6. Architectures for Robust and complex Integrated Systems (ARIS)

Group Leaders : M. Nicolaidis and R. Velazco
(e-mails: Michael.Nicolaidis@imag.fr, Raoul.Velazco@imag.fr)

Members : L. Anghel, S. Benhammadi, G. Bizot, A. Bocquillon, G. Canivet, B. Courtois, T. Dang, S. Fernandez, P. Ferreyra, J.B. Ferron, G. Foucard, R. Leveugle, V. Maingot, P. Maistri, J. Moreno, M. Nicolaidis, P. Peronnard, C. Rusu, C. Sahnine, S. Torrellas, P. Vanhauwaert, H. Yu, N. Zergainoh

Research areas	Contracts	Industrial Partners
- Methodology, tools and experimentation for the study of the IC's sensitivity to radiation; - Methods and tools for fault injection ; - HW and SW techniques for hardening digital/analog architectures for SOCs and NOCs; - SEU hardened cells; - SEL mitigation architecture; - Fault Tolerant Architectures for mitigating the flaws of Nanometric CMOS - Defect Tolerant Architectures targeting very high defect densities. - Secure digital implementations ; - Robust logic implementations based on single electron transistors ; - Carbon Nanotubes Transistors characterisation, study of dispersions - Computing Architectures for Nanotechnologies - Design and exploitation of experiments on-board satellites and high altitude balloons.	ATMEL, CNES, EADS, E2V, STMicroelectronics, ACI-SI Mars, IACI Nanosys MEDEA PARACHUTE ALFA , CLUSTER Aeronautique. FT-ORANGE, THALES, ARAVIS minalogic, ASTER minalogic	ARTISAN (USA), CEA/LETI, iROC (France), GEMPLUS (France), THALES COMMUNICATION (France), NASA GFSC (Washington, USA) AIRBUS (France), EADS-CCR (France), ATMEL, EADS-ST (France)

6.1 Summary

The ARIS group was created in 2007 as a continuation and extension of past activities performed in the RIS group (Reliable Integrated Systems) and then in the QLF group (QuaLiFication of circuits) of TIMA. Research activities of the group deal with the study of the IC behavior in harsh environment. Indeed different types of interferences and parasitic effects affect the reliability of modern electronic systems. Nanometer circuits, micro-electronics, micro-system technology and power electronic systems are already part of our daily life. However, these systems encounter many problems with natural and artificial interferences coming from various sources (e.g. particle radiation effects, electromagnetic interferences, etc). Another related area is the new threat on secure systems, related to fault-based attacks.

One of the main stress considered is radiation of nuclear and space environments, but it is interesting to mention that particles reaching the Earth's surface from the Sun, up to now innocuous for microelectronics circuits, have sufficient energy to flip bits in memories and corrupt logic inside processors for parts manufactured with less than 0.25 µm and supply voltages drop to less than 2.2 Volts. This can constitute a threat to avionics control systems (at 30,000 feet, the neutron activity is 4 to 8 times higher than the ground), and even to systems operating at sea level.

One of the important issues of these researches is the prediction of error rates of a studied system (circuit, architecture, software ...). The refinement of forecasting error rate strategies needs both to perform ground test by means of simulated radiation environment (particle accelerators) and to compare ground test results to data obtained from experiments aboard of spacecrafts. A satellite experiments developed in collaboration with CNES (French Space Agency) and NASA GFSC (Goddard Flight Space Center) aims at studying the sensitivity of

advanced FPGAs (Field Programmable Gate Arrays) to transient errors provoked by radiation, so-called Single Event Upsets (SEU). The satellite carrying this experiment, presently at the end of development phase, will be launched in 2011 in the frame of NASA LWS/SET project (Living With a Star/Space Environment Testbed). In the figure below is depicted the experiment developed at ARIS embedded in the LWS satellite carrier. The experiment includes an architecture implemented by means of a Virtex II SRAM-based FPGA in which was implemented a fault tolerant (Triple Modular Redundancy) architecture of a cryptographic application.

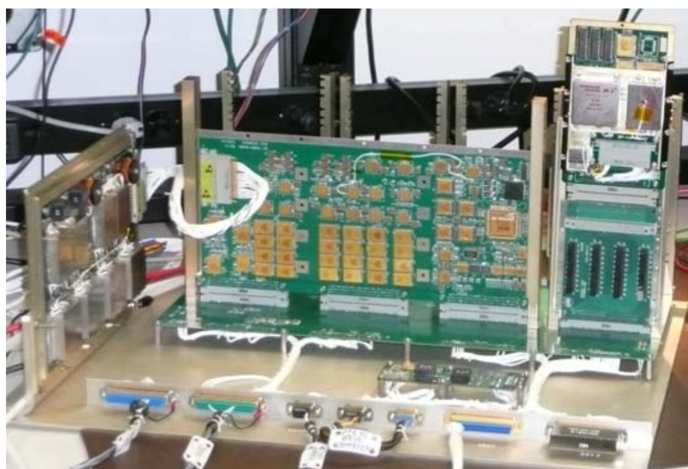

Figure 1. **Space Environment Testbed (SET) of Living With a Star (LWS) Satellite from NASA**

Another research field concern the development of innovative methods and tools dedicated to the predictive analysis, validation and qualification of integrated electronic systems using fault injections. The sensitivity predictive analysis platform covers the development of multilevel fault injection methods and tools to be applied at different system abstraction levels from RTL level to gate level descriptions.

