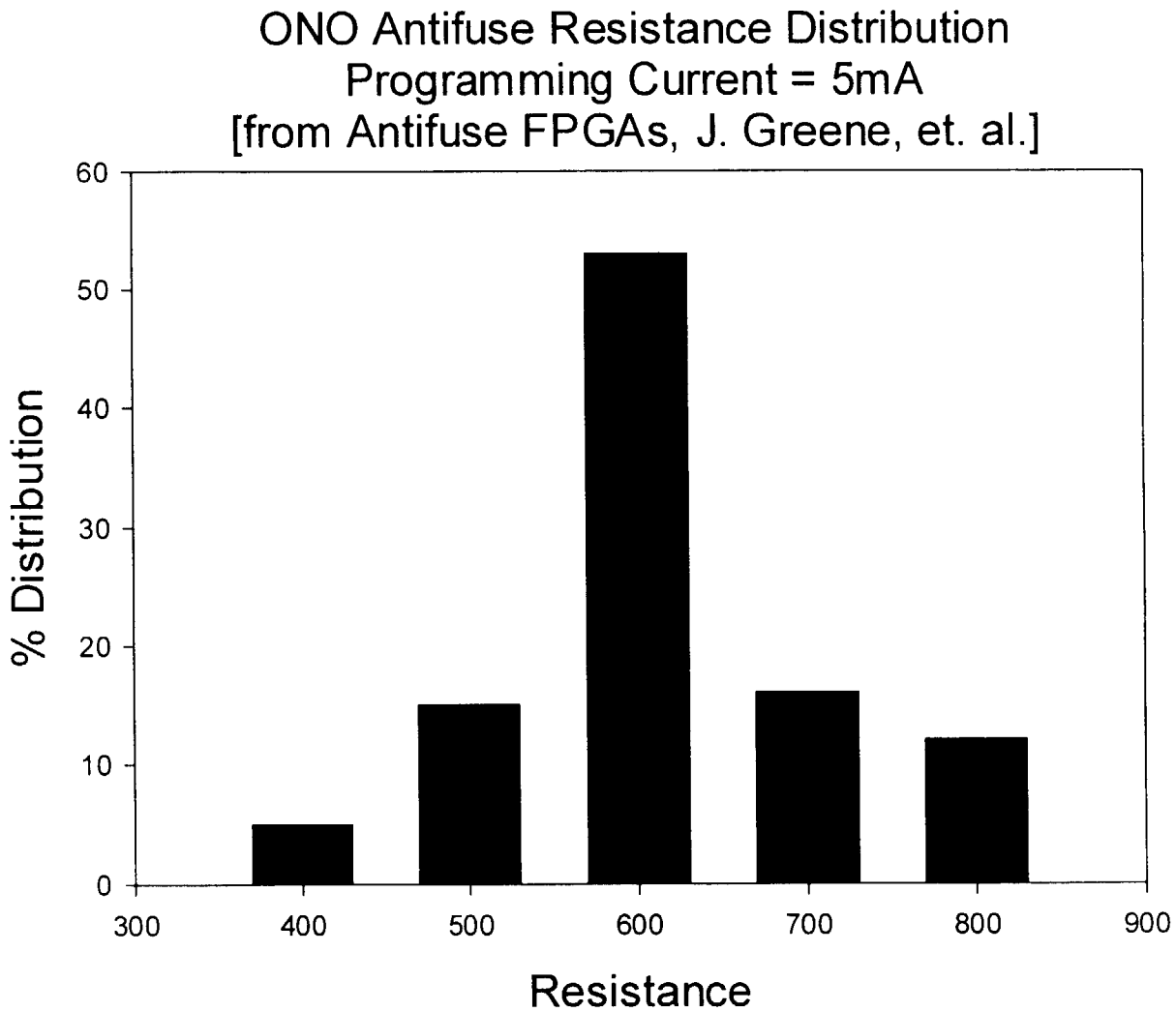
Just setting "MAX" or "MIN" does not account for variations as a result of fabrication differences, anti-fuse resistance, changes as a result of aging, etc, and will be too liberal.

A full MIN/MAX analysis is too conservative since elements near each other on the same die can vary that widely. I.e., one part can't be at 4.5VDC, the other at 5.5VDC.

For each environmental condition, it is fair to hold temperature, voltage, fixed.

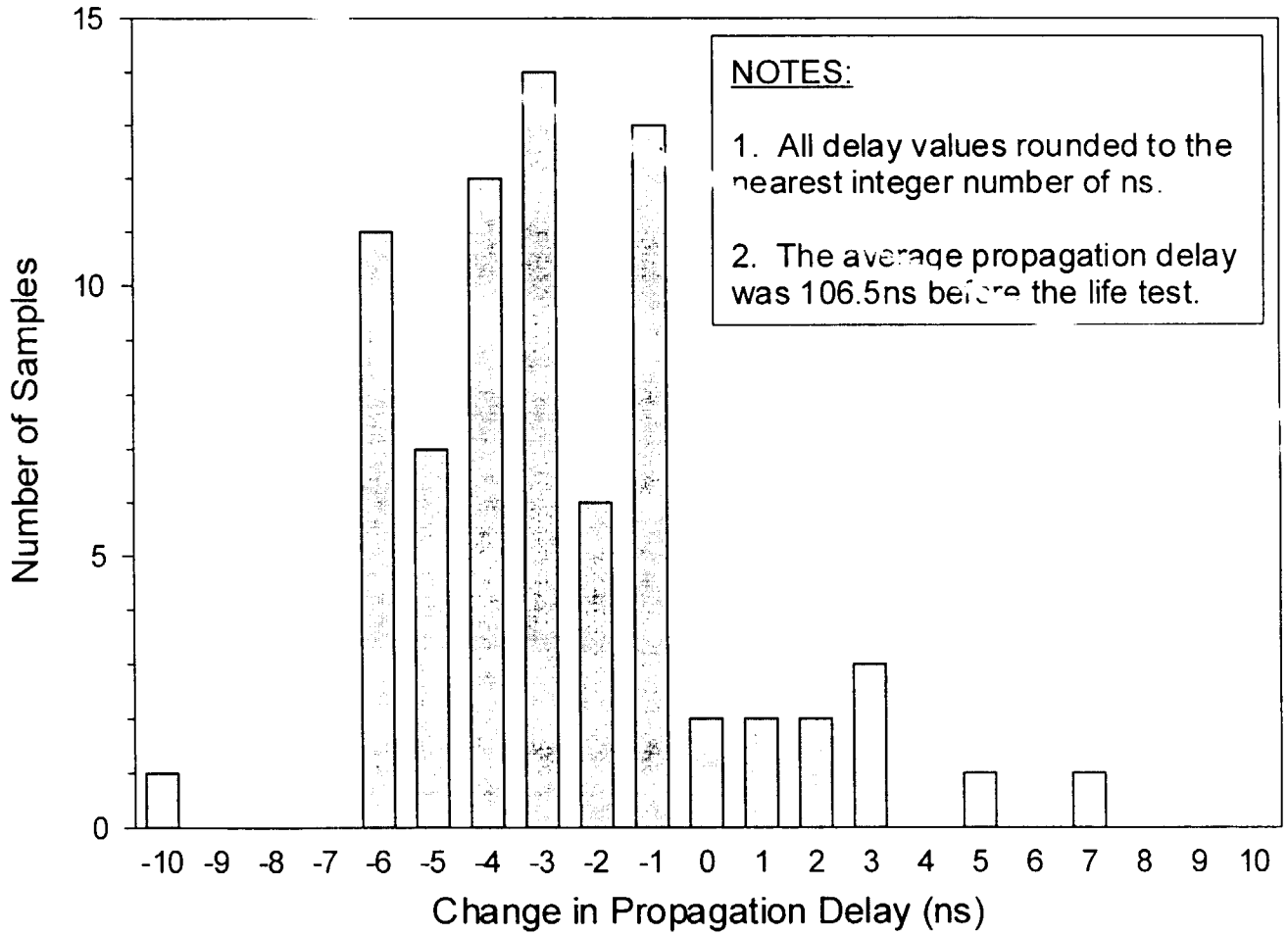
MIN/MAX will still be a bit conservative, since will range over all manufacturing conditions, not limited to variation within a single die.

Antifuse Resistance Variation



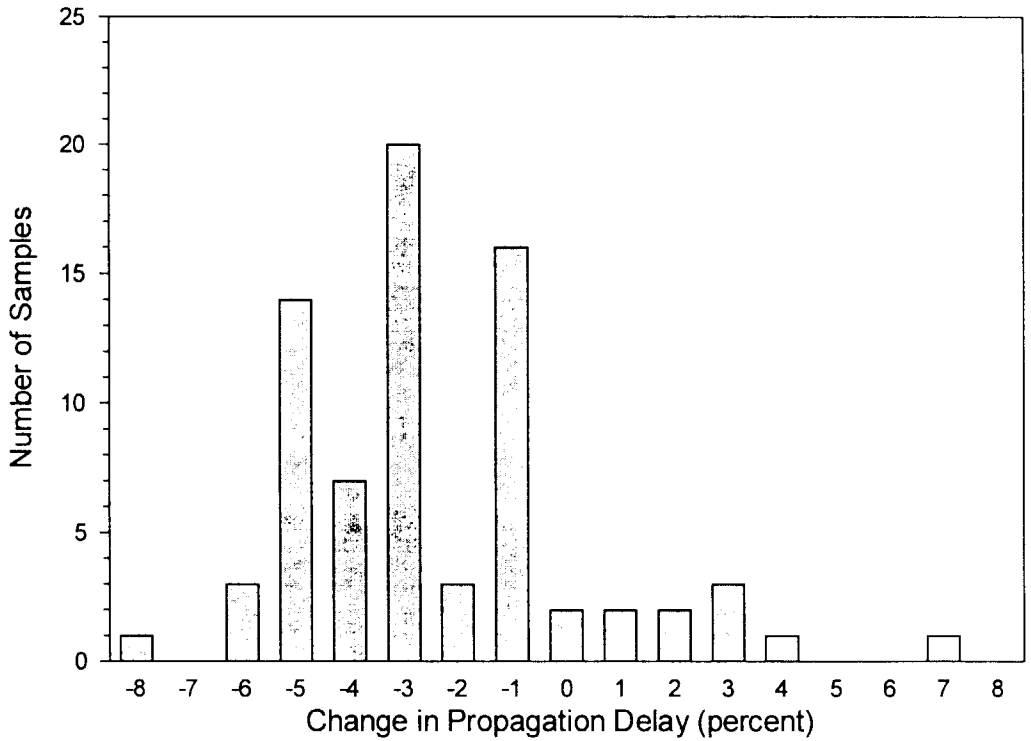
Prop Delay Delta vs. Life

RH1280 Change in Propagation Delay
After 1000 Hour Life Test
Tested at 4.5 Volts, 125C



Prop Delay Delta vs. Life

RH1280 Change in Propagation Delay
After 1000 Hour Life Test
Tested at 4.5 volts, 125C

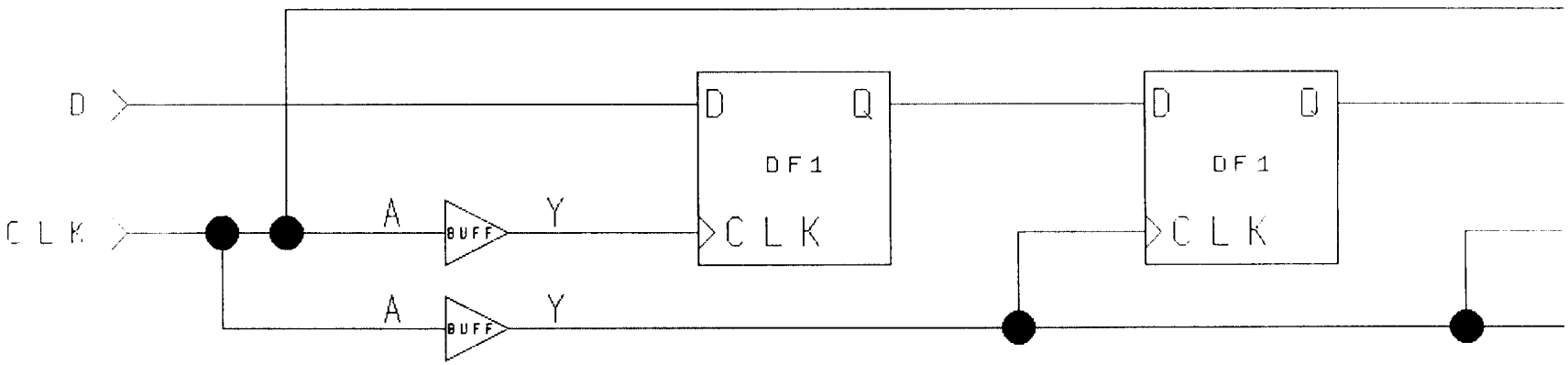


Note: Over a long path, 16 modules + I/O, T_P exceeding 100 ns.

