TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Mechatronics, Informatics
and Interdisciplinary Studies

RELIABILITY ASSESSMENT AND ADVANCED MEASUREMENTS IN MODERN NANOSCALE FPGAS

Dissertation

Study programme: P2612 – Electrical Engineering and Informatics
Study branch: 2612V045 – Technical cybernetics

Author: **Ing. Petr Pfeifer**
Supervisor: prof. Ing. Zdeněk Plíva, Ph.D.

Liberec 2014

Petr Pfeifer

A Ph.D. Dissertation thesis submitted to the Technical University of Liberec.

Liberec 2014

Study programme: P2612 – Electronics and Informatics
(Elektrotechnika a informatika)

Field of study/Study branch: 2612V045 – Technical Cybernetics
(Technická kybernetika)

Thesis Supervisor:

prof. Ing. Zdeněk Plíva, Ph.D.
Institute of Information Technology and Electronics (ITE)
Faculty of Mechatronics, Informatics and Interdisciplinary Studies
Technical University of Liberec
Studentská 1402/2
ZIP 46117 Liberec I
Czech Republic

Bibliographic Citation:

PFEIFER, P. *Reliability Assessment and Advanced Measurements in Modern Nanoscale FPGAs*, Doctoral Thesis, Technical University of Liberec, 2014

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Mechatronics, Informatics and Interdisciplinary Studies

Institute of Information Technology and Electronics

RELIABILITY ASSESSMENT AND ADVANCED MEASUREMENTS IN MODERN NANOSCALE FPGAS

Czech version:

Spolehlivost mikroelektronických obvodů a nanostruktur

Porovnání a zvyšování spolehlivosti číslicových aplikačně specifických a programovatelných integrovaných obvodů

Declaration

I hereby certify that I have been informed the Act 121/2000, the Copyright Act of the Czech Republic, namely §60 - Schoolwork, applies to my dissertation thesis in full scope. I acknowledge that the Technical University of Liberec (TUL) does not infringe my copyrights by using my dissertation thesis for TUL's internal purposes.

I hereby declare that I have written this dissertation thesis by myself and that I have referenced all the sources used therein (including of the Internet sources contained in the list of quoted literature). Concurrently I confirm that the printed version of my master thesis is coincident with an electronic version, inserted into the STAG.

Prohlášení

„Byl jsem seznámen s tím, že na moji disertační práci se plně vztahuje zákon č.121/2000 Sb., o právu autorském, zejména §60 – školní dílo. Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé disertační práce pro vnitřní potřebu TUL.

Prohlašuji, že jsem disertační práci zpracoval zcela samostatně, a že všechny citované zdroje (včetně internetových) jsou uvedeny v seznamu citované literatury. Současně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG."

In/V Liberec Date/Datum ……/……/2014. Signature/Podpis……

Abstract (EN)

This doctoral Ph.D. dissertation thesis (Thesis) deals with the study of possibilities to evaluate reliability of circuits based on modern nanostructures. It also presents a new way of measurement of various internal parameters of microelectronic circuits based on modern nanotechnologies. This thesis presents a new solution and methodology of utilization of BRAM in FPGA and utilization of this modern part in dependable systems, enabling a new easy way of implementation, reliability assessment methodology and measurements in modern nanoscale microelectronics, computer systems and architectures gaining from the amazing world of programmable technologies.

Keywords:

Microelectronics, nanotechnology, FPGA, BTI, BRAM, internal parameters, aging, reliability and dependable digital systems

Abstract (CZ)

Tato disertační práce se zabývá studiem možností stanovení určitých spolehlivostních parametrů moderních obvodů a nanostruktur. V této práci je prezentován nový způsob měření různých parametrů mikroelektronických obvodů moderních nanotechnologií. Zcela nové řešení a metodologie využívá BRAM bloků v programovatelných obvodech FPGA, jako běžnou součást moderních řešení použitých i v systémech se zvýšenou provozní spolehlivostí. Prezentované řešení je novou metodologií. Umožňuje nový jednoduchý způsob implementace, odhadu a stanovení spolehlivostních ukazatelů, včetně měření parametrů moderní mikro- a nanoelektroniky, počítačových systémů a architektur těžících z ohromujícího světa programovatelných technologií.

Klíčová slova:

Mikroelektronika, nanotechnologie, FPGA, BTI, BRAM, parametry a stárnutí obvodů, provozní spolehlivost a spolehlivé digitální systémy

Contents

List of Figures

List of Tables

Abbreviations, Symbols and Acronyms

6sigma	6σ - Six Sigma
A	Ampere
A/D	Analog-to-Digital
ADC	Analog-to-Digital Conversion
ALU	Arithmetic Logic Unit
ASIC	Application-Specific Integrated Circuits
BOX	Buried Oxide
BRAM	Block RAM
BTI	Bias Temperature Instability
C4	Controlled Collapse Chip Connection
CLB	Configurable Logic Block
CMOS	Complementary Metal–Oxide–Semiconductor
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit or Central Processor Unit
CV	Capacitance-Voltage
DFR	Design for Reliability
ECC	Error Check and Correct
EMI	Electromagnetic Interference
EOT	Equivalent Oxide Thickness
ESD	Electrostatic discharge
FDSOI	Fully Depleted Silicon On Insulator

FinFET	Fin-Shaped Field Effect Transistor
FET	Field Effect Transistor
FIT	Failures In Time
FPGA	Field Programmable Gate Array
fs	femtosecond (10^{-15} second)
GB, GiB	Gigabyte (2^{30} bytes)
GHz	Gigahertz (10^{9} Hertz)
GPU	Graphics Processing Unit
HKMG	High-k Metal Gate
Hz	Hertz
I/O	Input/Output
IC	Integrated Circuit
I_{ddq}	Stand-by Current
JTAG	Joint Test Action Group
KB, KiB	Kilobyte (2^{10} bytes)
LSB	Least Significant Bit
MB, MiB	Megabyte (2^{20} bytes)
MCU	Microcontroller
MEMS	Micro-Electro-Mechanical Systems
MHz	Megahertz (10^{6} Hertz)
MSB	Most Significant Bit
MOS	Metal–Oxide–Semiconductor
MOSFET	Metal–Oxide–Semiconductor Field-Effect Transistor
MSPS	Mega Samples Per Second

NMOS	n-type (n-channel) MOS(FET)
ns	Nanosecond (10^{-9} second)
PAR	Place and Route
PC	Personal Computer (here also a computer in general)
PCB	Printed Circuit Board
PDSOI	Partially Depleted Silicon On Insulator
PMOS	p-type (p-channel) MOS(FET)
PoF	Physics-of-Failure
ps	Picosecond (10^{-12} second)
QFN	Quad Flat No-leads package
QFP	Quad Flat Package
R/W	Read/Write
R/O	Read Only
RAM	Random Access Memory
RDD	Random Dopant Distribution
RMS	Root Mean Square
RO	Ring Oscillator
RTC	Real Time Clock
RTL	Register Transfer Level
SMT	Surface-Mount Technology
SET	Single-Event Transient
SEU	Single-Event Upset
SIE	Serial Interface Engine
SoC	System-On-Chip

SOI	Silicon On Insulator
TDP	Thermal Design Power
THT	Through-Hole Technology
TQFP	Thin Quad Flat Package
TSMC	Taiwan Semiconductor Manufacturing Company
TSV	Through-Silicon Via
UART	Universal Asynchronous Receiver/Transmitter
UIM	Universal Interconnect Matrix
ULSI	Ultra Large-Scale Integration
USB	Universal Serial Bus
V	Volt
V_{csmin}	Minimum (Array) Operation Voltage
VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuit
VLSI	Very Large Scale Integration
W	Watt
XOR	eXclusive OR

"Constant advances in manufacturing yield and field reliability are important enabling factors for electronic devices pervading our lives, from medical to consumer electronics, from railways to the automotive and avionics scenarios. At the same time, both technology and architectures are today at a turning point; many ideas are being proposed to postpone the end of Moore's law such as extending CMOS technology as well as finding alternatives to it like CNTFET, QCA, memristors, etc, while at the architectural level, the spin towards higher frequencies and aggressive dynamic instruction scheduling has been replaced by the trend of including many simpler cores on a single die. These paradigm shifts imply new dependability issues and thus require a rethinking of design, manufacturing, testing, and validation of reliable next-generation systems. These manufacturability and dependability issues will be resolved efficiently only if a cross-layer approach that takes into account technology, circuit and architectural aspects will be developed.",

from COST MEDIAN Action IC1103.

Preface

The speed of development and implementation of innovative technologies and introduction of advanced processes and methods is really extremely fast and amazing. Rapidly growing portfolio of new technologies in design and manufacturing of advanced integrated circuits allow higher integration of complex structures at ultra-high nano-scale densities. However, the new devices are sensitive to negative effects of various changes of the internal nanostructures and parameters. The extremely fast downscaling of the semiconductor technology makes reliability a first order concern in modern high-performance as well as large low-power designs. Most of the new technologies have introduced new faster or low-power circuits and solutions. However, they are very expensive and all the dramatically increasing complexity of the design and simulation phases, together with strong pressure towards shorter time-to-market intervals, makes any precise testing and research tasks of the new structures extremely difficult within the given time frames. In addition, the increased integration densities make the reliability of integrated circuits the most crucial point in modern advanced systems as well as in any dependable system. It also is the very important task to develop and validate advanced measurement and reliability assessment methods together or along with the new technologies, nanoscale integrated circuits and manufacturing processes.

Acknowledgements

There are several people who significantly influenced this dissertation. I'd like to thank my family very much for all the patience and support they gave me. I'd like to thank also prof. Zdenek Pliva, all my colleagues in TU Liberec, partners in Czech Republic as well as in BTU Germany, ZUSYS project, HiPEAC and COST MEDIAN partners, and also Dr. Ben Kaczer in imec Belgium.

Chapter 1

1 Introduction

Rapidly growing portfolio of new technologies in design and manufacturing of advanced integrated circuits allow higher integration of complex structures in ultra-high nano-scale densities. The speed of development and implementation of innovative technologies is amazing. FPGA (Field Programmable Gate Array) allow designing logic circuits directly in software. FPGAs consist of sets of high number of after-manufacturing custom configurable programmable circuits and memory block elements and units. In addition, FPGA devices are introduced very soon or just together with the new technologies used in ASIC (Application Specific Integrated Circuits). Today's technologies get closer and closer to the physical limits and the nature of physics. It also is one of the main reasons why the new devices are sensitive to negative effects of various changes of the internal nanostructures and parameters.

The process and parameter variability is increasing rapidly. The effects get much more visible on the latest generally available 28 nm, 22 nm (ready just now), or 14 to 16 nm technologies (under development or sampled in the first commercial lots nowadays) and their respective feature sizes. Voltage scaling does not keep pace with physical scaling and poses serious reliability issues like BTI (Bias Temperature Instability), HCI (Hot Carrier Injection), TDDB (Time-Dependant Dielectric Breakdown), etc. Higher current densities result in various electromigration effects. The aging of the electronic nanostructures, as well as the most of the generally negative internal changes due to various physical mechanisms, causes changes in parameters of CMOS structures; PMOS transistors are generally considered to be more sensitive than NMOS transistor structures. It is typically demonstrated as changes in the gate threshold levels. These changes also result in lowering of the maximal drain current as well as cut-off frequency, elongating the processing delays in the aging-affected circuits, compared to the original design. In

case of dependable systems, the key parameter lies in the negative changes in delays of critical paths. The system failures due to such negative effects must be avoided. Hence, all the critical changes have to be detected, in the ideal case the given or sufficient time before it results in the system failure. The new FinFET technology offers many advantages over the traditional planar MOSFETs; however their reliability performance is still not fully understood. NBTI in planar PMOS as PBTI in NMOS has been considered as a less important threat in the earlier nodes having SiO_2/SiON gate oxides. With the introduction of HKMG (High-*k* Metal Gate), the gate leakage has been reduced, but it has become a serious reliability concern along with BTI-related issues.

Changes in parameters due to process variations and aging along the working lifetime, as well as power supply voltage and temperature variations, can result in significant signal delays and may affect the final design quality and dependability. Especially BTI-inducted delays and timing variations may result in delay faults, propagating up to the device or equipment malfunction or failure. In deep-submicrometer devices and nano-scale technologies, it is why NBTI (Negative Bias Temperature Instability), caused in PMOS transistor structures by long low signal levels at the gates, or PBTI (Positive BTI), similar effect observed also in NMOS FET structures when scaling the technology down, also RTN (Random Telegraph Noise) and many new phenomena became visible and important factors influencing circuit's and the chip reliability parameters or lifetime.

Reliability of electronics will be the main concern in future design and development of new microelectronics and nanotechnologies. Reliability physics, reliability issues, its assessment and the system dependability aspects are one of the key areas to be solved and the key point of huge investments and work today. Teams all around the globe work on many advanced solutions.

This document presents an interesting new method, theory and results obtained in various tests including the important values of total delays or signal parametric changes. I do propose a new, low-cost and fast "on-chip" method without utilization of expensive external measurement equipment. It is directly linked to the quality issues of the devices,

allowing circuit parametric measurements. The proposed method and methodology allows wide range of basic as well as aging measurements fully on-chip. It could create the "holy-grail" of reliability measurements and also allows us to evaluate foundry technology directly on their product. The aspects of overall power consumption and other factors and conditions are also discussed. There are many measurement results present in this document. In addition, the measurements were performed on different technology nodes, including the latest low-power ones. This document also investigates the area of various effects caused by the main stress factors values to the FPGA chip design and related design trade-offs.

