SEU Mitigation Techniques for SRAM based FPGAs

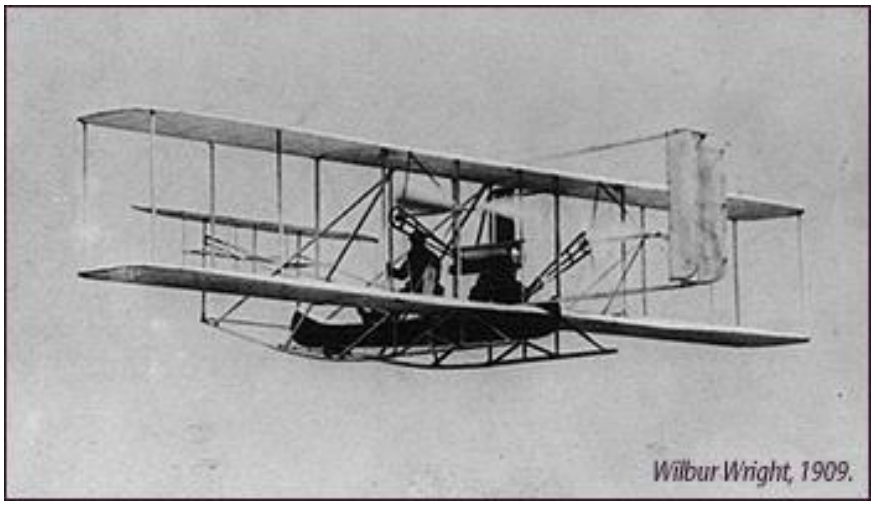
Ken Chapman

30th September 2015

TWEPP2015

Some Aviation History

Wright Flyer Model A
1 × 35hp piston engine



DH.89 Dragon Rapide
Introduced 1934
2 × 200hp piston engine

Some Xilinx SEU History

Xilinx is the only FPGA vendor that openly publishes SEU and Soft Error Rate measurements (see UG116).

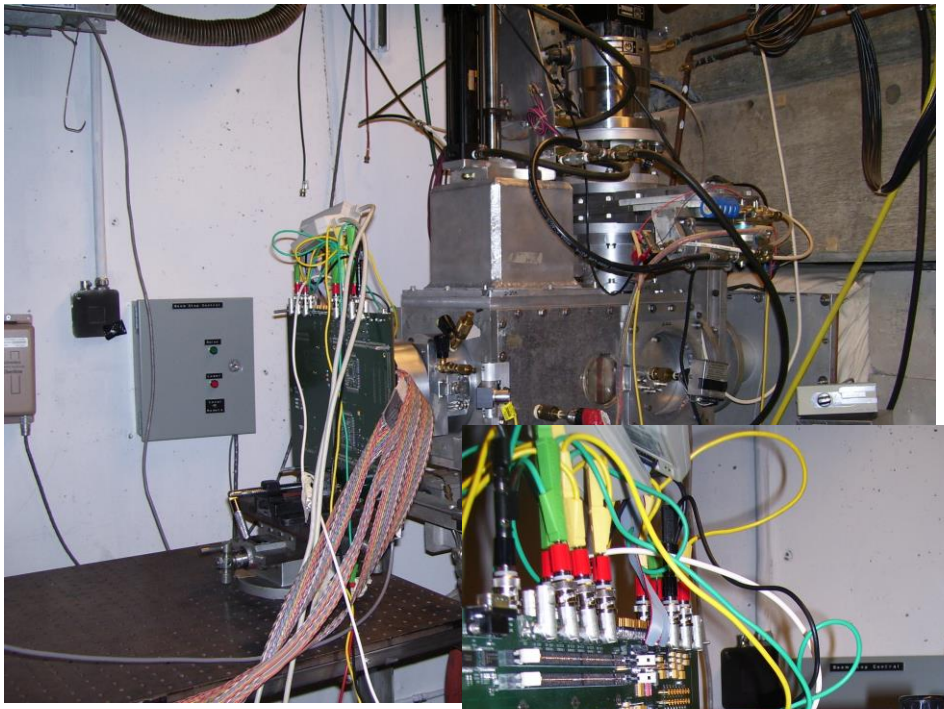
Observations and experiences of devices in the real atmosphere as well as during beam experiments have enabled Xilinx to understand the susceptibility of *our* devices.

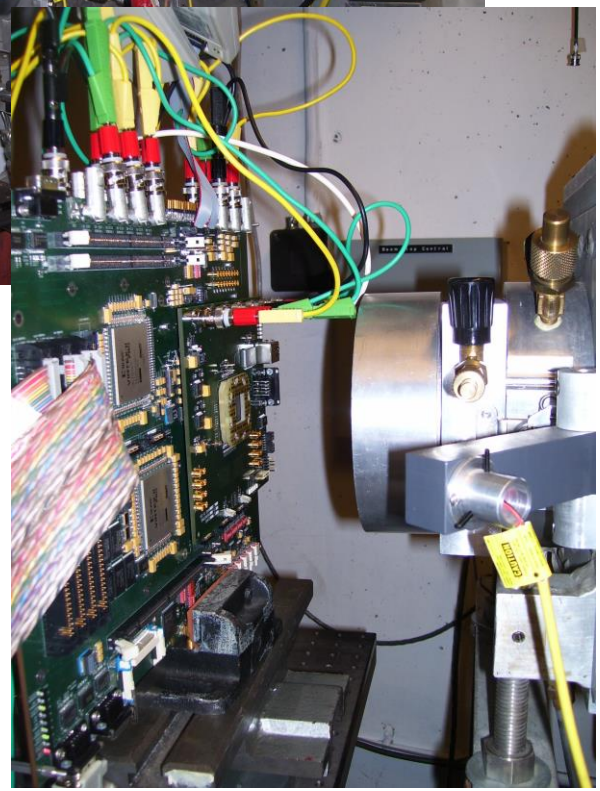
Improvements are often ‘by design’. We didn’t just get lucky!

Use known published data to make informed and relevant decisions about today’s devices.

	Tech Node	Product Family	FIT/Mb [6] (Real Time Soft Error Rate Per Event)[3]		
			CRAM	BRAM	Error[4]
1998	250 nm	Virtex	160	160	±20%
	180 nm	Virtex-E	181	181	±20%
	150 nm	Virtex-II	405	478	±8%
	130 nm	Virtex-II Pro	437	770	±8%
	90 nm	Virtex-4	263	484	±11%
	90 nm	Spartan-3	190	373	–50% +80%
	90 nm	Spartan-3E Spartan-3A	104	293	–80% +90%
	65 nm	Virtex-5	165	692	–13% +15%
	45 nm	Spartan-6	182	382	–10% +12%
	40 nm	Virtex-6	103	262	-12% +13%
	28 nm	7 series Artix and Zynq	87	79	-11% +13%
2015	20 nm	UltraScale	29[7]	50[7]	TBD[7]

Over 17 Years of ‘Rosetta’ and Beam Testing





Xilinx SEU; Past, Present and Future

UG116

			CRAM	BRAM
1998	250 nm	Virtex	160	160
2002	130 nm	Virtex-II Pro	437	770
2012 (Now)	28 nm	7 series Artix and Zynq	87	79
2015 (Now)	20 nm	UltraScale	29(7)	50(7)

Soft Event Rates at sea level New York

Events per million bits per 10^9 hours. Configuration memory (CRAM) and Block Memory (BRAM) in user design.

Things were definitely getting worse so this *had* to be addressed by design.

Xilinx FPGAs now have a lower susceptibility than they have ever had.

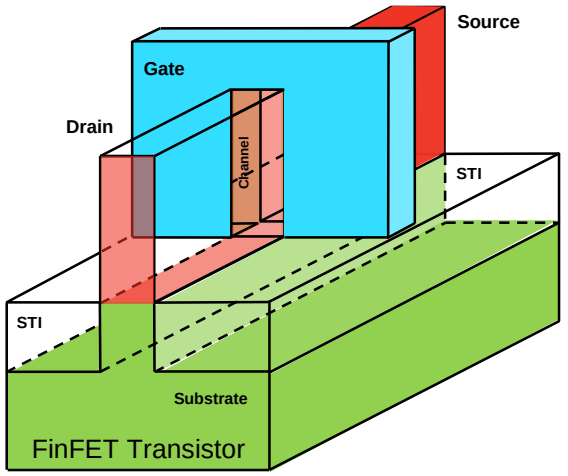
Coming soon…

Tests indicate

<5 FIT/Mb

Advanced 16nm FinFET
5× reduction in sensitive area

Design Rules
40+ Patents & Trade Secrets



Which is Safer?

Piper Seneca PA-34
- 6 Seats
- 2 × 220hp Piston Engine

Piper Meridian M500
- 6 Seats
- 1 × 500hp Turboprop Engine

The Weakest Link!

17th January 2008

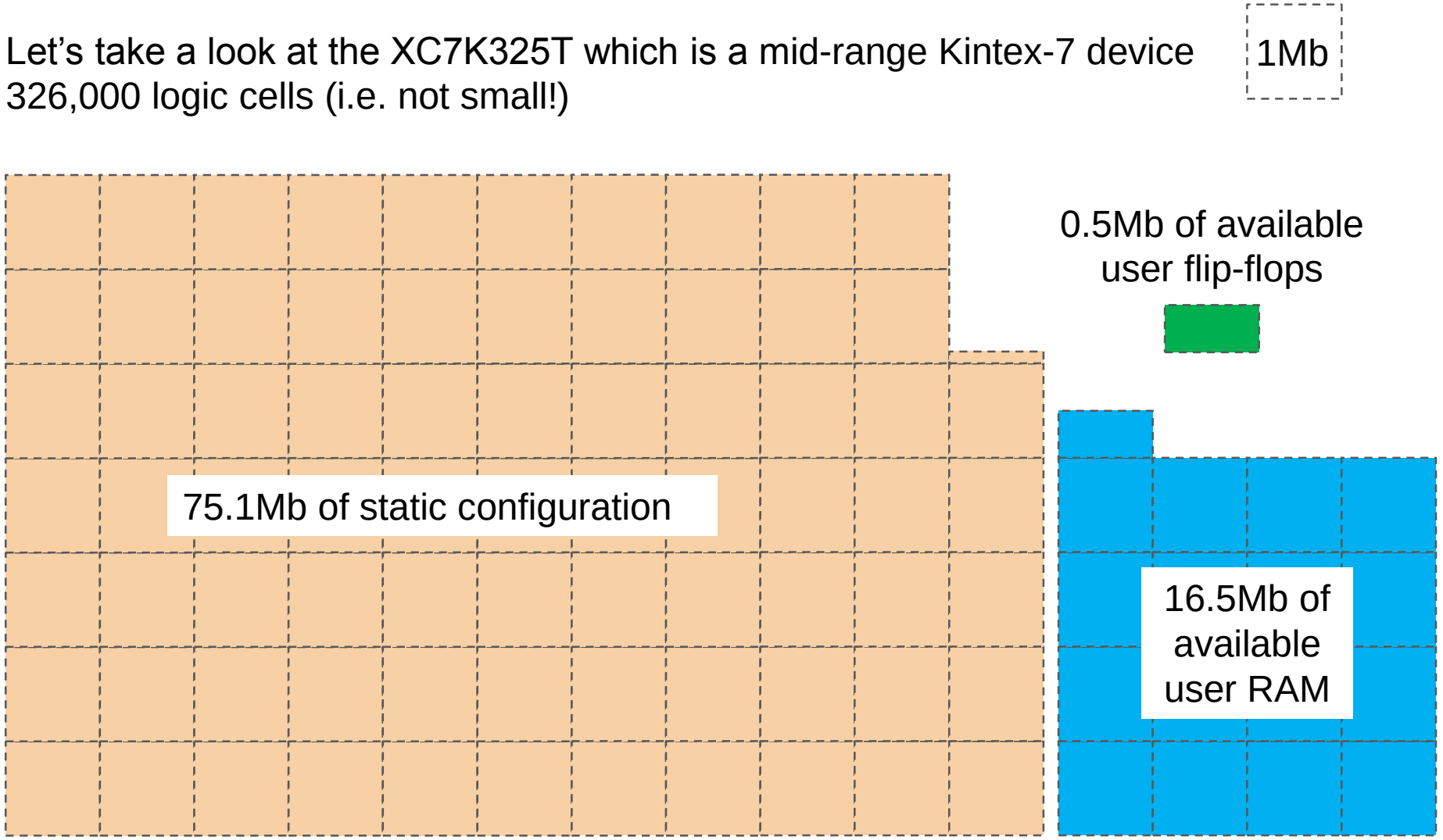
Boeing 777 with 2 Pratt & Whitney Engines

London Heathrow – Final approach to 27L

Why did both engines fail at the same time?

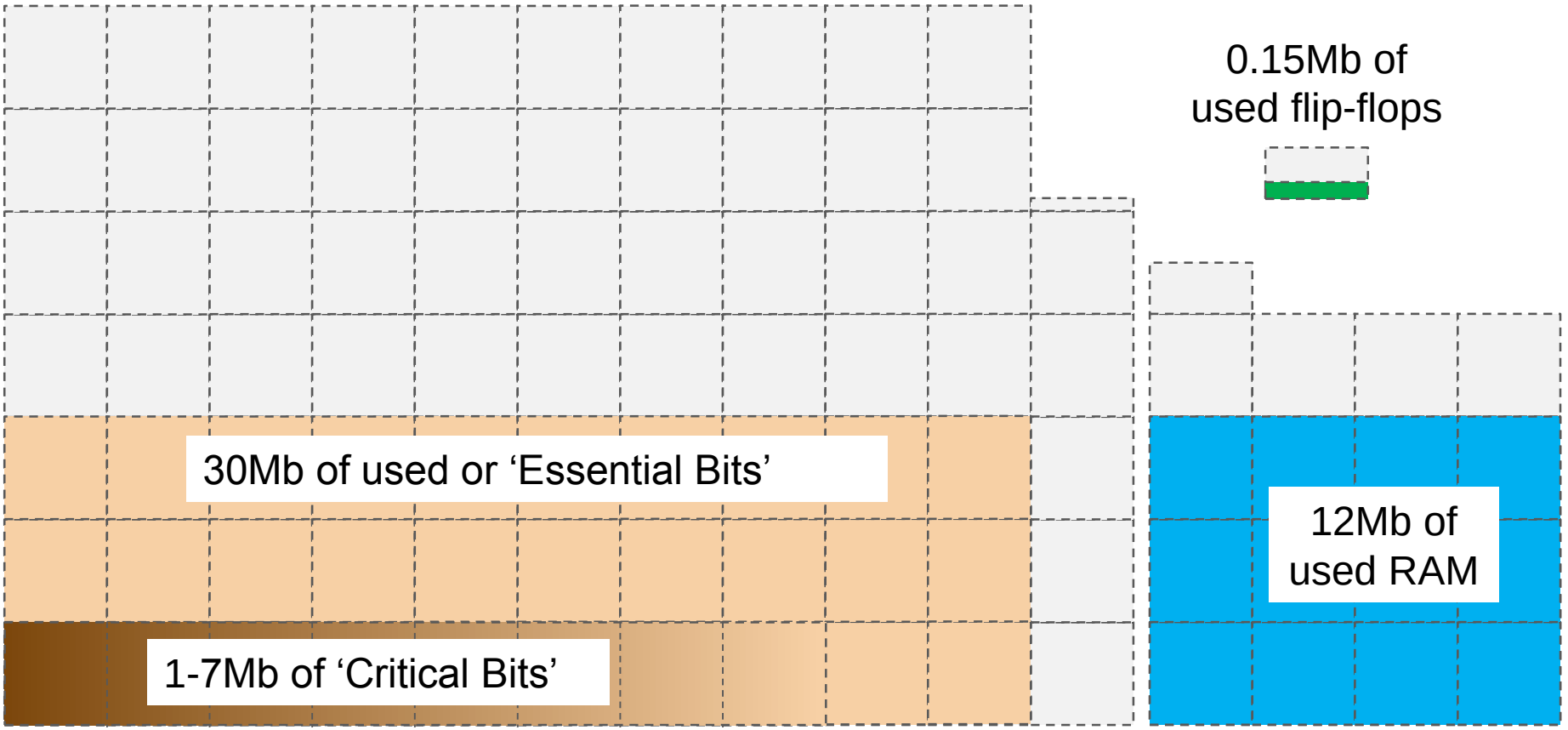
Risk Assessment – Whole Device

Let's take a look at the XC7K325T which is a mid-range Kintex-7 device
326,000 logic cells (i.e. not small!)



