POLITECNICO DI TORINO

Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering

XXXII cycle

Supervisor

Paolo Bernardi

Dependability of Safety-Critical Automotive SoC

PhD Candidate:

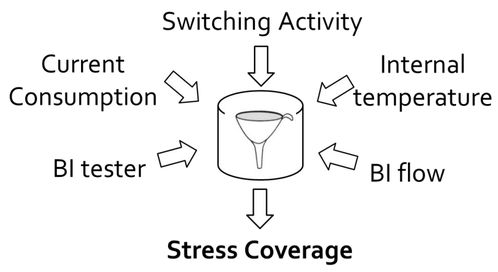
Marco Restifo

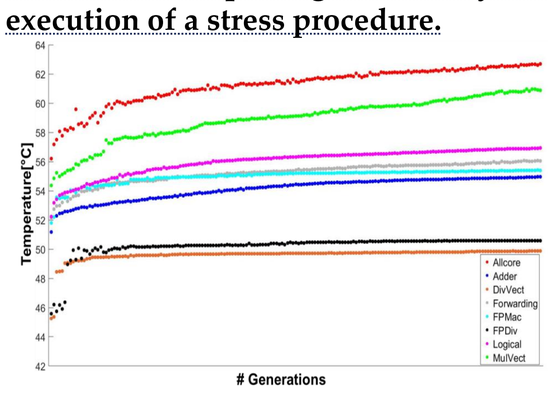
Abstract:

International standards for safety-critical applications are driving the state of the art for designers, providing necessary guidelines to ensure and achieve the required dependability constrains. Reliability, on-line testing and functional-safety are becoming relevant aspects. This study aims at improving the dependability of safety-critical Multi Processors System-on-Chip (MPSoC), focusing on automotive field. Three main topics have been addressed with industrial partners for enriching the state of the art on dependability field and for turning research results into business applications.

Reliability Challenges:

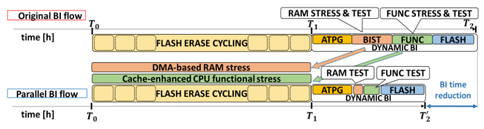
Comprehensive methodology for comparing the electrical stress strength of a Burn-In (BI) test. The novelty of our study with respect to prior works consists in a strategy that considers several kinds of measurements: circuit activity, internal temperature and current consumption generated by the execution of a stress procedure.

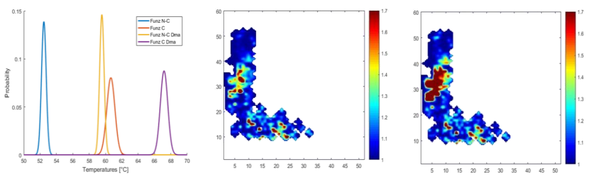




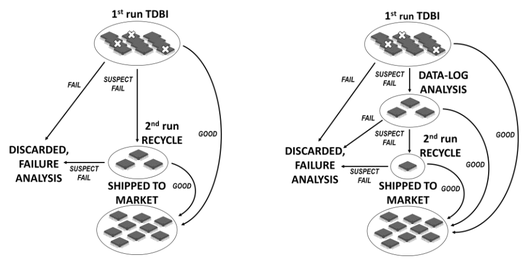
Comprehensive methodology for comparing the electrical stress strength. The novelty of our study with respect to prior works consists in a strategy that considers several kinds of measurements: circuit activity, internal temperature and current consumption generated by the execution of a stress procedure.

Maximization of functional stress by using a Direct Memory Access (DMA) and leveraging on cache memories. The DMA performs a march test on the flash memory while the cache enables the parallelization and speeds-up the functional stress program.





Introduction of a set of monitoring features able to collect information about BI criticalities that are responsible for false fails detection, potentially causing recycling and reducing the yield.

