HAL
archives-ouvertes.fr

A Comprehensive End-to-end Solution for a Secure and Dynamic Mixed-signal 1687 System

Michele Portolan, R. Silveira Feitoza, G. Takam Tchendjou, V. Reynaud, K. Senthamarai Kannan, Manuel J. Barragan, Emmanuel Simeu, Paolo Maistri, Lorena Anghel, R. Leveugle, et al.

▶ **To cite this version:**

Michele Portolan, R. Silveira Feitoza, G. Takam Tchendjou, V. Reynaud, K. Senthamarai Kannan, et al.. A Comprehensive End-to-end Solution for a Secure and Dynamic Mixed-signal 1687 System. 2020 International Symposium on On-Line Testing and Robust System Design (IOLTS 2020), Jul 2020, Naples (Virtual Conference), Italy. 10.1109/IOLTS50870.2020.9159721 . hal-02939302

HAL Id: hal-02939302
https://hal.archives-ouvertes.fr/hal-02939302

Submitted on 2 Oct 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial| 4.0 International License

This is the author's version of an article that has been published in this conference. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/IOLTS50870.2020.9159721

A Comprehensive End-to-end Solution for a Secure and Dynamic Mixed-signal 1687 System

M. Portolan, R. S. Feitoza, G. T. Tchendjou, V. Reynaud, K. Kannan, M. Barragán, E. Simeu, P. Maistri, L. Anghel, R. Leveugle, S. Mir

Univ. Grenoble Alpes, CNRS, Grenoble INP[1], TIMA, 38000 Grenoble, France

Abstract- The disruptive potential of the IEEE 1687 standard does not come from a single innovation, but rather from its capacity of providing a unified framework where heterogeneous approaches can co-exist and interact. In this Special Session, we will present the complementary research activities performed in the TIMA laboratory covering different aspects of the standard (Mixed-Signal instrument testing, Embedded Aging Monitors and Test Access Securization), and their coordination thanks to the Manager-for SoC Test (MAST) software environment.

Keywords—Mixed-Signal Testing, ADCs, Embedded Test Instruments, Circuit Aging, Secure Access, Authentication, Automated Test Environments

INTRODUCTION

The disruptive potential of the IEEE 1687 standard does not come from a single innovation, but rather from its capacity of providing a unified framework where heterogeneous approaches can co-exist and interact. The HADES project covers most of them: starting from mixed-signal and digital embedded instruments to the top-level software framework, passing through hierarchical scan architectures and secure access. In this Special Session, we will show how TIMA leveraged its multi-disciplinary skill set to propose a comprehensive solution: building around MAST, a new dynamic execution environment tailored around the needs of 1687 to overcome the limitations of legacy EDA tools [1], we have been working to merge the individual contributions into a rich Hardware-Software environment where all topics addressed by HADES coexist.

In this paper, each section will present TIMA's contribution to a given thematic and its integration into the MAST Environment.

I. REDUCED-CODE STATIC LINEARITY BIST OF SAR ADCS

The integrated successive approximation register (SAR) ADC has been widely used in the latest years due to their good trade-off between power efficiency and speed. However, these converters are susceptible to static errors that degrade the conversion accuracy. Hence, static linearity tests are required in order to guarantee a correct operation. These tests are usually a challenging and costly task that require expensive ATE. A promising alternative for reducing static linearity test complexity and cost is the reduced-code static test technique, that relies on the repetitive operation of some ADC architectures. The benefits are twofold: firstly, the number of necessary measurements for a complete static characterization is drastically reduced, and secondly, the reduced test complexity facilitates the on-chip implementation in a Built-In Self-Test (BIST) fashion. The static linearity of a SAR ADC is mainly dependent of the static performance of its internal DAC. Thus, it follows that we could infer the static linearity of a SAR ADC by characterizing the static linearity of its DAC. The core idea of the proposed reduced-code test technique is to employ the converter internal DACs to generate a DC voltage that is proportional to the length of the code associated to its Major Carrier Transitions (MCTs). In this project we have developed reduced-code algorithms for different families of SAR ADCs, including SAR ADCs based on a) binary weighted capacitor DACs [2], b) split-capacitor DACs [3], and c) resistor-based thermometric segmented DACs [4]. Furthermore, the techniques have been extended recently to include SAR ADCs employing the power-efficient Vcm-switching technique [5]. The generated DC voltages are then digitized by an embedded Incremental ΣΔ ADC (IADC) for an efficient and accurate conversion. This family of converters is very suitable for accurately digitizing DC voltages. We use a simple first-order IADC that consists of a switched-capacitor integrator, a comparator and a digital counter. Moreover, it has been shown that this converter can be merged with elements of the SAR ADC under test to further reduce area overhead [4]. A digital processing maps the obtained measurements to the length of the codes of the SAR ADC under test. The INL and DNL of the converter are then obtained from this inferred characteristic.

