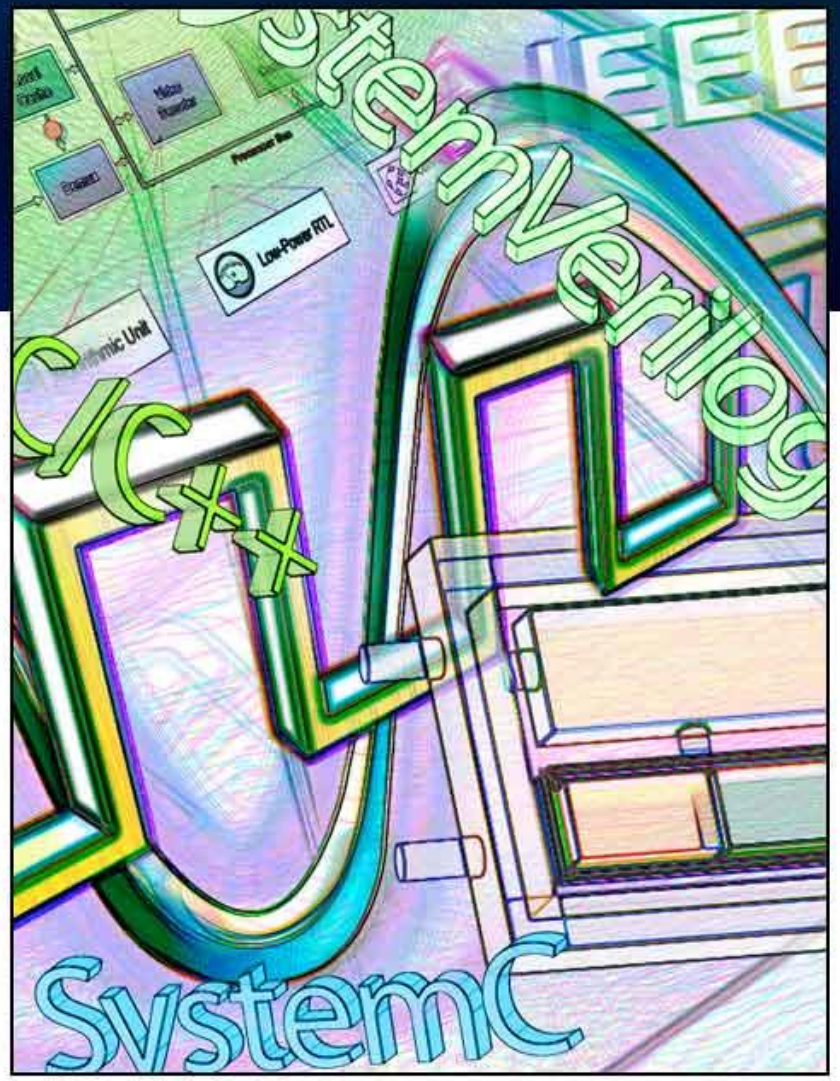


Fault analysis – what is your real FIT size?