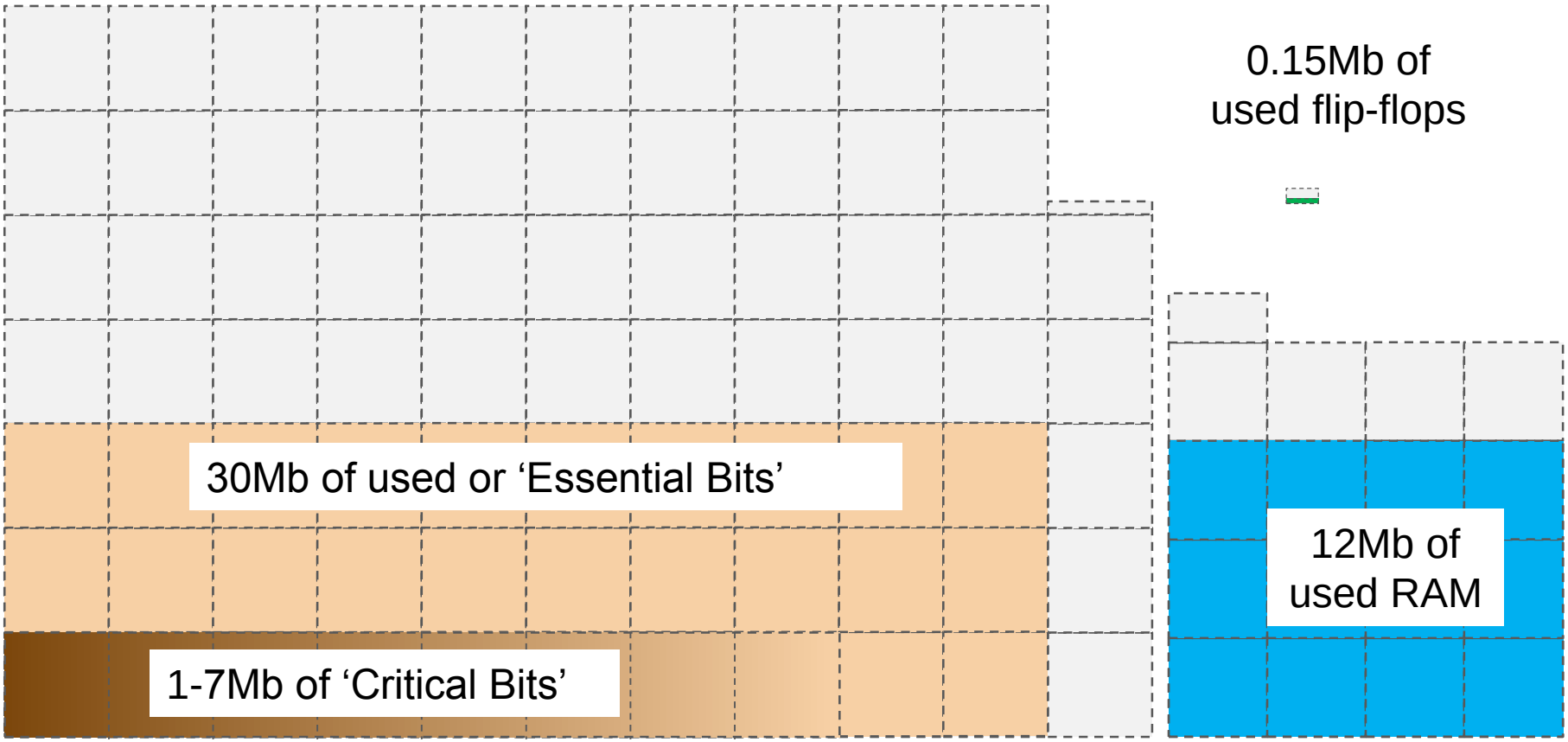
Risk Assessment – Resources Actually Used

Every design is different so obviously better to work with actual values.
But let's accept some typical figures for now…



Risk Assessment – Scaling for Susceptibility

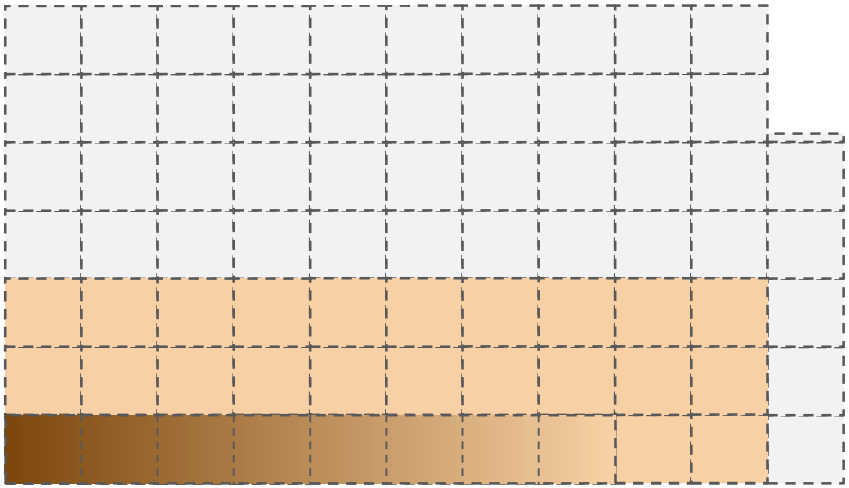
Different cells have different susceptibly.
Let's normalise for CRAM FIT Rate…



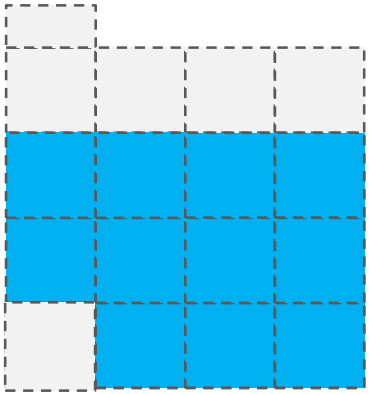
Still little doubt that Configuration and BRAM cells are the area of concern

Risk Assessment – Comparing Different ‘Engines’

20nm UltraScale



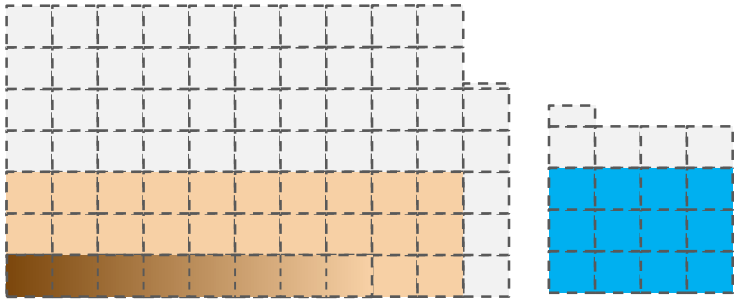
20nm UltraScale



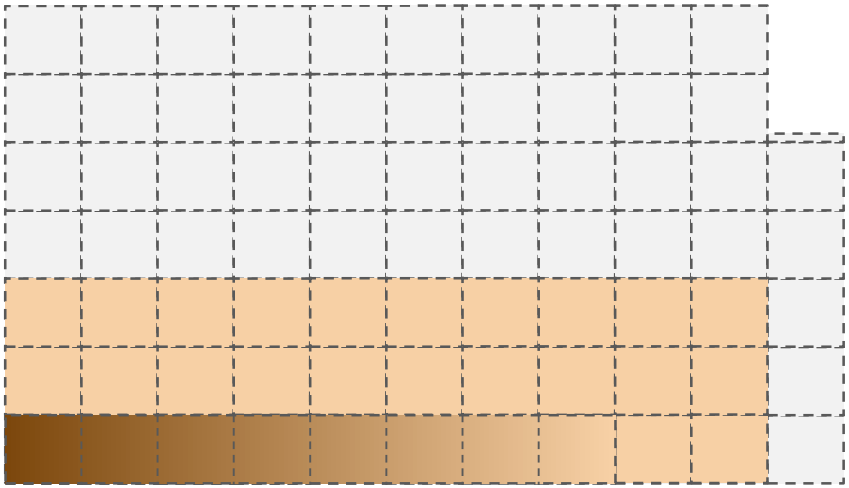
Base your design decisions of today on what is really happening today!

Risk Assessment – Comparing Different ‘Engines’

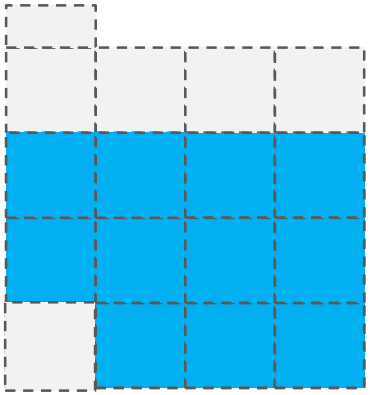
16nm UltraScale+



20nm UltraScale



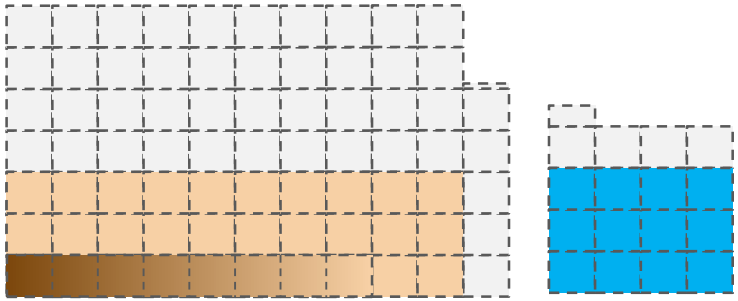
20nm UltraScale

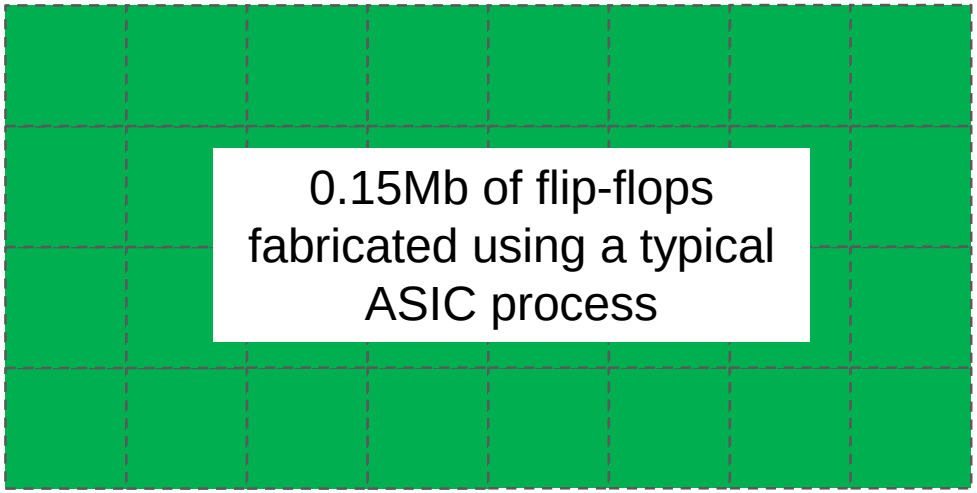


Base your design decisions of today on what is really happening today!

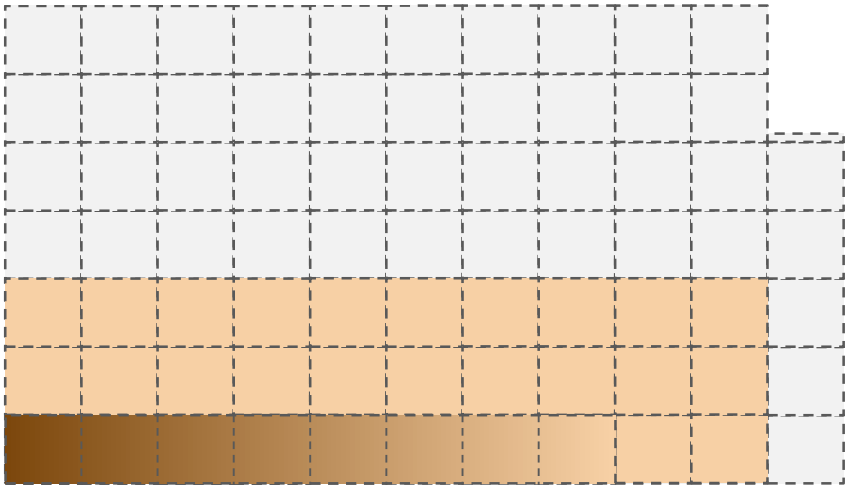
Risk Assessment – Comparing Different ‘Engines’