1.1 Background and Motivation

In 1975, Gordon Moore (born 1929 in San Francisco, California), co-founder of industry leader Intel Corporation, predicted that the number of transistors on a chip would double about every two years [*1*]. This is known as Moore's law and it says that technology revolution as the number of transistors integrated into microprocessor chips has to be exponentially increased for greater computing power. More has also predicted some limits, however those were and are successfully beaten as many other limits predicted many times years ago. In 1971, the Intel 4004 processor (4-bit) contained 2300 transistors, manufactured using 10 µm process and on the die area of 12 mm^2 and running at 741 kHz with max. TDP 0.63 W [*2*]. Since November 2011, the highest transistor count is in Intel's 61-core 244-thread Xeon Phi commercially available 64-bit CPU with over 5 billion transistors, manufactured using 22 nm 3-D tri-Gate transistor technology at the die area of about 700 mm^2 and it has Max. TDP of very high 300 W [*3*]. The product is codenamed Knights Landing using a 14nm process as it was announced in June 2013 [*4*]. The absolute record holds is probably held by NVIDIA Corporation with its Kepler GK110-based 7.1 billion transistor Super GPU, manufactured using TSMC's 28 nm manufacturing process [*5*] with max. TDP close to 300 W. In the world of programmable logic gates, the biggest chip today is Xilinx Virtex-7 2000T FPGA, which integrates 2 million logic cells providing an equivalent of 20 million ASIC gates and incorporating 6.8 billion transistors using Stacked Silicon Interconnect technology with 28 nm TSMC's HPL [*6*] (low power

with HKMG) die technology with 65 nm interposer and 19W max. TDP [*7*]. And the technology is moving forward extremely fast to 20 nm TSMC process generally available now for logic [***8***], Intel's 14 nm technology for high-end processors [***9***], and many other technologies for memories from 14 nm to 20 nm technology nodes and feature size from other key technology leaders, like Samsung, IBM, or the newest 15 nm Toshiba NAND memories [***10***]. Intel microprocessors adopted a non-planar tri-gate FinFET at 22 nm in 2012 that is faster and consumes less power than a conventional planar transistor [***11***].

Reliability of semiconductor devices and dependability of electronics equipment is one of the most discussed topics today. Many hard-working teams and scientists try to solve really hot issues worldwide. Working in this area for many years, I have performed number of researches and literature search using IEEE, Google and other search engines and also my original programs and scripts running on public as well as non-public databases, where a costly membership is required and offering much more information for my work. Base on a general search in the key areas, Figure 1 shows really strong evolution of the number of IEEE publications from publishers IEEE, AIP, IET, AVS, MITP, VDE, Alcatel-Lucent, IBM, BIAI, TUP and Morgan & Claypool, including conference publications, journals and magazines, books and eBooks, Early Access Articles, standards, and education and learning materials from available files since 1965. Figure 2 show search results for the publications about FPGA reliability. Figure 3 shows it for the second important keywords NBTI and CMOS. All the figures show strongly increasing number of published results or ideas, in fact doubled during the last 10 years. It is a clear evidence of very strong interest of research teams as well as development, manufacturing and also implicative interest of customers in work and results in these areas, as this documents aims at as well.

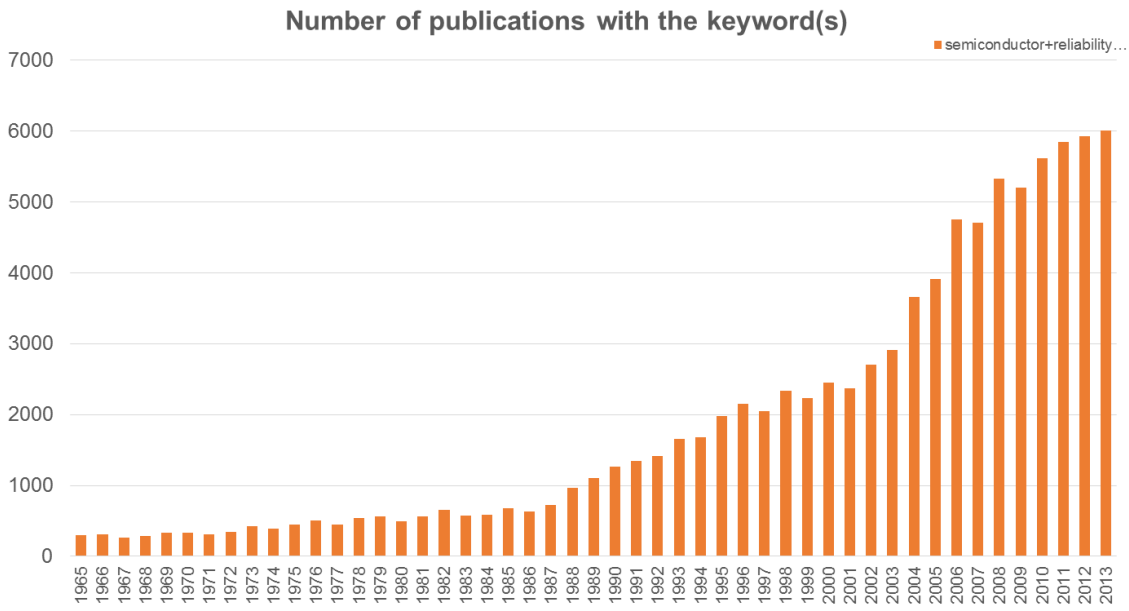


Figure 1. Evolution of the number of publications with keywords "semiconductor reliability".

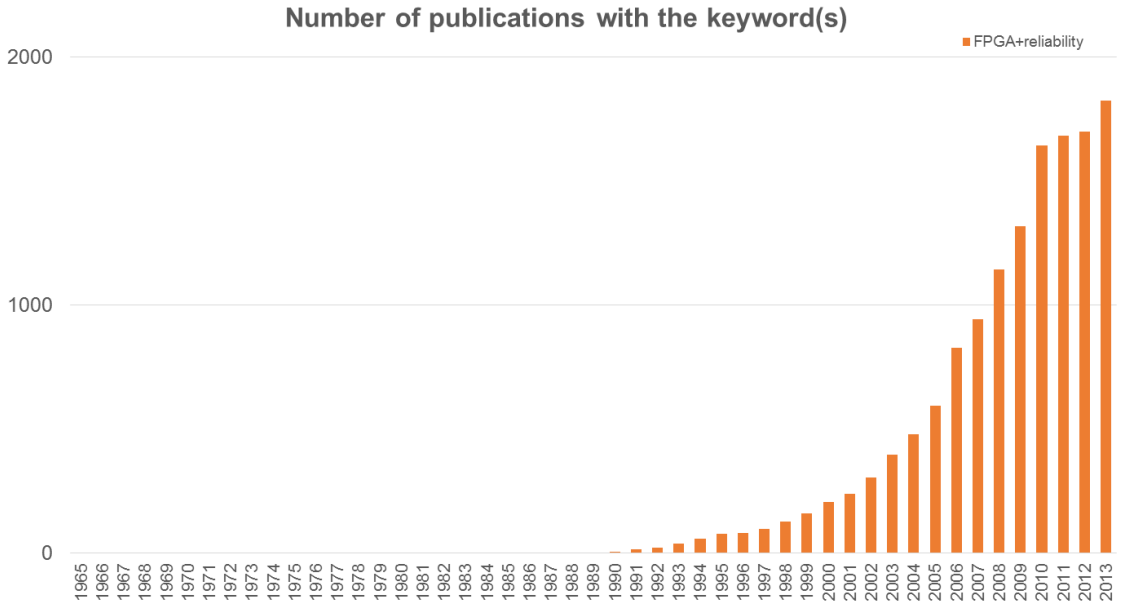


Figure 2. Evolution of the number of publications with keywords "FPGA reliability".

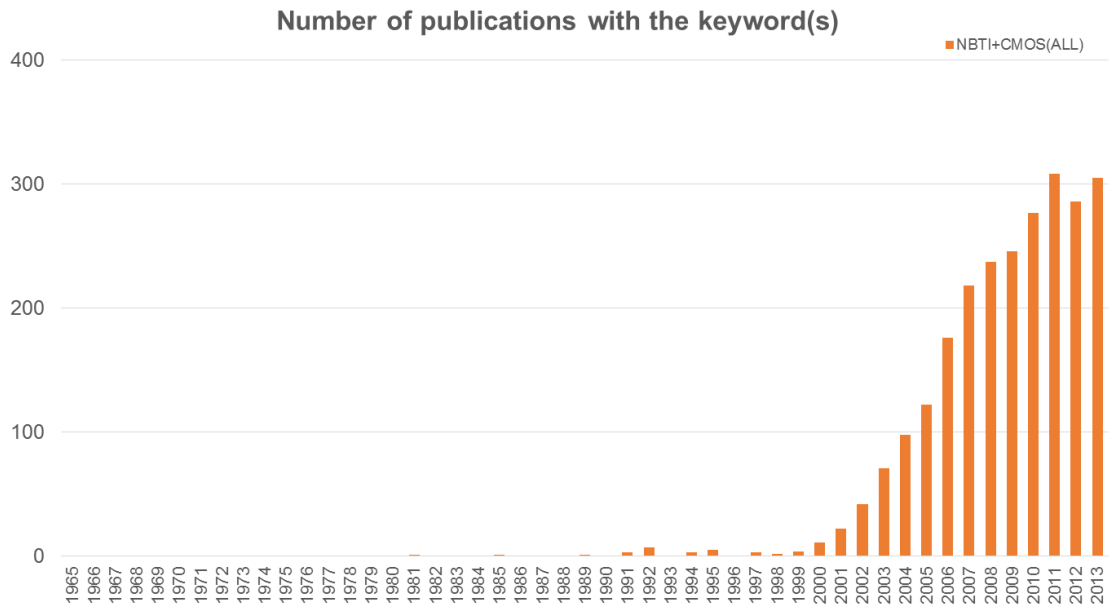


Figure 3. Evolution of the number of publications with keywords "NBTI CMOS".

The subchapter above shows the clearly increasing interest in the discussed areas and semiconductor reliability in general. The aggressive scaling of technologies requires utilization of new methods and materials. The nanoscale technologies and devices are subjects to various degradation processes. Application-specific integrated circuits (ASIC) allow design of special or support circuits, however such products are very expensive in their design as well as manufacturing processes. Fortunately, the invention of programmable devices, especially the Field Programmable Gate Array (FPGA) and their programmable structures have already enabled wider changes in the application functions after its manufacture process. In addition, the most advanced programmable chips are introduced at the newest available and the smallest feature sizes, the minimum designed size of a transistor or a wire in either the *x* or *y* axis or dimension, in very short time after the very first availability of new ASIC devices.

Parameters of devices and internal structures can be measured by external or internal circuits and methods. Today, BRAM (block random access memory) is the very standard part of all modern FPGAs. However, **there is absolutely no any publication that discuss or deals with such a way of utilization of BRAMs** for measurements in the chips and also using such data and results for evaluation of the device reliability parameters in order to analyse the actual platform, its actual state and estimate the system dependability. **Is possible to create and evaluate multiple programmable test structures, including the measurement blocks, directly on a Field-Programmable Gate Array (FPGA) chip? Is possible to perform a reliability assessment using Lab-On-Chip methodology and with BRAMs?**

The work-horse approach of reliability qualification has always been stressing and measuring of individual devices, either at wafer or at package levels (Figure 4a). To surpass constrains imposed by contacts and cabling, some groups have integrated part of their external instrumentation, such as GHz frequency sources, directly on chip (Figure 4b). Others have added multiple identical test structures, as well as on-chip selectors, allowing them to study time-dependent variability in deeply scaled technologies (Figure 4c). Using 28 nm technology Field-Programmable Gate Arrays, multiple test structures, including the measurement instrumentation, can be ad-hoc created and evaluated directly on the chip (Figure 4d). A concept of an entire "reliability lab-on-chip" is therefore demonstrated in this document. This concept can also be further extended by employing for example the high-end FPGA embedded processor in the aging evaluation (Figure 4e) of the platform itself, also enabling a completely new dimension of self-intelligence in self-awareness systems.