Clock Skew - From VHDL Coding Example

```
Library IEEE;
  Use IEEE.Std_Logic_1164.All;

Entity Skew Is
  Port ( Clk    : In  Std_Logic;
         D      : In  Std_Logic;
         Q      : Out Std_Logic   );
End Skew;

Library IEEE;
  Use IEEE.Std_Logic_1164.All;

Architecture Skew of Skew Is
Signal ShiftReg : Std_Logic_Vector (31 DownTo 0);
Begin
  P: Process ( Clk )
     Begin
       If Rising_Edge (Clk)
         Then Q                       <= ShiftReg(0);
              ShiftReg (30 DownTo 0) <= ShiftReg (31 DownTo 1);
              ShiftReg (31)          <= D;
         End If;
     End Process P;
End Skew;
```

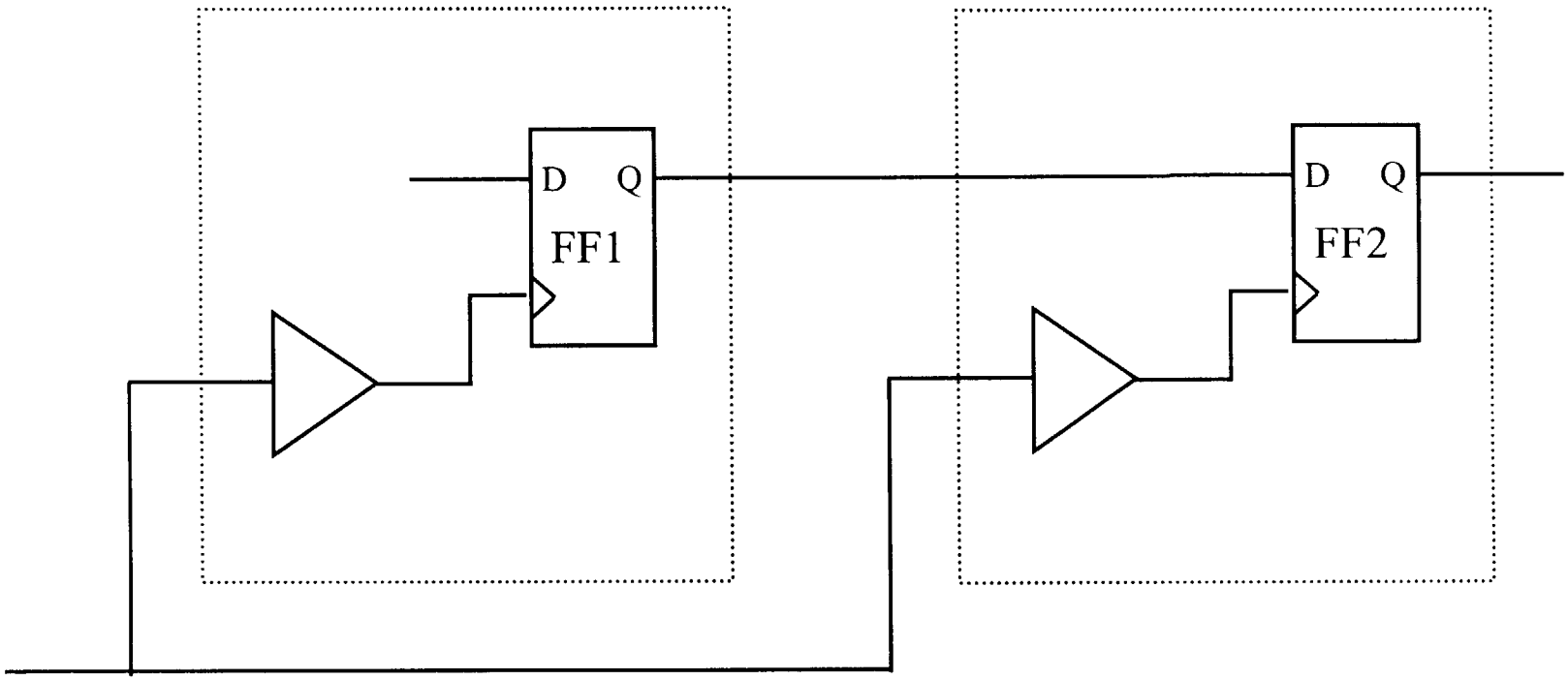
Clock Skew - From VHDL Synthesized Results



Results will depend on coding, directives and attributes, synthesizer, and synthesizer revision.

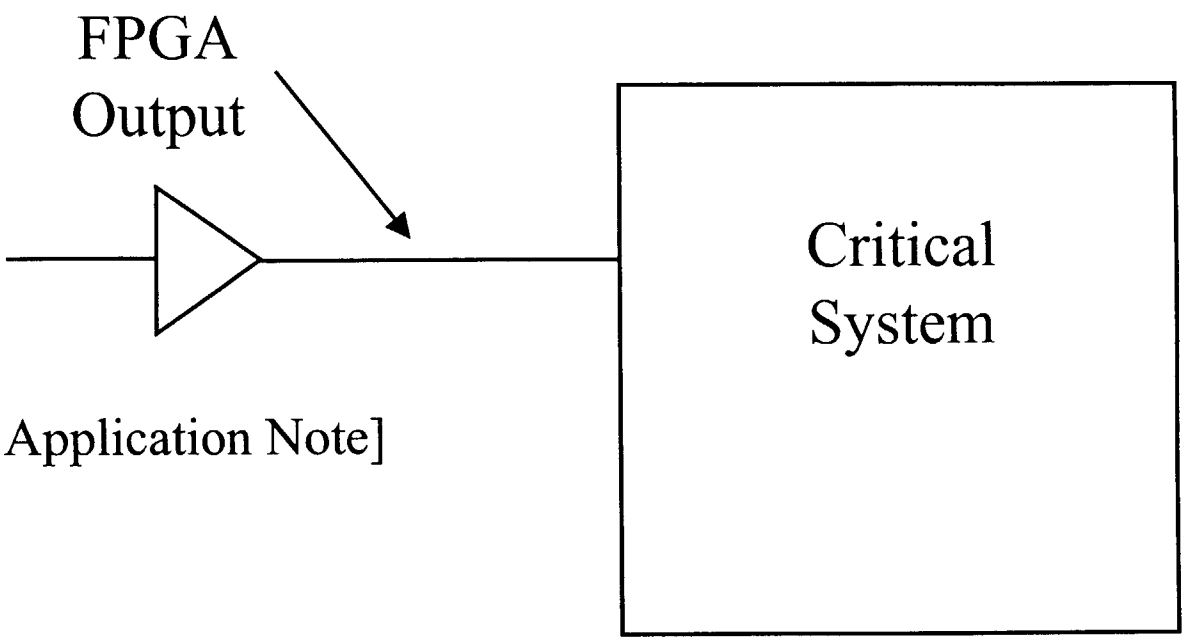
Here we see that the logic synthesizer generated a poor circuit.

Clock Skew - Chip-to-Chip



Analysis may show problems. Some architectures are designed with 0 ns t_H; others incorporate delay elements (configurable) on the data inputs to ensure reliable clocking.

Start up Transient - Outputs

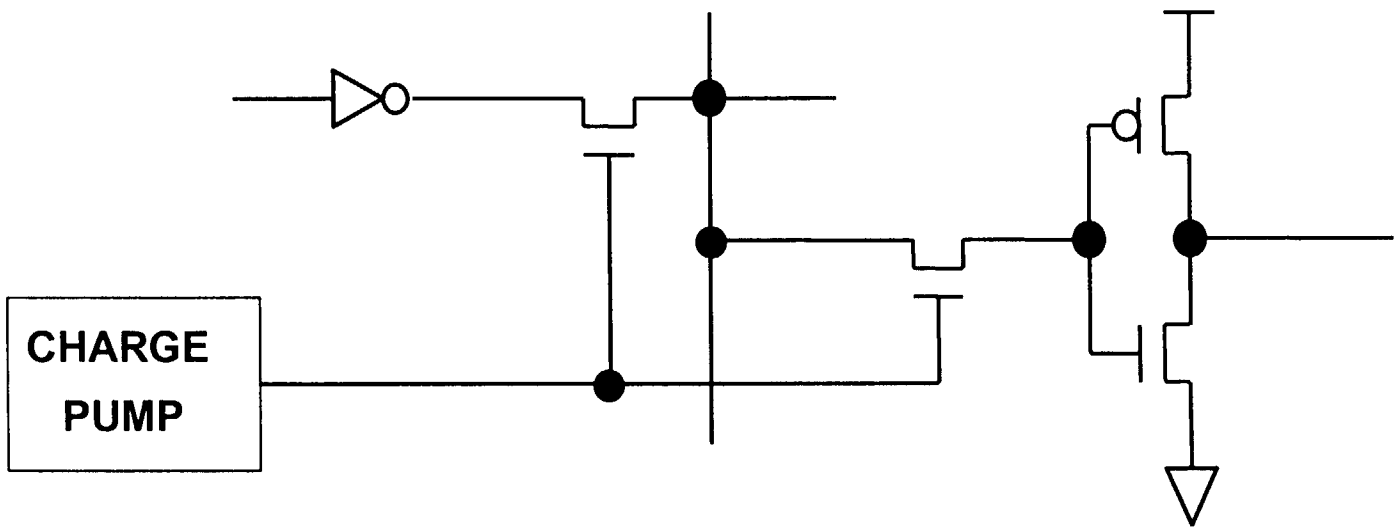


[from Actel Application Note]

Power Up

Actel FPGAs are nonvolatile and therefore require no external configuration circuitry on power up. However, at power up it does take a finite amount of time for the device to become stable and operate normally. For a V_{CC} slew rate of ~30 ns/V, it takes approximately 250 ms for the device to become fully operational. Power up time varies with temperature, where cold is worst case. At power up, the state of all flip-flops is undefined. Some new designs will be power up safe.

Start up Transient
Charge Pump and Isolation

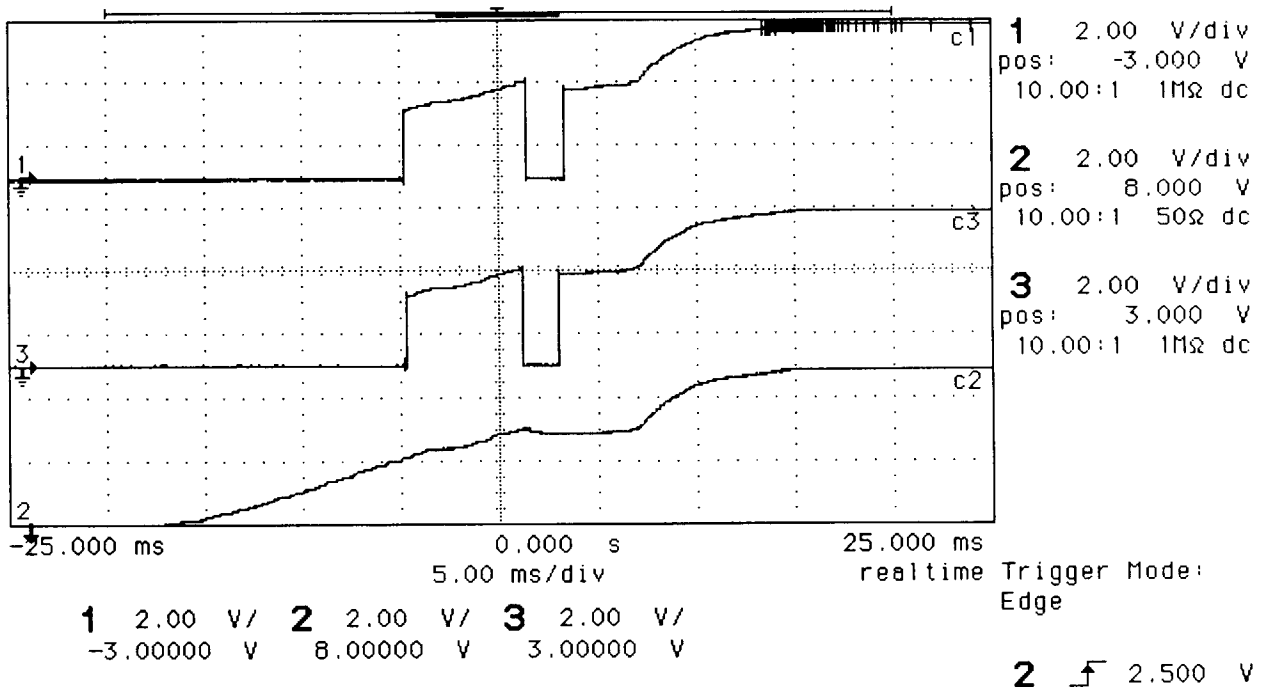


Start up Transient - Outputs

Cover

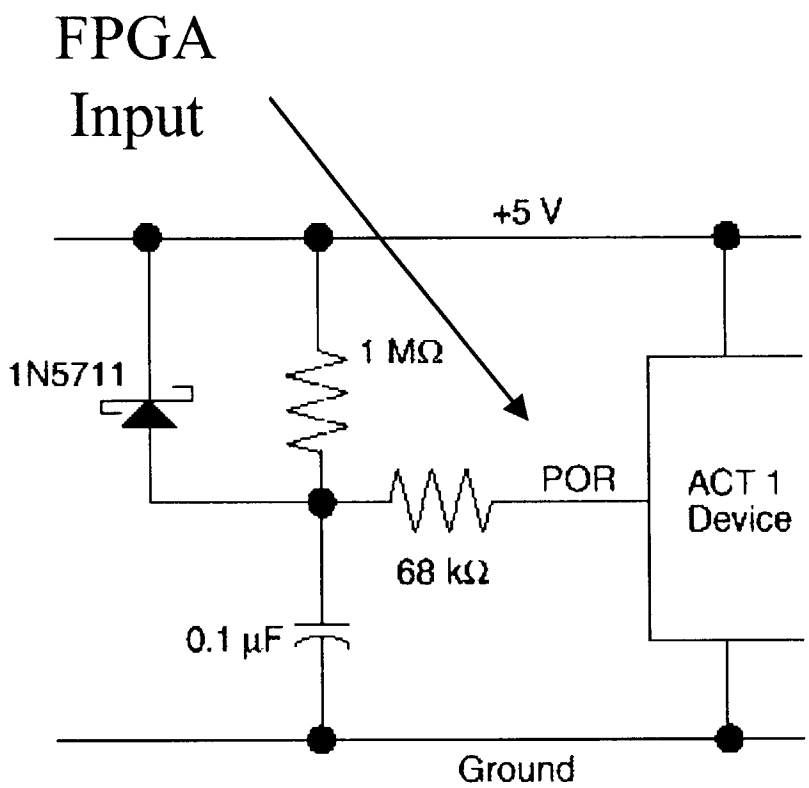
Arm

V_{CC}



5 ms / Division

Start up Transient - Inputs



During the start up time with many FPGA models, an input may source current. In this application, a buffer with Schmidt trigger inputs is recommended.

Metastability - Introduction

- Can occur if the setup, hold time, or clock pulse width of a flip-flop is not met.
- A problem for asynchronous systems or events.
- Can be a problem in synchronous systems.
- Three possible symptoms:
  - Increased CLK -> Q delay.
  - Output a non-logic level
  - Output switching and then returning to its original state.
- Theoretically, the amount of time a device stays in the metastable state may be infinite.
- Many designers are not aware of metastability.

Metastability

- In practical circuits, there is sufficient noise to move the device output of the metastable state and into one of the two legal ones. This time can not be bound. It is statistical.
- Factors that affect a flip-flop's metastable "performance" include the circuit design and the process the device is fabricated on.
- The resolution time is not linear with increased circuit time and the MTBF is an exponential function of the available slack time.