16nm UltraScale+

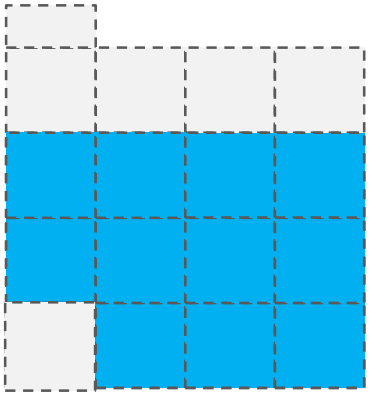




20nm UltraScale



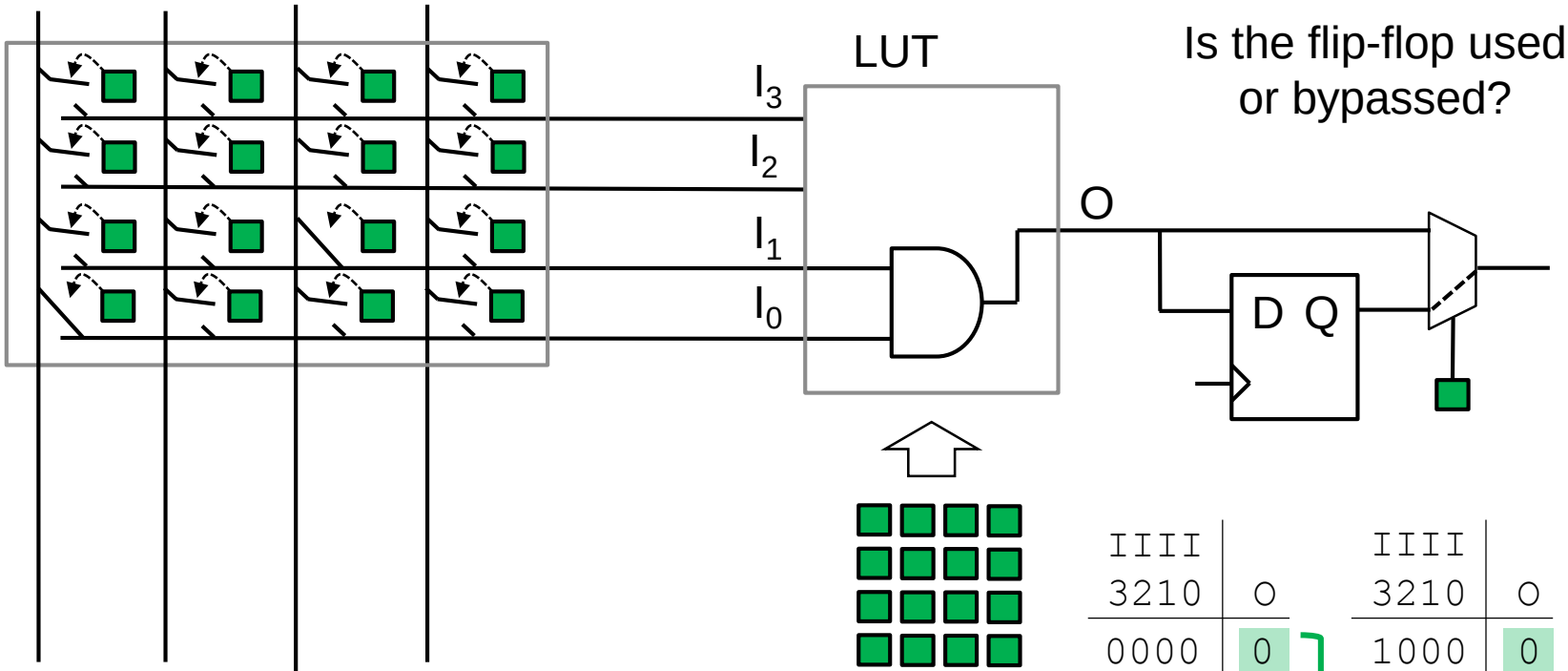
20nm UltraScale



Base your design decisions of today on what is really happening today!

What effects do upsets actually have?

Switch Matrix (i.e. routing)



Is the flip-flop used or bypassed?

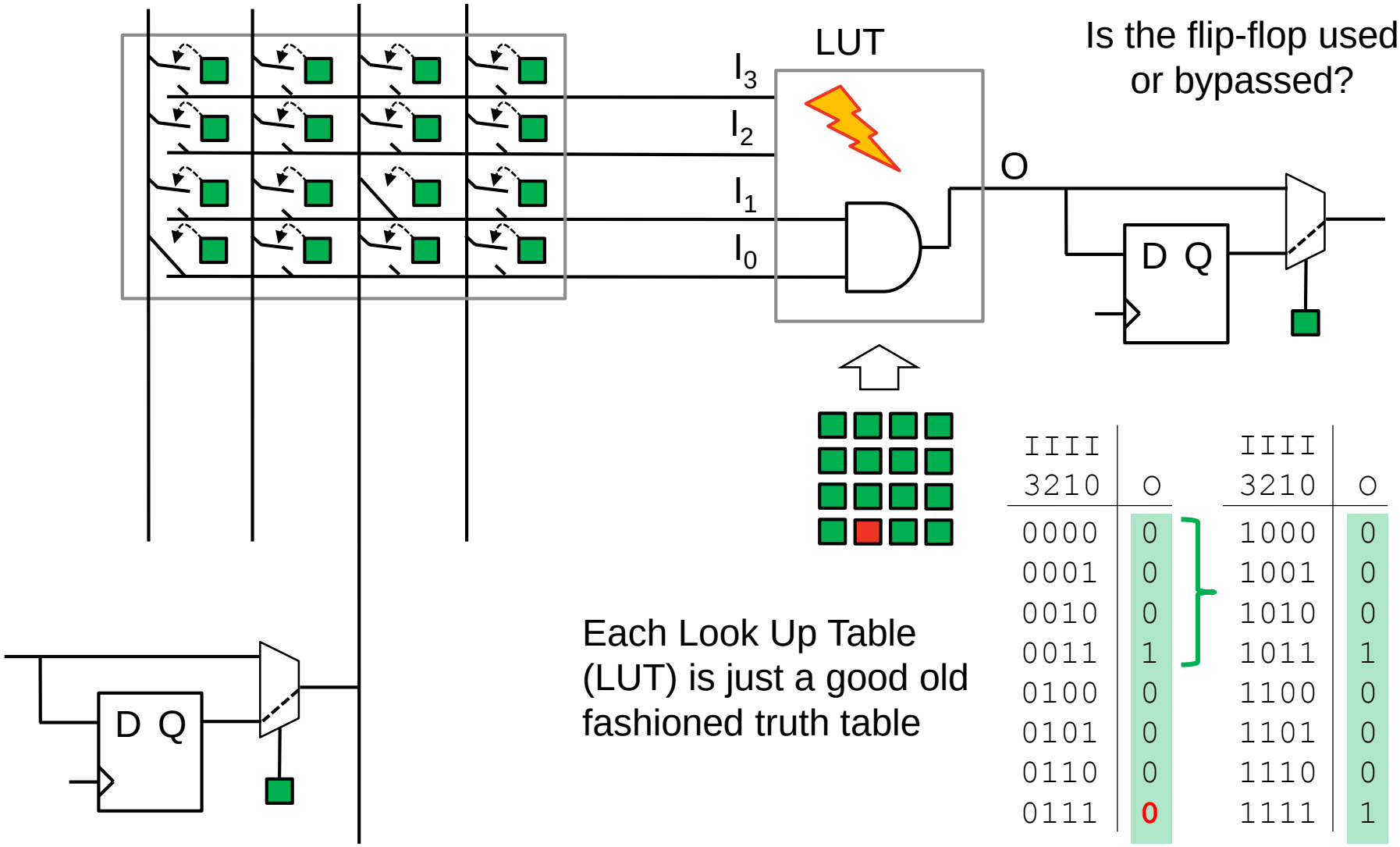
Each Look Up Table (LUT) is just a good old fashioned truth table

IIII 3210	O
0000	0
0001	0
0010	0
0011	1
0100	0
0101	0
0110	0
0111	1

IIII 3210	O
1000	0
1001	0
1010	0
1011	1
1100	0
1101	0
1110	0
1111	1

What effects do upsets actually have?

Switch Matrix (i.e. routing)



Is the flip-flop used or bypassed?

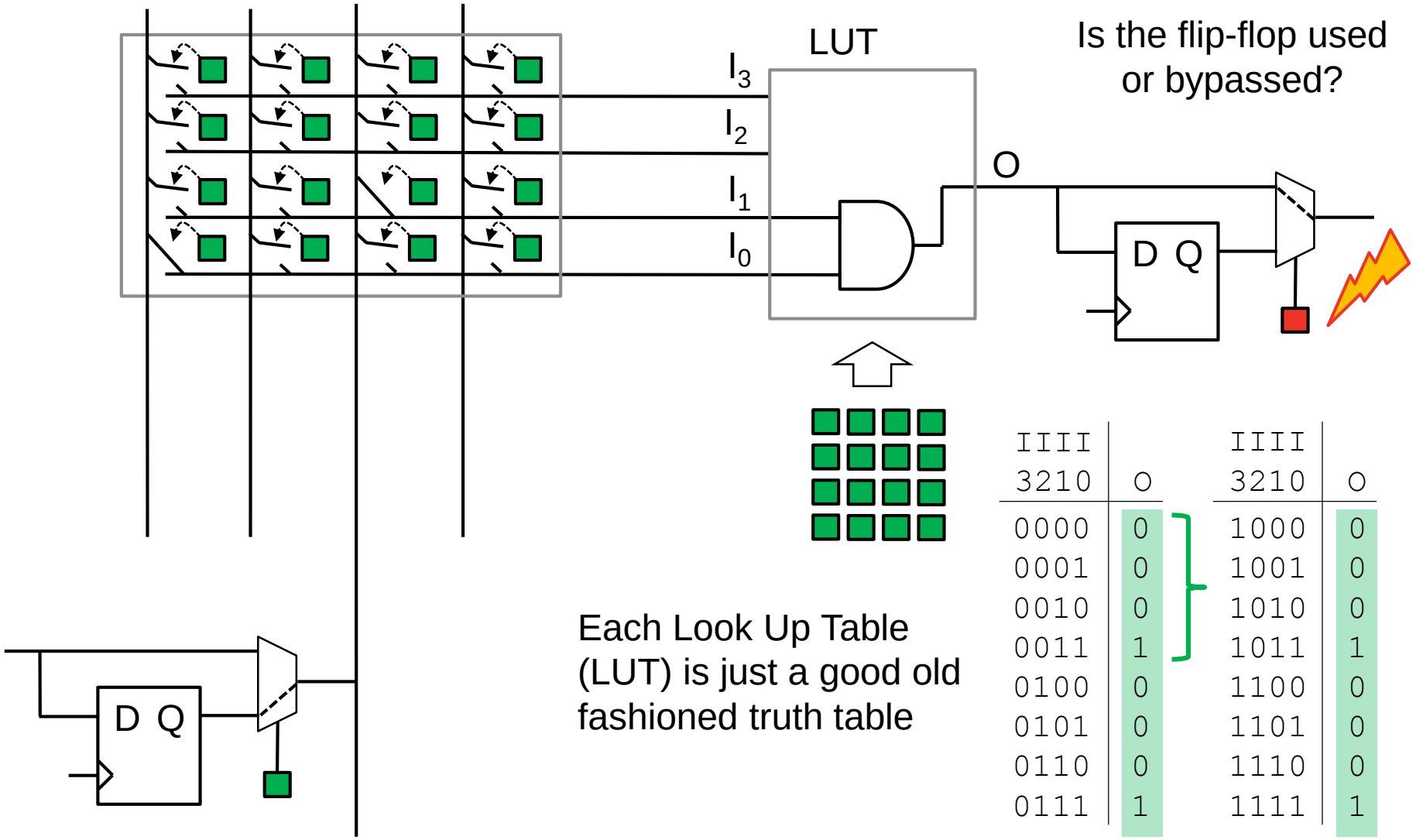
Each Look Up Table (LUT) is just a good old fashioned truth table

IIII 3210	O
0000	0
0001	0
0010	0
0011	1
0100	0
0101	0
0110	0
0111	0

IIII 3210	O
1000	0
1001	0
1010	0
1011	1
1100	0
1101	0
1110	0
1111	1

What effects do upsets actually have?

Switch Matrix (i.e. routing)



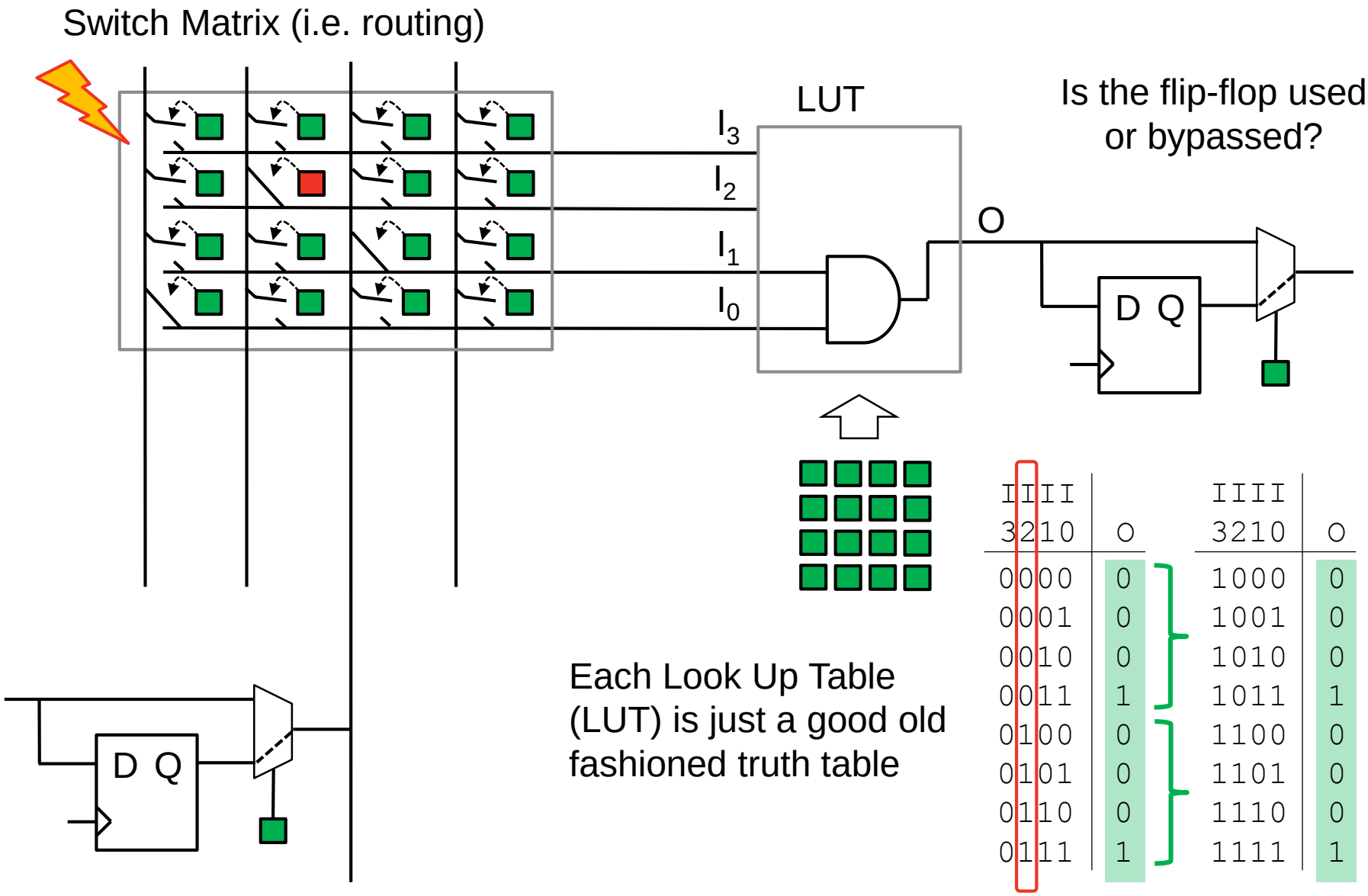
Is the flip-flop used or bypassed?

