Fault Campaign Framework for FuSa Verification of ISO 26262 Compliant Automotive Products

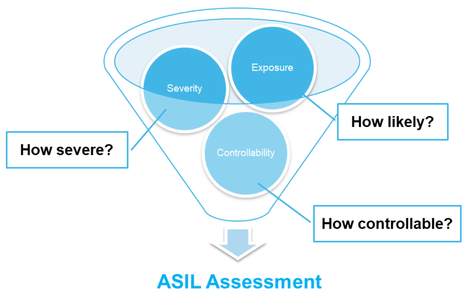
Prashantkumar Ravindra
Analog Devices
Prashantkumar.ravindra@analog.com

Mangesh Pande
Cadence Design System
mangesh@cadence.com

Vinay Rawat
Cadence Design System
vrawat@cadence.com

Introduction

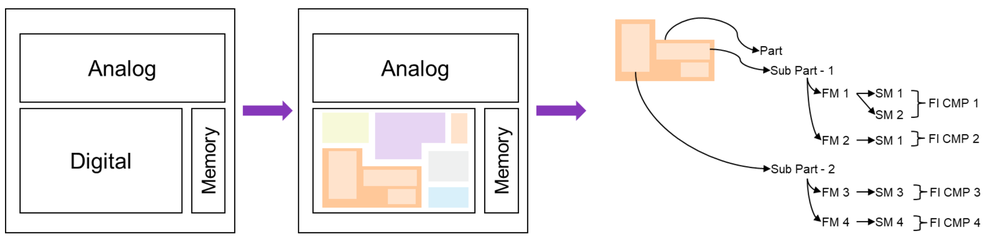
Electrification of Automobiles + Battery EVs = Complex Automotive Electronics
FuSa is critical to assure safety-critical systems offer risk reduction to ensure safety



ISO 26262 recommends Fault Injection as a methodology for

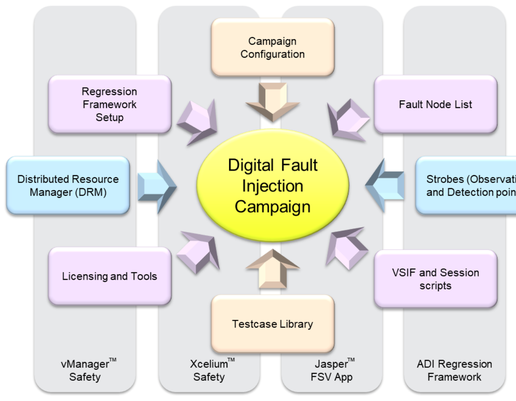
- Supporting the evaluation of the hardware architectural metrics
- Pre-silicon SM Verification

Planning a fault campaign to validate FMEDA metrics:

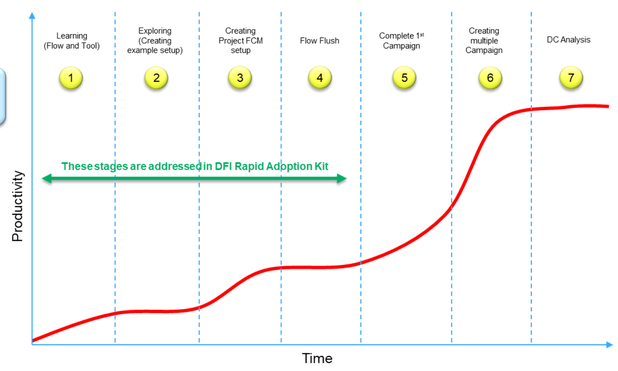


Challenges

- FMEDA is quantitative in nature, and this is over and above the SM verification
- FMEDA metrics validation requires highly automated EDA solution



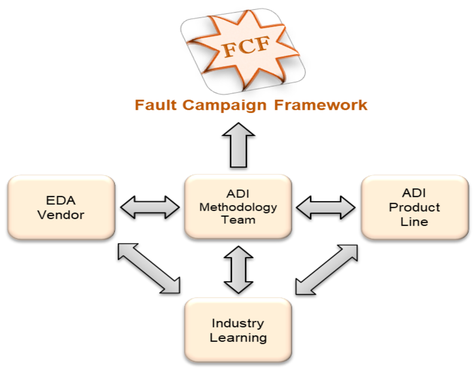
Time v/s Productivity Graph



Challenges:

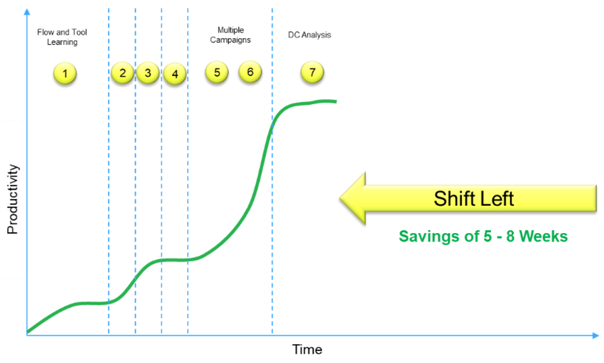
- Learning curve
- Setup bring-up time
- Setup complexities
- Flow failures
- Large fault node list
- Long campaign run-time
- Large set of UU faults
- Detailed analysis of fault/s

Fault Campaign Framework



- Standardized, Unified framework based on Cadence® Safety Solution
- Adapted for internal tools, flows and methodologies
- Agnostic to tool/scripting complexities

