2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Whose fault is it? Advanced techniques for optimizing ISO 26262 fault analysis

Avidan Efody,
Mentor Graphics Corp.

Motivation

- ISO 26262 requirements for fault analysis
  - Similar requirements from other standards
- Requirements from mission-critical domains
  - Data center
  - Networking
  - And many more
- No end-to-end how to available

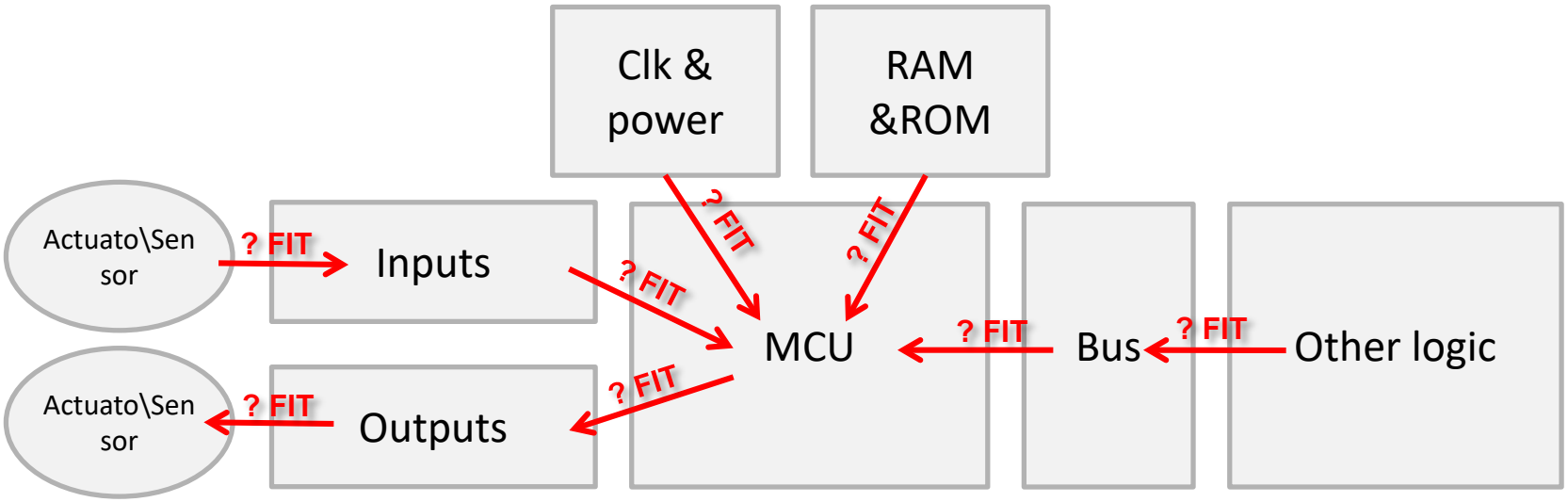
2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Agenda

- The problem
- Solution requirements
- Proposed solution

The problem : concept

- Safety concept is developed at high level
  - Failure In Time (FIT) budgets per part
  - Technical assumptions on IP (SEooC)
  - Safety mechanisms