As an example of application, we performed transistor-level transient simulations of a complete BIST system including a 10-bit split-DAC (6×4) Vcm-based SAR ADC under test with an embedded IADC for test. In order to provide a realistic validation of the technique, a worst-case sample (3σ variation) in terms of static linearity was selected and characterized using both the proposed reduced-code test strategy and the standard histogram test (with a high-resolution ramp stimulus and 128 hits-per-code). The obtained results for DNL and INL estimations are shown in Figure 1. It is important to notice that the reduced-code test only employs 9 measurements to derive the complete static characteristic, which represents less than 1% of the codes of the 10-bit SAR ADC under test. The obtained rms error in the estimation of the INL is below 0.25 LSB, with a maximum error below 0.6 LSB. The total test time for the reduced-code test strategy was 460.8 µs while the standard 128 hits-per-code histogram test takes 3.28 ms. The obtained test time reduction represents a test time saving of 86% compared to the standard histogram.

[1]Institute of Engineering Univ. Grenoble Alpes

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

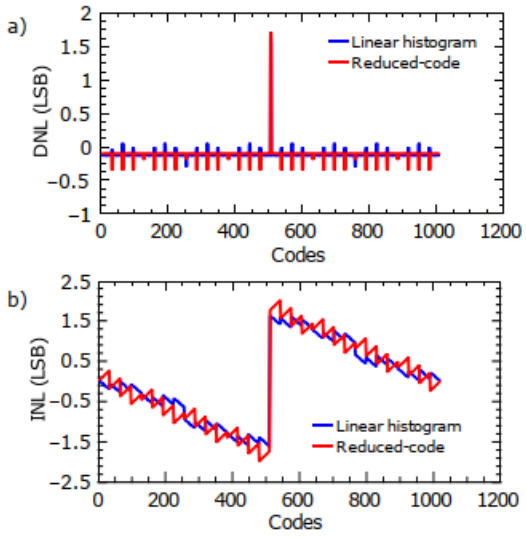

Figure 1. Static linearity test results comparing the standard linear histogram test and the proposed reduced-code test technique, a) DNL and b) INL.

Traditionally, the only solution to deliver and package complex instruments such are those presented is to make them completely self-contained as fully embedded BIST. In the framework of HADES, we leveraged the capacity of the MAST environment of handling the dynamic execution of test programs over a complex SoC hierarchy. In particular, it can be used to access embedded mixed-signal instruments inside SAR ADC arrays for CMOS imagers while offloading complex digital processing outside the chip, to obtain a flexible tradeoff between performances and area occupation without sacrificing portability and standard compliance [6]

II. Image Quality Evalution For Image Sensor Performance Assessment

Driven by massive investments and impressive technological advances, autonomous technologies are now being used in many sectors of activity. The rapid emergence of these new technologies is leading to new research challenges in terms of both security and reliability. To meet these challenges, processes for continuous monitoring of the performance of the autonomous system and its components is a promising way forward. This study proposes a performance monitoring loop for integrated devices involved in autonomous applications. The loop consists of an assessment phase in which performance is evaluated, and a monitoring phase in which performance is corrected if necessary. This approach is illustrated on image sensors for which a blind image quality assessment process is proposed for the estimation of an index of perceived image quality, using non-distortion specific and no-reference features extracted from the images. The proposed index is used in building a control loop to self-correct the image sensors.

Used for the restitution of the environment perception, the camera integrating image sensors is a central element in autonomous systems. The image sensor performance assessment is based on Indirect Learning Blind Image Quality Assessment (ILBQA) index, constructed by pooling, using machine learning techniques, several image features extracted from four concepts. The overall process of building this index is based on two learning phases and four feature extraction axes [7]. The proposed process for designing the prediction models of this index is shown on Figure 2.

