# Table of Contents

Page 3  Few Words about LIRMM and the Microelectronics Department  
- LIRMM  
- The Microelectronics Department  

Page 5  Staff members  
- Key numbers  
- List of members  

Page 7  Organization  
- SysMIC project  
- DEMAR project  

Page 9  Summary of 2010 Activities  
- PART ONE - Analysis and Models for Circuit Design  
- PART TWO - Test of Integrated Circuits and Systems  
  - Digital Testing  
  - Power-Aware Testing  
  - Memory Testing  
  - Test & Security  
  - Analog & RF Testing  
- PART THREE - Design and Test of MEMS  
- PART FOUR - Adaptive Circuits and Systems  
- PART FIVE - Biomedical Circuits and Systems  

Page 61  Summary of 2010 Publications  

Page 62  List of HDR and PhD Thesis defended in 2010  

Page 63  Some Key Features of the Microelectronics Department  
- Role and Involvement at the International and National Levels  
- International Academic Cooperation  
- National and European Research Projects  
- Industrial Relationships  
- ISyTest – A Joint Lab between LIRMM and NXP  
- Technological Platforms  

Page 70  Sample Gallery
Few Words about LIRMM

Montpellier Laboratory for Informatics, Robotics and Microelectronics (LIRMM) is a research laboratory supervised by both Montpellier University (Université Montpellier 2) and the French National Center for Scientific Research (CNRS). With a staff of 439 people (359 permanent + 80 temporary employees), LIRMM is one of the most important academic laboratories in France. Its research activities position the LIRMM at the heart of Information and Communication Technologies (ICT) and sciences. The spectrum of research activities covered by LIRMM is very broad, and includes:

- Algorithms, databases, information systems, software engineering, artificial intelligence, networks, arithmetic, optimization, natural language and bioinformatics,
- Design of mechanical systems, modeling, identification, control and perception,
- Design and verification of integrated, mobile and communicating systems

The combination of these skills results in interdisciplinary academic or industrial research projects conducted at national and international levels.

One of the LIRMM strengths is that each field of scientific expertise covers theory, tools, experiments and applications. The research works generally find applications in a great diversity of domains, such as biology, chemistry, telecommunications, health, environment, agronomy, etc., as well as in domains directly related to the own lab activities: informatics, electronics, and automation.

LIRMM is a laboratory dedicated to "produce" knowledge (more than 300 international publications per year) and educate future researchers (Masters, PhDs, post-docs), and is involved in a strong economical “dynamic”: industrial partnerships, innovative start-ups, national and international scientific leadership, etc.

The laboratory is organized in three departments: Informatics, Robotics and Microelectronics.
Few Words about the Microelectronics Department

The Microelectronics department is specialized in the research of innovative solutions to model, design and test complex integrated circuits and systems. Such systems are characterized by a high complexity, elevated performances, a high heterogeneity, and a 2D or 3D integration into a single package.

The expertise of the Department covers the following strategic topics:

- Development of new generations of processor architectures for applications like 4G mobile phones, signal and image processing, or multimedia;
- Design for testability, and test of integrated circuits and systems, which include all activities on modeling, detection and diagnostic of physical failures;
- Design, integration and test of micro-systems based on sensors and actuators;
- Secured design for the confidentiality and integrity of communications (in banking transactions for example);
- Design of circuits for the health and medical domains, with applications like neuro-stimulation systems implanted the human body.

The research activities are multidisciplinary and require skills in computer science, mathematics, physics, life sciences, etc. This allows the research team to provide answers to the various and numerous scientific, societal and economical challenges of today and tomorrow Microelectronics.

To conduct these research activities, the Department relies on a hundred of persons, including full-time researchers, professors, PhD students, post-doc students, research engineers and technicians. Owing to its high-level scientific production, its academic collaborations, its implication in numerous national and international research programs, its participation to the creation of start-up companies, and its activities of transfer and valorization towards the industry sector, the Department is now recognized as an essential actor in the landscape of the French and international scientific research in Microelectronics.
During the year 2010, the Microelectronics Department was composed of 27 permanent researchers (from University Montpellier 2, CNRS and INRIA), 1 associate member, 10 Post-Doctoral students, 48 PhD students, 1 ATER, 7 research engineers, technicians and administrative staff and a dozen of Master students.

Head of Department
Patrick Girard, CNRS Research Director

Deputy-Heads of Department
Serge Bernard, CNRS Researcher
Laurent Latorre, Associate Professor at Montpellier University

Full researchers and professors (27)
Florence Azais, CNRS Researcher
Nadine Azemard-Crestani, CNRS Researcher
Pascal Benoit, Associate Professor at University of Montpellier
Serge Bernard, CNRS Researcher
Yves Bertrand, Professor at University of Montpellier
Alberto Bosio, Associate Professor at University of Montpellier
Guy Cathebras, Professor at University of Montpellier
Mariane Comte, Associate Professor at University of Montpellier
Denis Deschacht, CNRS Research Director
Giorgio Di Natale, CNRS Researcher
Luigi Dilillo, CNRS Researcher
Marie-Lise Flottes, CNRS Researcher
Jérôme Galy, Associate Professor at University of Montpellier
Patrick Girard, CNRS Research Director
David Guiraud, INRIA Research Director
Laurent Latorre, Associate Professor at University of Montpellier
Frédérick Mailly, Associate Professor at University of Montpellier
Philippe Maure, Associate Professor at University of Montpellier
Pascal Nouet, Professor at University of Montpellier
Serge Pravossoudovitch, Professor at University of Montpellier
Michel Renovell, CNRS Research Director
Michel Robert, Professor at University of Montpellier
Bruno Rouzeyre, Professor at University of Montpellier
Gilles Sassatelli, CNRS Researcher Director
Fabien Soulier, Associate Professor at University of Montpellier
Lionel Torres, Professor at University of Montpellier
Arnaud Virazel, Associate Professor at University of Montpellier

Associate members (1)
Jean-Marc Gallière, PRAG Professor at University of Montpellier
<table>
<thead>
<tr>
<th>PHD students (48)</th>
<th>Post-doctoral students (10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syed Zahid Ahmed</td>
<td>Fanny le Floch</td>
</tr>
<tr>
<td>Boris Alandry</td>
<td>Victor Lomme</td>
</tr>
<tr>
<td>Renan Alves Fonseca</td>
<td>Imen Mansouri</td>
</tr>
<tr>
<td>Marina Aparicio</td>
<td>Gabriel Marchesan Almeida</td>
</tr>
<tr>
<td>Joao Azevedo</td>
<td>Baptiste Marechal</td>
</tr>
<tr>
<td>Lyonel Barthe</td>
<td>Pierre-Didier Mauroux</td>
</tr>
<tr>
<td>Youssef Benabboud</td>
<td>Nabila Moubdi</td>
</tr>
<tr>
<td>El Mehdi Boujamaa</td>
<td>Huy Binh Nguyen</td>
</tr>
<tr>
<td>Kaouthar Bousselam</td>
<td>Ziad Noun</td>
</tr>
<tr>
<td>Olivier Brousse</td>
<td>François Poucheret</td>
</tr>
<tr>
<td>Florent Bruguier</td>
<td>Nicolas Pous</td>
</tr>
<tr>
<td>Rémi Busseuil</td>
<td>Ahmed Rekik</td>
</tr>
<tr>
<td>Luis Vitorio Cargnini</td>
<td>Olivier Rossel</td>
</tr>
<tr>
<td>Jean Da Rolt</td>
<td>Zhenzhou Sun</td>
</tr>
<tr>
<td>Julien Dalmasso</td>
<td>Sébastien Tiran</td>
</tr>
<tr>
<td>Amine Dehbaoui</td>
<td>Karim Tobich</td>
</tr>
<tr>
<td>Pierre-François Desrumaux</td>
<td>Duc Anh Tran</td>
</tr>
<tr>
<td>Florian Devic</td>
<td>Miroslav Valka</td>
</tr>
<tr>
<td>Jérome Dibattista</td>
<td>Bruno Vaquie</td>
</tr>
<tr>
<td>Mouhamadou Dieng</td>
<td>Sameer Varyani</td>
</tr>
<tr>
<td>Haythem El Ayari</td>
<td>Lionel Vincent</td>
</tr>
<tr>
<td>Yoann Guillemenet</td>
<td>Fangmei Wu</td>
</tr>
<tr>
<td>Souha Hacine</td>
<td>Leonardo Zordan</td>
</tr>
<tr>
<td>Nicolas Hebert</td>
<td></td>
</tr>
<tr>
<td>Camille Jallier</td>
<td></td>
</tr>
</tbody>
</table>

**Temporary professors and researchers (1)**

Olivier Leman, *Temporary associate professor and researcher (ATER)*

**Research engineers, technicians and administrative staff (7)**

Laurent De Knyff, *technician at Montpellier University*
Caroline Drap, secretary
Thierry Gil, *CNRS research engineer*
Ludovic Guillaume-Sage, *technician*
Régis Lorival, *CNRS research engineer*
Olivier Potin, *research engineer*
Jérémie Salles, *research engineer*

**Guest professors (4)**

Paolo Bernardi, *Politecnico di Torino, Italy*
Brahim Mezghani, *University of Sfax, Tunisia*
François-Xavier Standaert, *Catholic University of Louvain, Belgium*
Hans-Joachim Wunderlich, *University of Stuttgart, Germany*
Organization

Research activities carried out by the Microelectronics Department are organized within two major research project teams:

- **SysMIC**: Design and Test of Microelectronic Systems
- **DEMAR**: Deambulation and Artificial Movement (joint team between LIRMM and INRIA, and joint team between Robotics and Microelectronics departments)

### SysMIC

The overall objective of the SysMIC team is to propose innovative solutions to model, design and test today’s and tomorrow’s integrated circuits and systems. The overall challenges that are addressed are: complexity, performances, power consumption, heterogeneity (digital, analog, RF, memory, MEMS, FPGA, etc.), reliability and robustness (ageing, impact of environment), manufacturing related issues (variability, high defect density), communications (network-on-chip, wireless, sensor networks), and emerging technologies (physical phenomena to understand, to model and to integrate).

The four main research areas are:

**Analysis and Models for Circuit Design** to develop analysis methods and models for electrical phenomena (e.g. crosstalk) and performance estimation (delay, power consumption), and to develop flows for process variability monitoring and security evaluation. The topics include:

- Performance analysis
- Process variability monitoring flows
- Security evaluation (through a platform)
- Counter-measures for secured circuits
- Attack definition (anticipating threats)
Test of Integrated Circuits and Systems to develop Design-for-Test techniques for complex systems (to ease test application and increase test efficiency), to develop fault models, methods, algorithms and tools to test manufacturing defects and deal with reliability issues, and for detection, diagnosis and in situ repair of various types of malfunctions. The topics include:

- Fault modeling
- Test of analog, mixed-Signal & RF circuits
- Test of memories (SRAM, Flash, MRAM)
- Test of low power designs
- Test of secured circuits
- Wireless testing
- Fault tolerance and test of fault tolerant structures
- Test of System-on-Chip (SoC), System-in-Package (SiP), and 3D ICs
- Fault diagnosis

Design and Test of MEMS to develop innovative solutions to promote the integration of low-cost MEMS devices and dedicated electronic interfaces relying on standard technologies. The topics include:

- MEMS integration
- CAD of heterogeneous systems
- Electronic Interfaces
- Design & Test of MEMS

Adaptive Circuits and Systems to explore and design self-aware / adaptive circuits & systems: online decision making for optimizing performance, power, reliability, security. The topics include:

- Adaptive MPSoCs
- Fault-tolerant MPSoCs
- Virtualization techniques
- Hybrid circuits (MRAM/CMOS)
- Emerging Technologies
- Secure systems and architectures
- Self-organizing sensor networks

DEMAR

The overall objective of the DEMAR team is to propose complete Functional Electrical Stimulation (FES) systems based on the patients’ demand discussed with the medical staff. The overall challenges that are addressed are: selectivity for stimulation and recording, power management, complexity and heterogeneity, physiological constraints, and safety for the patient (dependable systems). The main research area is the Development of Micro-Circuits for Neuro-Prothesis. The topics include:

- Distributed architecture (stimulation and recording units)
- Implantable micro-stimulator
- Modeling and recording of physiological signals
- Signal processing for ENG recording
- Design for Dependability
Summary of 2010 Activities

PART I
Analysis and Models for Circuit Design

PART II
Test of Integrated Circuits and Systems

PART III
Design and Test of MEMS

PART IV
Adaptive Circuits and Systems

PART V
Biomedical Circuits and Systems
Analysis and Models for Circuit Design
Interconnect Design for a 32nm Technology

D. DESCHACHT

Partners: LAHC, University of Chambery

When high speed integrated circuits technology scales down from one node to the other, ITRS suggests a reduction in size by a factor of around square of 2, and recommends 17% of improvement on performance. With the dimension shrink, the IC’s speed increase gained on active devices is partially loosed. This is mainly due to interconnects delays increase as dimensions of interconnects are shrunk to satisfy integration requirement. Moreover, from the 45 nm generation, worrying crosstalk (XT) levels are expected. These XT levels are particularly noticeable in the intermediate metal level of the Back-End of Line (BEOL) stack which contains relatively long interconnect (hundreds of µm long) that are very closed to each other. Signal integrity losses are further aggravated if multiple interconnect lines couple energy from or to each other. Operating frequencies that have increased over the past decade, are expected to maintain the same rate of increase over the next decade approaching 10 GHz by the year 2012. On-chip inductance is becoming necessary to be included in the model, and its importance will increase as technologies downscale. Simple 2-coupled lines are not sufficient enough to verify the signal coupling effects. Thus, it is considered here 3-coupled lines. This case is representative of a beam of interconnections, where a central line is studied surrounded with two neighboring lines. From a well tried 45 nm technological node, different EM simulations are carried out in order to extract RLCG parameters and access sensibility of interconnect width / space on line parameters, without modifying the various technological stages of manufacture, nor the materials used. Our works are focused on the impact on signal transmission delay along interconnects of decreasing the space and width. To avoid new industrial manufacturing constraints on cost and reliability, this study is performed without modifying process and materials used in the BEOL of CMOS 45 nm IC. We will study interconnects of 50 nm width, with a 50 nm space between lines in accordance with speed and crosstalk levels requirements of CMOS 32 nm BEOL. From a well tried 45nm technological node, we determined the conditions of designing less wide and less spaced interconnects (W = S = 50 nm), while answering to the required improvements expected for the 32 nm technological node in term of performance. The performance gain obtained with our design solutions is clearly better than ITRS recommendations. When it becomes hard to meet all requirements, we have shown that interconnect density constraints should be relaxed to enlarge the scope of application. By following these design rules, interconnect delays and circuits rates are strongly improved without modifying the 45 nm BEOL process.