The activities of the ARIS group concern both natural and intentional faults in integrated systems. Activities are also on-going on the design of secure circuits protected against fault-based attacks. These activities include the analysis of the circuit robustness against a whole panel of attacks (DFA, DPA, EMA) and the evaluation of protection techniques. Common approaches are developed to analyze the dependability level and protect circuits against both types of faults (natural and intentional), taking into account their different characteristics.

More recent research areas of the group include fault tolerant architectures for mitigating the flaws of nanometric CMOS (variability, accelerated circuit aging and parasitic effects); fault tolerant architectures for high defect densities targeting post CMOS nanotechnologies; and Computing architectures for nanotechnologies.

6.2 Study by real life experiments of the effects of radiation on the operation of submicronic integrated circuits

Members: P. Peronnard, R. Velazco, G. Foucard, S. Fernandez, P. Ferreyra

Ionization resulting from charged particles and atoms present in the substrate of CMOS circuits, may modify memory cell's content or provoke a transient pulse within a combinational circuit. This phenomenon which until recently was only considered to be a treat for space applications is nowadays a major concern for avionic equipments and even for any application operating at ground level. Thus it constitutes a potential obstacle to the reliable operation of circuits manufactured from future deep submicronic processes.

A first step towards a thorough study of this problematic consists in putting in evidence the phenomenon through experimentation with suitable test vehicles and an appropriate neutron beam. In February 2000 was carried out one of the first experiments performed in France in this area. A generic and versatile test platform, the THESIC (Test for Harsh Environment Studies of Integrated Circuits) was developed at ARIS and is used to perform radiation ground test experiments to evaluate the sensitivity of integrated circuits to different kind of particles (heavy ions, neutrons, protons,…). These experiments put in evidence the need for the use of hardening techniques (design hardened memory cells, error detecting and correcting codes,…) in future deep

submicronic circuits. Indeed, the number of detected bit flips suggest that next generation of SoCs (Systems on a Chip) or high-capacity static memories may be the source of frequent errors even for systems operating at sea level.

Current researches in this area are dealing with the design and exploitation of an experiment including a very large capacity SRAM memory, which will be exposed to the effects of natural atmospheric radiation at different sites, this to derive realistic error rates in real life environment of future submicronic components. Candidate SRAMs for this real life testing were evaluated using a fault simulation technique and dedicated tools (Giant 4). Obtaining real life versus accelerated test figures will help in giving trends for future technologies. This project started the experimental phase in 2007, phase that took benefit of the partnership offered by an European project, the ALFA (*America Latina Formation Académica*) NICRON project. The activities performed during ALFA NICRON allowed gathering preliminary results about the impact of atmospheric neutrons in advanced integrated circuits, this at different altitudes and latitudes, particularly using facilities at high altitude (available in Peru) or stratospheric balloons which will evolved in the so-called SAA (South America Anomaly) zone well known as being significantly more error prone than other regions of our planet. Three stratospheric balloons were successfully launched from an Air Force base in Uruguay (see photo depicted in Fig. 1). The short duration of the flights (around three hours) does not allow detecting SEUs, but these launchs allowed to validate the electronic equipment in the payload and the logistic of such experiments. Longterm experiments (flights expected to have a duration of many weeks) using more powefrull aerostatic balloons are planned to be performed in 2009. The same SRAM board was activated in different commercial flights, allowing to put in evidence the occurrence of MCU (Multiple Cell Upsets) which are of high concern for applications requiring high reliability. Indeed, one of the faults detected proved that as the impact of a single neutron 5 the content of five memory cells (the one impacted by the particle and its four neighbours) were corrupted. Such a multiple error may constitute a harsh challenge for the detection by using state-off-the-art techniques. An experiment was also installed at high altitude (at 3800 mts in an university of Cusco, Perou) and allowed to detect some SEUs. Such experiments must have a duration of many months to get statistics that can be used to extrapolate the obtained results to error rates at

Figure 2. Ballon launch from the Air Force base in Uruguay. The payload included a 1 Gbit SRAM

An experiment to be embedded in the SARE (*Satélite de imágenes de Alta Resolución*) from the Argentinien Space Agency (CONAE) is presently under development at ARIS research group.

6.3 Development of a test bed suitable for the qualification of integrated circuits devoted to operate in harsh environment

Members: R. Velazco, G. Foucard, P. Peronnard

With the miniaturization, integrated circuits become more and more sensitive to perturbations resulting from the effects of the environment (temperature, radiation, EMC...). This activity concerns the design of a test system which facilitates the realization and exploitation of qualification tests for all kind of circuits, from a simple register bench to complex components such as processors.

Screening tests are mandatory to predict error rates. They consist in exposing the studied parts, eventually operating in vacuum, to simulated stress conditions. The hardware and software developments related with such tests must take into account the random nature of event occurrence, both in time and space. On one hand this entails on-line error detection, on the other hand this makes mandatory the need for development of ad hoc hardware mechanisms related with critical errors detection (sequencing loss, system crashes, latchups) and recovering. Most of commercially available functional testers have these capabilities, potentially offering a powerful solution to qualification test implementation for all circuit types. Nevertheless, two main drawbacks must be mentioned:

- Functional testers cannot fit inside most of vacuum chambers available at generally used radiation facilities. The alternative consisting in using them outside the chamber connected to the device under test (DUT) inside the enclosure, may lead to serious signal propagation problems,
- Test stimuli are defined by a set of binary patterns corresponding to circuit pins values at each clock period. For complex circuits (processors for instance) the development and debugging at this low-level of such test programs can be a difficult task. Note that these constraints may also apply for testing under other type of conditions such as temperature, magnetic perturbation, vibrations, or other type of harsh environments.