Each Look Up Table (LUT) is just a good old fashioned truth table

IIII 3210	O
0000	0
0001	0
0010	0
0011	1
0100	0
0101	0
0110	0
0111	1

IIII 3210	O
1000	0
1001	0
1010	0
1011	1
1100	0
1101	0
1110	0
1111	1

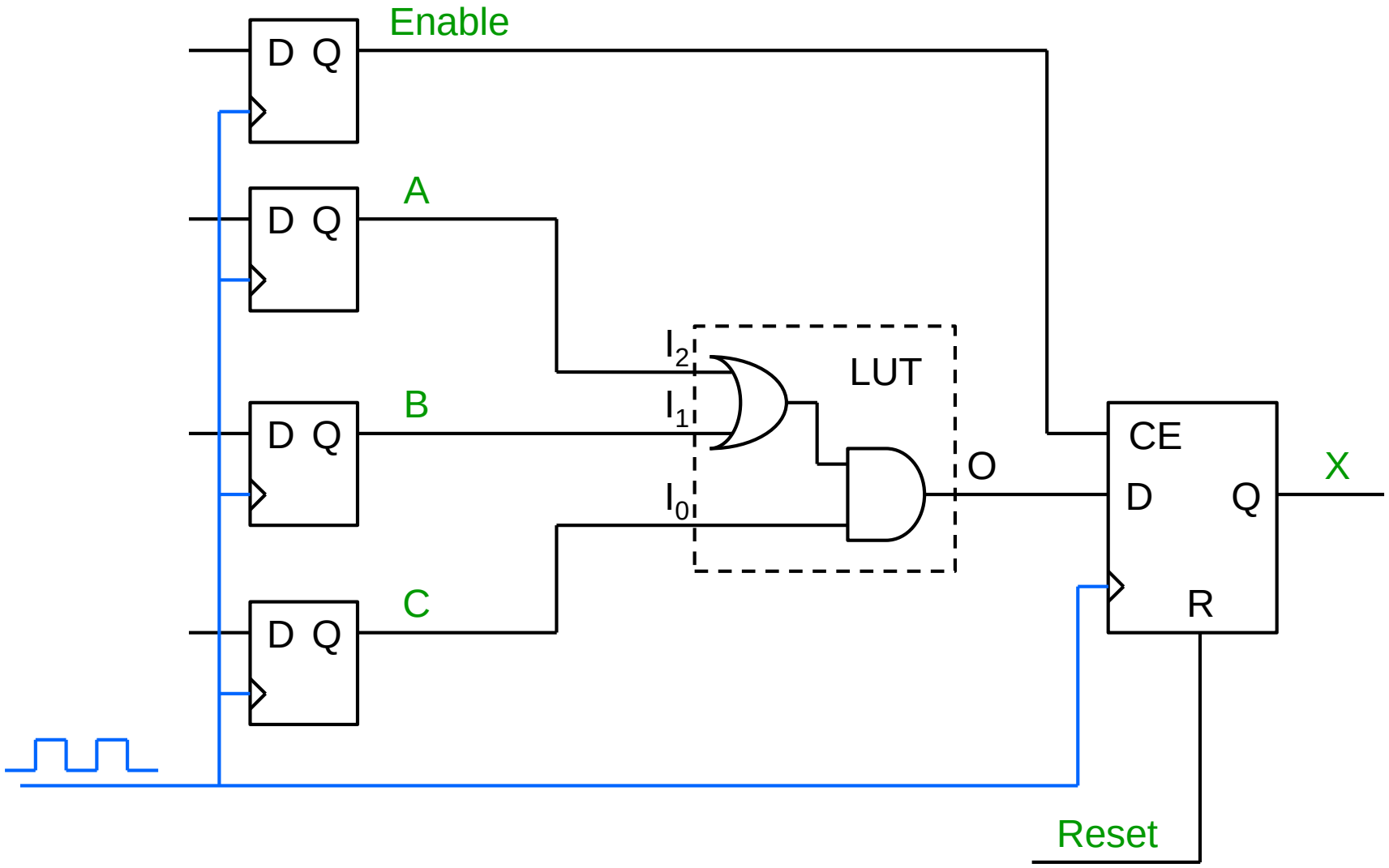
What effects do upsets actually have?



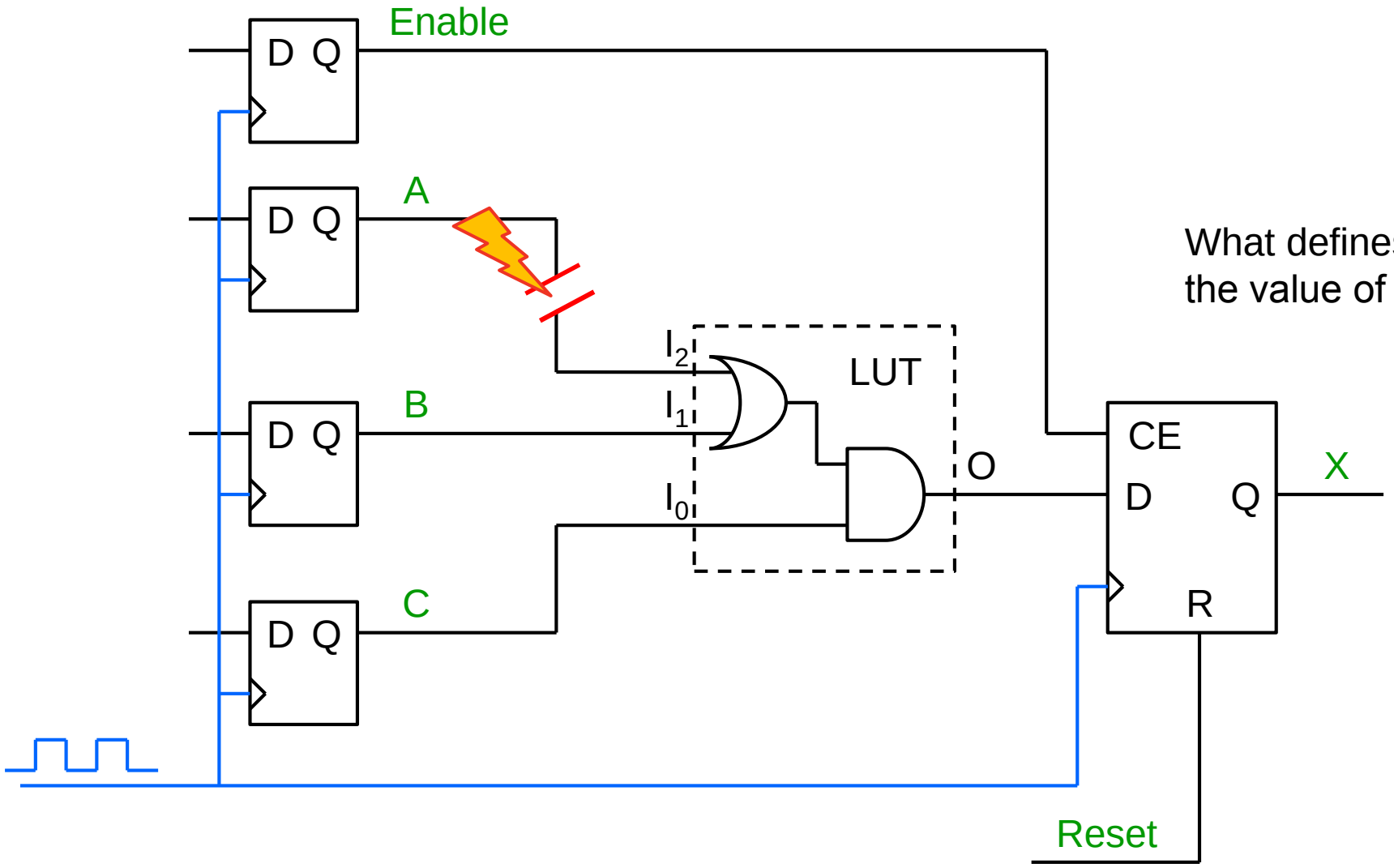
Each Look Up Table (LUT) is just a good old fashioned truth table

IIII 3210	O
0000	0
0001	0
0010	0
0011	1
0100	0
0101	0
0110	0
0111	1
1000	0
1001	0
1010	0
1011	1
1100	0
1101	0
1110	0
1111	1

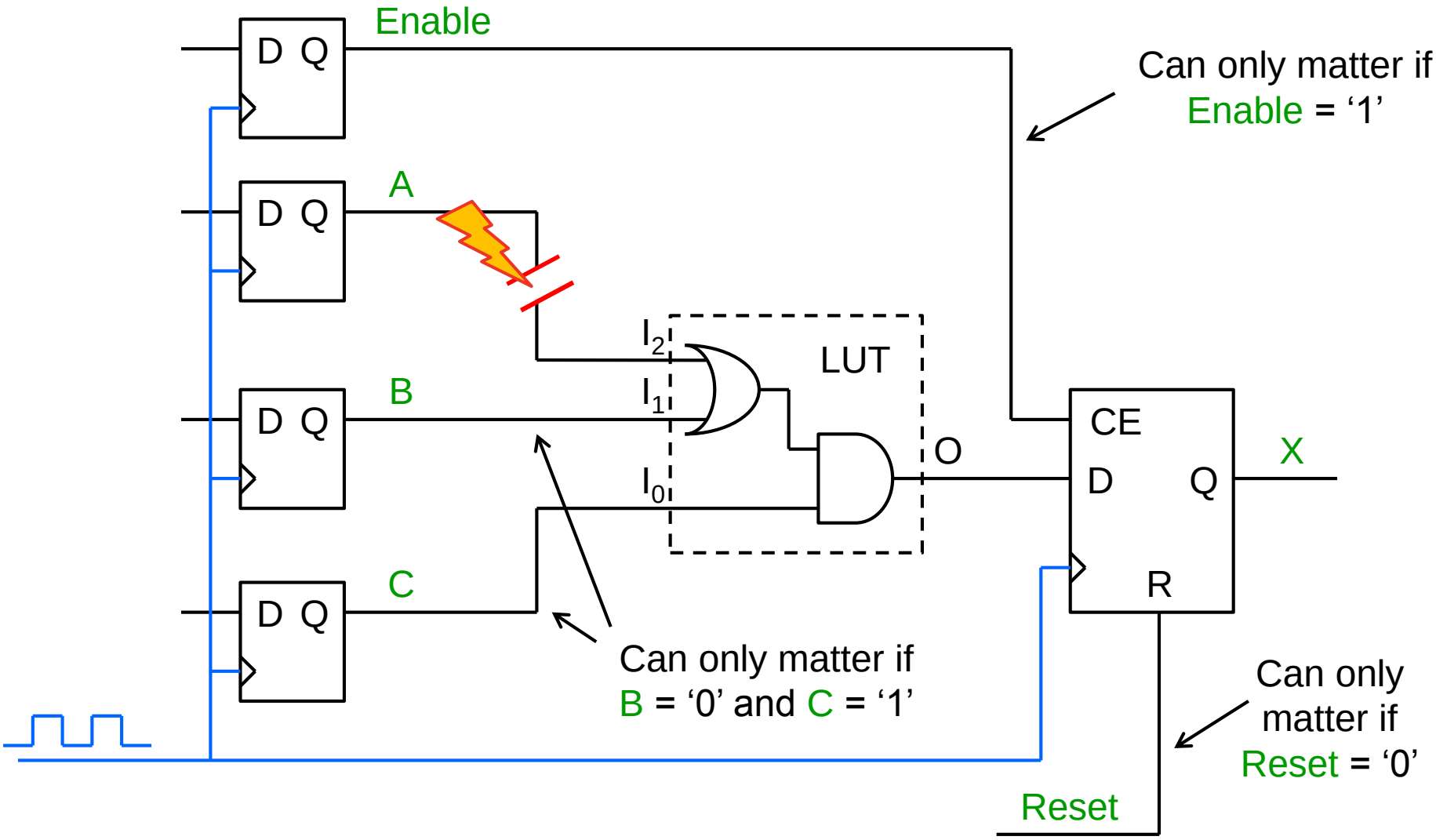
What Happens to ‘X’.....



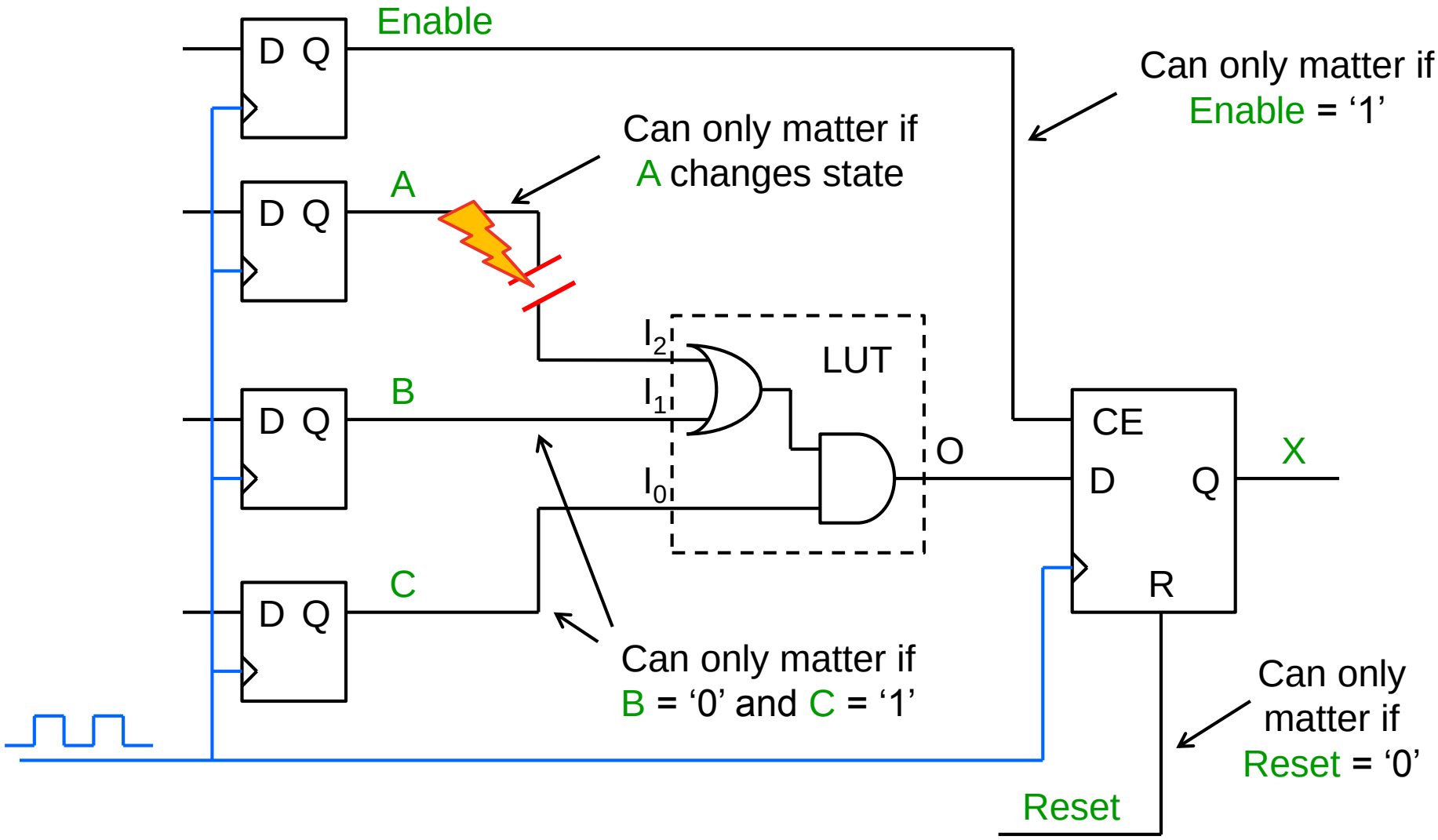
What Happens to ‘X’.....