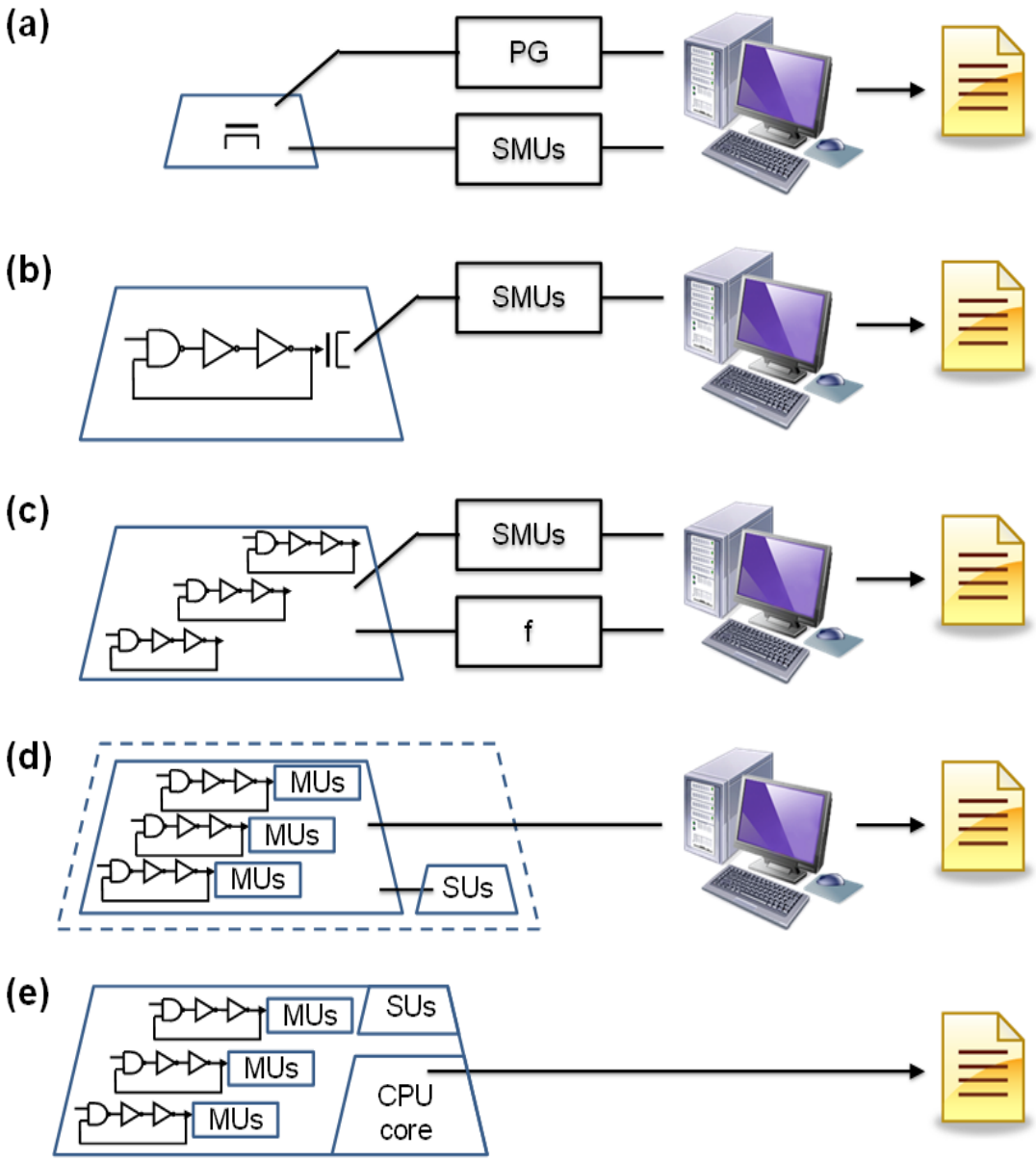


Figure 4. Evolution of technology reliability evaluation.[1]

[1] Legend: (a) Measurement of a single device under test with external instrumentation. (b) Signal generation on chip, measured with external instrumentation. (c) On-chip time-dependent variability measured with multiple on-chip circuits. (d) On-chip circuits and measurement instrumentation generated ad-hoc in advanced FPGAs, described in this work. (e) Near future: employing integrated processors for data analysis.

Note: This figure was created in cooperation with imec (B. Kaczer)

1.2 Structure of the Thesis

This document has about 190 pages in total and it is organized into 7 comprehensive chapters as follows:

- ***Chapter 1 - Introduction*** - describes the motivation behind the work efforts together with the goals. There is also *Problem Statement subchapter* showing the problem statement, contribution and structure of this thesis, as well as a large list of the main contributions of this thesis.
- ***Chapter 2 State-of-the-art and Theoretical Framework*** – tries to make and overview of the area discussed further and describes the actual level of knowledge related to the problem stated in this document. It also describes the details of the methodology and related theories.
- ***Chapter 3 – Description of the New Method*** introduces the new method and describes its details.
- ***Chapter 4 – Experiment and results*** - presents a number of experiments, performed measurements and their results.
- ***Chapter 5 - Delay-Fault Run-Time XOR-less Aging Detection Unit Using BRAM in modern FPGAs*** – introduces my second and completely new method, it describes a completely new solution which can be combined with the new method in order to analyse complex systems with much lower overhead.
- ***Chapter 6 - Integration of the Solutions in Complex Systems*** – deals with implementation of the methodology and the solution in selected modern systems.
- ***Chapter 7 - Conclusions*** makes an overview of this document, presented results, the contribution of the work itself, and it also deals with the future steps and possible further research work.
- References, Appendixes, Glossary and Index.

1.3 Problem Statement

This chapter contains a concise description of the main issues that need to be addressed before anyone try to solve the problem. Here is list of the problems that the following my research should address:

- The measurement and evaluation processes used in microelectronics and also on modern chips and ASIC devices are very expensive. Most of the reliability-related issues and methods require extremely cost- and time-intensive equipment and approach. Is possible to perform at least some tasks a bit cheaper and also faster and using public, generally available tools?

- There is absolutely no any publication that discuss or deals with such a way of utilization of BRAMs for measurements in the chips and also using such data and results for evaluation of the device reliability parameters in order to analyse the actual platform, its actual state and estimate the system dependability.

- Is possible to create and evaluate multiple programmable test structures, including the measurement blocks, directly on a Field-Programmable Gate Array (FPGA) chip?

- Can BRAMs sustain the testability of chips (also very important topic discussed today)?

- Is possible to perform a reliability assessment using Lab-On-Chip methodology and with BRAMs?

How the new materials can impact it and what could be the evolution of the discussed areas?

1.4 Contributions of the Thesis

This thesis has to be a significant contribution to the area of modern measurement methods and it tries to introduce, map and analyse a completely new area of research. It introduces many completely new methods, ideas, ways of implementation and also important results, not generally available before. The work is focused on SRAM-type or rewritable configuration cell based FPGAs, however many of the ideas and method are applicable to many other systems and technologies.

The following new information is to be introduced by my work and in this document:

- a new method and implementation of measurement of basic parameters of internal structures using BRAM and modified ring oscillator circuits,
- a new differential method for aging measurement purposes using BRAM,
- many new results from measurements of sub-micrometre, deep sub-micrometre and emerging very deep sub-micrometre technologies, especially 45nm, 40 nm and 28 nm FPGAs and technologies,
- technology bottlenecks and important facts observed during set up or during measurements and experiments under extreme conditions,
- an unusual comparison of modern technologies
- a number of new previously unpublished information and ideas.

Chapter 2

„If anything can go wrong, it will.“ – Murphy

2 State-of-the-art and Theoretical Framework

This chapter contains a minimal overview of the actual state-of-the-art as well as the required theoretical grounds and it also creates a basic vehicle to be used for further understanding presentation of the new method and all the methodology. I tried to select the main or key areas of research or information that may be required for a basic understanding of the background and inhere parts and core as well as outputs and application of results of my developed methodology.

The rapidly growing world of FPGA devices offers important as well as interesting platforms for analyses of process scaling. It also creates new study opportunities in process variations and degradation effects. Changes in parameters of FPGAs in time or under either power supply voltage or temperature variations result in timing variations or delays and may affect the final design quality and dependability. Such timing variations may result in delay faults, up to the final device or equipment malfunction or failure. Today, many dependable systems are based on programmable devices. Designs with programmable structures, such as FPGA devices, must be carefully simulated and tested during the design phase. This area is well-covered by many papers and publications and is being investigated again with the new processes and key technology nodes coming out every approximately 2 years.

Very interesting work and source is [*12*], where the authors published their wide work, which is close area to mine. There are also many other publications of this team from London available ([*13*], [*14*], [*15*], [*16*], etc.) , representing probably one of the top works in this area close to mine and also time. At that time (year 2011), I have developed similar solutions completely independently, my solutions use different circuits and I have been focused on new technologies. However it is nice to see similar independent approach, also validated by this as well as few other research teams.

The reliability of semiconductor devices and integrated circuits gets much more visible since 1960s, starting from works like [*17*] or [*18*] and [*19*], up to one of the latest papers [*20*] from the last year 2014. A great overview of the Design Tools for Reliability Analysis can be found in [*21*]. Ring Oscillator Reliability Model to Hardware Correlation in 45 nm SOI [*22*].

2.1 Dependability

Dependability is a measure of a system's availability, reliability, and its maintainability, standardized by a set of TC56 standards (IEC60050-191/2: Vocabulary, and so forth). It is also possible to find the following four dimensions of dependability - availability, reliability, safety and security. Dependability, or reliability, describes the ability of a system or component to function under stated conditions for a specified period of time. In order to achieve dependability, one need to avoid mistakes, defects, detect and remove errors and limit damage caused by a system or equipment failure. Hence, dependability has a very wide meaning and it is not necessarily a functional requirement. Dependability is also the most important system property for critical systems, where the costs of effects of the system or equipment failure may be very high. It is a case for example in safety-critical systems, where a failure may result in loss of life, injury or damage to the environment. In mission-critical systems, a failure results in failure of some goal-directed activity and in loss in unique or single-try tasks (fast flights, spacecraft, flights to another planets, etc.). There are also many other critical systems, like financial or business-critical systems, where a failure may result in huge economic losses (accounting systems in big banks). In today's world of information and communication, undependable systems may also cause information loss with a high consequent recovery cost. It is obvious that

dependability, and hence the reliability of all the key system components, has to be discussed and solicited in much more systems, than it could be observed years ago.

2.2 Reliability Parameters and Reliability Assessment

The reliability of a system can be defined as the ability to perform the specified function(s) under stated condition(s). Various approaches, difficulties, methods, e.g. exist. In general, mechanical Reliability Prediction is more difficult problem compared to pure electronics or software reliability.

The so-called bath-tube curve represents the typical life cycle and device reliability phases of any device, circuit, equipment or part of it. The exact waveform varies case-to-case, however all devices displays 3 basic phases, as shows in Figure 5. The reliability assessment works with the most stable and the most important part of the device lifetime – the useful time. It tries to evaluate the reliability parameters (like lambda) and to predict the length of the useful device life frame, estimate the point of end of time in the wear-out phase. It is generally considered to start at the point of the initial, post-manufacturing and post-burn-out phase, where devices are subjects to so-called initial or infant mortality.

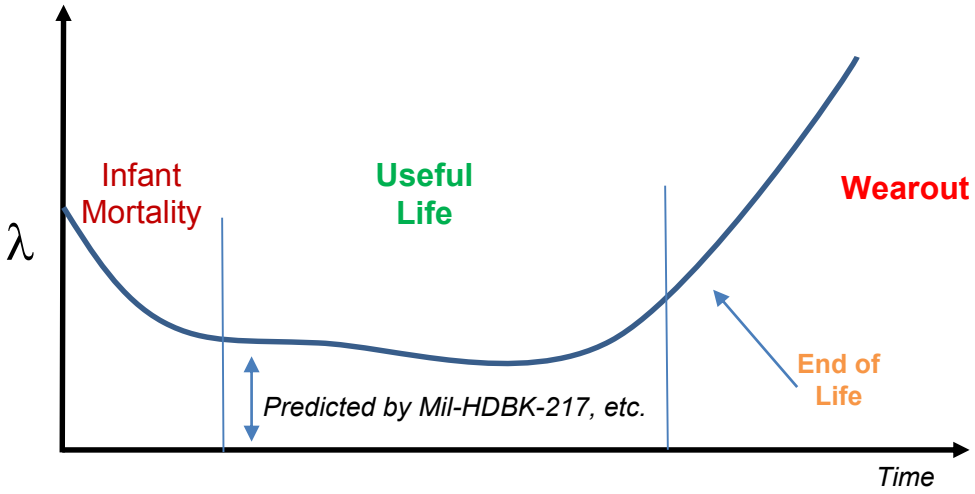


Figure 5. The Bathtub curve and typical lambda or failure rate

The following Figure 6 show how the bathtub curve changes with respect to the modern or latest technologies – the initial reliability is lower or infant mortality is higher, while the useful device life gets shorter and the failure rate during the wear out phase increases and the degradation of the device during this phase gets faster.