Metastability - Calculation

- $MTBF = e^{K2*t} / (K1 \times F_{CLK} \times F_{DATA})$

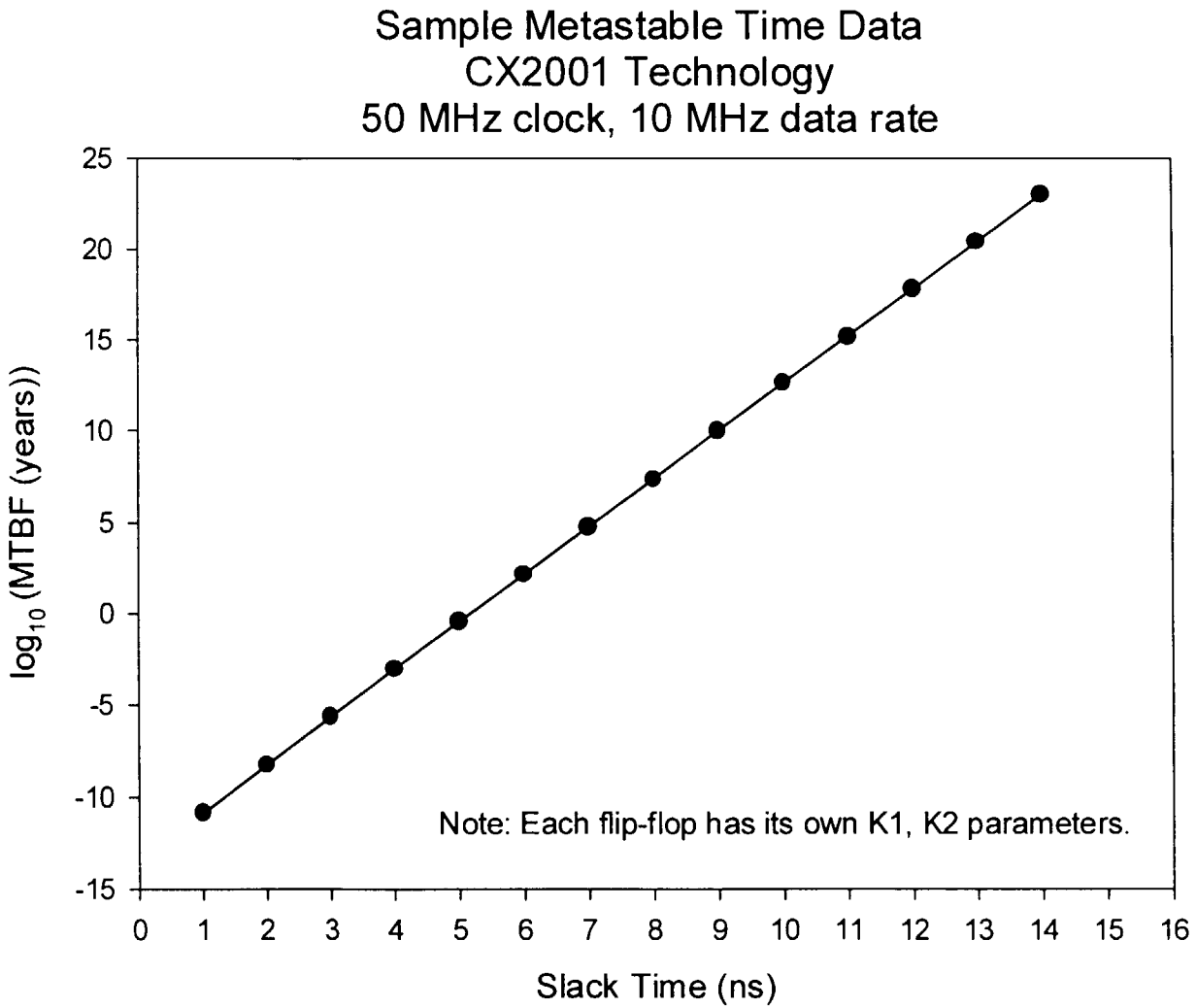
  t is the slack time available for settling

  K1 and K2 are constants that are characteristic of the flip-flop

  Fclock and Fdata are the frequency of the synchronizing clock and asynchronous data.

- Software is available to automate the calculations with built-in tables of parameters.
- Not all manufacturers provide data.

Metastability - Sample Data



Metastability - References

http://rk.gsfc.nasa.gov/richcontent/General_Application_Notes/mestablestates/xilinx_metastable_considerations.pdf
http://rk.gsfc.nasa.gov/richcontent/General_Application_Notes/mestablestates/xilinx_metastable_recovery.pdf
http://rk.gsfc.nasa.gov/richcontent/General_Application_Notes/mestablestates/xilinx_metastable_recovery_2.pdf
http://rk.gsfc.nasa.gov/richcontent/General_Application_Notes/mestablestates/meta_ti.pdf
http://rk.gsfc.nasa.gov/richcontent/General_Application_Notes/mestablestates/cypress_pldmeta.pdf
"Flip-Flops and Metastable States, " CX Technology Design Manual, Chip Express, 1997, pages 9-18 to 9-24.

"Metastable States," The Art of Electronics, Horowitz and Hill, 1989, page 552.

some of the other references that i have to go through and type in. send more if you have some!

http://soliton.physics.arizona.edu/~dls/1.html
Daniel L. Stein Noise-Assisted Escape from a
Metastable State. Robert Maier (Mathematics Department, University of Arizona) and I have developed a program.
--http://soliton.physics.arizona.edu/~dls/1.html

An article from the EDA Today Summary Report Vol.
3, No. 2, February 1997. Figure 8. Click here to go back to the main article, "Xilinx to Ride...
--http://www.edat.com/97pubs/2-97_XilinxHR4.htm

http://www.ti.com/sc/docs/psheets/abstract/apps/sdya006.htm
Digital and Impulse Circuits. Abbreviation: CIO. Credits: 6. Time: 3/2, 1st term, stage 2.
Prerequisites: Logical systems. Contents of Lectures: 1....
--http://www.fee.vutbr.cz/UIVT/courses/CIO/.iso-8859-1

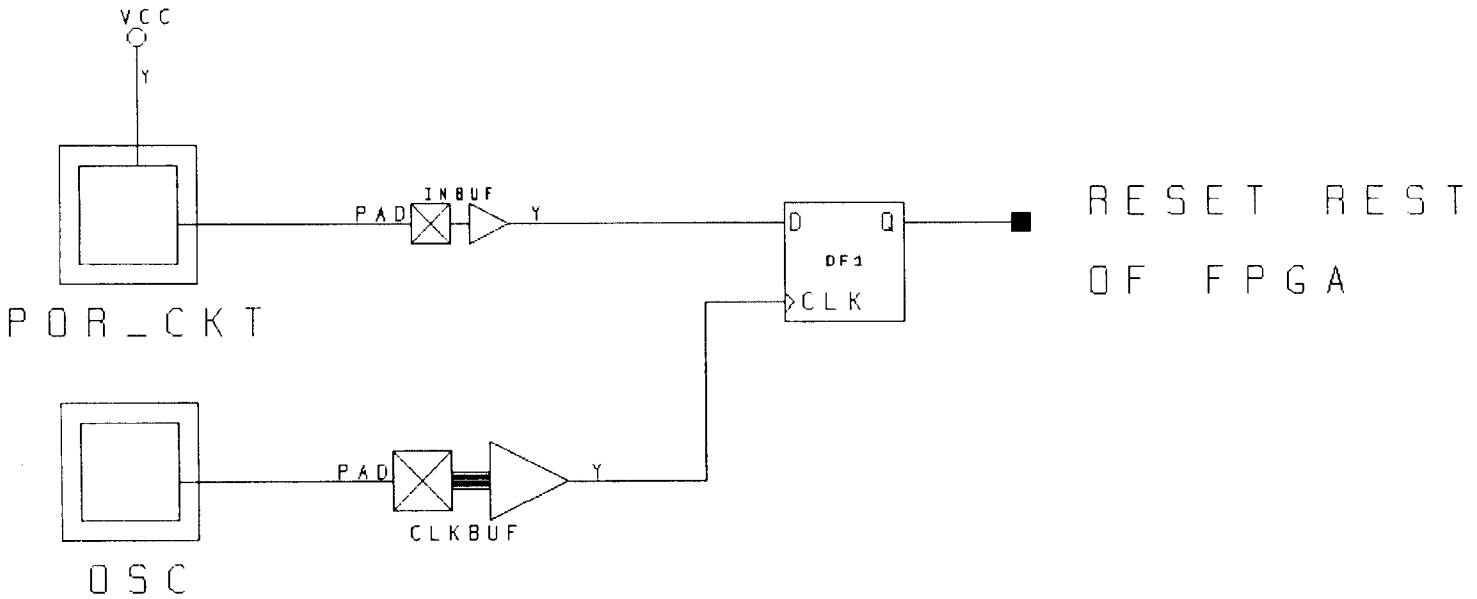
http://www.csu.edu.au/ci/vol2/djjpaper/node2.html
- Next: Chaos in asynchronous parallel digital machines Up: Limits to the Reliability Previous:
Introduction. Sources of uncertainty. One of us (MJU) [1]...
--http://www.csu.edu.au/ci/vol2/djjpaper/node2.html

http://digibowser.ecn.purdue.edu/ee566/Report/section3.html
.0 Design Narrative. The description of the details of this design have been broken down into
the three major sections of the design: the central...
--http://digibowser.ecn.purdue.edu/ee566/Report/section3.html

http://dlib.computer.org/dynaweb/tc/tc1995/@Generic__BookTextView/229808;td=3
IEEE Transactions on Computers 0018-9340/95$04.00 © 1995 IEEE Vol.
44, No. 6. June 1995, pp. 754-768 Manuscript received Sept. 15, 1993; revised June 5,...
--http://dlib.computer.org/dynaweb/tc/tc1995/@Generic__BookTextView/229808;td=3

http://www.nist.gov/srd/webguide/nist23/23guide.htm
Provides critically evaluated data for scientists and engineers
--http://www.nist.gov/srd/webguide/nist23/23guide.htm

Synchronous Reset

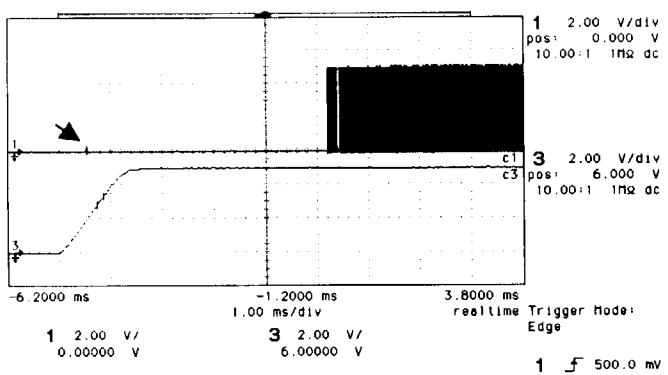


- FPGA may not be functional during power-on transient
- Crystal oscillator start time