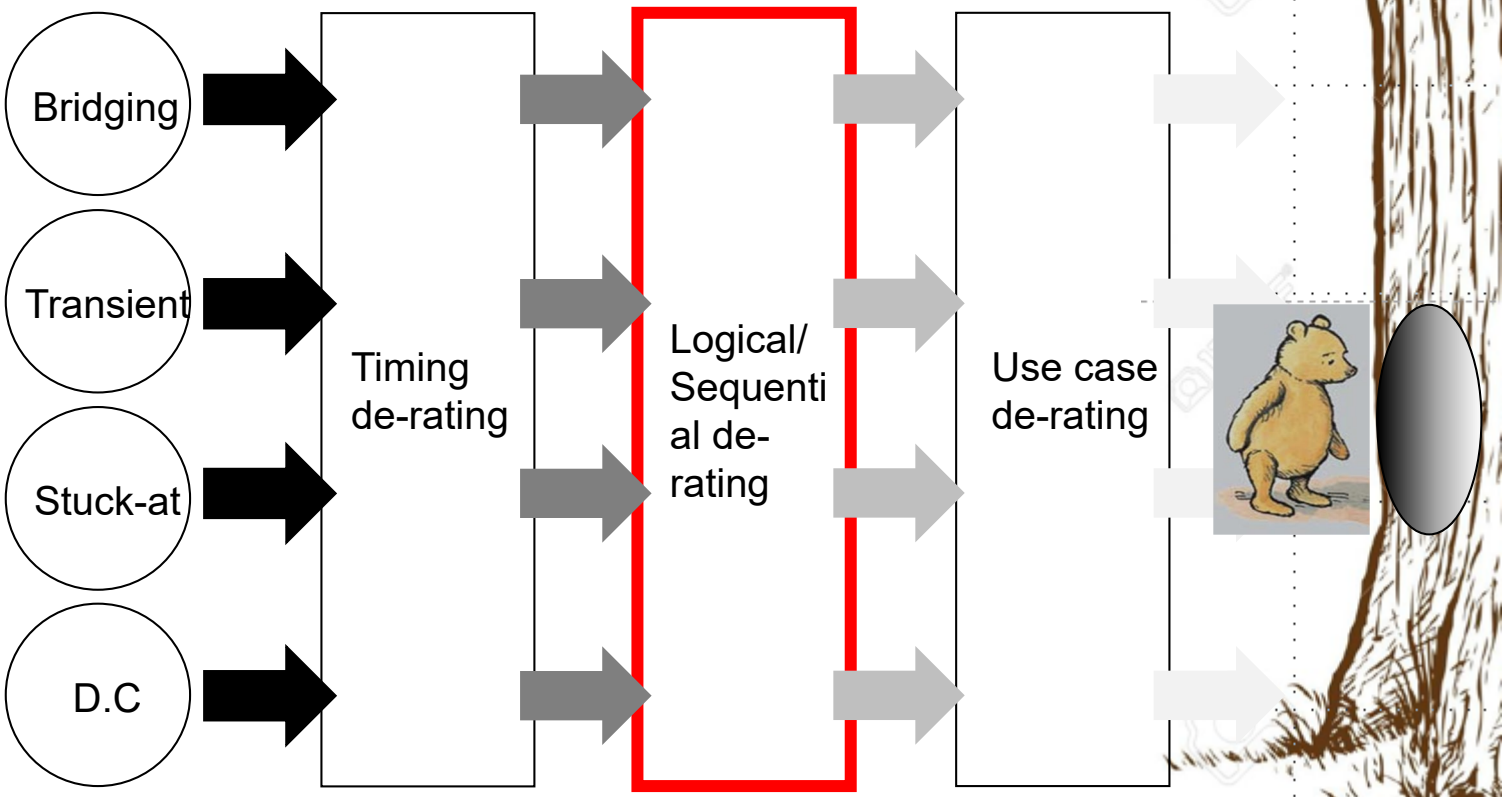


The problem : element requirements

- IP requirements derived from system analysis:
  - Contribution of element to overall FIT<10%
  - <10% of faults are single point/residual
  - Debug logic not used in safety-critical operation
    - Faults in debug logic are safe
  - More…

The problem: typical flow

- Once implementation is in place its FIT must be accurately measured



The problem: FIT doesn't fit

- What if FIT doesn't fit?
- Iterations are expensive
  - Re-plan, re-design, re-verify
  - Schedule delays