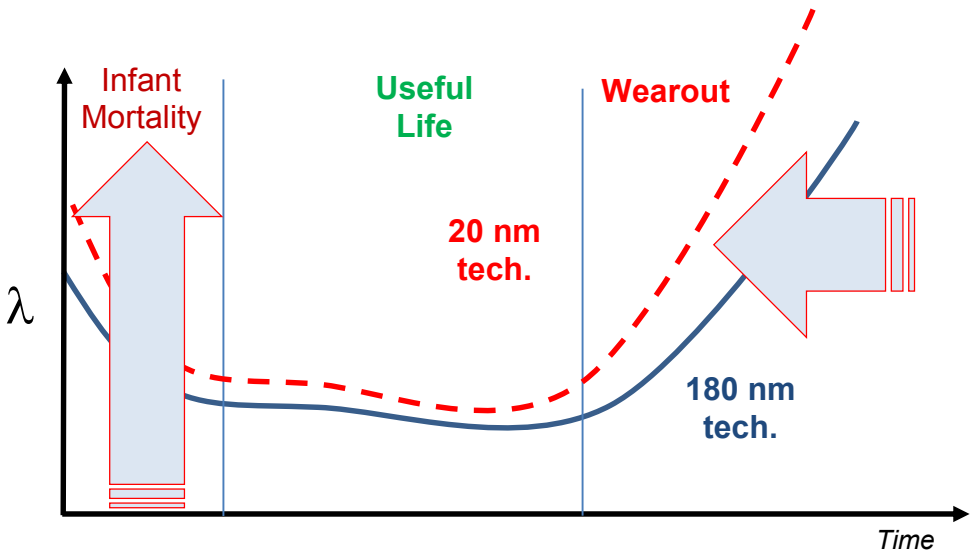


Figure 6. The Bathtub curve with respect to the new modern technologies

The objective of a reliability prediction is to determine if the equipment design will have the ability to perform its required functions for the duration of a specified mission profile under given conditions or environment. Reliability predictions are usually given in terms of fails per million hour or mean time between failures (MTBF) or failures in time (FIT).

Mean time between failures (MTBF) is the predicted elapsed time between inherent failures of a system during operation, calculated typically as the arithmetic mean (average) time between failures of a system. It is also used and valid for repairable products. Some systems are not intended to be repaired (non-repairable products, excluding production phase), hence mean time to failure (MTTF) is used in this case, which measures average time to failures with the modelling assumption that the failed system is not repaired. Hence it is very important to perform a classification of the work and repair conditions, device or component lifetime, failures, modes and repair actions.

It has direct impact to the way and evaluation of the reliability parameters and reliability assessment itself.

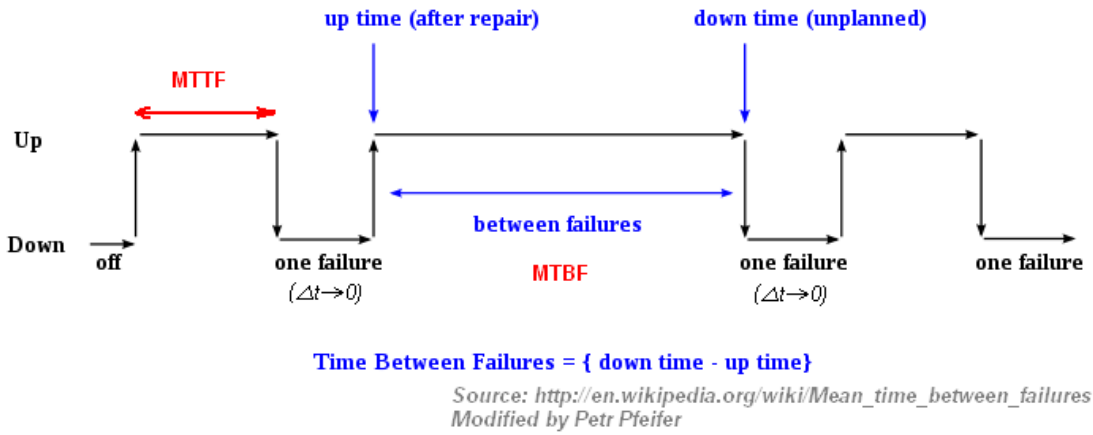


Figure 7. Mean time between failures.

A reliability block diagram (RBD), also known as a dependence diagram (DD), shows how component reliability contributes to the overall aggregated reliability parameters of a complex system. RBD is also known as a dependence diagram (DD). It is drawn as a series of blocks connected in series or parallel configurations, representing each single components of the system with a failure rate. Parallel paths are redundant causing that all paths must fail causing the complete parallel network to fail. Any failure along a series path causes the entire series path to fail.

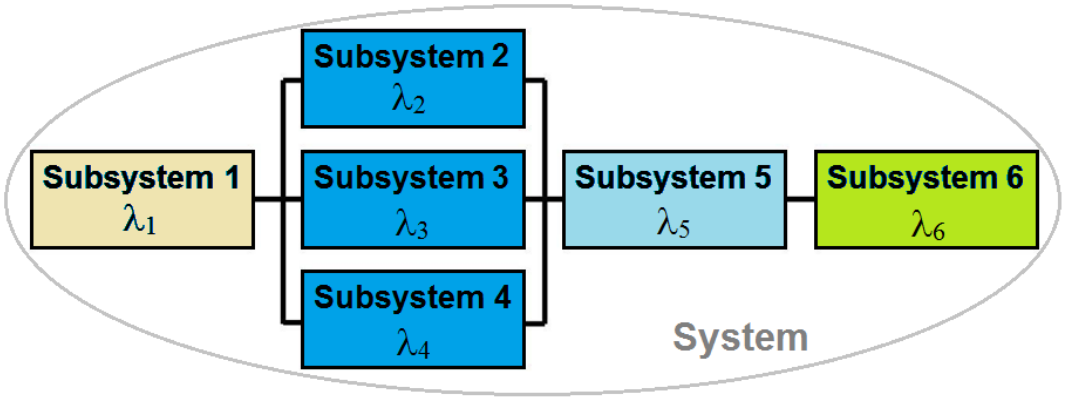


Figure 8. Reliability parameters across the complex systems – a reliability block diagram

It is important to mention that devices can influence MTBF from different start points, hence a short repair time condition can be very important one. The results are influenced by working conditions, but may be also significantly determined by experienced or applied work cycles (for nonzero repair time, etc.). Based on a given or used model, MTBF also includes reasonable repair time, however also repair can fail. Hence MTBF can be a function of the system age. Generally MTBF is a sum of MTTF + MTTR.

$$\text{Mean time between failures} = \text{MTBF} = \frac{\sum(\text{start of downtime} - \text{start of uptime})}{\text{number of failures}}. \tag{2-1}$$

And it can be calculated as

$$\text{MTBF} = \int_0^\infty t f(t)\, dt \tag{2-2}$$

The key reliability parameter lambda λ represents a failure rate. It can be expressed as

$$\lambda = \frac{1}{MTBF} \tag{2-3}$$

It can be sometimes in mentioned the base of 10^6 hours. It is typically calculated in FIT units (failure in time), where one FIT equals 1 failure per 1 billion (10^9) device hours. For example typically 5 FIT is equal to 5 fails of 1 million devices and 1000 test hours

$$\text{MTBF} = 1{,}000{,}000{,}000 \text{ x } 1/\text{FIT} \tag{2-4}$$

MTBF is to be MTTF only when all the parts fail with the same failure mode. MTTF can be counted in such simple way only when fail time of all tested devices is known.

FIT = 100 000 failures per 10^9 device-hours of operation (or 1 kpcs and 10^6 hours)

However, what is the probability that some device will be operational at time equal to the MTBF?

$$R(t) = e^{-t/MTBF}$$

$$\text{when } t = MTBF$$

$$R(t) = e^{-1} = 0.3677 \tag{2-5}$$

The probability that the device will survive to its calculated MTBF is only 37%. There is also important to consider and counting independent mechanisms - a model accounting for the end of life (wear out) failure rate.

$$R(t) = e^{-\frac{t}{MTBF}} . \prod_{i=1}^{m} (1 - F_{\lambda i}(t))$$

where:

m is number of independent wear-out mechanisms
$F_{\lambda i}$ is the time-dependant probability of failure for the i-th failure mechanism

(2-6)

Other variations of MTBF are reflecting the classification of unit malfunction, failures or task can be used:

- mean time between system aborts (MTBSA)
- mean time between critical failures (MTBCF)
- mean time between unit replacement (MTBUR)

- mean time to failure (MTTF) - in automotive area where system is replaced after a failure, since MTBF denotes time between failures in a system which is repaired.
- mean time to first failure (MTTFF)
- MTTR = Mean time to repair
- MLDT = Mean Logistics Delay Time
- For customers also interesting MTBF/(MTBF + MTTR + MLDT)
- A special case - MTBF with scheduled replacements, that can be calculated as

$$MTTF = \int_0^\infty tf(t)\,dt = \int_0^\infty R(t)\,dt$$

$$MTBR = T_r R(T_r) + \int_0^{T_r} xf(x)dx = \int_0^{T_r} R(x)dx$$

(T_r is replacement time in hours (scheduled time or in case of failure)) (2-7)

Reliability test plans are designed to achieve the specified reliability at the specified confidence level with the minimum number of test units and test time.

2.3 Reliability Prediction Methods

The reliability prediction methods can be empirical or fundamental. Empirical methods typically require large component and field data, are intended for specific application areas and hence new technologies and devices are not typically covered or not in a complete way due to limited number of statistical samples available. Al the fast improvement of processes and quality is not reflected and this fact typically results in too pessimistic estimations, especially in case of complex systems. However very large databases exist and are easily utilized by CAD/CAE systems. The failure of the components is not always due to component-intrinsic mechanisms but can be caused by

the system design. The reliability prediction models are based on industry-average values of failure rate, which are neither vendor-specific nor device-specific. It is also very hard to collect good quality field and manufacturing data, which are needed to define the adjustment factors. The advantages of empirical methods are in easy to use, and a lot of component models exist, they are relatively good performance as indicators of inherent reliability, they do provide an approximation of field failure rates.

Empirical method used today are:

- MIL-HDBK-217 – very old, basic concept is to use historical failure rate data to predict future system reliability, designed for both military and commercial areas, more parameters for specific components, includes power and voltage stresses, more types of environment, calculates MTBF, first issue 1961, last update 1995, minor changes up today, sometimes listed as cancelled, but still used by many companies today.
- Telcordia (Bellcore) TR-322/SR-332 - Designed to focus on telecommunications, more "positive" results, fewer parameters required for components, supports limited number of environments, calculates failure rate/failures in time, addresses failure rates at the infant mortality stage and at the steady-state stage with Methods I, II and III, method I is similar to the MIL-HDBK-217F parts count and part stress methods.
- IEEE 1413.x – Since 1998, this standard identifies required elements for an understandable and credible reliability prediction with information to evaluate the effective use of the prediction results. A reliability prediction generated according to this standard shall have sufficient information concerning inputs, assumptions, data sources, methodology(ies), and uncertainties so that the risk associated with using the prediction results can be considered.

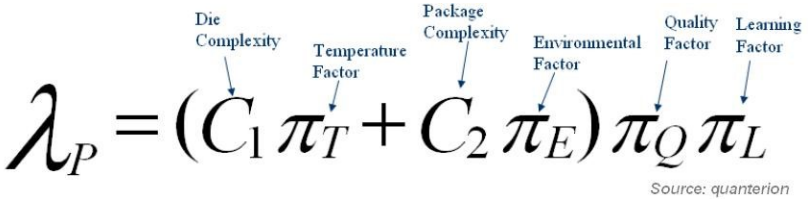
There are many other still used or cancelled standards (based mainly on the MIL-HDBK-217) like Handbook of Reliability Data for Components Used in Telecommunications Systems from British Telecom (1993), Reliability and Quality Specification Failure Rates of Components from Siemens (Standard SN 29500 /1999), Centre National D'Etudes des Telecommunications, Recueil De Donnes De Fiabilite Du CNET, (2000), Italtel

Reliability Prediction Handbook (1993), PRISM, Standard Reliability Table for Semiconductor Devices, (1986). Nippon Telegraph and Telephone Corporation, Chinese Military Standard: CHINA 299B (GJB/z 299B), and SAE Reliability Prediction Software PREL (1990) or French UTE-C 80–810 or RDF2000. There are also many other standards related to a specific issues or areas of the reliability problems, like IEEE1624, and other related for example to aerospace or defence areas. It is also very important to mention MIL-HDBK-338B standard. This Handbook provides a wide set of key information in order to understand of the concepts, principles, and methodologies covering all aspects of electronic systems reliability engineering and cost analysis as they relate to the design, acquisition, and deployment of DoD equipment/systems.

The fundamental methods are based on a physics, transistor theory and circuit analysis. It is represented by Physics-of-Failure (PoF) degradation models and can be better in faster covering of new technologies with prediction abilities. However, some complex mechanisms still are or cannot be not fully understood. Physics-of-failure is an approach that utilizes knowledge of a product's life cycle loading and failure mechanisms to perform reliability modelling, design, and assessment. It is based on the identification of potential failure modes, failure mechanisms and failure sites for the product at a particular life cycle loading conditions.