Flight Oscillator Start Time Sample

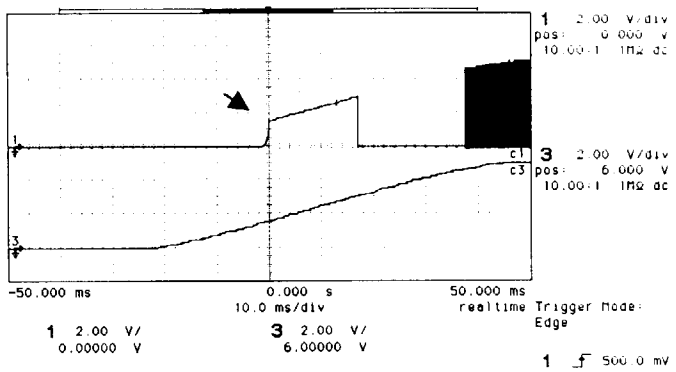
200 kHz

+5V



1 ms/div

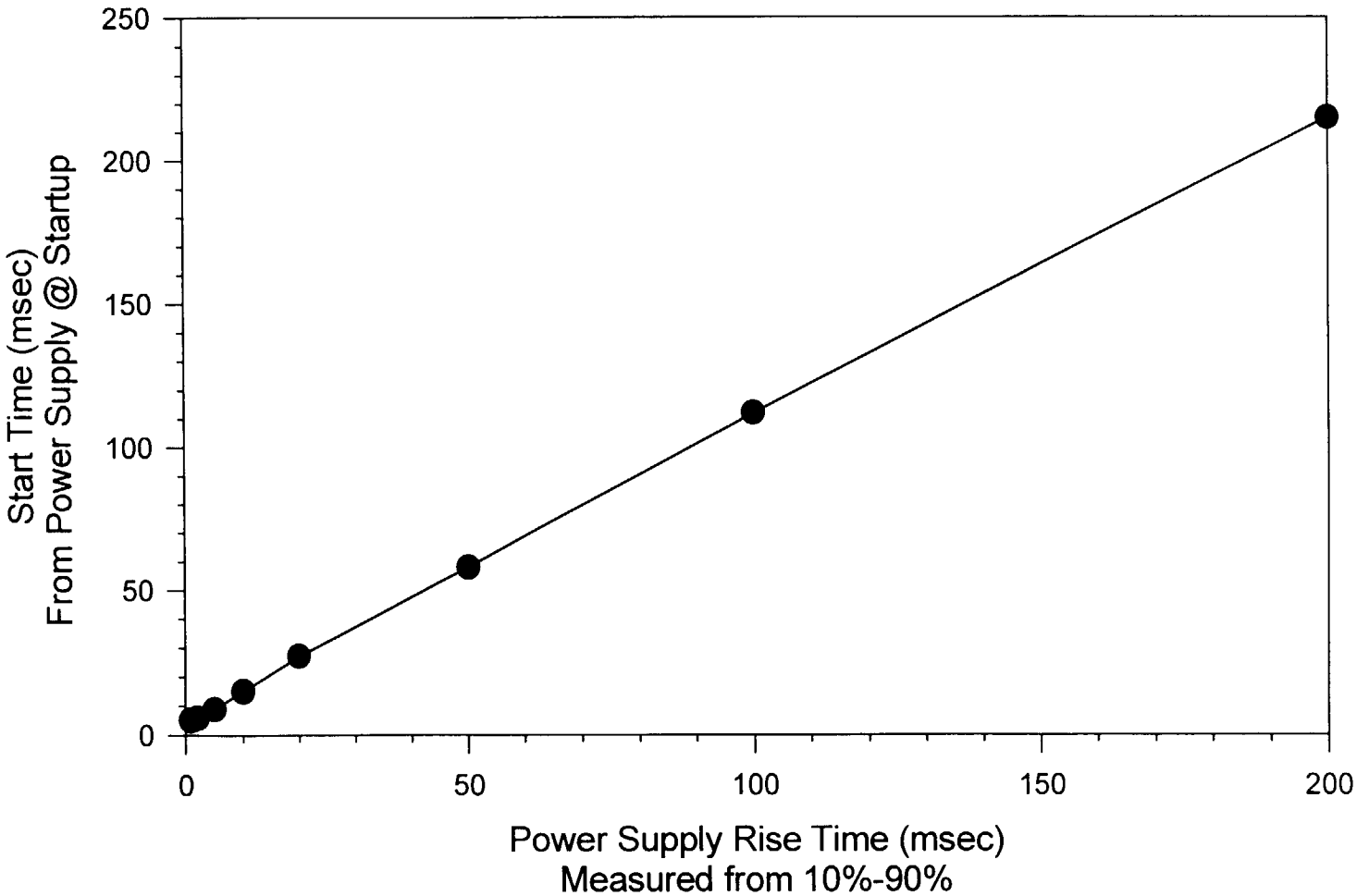
t_{RISE} = 1 ms



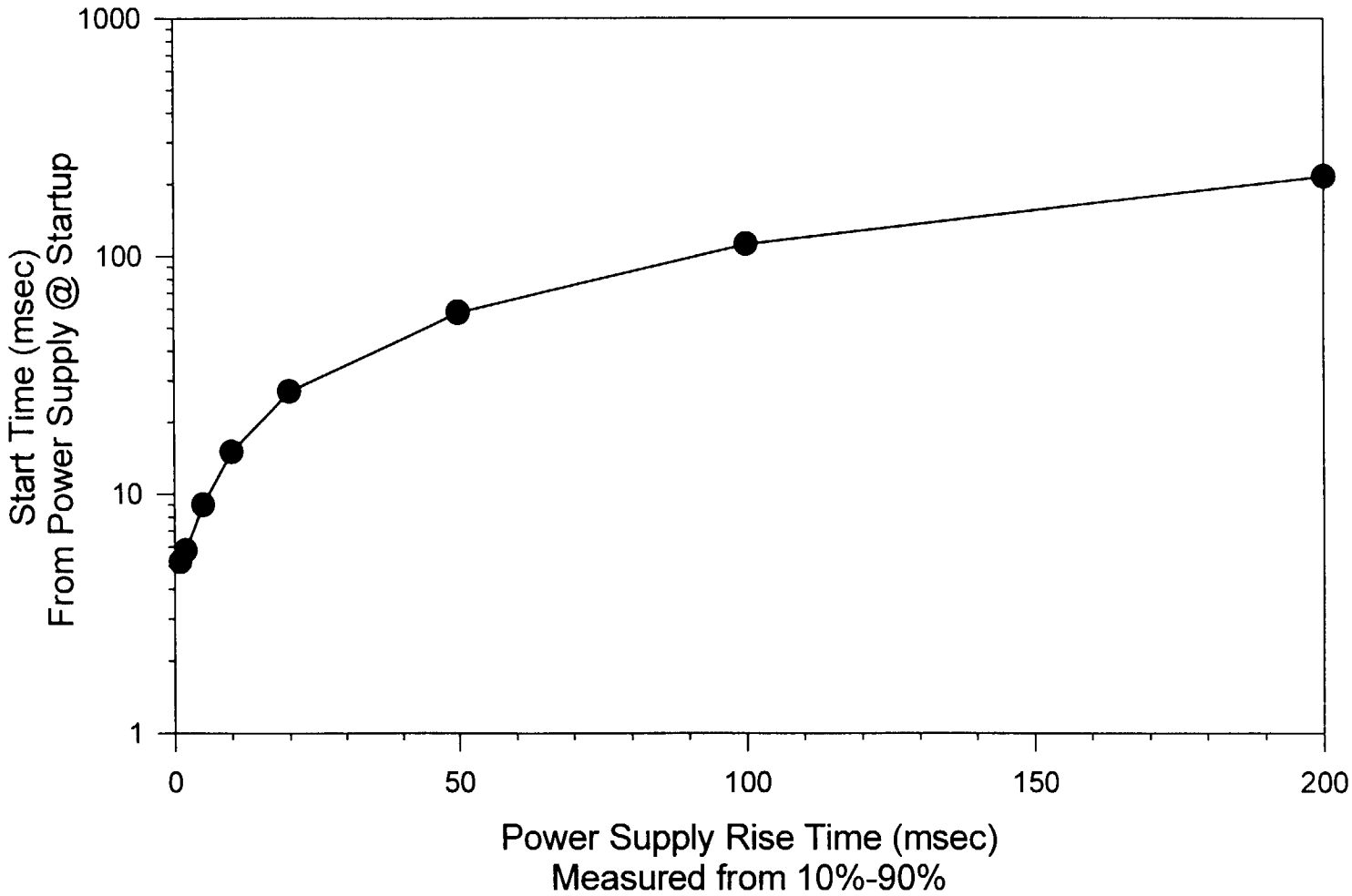
10 ms/div

t_{RISE} = 50 ms

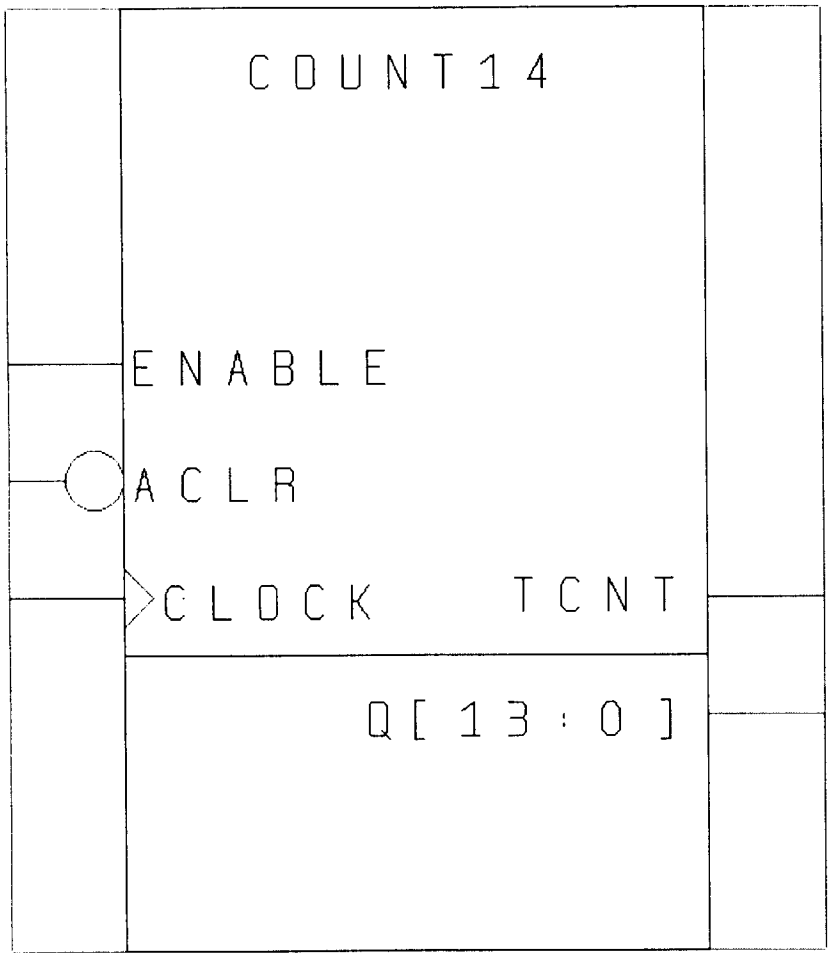
Flight Oscillator Start Time Summary



Flight Oscillator Start Time Summary

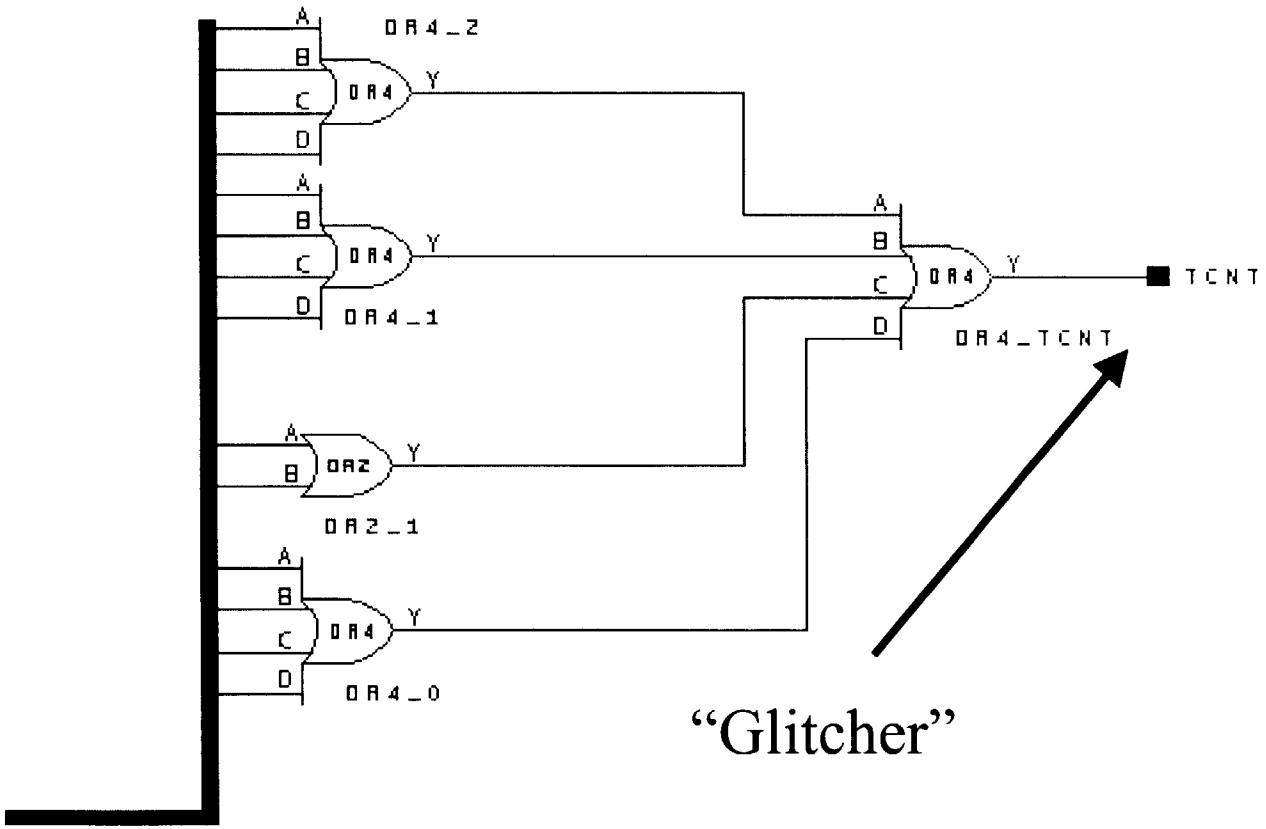


Asynchronous Decoding
High Level

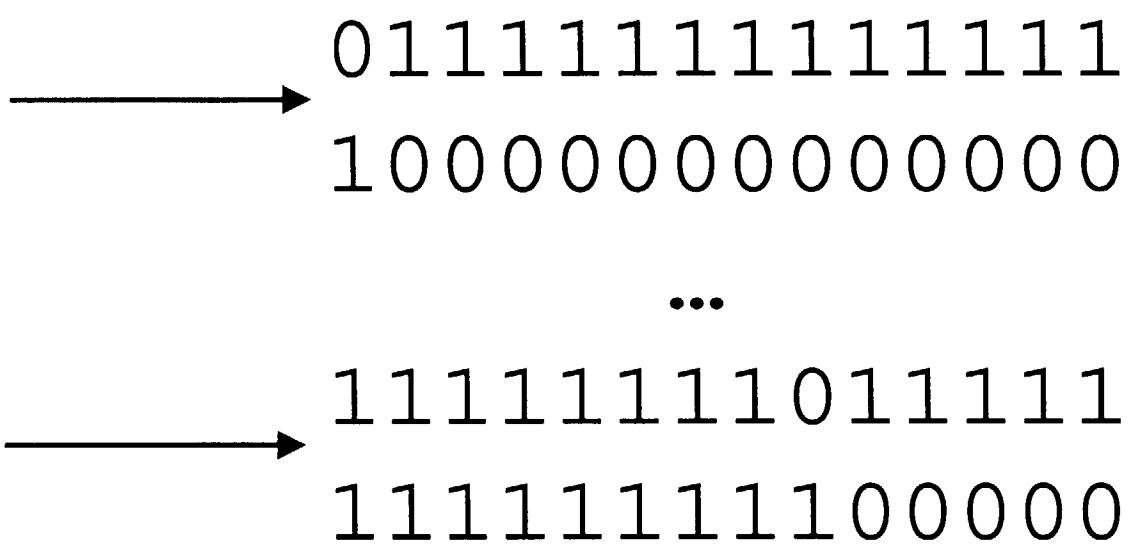


Used as a clock

Asynchronous Decoding Implementation Level

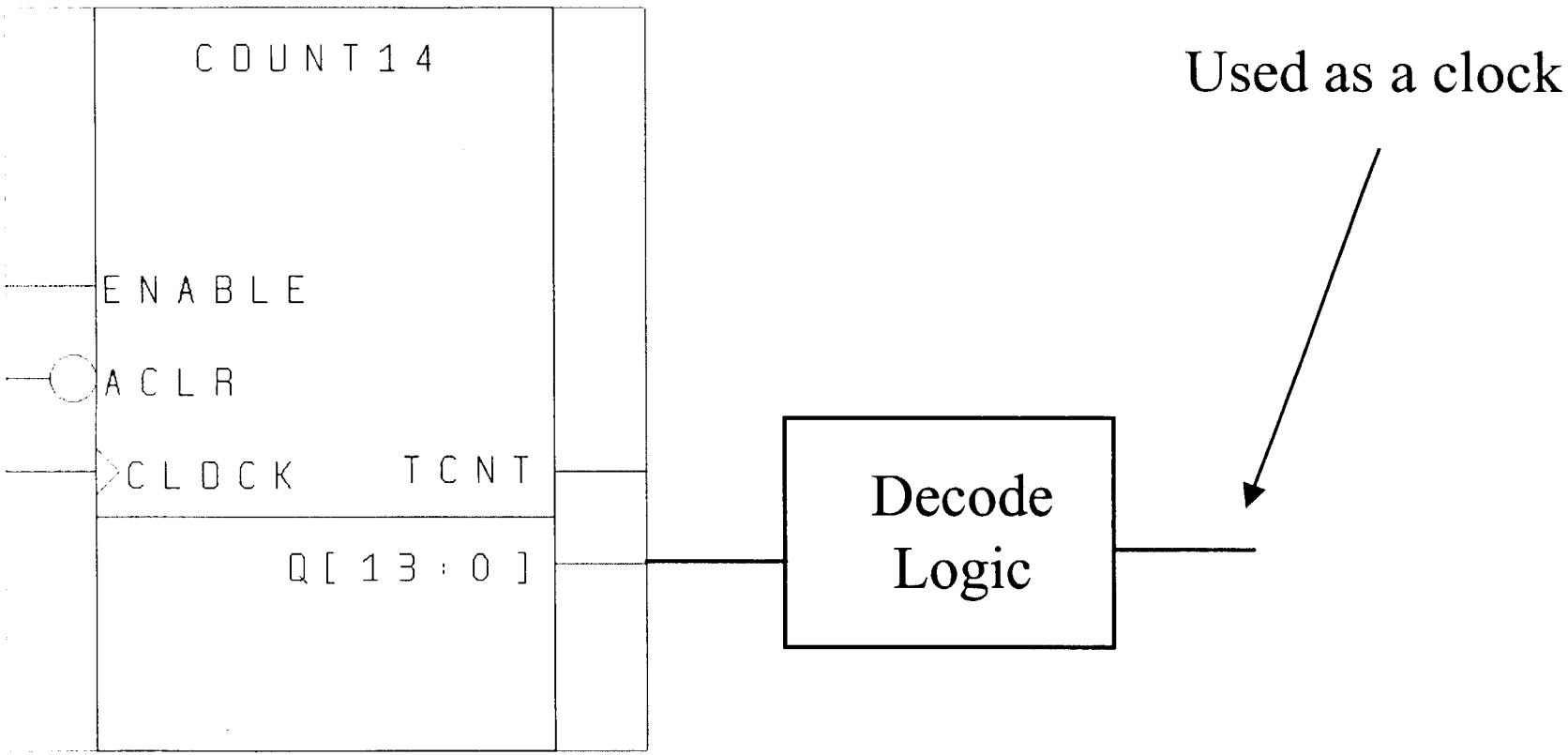