Solution requirements

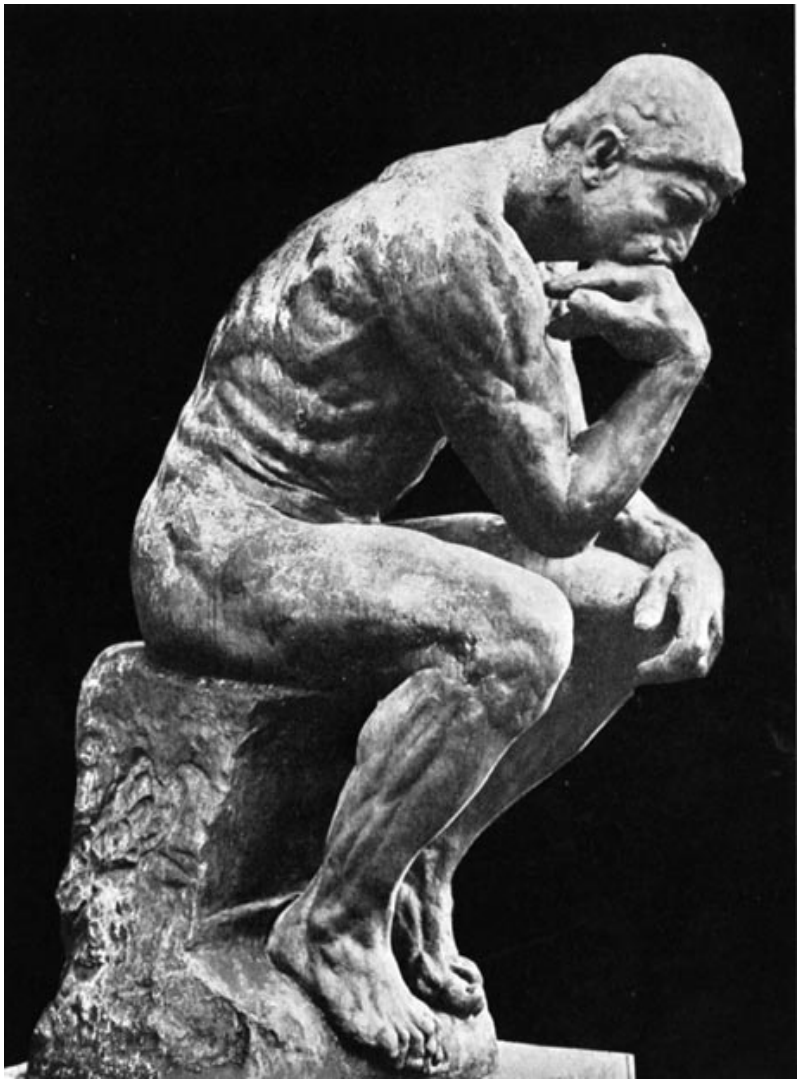
- Accuracy/cost trade-off
- Statistical strength
- Integrated with overall verification
- Seamless abstraction switch
- Multi-platform

Proposed solution

- Statistical sampling of faults
  - Population
  - Sample size
  - Fault points
  - Analysis
    - Traditional method
    - Avoiding reruns
    - Avoiding diff/duplication
    - Multi platform
  - Probabilistic metric

Population

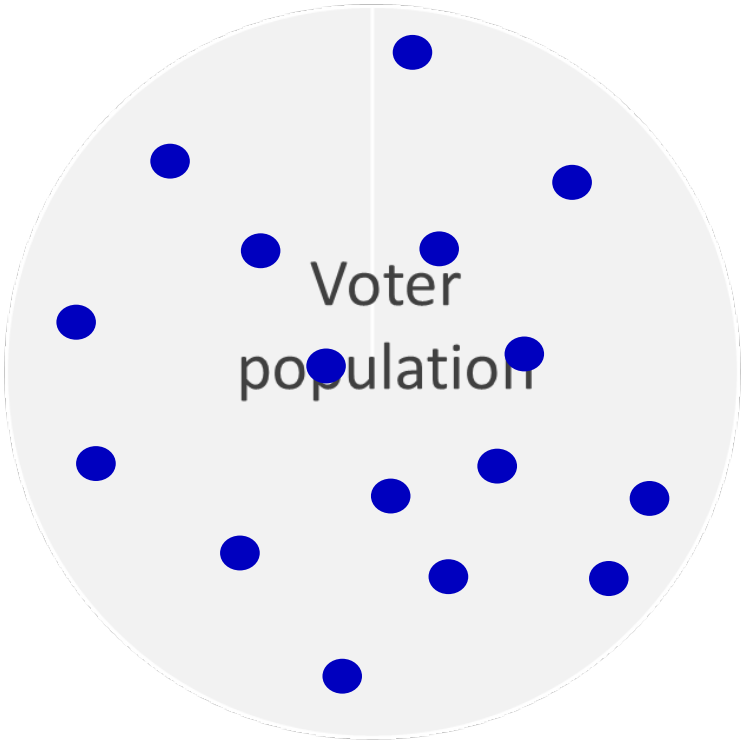
- = **test** X **cycle** X **signal**?
- Good enough:
  - Rigorous RBV
  - Interesting states covered
  - Biased to corner cases
- But:
  - Fault analysis leads to more stimuli requirements

