Architectures and Methods for Resilient Systems (AMfoRS)

Permanent Personnel
Lorena ANGHEL[1] (PR1 Grenoble INP, Section 61) Mounir BENABDENBI (MCFCN Grenoble INP, Section 61) Giorgio DI NATALE (DR2 CNRS, Section 7) Régis LEVEUGLE (PREX Grenoble INP, Section 27) Paolo MAISTRI[2] (CR1 CNRS, Section 7) Michele PORTOLAN[3] (MCFCN Grenoble INP, Section 27) Ioana VATAJELU (CRCN CNRS, Section 8)

[1] Team co-leader
[2] Team co-leader
[3] Mobility for academic collaboration to Politécnico de Torino until end 08/2019

Temporary personnel		
PhD Students	8	Noureddine AIT SAID Xavier AUBERT Valérian CINÇON Geoffrey DELAHAYE Pietro INGLESE Vincent REYNAUD Kalpana SENTHAMARAI KANNAN Riddhi SHAH
ATER, PAST, Emeritus	1	Dominique BORRIONE
Trainees	7	Ali BAWAB Ali Sohaib CHAFIK Mona EZZADEEN Alessandro FICI Victor MESNAGER Muhammad Talha QURESHI Lucas SANTANDER

Research Activities

The AMfoRS team addresses trust and dependability of digital systems at multiple abstraction levels. This can be achieved by guaranteeing that digital circuits possess a number of different properties, possibly depending on the specific application domain, such as reliability, safety, security, availability, specification compliance. The work is focused on design and analysis methods, techniques and tools applying to above-mentioned domains.

System-level test and standards

The IEEE 1687-2014 standard proposes solutions for the access and usage of Embedded Instruments. Even though the standard has already been published and industrial acceptance is high, Electronic Design Automation (EDA) is still limited to only a small subset of the new features, and the real novelties are not considered. In this context, in the frame of the Eureka European project HADES, we carry on developing an innovative Test Flow and Environment called "Manager for SoC Test" (MAST), a software backend able to provide features and performance superior to the industrial legacy solutions [RI-8]. We are using MAST as the basis for new experimentations and abstractions, and we have a strict interaction with the IEEE P1687.1 Working Group, which is evaluating our proposals for inclusion in the upcoming release of the standard.

Aging Induced Reliability evaluation and Robustness improvement

Process, voltage, temperature and other environmental variations in current CMOS nanometric digital designs cause performance degradations and may lead to functional failures, which can be serious issues in critical and mixed-critical systems (such as automotive, health-care, avionic and space applications). Usually timing errors can manifest on critical propagation paths and are detectable by timing-violation monitors. The usage of monitors for error and pre-error detection allow decreasing margins imposed on the overall design. They can be implemented together with Adaptive Voltage Scaling (AVS) or Dynamic Voltage Frequency Scaling (DVFS) techniques which are triggered by the pre-errors of in-situ timing monitors while adapting dynamically the frequency and the voltage according to the operating conditions and the application needs. In the framework of the European Eureka project HADES, we have continued the design of different pre-error monitor techniques. They are based on Replica Path principle, but the design has been optimized to allow sensing local and global variability and aging degradations. We also explore a new research direction consisting in finding a near-optimal monitor placement strategy based on predictive aging modeling. Therefore, we prioritize data-driven automated learning approaches to model the specific near-unpredictable behavior of transistor aging using ML-friendly models. This allowed us to couple a lightweight Machine Learning prediction framework with traditional, computationally intensive circuit simulations as validation. This Proof-of-Concept was presented in the past and given as a keynote talk in [INV-7], where we demonstrated its capability to accurately model path aging. The activity is progressing on two fronts: on the one hand port the model to the FDSOI 28nm technology, more prone to aging, and on the other hand, to apply the ML framework to the identification of an optimal set of monitor insertion points. Since 2018, we have worked on the design of a novel in-situ delay monitor adapted to detect delay faults, including hidden delay faults (i.e., a delay fault, which is smaller than the slack of the propagation path). Compared to existing solutions, the proposed monitor has a polymorphic behavior and can be used (i) during testing to perform user-defined hidden-delay-fault test, (ii) for reliability degradation estimation due to process, environmental variations and aging, and (iii) in security to detect the insertion of Trojan horses that alter the path delay [CI-9].