References:


Illustration of intermediate metal levels modeling in BEOL

Illustration of 3 coupled interconnects with respective loads and excitation
Differential Power Analysis for Designers

G. DI NATALE, M.L. FLOTTES, B. ROUZEYRE, M. VALKA

Project/Partners: DGA CELAR

Topic: Hardware Security

Security dedicated devices are now commonly used for protection of information in various domains of application. In addition to standard evaluation criteria in terms of performances, area and power consumption, these devices present specific design features that prevent ill-intentioned persons to attack the system, i.e. to retrieve confidential information by manipulation or observation of the chip.

Many attacks aiming to gather private information have been publicly detailed and commented in the past. Among them, one of the most intensively studied attacks is the Differential Power Analysis (DPA) proposed by P. Kocher et al. in 1999. This analysis relies on the observation of the chip power fluctuations during data processing.

Several design methodologies have been proposed to protect a circuit against this type of side-channel attack. However, the effectiveness of these counter measures is still evaluated by resorting to intensive DPA (simulated or real) and constitutes a very time-consuming design task. We have proposed two designer-oriented methods to reduce the time required to validate the effectiveness of a countermeasure, that exploit the knowledge of the circuit structure and the value of the secret key.

The first method [1] relies on a drastic reduction of the required number of power traces needed to retrieve the secret key. It is based on the selection of the best input messages that exalt and amplify the value of the difference between the two power packets for the correct key value.

In the second proposed method [2][3] the basic idea is to realign the circuit power consumption traces resulting from the stimulation of the circuit with different data, in such a way that the propagation delay taken into account by the correlation function is always the same, thus avoiding the spread of the energy along a large time window (Fig. 1). This new method is independent from the type of analysis since it concentrates the energy correlated to the secret key value thus helping any type of correlation-based power analysis (e.g., Correlation Power Analysis, or High Order DPA).

The novelty of these approaches rely on the possibility of quickly evaluate the strength of a small part of the design against simulation-based power attacks (even without sequential elements that help power analysis). From the designer point of view, if the circuit is not easily attackable by using the proposed approaches, it will be even less attackable when design information cannot be used (i.e., when a real attacker tries to discover the secret key).

References:


SSTA framework for process variability monitoring

N. AZEMARD, P. MAURINE, Z.WU

Project/Partners: ENIAC-MODERN, I3M

Contact: azemard@lirmm.fr

Topic: Models and methods for circuit design

With the « More Moore » and low power trends, optimizing or only well predicting the final performances of digital circuits become more and more difficult. Indeed, variability and hardness to model accurately transistor behavior impede the dimension scaling benefits. Current design methodologies generally use guard margins to prevent from the incertitude generated by these limits and to guarantee functional yield. But as we go in the nanometer era, the use of margin is not efficient anymore, because of an increasing over-design, limiting optimizations and decreasing both parametric and functional yield.

In order to increase the robustness to uncertainty during the design levels and to have better performance analysis, we propose a SSTA Framework Based on Moments Propagation (Figure1). We introduce a new statistical PDF propagation approach built on two concepts in probability theory: conditional mean and conditional variance. Our objective is to develop a simple and practical timing approach considering effect of structure correlations, input slope and output load variations. Such objective causes the introduction of new way to do cells timing characterization: log-normal distribution based model as input signal and inverters as charge. The proposed SSTA flow gives us satisfactory estimate of path delay distribution with maximal relative error 5% and 10% respectively on mean and on standard deviation.

The SSTA engine has been and continues to be verified in collaboration with STMicroelectronics in Crolles in France and the CEA-Leti in Grenoble in France. We have implemented the specific methodology called SSTA (Statistical Static Timing Analysis). We could verify that this SSTA flow allows performing statistical analysis on timing performances and accurately observing process variation effects on delays. This work is made in collaboration with the I3M lab of Montpellier.

We attempt to tackle the problem never been mentioned: estimate of structure correlations, which comes from the fact that output signal of one cell is input signal of the next stage.

More, we have realized in 2010 the project of a specific workshop on variability. We have organized the LIRMM in Montpellier, the Workshop VARI2010 (website: http://www.lirmm.fr/vari10/). It has been the first European workshop on CMOS Variability. The VARI meeting has answered to the need to have an European event on variability, where industry and academia meet to discuss. The VARI objective has been to provide a forum to discuss and investigate the CMOS variability problems in methodologies and tools for the design of upcoming generations of integrated circuits and systems. The technical program has focused on timing, performance and power consumption as well as architectural aspects with particular emphasis on modeling, design, characterization, analysis and optimization of variability.

This workshop has been a success. So, we have decided to continue this workshop and the next edition will be held in Grenoble on May 30-31, 2011 (Web site: http://www.vari-cmos.org/).

References:


Figure 1: The developed SSTA flow.
Physical Attacks based on ElectroMagnetic waves

P. MAURINE, L. TORRES, M. ROBERT

Project/Partners: CEA, STMicro, I3M, IES, PUCRS

Contact: pmaurine@lirmm.fr

Topic: Secure Circuit Evaluation

Physical Attacks aim at disclosing secret information hidden in secure circuits such as smart cards. Among the known attacks, one may identify two extremely efficient and low cost kinds of attacks:

- Side Channel Attacks are based on the statistical treatment of numerous observations of a physical leakage
- While Fault Attacks allow disclosing secret data by comparing faulty responses of secure IC to correct ones.

Within this context, the goal of this project is to evaluate the threat related to both Side Channel Attacks and Fault Attacks based on the exploitation of EM waves.

More precisely, this project aims at adapting or developing specific attacks exploiting the interesting properties of EM waves, both from a practical and a statistical point of views. The project also aims at defining countermeasures (at the right cost) against all newly identified threats.

Involved People at LIRMM
T. Ordas (Phd 06-09), V. Lomne (Phd 07-10), A. Dehbaoui (Phd 07-10), F. Poucheret (Phd 09-12), S. Tiran (Phd Student 10-13), K. Tobich (Phd 10-13), B. Vaquie (Phd 10-13), L. Torres, M. Robert, P. Maurine

Related Projects
- Calisson 1, 2007-2010, Pole de Compétitivité Mondial SCS
- Calisson 2, 2011-2014, Pole de Compétitivité Mondial SCS
- ANR ARPEGE EMAlSeCI

References:
Test of Integrated Circuits and Systems
Power Supply Noise and Ground Bounce Aware Pattern Generation for Delay Testing

A. TODRI, A. BOSIO, L. DILILLO, P. GIRARD, S. PRAVOSSOUDOVITCH, A. VIRAZEL

Contact: todri@lirmm.fr

Topic: Path Delay Testing, Speed Binning

As technology scales down, the effects of power supply noise and ground bounce are becoming significantly important. In the existing literature, it has been shown that excessive power supply noise can affect the path delay, while ground bounce is either neglected or assumed similar to power supply noise. Our work performs a detailed study of combined and uncorrelated power supply noise and ground bounce and their impact on the path delay. Our analyses show that different combination of power supply noise and ground bounce can lead to either delay speed-up or slow-down.

Our objective is to generate test patterns such that the combined effects of power supply noise and ground bounce are considered on circuit delay analysis. The impact of noise on delay is highly depended on the applied input patterns. Our research seeks to provide mathematical models to represent the circuit based on the physical extracted data after the circuit is placed & routed with power/ground grids. We propose close-form mathematical models to capture the impact of input patterns on path delay in the presence of power supply noise and ground bounce. We use a simulated annealing (SA) based approach to find patterns that maximize the critical path delay. In contrast to previous works which initially aim to find patterns for maximum supply noise and then compute delay, our method targets directly to find the worst case delay which might not necessarily occur under worst case power supply noise due to the speed-up/slow-down phenomena. Our method generates patterns that sensitize the path and also cause such power supply noise and ground bounce that leads to the maximum path delay.

References:


A Comprehensive System-on-Chip Logic Diagnosis

Y. BENABBoud, A. BOSIO, L. DILILLO, P. GIRARD, S. PRAVOSSOUDOVITCH, A. VIRAZEL

Contact: bosio@lirmm.fr

Project/Partners: ST-Microelectronics Topic: Logic Diagnosis

Silicon area is now so cheap and integration technologies so advanced that it is possible to embed in a System-on-Chip (SoC) all components and functions that historically were placed on a hardware board. Consequently, there are many defects that can affect a SoC and hence lead to yield loss: random, systematic and lithography defects. Random defects are related to the process only, while systematic and lithography defects are related to both process and design. These defects lead to failures that actually exhibit timing and/or parametric behaviors, and which cannot be modeled by the classical stuck-at fault model. In order to produce reliable and high quality circuits with zero defect, zero recurrence and zero excursion, diagnosis of defective chips becomes important not only to find physically defects inside a chip, but also to improve manufacturing and design processes.

In the past, the emphasis was concentrated in proposing meaningful techniques for test and diagnosis targeting single or multiple cores without considering the system level view. In fact, only dedicated techniques have been proposed so far to target specific cores: logic cores (logic diagnosis), memory cores (memory diagnosis) and analog cores (analog diagnosis).

Except industrial in-house diagnosis tools, few approaches targeting a full SoC at system level have been proposed in the literature. This work in [1] proposed an approach based on the Critical Path Tracing algorithm. Although this approach is able to manage several fault models at the same time and is always reliable (in terms of possible fault location), it suffers from a lower diagnosis resolution compared to industrial tools.

This work in [2] proposes a comprehensive diagnosis approach targeting SoCs. The key concept of the proposed approach is that diagnosis consists in a comparison between a set of pre-computed SoC failures and the set of failures observed during test.

The main advantages of this approach with respect to the state-of-the-art solutions are its capability (i) to manage both full-scan (combinational) and partial-scan (sequential) logic cores, (ii) to deal with several fault models at a time (both static and dynamic) and (iii) to address both single and multiple fault occurrences. A SoC case study (Figure 1) coming from STMicroelectronics has been considered to prove the efficiency of the proposed approach.

References:

Parallel Test of Identical Cores using Test Elevators in 3D circuits

A. BOSIO, G. DI NATALE

Contact: dinatale@lirmm.fr

Topic: Digital Test

Latest three-dimensional stacked integrated circuits (3D-SICs) are based on the Through Silicon Vias (TSVs) technology. TSVs are the key to allow many interconnections between stacked dies, thus providing new architectural paradigms and also new challenges from the test point of view. Design for Testability (DfT) has been widely used in the semiconductor industry leading to several standards starting from the board level (IEEE 1149) up to the System on Chip level (IEEE 1500).

We presented a DfT architecture targeting 3D-SICs exploiting TSVs in order to apply test in parallel when identical cores are stacked together. The main advantage is the reduced test time application while keeping the area cost very low.

Figure 1 shows the proposed solution at circuit level. Each die is composed of several cores and we suppose that it embeds an IEEE 1500 compliant wrapper. PB_WSI and PB_WSO are used to perform pre-bond test (and they will not be any more accessible after bonding). TSV_WSO and TSV_WSI are the test elevators used to connect one die to the next and the previous one. TSV_PWSO is the test elevator used to carry out test data. We proposed to add one test elevator called TSV_PWSI to handle the parallel test. In case of serial test, input data is enter from PB_WSI of accessible die (i.e., DIE1 in Figure 1), it is then sent through SoC1 from WSI to WSO, and by using TSV_WSO test elevator, it reaches the input port WSI of DIE2. This type of connection is repeated until the last die. The final output WSO of the last die (i.e., DIE 3 in Figure 1) is connected back to the accessible die through TSV_PWSO. Remaining dies are disconnected from TSV_PWSO. In case of identical cores, each WIR is first programmed in such a way that test data comes from the TSV_PWSI instead of TSV_WSI. Moreover, non-identical cores of each SoC are programmed in bypass mode. Then, test data is sent at the same time to all dies through TSV_PWSI that is connected to the accessible pad (PB_WSI of DIE1 in Figure 1).

To collect results, only WSO of one die must be connected to the TSV_PWSO bus that is read from the external ATE through the PB_WSO of the accessible die. On the contrary, all the remaining dies are connected to the TSV_PWSO in read mode, and at each clock cycle they compare the value present on the bus with the one coming from the local WSO. In such a way, the remaining dies self-compare test data output w.r.t to the die sending test data through TSV_PWSO.

References:

Defect Modeling in Nanometric CMOS Technologies

M. APARICIO, F. AZAIS, Y. BERTRAND, M. COMTE, M. RENOVELL

Project/Partners: Universities of Passau & Freiburg, CCUFB (Centre de Coopération Universitaire Franco-Bavaroise)

The general principle of digital Integrated Circuit (IC) testing consists in highlighting an awkward behavior that may result from a physical failure or a signal integrity matter. The general objective of the studies carried out in this topic is to study the electrical behavior of ICs affected by physical failures on the one hand and by undesired power variations on the other hand in order to propose realistic fault models for CMOS nanometric technologies meant to facilitate efficient IC tests.

The traditional stuck-at fault model does not manage any longer to cover all possible circuit failures. Some new models have appeared to complement the traditional ones. Let us mention the parametrical resistive short model that takes into account the resistance of the defects, and the compact model for transistors affected by a Gate-Oxide Short (GOS), both models developed by the LIRMM team, which has become expert in this field. These new fault models now consider the notion of defect random parameters (for instance its size, its resistance value), which are unpredictable by nature. Regarding signal integrity matters, a fine analysis of the noise in the power supplies has led to a better understanding of the affected circuit. Furthermore, with nanometric technologies emergence, new types of defects, which impact on the system behavior used to be negligible, tend to become as significant as previously known defects with comparable effects. One could mention ground bounce, IR drop or NBTI (Negative Bias Temperature Instability). It seems therefore necessary to consider these “new” defect impact as an additional contribution to the sum of defects and to take them into account within the framework of behavioral modeling.

A dynamic analysis of the electrical effects caused by a resistive short between two gate outputs has recently been carried out. This analysis takes into account the crosstalk capacitance between the involved lines. The electrical behavior of the node affected by the resistive short therefore depends not only on the parametrical value of the defect but also on the crosstalk capacitance as well as on the skew between input signal transitions on both lines. Figure 1 shows the transition delay evolution of one affected gate’s output versus the skew for different defect resistance values. A mathematical model has been proposed, validated and integrated into a fault simulator by the University Albert-Ludwigs of Freiburg.