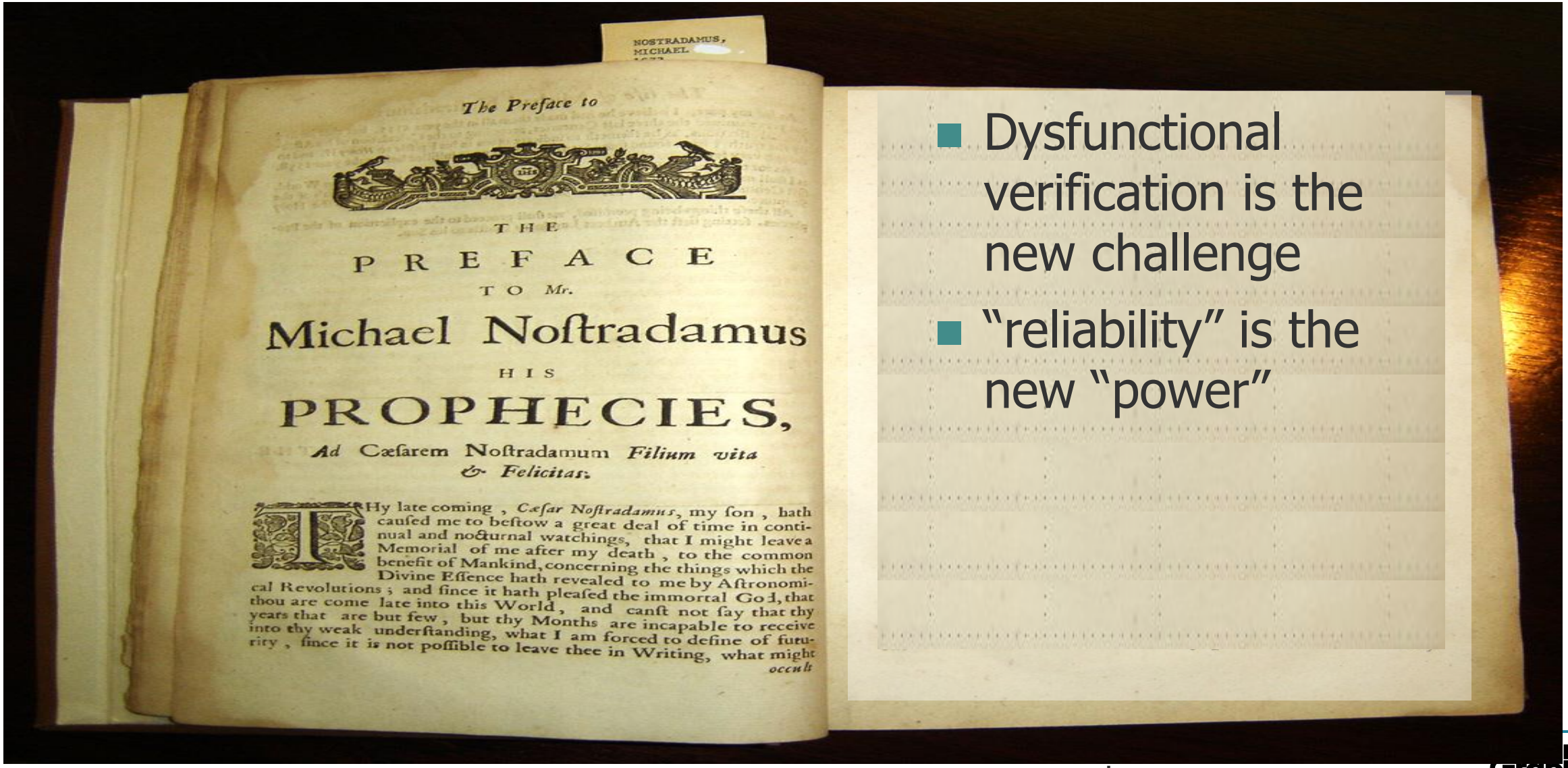
Avidan Efody,

Automotive Solutions Architect,

Mentor Graphics

Mentor Graphics®

Verification Futures



- Dysfunctional verification is the new challenge
- "reliability" is the new "power"