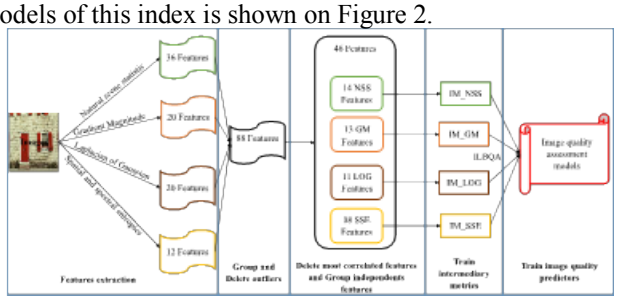

Figure 2. Image Quality Assessment.

The control loop process shown in Figure 3 consists of two main phases [8][9]. The first phase is the image quality assessment using the ILBQA index, and the second is the detection and concealment of defective pixels for image correction. The defective pixel detection method is based on the evaluation and analysis of local dispersion parameters of the pixel blocks, while the concealment method is based on local median filters. This control loop process takes an image and a target quality score as inputs and generates the corrected image when its quality score is above the target quality or when the quality decreases after a correction. This control loop has been implemented on FPGA demonstrating the feasibility of integrating the proposed solution in an image sensor.

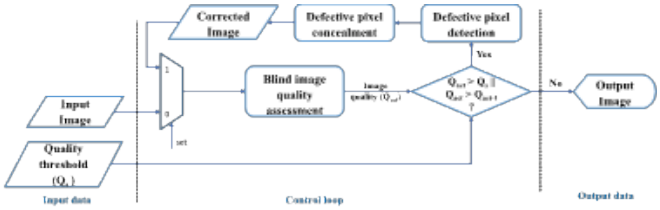

Figure 3. Performance control loop.

FPGA results are very encouraging, with more than 93% correlation for image quality assessment and a significant enhancement of the performance of image sensors in the control loop. Work in progress is oriented towards extracting information from the control loop to feed a dataset that will be used to evaluate wear features and device reliability.

III. Digital System Failure Prediction face to Variability and Aging

In complex SOC design manufactured in nanometric technologies, circuit functionality in all process corners and face to all kinds of variabilities needs to be verified. Variabilities and wear-out degradation impact system performance, potentially resulting in timing and functional failures. Indeed, local and global variability, aging phenomena, such as NBTI and HCI, have become the most critical reliability issues. Hence, taking into account these phenomena during design and validation steps is mandatory, especially for high reliable application such as automotive, health-care or other mixed-critical applications. In fact, these

reliability threats can severely degrade performance and in the worst case they can provoke system failures. It is common for most of these applications to embed reliability and performance monitors. The usage of in-situ monitors for error and pre-error detection allow decreasing the constraints imposed on the overall design. They are implemented together with Adaptive Voltage Scaling (AVS) or Dynamic Voltage Frequency Scaling (DVFS) which are triggered by pre-errors in-situ timing monitors while adapting dynamically the frequency and the voltage according to the operating conditions and the application needs [10]. Therefore, the performance degradation can be compensated and the circuit's lifetime can be extended. Different pre-error monitors have been proposed and characterized by different research teams since early 2000. The most efficient are based on Replica Path principle, but the design has been optimized to allow sensing local and global variability and aging degradations [11]. Externally-placed sensors in the intended design are suitable for easy-implementation and detection of global process centering and average aging, while in situ monitors are better for fine-grained detection of global as well as local variation and more accurate aging. Also, monitor failure prediction approach is better as they generate warnings prior to timing failures, giving the system enough time for correction through compensation strategies. In situ monitors are more accurate in terms of global and local variation detection compared to externally situated monitors due to their localization within the design. The drawback for the in–situ monitors insertion is the difficulty to close the timing and fix the critical path rankings. Indeed some initial selected set of endpoints at early physical synthesis steps or at place and route steps, can become sub-critical after the detailed routing steps, and in the same time, sub-critical endpoints can become critical at the final steps. In that last situation, ECO loop is carried out to fulfill this new critical path monitoring. The activation of in-situ monitor inserted on critical paths is another very important issue, because if the path is not activated during the workload execution, the in-situ monitor cannot raise pre-error signal. In a complex SoC where multiple functional modes are available, all in-situ monitors inserted on the critical paths may not be activated in a particular functional mode. This limitation can be overcome by using a combination of scan design and specific ATPG vectors that are periodically applied to the circuit. Therefore ISM inserted on critical paths can be activated and potential degradations can be detected. Effectiveness of monitors also depends on the insertion flow as it helps decide the selection of critical paths where monitors need to be inserted. The flow needs to be weakly intrusive with respect to the initial performance.