Safety and security evaluation

In the recent years, many domains have added functional safety to the classical list of design constraints, e.g. ISO 26262 standard in automotive towards autonomous vehicles. Similar standard evolutions occurred in other areas. Our work aimed at improving early evaluations of dependability w.r.t. errors induced by environmental disturbances. The goal, in order to reduce development and production costs, is to be able to evaluate accurately and at an early stage of the design the potential functional effects of (soft) errors. Classical fault-injection approaches at RT-level (where registers can be identified), known for a long time in the team, are not efficient enough even with emulation-based support. A software developed in the team called "EARS" has been leveraged to allow an accurate analysis of data lifetime in registers, in the context of approximate computing [CI-5] and also led, associated to other works, to an embedded tutorial at ETS19 [CI-4]. Following these works, we are working towards a more accurate evaluation of error consequences with respect to the global system, since all circuit output errors are not critical from a system point of view. This is done in the context of the Aura Region project Safe-Air, with contributions from both classical dependability analysis and formal verification techniques.

When considering the different hardware components, the memory components are more susceptible to soft errors, thus they have significant impact on the overall system reliability. We have presented an analytical methodology to measure the vulnerability of the memory components of a microprocessor-based computing system [RI-2]. It is based on the data and the instruction lifetime and residence [RI-5]. The proposed approach considers only the software-layer of the system, which makes it usable at early design stage when the hardware architecture is not fully defined. Then, to consider the hardware memory hierarchy (i.e., RAM, Caches, Register Files) at software level, we have developed a memory subsystem emulator that can be easily configured to support different features. The methodology can be used to perform a fast, easy and not costly cache-aware Design Space Exploration (DSE) to accurately evaluate the vulnerability of the RAM and the caches. We have validated the approach on small benchmarks (Mibench) and proven the efficiency of the proposed approach on a real industrial test case (i.e., a Flight Management System for avionic application). The results show that the proposed methodology gives precise results compared to a classical fault injection tool, and it scales well with the complexity of the application.

Robustness of emerging computing technologies

Today’s computing systems are facing a plethora of issues related to architectural and technological limitations. From a technology perspective, the main issues are related to CMOS technology scaling, i.e., diminished returns in performance and increased leakage power. To mitigate these issues, novel emerging technologies are being researched, such as memristive and spintronic devices, in conjunction with novel computing paradigms, such as computing in memory - CIM, or neuromorphic computing. Our current research and collaborations in relation with this topic are threefold: (i) to use enhanced compact models of emerging devices to perform failure analysis and define pertinent fault models [INV-2], (ii) to investigate meaningful reliability threats affecting the computing modules and architectures (CIM and neuromorphic), and derive solutions for their mitigation (Design-for-Reliability) [INV-6] ; and (iii) to establish design and test methodologies for these devices and architectures. This work has been presented as an ‘invited talk’ at the national Workshop GDR BioComp 2019. We have developed an in-house tool for training, inferring and evaluating the performance under faults of a spiking neural network (HW ready). To the best of our knowledge, this is the first tool containing a platform for fault injection in SNNs.