Asynchronous Decoding Glitch Generation

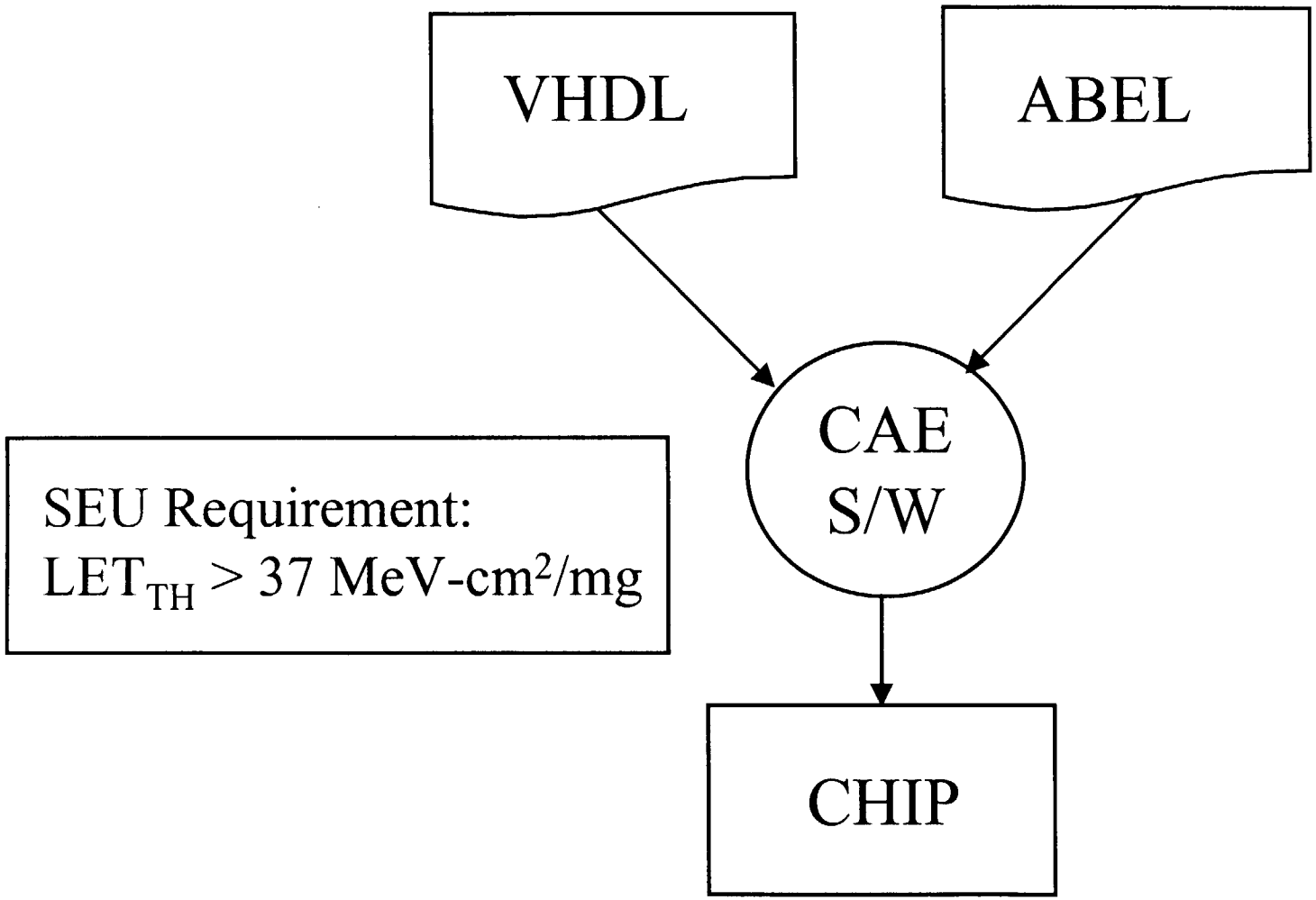


Because of unequal propagation delays, the sequence can momentarily go through state 1111111111111 generating a glitch.

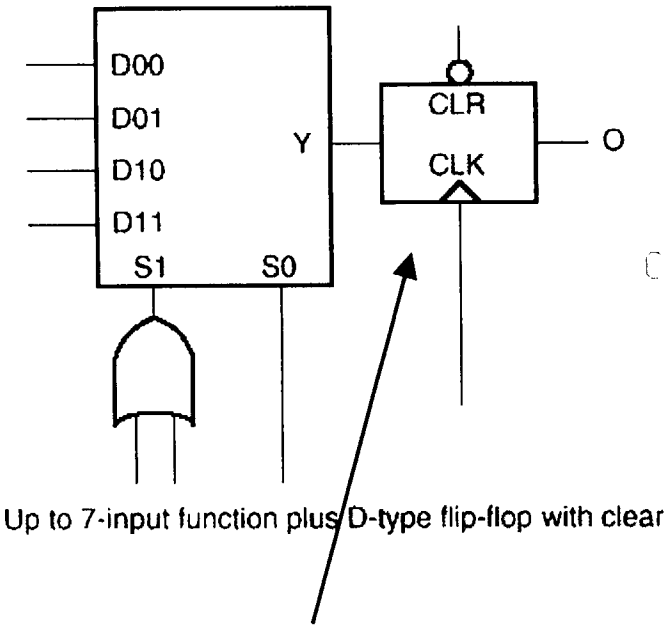
Asynchronous Decoding
High Level



An HDL Flow

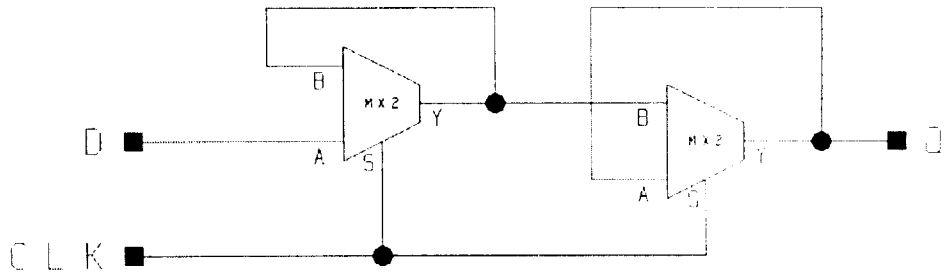


Act 2 Flip-flop Implementation



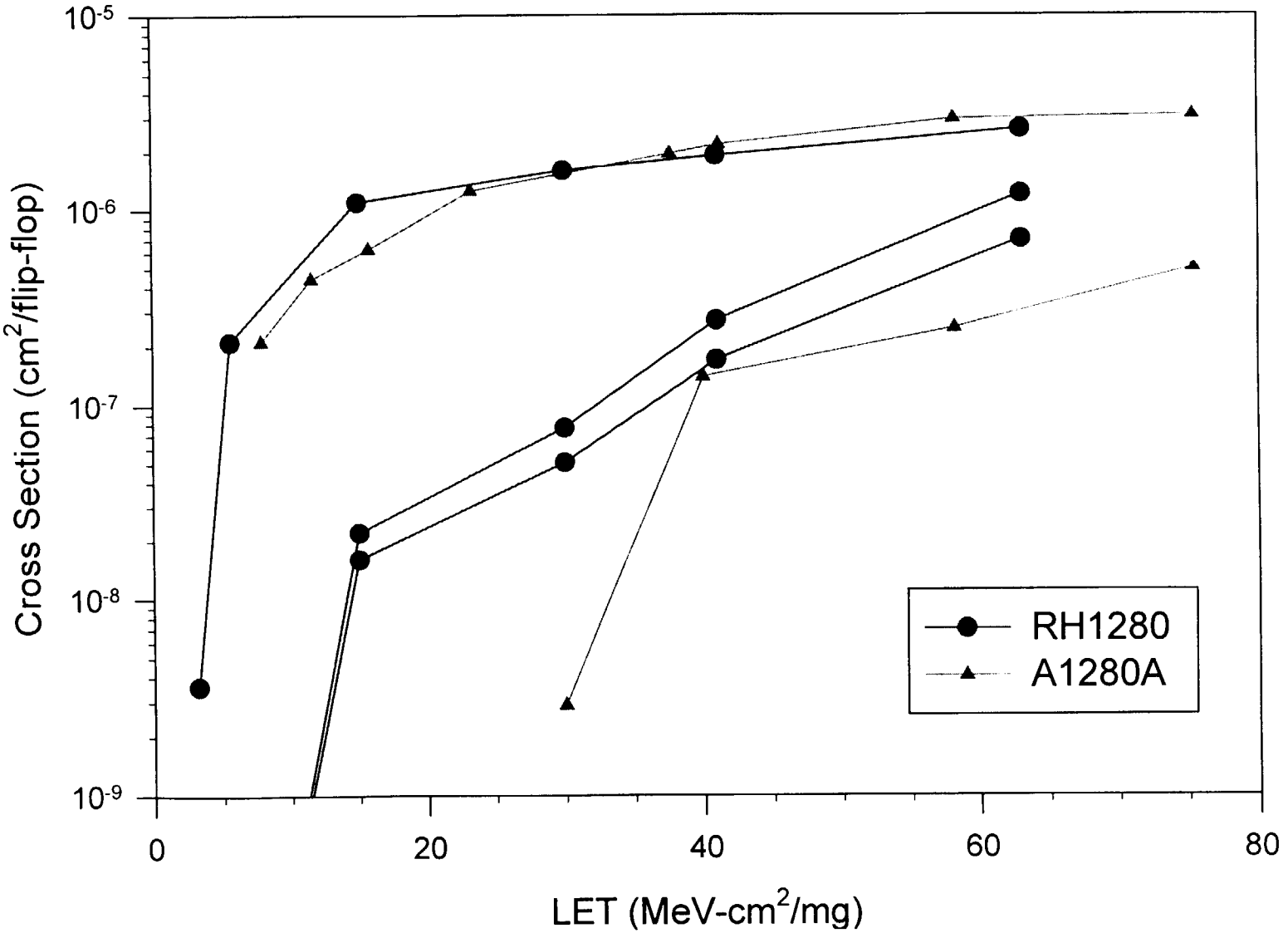
Up to 7-input function plus D-type flip-flop with clear

Hard-wired Flip-flop

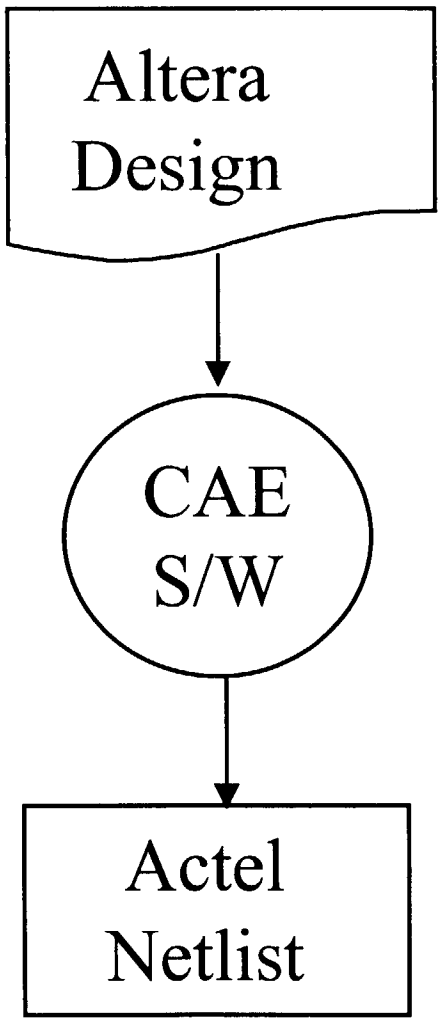


Routed Flip-flop
Feedback goes through antifuses (R) and routing segments (C)