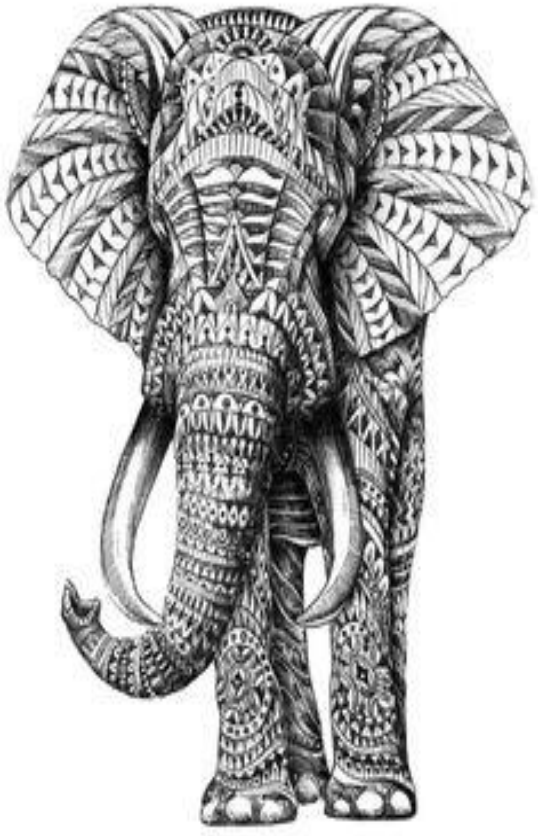
Dysfunctional verification

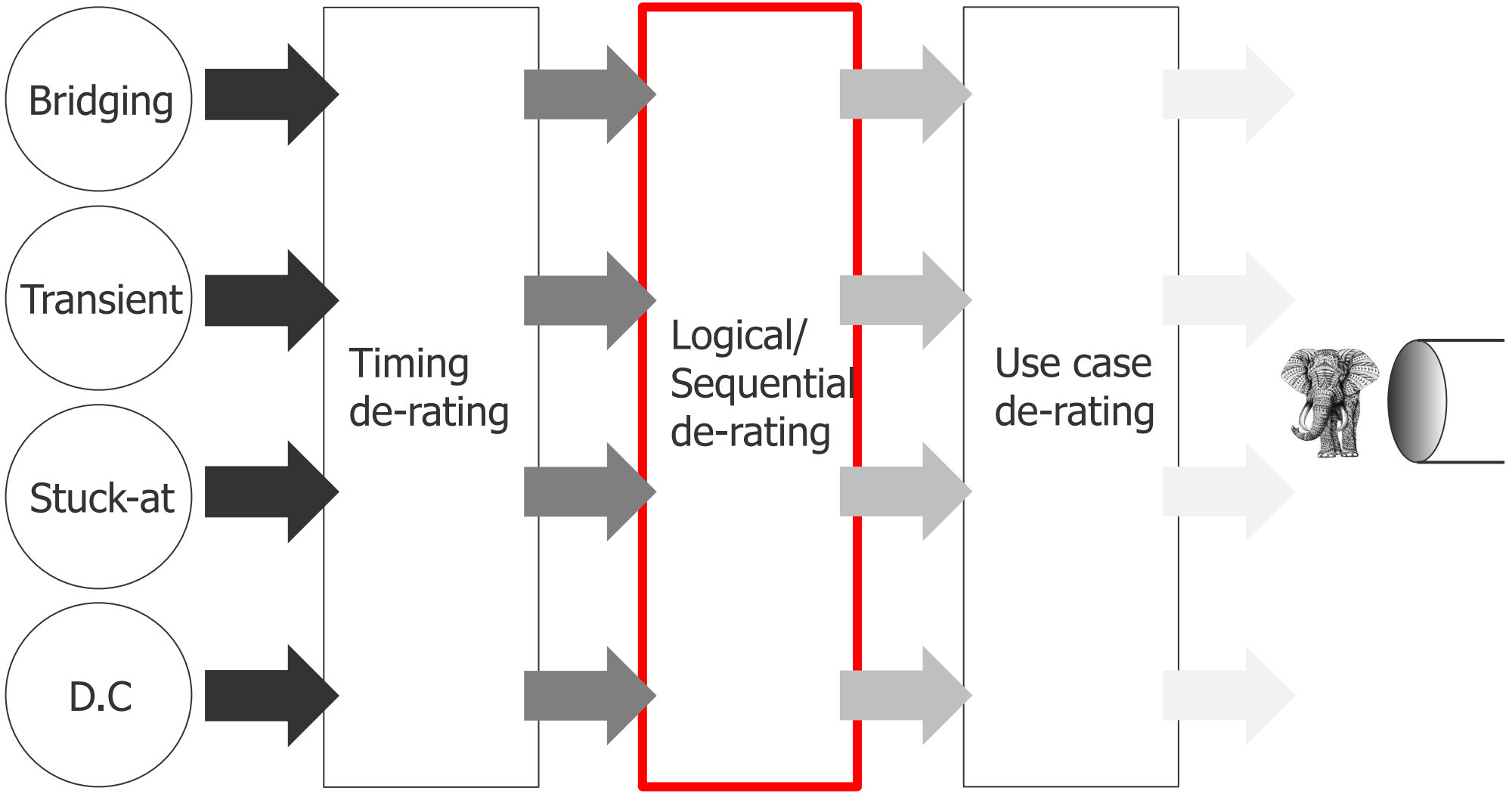
- Functional verification
  - Focuses on specified conditions
  - Even errors are "specified errors"
  - "non-specified" errors below cutline
- Dysfunctional verification
  - All non-specified errors
  - SM changes state without reason
  - Memory address changes
- Nothing is the same
  - What is the stimuli?
  - What is meaningful coverage?
  - How do you analyze results?