Since 1988 we have been collaborating with different European and American space agencies in projects aiming at the study of the behavior under radiation of circuits devoted to space applications. Our role was the development of the hardware and software aspects of the test under radiation of candidate circuits. Experiments were performed by means of a family of dedicated testers we designed and realized to cope with radiation testing requirements. The use of these testers for a wide range of circuits, including memories, general-purpose processors and dedicated processors, pointed out their capabilities for the qualification of complex digital ICs, but their adaptation to test a new device needs some hardware development, limited to the architecture of the Device Under Test (DUT) daughter-board. Even if such architectures are not too complex and follow quite close the basic principles of block diagrams exposed in the DUT's datasheet, the experience proved us that their development needed specialized skills constituting thus the main obstacle to easily "export" our tester concept to other teams.
In the past we have prototyped different versions of a dedicated test system having the following characteristics:

- The DUT operates in its "natural" digital environment, i.e. it is interfaced to a typical architecture. When the DUT is a processor, such architecture includes memories to store the boot and test programs, glue logic and needed power and clock circuitry. Instead of test vectors that mimic the activity of input pins at each clock cycle, during the test stimuli is applied to the processor under study as the result of the execution of a program stored in a suitable memory. Test results are stored in the memory as a byte sequence.
- An external board provides the interface with the user and controls the operation of the architecture built around the DUT.
- The whole system (DUT board and control board) communicates through a serial link with a computer for user's control of the experiment.

The last version of such a platform, called ASTERICS (Advanced System for the TEst under Radiation of Integrated Circuits and Systems), was designed to deal with the following requirements:

- The whole system must have a size allowing to entirely fitting it in enclosures commonly used for environmental qualification tests.
- The DUT must be tested on-line, operating in nominal conditions.
- The system should allow to exercise as many circuits (among candidates to a given project for instance) as possible, to avoid waste of time/money consequence of delays provoked by operating the facilities used to simulate the studied environment.
- Capability for the tester to be remotely controlled anywhere in the world through the internet network.

The ASTERICS system developed at TIMA/ARIS allows coping with these requirements. A block diagram is given in **Figure 3**.

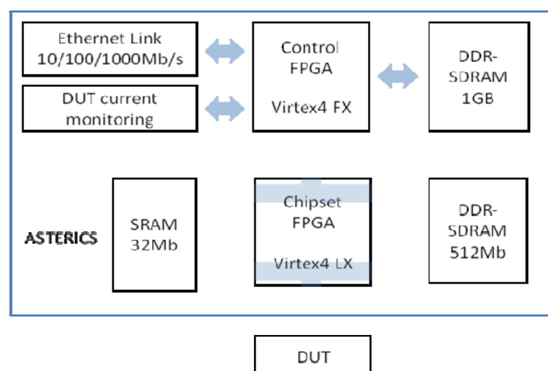

Figure 3. ASTERICS block diagram

The efficiency of this tester's architecture was proved by various cooperations with space agencies aiming at performing the test under radiation of processors candidate to their applications. As a significant example, it can be mentioned the use of the previous version, the so-called THESIC+, by JPL/NASA for the study of the behavior under heavy ions of the PPC750, a complex processor candidate to be included in the electronic equipments of a satellite. This architecture has also been used to test the ATMEL AT697 radiation hardened microprocessor.

The new ASTERICS test platform constitutes a powerful tool with generic capabilities for the qualification of digital circuits. The idea is to implement the whole DUT board architecture by means of an FPGA whose configuration is obtained from compiling the description of key features of the DUT in a hardware description language such as VHDL or Verilog. In this way, there is only a minor hardware development, limited to wiring the DUT pins to the ones of the tester connector. The architecture of ASTERICS is mainly composed of:

- A Xilinx Virtex4FX FPGA, containing a PowerPC hardware processor, having in charge the following tasks: it *control*s the circuit to qualify, runs on and off the test sequences and monitors the latchup circuit. It is also able to transfer test programs and to gather test results from the component being studied to/from the PC user interface via an Ethernet 10/100/1000 link. A second FPGA used as a *chipset* and several static and dynamic memory banks are also included in the board: a 32Mb SRAM memory organized in 2 banks of 512k*32bits (which should allow the test of advanced 64-bits processors) and 512Mb of DDR-SDRAM (16Mx32bits) to enable fast and efficient processor tests. To cope with a wide range of DUTs, all these memory banks are managed by the FPGA of ASTERICS's motherboard. We have chosen for this device a Virtex4LX FPGA from Xilinx which is optimized for high-performance logic. It is multi-volt Input/Outputs compliant, that means it can drive signals in 3.3, 2.5, 1.8, 1.5 and 1.2 Volts, reducing the number of components needed to interface the DUT. The FPGA must be properly configured in order to assign the interface board resources to the device under test. The Control FPGA is also capable to configure the Chipset FPGA through its JTAG port avoiding the use of a dedicated Xilinx programmer.

- The DUT board (called ''daughter-board'' in the previous tester) comprises exclusively the component to test and, in some cases voltage regulators.