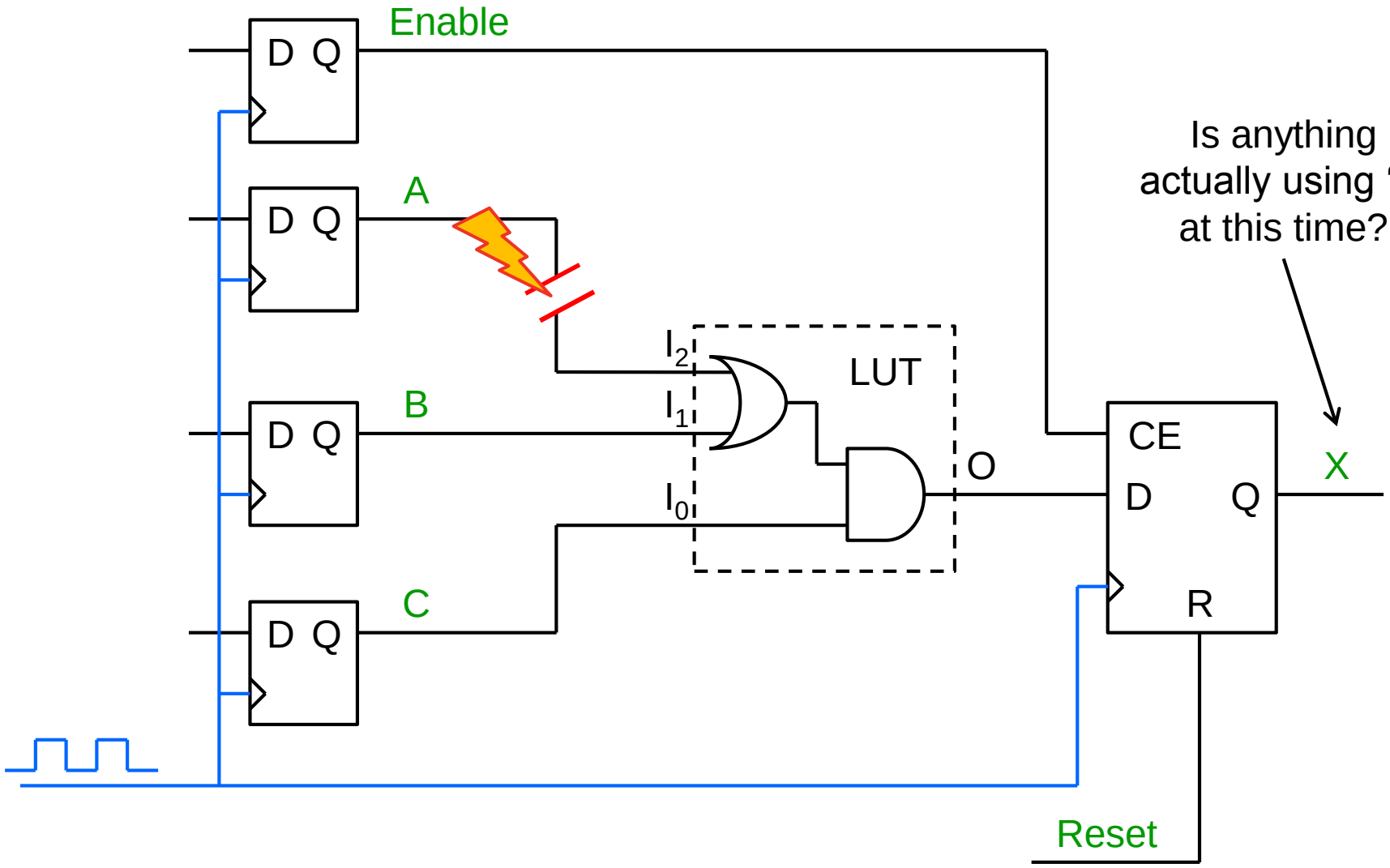
What Happens to ‘X’.....



What Happens to ‘X’.....



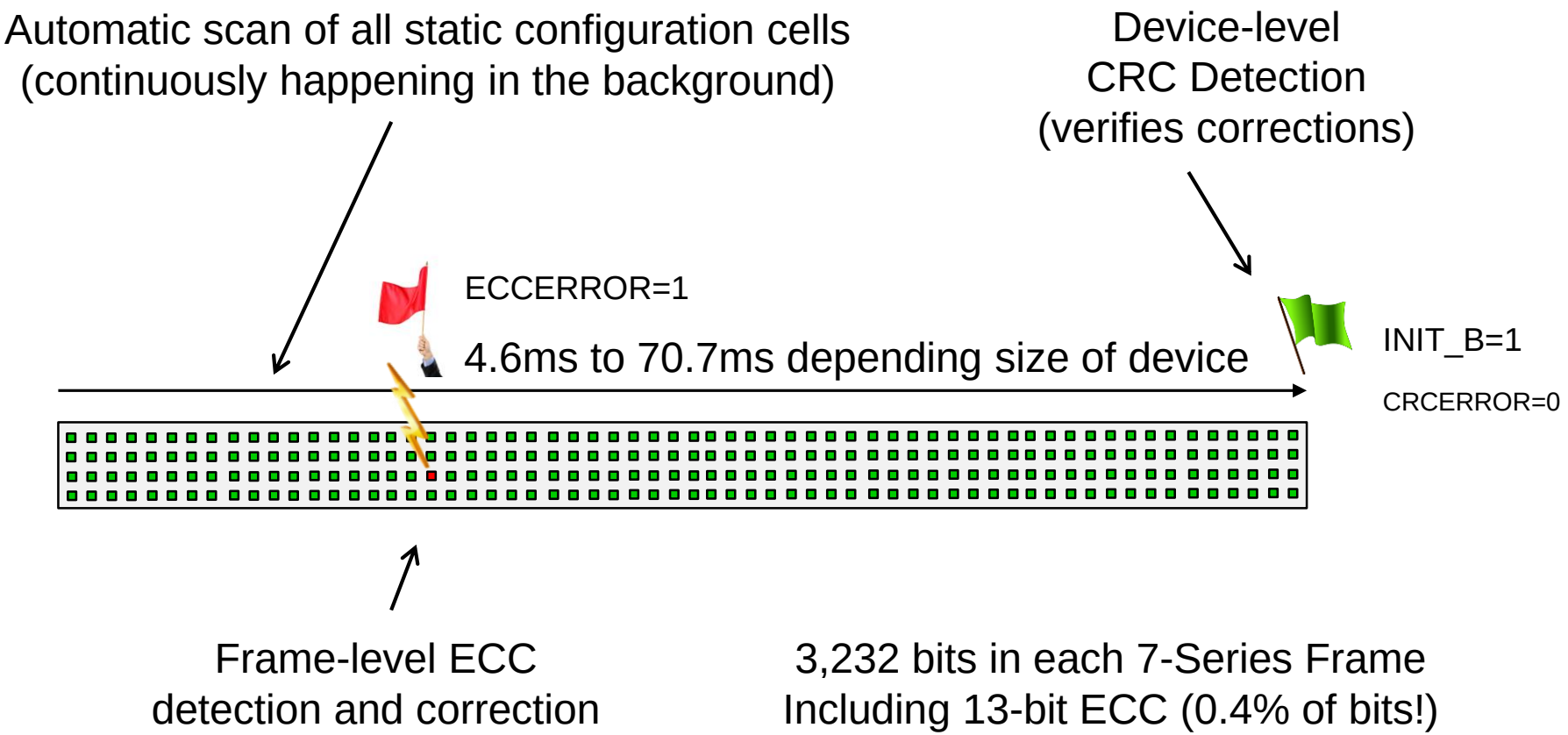
What Happens to ‘X’.....



Detecting and Correcting Errors Quickly

7-Series and UltraScale devices have *dedicated* error detection and correction circuits.

- Primarily for SEU but acts as an ongoing comprehensive BIST during device lifetime.



When ECC is not enough!

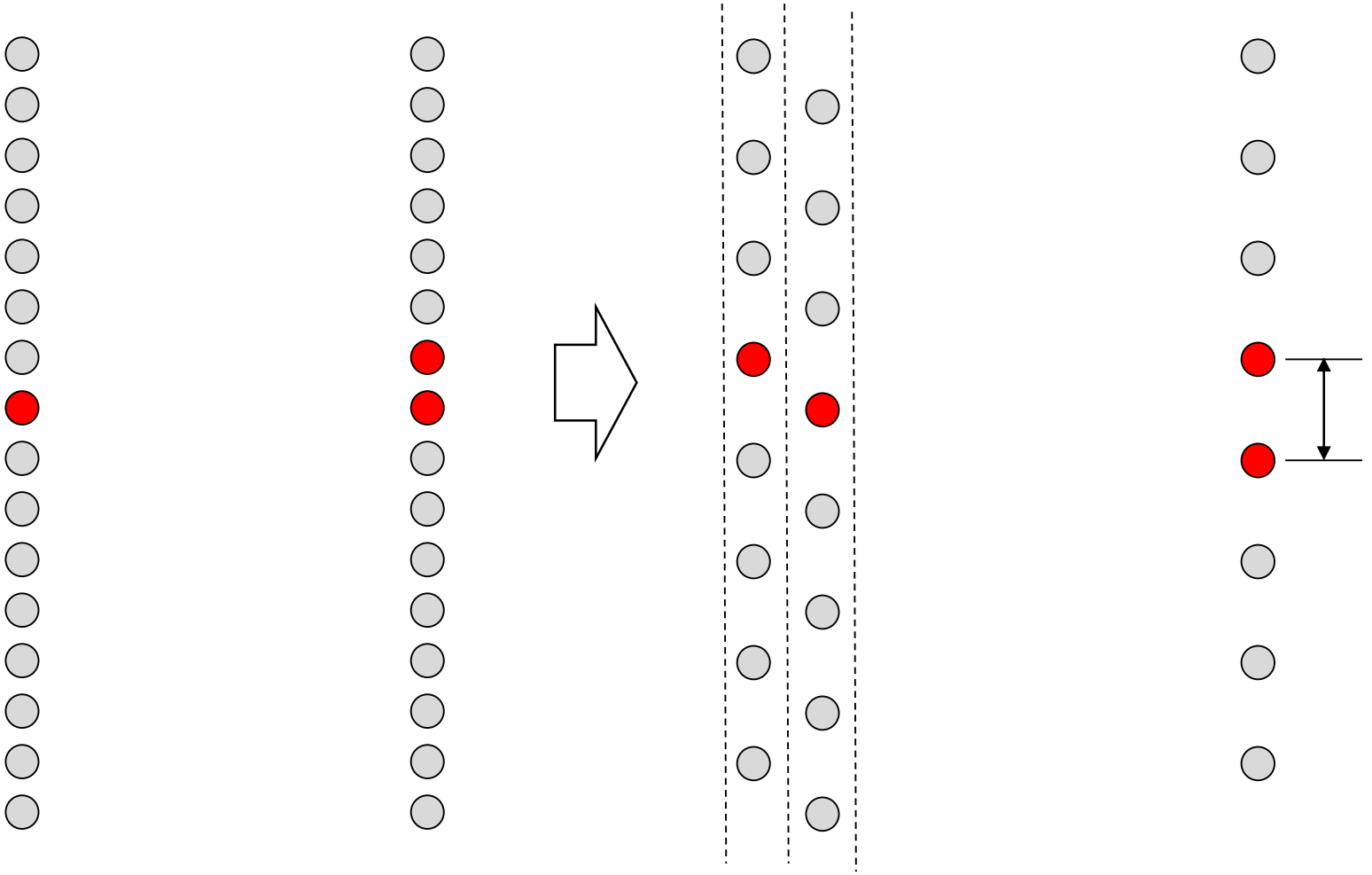
Upset rates are decreasing but the proportion of Multiple Bit Upsets are increasing.

Single Bit Error (SBE)

Double Bit Error (DBE)

= 2 × SBE

Same Frame Double Bit Error (DBE)



When ECC is not enough!

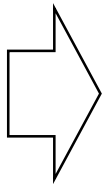
UltraScale has 2-way physical and 4-way virtual interleaving.

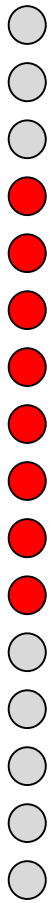
8 Bit Error (MBE)

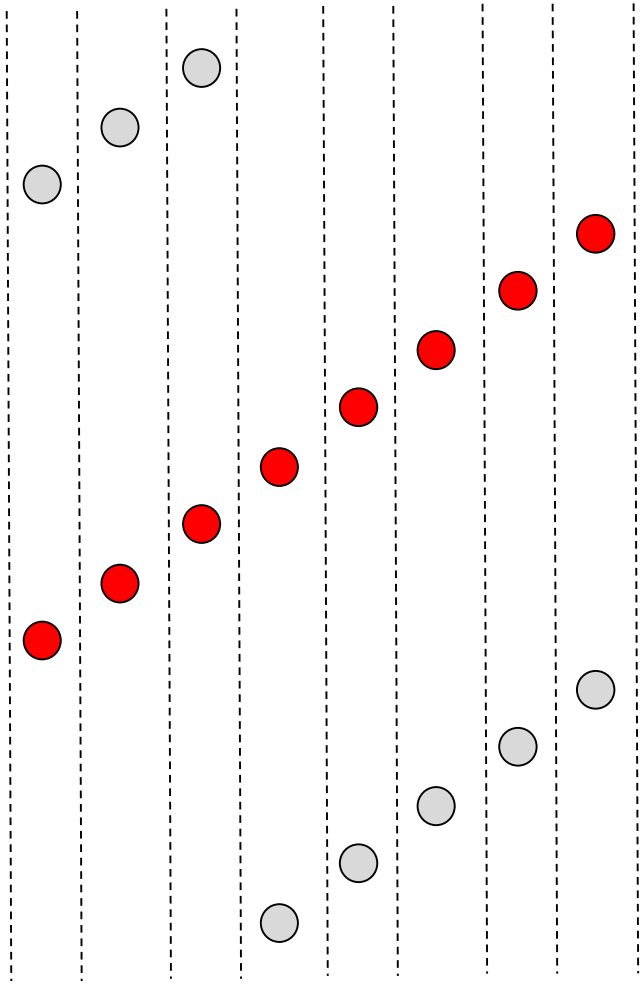
= 8 × SBE

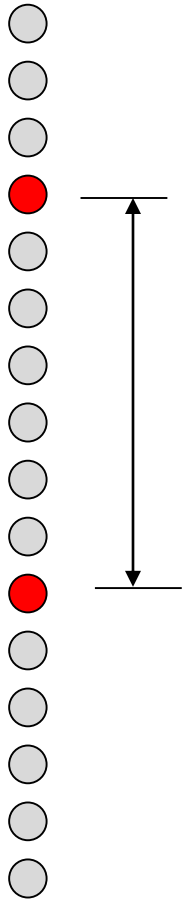
Same ‘ECC Frame’ Double Bit Error (DBE)

Highly unlikely upset!