Dysfunctional verification basics

- Aim:
  - FIT/MTBF < threshold
- Means:
  - Check statistical sample of faults
  - Determine safe/dangerous per fault
- Vocabulary:
  - Fault/error/failure
  - Fault model
  - Base FIT
  - De-rating

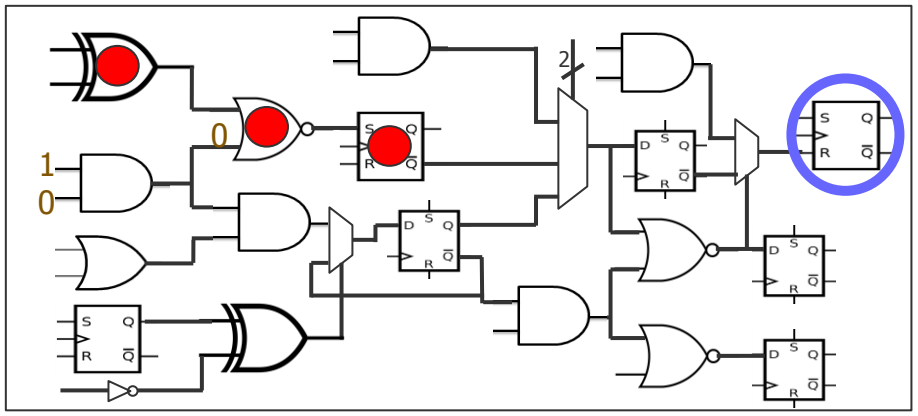
Dysfunctional verification flow



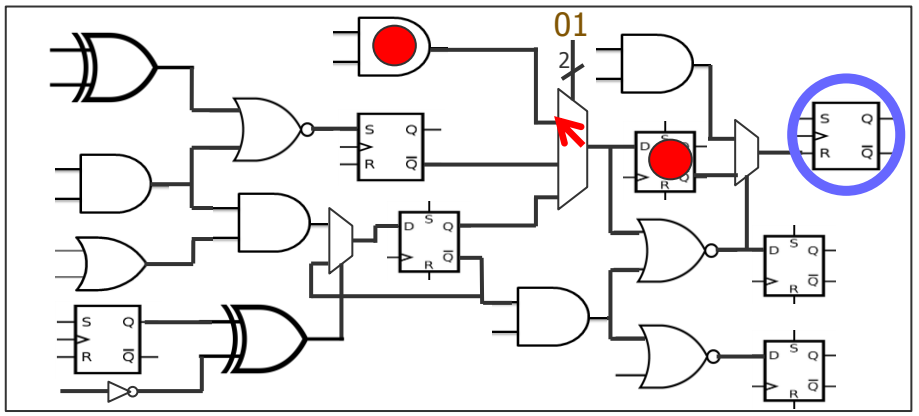