Current work concerns the analysis and modeling of the impact of voltage power drop (or IR-Drop) on the propagation delay of gates in nanometric CMOS technologies. The IR-Drop effect is generated by the parasitic resistors of the power grid. The voltage power drop may occur at a power supply via when several physically neighboring transistors fed by the power via experience simultaneous logic transitions in response to a change in the circuit inputs. Therefore, the IR-Drop propagation is closely related to the power grid structure. The voltage power drop may cause timing faults that must be taken into account in the fault tests. Our objective is to analyze and model how the voltage power drop propagates and dissipates in time and space and how it affects the neighboring gates connected to the same power supply.

References:


Robustness Improvement of Digital Circuits using Fault Tolerant Architectures

D.A. TRAN, A. VIRAZEL, A. BOSIO, L. DILILLO, P. GIRARD, S. PRAVOSSEUDOVITCH

Contact: virazel@lirmm.fr

Project/Partners: ITI, Stuttgart - Germany

CMOS technology scaling allows the realization of more and more complex systems, reduces production costs and optimizes performances and power consumption. Today, each CMOS technology node is facing reliability problems whilst there is currently no alternative technology as effective as CMOS in terms of cost and efficiency. Therefore, it becomes essential to develop methods that can guarantee a high robustness for future CMOS technology nodes.

To increase the robustness of future CMOS circuits and systems, fault tolerant architectures might be one solution. In fact, these architectures are commonly used to tolerate on-line faults, i.e. faults that appear during the normal functioning of the system, irrespective of their transient or permanent nature. Moreover, it has been shown that they could also tolerate permanent defects and thus help improving the manufacturing yield.

Fault tolerant techniques use redundancy, i.e. the property of having spare resources that perform a given function and tolerate defects. These techniques are generally classified according to the type of redundancy used. Basically, three types of redundancy are considered: information, temporal and hardware.

- In information redundancy, additional data are used, such as error detection and correction code.
- Temporal redundancy consists of forcing the system to repeat a given operation so that transient faults will be tolerated.
- Hardware redundancy consists of modifying the design by adding extra hardware, such as duplication or triplication of logic cores.

Various solutions using fault tolerant techniques for robustness improvement have been studied, targeting first and foremost the tolerance of transient and/or permanent faults. Minimizing the area of the scheme is commonly the second objective. Manufacturing yield improvement has recently been considered as a new goal. Beside these criteria, other aspects such as power consumption, aging and expected lifetime of circuits are of the same importance but have not been studied for random logic cores. Here for the first time, our study provides a fault tolerant architecture that targets different goals at the same time. Firstly, it increases circuit robustness by tolerating both transient/permanent online faults and manufacturing defects. Secondly, it is able to save power consumption compared to existing solutions. Finally, it deals with aging phenomenon and thus, increases the expected lifetime of logic circuits.

Figure 1 show the functional scheme of our hybrid architecture. The logic circuit is implemented three times (LC1, LC2, LC3) but only two of them are working in parallel and are selected with the help of two multiplexors (MUX_IN, MUX_OUT). The third logic circuit is in standby state. The comparator verifies the good functioning of the current configuration by comparing outputs of the two running logic circuits. Its output (Ok signal) controls the enable input of the registers. During fault free operations, the Ok signal is true and the current configuration does not change. As long as no error is detected, only two circuits are running. If the comparator detects an error, the OK signal becomes false and the registers are disabled. The Finite State Machine (FSM) changes the configuration to tolerate the detected error by controlling the multiplexors.

References:

Transition Faults: Test and Diagnosis in System-on-Chips

A. BOSIO, P. GIRARD, S. PRAVOSSOUDOVITCH

Project/Partners: PICS CNRS (Politecnico di Torino)

The System-on-Chip (SoC) design paradigm has become widely accepted for highly complex, heterogeneous embedded systems that can include digital, analog, mixed-signal, radio-frequency, micromechanical, and other components on a single piece of silicon. Due to the advances in manufacturing technologies and more aggressive clocking strategies used in modern design, more and more defects lead to failures that can no longer be modeled by classical stuck-at faults. Numerous actual failures exhibit timing or parametric behaviors that are not adequately modeled by stuck-at faults. Such failures have to be taken into account during the test process in order to reach acceptable DPM (Defect per Million) figures. The authors of show that a certain number of these failures can only be detected if the test vectors are applied at-speed.

Self-Test strategies, such as BIST and Software-Based Self-Test (SBST), effectively tackle the at-speed test application requirements while providing an effective manner to partition the complete SoC test. Furthermore, Self-Test techniques employment may reduce the test equipment costs since they requests a limited number of edge-sets, a reduced test management frequency and a few channels providing high speed clock signals (often referred to as free-running clocks).

The evaluation of at-speed stimuli application is a very expensive task in terms of required computational time. Designers that are measuring the effectiveness of their at-speed tests have often to wait for a long period to obtain meaningful fault coverage figures. This cost is stigmatized when considering timing defects, even if the transition fault model is adopted for its simplicity in modeling spot defects introducing gross-delay misbehavior at circuit nodes. The implemented at-speed stimuli transition fault grading is depicted in Figure 1.

Effective test generation achieving high fault coverage is not a trivial task, due to the fact that the test vectors generated using classical Automatic Test Pattern Generator (ATPG) at structural level must satisfy the functional constraints of the SoC. For example, a test pattern generated for a microprocessor must be converted into a legal microprocessor instruction to be used by SBST techniques.

The first goal of this work was to develop an efficient at-speed stimuli fault grading technique for delay faults. In the second part of this work, the focus will be moved to the development of an ATPG engine targeting delay faults. The ATPG must be able to generate both structural and functional test patterns to be applied on microprocessor by means of SBST techniques.

References:

Timing Issues of Transient Faults in Concurrent Error Detection Schemes

R. P. BASTOS, G. DI NATALE, M. L. FLOTTES, B. ROUZEYRE

Contact: flottes@lirmm.fr

Project/Partners: Catrene TOETS

IC-based systems are liable to encounter transient voltage variations induced by environmental or even intentional perturbation events. These effects – so-called transient faults (TFs) – are able to produce soft errors (SEs) by wrongly inverting stored results of circuit’s operations, and so they can also make failure scenarios in fault-tolerance applications. Moreover, SE-succeeded TFs can be used as a form of fault-based attack to infer secret data during the execution of encryption operations in security applications.

Related researches until the end of 20th century were focused essentially on protecting systems against TFs arising in memory elements, which were considered to be the system’s most vulnerable circuits. Hence, many concurrent error detection and/or correction mechanisms were thus proposed to mitigate direct SEs induced by TFs originating in memory circuits. Nevertheless, in the last decade IC-fabrication deeper-submicron technologies as well as novel classes of malicious fault injection-based attacks – e.g. differential fault analysis (DFA) – have also pushed on the use of countermeasures against indirect SEs due to TFs in system’s combinational logic circuits.

The traditional solution to face this issue is adding information, spatial, or time redundancy to the circuit. So if for instance a circuit’s original part fails, another redundant copy permits detecting or even correcting produced errors. In theory, such redundancy-based schemes cope very efficiently with scenarios of single SEs caused by short-duration Single TFs (i.e. STFs that last less time than a clock period), and they may not operate properly under long-duration STFs, multiple TFs, or multiple SEs. However, we reveal in our works that timing features of a short-duration STF in logic circuits can actually provoke harmful effects at the same time upon the redundancy scheme and circuit’s original parts. So, the protection can fail even for single indirect SE (SISE).

These previously-unknown SISE scenarios and STF-timing issues that make typical CED code-based schemes inefficient are further studied in our paper [1]. The schemes’ fail situations detailed in [1] have not yet been illustrated in the literature. Furthermore, [1][2] discuss timing conditions for a more efficient use of CED codes.

The vulnerability windows highlighted in this paper [1] represent risks for operations of systems that require fault tolerance; moreover they are such as attack-prone slots which could compromise secure systems. Another more efficient scheme solution is the use of a latch with an extra clock tree instead of a FF to register the error flag, but this approach would make much more complex the IC design due to the additional clock signals. Otherwise, another alternative could be improving the scheme efficiency by minimizing the STF-timing intervals for fails – discussed in [1] – in function of fitting the delay of blocks. However, this solution would not meet better timing conditions than schemes that avoid associating their redundant parts before a timing barrier.

Existing strategies for registering error signals of CED schemes are classified and analyzed in [3]. From this analysis it comes out that the choice of a strategy can considerably reduce the inherent system overheads imposed by CED schemes.

References:


A Functional Power Evaluation Flow for Defining Test Power Limits during At-Speed Delay Testing

M. VALKA, A. BOSIO, L. DILILLO, P. GIRARD, S. PRAVOSSOUDOVITCH, A. VIRAZEL

Contact: bosio@lirmm.fr

Project/Partners: Politecnico di Torino

Topic: Power-Aware Test

Testing for performance, required to catch timing or delay faults, is mandatory, and it is often implemented through at-speed scan testing for logic circuits. At-speed scan testing consists of using a rated (nominal) system clock period between launch and capture for each delay test pattern, while a longer clock period is normally used for scan shifting (load and unload cycles). In order to test for transition delay faults, two different schemes are used in practice during at-speed scan testing: Launch-off-Shift (LOS) and Launch-off-Capture (LOC).

Although at-speed scan testing is mandatory for high-quality delay fault testing, its applicability is severely challenged by test-induced yield loss, which may occur when a good chip is declared as faulty during at-speed scan testing. Both schemes (LOS and LOC) may suffer from this problem, whose the major cause is Power Supply Noise (PSN), i.e., IR-drop and Ldi/dt events, caused by excessive switching activity (leading to excessive power consumption) during the launch-to-capture cycle of delay testing schemes. In order to deal with this problem, dedicated techniques to reduce the risk of artificial yield loss induced by excessive PSN during at-speed scan testing have been proposed in the literature. These techniques are mainly based on test pattern modification or power-aware Design-for-Testability (DFT).

Despite the fact that reduction of test power is mandatory to minimize the risk of yield loss, some experimental results have proved that too much test power reduction might lead to test escape and reliability problems because of the under-stress of the circuit during test. So, in order to avoid any yield loss and test escape due to power issues during test, test power has to map the power consumed during functional mode. To this purpose, the knowledge of the functional power for a given CUT is required and may be used as a reference for defining the power consumption (upper and lower) limits during power-aware delay test pattern generation for LOS or LOC. Some techniques have been proposed so far to modify the structural patterns (e.g., LOS or LOC) in order to obtain so-called pseudo-functional patterns. These pseudo-functional patterns are able to mimic the power consumption of real functional patterns.

In this work, we propose a framework where functional patterns are generated to maximize the switching activity of a given design. Such functional patterns can be used to determine the test power limits during at-speed delay testing. To validate our framework, we developed a methodology in order to compare the power consumption of the generated functional patterns with respect to other types of patterns (e.g., LOS, LOC or pseudo-functional patterns). For each type of patterns (e.g., functional, LOS, LOC and pseudo-functional) a power estimation flow has been developed. For example Figure 1 reports the generation and power estimation flow related to the LOS scheme.

![Figure 1: Power estimation flow](image)

References:

Test Strategies for Low Power Digital Designs

M. VALKA, A. BOSIO, L. DILILLO, P. GIRARD, S. PRAVOSSOUDOVITCH, A. VIRAZEL

Contact: bosio@lirmm.fr

Project/Partners: ST-Ericsson

Topic: Power-Aware Test, Low-Power Design

Nowadays electronics products present various issues that become more important with CMOS technology scaling. Typically, with high operation speed and huge complexity, power consumption is now one of the most critical constraints during design of complex systems. The severe limitations imposed on power density increase and the large diffusion of portable equipments exacerbates the need for low power design techniques. These needs influence not only the design of devices, but also the choice of appropriate test schemes that have to deal between production yield, test quality and test cost.

To reduce power consumption different strategies have been developed like “voltage scaling” or “clock gating” techniques. Voltage scaling allows the dynamic supply voltage control, while clock gating allows inhibiting some parts of the circuit. Figure 1 gives an example of low-power devices that embed the above techniques. These techniques allow to efficiently satisfying the energy requirements of the system while maintaining the power consumption under a critical threshold.

Although high-quality test solutions are mandatory, their applicability is being severely challenged by test-induced yield loss, which occurs when functionally good chips fail only during test. Test strategies may suffer from these erroneous results, and the major cause for this problem is the excessive power consumption during test application compared to the power consumption during functional mode.

Up to now many researches have been devoted to the design of low power circuits (“low power design”). Similarly, problems induced by excessive switching activity generated during test of conventional circuits (i.e., circuits that do not include low power management structures) have been deeply studied. On the other hand, issues coming from test of low power circuits are new and offer important research perspectives.

The goal of this work is to define and implement solutions targeting power reduction during test application for low power circuits and systems. This is a new topic that offers research perspectives to a wide range of industrial applications.

In the first part of this work, we will study the main low power design techniques (i.e., voltage scaling, clock gating, power gating, etc.) and classical structural test solutions. Then, new DFT-based and ATPG-based solutions will be developed to address the challenges imposed by the test of these low-power designs. Finally, the developed test solutions will be implemented in industrial designs provided by ST-Ericsson.

Figure 1: Low-Power designs examples
Power Optimization of Transition Fault Test Vectors for At-Speed LOS Testing

F.WU, L. DILILLO, A. BOSIO, P. GIRARD, S. PRAVOSSOUDOVITCH, A. VIRAZEL

Project/Partners: Catrene TOETS

Nowadays, at-speed scan testing is mandatory for performance verification. In this context, two main test schemes targeting delay faults are predominant: LOC (Launch-Off-Capture) and LOS (Launch-Off-Shift). Although LOC testing has been more widely investigated so far, LOS testing is now used in practice in industry and needs to be improved.

In this context, our goal has been to accurately evaluate peak and average power consumption during LOS testing, so as to propose effective techniques to generate power-aware tests. For this purpose, we proposed a test flow, shown in Figure 1, and performed a detailed analysis of LOC and LOS test schemes in terms of Transition Fault Coverage (TFC) and power consumption. The results achieved lead to the following conclusions: a) LOS performs better than LOC in terms of TFC and test length b) LOS peak power is significantly higher than LOC peak power during the Launch-to-Capture cycle.