Aviate, Navigate, Communicate

17th January 2008

Boeing 777 with 2 Pratt & Whitney Engines

London Heathrow – Final approach to 27L

Captain Peter Burkill & Senior first officer John Coward did an outstanding job in giving the highest priority to ‘Aviate’.

Unfortunately, rather more accidents are the result of ‘pilot error’.

Training and Simulation

Enables pilots to experience situations and learn how to deal with them in the best ways.

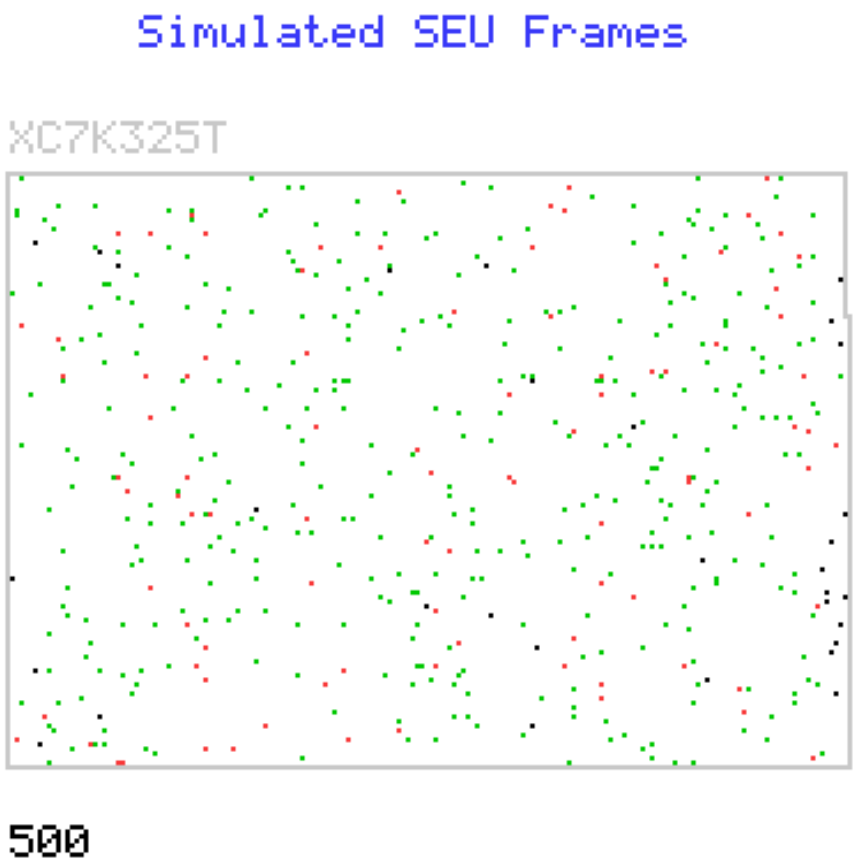
Boeing 777 Simulator

Also an opportunity to refine emergency procedures based on observations of ‘Human Factors and Performance’.

Observe What Happens & What Actions Are Needed

Aircraft have become extremely reliable so are the pilots now the weakest link?
Must not overload and distract pilots but also need to keep them engaged.

UltraScale+ will be ~50× less susceptible to SEU than Virtex-5 – That's a big change.
Do not implement mitigation schemes that make things less reliable!



Soft Error Mitigation (SEM) exploits partial reconfiguration to facilitate controlled simulation of SEUs (not everyone has a particle accelerator you know ☺).

500 simulated SEU in XC7325T.
Red dots = Disturbance observed ('Critical Bits').

Experiments = Knowledge (not guessing)

Do you need mitigation?
Where do you need mitigation?
What type of mitigation is suitable?
Will mitigation be more disruptive than doing nothing?

Yes, But Two Engines Are Still Better Than One

Ok, let's put you in the pilot's seat of the Piper Seneca PA-34…

Yes, But Two Engines Are Still Better Than One

Q. When is it most likely that that one of your engines will quit?

Yes, But Two Engines Are Still Better Than One

Q. When is it most likely that that one of your engines will quit?

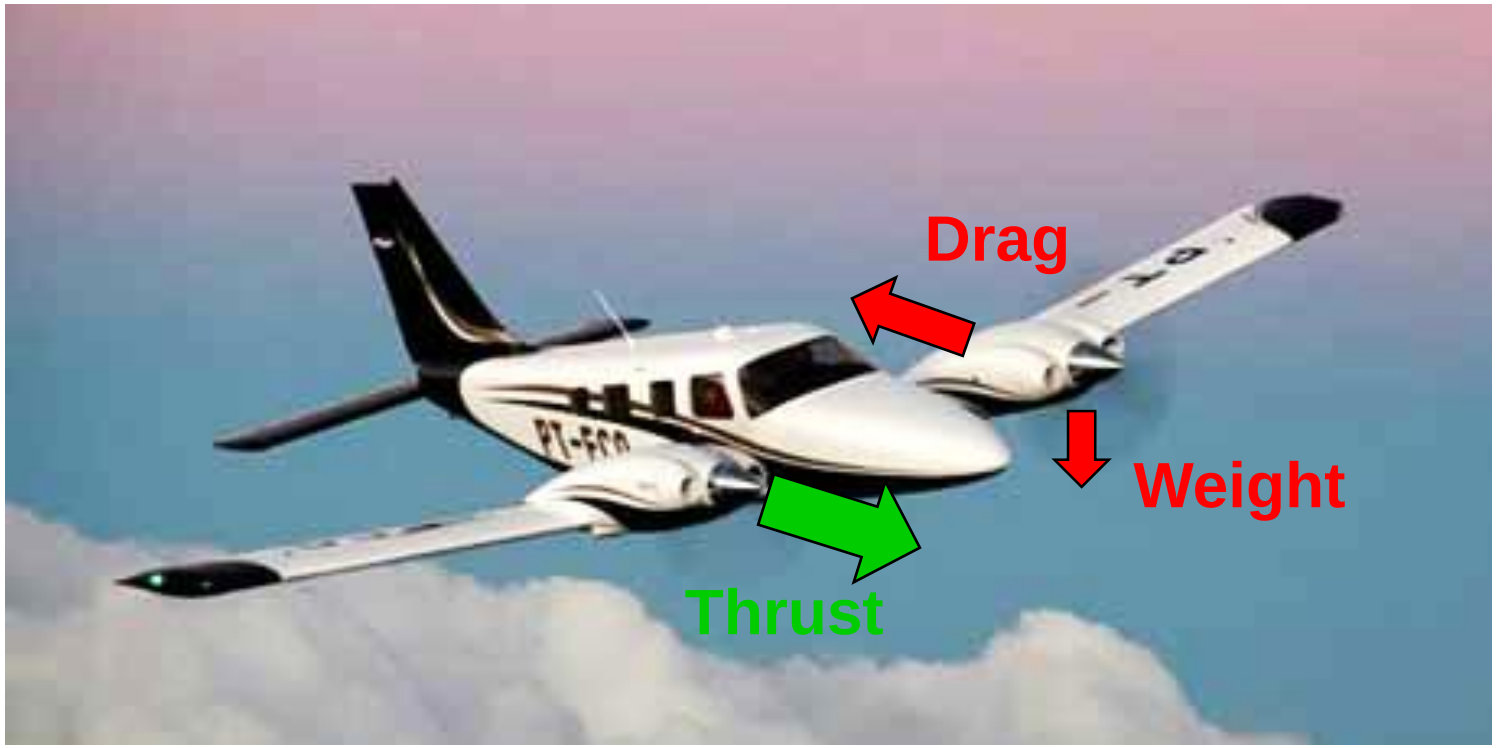
A. Just after take off when low, slow and climbing.

Yes, But Two Engines Are Still Better Than One

Q. Now what do you need to do?

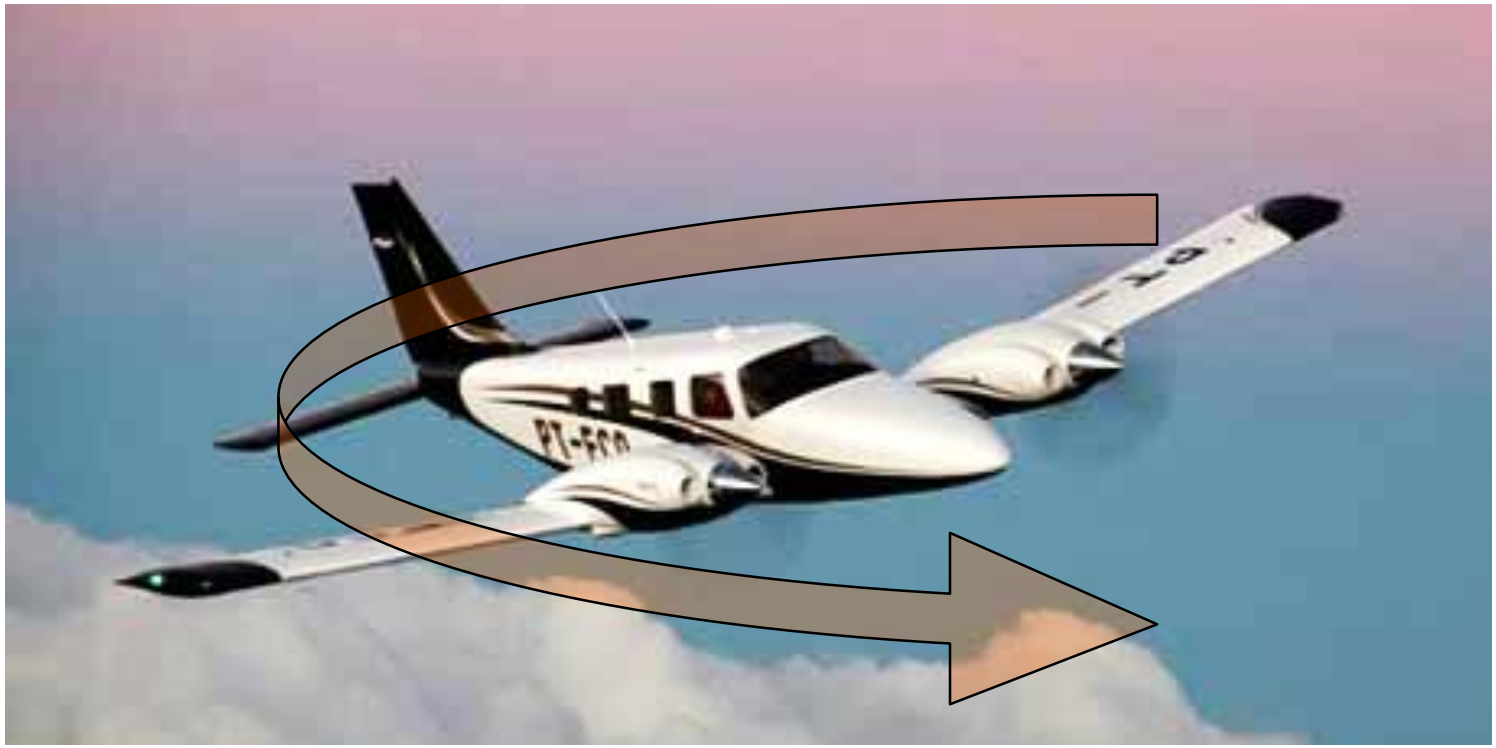
Yes, But Two Engines Are Still Better Than One

A. Stay calm and apply everything you learnt during your training!



Yes, But Two Engines Are Still Better Than One

A. Stay calm and apply everything you learnt during your training!



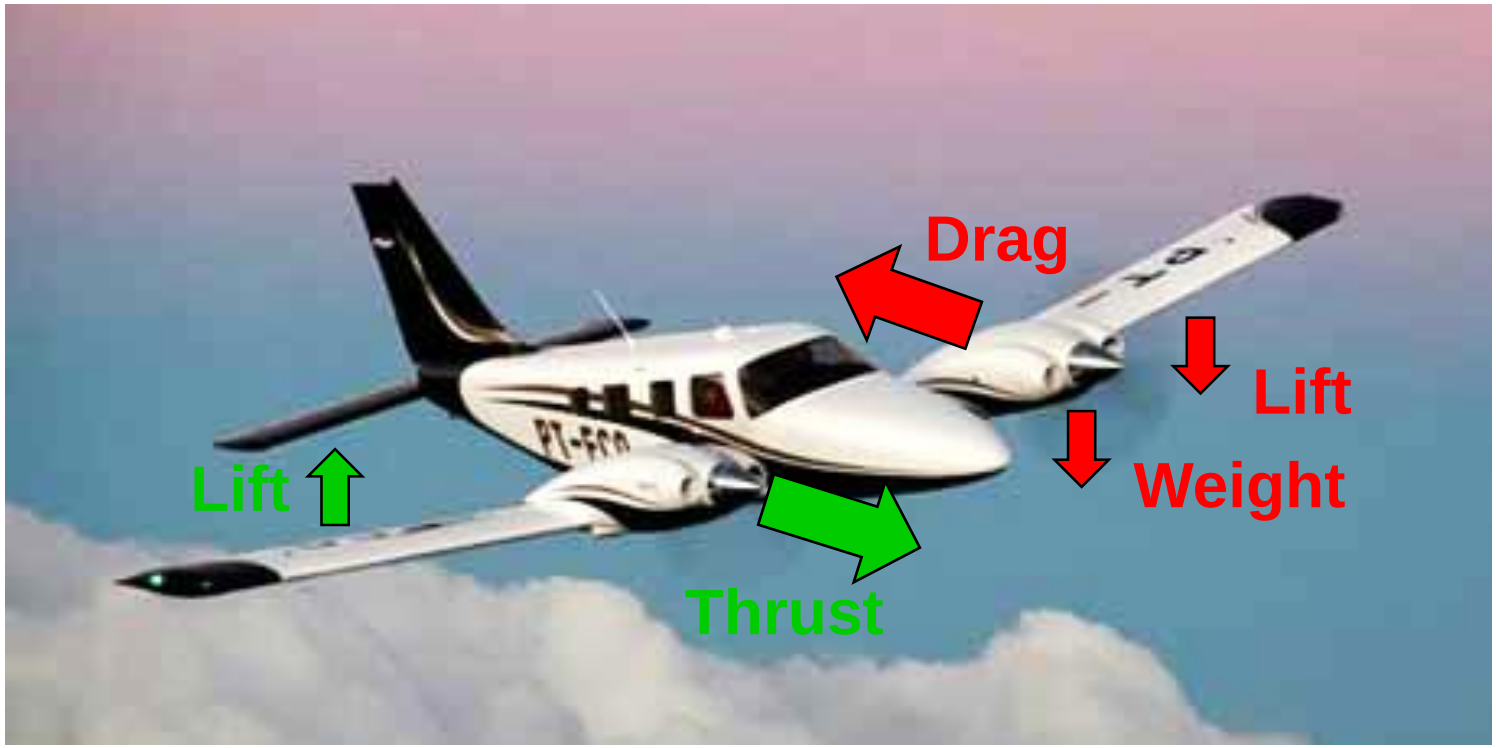
Yes, But Two Engines Are Still Better Than One

QUICKLY…

1. Lots of right rudder to stop the aircraft yawing to the left.
2. Lower the nose to maintain airspeed with reduced power.
3. Feather the port propeller to reduce drag.