Dysfunctional verification analysis

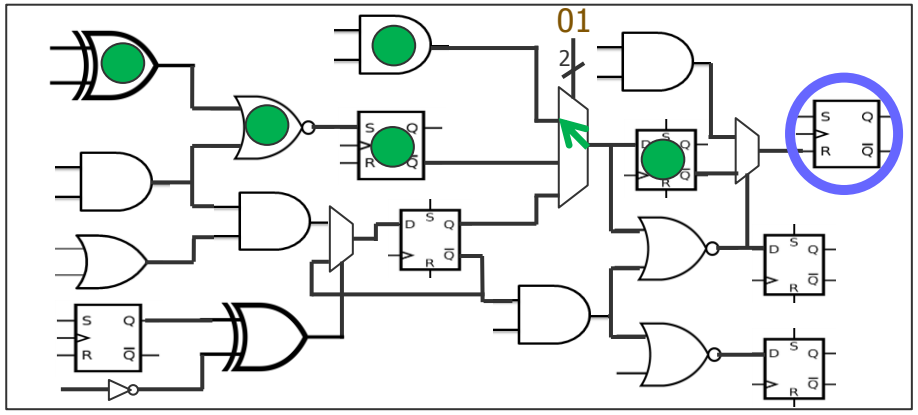
T=0
Fault->
Error



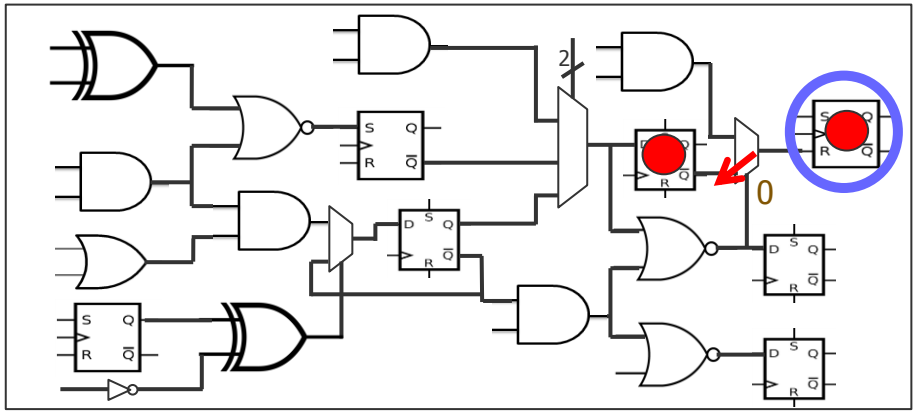
T=100
Fault->
Error



T=1
Error
masked

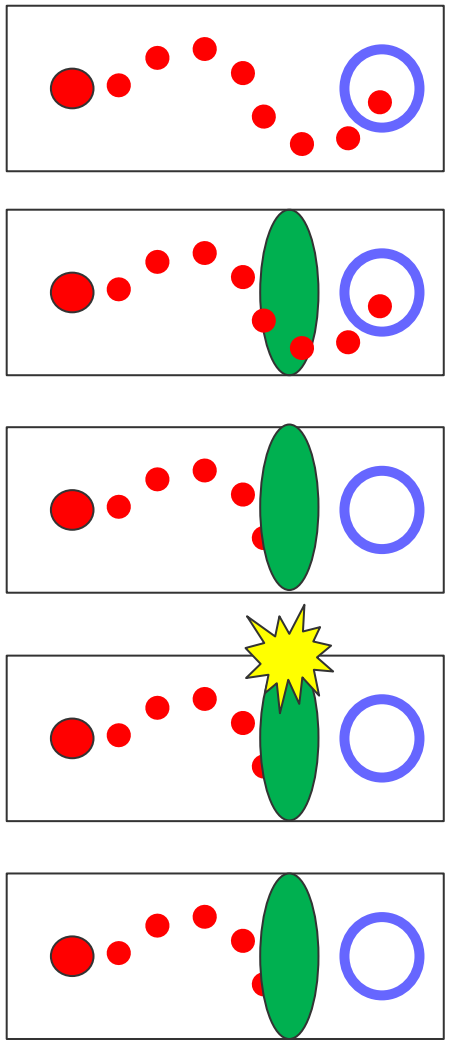


T=101
Error->
Failure



- Similar to x-propagation problem
  - X propagates to flop -> Error
  - X propagates to outputs -> Failure