2.3.1 MIL-HDBK-217

This method and handbook is intended for use early in equipment design phases. It requires detailed knowledge of applied stresses, temperature, device complexity, etc., however some parameters are ignored (e.g. temp. cycling). Any part and environment can be described by selecting an appropriate sub parameter from a given set of tables. Then the lambda can be calculated as:



(2-8)

Then the final reliability parameter can be calculated using the following formula:

$$MTBF = \frac{1}{\lambda_{Equip}} = \frac{1}{\sum_{i=1}^{n} \lambda_i} = \frac{1}{\sum_{i=1}^{m} N_i (\pi_Q \lambda_g)_i}$$

where:

λ_{Equip} is the total equipment failure rate (typically in failures/10^6 hours - MIL-HDBK-217).
n is quantity of device used
m is quantity of different device used (generic parts)
N_i is the quantity of i-th generic part
π_Q is the quality factor for i-th generic part
λ_g is the generic failure rate for i-th generic part

(2-9)

2.3.2 FIDES

A consortium of European companies created similar methodology covering electronic components – FIDES reliability methodology. „*The FIDES methodology covers items from elementary electronic components to electronic modules or subassemblies with well-defined functions. The FIDES coverage of component families is not fully exhaustive. However, it is sufficient to allow a representative assessment of the reliability in almost all cases. The methodology applies to COTS (for which it was originally developed) and also to specific items whose technical characteristics match those described in this guide. The COTS (Commercial Off-The-Shelf) acronym designates all catalog-bought items, available on the domestic or foreign market, with a supplier P/N, and for which the customer has no input on the definition or production. This item may be modified, its production or maintenance stopped with no possible opposition from the customer. There may be only one or several suppliers for each item*." *Source: FIDES*

2.4 Making Reliability Assessments and MTBF/MTTF prediction report

When making the reliability assessments, MTBF or MTTF prediction reports, first the environment specification/ category must be available and also conditions determining environmental factors, used methods and standards. Then manufacturing part numbers, reference codes or numbers, quantity, functional part and total block failure rate, calculated and expected temperature rise and available or applicable stress factors (%) must be obtained and calculated. A reliability function plot is typically used, representing and estimating the probability of survival. MTBF is evaluated with respect to temperature or other important factors or modes. An addendum typically contains also manufacturer's reliability data and reports.

2.5 Issues Inherent to CMOS Design

Integrated circuits are made from semiconductor materials such as silicon and insulating materials such as silicon dioxide. There are many passive and active components created by various technologies and creating the desired function of the integrated circuit. Complementary metal–oxide–semiconductor (CMOS) is one of the most widely used technologies in integrated circuits. CMOS uses complementary and symmetrical pairs of p-type and n-type metal oxide semiconductor field effect transistors (MOSFETs) for logic functions. It has very good noise immunity and low static power consumption.

Figure 9 shows the main issues inherent to CMOS design[2]. There are many other issues related to the testing, packaging and other upper deign level layers, like antenna effects causing corruption of structures during plasma etching process, ESD, etc. Most of such issues can be neglected in case of proper design and manufacturing or storage and assembly phases during the device development, manufacturing and all the life time. In

[2] The figure is based on the work of Edward Wyrwas – Physics-of-Failure Approach to Integrated Circuit Reliability, DfR Solutions

special cases (equipment with long wire connection in harsh environment), also ESD should be taken into account.

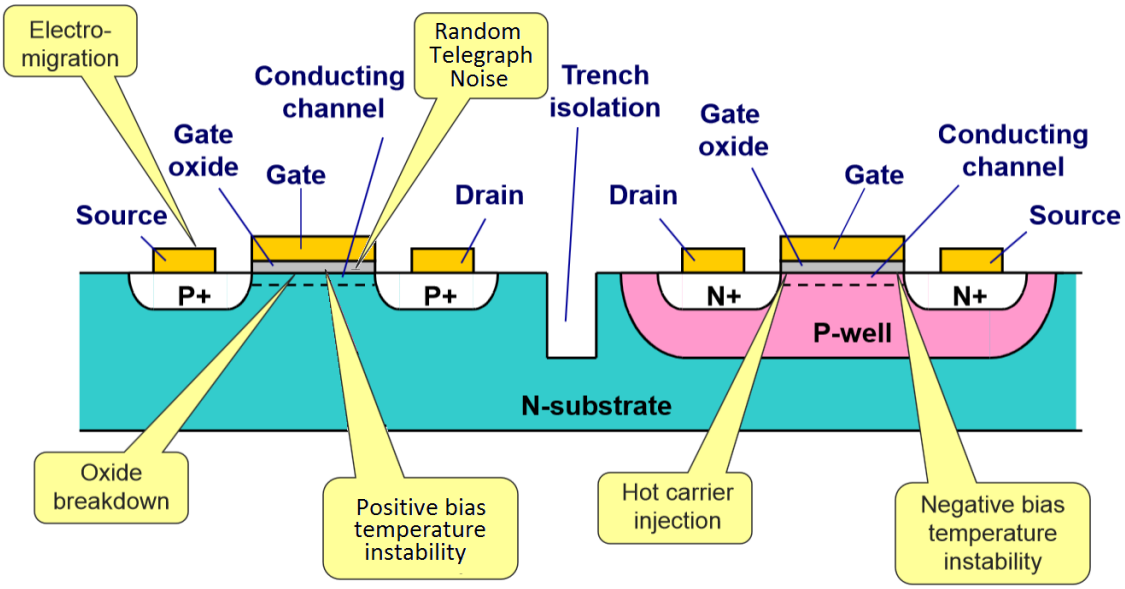


Figure 9. Issues inherent to CMOS design

Most of the strong phenomena cause damage to insulators, weakening of the insulator structures and leading to accelerated breakdown and/or increased leakage, increasing leakage currents in general or in reverse biased state. On the opposite side, a damage to wires and junctions results in increasing resistance, increasing resistance in forward biased state of switches, etc. Increased resistance may result for example in increased rate of electromigration, even above the limit model cases used during the design phases.

In modern consumer electronic devices, integrated circuits rarely fail due to electromigration effects due to proper semiconductor design practices incorporate the effects of electromigration into the IC's layout. But some exceptions and weak design or series of integrated circuits may occur. Nearly all IC design companies use automated EDA tools to check and correct electromigration problems at many levels, hence when integrated circuits are operated within the manufacturer's specified temperature and voltage range, a properly designed IC device is more likely to fail from other causes, like environmental ones, etc. However, this phenomena may be more visible in active power

parts of the design, high-power and high-performance systems. Also in the case of wrong designs of the power supply units or design or power distribution and power management circuits in general, the manufacturer's recommended conditions may be violated, not necessarily causing any immediate change in the equipment functionality, but manifesting itself after unexpected time or number of accumulation cycles.

NBTI (Negative bias temperature instability) is a key reliability issue in MOSFETs, affecting the gate-channel interface and manifesting itself as an increase in the absolute threshold voltage (even under higher temperature) and consequent decrease in drain current and transconductance of a PMOS field-effect transistor structures. There is nitrogen incorporated into the silicon gate oxide to reduce the gate leakage current density and prevent boron penetration, or alternatives in modern high-*k* metal gate stacks and new materials like hafnium oxides, etc. Also water and many solutions are used during the long and very complex sophisticated manufacturing processes. Obviously, the electric field between the gate and the channel cause creation of interface traps and oxide charge, or migration of sub particles as breaking of SiH bonds at the SiO_2/Si substrate interface by a combination of higher electric field, holes, under temperature, above a certain level of activation energy and over longer time intervals. Hence, NBTI is caused at PMOS transistor structures by long zero/L signal levels at the gate. Therefore the duty cycle (DC) value close to 0 indicates increased probability of NBTI effect at the given signal path. Scaling the technology down, similar effect is also observed in NMOS transistor structures (Positive BTI – PBTI). BTI-inducted delays and timing variations may result in delay faults, propagating up to the device or equipment malfunction or failure, especially in deep-submicrometer devices and nano-scale technologies. The details of how BTI occurs in modern technologies are still not entirely clear, however.

Hot carrier injection (HCI) is a phenomenon where one or more of the charge carriers, an electron or a "hole", gains sufficient kinetic energy in the channel to overcome a potential barrier necessary to break an interface state. The charge carriers can become trapped in the gate dielectric of a PMOS or NMOS transistor and the switching characteristics of the transistor can be permanently changed, causing especially the threshold voltage shift.

Random telegraph noise (RTN) is also one of main raising issues and causes of image degradation in complementary metal-oxide semiconductor (CMOS) devices. It is caused mainly by current fluctuation originating in charge trapping and de-trapping at the gate insulator of transistors. Most of conventional device simulators still cannot reproduce the dynamic behaviour of charge trapping and de-trapping at a gate insulator, it is difficult to reduce the effect of the random telegraph noise efficiently. The aspects of Random Telegraph Noise (RTN) can be found in [*23*], [*24*] or [*25*].

Besides the phenomena mentioned above, there are other issues that are typically common to wider set of technologies and structures. For example, time-dependent dielectric breakdown (or sometimes referred as gate oxide breakdown) (TDDB) is a failure mechanism in field-effect transistor structures, when the gate oxide breaks down as a result of long-time application of even relatively low electric field by formation of a conducting path through the gate oxide to substrate due to electron tunnelling current. It is especially when MOSFET structures are operated close to or beyond their specified operating voltages.

There are also other many effects, for example, electrostatic discharge (ESD) is a phenomenon caused by a sudden and typically momentary electric current that flows between two objects at very different electrical potentials. Such unwanted currents may cause damage to electronic equipment, including integrated circuits. Strong ESD as well as strong electric fields typically cause a damage (immediate breakdown , direct or hidden) to an integrated circuit. However, like in case of other degradation processes, ESD can even cause a parametric performance failure, when the device still operates, but its parameters are shifted. ESD can also cause latent failures. The failure may manifest in stress testing or under exceptional conditions. ESD is observed as near completely solved issue today, but the key problem of the hidden ESD issues remain the main issue affecting the final device reliability and equipment dependability in special cases. ESD can also cause latent failures. Another cause of ESD damage is through electrostatic induction. Hidden ESD events and work in harsh environments may be cumulated in the structures and affect the final reliability of the devices or equipment.

In the past years, there were also many issues related to power dissipation (eliminated by proper IC design and packaging), material purity and isotope type or selection issues (emphasizing single-event transition and upset problems especially in 1990's), metastability issues, latch-up (eliminated by actually standard I/O circuits, eliminated on low V_{dd} technologies and in fact not present on SOI –Silicon-On-Insulator technologies, etc.), antenna effects causing corruption of structures during plasma etching process, etc. seems to be solved for now in very sufficient ways and at many levels. However, the following trends and reliability considerations must be taken into account, reduction of gate oxide thicknesses, reduction of interconnect dimensions, while increasing total wire lengths and number of connections, increasing power densities especially in high-end high-performance devices resulting in thermal issues and higher device operating temperatures, hot-spots, increasing sensitivity to process variations and increase of variations itself, and many new materials introduced or required, while sometimes replacing the old proven ones.

Models for the simultaneous degradation behaviour of multiple failure mechanisms on integrated circuit devices and widely accepted degradation models are available for example from NASA, JPL, University of Maryland, others. Software design tools and large software packs for design of integrated devices and circuits do incorporate them as well. All chip manufacturers do create their own exact models and wide databases, fed by large amount of data available from the production lines, test lines and feedback from the field or customers in general.

I have performed a wide literature search in the area of papers, publications and other especially IEEE research papers with respect to the keywords reliability and FPGAs. The following figures show all the very interesting evolution of the number of publications with the keywords "Aging sensor" and "CMOS NBTI" as listed by the IEEE Xplore database of conference papers and journal articles starting from the year 1980 up to year 2013.

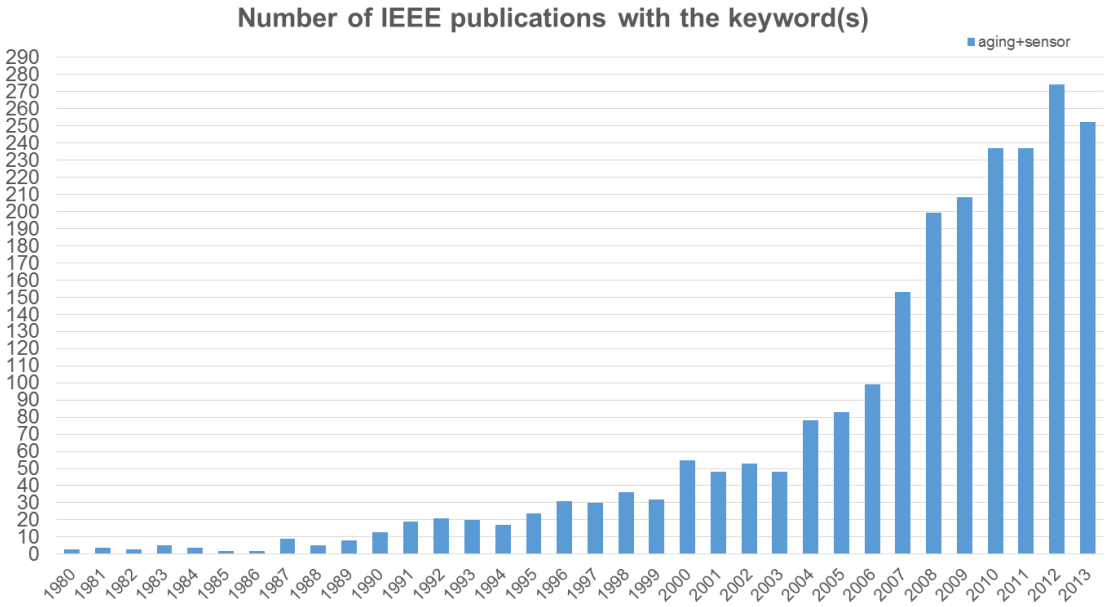


Figure 10. Evolution of the number of publications with keywords "Aging sensor" as listed by IEEE Xplore