Consequently, LOS shows potential to be widespread used, provided that power consumption can be reduced or, better, mapped to the functional power. Targeting the functional power reduces yield loss due to over-stress and test escape due to under-test. In this work, we proposed a power-aware test pattern generation flow for LOS testing, shown in Figure 2. The goal is to obtain a final test set with peak power consumption as close as possible to the functional power consumption. The novelty of the proposed approach is twofold: (i) a test relaxation mechanism is used to identify don’t-care bits in a given test set, avoiding any loss in TFC and not increasing test length compared to conventional ATPG; (ii) X-filling is performed to tune the power consumption during the launch-to-capture cycle and thus map test peak power to functional peak power.

Experiments have been performed on ITC’99 circuits synthesized in a 65nm technology. The maximum peak power reduction achieved was about 50%. For large circuits, the average reduction was about 40% with 0-filling and Adjacent-filling, and 30% with 1-filling. In all cases, the combined use of these X-filling options with the conventional random filling option allows to obtain test patterns with a test power mapping functional power consumption.

References:


Modeling and Test of the ATMEL TSTAC™ eFlash Memory Technology

P.-D. MAUROUX, A. VIRAZEL, A. BOSIO, L. DILILLO, P. GIRARD, S. PRAVOSSOUĐOVITCH

Topic: NV-Memory, Flash, Memory testing

The increased usage of portable electronic devices such as mobile phones and digital camera produces a high demand for Flash memories. Flash memories are non-volatile memories that allow programming and erasing memory data electronically. The mainstream operation is based on the floating-gate concept in which charges can be stored and removed. Its low-power consumption and high integration density make it popular for portable devices.

The high integration density of eFlash memories and their particular manufacturing process steps make them prone to defects. Moreover, as high electric field is required to support its various operation, eFlash may be subject to complex disturbance phenomena.

In order to develop efficient tests for TSTAC™ eFlash memories, several type of defects have to be considered such as actual hard (open and short), resistive and coupling defects. For resistive defects presented Figure 1, electrical simulations become mandatory to analyze the possible resulting faulty behaviors of the TSTAC™ eFlash under read, write and erase operations.

In this case, electrical simulations can be easily done by means of SPICE-like description with an appropriate core-cell set-up and voltage levels on eFlash array nodes. We have proposed an electrical model of the TSTAC™ eFlash core-cell presented in Figure 2. A specific device from the ATMEL technology was used to model the two select transistors. Concerning the FG-transistor (in dashed line), the description was more complex due to particular coupling effects ($K_c$ and $K_g$ blocks) and the Fowler-Nordheim tunneling effect (FN block) phenomenon to be considered.

Another advantage of the proposed SPICE-like model is its ability to predict the behavior of the eFlash memory under technology shrinking. The model is able to consider the coupling capacitances between FG-transistors and SG-transistors. These coupling are due to capacitances between the gates of $SG_1$ or $SG_2$ transistors and the neighbor FG on the same bit line at the poly-silicon layer.

References:

Nowadays, embedded memories are made with the fastest technologies and are among the most important components in complex systems. Within SoCs, memory devices are the most diffuse components, accounting for up to 90% of the chip area. Among the different embedded memory types, SRAMs are one of the most common and are of crucial importance in modern electronic systems.

The SRAM bit-cell transistors are often designed using the minimal dimensions of the technology node. As a consequence, SRAMs are more sensitive to new physical phenomena that occur in these technologies.

Our work on SRAMs can be divided in five main branches. Some branches are devoted to improve the post-production test process. We work also with characterization and new techniques of SRAM repair. Figure 1 shows a simplified scheme that allows us to visualize how each branch of our work is placed in the context of the SRAM Test and Reliability topic. The five branches are named:

1. Resistive-bridging Analysis
2. Stress Conditions
3. Statistical Simulation
4. Variability Characterization
5. Repair Techniques

The first branch, Resistive-bridging Analysis, is an historical topic of our research group. This work completes a series of studies on resistive defect insertion on the SRAM design. In the branch Stress Conditions, we propose methodology to improve the detection of non-deterministic faults during post production test. We take into account physical phenomena that occur in modern CMOS fabrication process. This methodology is based on statistical simulations and requires simulations with extreme accuracy. A study on statistical simulation methods was then proposed, in order to achieve the accuracy requirements for SRAM bit-cell statistical simulation.

These three branches contribute to the development of more efficient test strategies. Branch number 3, Statistical Simulation, is also related to the design of SRAM bit-cells, since we proposed a method that is suitable to be used in optimization problems, due to its high efficiency.

In branch number 4, Variability Characterization, we work with silicon measurements to gather physical information that will be further used on the test development and on SRAM design activities. Thanks to the collaboration with Intel Mobile Communications, we have access to measurements performed on latest technology test chips. Finally, in our branch Repair Techniques, we work on the development of new techniques of SRAM repair. We propose an innovative fault tolerance technique that does not use traditional redundant parts, reducing area and improving timing performance.

References:

Test of Low Power SRAM Memories

L. ZORDAN, A. BOSIO, L. DILILLO, P. GIRARD, S. PRAVOSSOUĐOVITCH, A. VIRAZEL

Contact : bosio@lirmm.fr

Project/Partners: Intel Mobile Communications

Topic: Test, Low-Power, SRAMs

For several current applications (audio, video, data processing), the system performances are strictly related to the capacity (size) and speed of its memory elements. This is one of the main reasons of the memory predominance in embedded systems and System-on-a-Chip (SoC). This is confirmed by the Semiconductor Industry Association roadmap, which forecasts that in 2014 more than 94% of the overall SoC area will be composed of memories.

Memories are designed to exploit the technology limits in order to reach the highest storage density and the highest access speed. The main consequence is that memory devices are statistically more likely to be affected by manufacturing defects than other devices. Since memories are contributing for a major part in the overall SoC yield and represent a large percentage of their cost, providing efficient test solutions to successfully revealing these defects during manufacturing test is mandatory for these devices.

SRAM memories for low power applications embed either “voltage scaling” or “power gating” facilities. Voltage scaling allows the dynamic supply voltage control, while power gating allows to put unused parts of the SRAM in sleep mode. Both voltage scaling and power gating techniques are adopted in order to reduce the power consumption in functional mode. For example, Figure 1 shows an SRAM Low-Power architecture that embeds a “voltage regulator”. Owing to this voltage regulator, it is possible to specify four power modes:

1. Standby mode
2. Sleep mode (lowered power)
3. Deep Sleep mode (ultra-low power)
4. Power-off mode

In this architecture, an important aspect is to ensure data retention in sleep and deep-sleep modes.

The use of these mechanisms (e.g., voltage scaling or power gating) has various impacts on manufacturing test and reliability of these memories. First, beside classical objectives that consist in reducing test time and improving fault coverage, memory test has to deal with power constraints, and be so that power during test does not exceed power during functional mode. Second, these mechanisms themselves require the development and use of specific test procedures to exhibit potential failures.

SRAM memories for low power applications embed either “voltage scaling” or “power gating” facilities. Voltage scaling allows the dynamic supply voltage control, while power gating allows to put unused parts of the SRAM in sleep mode. Both voltage scaling and power gating techniques are adopted in order to reduce the power consumption in functional mode. For example, Figure 1 shows an SRAM Low-Power architecture that embeds a “voltage regulator”. Owing to this voltage regulator, it is possible to specify four power modes:

1. Standby mode
2. Sleep mode (lowered power)
3. Deep Sleep mode (ultra-low power)
4. Power-off mode

In this architecture, an important aspect is to ensure data retention in sleep and deep-sleep modes.

The main goal of this work will be to produce new generic and efficient test solutions for low power SRAMs. This is a new topic that offers research perspectives to a wide range of industrial applications.

We have started by a study of devices and structures used to design low power SRAM memories. Then, failure mechanisms that occur in nanometric technologies used for this type of memories, as well as their impact on current test solutions, will be studied. Finally, new test techniques and algorithms will be developed and validated on industrial low power SRAM memories.

References:

Effects of High-Altitude Radiations on SRAMs

P. RECH, L. DILILLO, P. GIRARD, S. PRAVOSSOUDOVITCH

Project/Partners: CNES, ATMEL, TRAD, IES, IM2NP

Topic: Radiation effects on electronics

Radiation effects are a major concern for electronic systems in radiation harsh environments as the space and for common electronics at sea level. Impinging particles may corrupt bits stored in the memory array (Single Event Upset – SEU, or Multiple Bit Upsets – MBUs) or generate temporary voltage pulses in logic circuitry (Single Event Transients, SETs).

We focused our attention on the study of neutron effects on SRAMs. In particular, we studied the difference of errors occurrence between Static mode (data hold) and Dynamic mode (read/write accesses).

For the former, write operations initialize the array, and read operations (performed after a predefined time, e.g. 1 hour) reveal the errors due to radiation. The dynamic mode consists of a specific sequence of operations (read/write) to be applied on the memory in order to stimulate (stress) both the cell array and the logic control circuitry.

We first performed SPICE simulations, which revealed that a traditional static test might underestimate the effective device sensitivity to neutrons, especially when the cells are affected by resistive-open defects [1]. Then, we developed a test platform composed of a large amount of memories to perform radiation tests in natural environment and by using accelerated neutron beams. This system is based on the principle of Built-On-Board-Self-Test (BOBST) that is capable of applying specific stressing sequences to the memories. We have also developed a software-based memory emulator that, connected to the BOBST, allows validating the test strategies before the actual experiments on field [2]. The simulation experiment demonstrated that our system (BOBST based) is capable of detecting any radiation-induced error in the array as well as in the logic circuitry. Then, we performed accelerated experiment at TSL neutrons facility in Uppsala, Sweden [3].

We irradiate 4Mbits SRAMs with Quasi-Monoenergetic Neutron fluxes (QMN) of 114, 150, and 180MeV and with ANITA spectrum that mimics the atmospheric environment. Fig. 1 represents the equipment used during the irradiation experiments. Results demonstrate how the stressed memory (dynamic mode) experiences a higher number of radiation-induced errors (higher cross section, Fig. 2).

We are currently developing dedicated test algorithms to be run on the irradiated memories to obtain realistic and worst case error rate occurrence in SRAMs.

Figure 1: Experimental setup inside the Blue Hall of the TSL neutron facility, Uppsala, Sweden.

Figure 2: Cross Sections of the 4Mbit SRAM for QMN fluxes obtained with static test (solid line) and dynamic-stress test (dotted line).

References:


Cryptographic algorithms are used to protect sensitive information when the communication medium is not secure. Unfortunately, the hardware implementation of these cryptographic algorithms allows secret key retrieval using different forms of attacks based on the observation of key-related information: physical information (side-channel attacks), faulty behaviors (fault-based attacks), or internal states (DFT-based attacks) for instance.

Since high quality product for secure applications is mandatory, the test of every component of the secure device must be performed. However, testing those devices faces a double dilemma: (i) how to test and, possibly, develop design-for-testability schemes providing high testability (high controllability and observability) while maintaining high security (no leakage), (ii) how to provide high security using dedicated design rules while maintaining high testability.

In the last 5 years we have proposed several techniques based either on the adaption of scan-based test to security constraints, or on the use of Built-In Self-Test architectures that allow high security while guaranteeing high levels of testability.

Scan chains, which aim to provide full controllability and observability of internal states, are against the principle of security that requires minimal controllability and observability. Techniques to adapt scan chain-based designs with respect to security constraints are based on secure scan-chain controller, detection of unauthorized scan shift by test pattern watermarking, spy flip flops, scan enable tree inspection, and data confusion.

However, we have proved that crypto-devices are well suitable for this type of test. Indeed, from one side BIST approaches are effective for secure circuits since they do not rely on visible scan chains, thus preventing scan-based attacks. Moreover, it is shown how particular characteristics of crypto-devices allow very effective pseudo random tests.

We also analyze on-line BIST solutions to increase the fault tolerance of such devices, in particular against fault attacks. This attack is based on the intentional injection of faults (for instance by using a laser beam) into the system while an encryption occurs. By comparing the outputs of the circuits with and without the injection of the fault, it is possible to identify the secret key. To face this problem we analyze how to use error detection and correction codes as counter measure.

Since dedicated design for security techniques have been proposed so far (e.g., development of specific secure cell libraries, or implementation of extra functions for preventing the leakage of useful information for key identification), we eventually discuss perspectives and trends in digital testing of such dedicated components.

References:


Fault Detection in Crypto-Devices

K. BOUSSELM, G. DI NATALE, M-L. FLOTTES, B. ROUZEYRE

Project: Catrene TOETS

Topic: Test & security, Reliability

Hardware implementations of cryptographic functions are analyzed with respect to their reliability.

Many everyday applications require confidentiality and rely on the implementation of cryptographic functions in tamper resistant devices. As any other IC, crypto-cores can be affected by permanent, intermittent or transient faults, and fail in their function, due to material defects, ageing or natural radiations. In addition, crypto-cores can also be the target of fault attacks. Intentional transient faults are used in order to by-pass security mechanisms or retrieve secret information processed by the secure device. Analysis of error-free and erroneous encrypted data, for instance, allows retrieving the encryption key. These attacks are referred as “Differential Fault Analysis” (DPA). For all these reasons, reliability of crypto-cores is of prime importance.

Among the different forms of redundancies used for on-line fault detection, we focused on information redundancy, analyzing strength and weakness of several codes with respect to their implementation on encryption standards. Due to the encryption processing, which relies on non-linear functions, basic implementation of error detection schemes involves a module for code prediction before (part of) encryption, and one for code computation after (part of) encryption (Fig.1). Predicted and computed codes are compared afterward. Code-based error detection techniques are classically compared assuming an even repartition of errors on the analyzed data.

We used one-clock-period long stuck-at faults as transient fault models and an in-house fault simulation tool [ref] for comparing several error detection schemes in terms of capability to detect errors of different multiplicities on several design implementations. We showed that error repartition due transient fault injection on gate-level nodes is extremely dependent of the crypto-core implementation. According to these implementations, fault injection result in large or small errors multiplicities. Codes, which are generally considered as the most efficient because there are able to detect large error multiplicities, are useless when the majority of fault result in small number of erroneous bit on the checked output.

References:


Scan-based Test and Security

J. DA ROLT, G. DI NATALE, ML. FLOTTES, B. ROUZERYE

Project/Partners: PROSECURE

Weaknesses of testable secure devices are questioned with respect to current Design for Testability strategies.

Insertion of scan chains is the most common technique to ensure full observability and controllability of sequential elements in an integrated circuit. However, when the chip deals with secret information, the scan chain can be used as back door for accessing secret (or hidden) information, and thus jeopardize the overall device security. Scan-based attacks assume single scan chain designs. However current very large designs and restrictions in terms of test costs require the implementation of many scan chains and additional test infrastructures for test data compression.