- Incorporate recommendations from
  - FuSa experts (Internal and Vendor)
  - Industry-standard practices
- Bring up project fault campaign setup *in less than a day*
- Flow failures are *easy to debug*



Fault Campaign Improvement Methodolgies

Fault Space Reduction — FST and FSV TC

FST Step

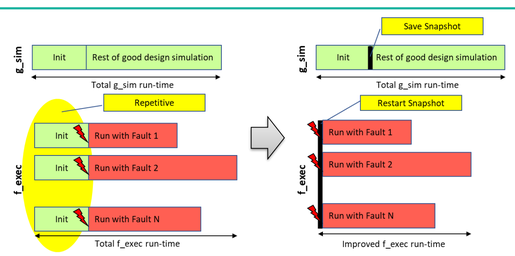
FSV Summary				
Total:	3973		(3973)	
Equivalent:	0			
Unobservable	725	[18%]	(725	[18%])
COI:	588			
Constant:	96			
Unpropagatable:	41			
Dangerous:	0	[0%]	(0	[0%])
Unknown:	3248	[81%]	(3248	[81%])
Unprocessed:	0	[0%]	(0	[0%])
Undetectable:	1579	[39%]	(1579	[39%])
COI:	1442			
Constant:	96			
Undetectable:	41			
Detected:	0	[0%]	(0	[0%])
Unknown:	0	[0%]	(0	[0%])
Unprocessed:	2394	[60%]	(2394	[60%])
To be injected:	3248 of 3973	[81%]		
Reduction:	725 of 3973	[18%]		

FSV_TC Step

FSV Summary				
Total:	3248		(2334)	
Equivalent:	914			
Unobservable	1498	[46%]	(1024	[43%])
COI:	0			
Constant:	1118			
Unpropagatable:	380			
Dangerous:	0	[0%]	(0	[0%])
Unknown:	1750	[53%]	(1310	[56%])
Unprocessed:	0	[0%]	(0	[0%])
Undetectable:	1883	[57%]	(1321	[56%])
COI:	910			
Constant:	733			
Undetectable:	240			
Detected:	0	[0%]	(0	[0%])
Unknown:	0	[0%]	(0	[0%])
Unprocessed:	1365	[42%]	(1013	[43%])
To be injected:	1310 of 3248	[40%]		
Reduction:	1938 of 3248	[59%]		

>50% reduction in fault space

Fault Sim Optimization — Save and Restart



15 - 30% improvement in f_exec run-time

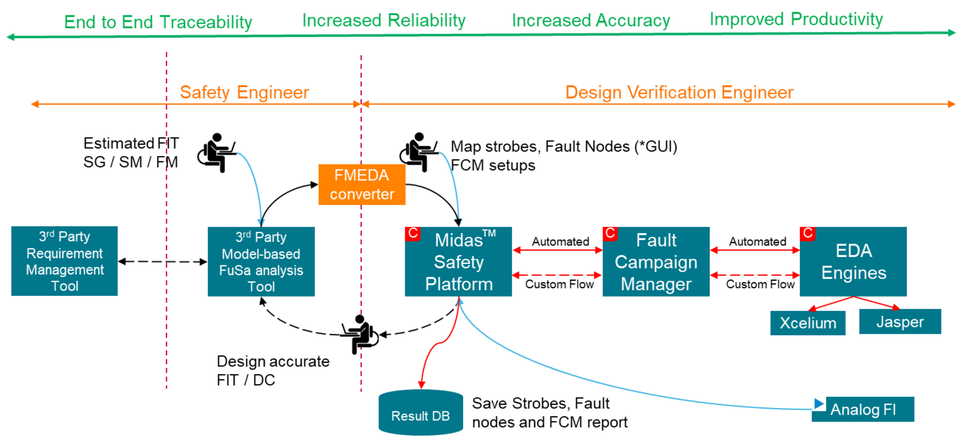
Throughput Improvement — Concurrent FI

- **Setup**: GLS + w/o SDF + STL
- Fault nodes: 38k
- 2k faults per sim
- 21 hrs with 5 parallel runs

>100x Raw Speed-up
~1000x Disk space savings
QoR : 100% Match with Serial
~2000x Less log files
Significant savings on compute resources

Bridging Safety Analysis and Safety Verification

- End-to-End traceability is a key requirement in safety verification and validation
- Unified flow with seamless integration is critical
- Cadence® Midas™ Safety Platform was evaluated for ADI usecases & flow (involving multiple tools)



Key Challenge:
Vendor tools/solutions do not have common/standard format data exchange

Summary

1. ISO 26262 compliance is quantitative and requires fully automated *semiconductor specific solution*
2. Fault Campaign Framework built upon Cadence® Safety Solution significantly improves *productivity* of engineers and the *efficiency* of the fault campaigns
3. Methodologies such as *Formal*, *Save and Restart* and *Concurrent fault simulation* improves the fault campaign throughput; close collaboration with EDA vendor has helped to deploy these methodologies in multiple projects
4. Fault campaigns must be thoughtfully planned to close on Diagnostic Coverage *faster* and *efficiently*
5. ***Standardizing FS Data*** : Accellera FuSa WG's efforts could enable *FS data sharing* between vendors

REFERENCES

1. ISO 26262-1:2018 Road vehicles — Functional safety, 2018 (https://www.iso.org/standard/68383.html)
2. Functional Safety White Paper, 2021 (https://www.accellera.org/downloads/standards/functional-safety)