Current design practices perform monitors insertion in near-critical paths, identified by classical techniques such as Static Timing Analysis (STA), with the assumption that they should be the first affected by transistor degradation. Even if promising this approach still has a serious weak point: phenomena such as NBTI and HCI are strictly correlated to circuit activity, generated by the executed workload. This means that aging is not necessarily coherent with STA results, as near-critical paths could be seldom activated [11]. Experiments demonstrated how STA performed on aged circuits can deliver a significantly different set of near-critical paths depending on the workload. In a complex digital design, the number of monitors to be inserted can become rapidly huge, and the decision to detect global and local variations as well as aging has to be taken at design time. Complex designs have hundreds of thousands of Flip Flops, where each endpoint is the destination of a path or multiple paths converging to the same endpoints. Therefore, careful consideration of the overall timing of the critical and subcritical paths in a complex digital design is mandatory, and has to include the impact of all mentioned variations.

To tackle the above-mentioned issue, we decided to explore a new research direction consisting in find 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. Our research activities focused on the development of Machine Learning algorithms for predicting circuit aging. This implied a deep bibliographic effort to identify the main physical aging phenomena and insert them in a ML-friendly model. This allowed us to couple a lightweight Machine Learning prediction framework with traditional, computationally intensive circuit simulations as validation. First applied on the older technology, this Proof-of-Concept was presented with success as a Poster [12], where it was demonstrated the capability to reliably 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.

Like all ML approaches, our solution relies on the quality of input data. For this reason, we are planning to use MAST to implement the Aging framework on an Embedded Processor and exploit 1687 to access integrated monitors to calibrate the prediction thanks to real usage and aging data.

IV. Dynamic Authentication-Based Secure Access to Test Infrastructure

Testing circuits after manufacturing and during their lifetime has become an increasingly important challenge for designers over time. In order to face the increasing complexity of Systems-on-Chips (SoCs), those standards have continuously evolved. In recent years, IEEE 1687 has introduced the dynamic reconfiguration of the scan chain, where specific segments can be included or excluded at will to target specific subparts of the circuit in the most efficient way. Unfortunately, these test facilities may create an important security backdoor into the circuit, which may be used by malicious users. Possible outcomes may consist in leakage of sensitive and critical data, illegal tampering of circuit behavior, or theft of Intellectual Property. Therefore, to seal this security breach it is mandatory to implement a protection layer over the test infrastructure. The literature proposes some secure solutions [13][14], where the access to the test infrastructure is granted only after the User has successfully performed some kind of authentication thanks to at least one secret key. So far, these solutions were either vulnerable to

simple threats such as replay or man-in-the-middle attacks, or would require custom procedures which are difficult to implement in the classical Test Automation Flow, which effectively limit their usability in a real industrial scenario regardless of their technical merit.

In this context, TIMA's effort first focused on the development of Segment Set Authorization Keys (SSAK) [15], an authentication framework optimized for embedded usage. Instrument keys are replaced by configuration keys or Segment Set Authorization Keys (SSAK). These new keys can resolve any authentication in just one cryptographic computation. To reduce the memory footprint need to store the secret key, SSAK introduces a procedural generation key mechanism presented in Figure 4. All the configurations keys of a circuit instance are dynamically generated from the unique secret key of the circuit and the related configuration vector. This configuration vector has to contain the list of targeted instruments and can also contain an identification number if the keys need to be different for each user. The generation consists in an encryption of the configuration vector using the circuit key as encryption key. The security provider can distribute credentials composed of configuration and SSAK to the users. On the other side, the Circuit Key is securely stored in the reconfigurable memory of the Authorization Controller.

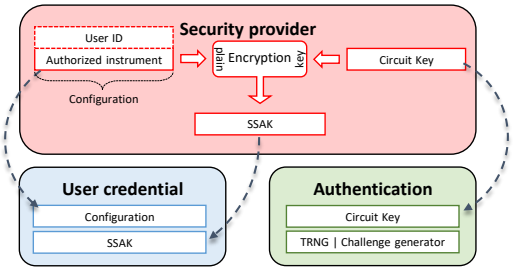

Figure 4. SSAK procedural key generation and distribution.