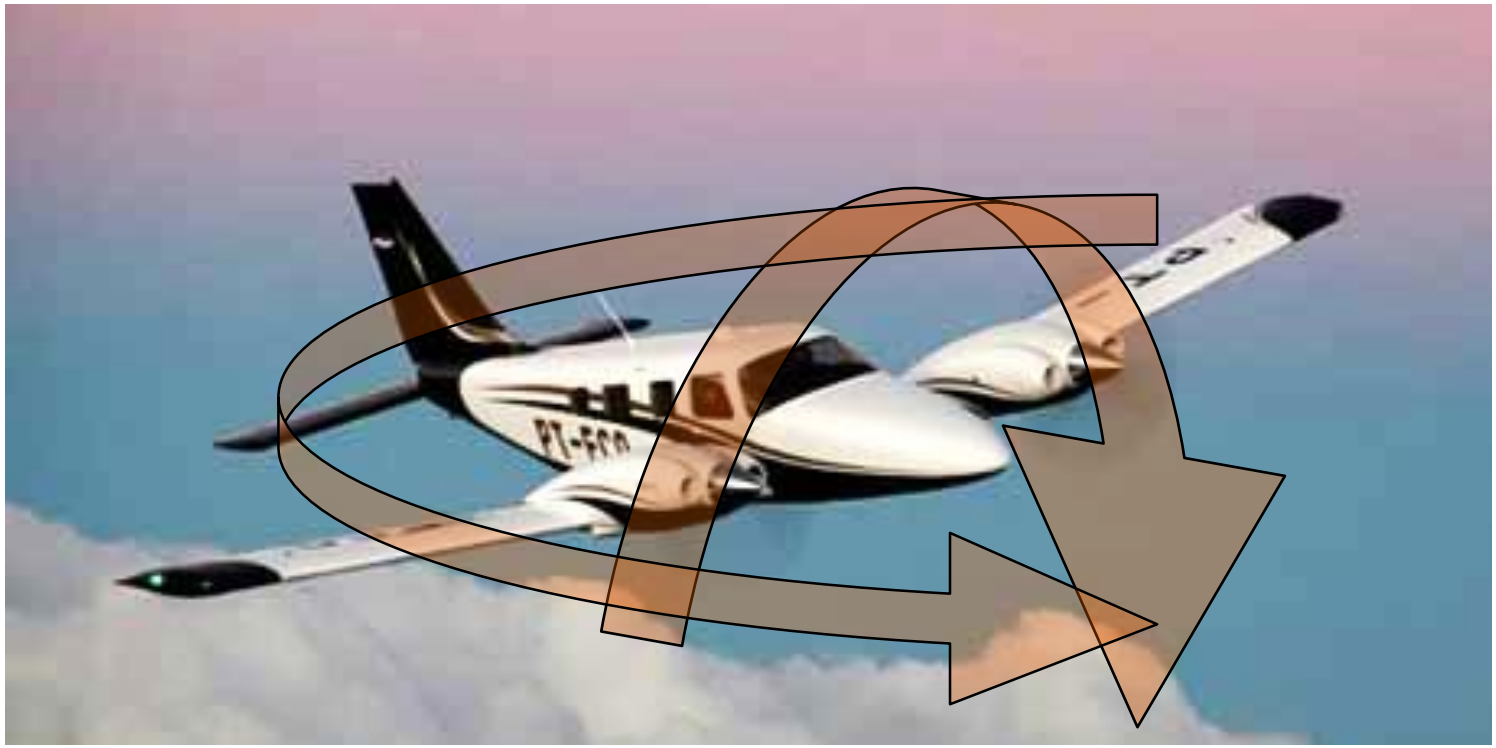
Yes, But Two Engines Are Still Better Than One

If you don't……



Two Engines Are NOT The Whole Answer!

…You yaw and roll to the left, stall and spiral into the ground!
With an otherwise perfectly good aeroplane and one working engine.



Only One Engine

Now let's put you in the pilot's seat of the Piper Meridian M500…

Much lower probability of experiencing an engine failure.

Only One Engine

But….

Not ideal to know that we are going down but we KNOW that is what is happening and we have a simple plan of action…

Only One Engine

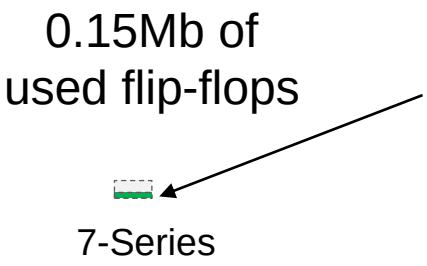
1. Lower the nose to maintain airspeed for best glide range.
2. Look for somewhere suitable to land.

Only One Engine

With *minimal* effort needed to continue flying….

3. Feather propeller to reduce drag.
4. Use available time to see if there is anything you can do to restart the engine.

Upsets in ‘Data’ Flip-Flops

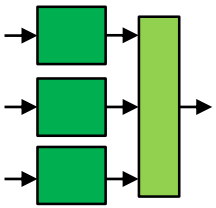


Flip-flops in *Xilinx FPGAs* are the *lowest risk* but if their contents are really that critical then you must include mitigation in *your* design. But can your design truly improve the reliability without making things worse?

Mitigation schemes typically employ one or combinations of the following…

- Parity bits and calculations for detection.
- ECC bits and calculations for detection and correction.

- Dual Modular Redundancy (DMR) detects errors but not location.
- Triple Modular Redundancy (TMR) detects and can isolate failing module.

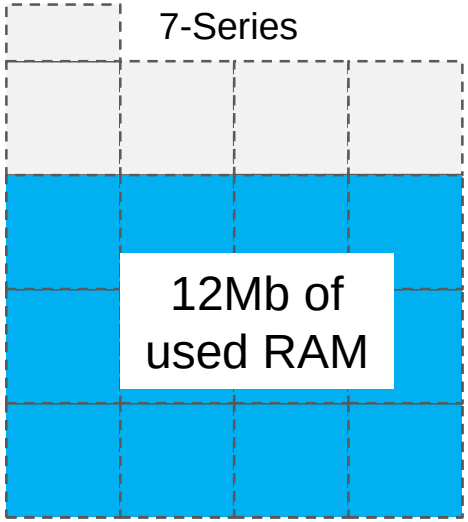


Key Observations

- All schemes increase design size and therefore *increase* underlying upset rates.
- Watch out for single and common points of failure: where is the weakest link?
- Extreme care needed to avoid introducing ‘complexity related failures’ (*emulate*).

- In-circuit error detection and/or correction should reveal anything you really care about so these schemes should, by default, cover all ‘critical bits’.

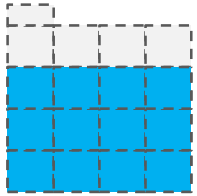
Upsets in ‘Data’ RAM



Mainly driven by sheer quantity, the risk of data corruption in memory is significantly greater that that held in flip-flops.

BRAM has multiple applications…
- Data and sample storage (RAM)
- Data buffers (e.g. FIFO mode)
- Program memory (ROM)
- Coefficients and Tables (ROM)
- State Machines (ROM)

16nm UltraScale+



If you care about BRAM contents then you must provide mitigation in *your* design.
In this case Xilinx have provided you with ECC protection…

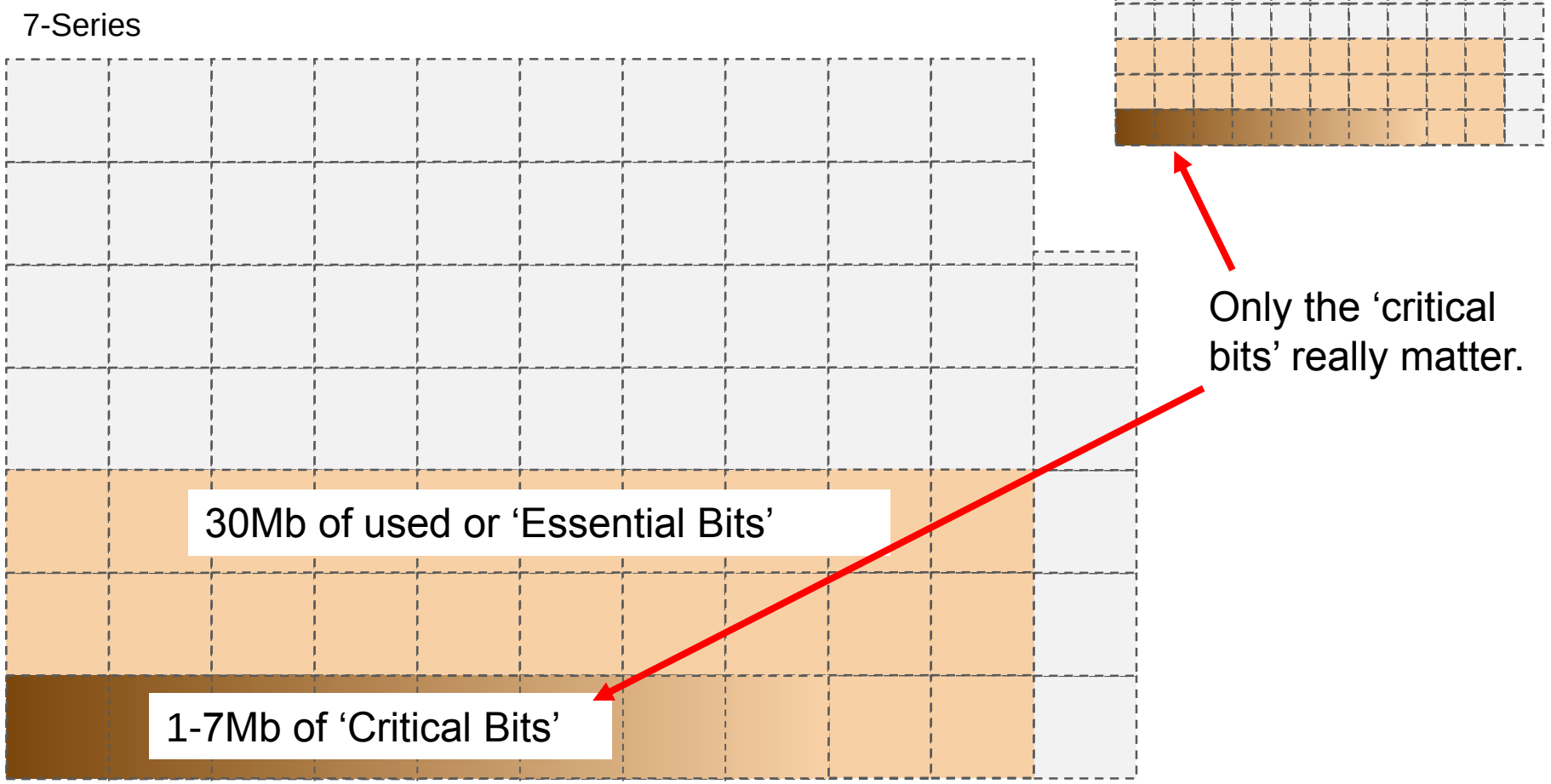
- Every BRAM has this option; you decide where and when to enable it.
- 64-bit data with 8-bit ECC (Simple Dual Port and FIFO).
- 4-way physical interleaving of memory cells.

Key Observations

- Zero un-correctable errors observed during any real SEU testing.
- Very unlikely that any redundancy schemes would improve reliability.
- ECC corrects a value as it is read so consider writing back ROM contents.

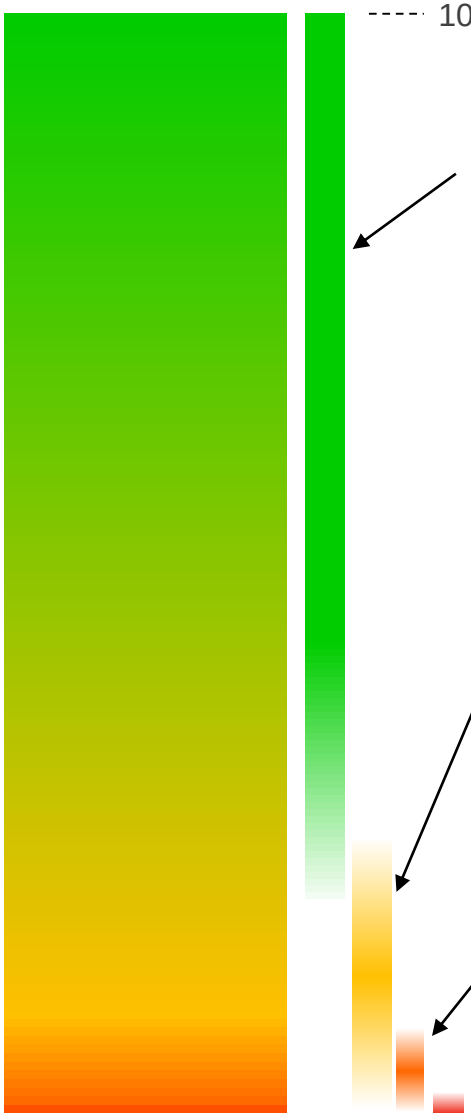
Upsets in Configuration

The ‘Engine’ is becoming ever more reliable..



Built-in error detection and correction means that the vast majority of upsets only result in a *temporary* soft error (e.g. 4.6ms to 70.7ms in 7-Series).

Categorisation of Configuration Upsets



Observed results for a variety of real applications
(normalised for device utilisation)

60-80% Completely miss the design so have no effect.
- All detections are reported.
- Be careful NOT to overreact and lower reliability.
- 'Essential Bit Mask' can classify upset locations.

10-40% 'Touch' the design.
- Typically less than 1 in 3 have any effect.
- Be careful NOT to overreact and lower reliability.
- Consider 'Prioritised Essential Bits Mask'

<10% will be observed to have any effect.
- 1% to 5% is a more typical observation rate.

<1% have an undesirable effect on operation.
- 'Critical bits' are those that really matter.

Exploit error injection (SEU simulation/emulation)
to learn and appreciate which circuits really matter.

Mitigation Of Configuration Upsets

1. Enable error detection and correction.

2a. Use SEM IP to emulate SEU and understand the susceptibility of YOUR design.
~1,000 random injections really will help you to appreciate what happens.
2b. Scale results using published soft error rates (UG116) and expected flux density.

Once you actually know what happens and you actually know what you need…

3. Choose a mitigation strategy.

4. Ensure that *everyone* knows what the strategy is and will implement it.

5. Implement your strategy.

6. Use SEM IP to emulate SEU and verify that your strategy works.
- Check that your 'pilots' know how to do their job and are not get confused!

Configuration Upsets: Do (almost) Nothing?