Dysfunctional verification metrics

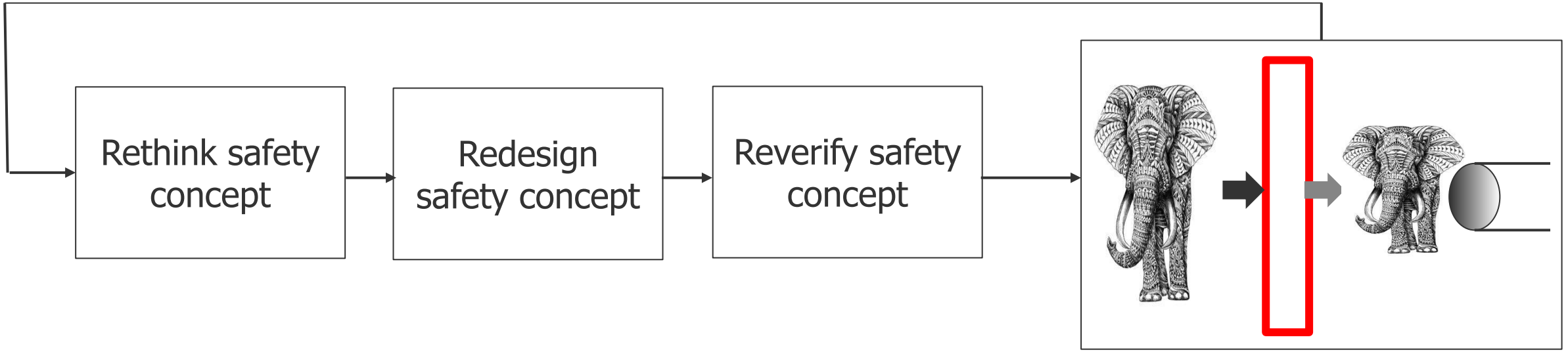


- Single Point Fault
  - No safety mechanism
- Residual Fault
  - Safety mechanism miss
- Multi Point Fault
  - Safety mechanism hit*
- Detected MPF
  - MPF + alarm
- Latent MPF
  - MPF + no alarm

- Mom's genius:
  - Assume stuck-at and periodical test pattern. Is stuck-at detected MPF or SPF?
  - How would you categorize a transient that is logically masked? Sequentially masked?

Zoom out to complete flow

- What happens if we can't squeeze that elephant in the hole?



- Similarities with power:
  - Concept at high level
  - Successive refinement
  - Accurate measure at RTL/Gate
  - Problems discovered late

Wrap up

- Safety can't be added-on, must be built-into flow
  - A vertical concern that must be considered in every step of the flow
- Challenges:
  - Smooth safety flow across level of abstraction
  - Dysfunctional verification alongside functional verification
  - And many more not discussed here…
- Safety/Security concerns are great news for all of us!

www.mentor.com

Fault analysis at RTL/Gate

- Metrics requirements
  - Produce report
  - ISO metrics
  - UCDB/VM integration
- Partner:
  - Yogitech
  - Astrel?
- Or build our own:
  - Little effort
  - Needs qual?

	Die		Package
	Permanent	Transient	Permanent
Total FIT (Raw FIT)	9.24	724.99	71.82
Safety related FIT	9.23	722.00	71.82
Probabilistic Metrics for random Hardware Failures - PMHF (in FIT)	0.06	2.00	0.13
Single Point Fault Metric - SPFM	99.36%	99.72%	99.81%
Latent Fault Metric - LFM	99.98%	NA	99.81%

ISO 26262 categorization as in ISO 26262:2011-10, 8.1.8

		Die		Package
		Permanent	Transient	Permanent
Total faults	λ	9.24	724.99	71.82
Total Safety Related faults	λ_{SR}	9.23	722.00	71.82
Total Not Safety Related faults	λ_{nSR}	0.00	2.98	0.00
Total Safe faults	λ_{S}	4.71	361.82	35.94
Total not Safe faults	λ_{nS}	4.53	360.18	35.94
Total faults with prob. of violate the SG	λ_{PVSG}	4.38	355.79	35.94
Total single point faults	λ_{SPF}	0.00	0.00	0.00
Total residual faults	λ_{RF}	0.06	2.00	0.13
Total Multi Point (ad)	$\lambda_{MPF}^{(ad)}$	0.14	NA	0.00
Total Multi Point (t)	$\lambda_{MPF}^{(t)}$	4.32	358.18	35.81
Total Multi Point detected faults	λ_{MPF_det}	4.46	NA	35.81
Total Multi Point latent faults	$\lambda_{MPF,l}$	0.00	0.00	0.00