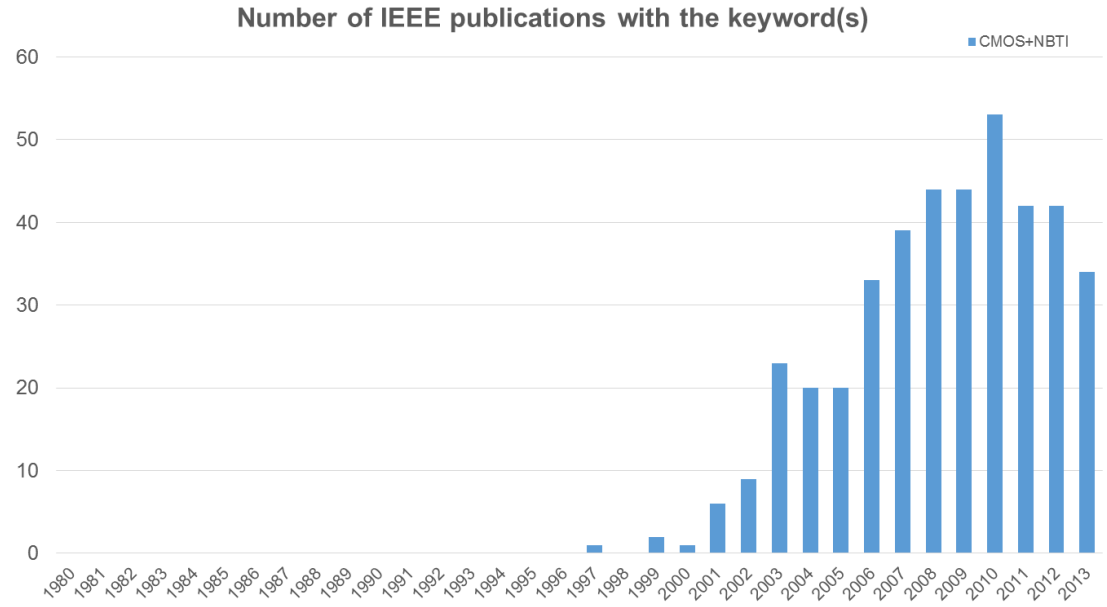


Figure 11. Evolution of the number of publications with keywords "CMOS NBTI" as listed by IEEE Xplore

2.6 Electromigration

Electromigration is a phenomenon occurring when some of the momentum of a moving electron is transferred to a nearby atom or activated ion, causing the ion to move from its original position. There are two basic forces affecting ionized atoms in a conductor: the direct electrostatic force as a result from the electric field (therefore having the same direction), and the force from the exchange of momentum with other charge carriers (toward the flow of charge carriers), caused by a so-called "electron wind" or "Ion wind".

During the 1960s James R. Black developed and published (in journal on IEEE Transactions on Electron Devices [*26*] in year 1969, however mentioned already in 1967 in [*27*] at page 150, etc.) an empirical model to estimate the MTTF (mean time to failure, in his paper only MTF) of a wire. It takes electromigration into consideration and since then, the following his famous formula has gained popularity in the semiconductor industry:

$$\frac{1}{MTF} = A\, J^2\, e^{-\frac{\phi}{kT}} \tag{2-10}$$

where

MTF is median time to failure in hours,

A is a constant which contains a factor involving the cross-sectional area of the conducting film,

J is the current density in amperes per square centimeter,

ϕ is an activation energy in electron volts,

k is Boltzman's constant, and

T is film temperature in degrees Kelvin.

Today is generally used form of the formula is:

$$MTTF = A J^{-n} e^{\left(\frac{Q}{kT}\right)} \tag{2-11}$$

His theory and formulas were also elaborated in his other paper, starting from [*28*].

The area of reliability is very complex in electronics and much complex in other areas, for example in mechanical components [*29*]. The term Reliability *R(t)* can be understood as the probability of a system to perform desired functions until or along a given time *t*. The failure rate λ expresses the probability that a system fails in a given time interval. The probabilistic expressions of reliability and failure rate is the Mean Time To Failure (MTTF), which is the average time that a system runs until it fails and it is equal to the expected lifetime, expressed as the inverse of the constant failure rate λ as follows:

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda} \tag{2-12}$$

Other information can be found in many sources, for example [*30*], [*31*], [*32*] or [*33*].

2.7 Bias Temperature Instability

The effects of NBTI has already been reported in 1960's ([*34*]) and the charge trapping in the oxide was considered an important aspect of this type of degradation. The details of how BTI occurs in modern technologies are still not entirely clear and there are more models available today. The exact parameters are often strictly linked to the manufacturing technologies. The most widely used is the reaction- diffusion model. The level of aging due to this phenomena is typically related to the power supply voltage, temperature and an input signal probability, which is defined as the probability that input signal is at logic 0 for NBTI in PMOS transistors.

A reaction- diffusion (R-D) model is often used for the simulation of NBTI degradation. This model has been accurately reproducing old experimental NBTI data, but there is a low accuracy observed in the case of modern technologies. This model states that the build-up of interface traps arises from dissociation of hydrogen governed by an electrochemical reaction between inversion layer holes and Si-H bonds. During the stress phase, the released hydrogen diffuses away into the oxide from the silicon-oxide interface. It can also react with the dangling silicon bond. In the relaxation phase, when the transistor is switched off, an annealing process recovers the transistor original parameters by returning the diffused released hydrogen back to the interface region. In the first few seconds (generally a short time after begin of application the stress conditions) the trap generation is controlled by reaction process, while the long-time stress and generation is governed by the diffusion process. The stress-induced leakage currents generally depend on the oxide thickness, temperature and gate voltage. The generation of bulk traps caused by injection of hot holes into the oxide shows typically a much stronger voltage dependence than the generation of the interface trap, especially under low or medium gate voltages. The degradation process depend on the gate voltage in a non-linear manner, while this way of dependence stays much more visible under higher stress voltage. In case of the frequency dependence, very limited number of information can be found in literature, sometimes also with contrary statements. The general reaction-diffusion model predicts no frequency dependence of the NBTI

degradation, expecting only the effect of the duty cycle of the gate signal. The measurements often show very low degradation for higher frequencies and short stress times. Long-time stress may emphasize the NBTI degradation also for higher frequencies. The exact range of frequencies is generally not very clear and it strongly depends on many conditions including the technology. In addition, NBTI simulations in the range of years and high-frequency operations are not accurate and also feasible due to insufficiently very small time resolution required in such a case.

A Tsetseris' model has investigated the subject of BTI at atomic level and the team of authors did propose a proton based dissociation model in [*35*] in order to better to describe the BTI induced breaking of Si-H bonds at the silicon-dielectric interface. But when using this model for standard bulk processes, the time exponents may result in unrealistic values, so some papers reported an idea, that the model in the form present in the papers might be still incomplete.

An advanced temporal charge trap models of Grassers's team ([*36*], [*37*], [*38*], [*39*], [*39*], etc.) based on switching oxide traps are now able to explain the bulk of the experimental data and seem to be very close to the real mechanism, numbers and physics.

It is obvious that two square waveforms with different time periods can have the same duty cycle (50%). Hence not only duty cycle, but also the frequency can play the role. In addition, there could be more modes or power states of the aged devices:

- The devices is disconnected and unpowered, here the general assumption says that BTI is negligible, but some re-combination processes due to higher storage temperature may occur.
- The devices is in power-down or standby-mode, experiencing so called static BTI, when the transistors are under constant voltage stress for longer time.
- The devices is under a given operational mode, experiencing so called dynamic BTI, it means that both stress and recovery phases exist due to the changing signal.

The atomic hydrogen in the bulk diffuses typically faster than the molecular hydrogen in the dielectric. The interface traps which are generated during the on-state are partially annealed in the off-state under dynamic operation of the transistor. Therefore the AC degradation is significantly lower than the DC degradation for any given stress time. The

magnitude of the BTI driven parameter shift over time is significantly reduced for higher frequencies or smaller duty cycle ratio [*40*] , [*41*], [*42*].

2.8 Single-event Transients and Single-event Upsets

Single-event transients (in a logic part) and single-event upsets (cased in memory elements or flip-flops) were and still are important factors that has to be taken into account in modern dependable systems or systems with increased reliability requirements. It is still possible, that a particle (even present in the packaging materials, as a product of various decay processes, or coming outside the chip and package itself), can cause internal temporary or permanent changes in the material, structures or at least circuits functionality. There were new designs developed and also successfully introduced in integrated devices. Some of them remain successful on the market, but many of the promising and widely published technologies were stopped or have never been introduced in mass production of integrated circuits. For example very popular Dual Interlocking storage CEll (DICE) used for years to protect memory cells are no longer efficient with cell compaction on today's technologies. Many others as well as the results of Xilinx Rosetta program [*43*] show much better flip-flop error rate in modern 28 nm technologies that expected when old or even DICE projects were ported from older 65 nm, 40 nm, or 32 nm BULK processes. Obviously, the cell compaction causes less chance of being hit. On the opposite side, many sources have demonstrated the fact that charges from a single particle may more easily be shared among several cells, since it is less charge collected by individual cell in today's modern nanotechnologies. All the events doesn't appear as purely isolated ones like years before. Much better manufacturing processes, pure materials and boron isotope in the substrate and passivation layers have resulted in very good reliability parameters, increasing the immunity of modern integrated circuits to this phenomena and significantly lowering or even minimizing this effects in modern technologies.

The work presented in this document partially reflects also this area. Thanks to the usage of memory blocks and the way of implementation and interconnections, SEU events can be detected and analysed by its built-in feature.

2.9 Testing and Testability Issues

Testability, as a possibility to test all required parts of the chips either the manufacturing time or during the device lifetime, is very important aspect that has to be reflected the during development phases of any modern chip solutions. It requires a special approach in order to create an optimal trade-off between the main design complexity and design cost, and the cost and area overhead caused by new circuits added to the original design in order to enable the testability features of the system.

There are two basic types of faults in digital circuits that may occur:

- hard-type faults, that remain in the devices or equipment, some of them are recoverable after application of a special treatment or power-down/power-up phases, etc. Now, it is very well covered by technology, area or time redundancy methods, however unrecoverable part of the aging effects on modern technologies can still cause problems,

- soft-type faults – which typically appear and disappear, having duration few ps up to ns in time, but which can cause temporary changes in logic (SET) or up to permanent changes, when acquired by flip-flops during their active phases (SEU). This area is again solved by many hardening techniques.

My method enables this important area while it tries to keep the required overhead at the most minimal level. I have extended the basic model of the typical faults in integrated circuits and hence also FPGAs, as it is presented in Figure 12, to the possibility to test wide range of delay faults and also leakages or crosstalk effects, measured by digital methods and with support of standard functionally dedicated units.

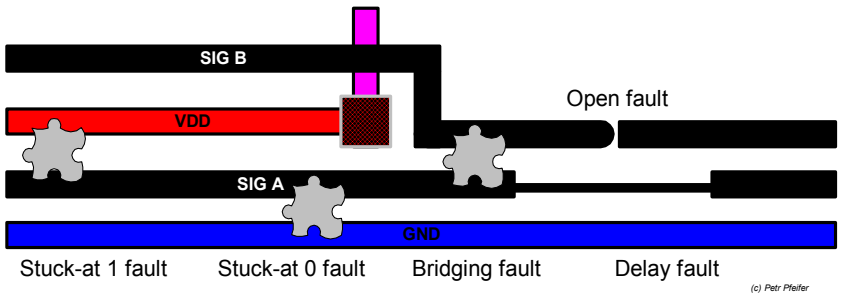


Figure 12. Typical and basic model types of permanent faults in integrated circuits.

2.10 Device Testing Procedures

The typical set of test procedures used in microelectronics and also FPGAs consists of (based on available data from IC manufacturers including Altera and Xilinx producing FPGAs):

a) Overvoltage stress test – where the device is tested under higher voltages, typically +20 % of the nominal voltage, also under higher temperatures or overheated.

b) High-Temperature Operating Life Test – where the test is conducted under the conditions of high junction temperature (over 125 °C) temperature, maximum rated power supply voltage, and either dynamic or static operation.

c) Temperature Humidity with Bias Test - this test is conducted under the conditions of 85 °C and 85% relative humidity and power supply bias. Package preconditioning is performed on the testing samples prior to this test.

d) Temperature Humidity Test – This test is conducted under the conditions of 85 °C and 85 % relative humidity. Package preconditioning is performed on the testing samples prior to this test.

e) Temperature Cycling Test - The temperature cycling test is conducted under the conditions of predefined maximum and minimum temperatures and in air-to-air environment. Package precondition is performed on the testing samples prior to the temperature cycling test.

f) Autoclave Test - The autoclave test is conducted under the conditions of 121 °C, 100% relative humidity (unbiased), and higher 200 kPa pressure. Package preconditioning is performed on the testing samples prior to the autoclave stress test.

g) High Accelerated Stress Test - This test is conducted under the conditions of temperature 110 °C or 130 °C, 85 % relative humidity and power supply bias. Package preconditioning is performed on the testing samples prior to this test.

h) Unbiased High Accelerated Stress Test – This test is conducted under the conditions of 130 °C, 85 % relative humidity or 110 °C, 85 % relative humidity. Package preconditioning is performed on the testing samples prior to this test.

i) High-Temperature Storage Life - This test is conducted under the conditions of 150 °C and with the device unbiased.

j) other stress tests, performed also under cycling,

k) other tests related to the concrete or critical part of an unique technology, etc.

l) special material tests or required sample tests.