Obviously, a computer is also needed in ATERICS as a user's interface. It allows the on-line control of test operations, the display of results and their storage in a mass memory in convenient formats for future analysis. It is important to notice that this computer can be located anywhere in the world, ensuring the remote control through internet. A particular effort was invested on the development of a friendly and powerful user interface capable to provide the operator with on-line test result data.

The TIMA's ASTERICS platform will be used to test under heavy ions and neutrons, in cooperation between iRoc, CNES and E2V, a complex processor (PowerPC). This study is done in the frame of the SCADRI project performed in the frame of Rhône Alpes CLUSTER AERONAUTIQUE).

6.4 Predicting SEU error rates from Radiation Ground Testing and Fault Injection

Members: R. Velazco, P. Peronnard, G. Foucard

When estimating the sensitivity to radiation of an integrated circuit the goal is to evaluate the average number of impinging particles required to provoke a fault. Main considered faults for advanced ICs are SE (Single Event Upset), MBU (Multiple Bit Upset), MCU (Multiple Cell Upset and SEFI (Single Event Functional Interrupt).This can be achieved by means of fault injection techniques, but in all the cases is required a measure of the intrinsic sensitivity of the target circuit to the considered Single Event.
σ is called the interaction cross-section and is a direct measure of the IC sensitivity. Its unit is the cm² or it is expressed in barn (1 barn = 10^{-24} cm²). Generally σ is given as an interaction cross-section per device (or per bit).

$$\sigma_{dev} = \frac{\text{\# of single event recorded during the experiment}}{\text{fluence of the experiment}}$$

$$\sigma_{bit} = \frac{\text{\# of single event recorded during the experiment}}{\text{fluence of the experiment} \times \text{\# of bits}}$$

As a consequence, the end-product of a radiation ground testing will be a plot of the interaction cross-section versus particle energy (measured in terms of Linear Energy Transfer or LET which is the energy transferred to the Silicon during by the particle.

Processors are included in most of the architectures devoted to embedded systems. The determination of SEU cross-section of microprocessor's memory elements requires the use of a so-called *static test* which consists in exposing the device to a suitable particle flux while the content of the DUT's registers and memory elements are observed. This is usually attained by executing a test program in charge of initializing these memories and dumping their content after a given period of time. The usually obtained measure, called *cross-section* (the number observed bit flips divided by the number of incident particles) is used to predict the final error-rate of the tested device in a given harsh environment. However it has been shown that the measured static cross-section can significantly overestimate the one the circuit while it executes a real application. The reason is simple: while a test program is written to maximize the number of errors observed, a real application is not. Moreover, many memory bits are not used, or are refreshed so often that SEUs in these regions have no impact on the system's behavior.

Fault injection may helps in predicting the behavior of a real program which would be used for the final application. It was demonstrated by many experiments that the final cross section of an application executed by a processor can be obtained by multiplying the static cross-section with the error rate obtained during fault injection. The key point is how to perform a fault injection campaign where instants and location of injected faults match the ones of faults occurring when the application will operate in the final environment.

Fault Injection strategies can be classified in two families: software based and hardware based. Among software based ones, depending on the available DUT description level, can mentioned:
- SPICE based fault injection, if a SPICE net-list is available;
- VHDL / Verilog fault injection when a behavioral or RTL description does exist;
- ISS based fault injection if an Instruction Set Simulator is available.

Hardware based fault injection requires a physical device, and faults can be injected using:
- FPGA based fault injection, if a RTL description is available and mapped to an FPGA;
- The CEU (Code Emulated Upset) method, based in the random activation of interrupt signals.

An extended version of the CEU fault injection methodology, published by ARIS for the first time in 2000, able to target cache memories as well as register files was explored in the frame of SCADRI project (project from Rhone-Alpes Aeronautic Cluster) targeting two consecutive generation of advanced processors: the Power PC

7447 and 7448. Basically, it consists in triggering an interrupt while the processor is running. When the DUT receives the interrupt, it transfers the control from the executed benchmark to a trap handler. This handler then flips the content of a randomly chosen bit and resumes the benchmark execution. Obtained results proved that the predicted error rate fit very well the measured ones. Radiation ground testing results were gathered during experiments performed at Louvain-La-Neuve heavy ions facility. We used the resulting cross-sections and flux settings as inputs to our fault injection set-up. Outputs of the fault injection experiments were analyzed with *exactly the same tools* used to analyze the radiation ground test results. At the 95% confidence level, there was no disagreement. The test set-up cannot see differences between SEU induced by radiations and SEU-like faults injected.

As a conclusion, given a cross-section measured beforehand and a particle flux, this technique allows to correctly reproducing the upsets arrival times of a real radiation ground based test. Moreover, it provides the user with an estimation of its own accuracy at the 95% confidence level. Once the underlying cross-section of the microprocessor memory elements has been obtained by radiation ground testing, this method can be used to study with a good accuracy the behavior of any other application without running it under radiation.