Concerning the authentication protocol, only the challenge resolution is performed. The controller receives the configuration vector from the user, and then thanks to the procedural key generation, it is able to compute the associated SSAK, using its embedded encryption processor. Then, still using the same encryption hardware, the controller can resolve the challenge with this SSAK. On the user side, the process is easier as the SSAK is already known, so the user only needs to encrypt the challenge with the key contained in the credentials. Once the SSAK framework was completed and validated, we exploited MAST to insert it into the standard 1687 flow, as depicted in Figure 5. The principle, described in details in [16], is to remove responsibility for the authentication from the User and assign it to the EDA Tool (MAST in this case), to provide a truly flexible and portable solution.

ACKNOWLEDGMENTS

This work has been partly funded by the French Government under the framework of the PENTA HADES ("Hierarchy-Aware and secure embedded test infrastructure for Dependability and performance Enhancement of integrated Systems") European project.

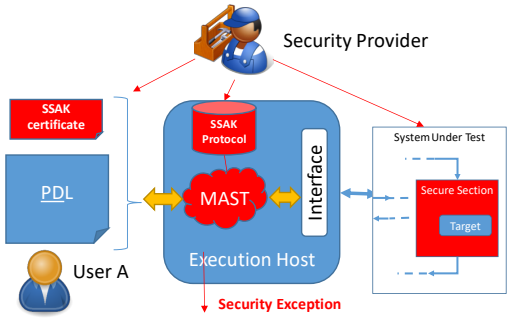

Figure 5. SSAK Integration into the standard flow [16].

REFERENCES

[1] M. Portolan, "Automated Test Flow: the Present and the Future", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, December 2019 .

[2] R. S. Feitoza et al., "Reduced-code static linearity test of SAR ADCs using a built-in incremental converter," in Int. Symposium on On-Line Testing And Robust System Design (IOLTS), July 2018, pp. 29–34.

[3] R. S. Feitoza et al., "Reduced-code static linearity test of split-capacitor SAR ADCs using an embedded incremental ΣΔ converter," IEEE Trans. on Device and Materials Reliability, pp. 37-45, 2019.

[4] R. S. Feitoza et al., "Reduced-Code Techniques for On-Chip Static Linearity Test of SAR ADCs," in 2019 IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC), October 2019, pp. 263–268.

[5] R.S. Feitoza et al., "On-chip reduced-code static linearity test of Vcm-based switching SAR ADCs using an incremental analog-to-digital converter," European Test Symposium (ETS), 2020.

[6] M. Portolan, M. J. Barragan, R.Alhakim, S. Mir , "Mixed-signal BIST computation offloading using IEEE 1687", 22nd IEEE European Test Symposium (ETS), 2017, pp.1–2.

[7] G. T. Tchendjou et al. "Fuzzy logic based objective image quality assessment with fpga implementation," Journal of Systems Architecture, vol. 82, 2018, pp. 24–36.

[8] G. T. Tchendjou and E. Simeu, "Defective pixel analysis for image sensor online diagnostic and self-healing," IEEE 37th VLSI Test Symposium (VTS), 2019, pp. 1–6.

[9] G. T. Tchendjou, E. Simeu, "Detection, Location and Concealment of Defective Pixels in Image Sensors," IEEE Transactions on Emerging Topics in Computing (to appear).

[10] A. Benhassain et al., "Robustness of Timing In-Situ Monitors for AVS Management", IEEE International Reliability for Physics of Semiconductors (IRPS), 2016.

[11] R. Shah et al., "Aging Investigation of Digital Circuit using In Situ Monitors", IEEE International Integrated Reliability Workshop (IIRW), USA, 2019.

[12] K.Kannan et al., "Run-Time Aging Prediction Through Machine-Learning", IEEE International Test Conference, October 28th-November 1st 2018, Phoenix, AZ, USA.

[13] Jennifer Dworak et al., "Don't Forget to Lock your SIB: Hiding Instruments using P1687", IEEE International Test Conference, USA, 2013.

[14] B. Rafal et al., "Fine-Grained Access Management in Reconfigurable Scan Networks," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, pp. 934-947, 2015.

[15] Marc Merandat et al., "A Comprehensive Approach to a Trusted Test Infrastructure," in IEEE Internation Verification and Security Workshop, Rhodes, Greece, 2019.

[16] M. Portolan, V. Reynaud, P. Maistri and R. Leveugle, "Dynamic Authentication-Based Secure Access to Test Infrastructure", IEEE European Test Symposium (ETS), May 2020.