Recent publications claim that embedded vector decompression and response compaction lead to security improvements, and that the previous published scan attacks are not applicable in this case. In [1] we introduce a new scan attack that allows to retrieve the secret key by observing the parity of the Advanced Encryption Standard round-register (observation after test response spatial compaction), showing that test response compaction does not provide a good level of security. This attack can be used in scenarios with single or multiple scan chains and with or without spatial compressors since the parity is observable in all these cases. We also propose two dedicated counter-measures in order to mask the round-register parity while being compatible with the design and test flow.

References:

Low-Cost Testing of Analog/RF Integrated Circuits at Wafer-Level

F. AZAIS, L. LATORRE, N. POUS

Project/Partners: VERIGY

The production test of analog and RF devices is one of the major challenges for the development of modern microelectronic products. The test of these devices traditionally involves dedicated instruments to perform the acquisition or generation of analog signals. Compared to traditional digital resources, the cost of these instruments is extremely high.

Analog/RF devices are often tested twice, at the wafer-level and again at the package-level. Implementing a quality test at wafer-level is extremely difficult due to probing issues, while the inability to perform multi-site testing due to a small count of available test resources decreases the throughput. Our objective is to propose a test solution applicable with low-cost test equipment that provides wafer-level test coverage and permits multi-site testing for analog/RF signals. The fundamental idea is to complement a standard digital ATE with signal processing techniques so that it permits the analysis of analog/RF signals. More precisely, the idea is to use the comparator of a standard digital ATE channel to sample the analog/RF signal. This comparator acts as a 1-bit digitizer and converts the amplitude and/or frequency information of the analog signal in timing information into the resulting bit stream. Post-processing algorithms can then be developed to retrieve this information.

Figure 1 illustrates the 1-bit data conversion performed by the digital ATE channel. Methods have been proposed to determine level-crossing time from noisy signals [1]. Based on level crossing Time-Stamps the demodulation of AM [2], PM, and FM [3] has been investigated both in simulation and experimentally with setup shown in figure 2.

Making use of coherent under-sampling techniques, fine time resolution have been reached on high-speed signals. The demodulation of QAM signals using this technique is currently under investigation.

References:


Testing Converters with Random-phase Harmonics

V. KERZERHO, F. AZAIS, M. COMTE, S. BERNARD, M. RENOVELL

The popularity of portable data and communication applications like smart phones, laptops, or MP3/MP4 players is currently the wellspring for integration of many different functions into a single package. Systems-in-Package (SiPs) or Systems-On-Chip (SOCs) that integrate very different analogue or mixed-signal blocks have been developed toward this aim. Although they offer clear benefits such as extreme miniaturization or connection length reduction, they imply in compensation very significant test challenges. Indeed in many mixed-signal circuits, the test of the analogue blocks may represent up to 90% of the whole test effort while these blocks represent only 10% of the whole chip area. The reason of such a challenge is twofold. Firstly, analogue testing is made of a long sequence of parametric measurements that are performed using highly precise, but very expensive, instruments. Secondly, the access, the control and the observation of deeply embedded analogue blocks— and consequently, the test access, the test control and the test observation— are increasingly limited, as far as the number of pads is greatly reduced.

In order to address the issues related to the test of embedded converters, the analogue Network of Converters (ANC) concept has been defined. The ANC, presented by Figure 1, is a Design-for-Test (DfT) concept developed to enable the fully digital test of a set of DACs and ADCs embedded in a complex system.

Those innovative test configurations are supported by a signal-processing algorithm, used to discriminate the harmonic distortions induced by each converter. A limitation of the ANC-based method is that the phase of the harmonics is not taken into account in the mathematical developments of the signal processing algorithm. However the assumption that the harmonics’ phase is linearly proportional to the input signal nominal phase is not always verified and highly depends on the converter architecture. We have seen that this assumption is often verified for types of architecture that use a sample-and-hold stage, but it cannot be assessed for other architectures where filtering (cf. Figure 2) and noise may affect the harmonics’ phase.

![Figure 2: measurement setting inducing random-phase harmonics](image)

We have improved [1] [2] the ANC-based method to cover all the real-life cases. The fundamental principle of this improved version of the ANC-based method is the same, but the mathematical developments have now been established using the complete model of the general case i.e. the model described by the following equation.

\[
s(n) = x(n) + \sum_{k \geq 0} H_k \cos(k\theta_n + \theta_k) + \epsilon(n)
\]

Where \(s(\cdot)\) is the equation of a sinewave deteriorated by a converter, with \(x(\cdot)\) the sampling sinewave, \(n\) the sample index, \(\theta_i\) the input phase, \(\theta_k\) the potentially random phase of the \(k^{th}\) harmonic, \(\epsilon(\cdot)\) the noise that affect the converted signal, and \(\theta_n\) the nominal sampling phase.

![Figure 1: Analog Network of Converters (ANC) concept](image)

References:


The semiconductor industry tend to constantly increase the performances of developed systems with an ever-shorter time-to-market. In this context, the conventional strategy for mixed-signal component design, which is based only on analog design effort, will no longer be suitable.

In order to combine ADC performance with short time to design, an alternative solution is the correction of Integral Non-Linearity (INL). As presented by Figure 1, the developed solution consists in using a post-processing correction table, also called Look-Up-Table (LUT).

The efficiency of this technique is obviously based on the quality of the table used to correct the non-linearity. The table is usually computed using measurements of the Integral Non-Linearity (INL) of the ADC. INL is a conventional test parameter generally measured using a histogram-based method. This method has demonstrated its effectiveness for long periods but its main drawback is the huge amount of sampling required to compute the INL. As ADC resolution increases, test time also increases. With the rapid increase of ADC resolution, it is going to be difficult to implement this method. This is why we propose [1] alternative techniques to avoid the need for a histogram-based method to measure INL.

Based on our test vehicle, a 12-bit Folding-and-interpolating ADC, we have successfully validated a static correction table.

The study of the robustness of the proposed technique has showed that the domain of validity is very large and covers the ADC application field.

The previous study [1] has enlightened the great interest in using a LUT-based correction for ADC. The robustness validation of the approach consisting in varying several functional (sampling frequency, converting frequency) and environmental (temperature) parameters has demonstrated that the correction is optimized when the operating conditions are the same as the conditions settled for the computation of the correction table.

Based on this observation, we proposed [2] a solution for “on-line” self-calibration of ADC with the on-chip capability of computing and filling the LUT (cf. Figure 2).

As much as for Built-In-Self Test (BIST) solutions, the on-chip dedicated resources, for analog signal generation and INL measurement, has been carefully designed in order to reduce their area.

By completing the LUT ‘in situ’, i.e. directly in the application, the corrected codes are computed according to the input signal dynamic, aging and environment conditions. Indeed the calibration is performed with an integrated adaptive signal generator providing an input signal tuned according to the application.

The whole correction scheme is proved to be effective through extensive simulations.

References:
Self-Calibration of NFC Antennas

F. AZAIS, S. BERNARD, Y. BERTRAND, M. COMTE, M. DIENG, V. KERZERHO, O. POTIN, M. RENOVELL

Contact : comte@lirmm.fr

Project/Partners: NXP Semiconductors

As a result of the evolution of different applications like access control, ticketing, payment and e-documents, the deployment of Near Field Communication (NFC) devices has been growing rapidly for several years. In particular, a variety of mobile phones equipped with NFC technology to enable such applications have emerged.

Due to the wide range of devices and applications, a predefinition of antenna geometry and corresponding electrical parameters is hardly possible. Each device shows different antenna physical characteristics; moreover each application for a given device shows different needs in terms of achievable distance... Therefore, each integrator associates the NFC IC with its own antenna for each device. Current NFC transmission modules require the antenna circuitry to be manually matched with the integrated circuit (IC) (see Application tuning block on fig. 1). This step is crucial to maximize the magnetic field and, therefore, to maximize the read range and the quality of the transmitted signal. According to the ISO 14443 standard, only well-matched reader devices fulfill the standard requirements and thus enable interoperability. Manual matching of the antenna characteristics is a rather lengthy and complicated procedure. Moreover, the matching can be done only once at the device design level, regardless of the communication mode (reader, card or peer to peer) and regardless of the secondary antenna influence on the primary antenna characteristics. Therefore, the manual matching is not optimal as far as the application and environment will detune the antenna in use.

The first step in our investigation is to study the physical phenomena associated with these antennas. The goal is to predict the variations of the antenna current and magnetic field by a mathematical model. The major difficulty of this exercise is to identify the effects associated with the coupling phenomena (mutual inductance) between different antennas when the NFC system communicates with another device (fig. 2). When the primary and secondary are coupled, that modifies the antenna characteristics based on the coupling coefficient that depends on the shapes, sizes, position, etc.

The second step of this study concerns the means to monitor and control the antenna performances via a self-calibration. The NFC circuitry should be able to adapt itself to its own antenna characteristics, which may differ from one application to another. The aim is to perform a self-diagnosis of the antenna characteristics and performances in its working environment using only the NFC circuit as interface (fig. 3).

Several assessment tools available in the core of the integrated circuit can be used to derive the maximum information. Analysis in these results is expected to monitor in real time the influence of the environmental area on the antenna characteristics and act on the internal components of the circuit as well as on a part of the application tuning circuit to improve performances for better communication.
Indirect Testing of RF ICs

H. AYARI, F. AZAIS, S. BERNARD, Y. BERTRAND, M. COMTE, V. KERZERHO, O. POTIN, M. RENOVELL

Contact: azais@lirmm.fr

Project/Partners: NXP Semiconductors

Topic: RF, Analog & Mixed Signal Testing

The conventional approach for testing RF circuits is specification-based testing, which involves verifying sequentially all specification requirements that are promised in the data sheet. This approach is a long-time effective test approach but nowadays suffers from significant drawbacks. First, it requires generation and capture of test signals at the DUT operating frequency. As the operational frequencies of DUT are increasing, it becomes difficult to manage signal generation and capture using ATE. As a consequence, there is a need of expensive and specialized equipment. In addition, as conventional tests target several parameters, there is a need of several data captures and multiple test configurations. As a consequence, by adding settling time between each test and test application time, the whole test time becomes very long, and the test board very complex.

Another challenge regarding RF circuit testing is wafer-level testing. Indeed, the implementation of specification-based tests at wafer level is extremely difficult due to probing issues and high parasitic effects on the test interface. Moreover, multi-site testing is usually not an option due to the small count of available RF test resources, which decreases test throughput. Hence, the current practice is often to verify the device specifications only after packaging. The problem with this solution is that defective dies are identified late in the manufacturing flow, which leads to packaging loss and decreases the global yield of the process. In order to reduce production costs, there is therefore a need to develop test solutions applicable at wafer level, so that faulty circuits can be removed very early in the production flow. This is particularly important for dies designed to be integrated in Systems-In-Package (SIP).

In this context, a promising solution is to develop indirect test methods. Basically, it consists in using DUT signatures to non-conventional stimuli to predict the result of conventional tests. As illustrated in figure 1, the underlying idea is to learn during an initial phase the unknown dependency between simple measurements and conventional tests. This dependency can then be modeled through regression functions. During the testing phase, only the indirect measurements are performed and specifications are predicted using the regression model built in the learning phase.

This approach has been applied to a LNA from NXP. Simple Design-for-Testability (DfT) circuitry has been inserted within the chip to allow observation of some internal nodes. Embedded sensors can also be considered to give information on the variability of some crucial process parameters. Indirect parameter measurements only involve DC and low-frequency measurements. As an illustration of the performance of the method, figure 2 shows the predicted gain using only indirect measurements vs the gain measured with a conventional RF test; a good correlation can be observed.

The main benefits of this approach are: (i) no need of expensive RF ATE since only DC and low-frequency measurements are performed, (ii) test time reduction since only a limited number of test configurations are used, and (iii) fault coverage at wafer level.

Figure 1: Indirect RF IC test synopsis

Figure 2: Example of correlation between measured and predicted RF parameters
Design & Test of MEMs
Alternate Electrical Test & Calibration of MEMS Accelerometers

F. AZAIS, N. DUMAS, F. MAILLY, P. NOUET, A.A. REKIK, Contact: azais@lirmm.fr

Project/Partners: ENIS, University of Sfax, Tunisia Topic: MEMS Testing

MEMS are multi-domain systems that find an increasing use in a number of applications. In particular, their deployment for high-volume and low-cost applications is expected to keep on growing. In this context, there is of great interest to reduce test and calibrations costs, which represent an important part of the total manufacturing costs. Indeed due to their multi-domain nature, they usually require the application of physical test stimuli to verify their specifications, necessitating specific and sophisticated test equipment much more expensive than a standard ATE. Moreover, MEMS devices are generally quite sensitive to manufacturing process variations and calibration is often required to achieve satisfactory yield.

An interesting approach is to develop alternate electrical-only test and calibration techniques. A number of solutions have been proposed in the last decade for various types of MEMS such as accelerometers, magnetic field sensors, or pressure sensors. This project focuses on test and calibration of MEMS accelerometers’ sensitivity, which is the most challenging specification to measure without applying a calibrated acceleration. Two different types of accelerometer are considered, i.e. capacitive and convective accelerometers (see fig. 1 and 2).

The proposed approach (see fig.3) relies on an initial learning phase in which sensitivity to acceleration is measured directly as well as alternate electrical test parameters on a learning set of devices. These data are then used to derive a regression model that maps the pattern of electrical measurements to sensitivity. During the testing phase, only electrical measurements are used to estimate each new device sensitivity performance. The estimated sensitivity ($S_e$) can then be used for test and calibration.

References:


Smart Wafer-level Packaging for Micro-Electro-Mechanical Systems

N. DUMAS, S. HACINE, L. LATORRE, F. MAILLY, P. NOUET

Contact: mailly@lirmm.fr

Project/Partners: ANR Midisppi, IMS, IEF, NXP, KFM

Topic: Integrated Sensors

In mobile applications, Systems in Package (SiP) are commonly used. Figure 1 presents a SiP example from NXP Semiconductors where radio frequency (RF), analog, mixed signal and digital circuits are connected together by means of a silicon-based passive substrate. This substrate replaces the printed circuit board (PCB) and can be used to integrate RF passive components such as resistors or 3D-capacitors.