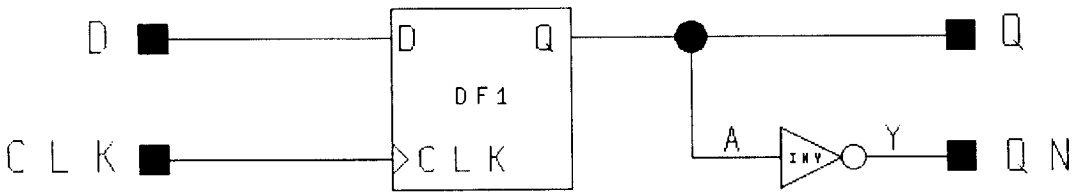
Act 2 SEU Flip-Flop Data



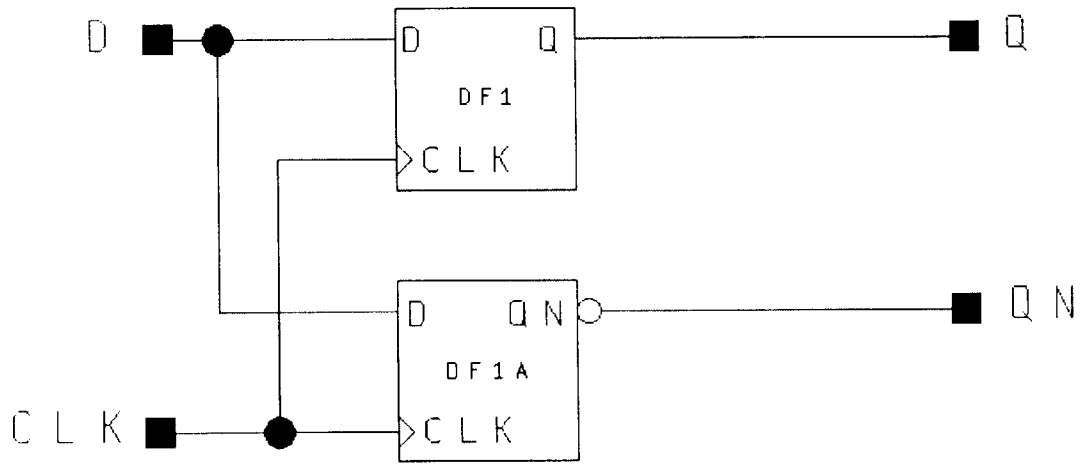
Logic Translation/Optimization Flow



Logic Translation/Optimization Implementation

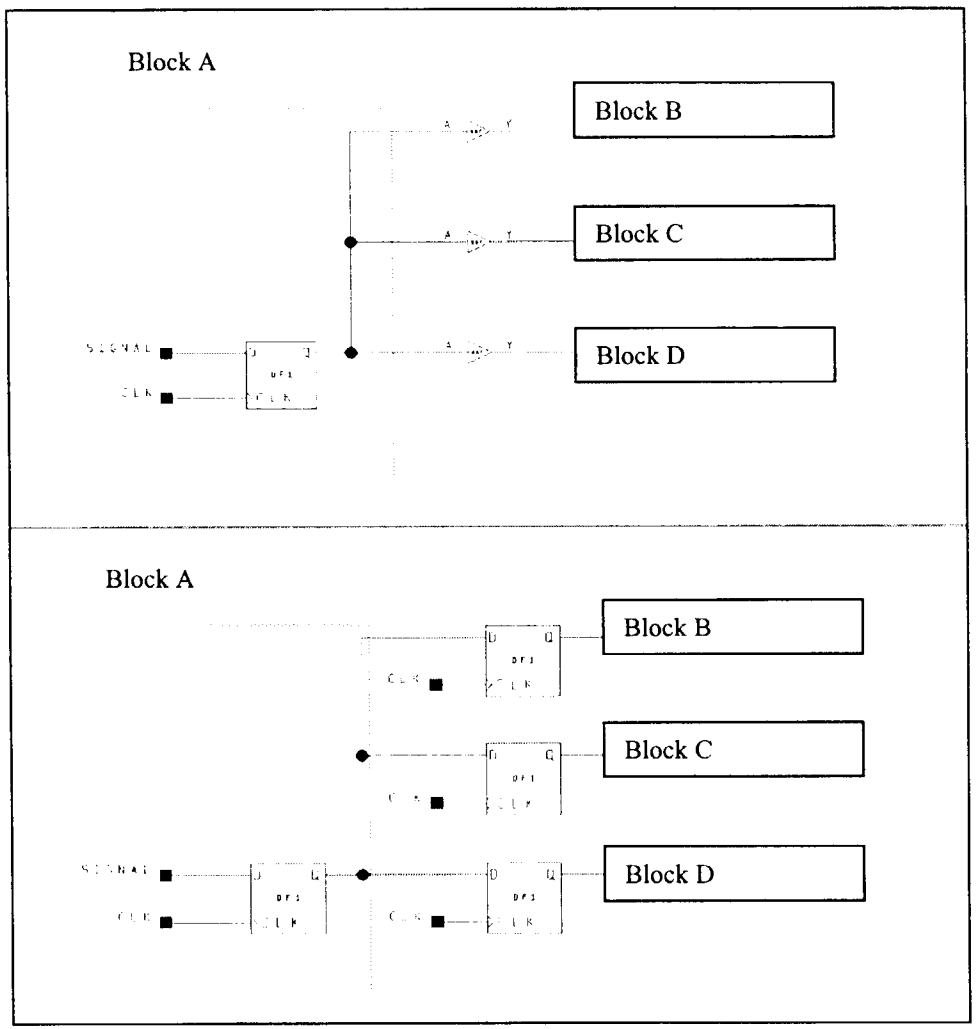


Original

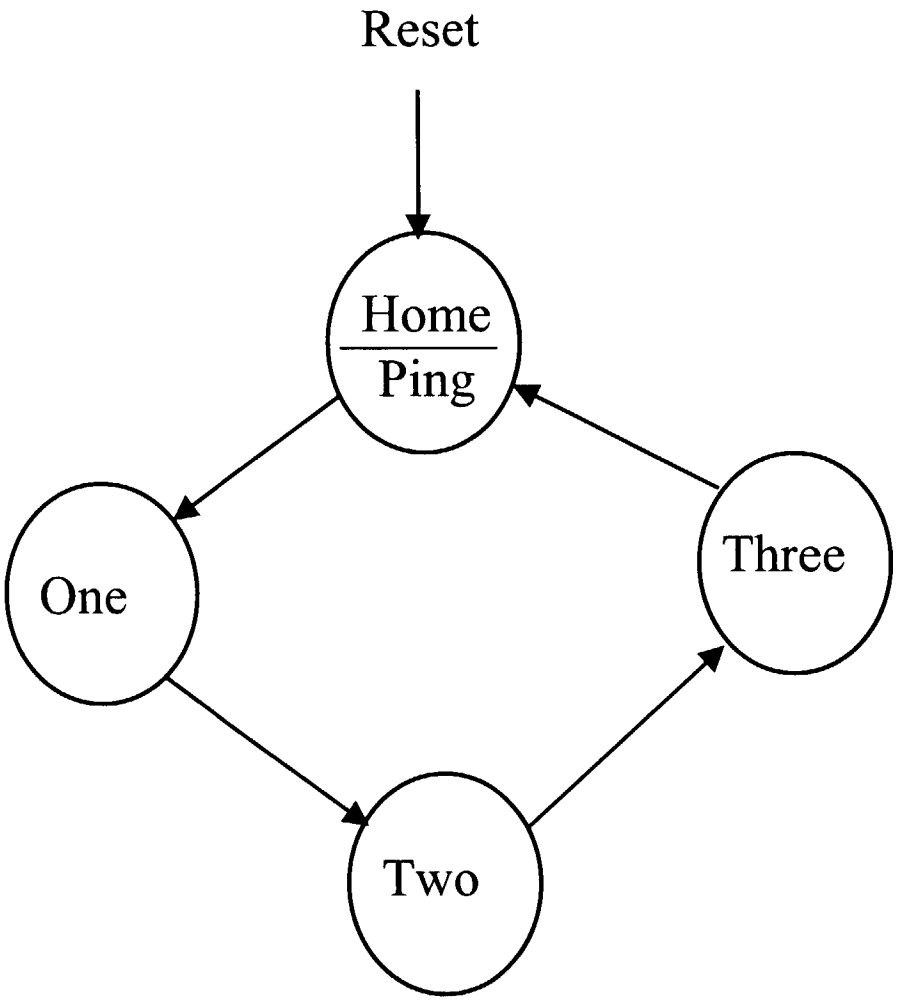


"Optimized"

Logic Replication



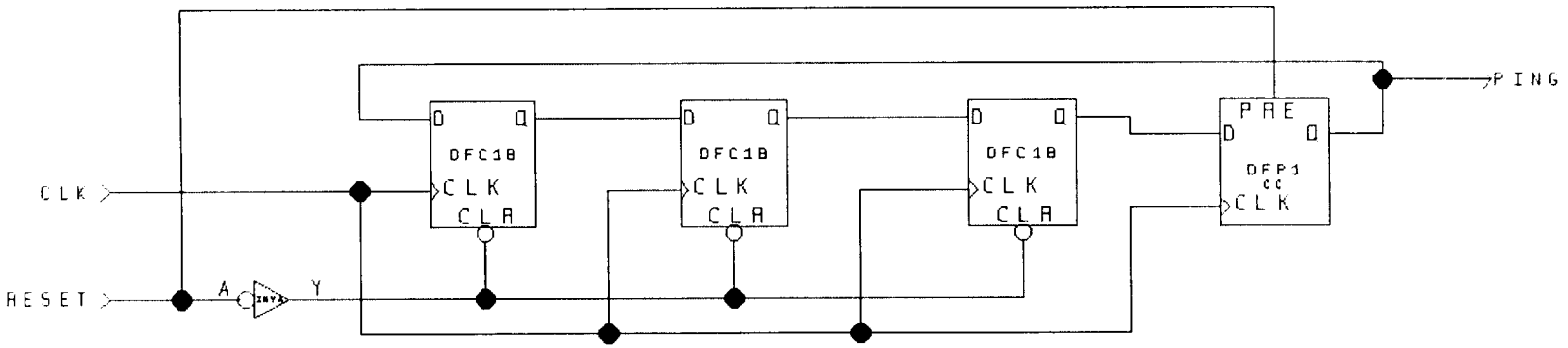
Lockup States



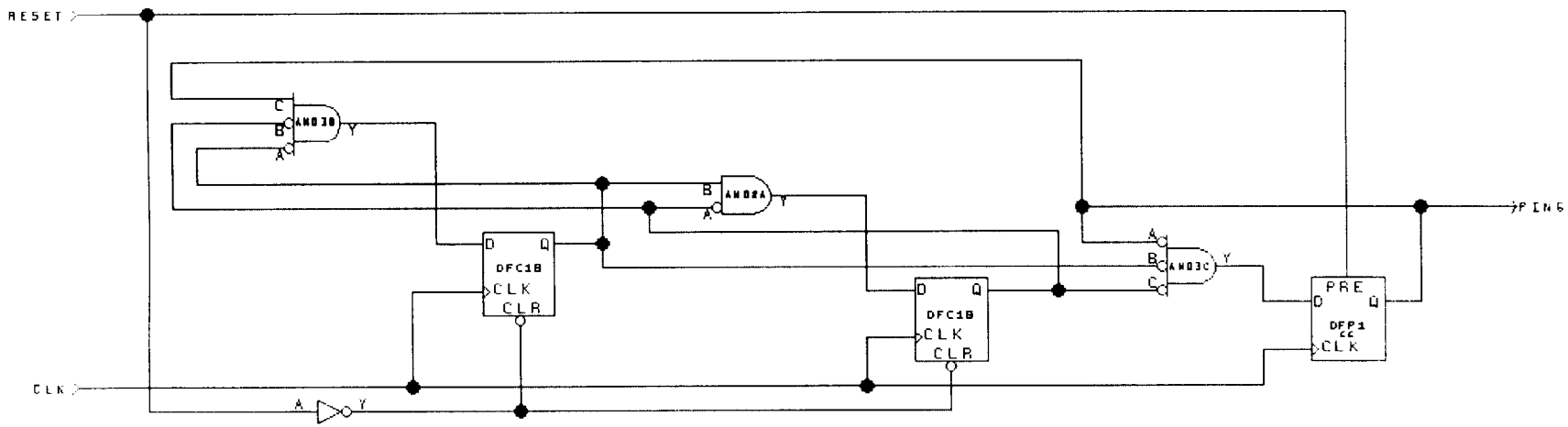
Lockup States - Coding

```
Library IEEE;  Use IEEE.Std_Logic_1164.All;
Entity Onehot_Simple_Act Is
  Port ( Clk    : In  Std_Logic;
         Reset  : In  Std_Logic;
         Ping   : Out Std_Logic   );
End Onehot_Simple_Act;

Library IEEE;  Use IEEE.Std_Logic_1164.All;
Architecture Onehot_Simple_Act of Onehot_Simple_Act Is
Type      StateType Is ( Home, One, Two, Three );
Signal    State     :  Statetype;

Begin
  M: Process ( Clk, Reset )
     Begin
       If ( Reset = '1' )
         Then State <= Home;
         Else If Rising_Edge (Clk)
                Then Case State Is
                       When Home  => State <= One;
                       When One   => State <= Two;
                       When Two   => State <= Three;
                       When Three => State <= Home;
                       End Case;
                End If;
         End If;
     End Process M;
  O: Process (State)
     Begin
       If (State = Home)
         Then Ping <= '1';
         Else Ping <= '0';
         End If;
     End Process O;
End Onehot_Simple_Act;
```