6.5 Design time behavioural level analysis of soft error consequences in complex digital circuits

Members: R. Leveugle, P. Maistri, P. Vanhauwaert, J. B. Ferron, L. Anghel, R. Clavel (VDS), L. Pierre (VDS)

Significant effort was targeted during the last years on developing efficient techniques to analyze at design time the functional consequences of soft errors. The goal is to precisely identify the soft errors leading to unacceptable application disturbances, in spite of all the possible masking effects due to the circuit architecture (redundancy, performance-oriented features, etc.) or to the application characteristics (meaningless computations in a parallel structure, meaningless precision of some data, etc.). Targeted circuits have essentially been synchronous digital circuits. The analysis is carried out as soon as a functional model of the circuit or system is available, so that necessary corrections can be made early in the design flow. Most of the techniques, developed since more than ten years in the team, start from synthesizable RTL descriptions. Such descriptions are already close to the final hardware in terms of cycle accuracy and in terms of memory cells identification. Higher level descriptions may in some cases be used, with limited representation of soft error locations and reduced accuracy in terms of propagation analysis.

All early robustness evaluations do not seek the same kind of answer. This point is important, because some techniques may be very efficient with respect to some outcomes, but completely inadequate with respect to others. The main types of outcomes that can be expected are:

- classification of faults/errors – Injected faults or errors are classified with respect to a list of potential effects defined by the designer. These effects may include application failure modes, error tolerance or detection (when mechanisms exist), or just nothing (silent errors, without any consequence on the application). Such a classification can be used to evaluate the intrinsic robustness level of a circuit and/or to validate the protection mechanisms implemented in the circuit.

- quantification of derating factors – Evaluating timing and architectural derating factors corresponds to identifying the fraction of the errors having no impact on the system behaviour.

- identification of error propagation paths – Classifying the errors does not give any insight into how they propagate within the circuit from their origin to the recorded effect. In order to identify the best positions in the circuit where protection must be added it is necessary to make a more detailed analysis of the error propagation from the original soft error up to the activated failure mode.

- identification of critical locations – When selective (or "pragmatic") hardening is the goal, the identification of error propagation paths allows the designer to pinpoint efficient locations where propagations can be stopped. Another possibility is to avoid using sensitive cells to implement registers that may be the origin of the most critical consequences (e.g. using specific hardened flip-flops on those locations). In that case, it is necessary to order the list of flip-flops with respect to the probability that an error in them will result in a critical event for the application. This will be called flip-flop or register grading.

- proof of a given set of properties – In that case, an expected system property and/or the efficiency of detection or tolerance mechanisms must be guaranteed for all errors in the expected error set.

A lot of work was done in our team on fault injection techniques, based on simulation, then emulation. These techniques can be used for all expected outcomes. However, the main limitation is the huge amount of time required to run the experiments when many faults have to be injected in a complex circuit running a long workload. Using hardware emulation leads to noticeable time savings, and we have developed during the last years efficient injection platforms based on SoPCs (System on Programmable Chip). This platform takes advantage of the processor core integrated in the SoPC to reduce the quantity of data exchanges with the host computer, thus accelerating the experiments, while maintaining the largest flexibility with respect to the type of possible dependability analyses. Unfortunately, even with such an acceleration, exhaustive fault injections often remain unaffordable in a reasonable time.

This leads in most cases to perform only partial analyses based on a randomly (and often arbitrarily) selected set of faults or errors. Such a statistical fault injection (SFI) has been very extensively used in the literature but the margin of error on the results given on such a basis was unknown. We have therefore proposed and validated in 2008 an approach to quantify the error on the results with a given confidence level, or conversely to evaluate the number of injections to perform in order to achieve a given error/confidence level. The method will in particular be presented at the DATE Conference in 2009.

SFI can then be very useful in doing quick classification or derating factor estimations, with a controlled margin of error. Unfortunately, this approach does not address all possible expected outcomes of a fault injection campaign. In the case of a large number of potential errors and workload cycles, only a very small proportion of the registers are actually perturbed at a few cycles. This means that such results cannot help in identifying the most critical registers or clock cycles. Flip-flop grading remains possible when the random selection is only used to reduce the number of injection cycles in each flip-flop; however, in that case, the efficiency of SFI is noticeably reduced and the required number of experiments remains very large. Error propagation paths are also only partially exercised, so decisions on the best hardening positions are hard to make. Finally, SFI cannot guarantee that a given property always holds; this can at best be assessed with a given margin of error.

Several complementary approaches are therefore currently under study in order to more efficiently obtain some expected outcomes.

An approach based on Timed Petri Net models has been proposed and evaluated. It has been shown that this type of model can efficiently identify some harmless errors even in the case of architectures difficult to analyze with classical fault pruning techniques. Such models can therefore be used to reduce the number of injection experiments. They can also help in grading the criticality of the flip-flops in a circuit. At medium term, we plan to develop an environment allowing a designer to automatically generate such models from available circuit descriptions (synthesizable RTL or netlists). The extension of the approach towards error propagation analysis is also under consideration. This will be complementary to probabilistic propagation analyses, another approach under study in the team. One of the important aspects will be to make a compositional approach possible, so that results obtained at block level can be directly re-used to evaluate the dependability of a complex circuit.

Another study targets the proof of properties even in presence of faults. This follows 2005 experiments based on formal property checking. The current study is done in collaboration with the VDS group in TIMA and the LIP6 laboratory, in the frame of the FME3 project, supported in the period 2008-2010 by the French national research agency (ANR). Model checking techniques and theorem provers are currently experimented. In particular, an approach has been developed to efficiently model the effect of single or multiple bit errors and prove properties in presence of such errors with the ACL2 theorem prover.