More recently, MEMS components have also been integrated within SiP. They need to be enclosed in a sealed cavity which quality has to be guaranteed in terms of pressure and humidity. For this purpose, environmental sensors (temperature, pressure and humidity sensors) may be integrated in the wafer-level packaging so that the final manufacturing test consists in checking the environmental parameters directly from those sensors. Moreover, during the life of the system, a periodic check of these sensors may be useful to be sure that MEMS performances are still within the specifications. At last, for a low deviation of the environmental parameters, and thus of system performances, sensor data can be used to calibrate the functional MEMS using an electronic loopback. Therefore, this smart wafer-level packaging will increase the manufacturing yield and the long-term stability of the system. Figure 2 shows a pressure sensor for such application. It is based on the Pirani gauge principle: the pressure-dependent heat losses of a self-heated microbridge through a surrounding gas. The sensor has been modeled and two different architectures have been investigated for electronic conditioning [1, 2]. For temperature sensing, an ultra low power sensor (Figure 3) has also been developed with a direct digital output [3].

References:


One-Chip Inertial Measurement Unit: Low-cost 3D Orientation Determination System

B. ALANDRY, F. MAILLY, L. LATORRE, P. NOUET

Contact: nouet@lirmm.fr

Topic: Integrated Sensors

A multi-sensor platform has been developed to demonstrate our capabilities in sensor integration. Most of the know-how of the research team is illustrated in this project: sensor behavioral modeling, system-level simulation, front-end electronics, power management, wireless communication, embedded software, human machine interface...

The choice of a mature technology for the sensors makes the system suitable for low-end applications (e.g. consumer electronics) where the main trade-off concerns the power consumption, the cost and the size of the device. Our objective is thus to develop a low-cost, low-power, medium performance, highly integrated system.

The complete system is composed with three different sensors (a 2D in-plane accelerometer, a 1D out-of-plane accelerometer, a 2D in-plane magnetometer). All of them result from our previous research and have been extensively studied. Each sensor is connected to a specific front-end electronics that allow efficient offset compensation and cancellation schemes that are mandatory due to the low intrinsic performance of bare sensors. This architecture is completed with an embedded controller and a wireless communication module. The whole is powered by a battery. Details on most of these blocks are available elsewhere when browsing the research activity of our team.

SiP integration (figure 1) uses a passive substrate traditionally used to implement passive elements (R,L,C) and to connect them with one or several ICs to realize compact systems in a single package...

In our case, all sensors have been fabricated on the same technology and a CMOS electronic front-end has been added.

SoC integration (figure 2) is based on a CMOS 0.35 µm process that ensures a good trade-off between sensor cost and efficient electronic front-end. In both cases, electromechanical parts are released using wet etching as a self-aligned CMOS post-process.

Figure 1: Individual dies of the SiP IMU (z-axis accelerometer die not shown).

Figure 2: One-Chip IMU includes three different sensors and the front-end electronics on the same CMOS die.

References:


This study is part of a project that targets the design of reflect array antennas for telecom applications. In this application, thousands of MEMS switches are embedded into RF cells to open or short RF paths so that a continuous phase shift is achieved between incident and reflected waves. Because a huge quantity of MEMS is used in a small surface the control and driving circuitry must be integrated close to the active area and a control architecture based on high-voltage ASICs has been defined. As different switch configurations may achieve the same phase shift, the architecture features an intrinsic redundancy so that alternate RF path may be used if non-working MEMS are identified. This is the reason why we proposed a diagnosis circuitry. From a RF point of view, this diagnosis is non-invasive since RF paths are not altered in any manner. It is based on the monitoring of the actuation current and thus only concerns the actuation circuitry. The measure must be as insensitive as possible to the routing between the driver and the switch.

We have investigated simple and fully integrated solutions for measuring the capacitance variation during pull-in event. The first one is based on a single step actuation voltage and a time-based technique to discriminate actuation capacitance increase during pull-in from stray capacitance. The second one is based on a two step actuation voltage and a differential technique. Finally, the use of a ramp-shaped actuation voltage provides good results in detecting both pull-in and pull-off events.

Switches depicted in figure 1 are fabricated by a partner. The design of the drivers includes the switch modeling in Verilog-A language and co-simulation within Cadence®. Figure 2 shows the 2nd generation of drivers integrated using a 0.35µm 50V CMOS technology.

The measure in figure 3 shows the peak in actuation voltage related to the pull-in event, which is used to perform the diagnosis. All drivers have been experimentally validated on various switches.

References:


Integrated Spin-Valves for Bio-Systems and Current-Sensors

N. DUMAS, S. HACINE, F. MAILLY, L. LATORRE, P. NOUET

Project/Partners: ANR SPIN/CEA-LETI, CEA-LIST, 3D+

Giant Magneto Resistive (GMR) effect discovery has paved the way for the application of spintronics science to new integrated circuits based on the spin of electrons. It had a great impact on data storage device. Another domain where GMR effect is expected to lead to significant advances is integrated magnetic field sensing through spin-valves. The LIRMM is involved in designing the adapted read-out electronic of the spin-valves for two applications. The first one concerns the integration of an array of very sensitive magnetic sensor for detecting specific particle in medical application. The second one aims the integration of current and monitoring systems with high insulation for fuel cells used in automotive for example.

A new patented structure [1] for resistive sensors has been adapted and designed for these two previously described applications. It will allow evaluating this alternative to the Wheatstone in real conditions. This solution, called active bridge, has been demonstrated to provide an advantage in terms of trade off between SNR and power consumption. It can be used in an open loop in order to directly provide a strongly amplified analogue signal. For better sensitivity control, an analogue or digital closed loop system are preferred.

For biochip application, the analogue feedback provides amplification with a simple operational amplifier (figure 1). This simple circuit provides the equivalent performance compared to a Wheatstone bridge followed an instrumentation amplifier.

For the current sensing application a digital feedback provides directly a digital output (see on figure 2). This work has been published in a workshop on new integrated circuits and systems [2]. We demonstrated that the proposed read out structure should be independent on the power supply voltage and the temperature. A study of the best digital solution to feedback the structure has also been conducted. Finally a chip (figure 3) with a SPI interface has been designed and fabricated and is currently under characterization.

---

References:


Exploitation of NonLinear Dynamics to improve the Performance of Energy Harvesters

C. TRIGONA, N. DUMAS, F. MAILLY, L. LATORRE, P. NOUET

Project/Partners: DIEEI, University of Catania

This study is part of a research that targets the exploitation of novel nonlinear MEMS mechanisms for energy harvesting applications based on ambient vibrations. The increasing demand for self-powered devices and autonomous sensor nodes has caused an increase of research into power harvesting devices in recent years. Energy harvesting can be obtained from different energy sources; in particular, we focus on mechanical vibrations. A common approach is based on vibrating mechanical bodies that collect energy through the adoption of self-generating materials. This family of systems has a linear mass–spring–damping behavior and shows good performance around its natural frequency. However, it is generally not suitable to harvest energy in a wide spectrum of frequencies as expected in the vast majority of cases. Indeed, when ambient vibrations are considered, energy is distributed over a wide range of frequencies. Furthermore, whenever vibrations have a low frequency component, the implementation of an integrated energy harvesting device is challenging; in fact, large masses and devices would be needed to obtain resonances at low frequencies. The idea pursued here is to consider the nonlinear behavior of a bistable system to enhance device performances in terms of response to external vibrations.

The switching mechanism is based on a structure that oscillates around one of the two stable states (Fig.1) when the stimulus is not large enough to switch to the other stable state and that moves around the other stable state as soon as it is excited over the threshold (Fig.2). Compared to the classical linear approach, a response improvement can be demonstrated (Fig.3). Indeed, a wider spectrum appears as a consequence of the nonlinear term and a significant amount of energy is collected at low frequencies [1].

References:

Low-Power Front-End for Resistive Sensors

E.M. BOUJAMAA, N. DUMAS, S. HACINE, L. LATORRE, F. MAILLY, P. NOUET

Interest for cheap and low-power integrated sensors is constantly growing with the development of low-cost portable consumer products and Wireless Sensor Networks (WSN). The use of standard CMOS technology together with cheap wet-etching post-process enables the batch fabrication of monolithic multi-sensor circuits that include accelerometers, magnetometers, microphones, pressure sensors, and temperature sensors. The design of such low-cost multi-sensors system is limited by a set of fabrication constraints that makes the use of capacitive sensing very difficult if not impossible. Therefore, resistive sensing is generally considered using either the piezoresistivity of polysilicon for mechanical devices or the temperature dependence of integrated resistors for thermal applications (including thermal accelerometers).

Resistive sensing is commonly valued for its low cost and ease of implementation but suffers from poor performance regarding the power consumption and the signal-to-noise ratio. In this context, we have proposed and patented an innovative circuit for the conditioning of resistive sensors that addresses the above mentioned issues. This so-called “Active Bridge” (figure 1) structure aims at providing amplification and limited noise contribution while using the same current to bias both sensing elements and amplification circuitry.

The Active Bridge main features are a high gain and high output impedance at very low biasing current (typically in the µA range or below). The implementation of a feedback circuitry is necessary to address gain and process mismatch issues.

Both analog (i.e. continuous time) and digital (i.e. ΣΔ) feedback schemes have been investigated in various applications (inertial sensing, magnetic sensing). A digital output, high-resolution, micro-power, temperature sensors based on complementary temperature coefficient of resistors in an Active Bridge has been also developed and characterized.

\[ v_{out} = -4g_m I_0 \left( \frac{r_{ds1}}{r_{ds2}} \right) \Delta R_{eff} \]

Figure 1: Architecture of the “Active Bridge”

Both analog (i.e. continuous time) and digital (i.e. ΣΔ) feedback schemes have been investigated in various applications (inertial sensing, magnetic sensing). A digital output, high-resolution, micro-power, temperature sensors based on complementary temperature coefficient of resistors in an Active Bridge has been also developed and characterized.

Figure 2: CMOS Temperature sensor based on the Active Bridge and polysilicon thermistors

References:


Adaptive Circuits & Systems
Adaptive Techniques for Massively Parallel Multiprocessor Systems-on-Chip (MPSoCs)

G. SASSATELLI, P. BENOIT, L. TORRES, M. ROBERT, G. M. ALMEIDA, N. HEBERT

Contact: sassatelli@lirmm.fr

Project/Partners: Eniac MODERN / LIP6, CEA-LETI, ST-Microelectronics

Topic: MPSOC

The exponentially increasing number of transistors that can be placed on an integrated circuit is permitted by the dropping of technology feature sizes. This trend plays an important role at the economic level, although the price per transistor is rapidly dropping the NRE (Nonrecurring Engineering) costs, and fixed manufacturing costs increase significantly. This pushes the profitability threshold to higher production volumes opening a new market for flexible circuits which can be reused for several product lines or generations and scalable systems which can be designed more rapidly in order to decrease the Time-to-Market. Moreover, at a technological point of view, current variability issues could be compensated by more flexible and scalable designs. In this context, Multiprocessor Systems-on-Chips (MPSoCs) are becoming an increasingly popular solution that combines flexibility of software along with potentially significant speedups.

These facts challenge the design techniques and methods that have been used for decades and push the community to research new approaches for achieving system adaptability and reliability (out of unreliable technology components). Since this work targets massively parallel on-chip Multiprocessor systems, scalability is a major concern in the approach. For this reason, we put focus on distributed memory machines and therefore choose a message passing programming model for it provides a natural mapping to such machines.

The proposed system is based on an array of compact general-purpose PEs interconnected through a packet switching Network-on-Chip.

The architecture is a purely distributed memory system that is programmed using a simple message passing protocol. Contrary to MPI, processes must not be mapped to a given processor but shall freely move in the system according to user-definable policies that may aim at optimizing a given property in the system, such as performance or power consumption. Both hardware and software resources are intended to be minimalist for favoring compactness of processors and therefore encouraging massive parallelism. Also, for scalability reasons, there exists no master in the system unless a given application requires it. Figure 1 presents a structural view of the architecture.

References:


Distributed Mechanisms for Adaptive Architecture Control

I. MANSOURI (CEA LETI), P. BENOIT, L. TORRES, F. CLERMIDY (CEA LETI)

Project/Partners: ANR ADAM / CEA LETI

In 2008, the International Technology Roadmap for Semiconductors (ITRS) predicted that the number of processing cores in SoC (System on Chip) for consumer portable systems will increase, reaching up to six hundred cores in the next 10 years. Such systems provide more functionality with potentially higher performance. In the other hand, their complexity underlines many challenges, such as power management.

We address the energy management issue in multi-core architectures articulated around a Network-on-Chip (NoC) as illustrated in Fig.1, assuming distributed sensors to collect the power consumption of each core, and actuators to adapt the voltage and frequency (DVFS) of each Processing Element (PE).

Considering multi-core architectures, the challenge is to go towards a scalable scheme of power management, where centralized control approaches are no more possible as it was demonstrated in [3]. Our focus is on a run-time distributed approach.

An existing controller inspired by game theory concepts, aims at modeling PEs as independent players, which can adjust their local frequencies via an in situ DVFS engine. We proposed Hardware/Software implementations of this technique and we evaluate induced overheads [2] in terms of area and latency.

While implementation results are promising, some problems related to the equilibrium stability and communications load were consequent. As alternative, we used consensus-based algorithms with limited neighborhood. Each PE operates with its nearby neighbors to reach an overall global “consensus” on the optimal settings corresponding to a given application. Depending on applied constraints, energy gains reach 46% compared to a worst-case static configuration as shown in Fig.2 [1].

Our current work includes the integration of some digital activity sensors in our control scheme, in order to feed our algorithm with accurate estimation of the system whole consumption.

References:
Variability has become a major issue in the semiconductor market due to its impact on manufacturing yields, performance and power consumption. A fine management of these physical disparities is a key to success for more reliable technologies. Despite suffering from the same symptoms, FPGAs have great advantages over other circuits: the regularity and the reconfigurability. These fundamental characteristics offer the possibility to map the same design to different regions of the circuit.

In our work, we investigate the problem of variability characterization in FPGAs. We provide a twofold method for variability compensation based on digital sensors used either at design-time or at run-time. Basically, it uses FPGA digital resources (LUTs and interconnects) to implement Hard Macro sensors. An overview of our methodology is depicted in Figure 1.

First, the FPGA performance is deeply analyzed off-line at a fine granularity by our dedicated monitors at design-time. In order to realize an accurate characterization of performances, an array of sensors covering the whole area is used (Fig. 1(a)). Sensor data are collected and analyzed to build a cartography of the floorplan (Fig. 1(b)). Once the cartography of the FPGA is built, a placement strategy is performed, considering both the system and its run-time monitoring service (Fig. 1(c)).