Lockup States
A One-Hot Implementation

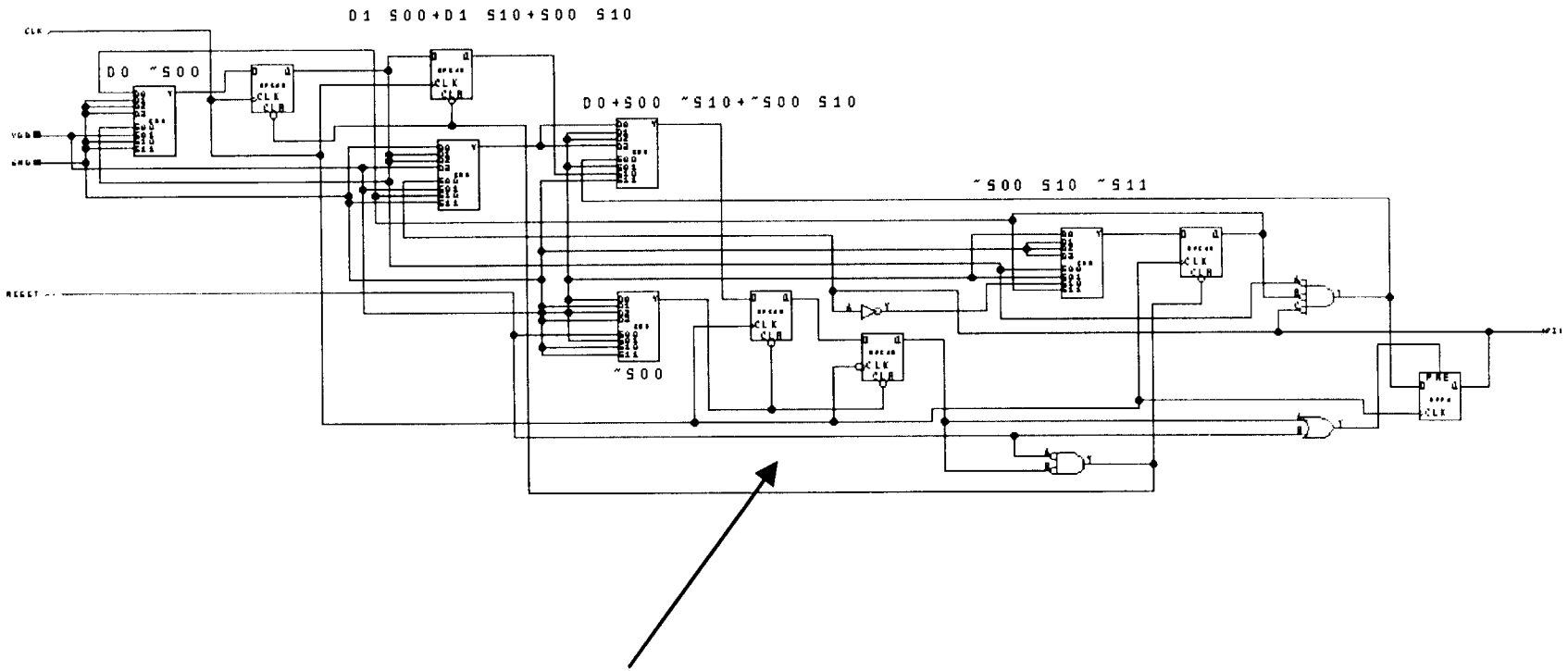


Lockup States
Another One-Hot
Implementation



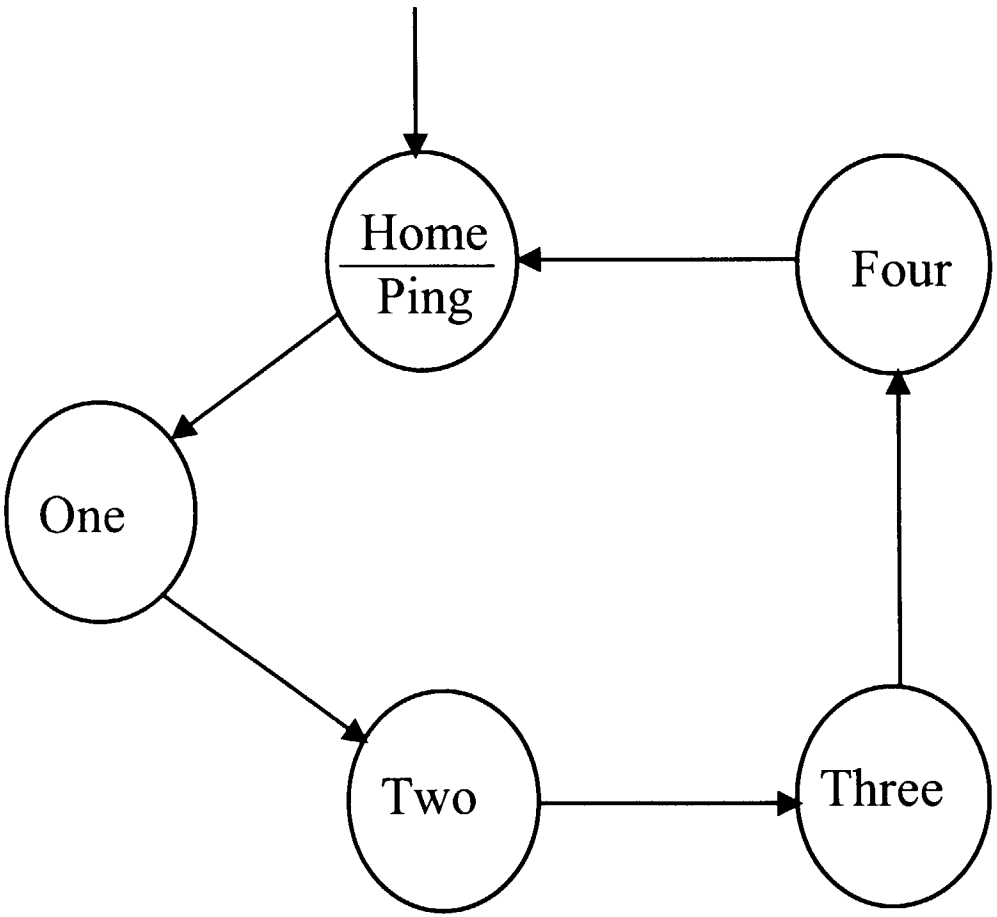
Note: Results depend on version of synthesis software.

Lockup States
A "Safe" One-Hot Implementation



Reset flip-flops. Note second one is on falling edge of the clock. This implementation uses 6 flip-flops.

Lockup States - Binary Encoding



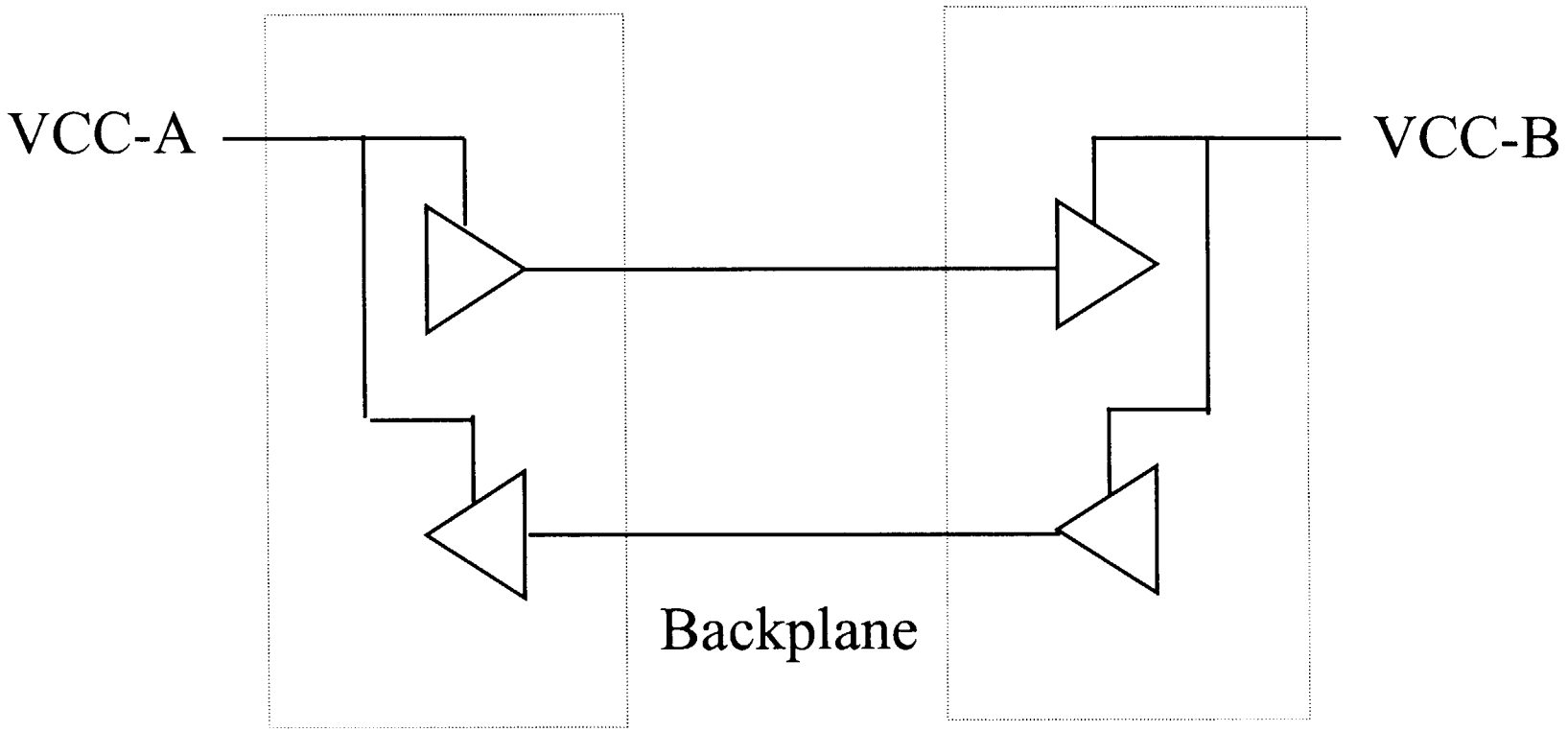
Three unused states.

Lockup States - Binary Encoding

```
Type     StateType Is ( Home, One, Two, Three , Four);
Signal   State      :  Statetype;

            …

Case State Is

            …

        When Others => State <= Home;
```

"When Others" refers to states in the enumeration, not the physical implementation. Also, states that are not reachable can be deleted, depending on the software and settings.

Interfacing - Blocks

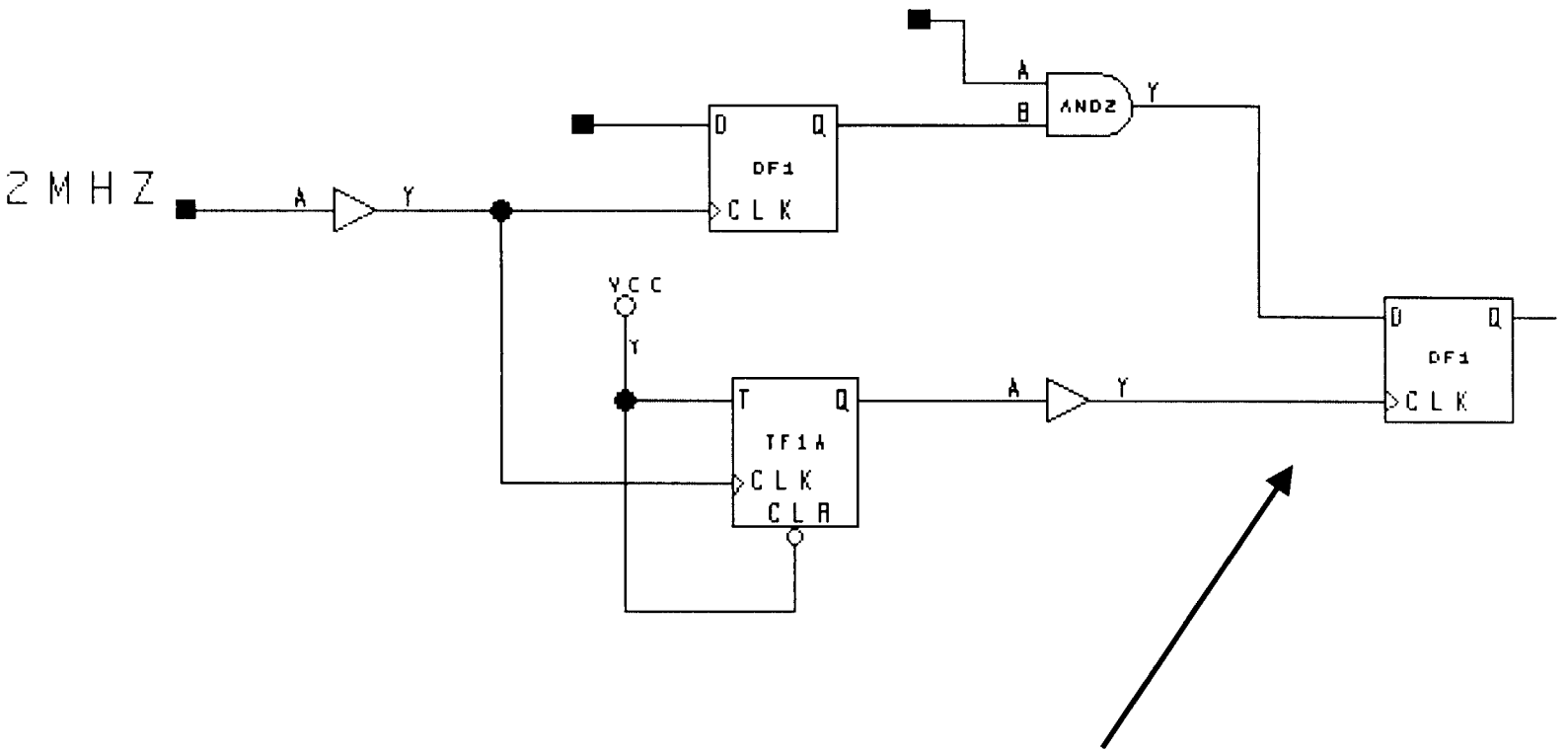


ESD and parasitic diodes (not shown here) to the power bus (present in most CMOS devices) form a sneak path.

Interfacing - Voltage Margin

- TTL → CMOS
  - Problem with discrete circuits (still seen)
  - Normally not a problem with 5V FPGAs
  - Issue with new FPGAs
    - 0.35 μm may only pull up to 3.3 VDC
    - 0.25 μm may only pull up to 2.5 VDC
    - Can be issue with parts having a $V_{IH} = 70\% V_{DD}$
    - Ringing can cause false triggering
- $V_{IL} = 0.8V$ and fast devices are sensitive to ringing on a backplane.