2.11 FPGAs in General

FPGAs are integrated circuits, containing an array of initially uncommitted circuit elements, widely configurable logic blocks (CLBs), and interconnect resources, that can be configured at any time by the end user. The configurable logic blocks create the desired logic functions and contain also flip-flop memory elements. Figure 13 shows an example of a standard FPGA arrangement with a standard functional block set - configuration logic blocks, dedicated memory block and interconnect resources with switch matrixes, all surrounded by Input/Output blocks. Modern FPGA chips also typically contain many additional dedicated blocks, like multipliers, processor cores, and also important support and power management units (not shown in the figure). Modern programmable devices also use dedicated memory blocks (BRAM). They are designed as 8-transistor cell synchronous dual-port memories. This memory block structure is very useful for implementation of the method proposed and presented in this document, and it can be also used and directly combined with the novel XOR-less aging detection unit, introduced in [*44*] in 2012 year.

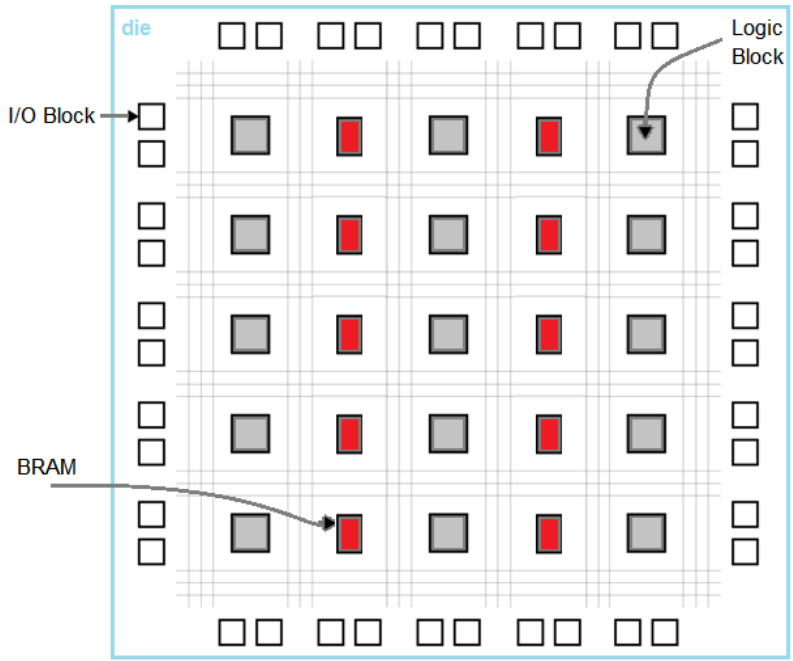


Figure 13. A standard FPGA arrangement with a standard functional block set.

Figure 14 shows the very standard basic set of basic configuration units, available in configuration logic blocks in FPGAs, and how it can be connected to the interconnect mesh, local or global interconnects and BRAM blocks are populated across the die, as shown in the previous figure. Modern programmable devices use various technologies, however the full and fast re-configurability (complete or partial change of the logic content or flip-flops or memories in the integrated circuit) at any given time or on-demand base is best provided only by SRAM–based FPGAs, where all the information about the internal functions of the integrated circuit is stored in static read-write memory cells.

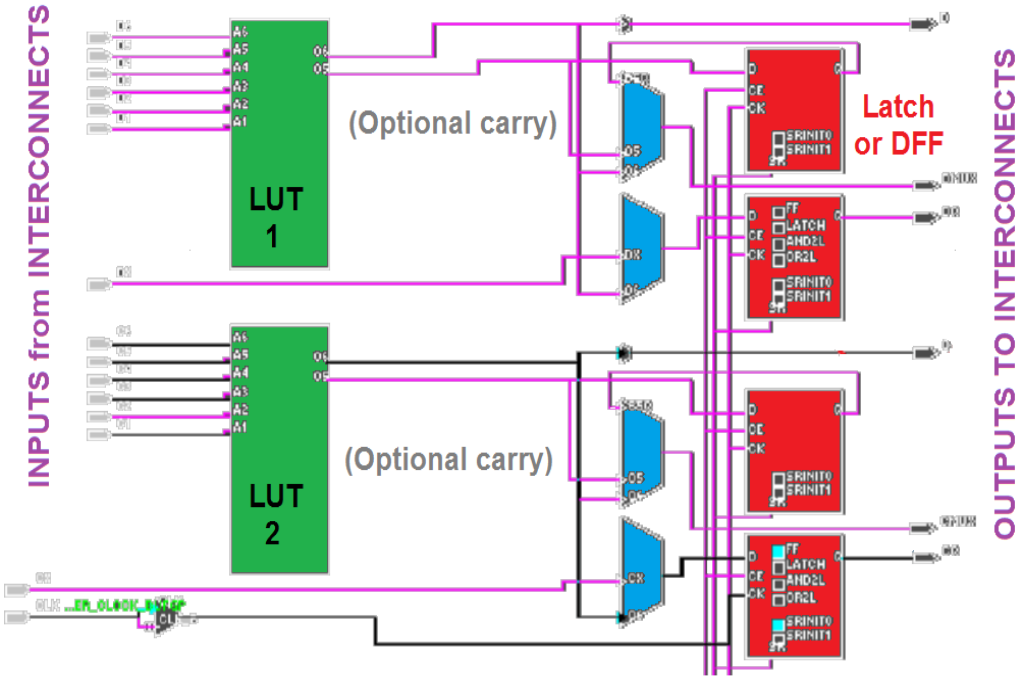


Figure 14. An example of a very standard circuit set available in configuration logic blocks.[3]

[3] Legend: - green look-up-tables (memory cells, pass-gates and inverters and/or signal shapers), blue multiplexers and red flip-flops (configured as latch or D-FF, utilizing 3 or 5 inverters and 2 or 4 pass-gates). The optional carry paths and logic with XOR gates are used for an overflow signals into the next digit of a

2.12 FPGA Technology Reliability Issues

Since the world of FPGA devices is a kind if subset of the world of ASIC, FPGAs and issues inherent to technologies used in FPGA devices are very close to the issues inherent to technologies used in pure ASIC devices. The new FPGAs can also be directly taken as a specialized ASIC designs, which are similar ones across many technologies in the main point of view, however sometimes strongly adjusted for new technologies. There are many publications dealing with designs and FPGA, however the number of publications strictly related to FPGAs is very limited. I did try to summarize or draw one the best figures illustrating this area, but I have found a great work [*45*] of Dr. Douglas Sheldon from the Jet Propulsion Laboratory, California Institute of Technology, using also the key figure from the Stanford University[4] and hence the following figure has been, exceptionally, taken from this source. I think that is really difficult to find any better figure illustrating exactly the discussed area of research.

multi-digit addition, or speed-up and implementation of efficient parallelism in intensive computational tasks and blocks.

[4] *Source: http://stanford-online.stanford.edu/sesi04moore/docs/LowKDielectics4.pdf*

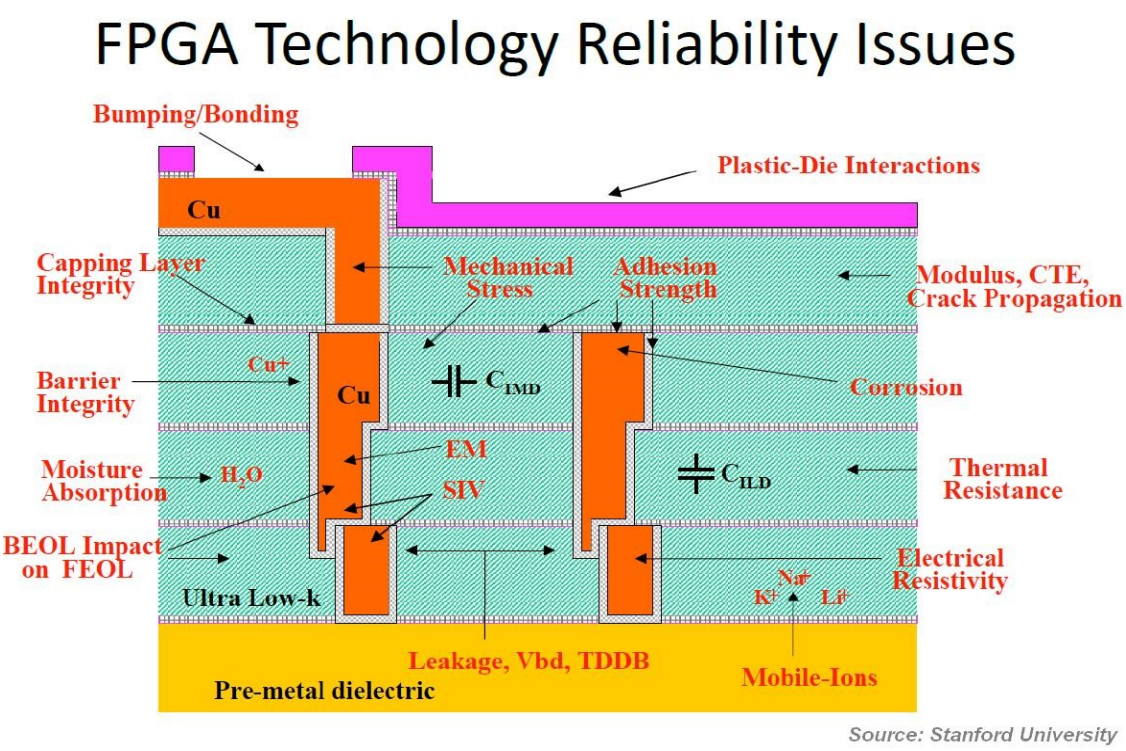


Figure 15. Physical phenomena causing lowering of reliability of the FPGA technologies

2.12.1 Reliability and FPGAs

I have performed a wide literature search in the area of papers, publications and other especially IEEE research papers with respect to the keywords reliability and FPGAs The following figures show all the very interesting evolution of the number of publications with the keywords “FPGA reliability”, and “FPGA aging” as listed by the IEEE Xplore database of conference papers and journal articles starting from the year 1980 up to year 2013. It is obvious, that the reliability of FPGAs stays very important topic and the number of the papers has clearly increasing trend. It is the same for the “FPGA aging” keyword, where the number of published papers is limited to few tens of them annually.

2.12.2 Accelerating factors

Temperature and voltage are the two basic acceleration factors, which can be applied to the integrated circuit and FPGAs in general very easily. It is obvious that the degradation

and aging processes can be accelerated by these environmental conditions and therefore detectable or measurable within typically much shorter timeframe. This works well in case of older technologies (for example the experiments performed on Cyclone III EP3C25 using 65 nm TSMC process ([*46*] and [*47*]) and results presented in [*14*]. However no similar tests and results are available for 28 nm technologies. I will presents such results from Xilinx FPGAs using 28 nm TSMC technology in the chapter 4, dedicated to my main experiments and results.

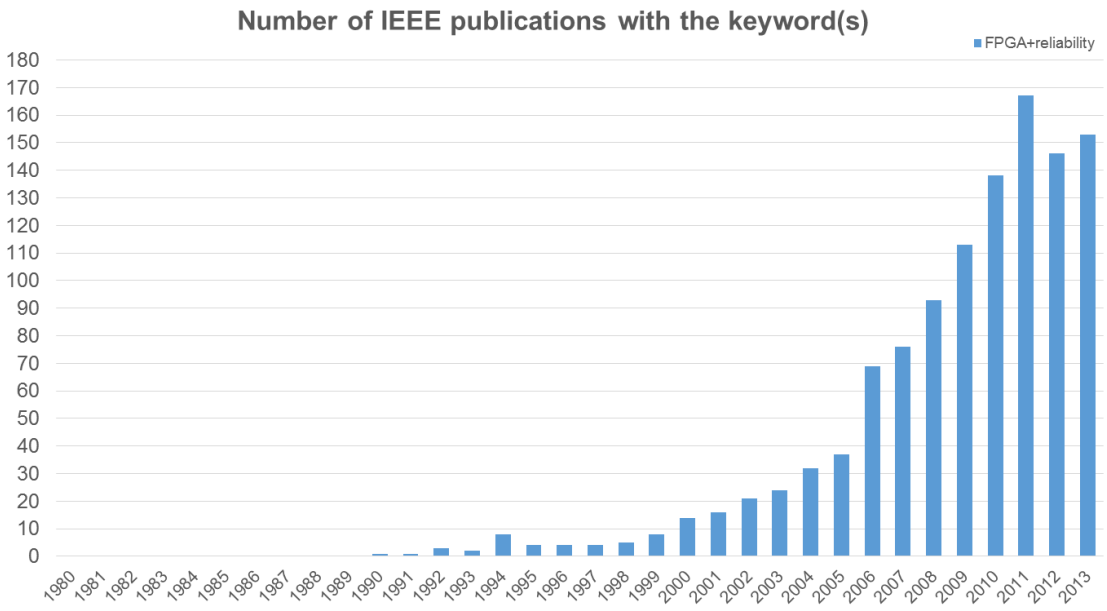


Figure 16. Evolution of the number of publications with keywords "FPGA reliability" as listed by IEEE Xplore