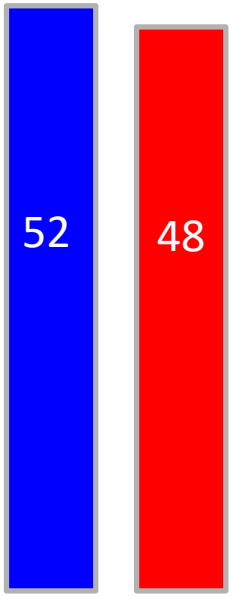


Sample size

- Variance $\propto 1/\sqrt{N}$
  - Brute force method
- Sanity check:
  - $\propto$ De-rating factor
  - Let some faults -> Failures
- Final analysis:
  - $\propto$ required accuracy
- High level trade-off
  - Analysis cost <> design cost

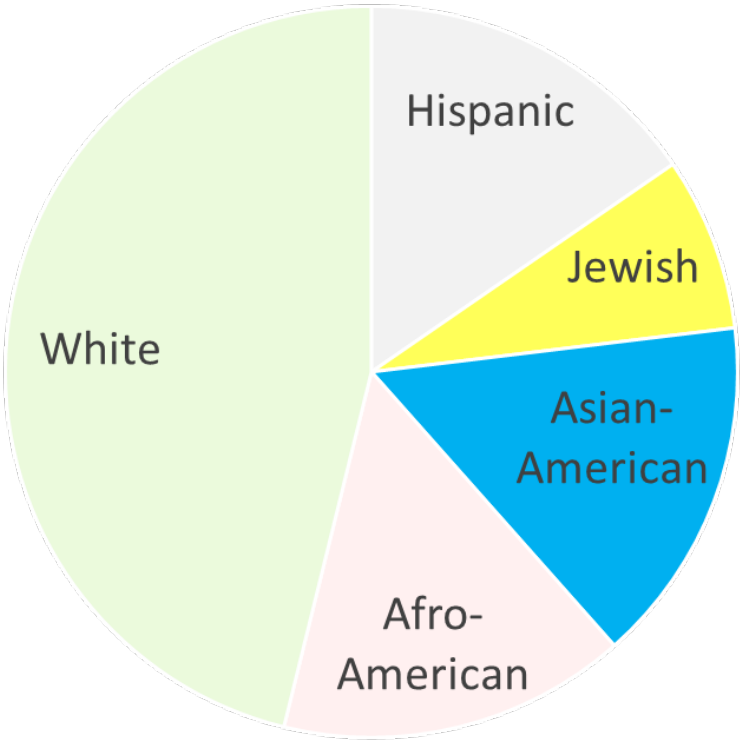
Fault points

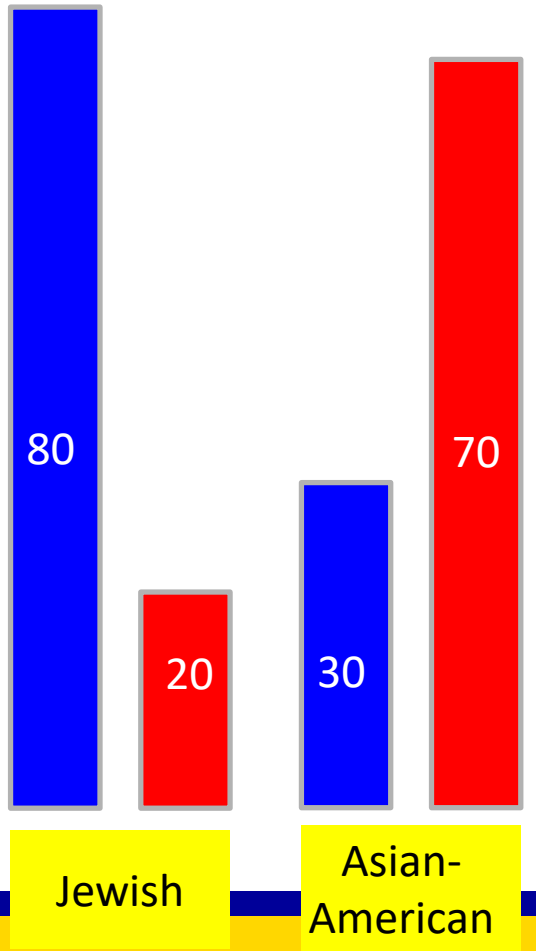