Situation ‘A’

You’ve evaluated the susceptibility and effects on your design and have determined that the ‘failure’ rate and nature of ‘failures’ are of an acceptable level.

Enable built-in error detection and correction and worry about other weaker links ☺

Situation ‘B’

You are totally paranoid about everything and need to keep operating correctly regardless of what happens. You have already decided that you cannot even accept an upset to a single flip-flop in your design so you have implement a TMR scheme.

Enable built-in error detection and correction.

Your design should be more than capable of looking after itself (but is it really?).

Auto correction means that configuration errors will be temporary.

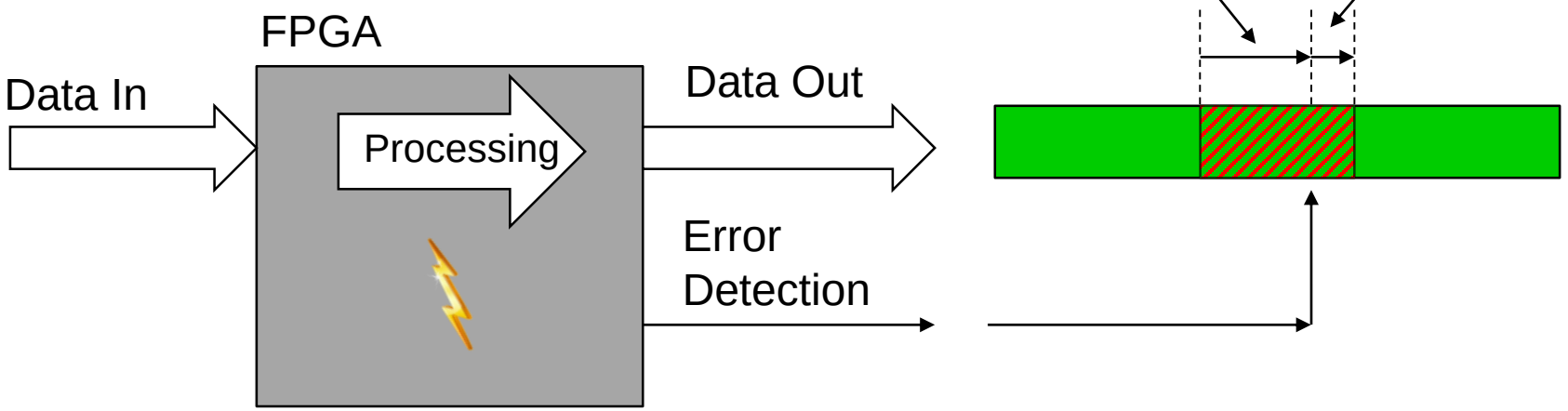
- No ‘dead engine’ to carry around after an event.
- Redundancy quickly restored reducing reliance on remaining module(s).

Configuration Upsets: Do (almost) Nothing?

Situation ‘C’

Of course it would be better if we didn’t have any errors but I can cope with a few just as long as I know about them. Silent errors are unacceptable.

Enable built-in error detection and correction.
Report and log errors (time stamps).
Consider discarding any potentially corrupt data.



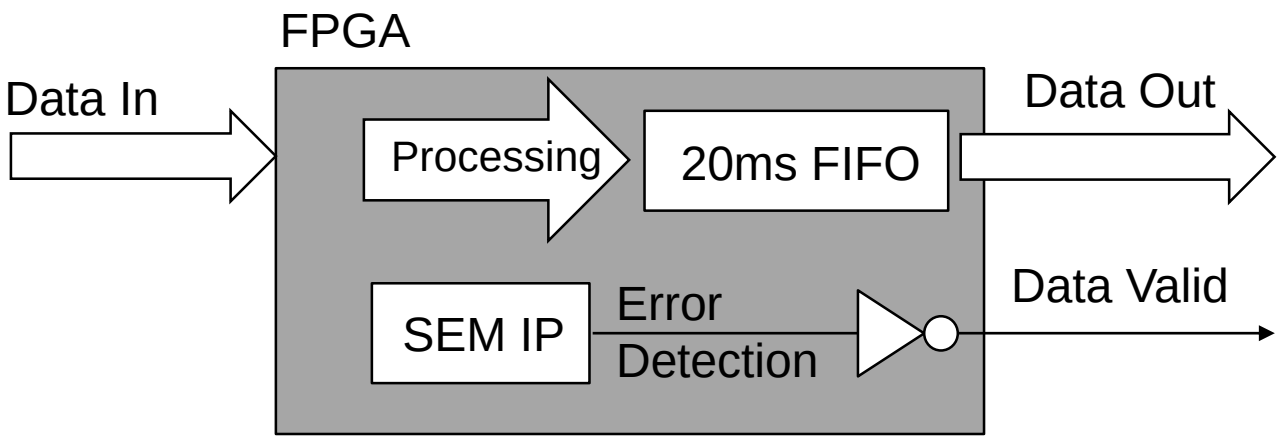
Was data at that time actually needed?
Can the data be received again?

Configuration Upsets: Do (almost) Nothing?

Situation ‘C’

Of course it would be better if we didn’t have any errors but I can cope with a few just as long as I know about them. Silent errors are unacceptable.

Enable built-in error detection and correction.
Report and log errors (time stamps).
Consider discarding any potentially corrupt data.



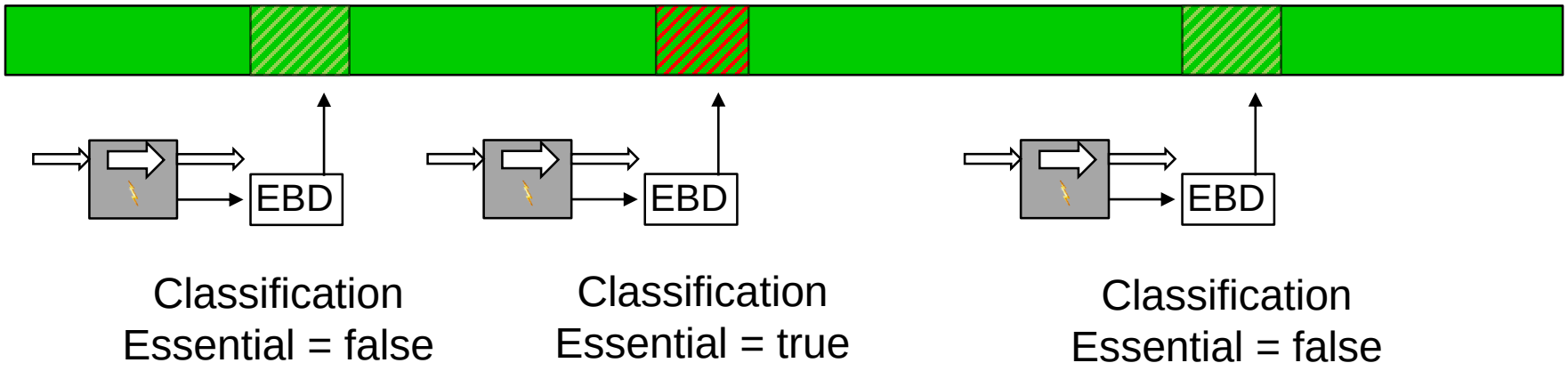
Inserting a delay equivalent to one Readback CRC scan period of the device would ensure that validity of presented output data is ensured.

Configuration Upsets: Error Classification

Situation ‘D’

I’m Ok discarding some of my data but I don’t want to discard too much.

Enable built-in error detection and correction.
Report error locations and timestamps.
Use ‘Essential Bits’ or ‘Prioritised essential Bits’ to classify each location detected.
Only consider discarding the data that has a higher probability of being corrupted.

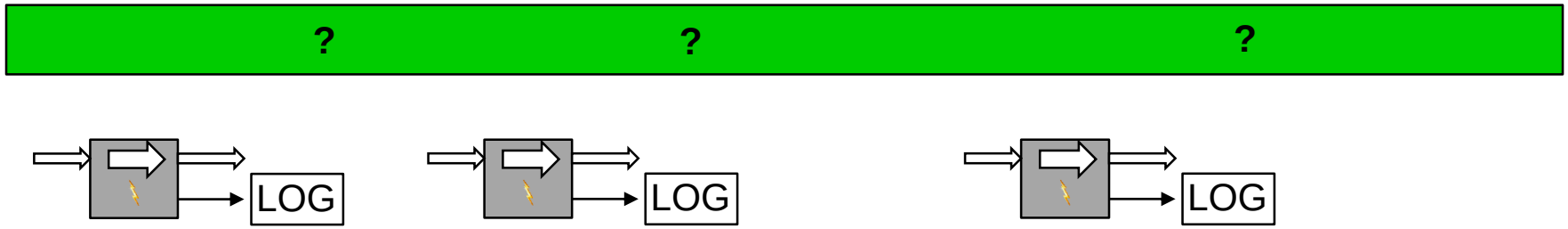


Configuration Upsets: Error Classification

Situation ‘E’

When I run an experiment I don’t want to discard anything that could be important during analysis.

Enable built-in error detection and correction.
Report and log errors including locations and time stamps.



Post Collection Data Validation

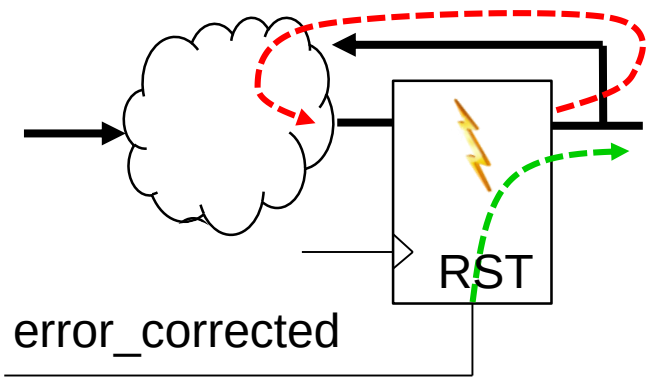
- Use ‘Essential Bits’ or ‘Prioritised essential Bits’ to eliminate ‘false alarms’.
- Evaluate if data associated with remaining events could be useful.
- Exploit error injection to evaluate likelihood that upset location corrupted data.

Configuration Upsets: Local Reset

Situation ‘F’

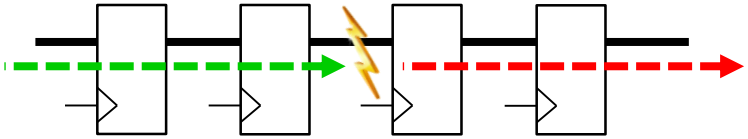
I can tolerate a temporary interruption to service but need high certainly of correct operation following the event. I can’t afford TMR and/or I don’t want to implement it!

Enable built-in error detection and correction.
Use report of error correction to *locally* ‘reset’ circuits with **feedback**.
Where possible arrange ‘reset’ to reinforce the normal operational state.
Use ‘Essential Bits’ to reduce interruption rates (but only if required).



e.g. A state machine could be forced into a different state and then remain in one or more incorrect states for a prolonged period.

A pipeline will ‘flush through’



⇨ High quality of design is vital (i.e. be very careful not to make things worse!)
e.g. ‘Global asynchronous resets’ should be forbidden!

What Did The Space Program Ever Do For Me?

XILINX®

Radiation-Hardened, Space-Grade Virtex-5QV Family Overview

DS192 (v1.3) March 8, 2012 — **Product Specification**

Table 1: **Virtex-5QV FPGA Family Members**

Device	Configurable Logic Blocks (CLBs)				DSP48E Slices(2)	Block RAM Blocks			CMTs (4)	Endpoint Blocks for PCI Express	Ethernet MACs(5)	Max RocketIO GTX Transceivers (6)	Total I/O Banks (7)	Max User I/O(8)
	Logic Cells	Array (Row x Col)	CLB Slices (1)	Max Distributed RAM (Kb)		18 Kb (3)	36 Kb	Max (Kb)						
XQR5VFX130	131,072	200 x 56	20,480	1,580	320	596	298	10,728	6	3	6	18	24	836

Table 2: **Radiation Tolerances**

Symbol	Description	Min	Typical	Max	Units
TID	Total ionizing dose: Method 1019, dose rate 300 rad(Si)/sec	1	–	–	Mrad(Si)
SEL	Single-event latch-up immunity: Heavy ion linear energy transfer (LET) threshold	100	–	–	LET (MeV-cm^2/mg)
SEFI	Single-event functional interrupt GEO 36,000 km typical day	–	2.76E-07	–	Upsets/device/day
SEU_{CFG}	Single-event Upset in Configuration Memory: GEO 36,000 km typical day. Total bits: 35M	–	3.80E-10	–	Upsets/bit/day

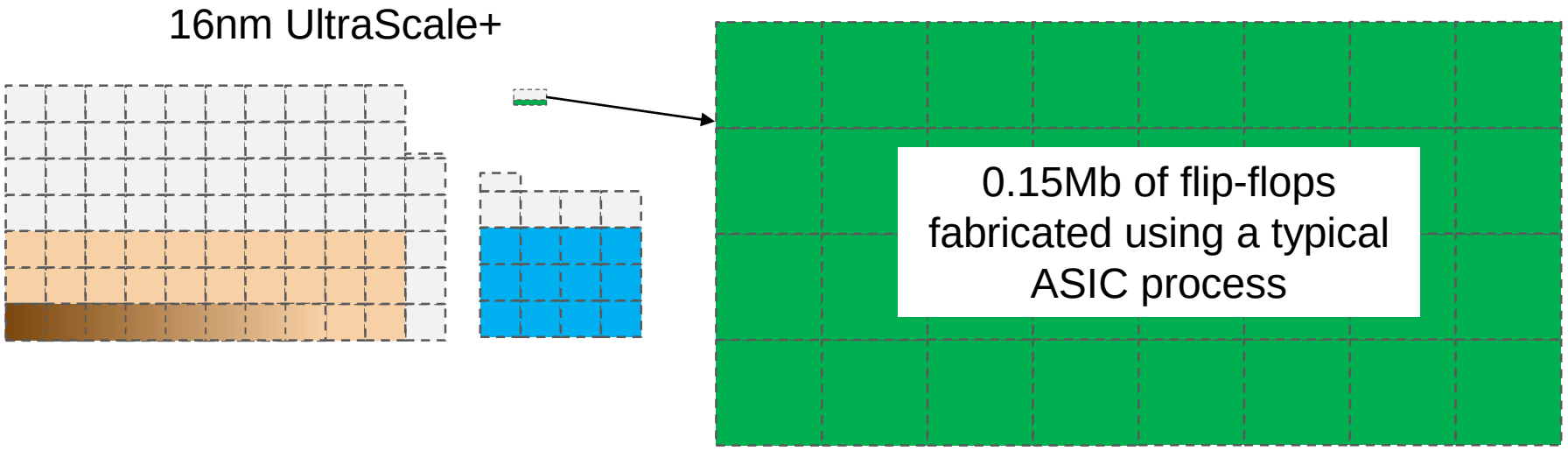
MTBF

9,926yrs

75 days

- **Great for space and very special situations but is it affordable?**
- **Standard products have benefitted from our space program.**
- ***Engineer* solutions for lower cost.**

The ‘Game’ has changed…



Implement a mitigation scheme that actually mitigates the highest risks.