Security primitives and hardware trust

The implementation of security primitives has been enriched with the use of high-level synthesis tools and methodologies. In the IoT context, innovative ways have to be explored to achieve low cost and security: we have proposed some approaches to improve the global security at low cost. In particular, we proposed an improved approach to provide secure authenticated access to test structures [CI-1]. On a second front, our research activities covered the design and evaluation of True Random Number Generators (TRNG) and Physically Unclonable Functions (PUF). True Random Number Generators (TRNGs) are used to generate random numbers from a physical process. We have proposed a solution exploiting the intrinsic stochastic properties characterizing the write operation in magnetic devices [RI-4]. Indeed, the write operation has a stochastic behavior, which can be manipulated to set the write probability to 50%, thus generating random numbers. The design is straightforward and the quality of the random numbers is guaranteed from the first generated bit. Physically Unclonable Functions (PUFs), on the other hand, exploit intrinsic manufacturing variability introduced in a device during the fabrication process to generate a signature, unique to each single device and robust w.r.t. aging and environmental variations. In this context, our research is focused on the hardware implementation of reliable and attack-resistant PUFs. We have proposed solutions to identify and mask unreliable PUF responses; we then exploited this information to design a PUF scheme able to generate Zero Bit-Error-Rate response. In addition, we are presenting a novel approach for building Strong PUFs that are inherently resistant to modeling attacks in IOLTS'19 and a solution to analyze and improve the reliability of PUFs [CI-11]. These results have been also presented in a keynote talk in PESW'19 |INV-5].

New hardware computing approaches

In the last few years, a promising solution known as "Approximate Computing" (AC), has been gaining more and more interest in the scientific community both in the industry and in academia. AC is based on the intuitive observation that, while performing exact computation requires a high amount of resources, allowing selective approximation or occasional violation of the specification can provide significant gains in power consumption. Or, for the same amount of consumption, performances can be enhanced. Various applications of AC were surveyed by the scientific community such as data analytics, scientific computing, multimedia, signal processing, machine learning and so forth. We are collaborating with the LIRMM Laboratory on this topic. At circuit level, we developed, in collaboration with the CDSI team, adders, multipliers and MACs using redundant arithmetic [CI-10]. At system level, we are developing a precision evaluation platform based on Berkeley's Rocket Chip HW/SW environment (RISC V based).

Nano-crossbar arrays have emerged as area- and power-efficient structures with an aim of achieving high performance computing beyond the limits of current CMOS. Due to the stochastic nature of nano-fabrication, nano arrays show different properties both in structural and physical device levels compared to conventional technologies. A competent logic synthesis methodology must consider basic technology characteristics for switching elements, defect or fault rates of the given nano switching element and the variation values, as well as their effects on performance metrics including power, delay, and area. Our current interests are leading towards development of a complete synthesis and optimization methodology for switching nano-crossbar arrays to enable design and construction of emerging nanocomputer. This work has been done in collaboration with U of Milano. Moreover, we have investigated the possible defects and faults that can occur in these types of structures and related technologies and proposed defect tolerance techniques which can be employed during logic synthesis. The impact of the crossbar sensitivity on the algorithm is leading to a lot of challenges [INV-7]. Our current and future research and collaborations are related to logic synthesis-dependent defect/fault tolerance techniques, and variation-area-power-delay performance optimization of logic and arithmetic operations mapped on crossbars.

Highlights

- Interaction with the IEEE P1687.1 Working Group
- Keynote talk in LATS 2019 in test and security embedded monitors
- Open-source fault injection tool for SNNs
- Participation to the Grenoble Alpes CyberSecurity Institute for post-quantum cryptography
- Keynote talk at PESW 2019

Indicators

Scientific production	2019
International journals	9
International conferences	18
Book chapters	1
National journals	1
National conferences	2
Other communications	4

Scientific recognition	2019
Prizes and distinctions	1
Invited conferences	8
Conference/workshop Committees	27
Journal Edition Committees	3

Contracts 2019		
ANR	1	Eminent (2019-2023)
ANRT	3	STMicroelectronics (2) / Dolphin (1)
CEC	1	NanoxComp (2016-2019)
EPST	4	IDEX Grenoble IRS (2), MIAI Institute (1), IRT Nanoelec (1)
EUREKA	1	Hades (2017-2020)
Région	1	Safe-air (2017-2022)