Fault points

- Smaller variance -> cheaper analysis
  - Segmentation of population helps



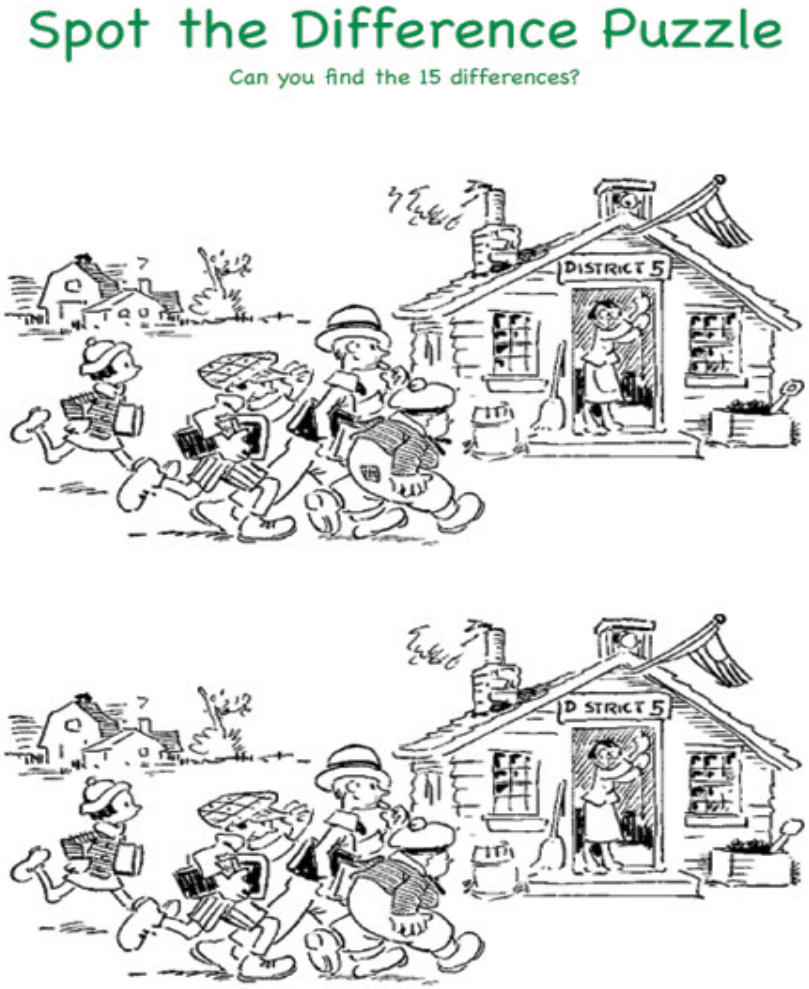


Fault points

- Transient faults
  - SET – in logic
  - SEU – in memory
- Makes sense to separate
  - SET de-rating is lot higher
- Also, cell FIT ratio different
  - FF/Mem FIT rate higher
- Separate statistics
  - Smaller variance
  - Smaller cost