The specific case of configuration errors in SRAM-based FPGAs is also addressed. A tool allowing a designer to analyze the effect of faults in the configuration of a Virtex II FPGA had been developed and has been extended within the MEDEA+ Parachute project to analyze Atmel FPGAs. The tool can be used to analyze the effect of attacks on such a reconfigurable platform. This has been done in particular for several attack campaigns using power glitches and several types of lasers. Such analyses lead to better understand the type of perturbations induced by attacks and to determine more realistic error models. It has also been shown on Virtex II that the probability to flip a configuration bit noticeably depends on the fault-free value of this bit (publication at VTS in 2009). For a given design, and therefore a given configuration bitstream, the configuration bits can be classified

at design time as critical, transparent or suspect (CTS classification). Transparent bits correspond to bits whose value cannot impact the expected functionality; errors in these bits are therefore harmless. Suspect bits correspond to bits whose impact depends on the propagated data or on the configuration of other FPGA cells. Algorithms have been developed to reduce the size of this set of bits; they are currently being implemented in the tool. Results of injections by laser have been used to validate the current classification determined by the tool and the refinement obtained with the new algorithms will be evaluated in 2009. This approach is complementary to the experimental approach described in section 2.9.

6.6 Multi-level hardening of integrated embedded system for safety/availability and security

Members: R. Leveugle, P. Maistri, L. Anghel, G. Canivet, V. Maingot, J. B. Ferron

The goal of this project is to develop methods, libraries and tools to design robust integrated embedded systems. These systems must be able to cope with both natural faults and security-related fault-based attacks. Protections against fault-based attacks are evaluated with respect to their fault detection/tolerance capability, but also with respect to their potential impact on the robustness against side-channels attacks. The protection mechanisms are studied at several levels: logic, architecture, operating system and software. Complementary approaches are considered to provide a complete toolbox to a designer.

The first approach is the development of robust versions of processor or coprocessor cores. In particular, robust versions of the Leon2 processor and of an AES cryptographic coprocessor have been designed. The DDR scheme used for the AES has been published in the IEEE Transactions on Computers in 2008 and attacks on a FPGA-based prototype are on-going. Modifications of the eCoS real-time operating system had also been defined to provide low-cost fault tolerance and an embedded system demonstrator was developed, implemented on a Xilinx Virtex II Pro development board.

In addition to the development of hardening techniques and hardened IPs, a study has aimed at evaluating the impact of fault-oriented protections on leakage information. As a matter of fact, in the security context, it is useless to protect a circuit against only one type of attack, since a hacker could use several approaches to obtain secret information. Fault-based attacks are one type of threats. Another one is the use of so-called "side channels", and in particular the power consumption or the electromagnetic emissions, to infer some confidential data used during a computation. It is therefore very important to ensure that protections against fault-based attacks do not facilitate an attack using the side channels (and vice-versa). Results were obtained in the frame of the MARS project (2004-2007), part of the program "ACI Sécurité & Informatique" supported by the French Ministry of Research. Complementary experiments made in 2008 have in particular shown that the implementation of error detecting or correcting codes in a circuit does not have a very strong impact on the sensitivity to power-based (DPA) attacks. However, the code check bits can be attacked as well as the original data bits. Also, the combinatorial logic in the circuit has a significant influence on the circuit DPA sensitivity. Finally, error correcting codes may be interesting, not to achieve error correction (the probability of a correction in case of multiple errors is low) but to increase error detection and (slightly) reduce the DPA sensitivity.

Another important aspect when designing a secure circuit is the impact of the Design for Test (DfT) approaches (scanpath insertion, boundary scan, …) on the circuit robustness. DfT aims at increasing the level of observability and controllability that is just the opposite of the security constraints. We have therefore evaluated an approach based on Software-based BIST (also called SBST), to achieve better compatibility between testability and security. The main conclusion is that the approach can allow very cheap self-test of an AES core in a system including a main processor, but achieving 100% fault coverage can be difficult and the protections implemented in the cryptographic core against fault-based attacks can still reduce the achieved fault coverage.

Due to the increasing spatial multiplicity of error patterns, protecting a circuit with information redundancy is more and more difficult. Another approach consists in using functional checks. In this context, we have developed in 2008 a new control-flow checking technique. This technique is non-intrusive and does not require a modification of the initial microprocessor-based system. Checks include not only the control flow itself, but also the integrity verification of critical data, with several possible trade-offs between overheads and error detection. The approach is compatible with the norms requiring a complete separation between the nominal functions and the checking features (e.g. for automotive applications). This technique will be evaluated on a prototype in 2009.

Finally, studies are on-going on the problems related to errors in SRAM-based FPGAs. The goal is to propose specific design techniques to achieve robustness at lower cost than the classical massive redundancy approach.

6.7 Towards robust nanoelectronics design

Members: L. Anghel, T. Dang, R. Leveugle

Some work has started in 2000 on the implementation of logic circuits using nanoelectronic devices. This project had been initially defined in collaboration with CEA/LETI and aimed at taking advantage of silicon-based single-electron transistors (SETs). A study of the state-of-the-art had been performed, including the study of simple logic and arithmetic components and some expertise of the simulation approaches available for such devices. More recently, the use of carbon nanotube transistors (CNTFETs) has been considered. Between 2004 and 2007, our work in this area was part of the NANOSYS project, started in the framework of the program "ACI Nanosciences" supported by the French Ministry of Research, in collaboration with many French research teams.