The second stage of the compensation flow is based on hardware run-time monitoring. The run-time system implemented in the FPGA is composed of a microprocessor, some peripherals, a Management Unit (MU), a set of sensors and actuators. The on-line monitoring process is illustrated in Figure 1(c). Our objective is to perform a dynamic compensation of system variations. For this purpose, a subset of digital sensors using the FPGA resources is implemented. Digital sensors measure performances; data monitoring are then collected and analyzed by a management unit. Based on the information available, this unit can adapt the system to the actual performances.

References:


System-Level Dependable Methods for MPSoCs

P. BENOIT, G. SASSATELLI, L. TORRES, N. HEBERT

Project/Partners: ST-Microelectronics

Topic: MPSoC, Fault tolerance

The natural redundancy of MPSoCs is increasingly seen as a possible attractive means to the purpose of producing reliable systems out of unreliable technology devices. Amongst the main arising challenges, maintaining the dependability attributes of massively parallel multiprocessor systems under increasing defect rates is an important concern yet to be addressed.

This work targets a scalable hardware/software framework aimed at detecting, isolating and enabling system recovery while maintaining a reduced area and performance overhead [2].

The method called D-Scale [1] (Dependable-Scalable, Figure 1) has been developed, that aims at reducing to the minimum overall overhead and to maintain high coverage of crash faults for the targeted application domain. In order to be transparent, the approach has to be autonomous, scalable and distributed. This low cost solution intends to detect crash faults on any processor, to take remedial decisions (recovery phase), and maintain statistics across system reboots for fine-tuning the decision-making strategy that ranges from scaling electrical parameters (voltage and frequency) to definitive processor isolation.

Figure 1: D-Scale overview.

Figure 2 shows a comparison of the reliability between the original MPSoC without any protection and the MPSoC with D-Scale. For different test cases, the MTTF (Mean Time To Failure) has been improved by a factor of 2.71 to 2.91 compared to the original MPSoC.

References:


Securing an Embedded Linux Boot on FPGA: a Trusted Chain from Bitstream to OS

F. DEVIC, L. TORRES

Project/Partners: ANR SecReSoC / Netheos

Contact: torres@lirmm.fr

With most of the FPGAs, the OS is stored into an external memory (usually Flash) and running on a processor embedded into the FPGA. We consider that FPGA embedded processor is able to process the OS update through, for instance, an insecure network. However, these features may give rise to security flaws affecting the system integrity or freshness. Spoofing or modifying data in order to introduce malicious code can alter integrity. In the same way, updated configuration (versioning) can be affected by replaying an old configuration in order to downgrade the system.

This work proposes a trusted computing mechanism taking into account the whole security chain from bitstream-to-kernel-boot ensuring, both hardware and software, integrity while preventing replay attacks into FPGA devices.

Figure 1 illustrates how to secure remote bitstream updates preventing replay attacks on FPGA embedding user non-volatile memory. The objective is to lock the FPGA to a dedicated bitstream version preventing downgrades. The bitstream version number (TAG) is stored in non-volatile user memory and can be incremented thanks to our protocol using secret keys [1].

Figure 2 describes the protected boot steps of the embedded Linux on generic FPGA. This boot mechanism precludes kernel modifications using Sha-256 hash function, prevents against replays attacks and supports updates [2]. It uses a flexibility improvement involving asymmetric cryptography that allows changing the kernel in external memory without changing the bitstream.

References:


Securing Microprocessors against Side-Channel Attacks

P. BENOIT, L. TORRES, L. BARTHE

Project/Partners: ANR SecReSoc / DGA

Contact: pbenoit@lirmm.fr

Topic: Hardware Security

Designing efficient countermeasures to thwart Side-Channel Attacks is a real challenge. By combining judicious countermeasures, the resistance of integrated circuits against such malicious attacks can be significantly improved. But a secure implementation does not come for free. The extra-hardware cost usually leads to an increased power consumption, and performance penalties. These observations are all the more important for embedded systems, where hardware constraints are a challenging issue. Hence, the security questions of crypto-systems have introduced new strategies for designers aiming at striking the balance between security issues, and embedded requirements. The scope of this work is to investigate side-channel threat models for embedded processors, as well as to develop new approaches, models, and techniques to address security problems.

The evaluation of a standard 5-stage RISC processor was performed with the Data Encryption Standard (DES), one of the most famous symmetric crypto-algorithm, implemented in ANSI C code on a Xilinx Spartan-3 Starter Kit board. A Differential ElectroMagnetic Analysis (DEMA) was conducted and the secret key was discovered with very few measurements: less than 500 electromagnetic traces with different experimental settings were sufficient to break the crypto-algorithm. Besides, the most interesting result concerns the effect of the pipelining technique. Fig. 1 illustrates the DEMA obtained for the first sub-key, with a large number of electromagnetic traces (50,000), in order to emphasize the impact of this hardware feature. In the following picture, the black curve indicates the correct sub-key, while the others correspond to the wrong sub-key hypotheses.

Reference:


Figure 1: DEMA traces for the first sub-key of the DES.

These results underline the considerable vulnerability of a pipelined processor architecture. The margin, which is basically defined as the minimal relative difference between the amplitude of the differential trace obtained for the guessed sub-key (black curve) and the amplitude of the differential traces obtained for the other sub-keys (other curves), reaches more than 50% for the correct sub-key during several time periods. In order to tackle such vulnerability, a dedicated masking countermeasure has been investigated in [1]. The significant reduction of the undesirable effects of the pipelining technique is the most striking benefit of this study. The experimental results also revealed that this approach must be coupled to other protection mechanisms in order to provide efficient security services towards side-channel analysis.
Magnetic Memory (MRAM) Based Architecture: FPGA to Processor

LV. CARGNINI, R. BRUM, Y. GUILLEMENET, G. SASSATELLI, L. TORRES

Project/Partners: ANR Cilomag, ANR Spin / CEA, CROCUS, EADS

Topic: Reconfigurable Architecture

Most Field programmable Gate Arrays (FPGAs) are currently SRAM based [1]. In these devices, configuration memory is distributed throughout the chip. Each memory element has to be readable independently because each of these cells drives a transistor’s gate or a look-up table (LUT) input [1].

The short access time of the static random access memory (SRAM) technology makes it popular in the FPGA industry. Nonetheless, its volatility and the need of an external non-volatile memory to store the configuration data makes it not suitable for many embedded applications. Indeed, in embedded FPGA devices, the use of a non-volatile internal memories such as Flash technology allows powering off of the device for saving energy without requiring reloading of the bitstream at each power-up. Some FPGAs and complex programmable logic devices use flash memories such as Actel’s fusion products that indeed benefit from instant availability upon power-up.

However, distribution of the memory throughout the chip raises some technological constraints and requires additional masks (10–15 for the Flash technology) and dedicated process steps, thereby increasing manufacturing costs. Moreover, these FPGAs lack several features compared to SRAM-based devices, such as partial or dynamical reconfiguration and fast reprogramming speed, due to long access time inherent in the flash memory.

The use of non-volatile memories such as Magnetic Random Access Memories (MRAMs) helps to overcome the drawbacks of classical SRAM-based FPGAs without significant speed penalty. MRAMs exhibit interesting features that include high timing performance, high integration density, reliable data storage and good endurance. Furthermore, a less number of additional masks are required for the magnetic post-processing. For this reason a first FPGA architecture has been designed and proposed in 2010 [2]. Now, with the knowledge gained in this study we are interested now to perform new research in the area of embedded processor coupled with MRAM technology.

The research aims to evaluate the impact and improvements on processor architecture, replacing memory elements by non-volatile ones. One possible research activity also will be to evaluate the reliability of MRAM based processor against SEU effects for instance [3].

Figure 1: MRAM based FPGA (CMOS 130nm, MRAM 120nm).

The research aims to evaluate the impact and improvements on processor architecture, replacing memory elements by non-volatile ones. One possible research activity also will be to evaluate the reliability of MRAM based processor against SEU effects for instance [3].

References:


eFPGAs Architecture Design, System Integration & Survey of Programmable Technologies in Industry

S. Z. AHMED, G. SASSATELLI, L. TORRES

Contact: torres@lirmm.fr

Project/Partners: MENTA

Topic: Embedded FPGAs & Configurable SOC

Rising design complexities and high manufacturing costs of System on Chip (SoCs) in deep submicron nodes (below 90nm) have reached levels where dedicated SoCs can no longer be designed for every application. They must have some post manufacturing flexibility to amortize the high development costs to several end markets. The Field Programmable Gate Arrays (FPGAs) are well known for their flexibility and ease of design modification. With Moore’s law they have become programmable platforms and in many cases provide a good alternative to implement SoCs directly on them. Unfortunately FPGAs suffer from large silicon gap compared to ASICs (SoCs), inhibiting them for high volume products. Our research work focuses on embedded FPGAs (eFPGAs) which are interesting alternative to bridge SoCs and FPGAs. The research is focused in three major axes. (i) Survey and analysis of programmable technologies to investigate scope, potential, challenges of eFPGAs. (ii) eFPGAs architectural explorations and tools infrastructure to create silicon-efficient (area, power, speed) customized eFPGAs. (iii) eFPGAs system integration (particularly for reconfigurable acceleration) and investigations of potentials of emerging technologies like MRAM memories for eFPGAs and FPGAs.

Figure 1 presents the theme concept of eFPGAs for SoC, highlighting they can be integrated as an IP along with other components. This allows bringing key benefits of FPGAs like flexibility, time to market, product differentiation etc. right inside SoC. Figure 2 depicts the architecture of eFPGAs which has a classical FPGA-like 2D mesh Look-up Table (LUT) based architecture. The eFPGA can be programmed using standard RTL flow like FPGAs making their benefits for SoCs further prominent. [1] Presents a general survey highlighting key programmable technologies in industry, changing trends and their effect on/for research community. [2] Presents infrastructure developed in our research to create eFPGAs. [3] Outlines the potentials of eFPGAs for reconfigurable acceleration (with specific focus on silicon tradeoffs and programming complexity) with practical experimental analysis. [4] Describes the potentials of emerging MRAM memories for FPGAs and how with effective synergetic research efforts of LIRMM with its partners helped taping-out physical FPGA test chips based on hybrid (CMOS+MRAM) technology, well-noticed by industry observers.

References:


Biomedical circuits and systems
Functional Electrical Stimulation (FES) has been used for about 30 years in order to restore deficient physiological functions. At the beginning, only surface stimulation was possible and thus only used in a clinical context due to the low reliability of electrode placements. In the early eighties, implanted FES appeared through well-known applications: pacemaker, Brindley bladder control, cochlear implant, and more recently deep brain stimulation (DBS).

Currently, FES is the only way to restore motor function even though biological solutions are studied, but not yet successfully tested on humans. Few teams carry out researches on implanted FES and the functional results remain poor.

The team developed a microstimulator in 2006 and a prototype (ASIC) was fabricated. The microstimulator can be divided into two main parts: a controller (digital) and an active part (analog). In the active part, the output stage gets its input current from an external DAC converter which set the maximum stimulation amplitude. This current is then distributed to a twelve-pole stimulating electrode. A pole can be set in four different states: anode, cathode (both current controlled), open (high impedance) or shunt (voltage-controlled). A digital block controls the evolution of the pole states and the ratio of the stimulation current on each pole.

Some faults were observed while carrying out the circuit characterization. These faults were of four main kinds:

- asymmetry between poles (up to 108 μA),
- input/output non-linearities (over 4 LSB),
- over-consumption on idle state,
- erratic level-shifter behavior.

Since 2006, some researchs and experiments were carried out and few subcircuits were developed to fully access its faults and correct them. Finally, a corrected version was designed in 2010. The new IC offers three structural modifications and better layout techniques to improve the stimulator characteristics. Some simulation results are presented in the following pictures. The fig. 1 shows an improvement of the symmetry between poles (down to 39 μA) while the fig. 2 highlights a non-linearity reduction to 0.66 LSB. The command structure was also modified to get rid of the over-consumption. Finally, the level-shifter parts were designed anew.

The corrected ASIC was manufactured on November 2010 and is now under test and characterization.

![Figure 1: Simulated voltage/current characteristics of CAFE12](image1)

![Figure 2: Simulated non-linearities of a typical electrode (cathode in red and anode in black)](image2)
The FES (Functional Electrical Stimulation) implanted system may be hazardous for patient and the reliability and dependability of the system must be maximal. Unfortunately, the associated systems are more and more complex and the fact that their development needs very cross-disciplinary experts is not favorable to safety. Moreover, the direct adaptation of the existing dependability techniques from domains such as space or automotive is not suitable. Therefore, we have developed a strategy for risk management at system level for FES medical implant. The idea is to give a uniform framework where all possible hazards are highlighted and associated consequences are minimized.

The base of the proposed risk management method is an algorithm. This algorithm must be as simple as possible to achieve the best coverage of defective cases and propose the highest level of confidence and safety of the system (see figure 1).

The functional Analysis defines the system, its environment and its external limits. Then, we create specific expertise group defined according to their skills. Each working team will now write its own hazard’s analysis which draws up the full list. Once each working team has established its specific hazard’s analysis, it is then sent to the person in charge of the dependability study. The hazard chart has to be as exhaustive as possible. Afterwards, a global risk analysis will be conducted.

We associate to each hazard a probability of occurrence and a level of consequence. According to this classification, each working team will be asked to either decrease the probability of occurrence or the consequence of a risk with appropriate countermeasures. They will develop specific Built-In-Self-Test and Built-In-Self-Repair solutions of hazards that can occur in order to increase the dependability of the system. The dependability study has to be carried on over the entire life of the project, thanks to the experience feedback, the study can be completed and improved.

References:
Selective Electroneurogram Recording

O. ROSSEL, F. SOULIER, S. BERNARD, G. CATHEBRAS

Contact: soulier@lirmm.fr

Project/Partners: AXA, INSERM

Topic: Nerve Model & Analog Signal Processing

In the context of FES, neural recording is one of the most promising research areas. Artificial control of human limbs needs to know the position of the different parts of the human body. Natural sensors (like neuromuscular spindles and Golgi tendon organs) can bring information about the stretching, velocity and force of the muscles. This information is carried on afferent peripheral nerves and can be recovered from electroneurogram (ENG). We propose to investigate the topic of extracellular action potentials (AP) composing ENG, in order to design a new kind of electrode and the associated microelectronics to create an implantable acquisition system.

The presence of high spatial frequencies in the AP signal means that the amplitude of a measured AP depends on the electrode position. In other words, electrodes spaced by some hundreds micrometers one from each other on the longitudinal axis of the nerve should get different measures. A first experiment was made using a worm because this simple animal model exhibits giant axons analogous to a certain extent to mammalian myelinated fibers. A second one was made using a database of rabbit intra-fascicular recordings to prove this postulate. Eight electrodes were used in the experimentation on the worm, and four for the rabbit.