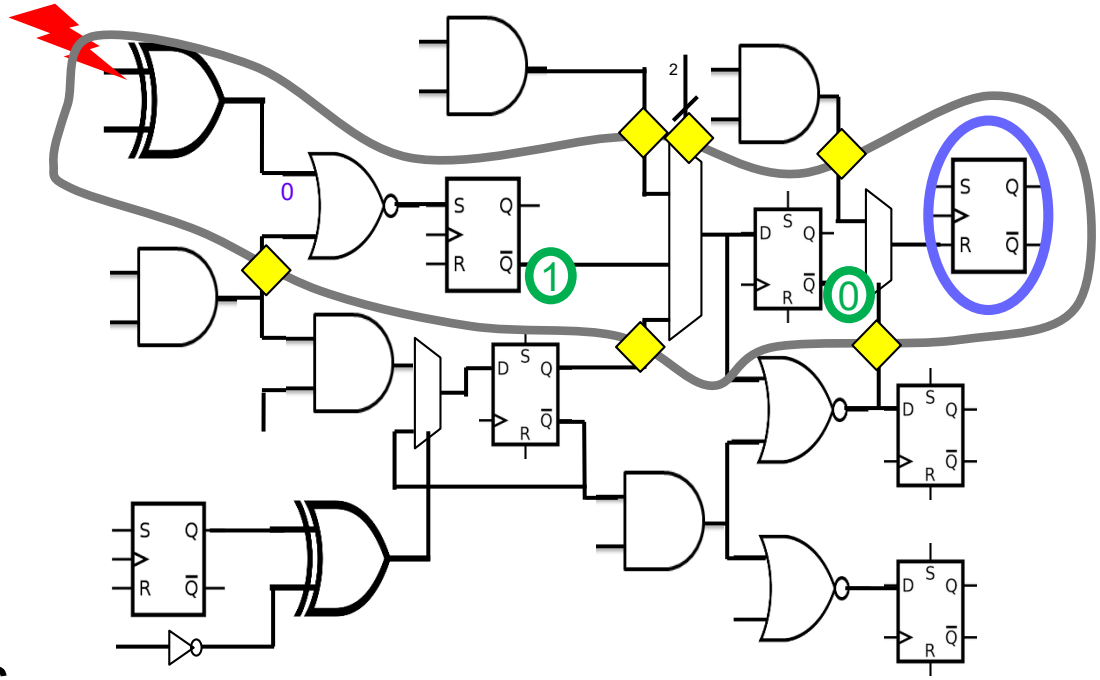
Analysis : Traditional flow

- Run reference test
- Rerun test with fault
- Diff safety critical
- How can we optimize that?



Analysis : Minimize scope

- Time scope:
  - Fault time -> 0
- Design Scope:
  - ∩ between:
    - Fault point fan-out
    - Safety critical fan-in
- Stimuli
  - Initialize FFs, Mems
  - Scope inputs forced