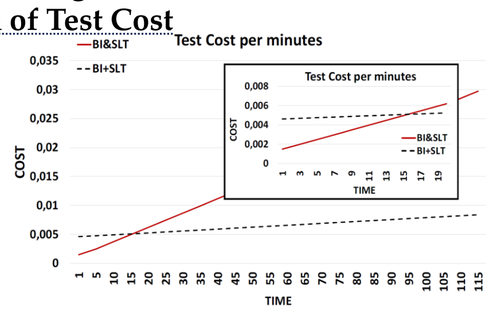


- **ATE DYNAMIC SCHEDULE ARCHITECTURE**
  - Power supply can drive a certain number of DUT during the burn-in
  - TDBI is statically scheduled
  - Test scheduling optimization
- **SoC ON-LINE SCHEDULER**
  - Flash erase duration depends on temperature and it spans from 25 to 45 s
  - Necessity to manage the erase time variability

Two-layered scheduling technique to optimize the stress application during the flash cycling phase and to reduce dramatically the length of the overall BI test phase; adaptive techniques are working both at chip and test equipment levels.

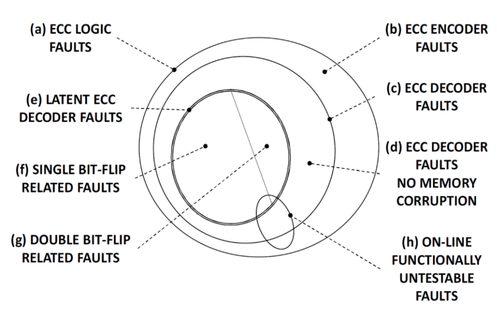
System Level Test (SLT) often complements the other steps of a test flow, which include Wafer Sort, Burn-In and Final Test, using functional test. The functional test complements the structural test because it covers some defects that structural test does not detect. My work aims at providing a solution to rearrange the test flow merging the BI and the SLT in a single step. Moreover, my work presents a way for accessing to the Design for testability (DfT) structures using the JTAG interface. The main goal of the combination of the BI and SLT in a single step is the reduction of Test Cost

	Original BI+SLT		Proposed BI&SLT
N of stages	2		1
Stage	Burn-In	SLT	Burn-In & SLT
Equip. cost (arb. unit)	500,000	500,000	1,000,000
Board parallelism	100	64	64
Additional costs	120 min of Load/Unload devices	None	None
Equip. Depreciation period	6 Years	6 Years	6 Years
Test cost per device per min (arbitrary unit/minutes)	0,0000330	0,0001239	0,0002477



On-Line Self-Test:

ECC logic is a redundancy module and it is not very intuitive a classification of ECC logic faults according to a produced effect. A fault taxonomy and a new kind of fault labeled as "Latent Fault". A Latent Fault is a fault visible only in presence on another fault. For ECC, Latent Faults are the faults of the correction logic of the decoder. It uses a debugger module for injecting memory corruptions on Random Access Memory (RAM), thus the faults inside the ECC logic are exited and are observed using load and store operations. The target of ECC testing topic has been an Automotive SoC by STMicroelectronics.



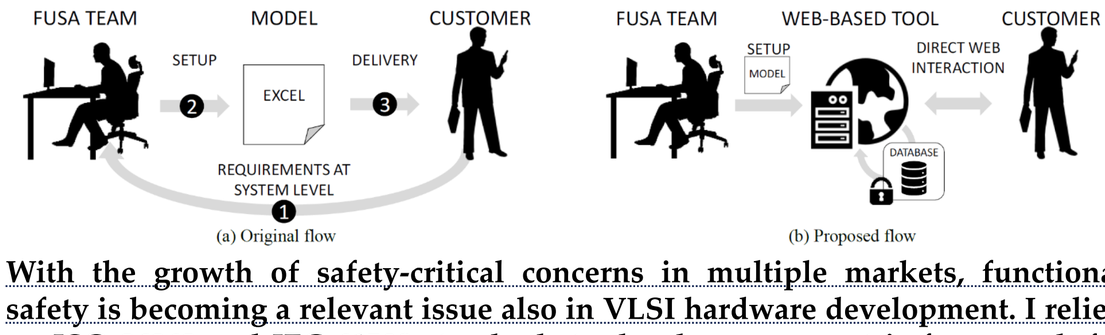
LOGIC	#FAULTS	FAULT COVERAGE %		
		SW BIST [16]	SBST Random	SBST ATPG
Ecc logic	**31,608**	**61.60**	**85.97**	**93.00**
Ecc encoder	13,275	85.12	86.77	94.39
Ecc decoder	18,864	44.90	81.25	92.06
Ecc decoder *no memory corruption*	11,379	74.43	78.52	92.22
Ecc decoder *Latent faults*	6,868	0	93.08	96.13
Single bit-flip	6,410	0	93.27	96.44
Double bit-flip	458	0	90.39	91.72
On-line functionally untestable faults	689	-	-	-