The work aimed at proposing solutions to implement robust logic elements based on these components. This implies defect tolerance due to the expected high density of manufacturing defects, as well as fault tolerance to cope with other problems such as process parameter variability and transient faults. The work was based on CNTFET simulation models provided by Nanosys partners. These models have been used to compare the characteristics of a set of logic gate structures. Dispersion analysis has been done on some logic gates, showing that very small variations in the diameter of carbon nanotubes, or other physical parameter may lead to important dispersion of static characteristics of analyzed gates. Dynamic behaviour has also been studied and a tool for random defects injection has been developed. Finally, the robustness of redundant structures has been evaluated. These results have been summarized in the PhD dissertation of Trinh Dang.

6.8 Multiple Defects Tolerant Devices for Unreliable Future Nanotechnologies

Members: L. Anghel, C. Lazzari, M. Nicolaidis

Nanotechnology solutions point at the horizon with the sophistication of the chemical synthesis processes, making possible to synthesize chemically electronic components and their interconnections, to create very complex systems at low cost. These solutions are today needed to surmount technical barriers (high leakage currents, signal integrity, power density, small node storage capacities, ...) but also economical barriers (e.g. excessive cost expected for the fab-lines of future CMOS process generations). Although most of the new nanoelectronic solutions (e.g. single electron devices, quantum cellular automata, carbon nanotubes, molecular components, semiconductor nanowires, chemically assembled electronic nanocomputers (CAEN)) are still in the research domain, significant improvements have been done in assembling them into logic gates and memory arrays to compute very complex computational systems with a much higher integration density than in nowadays CMOS, lower power consumption and higher speed. It is forecasted that these systems would integrate hundreds of billion devices in regular networks.
However, for such a densely integrated circuit to perform a useful computation, it has to deal with the inaccuracies and instabilities introduced by fabrication processes and the tiny devices themselves. Permanent faults occurring during fabrication are intimately related to the process used to fabricate the structures of a design. Different fabrication processes will result on different defect densities. For instance, if the product is fabricated by chemically synthesis of the components and interconnections, the defect densities related to such a process could be very high. On the other hand, transient faults are determined by the environment, physics and the devices operation conditions, which are not necessarily related on the way they are fabricated. Future nanoelectronic architectures have to be able to tolerate an extremely large number of defects and faults. Today it is not known which will be the nanotechnologies that will be adopted in the future to build complex computational systems, and in addition we do not know exactly which will be the causes of transient and permanent faults.
Although recent research has resulted in the development of basic logic elements and simple circuits in nanoscale, there are still debates on what logic style and architecture will be the best for nanocomputers.
For most of the solutions proposed in the literature it is predicted that the defect densities could be as high as 10^{-2}, which could be seen as a few defective cells for every 100 memory cells.
The design of defect-tolerant architectures for the ultra-large integration of highly unreliable nanometer devices is therefore inevitable.

However, new fault tolerant design paradigm is needed, since with these high defect densities both the regular resources and the redundant ones will be affected by the defects, disabling the basic principle of traditional fault tolerance (use of a fault-free redundant unit to perform the job of a faulty regular unit). Several approaches have been proposed in the last 3 years in TIMA laboratory, dealing with self repairing memory architectures for high defect.
Today there is an increasing interest in using hardware redundancy to mask faulty behavior in nanoelectronic components. Two of improved versions of von Neumann multiplexing gates are currently under research as well as a multiple defects tolerance techniques at transistor and logic level that can apply to any logic gate including flip flops and memory elements.

6.9 Experimental radiation qualification of SRAM-based FPGAs

Members: G. Foucard , A. Bocquillon, R. Velazco

The increasing popularity of low-cost safety-critical computer-based applications in a large scope of areas (such as space and avionic's applications, automotive, biomedical, telecontrol, etc.) requires the availability of new circuits and methods for designing dependable systems. In particular, in the areas where computer-based dependable systems are currently being introduced, the cost (and hence the design and development time) is often a major concern, and the adoption of commercial reconfigurable hardware, such as SRAM-based FPGAs (Field Programmable Gate Arrays) is a common practice. As a result software implemented fault tolerance is an attractive solution for this class of applications, since it allows the implementation of dependable systems without incurring the high costs coming from designing custom hardware or using hardware redundancy.
Despite these attractive characteristics, designers are reluctant to use these components for critical applications due to their sensitivity to Single Event Upsets (SEUs) provoked by radiations. Indeed an energetic particle hitting a memory cell may induce a modification of its content (bit-flip). All SRAM-based FPGA resources are controlled by its configuration memory, an SEU in this area may thus change the original behavior of the application. Moreover a fault affecting this memory is permanent until the device is configurated again.

Quantifying the sensitivity of the configuration memory is therefore mandatory in order to evaluate the sensitivity of a specific application. This project focuses on the methods and tools to evaluate the sensitivity to radiation of applications implemented in the target FPGA. Experiments must be performed using radiation facilities (particle accelerators, laser systems,…) to inject faults in the target device and quantify the error rate of the studied application.

The Virtex II FPGA was used as a demonstrator for this project. Two complementary facilities were used: the HIF Cyclotron and a pulsed laser. The firstone allowed to put in evidence the significant contribution of the SRAM configuration memory to the sensitivity of any application implemented on a SRAM-based FPGA. The static-cross section was obtained and is presently used to explore the obtention of the dynamic cross-section by fault injection. The laser experiments allowed to identify potential single-point failures of fault tolerant techniques, this by exhaustive mapping of selected area in which faults are injected with step by step (in our case with a 1 micron step) in the configuration memory.