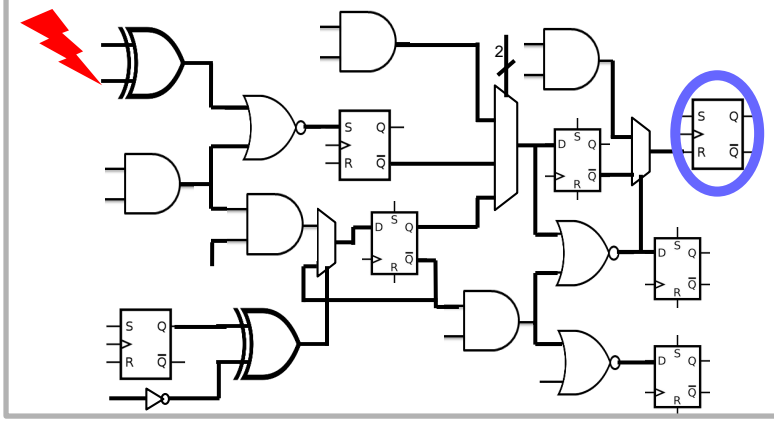


Analysis: Minimize compare

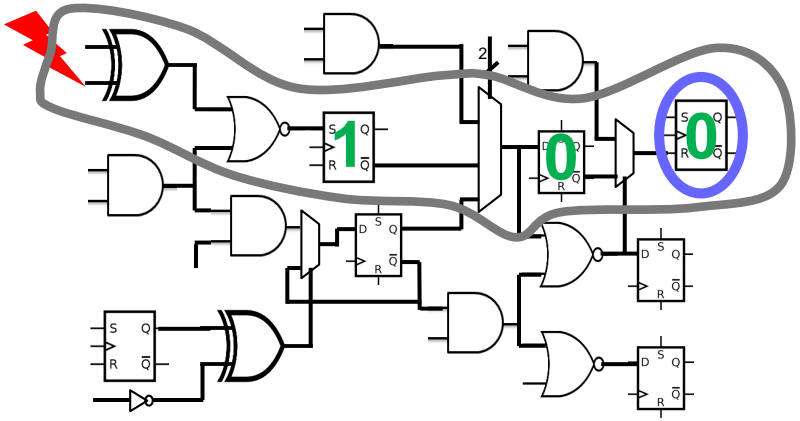
- RTL simulators already have a way to capture undefined state…
  - Good tool support
  - Attention to X optimism/pessimism (at RTL)

Analysis: decision

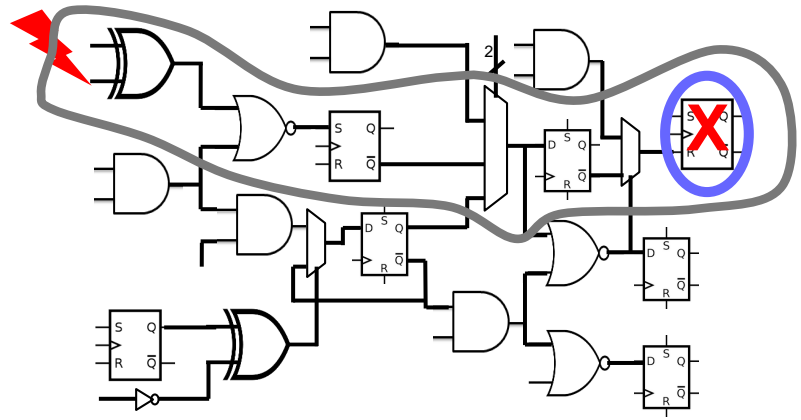
T=0



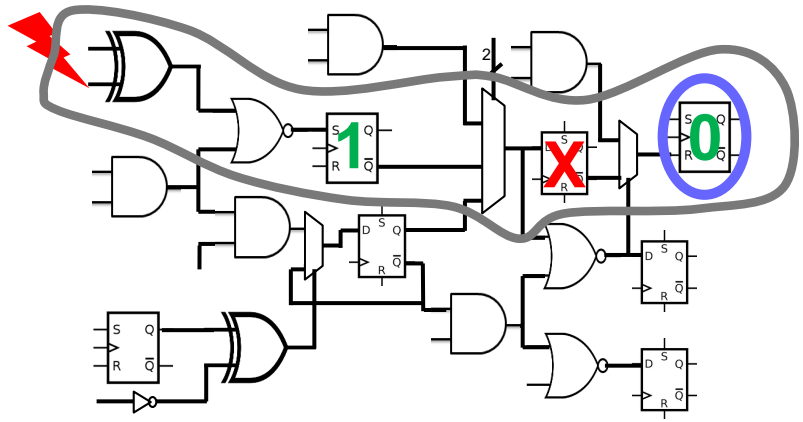
T=10 => MPF



T=10 => SPF or RF



T=End => USER



Analysis : abstraction

- RTL or structural gate?
  - SET
    - Structural gate to 1st FF
    - RTL from there
  - SEU
    - RTL all the way
- Requires RTL->GL flop mapping

Analysis: multi platform

- Emulation/prototypes can fit in flow if:
  - Results can be reproduced
  - FFs/Memories can be dumped
  - Signals into scope can be logged
- Combine platforms strengths
  - Emulation/prototyping for long runs
  - Simulation for X injection

PMHF

- Example, assume no SM
- Outputs of above:
  - SEU SPF rate +/-
  - SET SPF rate +/-
- PMHF:
  - (SPF RATE) * (# of FF) * (FF FIT) + …
- Probability of PMHF < Target
  - Target – PMHF >= 5σ => 0.9999997
  - Target – PMHF >= 7σ => 0.99999999998

2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Summary

- Fault simulation is an interesting challenge
  - There's more than just diff to it
  - Requires upfront consideration/planning
  - And an end-to-end flow
- Hopefully this paper will help…

Thanks