How to reach enough level of fault coverage during in field lifetime of a device requires a lot of attention today. This work proposes an new strategy for the in-field testing of automotive devices, the innovative idea is to perform a concurrently Software-Based Self-Test (SBST) and Logic Build-In Self-Test (LBIST) procedures. In more details, this strategy is based on the following features and scheduling principles:

1. the processor inside a System-on-Chip has its own SBST library
2. the system includes a Logic BIST, connected through a multiplexing logic
3. the LBIST is activated during the SBST execution, LBIST aims at self-testing the modules that the SBST library doesn't test by the current procedure.

Target of SBST \ Module for LBIST	Clock Cycles	Number of Faults: 4906 PC	4320 CTRL	39056 RF	2530 MUX	11172 ALU	39398 MAC	5522 SPRS	2708 LSU	2286 WB	109612 CPU
		% of Stuck-at Faults coverage									
Program Counter (PC)	24,914	**56.21**	74.39	65.96	95.19	58.24	23.07	15.33	49.82	64.76	**48.05**
Control Unit (CTRL)	538	54.95	**78.33**	39.25	90.89	54.86	52.45	35.18	56.52	71.13	**47.38**
Register File (RF)	1,502	57.13	68.43	**82.78**	89.51	**5.51→0**	0	9.95	51.28	55.76	**43.10**
Operational Muxes (MUX)	308	54.69	74.39	37.90	**92.50**	53.35	43.84	23.70	66.63	71.90	**43.92**
Arithmetic Logic Unit (ALU)	10,820	57.49	72.02	67.58	90.29	**89.05**	40.44	10.11	63.58	67.73	**54.19**
Multiply and Accumulate (MAC)	3,248	55.95	76.45	49.07	96.49	50.40	**88.78**	30.87	51.10	71.95	**61.17**
Load/Store Unit (LSU)	2,108	56.98	70.91	61.49	94.84	41.00	**0**	9.95	**92.22**	67.89	**37.50**
WriteBack (WB)	538	54.98	78.33	39.34	91.46	54.86	52.45	35.18	56.94	**71.73**	**47.46**
TOTAL per module	**43,976**	**56,39**	**69,41**	**90,69**	**96,83**	**93,83**	**92,72**	**39,74**	**75,56**	**76,4**	**88,16**
Hybrid coverage	**43,976**	56,39	69,41	90,69	96,83	**99,44**	**98,87**	39,74	75,56	76,4	**90.94**

Functional Safety:



With the growth of safety-critical concerns in multiple markets, functional safety is becoming a relevant issue also in VLSI hardware development. I relied on ISO 26262 and IEC 61508 standards to develop a parametric framework for Failure Mode Effect and Diagnostic Analysis (FMEDA). The framework allows users to evaluate safety metrics of a system depending on the activation/de-activation of some safety requirements at system level and tuning other parameters.

The framework has been developed to protect the internal information about the intellectual properties of the semiconductor vendor while customers can customize safety related parameters to tailor results to the Automotive Safety Integrity Level (ASIL) of their target application.

Finally, the framework becomes an industrial tool used in the production of Xilinx on Zynq Ultrascale+ MPSoC