The results tend to prove that there are actually some differences on the measured amplitude of an AP according to the electrode location. Unfortunately, it was difficult to positively conclude due to the noise level of the signal. Nevertheless, thanks to these preliminary experiments, we can conclude that the number of recording channels has to be increased and the noise level has to be lowered as much as possible. The investigated solution is the design of a 32-channel high-gain and low-noise amplifier.
Continuous Intra Ocular Pressure Measurement for Glaucoma Diagnosis

S. BERNARD, F. SOULIER, O. POTIN

Project/Partners: MATEO / Ophtimalia, Institut de la Vision, ESIEE, CEA

Glaucoma being an ocular pathology and the second cause of blindness in people over the age of 50, the aging of the world population will lead to further increase the number of patients greatly visually impaired by this disease. In most cases, glaucoma is associated with an increase in Intra Ocular Pressure (IOP). In this work funded within the ANR-TecSan project MATEO, we are developing disposable eye lenses including a specific pressure sensor to measure IOP all day long. The instrumented lens will communicate by radio frequency to an electronic chip located on glasses arms and daily information would thus be available for ophthalmologists to improve diagnoses.

The system consists of a sensor implanted on a lens and an external reader on the glasses, see figure 1. The system is therefore based on inductive coupling between the coils L1 and L2 respectively representing the reader and the embedded sensor.

Figure 1: Principle of the wireless communication (sensor in the lens and reader on glasses).

So any parameter variation on the lens induced by a mechanical deformation of the cornea will be converted into a frequency shift, detectable while measuring either the impedance magnitude or phase.

The challenges are multiple. Firstly, the sensor design must offer the maximum sensitivity due to the small deformation of the cornea (less than 3µm). Secondly, it should be coupled with the integrated antenna on a small transparent polymer lens. Thirdly, electronics should deal with a composite signal degraded by strong interferences to extract data and provide a reliable and accurate IOP measurement.

We proceed by modeling the complete system (see figure 2) from the mechanical deformation of the eye to the electrical measurement. This model permits to propose implementations of signal processing and high-level architecture of the active integrated circuit, under high constraints in terms of area overhead, power consumption, robustness, testability and safety. Moreover, we develop algorithms for measurement data extraction. Finally, a key point remains the integration of auto-test techniques to guarantee the reliability of the system. The aims are both to analyze the system before delivery and adapt it to environment variations by an auto-calibration process.

Figure 2: high-level model of the measurement system.

In parallel, first experimental results demonstrate the feasibility of the IOP measurement with the prototype sensor. We can observe on figure 3 that the impedance phase slightly changes while the IOP is increased by injecting fluid inside pig eyes on which the sensor is tested.

Figure 3: Measured phase vs frequency with IOP varying from 10 to 70mmHg.

References:
Summary of 2010 Publications

Summary

<table>
<thead>
<tr>
<th>Article Type</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Articles in International Journals</td>
<td>17</td>
</tr>
<tr>
<td>Invited Conferences</td>
<td>7</td>
</tr>
<tr>
<td>Papers in International Conferences with Review Process and Proceedings</td>
<td>78</td>
</tr>
<tr>
<td>Books</td>
<td>2</td>
</tr>
<tr>
<td>Patents</td>
<td>1</td>
</tr>
</tbody>
</table>

Notes

- Papers published in proceedings of major international conferences, symposia and workshops:
  - DAC
  - DATE
  - ESSCIRC / ESSDERC
  - IEEE SENSORS
  - ISCAS
  - ASP-DAC
  - ITC
  - ICCAD
  - ICCD
  - ASYNC
  - NOCS
  - CHES
  - FPL
  - ISVLSI
  - DTIP
  - IPDPS
  - PATMOS
  - IEEE SPI
  - FFCM
  - FPGA
  - IEEE SoC
  - ETS
  - IOLTS
  - ATS
  - VTS
  - DFT
  - ISQED
  - VLSI Design

- 25% of publications with external academic co-authors

- 25% of publications with industrial co-authors
List of HDR and Ph.D. Thesis Defended in 2010

Habilitation à Diriger les Recherches (HDR)

- Serge Bernard: "Contribution à la qualité et à la fiabilité des circuits et systèmes intégrés et à la microélectronique médicale". HDR. April 2010.

Ph.D. Thesis

Role and Involvement at the International and National Levels

Societies
- Test Technology Technical Council (TTTC) of the IEEE Computer Society
- IFIP Technical Committee

Editorial Board of Journals
- IEEE Transactions on VLSI
- IEEE Design & Test of Computers
- ASP Journal of Low Power Electronics
- The VLSI journal (Elsevier)
- International Journal of Reconfigurable Computing (Hindawi)
- IOP Journal of Neural Engineering

Conference Committees (General Chairs & Program Chairs)
- The 5th International Symposium on Electronic Design, Test and Applications (IEEE DELTA 2010)
- The 3rd International Workshop on Impact of Low-Power design on Test and Reliability (LPonTR’10)
- The 16th International Mixed-Signals, Sensors, and Systems Test Workshop (IEEE IMSTW’10)
- The first European workshop on CMOS Variability (VARI’10)

Executive Committees of Conferences
- IEEE /ACM Design, Automation, and Test in Europe conference (DATE)
- IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)
- IEEE International Symposium on Electronic Design, Test and Applications (DELTA)
- Design &Technology of Integrated Systems in Nano-scale Era (DTIS)
- IEEE European Test Symposium (ETS)
- International Conference on Field Programmable Logic and Applications (FPL)
- IEEE Computer Society Annual Symposium on VLSI (ISVLSI)
- IEEE Workshop on Signal Propagation on Interconnects (SPI)
- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)
- IEEE International Conference on Reconfigurable Computing (ReConfig)

CNRS: Centre National de la Recherche Scientifique
- Délégué Scientifique
- Membre du Conseil Scientifique (INS2I)
- Directeur et membres de comité de pilotage du GDR SoC-SiP, du GDR MNS

ANR: Agence Nationale de la Recherche
- Membres de comités de pilotage (programmes ARPEGE)

AERES: Agence d'évaluation de la Recherche et de l'enseignement supérieur
- Présidents et membres de comités d'évaluation de laboratoire français
International Academic Cooperations

- **Brazil**: UFRGS, PUCRS (Porto Alegre) – Capes/Cofecub
- **Canada**: Univ. of Waterloo, McMaster University (Hamilton)
- **Germany**: Univ. of Darmstadt, Univ. of Stuttgart, Karlsruhe Institute of Technology, Univ. of Freiburg
- **Denmark**: University of Aalborg
- **Italy**: Politecnico di Torino, Univ. of Catania, Campus Biomedico of Roma, SSA Pisa
- **Japan**: Kyushu Institute of Technology, Univ. of Tokyo
- **Spain**: UPC Barcelona, UAB Barcelona
- **Switzerland**: UNIL Lausanne, EPFL Neuchâtel
- **Tunisia**: University of SFAX
- **United Kingdom**: University of Lancaster
- **USA**: UMASS Amherst, Univ. of Connecticut, Stanford University
Ongoing European and National Projects

- **3 projects in the framework of CATRENE and ENIAC European programs:**
  - CATRENE European program: “TOETS, Towards One European Test Solution” (2009-2011)
  - ENIAC European program: “MODERN, Modeling and Design of Reliable, process variation-aware Nanoelectronic devices, circuits and systems” (2009-2011)
  - FP7 European program: “TIME, Transverse Intrafascicular Multichannel Electrode system for induction of sensation and treatment of phantom limb pain in amputees” (2008-2012)

- **10 ANR Projects in the fields of Microsystems, Secured Systems, Multi-processors Architectures, Healthcare, Emerging Technologies, Test & Reliability of Memories:**
  - ADAM
  - CILOMAG
  - EMAISecCi
  - EMYR
  - HAMLET
  - MATEO
  - MIDISPPI
  - R3MEMS
  - SECRESOC
  - SPIN

- **1 International Scientific Collaborative Project (PICS) with Politecnico di Torino, Italy**

- **2 FCE projects in the fields of Design and Test of secured integrated circuits and systems:**
  - CALISSON
  - PROSECURE

- **1 other FCE project**
  - NEUROCOM

- Several funded bi-national research projects with Karlsruhe Institute of Technology (PROCOPE-MOKA) and PUCRS (CAPES/COFECUB)
- Main academic partners: TIMA, LIP6, CEA, LabSTICC, ParisTech, IEF, IMS, LAAS, IETR, CMP, SPINTEC, IM2NP, LaHc, ENSMSE
Industrial Partners

Medical Partners
ISyTest: A Joint Institute between LIRMM and NXP

- LIRMM and NXP: a cooperative effort resulting from a European MEDEA+ program
- Multiple types of adaptive equipment and test chips for research and development of test methods
- Multi-site institute based in Montpellier (LIRMM) and Caen (NXP Semiconductors), France
SECNUM Platform

SECNUM: A Unique Hardware Security Platform

Nowadays, digital systems are the main information support, in spite of the paper. This evolution implies a growing interest for the domain of cryptology regarding the conception of these systems. The hardware/software implementation has become the main weakness of security applications and hardware attacks, or "side channel attacks", like the DPA (Differential Power Analysis) for instance, have become standard. They are now identified as the most dangerous attacks, i.e. they allow ciphering algorithm keys obtention, like those used in our smartcard, with minor cost and effort.

In this context, the missions of this platform, supported by the "Région Languedoc Roussillon" and the "Université Montpellier 2", are to analyze the security potentialities of hardware platforms and embedded systems.

This platform involves disciplinary competencies like Mathematics (I3M laboratory, Montpellier), Informatics and Microelectronics (LIRMM laboratory, Montpellier) and Electronics (IES laboratory, Montpellier). This platform is clearly part of a scientific and technical transverse approach in the "Université Montpellier 2" and "Pôle MIPS" (Mathematics, Informatic, Physics et System) scene.

The objective of this platform supported by the Languedoc Roussillon region is to analyze the potentialities of hardware platform and embedded systems in terms of security.

- Side Channel Analysis
- Software & Hardware Experiments
- Academic & Industrial Applications
- National & International Impact

→ http://www.lirmm.fr/Secnum
Supported Platforms

The microelectronics department of LIRMM is deeply involved in the activity of the CNFM center of Montpellier. CNFM is a national federation of schools and universities concerned by the microelectronics education at various levels.

CNFM Computer Aided Design (CAD) Resource Center:

This national service aims at providing access (licenses and support) to design software and FPGA prototyping kits to academics. Proposed services include:

- Gathering of needs inside the CNFM network
- Evaluation of tools (software and FPGA kits) available on the market
- Trading with vendors
- Training for trainers
- Distribution or hosting of software licenses, distribution of FPGA kits
- Support to users
- Software updates

CNFM Test Resource Center

The Test Resource Center of CNFM hosts leading edge automated test equipment for integrated circuits (VERIGY V93K). This platform is open to academic (training and research) and industrial (training, engineering) needs.

Proposed services include:

- Development and organization of training sessions for students and educators
- Technical support for remote access
- Putting qualified educator at partners disposal for external trainings
- Development of training material
- Support to research
- Test Engineering

Available trainings concern digital and mixed-signal circuits.

→ http://cmos.cnfm.fr
Sample Gallery

**TAS-MRAM Collaborative Circuit,** STM CMOS 130nm + Magnetic Back-End, 4mm², CIOMAG (IEF, SPINTEC, LETI, LIRMM), Y. Guillemenet

**EM Evaluation,** AMS CMOS 0.35µm, 4mm², J. Le-Coz, P. Maurine

**EM Counter-measure Evaluation,** STM CMOS 90nm, 1mm², R. Lounis, B. Vacquie, P. Maurine

**LUTs FPGA TAS-MRAM,** AMS CMOS 0.35µm + Magnetic Back-End, 4mm², CIOMAG, Y. Guillemenet

**MEMS Sensors,** NXP PICS + TMAH Etching, 150mm², F. Mailly, L.Latorre

**EM Evaluation,** ST CMOS 65nm, 0.5mm², CALISSON, R. Lounis, P. Maurine

**Electronic Front-End for MEMS,** AMS CMOS 0.35µm, 4mm², B. Alandry

**MEMS Switches Drivers,** AMS HV CMOS 0.35µm, R3MEMS, 7mm², N. Dumas

**MEMS Switches Drivers,** AMS HV CMOS 0.35µm, R3MEMS, 9mm², N. Dumas
Sample Gallery

**Inertial Measurment Unit.** AMS CMOS 0.35µm + TMAH Etching, 7.3mm², B. Alandry, E.M. Boujamaa, L. Latorre

**Low-Power conditioning Circuit for MEMS.** AMS CMOS 0.35µm + TMAH Etching, 2mm², E.M. Boujamaa, L. Latorre

**Integrated Compass.** AMS CMOS 0.35µm + TMAH Etching, 10.6mm², N. Dumas

**Capture Circuit.** 24 channels 0-20V, 10 bits, AMS HV CMOS 0.35µm, 5.6mm², DEMAR Neurocom, L. Bourguine, G. Cathébras

**Low-noise Amplifier for ENG.** AMS CMOS 0.35µm, 3.1mm², DEMAR, L. Gouyet, G. Cathébras

**8 bits DAC.** AMS CMOS 0.35µm, 2.5mm², DEMAR, J-B. Lerat, G. Cathébras

**Neural Stimulation Circuit.** 12 channels 0 to 5 mA, AMS CMOS 0.35µm, 9.2mm², DEMAR SENIS, J-B. Lerat, G. Cathébras

**MRAM-FPGA.** ST CMOS 130nm, 22mm², SPIN, Y. Guillemenet

**Front-End for Magnetic Sensors.** 32 channels 14 bits ADC, AMS CMOS 0.35µm, 35mm², SPIN, N. Dumas.
Laboratoire d’Informatique, de Robotique et de Microélectronique de Montpellier
161 rue Ada - 34095 Montpellier - Cedex 05 - FRANCE
Tel: 33 (0)4 67 41 85 85 - Fax: 33 (0)4 67 41 85 00
www.lirmm.fr

Head of the Microelectronics Department: Patrick Girard
Patrick.Girard@lirmm.fr - Tel: 33 (0)4 67 41 86 29

Deputy Head of Department: Serge Bernard
bernard@lirmm.fr - Tel: 33 (0)4 67 41 86 66

Deputy Head of Department: Laurent Latorre
latorre@lirmm.fr - Tel: 33 (0)4 67 41 86 65