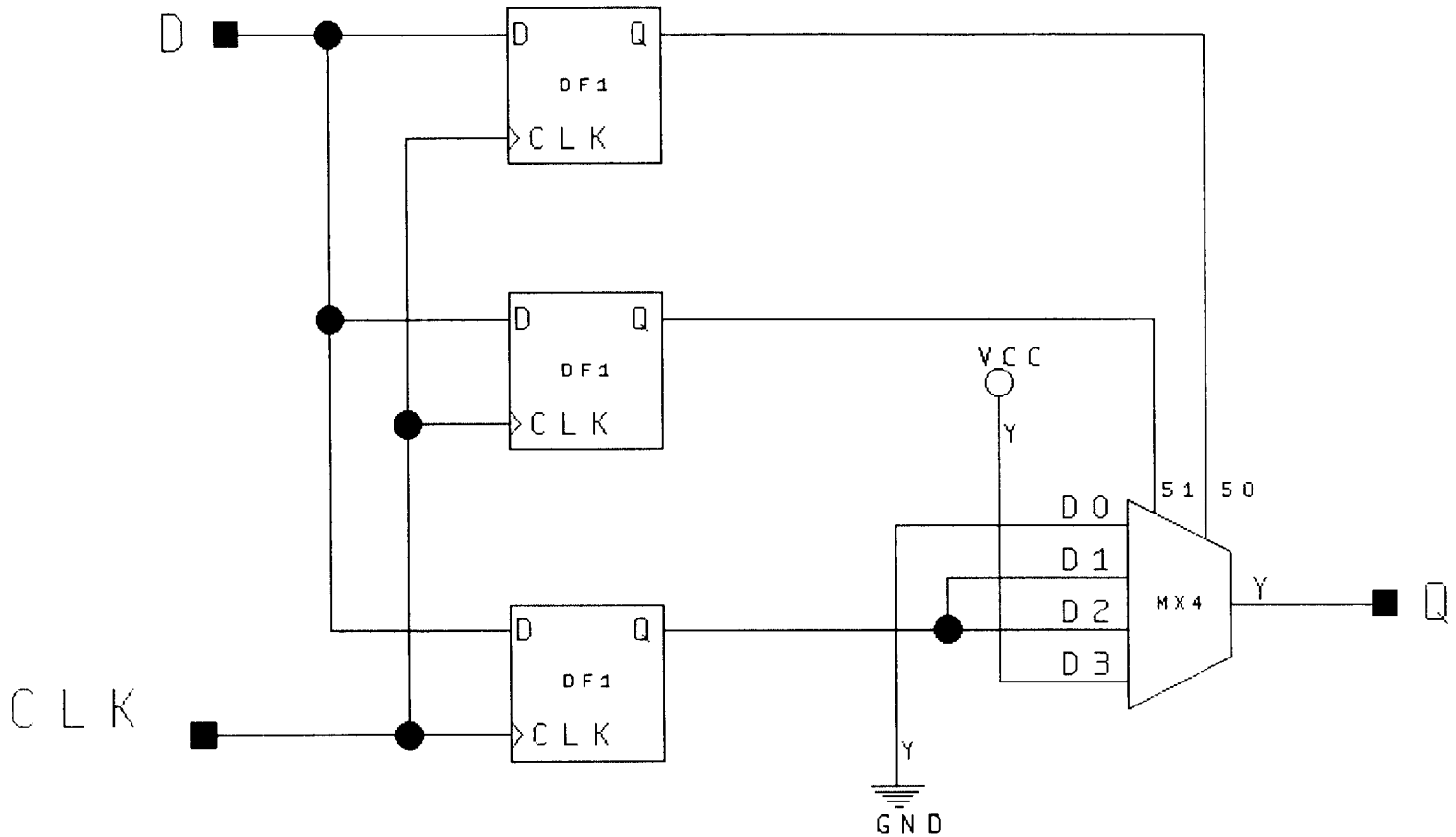
Multiple "Synchronous" Clocks



Verification

- Macro generators fail
  - Expect them to be correct by construction
  - Working macro fails in later revisions
    - ex., modulo counter
- VHDL Synthesis
  - Simulated vs. Synthesized Results
    - Latch vs. Flip-flops.
- Some designers do no simulations or timing analysis.

TMR/Voter Structures



With no active clock, it's an SEU integrator.

Reliance on Logic Simulators General Principles

- Run Time Limited
- Number of Vectors
- Vector Generation
- Number of Operating Modes
- Time for Modeling External Circuitry
- CAE S/W Limitations

Reliance on Logic Simulators Case Study 1

- Simulator Could Only Simulate 1 ms.
  - Instrument Had a 125 ms Cycle Time.
- Simulating All Inputs Not Practical
  - Too Many Combinations

→Failed to Find a Logic Error Which Caused an Arithmetic Error

Reliance on Logic Simulators Case Study 2

- FPGA Converted to ASIC
- No Gate Level Design Review Performed at Any Stage
- Test Vectors from FPGA Version Were Not Run on the ASIC Version
- Test Vectors Were Capable of Detecting the Design Error

Specifications
General Principles

- No Specification Produced
- Specification not Followed

- Common Error - Seen More Often Than One Would Expect

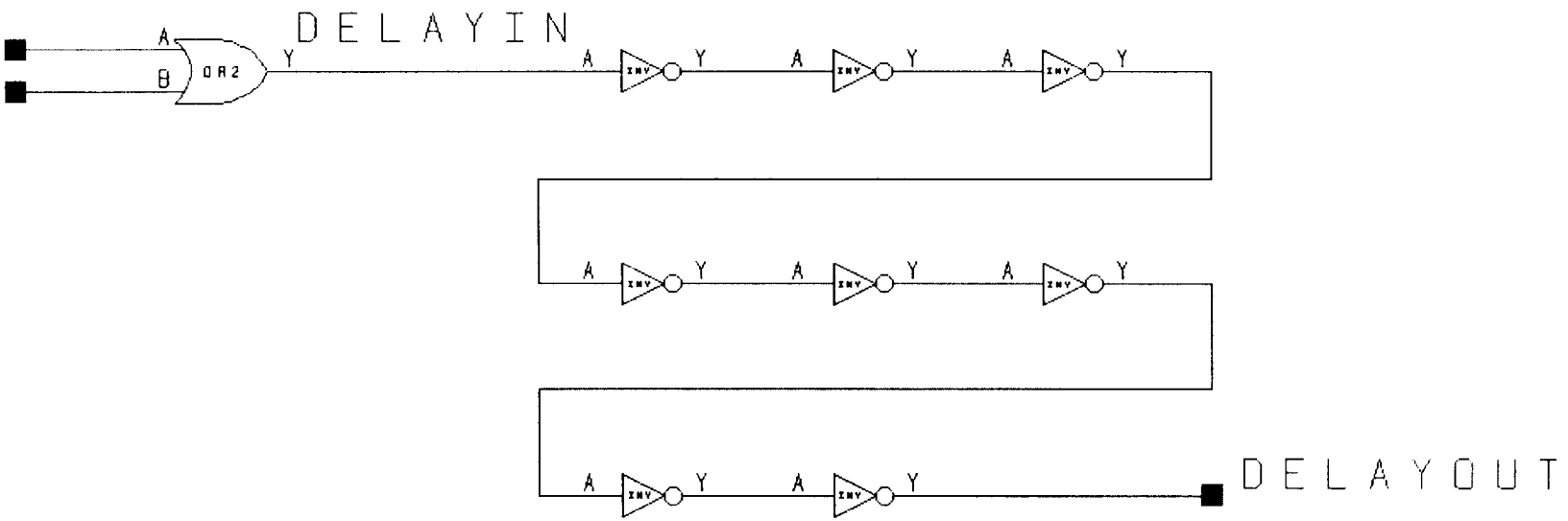
Specifications
Case Study 1

- Gate Array Operation Differed from Specification
  - No Continuity of Personnel on Project
  - Features Added and Deleted During Development
  - Changes Were Not Documented in Specification

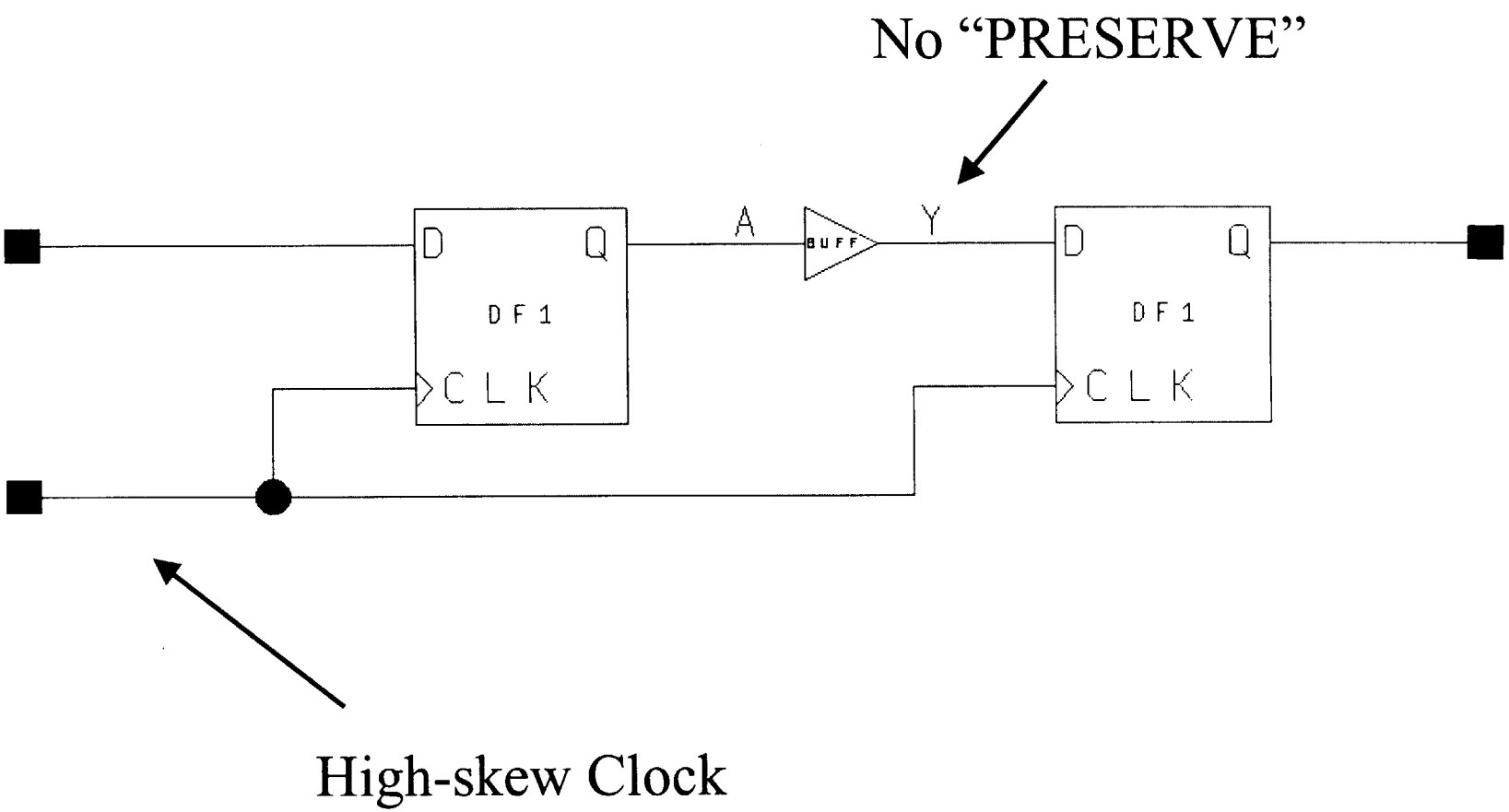
Specifications
Case Study 2

- Continual Updates to FPGAs Caused Delays to Project
  - Drifting Software Requirements Impacted FPGA
  - Drifting System Requirements Impacted FPGA
- No Stable Specification

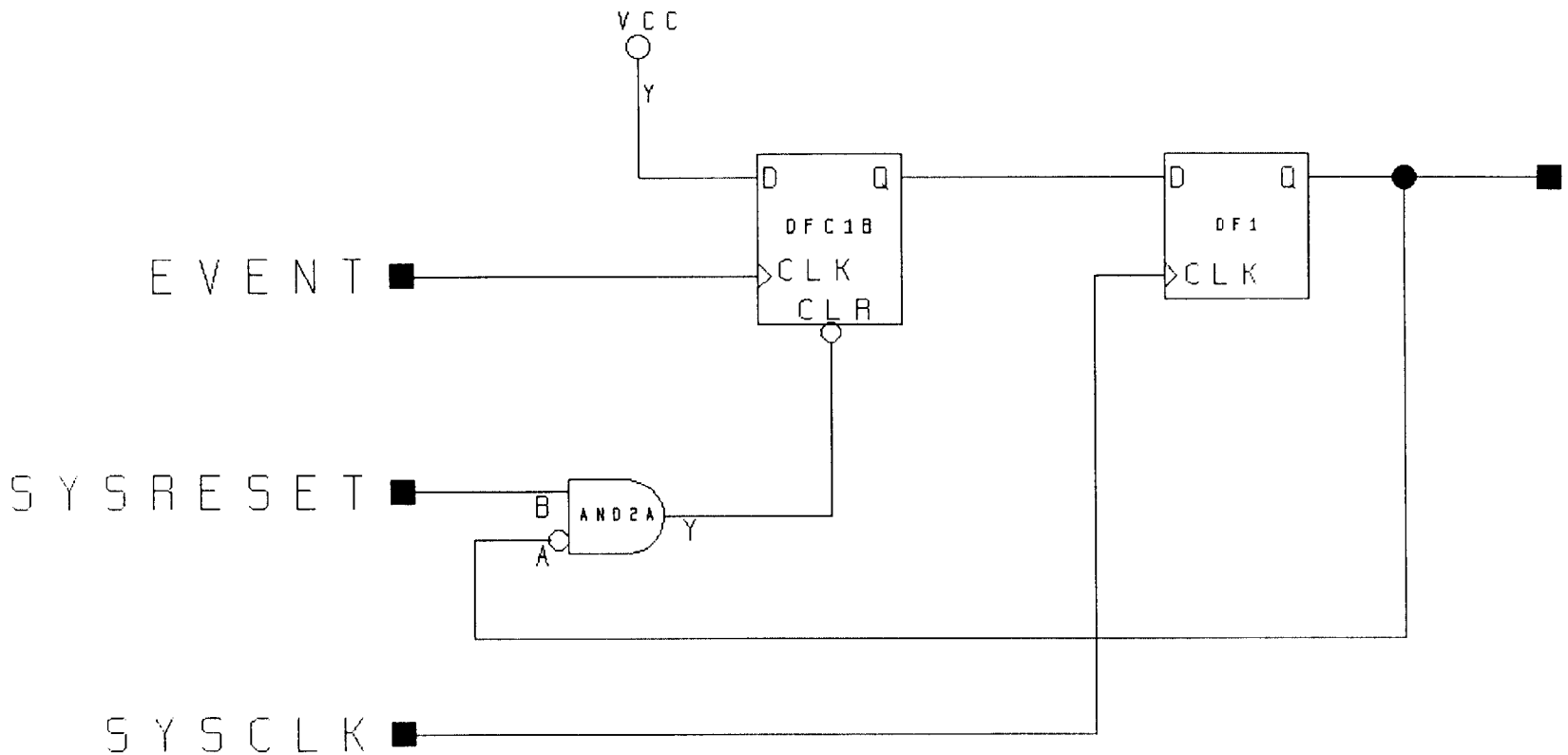
Delay Generation



Clock Skew Correction



Synchronizer



Conclusion

- Stable Specifications Required
- Continuity of Personnel Needed
- Detailed Reviews Required
- Simulation Does Not Replace Analysis
  - Limitations of Simulators
  - Fidelity of Models
- Abstractions Useful for Limiting Complexity at One Stage
  - Does Not Eliminate the Need to Understand the Technology at Lower Levels of Abstraction