This project is done in collaboration with IMS laboratory (Bordeaux), EADS (Suresne).and UCL (Université Catholique de Louvain-la-Neuve).

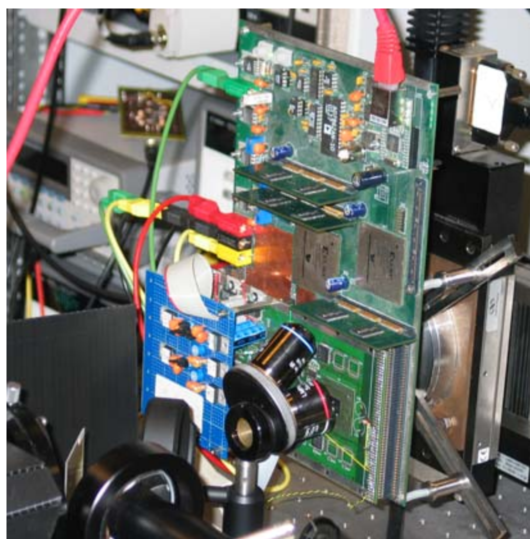

Figure 4. The THESIC test platform at the ATLAS laser facility of IMS (University of Bordeaux)

6.10 Hardened memory cells

Members: L. Anghel, M. Nicolaidis, R. Velazco

Radiation-induced transient effects in silicon CMOS circuits are essentially charge collection and transport phenomena resulting from direct ionization. The collected charges may inadvertently change, for short time intervals, the internal node voltages of the circuit (single event upset). These transients may change the electrical behavior of the MOS transistors in digital and analog circuits.

Design hardening techniques at circuit level can be developed to achieve immunity to upsets. A lot of hardened-by-design memory elements have been proposed in the last years. In 1994 and 1997 were developed two hardened cells in TIMA laboratory, so-called, HIT2 (Heavy Ion Tolerant cell) and DICE (Dual Interlocked Cell) respectively. The philosophy was to strengthen the feedback of the cell in order to restore the data potentially corrupted by the impact of a charged particle. However, the price to pay is an increase of the cell area as well as higher power consumption. A recently developed hardened memory cell is under evaluation at TIMA/ARIS. The new architecture includes extra transistors to introduce means to delay the transient signal from the feedback path, thus avoiding the appearance of the SEU.

The performances of different kinds of SRAM cells built using the same CMOS technology will be compared.

6.11 Low-cost Single Event Latchup Mitigation Architecture for Memories

Members: M. Nicolaidis (in collaboration with CMP)

Existing single event latchup (SEL) mitigation approaches include process level mitigation, which is very often undesirable as it may costly and/or affect circuit performance; insertion of guard ring structures, which increase significantly area and may also impact performance; power recycling which removes latchup but destroys circuit state. The proposed scheme combines Error Control codes, usually used for mitigating SEUs, and sleep transistors, usually used to reduce power, in an original architecture that enables:

- latchup effect containment,
- latchup detection,
- latchup elimination,
- correction of latchup induced errors.

The resulting architecture is fully protected against SELs without affecting system operation, and induces insignificant area, performance and power penalties.

6.12 Fault Tolerant Architectures for Mitigating the Flaws of Nanometric Technologies

Members: L. Anghel, M. Nicolaidis, C. Rusu, H. Yu, N. Zergainoh

Silicon-based CMOS technologies are fast approaching their ultimate limits. By approaching these limits, power dissipation, fabrication yield, and reliability worsen steadily making further nanometric scaling increasingly difficult. These problems would stop further scaling of silicon-based CMOS technologies at channel lengths between 10 and 20 nm. But even before reaching these limits, these problems could become show-stoppers unless new techniques are introduced to maintain acceptable levels of power dissipation, yield and reliability. Fault tolerant design is a powerfull solution for improving reliability and yield. However, traditional fault-tolerant architectures incur very high cost in terms of silicon area and power penalty. High area cost reduces their interest for commercial applications, while high power penalty makes them inacceptable in terms of battery life in portable devices and in terms of power density constraints in nanometric process nodes. In this work we develop innovative time-redundancy based fault-tolerant architectures able to mitigate the effects of faults induced by variability (process, temperature and voltage), circuit aging, EM interferences and ionizing particles. Due to their innovative principles, these architectures incur very low area and power penalty. Their combination with a dynamic frequency-voltage scaling approach allows operating at very low voltage, enabling significant power dissipation reduction.

6.13 Combining Circuit-level Fault Tolerance with OS-level Scheduling for Efficient DFVS

Members: G. Bizot, M. Nicolaidis, N. Zergainoh

Circuit-level error detection signals are monitored to adapt frequency, voltage and body biasing to the application requirements and circuit delay degradation induced by variability, EMI and aging.

6.14 Computing Architectures for Nanotechnologies

Members: L. Anghel, M. Nicolaidis, N. Zergainoh

Silicon-based CMOS technologies are predicted to reach their ultimate limits by the end of the next decade. Research on nanotechnologies is actively conducted in a world-wide effort to develop new technologies able to maintain the Moore's law. They promise revolutionizing the computing systems by integrating tremendous numbers of devices at low cost. These trends will provide new computing opportunities and will have a profound impact on the architectures of computing systems. This work describes architectures able to exploit the extraordinary computing power promised by nanotechnologies in order to model and simulate complex natural or artificial systems composed of huge numbers of simple elements.