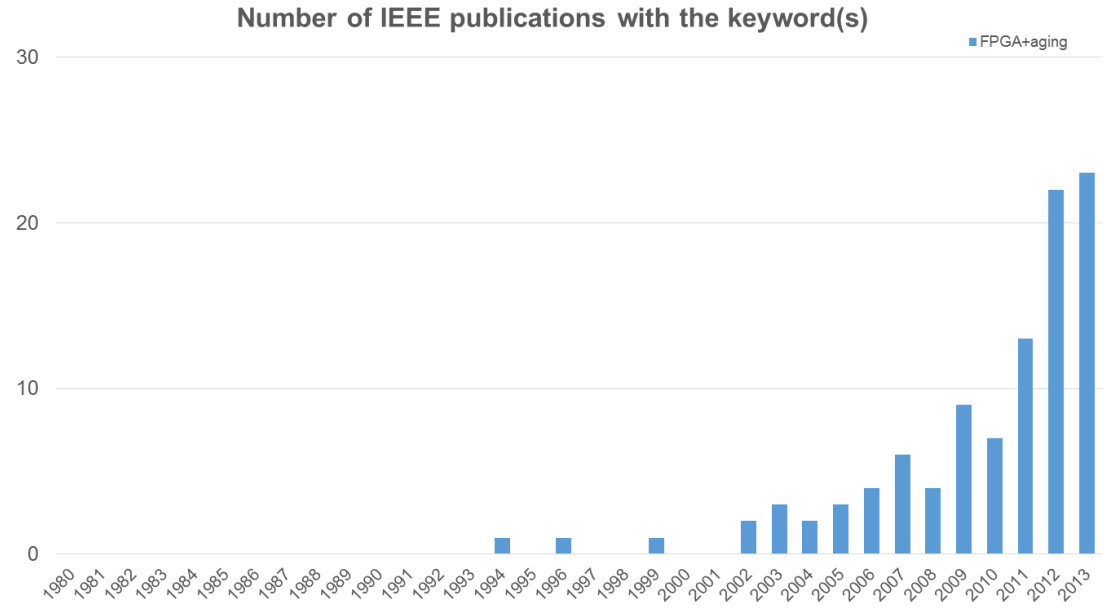


Figure 17. Evolution of the number of publications with keywords "FPGA aging" as listed by IEEE Xplore

2.13 Aging and variability in parameters

Aging (or ageing) is the typical issues being investigated today as the leading degradation process in modern nanoscale structures and devices. The information in this subchapter comes mainly from sources [*48*], [*49*], [*50*] and [*51*], including NBTI Degradation: A Problem or a Scare [*52*].

For example Asenov et al. have showed in [*53*] that the number of dopant atoms and the number of defects in each device reduces to numerable levels with the aggressive scaling of CMOS device size. This trend has significant technological implications showed e.g. in [*39*] or [*54*], when it results in increased time-zero variability, but also considerable time-dependent variability. The time-dependent variability in nanoscaled devices leads to a shift in our perception of reliability and the deterministic lifetimes measured on large area devices have to be replaced by lifetime distributions [*55*].

Product burn-in stresses are commonly performed on SRAM array to accelerate transistor failure mechanism and screen out weak SRAM cells. Li Wang et al. from IBM showed in [*56*] that PFET NBTI is the dominant factor that is responsible for the degradation of SRAM array stability, and its impact on V_{csmin} is predictable by I_{ddq} data and modelling.

Also the properties of individual charged gate oxide defects, specified also by the capture and emission times, can be directly observed and measured in deeply scaled MOSFETs [*57*], [*36*], and some related issues in [*37*], [*38*] or [*58*] and [*59*].

A research team from imec (Belgium) and T.U. Wien has published a way of reduction of the BTI time-dependent variability in nanoscale MOSFETs in [*55*]. They

show how Random Dopant Distribution (RDD) causes a non-uniform potential profile in the channel and the carrier conduction proceeds through percolation paths.

This phenomena is tightly linked to the capture and emission paths, and it could be potentially used for general methodology and models for Bias Temperature Instability, Random Telegraph Noise and other similar phenomena and degradation effects with respect to the Fermi levels.

Other related data has been published in [*60*] and also in [*61*] showing a way of detection of trap generation due to constant voltage stress in the latest generally used materials and technologies. The reliability issues are discussed for example in [*62*] or [*63*].

The aspects of usage of ring oscillators and direct measures of path delays on commercial FPGA chips are mentioned in [*64*], supported by an empirical model for accurate estimation of routing delay in FPGAs in [*65*].

2.13.1 Time-zero Variability

Time-zero variability is a variability introduced during the chip manufacturing process as an as-fabricated natural or inducted spread in given parameters. The basic chip specifications already reflect this issue and all the shifts in given parameters. However, the new technologies have introduced much wider spread of parameters and variations that have to be reflected during design and expected to be present in new modern devices.

2.13.2 Lifetime Variability

Time-dependent variability (i.e., reduced reliability) is variability directly influencing the reliability and dependability of the system and, in addition, in negative and mostly in very difficult-to-predict ways. It is based on the time-zero variability and other initial conditions, while adding or reflecting all the conditions and material or charge distribution experienced by the circuits during the devices or chip lifetime. It means that

the exact device reliability parameters strictly depend on the working conditions, like temperature, voltage, etc., absorbed by a given chip during its lifetime or mission, sometimes also including non-active phases and storage environmental conditions (various non-volatile memories, etc.). It is extremely emphasized in the latest nanoscale technologies. The reliability assessment is directly related to this issues as well. Due to the prediction difficulties, it is generally considered to be better to implement on-line and on-demand measurement and detection mechanisms, not extrapolate or estimate the reliability parameters based on initial or years-old values.

2.14 Redefinition of Critical Paths (aging-critical paths)

The original meaning of the **critical path** was defined as **the longest path**, the path with the longest delay, the longest execution and signal distribution time in a given design or its subset or circuit. Such a path typically determines the maximal working frequency of the given synchronous system - the maximum possible clock rate in the system is determined by the slowest logic path and the parameters of the clock distribution network. Introducing the matters of the wide range of negative and degradation processes, the critical path raised the need of a new term or a redefinition this original one in the way, that it has to be the path, which **can potentially stay the longest one**(s) **within a given time frame,** and/or **under given conditions**. It also is called the **aging-critical path**, especially in the case, when this path degrades in some important parameter(s) in the fastest way. It means that in a real system it may result in the fact, that a given longest path P_1 (consisting of so-called fresh gates) with the initial delay d_{P1} = 10.00 ns, evaluated by a pure static design analysis or method, having for example only 5% degradation coefficient, defined as the ratio between the path delay at the end to the begin of a given interval, can lose its original criticality over time. Performing the new system analysis within 10 years of the required working time, this path can be less critical to the overall system reliability than any other path, having the initial delay d_{P2} for example -10% of d_{P1} (it means $d_{P2} = 0.9 \cdot d_{P1}$), but manifesting 4 times stronger impact of degradation processes with 20% degradation coefficient and/or lower or no possibility of effective relaxation events resulting in aggressive degradation effects and in much longer path

delays. Hence, after the required 10 years of the system activity, the path *P1* (consisting of so-called aged gates) stays +5% longer, prolongating itself to the final delay of

$$d_{P1y10} = 10.00\text{ns} \cdot 1.05 = 10.50\text{ns}.$$

Another path *P2,* with the same importance of both the logic signals and paths, has the original delay

$$d_{P2} = d_{P1} \cdot 0.9 = 10.00\text{ns} \cdot 0.9 = 9.00\text{ns},$$

and it stays +20% longer to the final delay of

$$d_{P2y10} = d_{P2} \cdot 1.20 = 0.9 \cdot 1.2 = 10.80\text{ns}.$$

This path is actually longer of 8% to the initial delay d_{P1}, and near 3% longer to the final delay of the original critical path *P1*. This one can cause serious troubles in today's systems when some old methodologies are applied to the modern systems utilizing modern technologies with high degradation coefficients, nowadays in the very common range of tens of percent, as it is shown later also in this document.

It has to be mention here that, despite of the fact that the impact of aging and degradation processes typically result in negative numbers or elongation of delays and important parameters, the parameter or aging coefficients can be naturally real or even complex numbers in general. Hence the final impact of aging may result in even better timing in some circuits and technologies or under given circumstances, as it was already observed in for example in the area of bipolar technologies. It is also very difficult to predict the aging parameters of the future nano- or sub-nano (femto) unknown, unheralded or new emerging technologies, even the level and understanding of the inner physical phenomena still points to degradation in the key delay parameters in total most of cases.

Chapter 3

3 Description of the New Method

This document introduces details of the new method, which is really novel in many points. In any case, the core of the method is based on very old, proved and generally used analogue sampling theorems, supported by the general theory of ring oscillators and its wide usage in many areas including analyses and specifications of new processes and technologies.

3.1 The New Method in General

The ASIC test ring oscillators are typically designed as a series of transistors or any basic structures in such a way which allows oscillations in the chain and generation of desired signals. The test rings consist of *n* stages or repeated structures. It has to be noted here that the presented method is primarily based on only 1 inverter (logic gate) plus *n-1* delay stages. In other my experiments, where *n* inverters were utilized in the ring chain, the rings were too sensitive to the power conditions and generated too high noise. It is one of the biggest differences to most of designs and methods that are used or can be found in industrial or research papers.

The method utilizes BRAM (Block RAM) and undersampling within corresponding Nyquist zones, delivering relative as well as absolute data. Duty cycle can be also calculated very easily. The presented method allows both the external as well as complete in-situ data acquisition and processing. Me and my colleagues have already presented a VARP VLIW solution in [*66*] and [*67*], allowing complete, extremely easy and low-cost implementation of the method into soft-cores on many Xilinx and Altera platforms. In addition, this solution can be directly combined with the novel XOR-less aging detection unit, introduced in [*44*]. The data can be processed directly on the FPGA chip or by an

external PC (offline). The original usage of the developed solution was for the purposes of aging measurement; however the method has much wider usage.

When incorporated in some final design, the selected (measured) or critical path aging effects can be estimated based on the measurement of duty cycle of the signal. As reported many times, NBTI (Negative bias temperature instability) is caused at PMOS transistor structures by long zero/L signal levels at the gate; hence duty cycle DC in value close to 0 indicates increased probability of NBTI effect at the given channel. Scaling the technology down, similar effect is observed also in NMOS transistor structures (Positive BTI – PBTI).

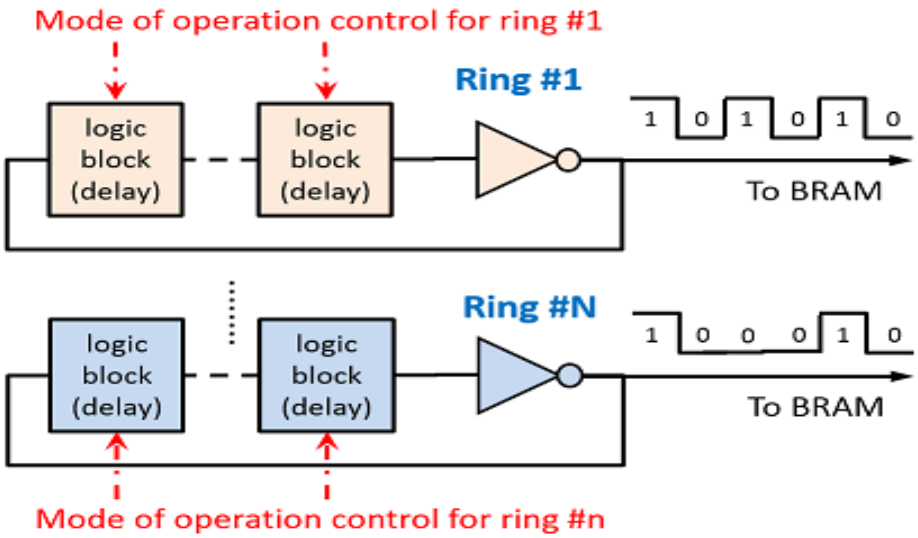


Figure 18. The first part of the basic principle of on-chip parameter measurements.[5]

The results of measurement of the SLICE or CLB parameters presented further in this document were obtained by a frequency measurement method, delivering very stable results and capable of measurement of delays with the resolution in the range of 0.1 ps (typically 100 fs, in some cases the resolution can be better, but it could be influenced by the noise level among the circuit modes). It is possible to perform the measurement without a need of any external equipment, utilizing just one precise on-board 100MHz or

[5] Available FPGA blocks are configured into multiple digital oscillators across the chip and the resulting AC data streams are sampled in the synchronous memory blocks as the way of using BRAM blocks.

200 MHz crystal or MEMS-based oscillator as the base clock frequency used in most of high-end solutions today. This value of the reference frequency was selected because of its simplicity and also it is selectable all across the main development kits and platform.

The method typically allows measurement of parameters of the FPGA basic configurable units, however also measurement of internal circuits and devices down to CMOS inverter or pass-gate levels is possible even within selected, already existing and available types of programmable integrated circuits. Special modes of operation allow reconfigurations in the number of active stages or set up the active stress voltage levels all along selected temporarily inactive ring oscillators. A *differential* method (e.g. BTI impact and reliability assessment purposes, [*68*] or [*69*]) compares on-line a path of selected ring in stressed mode 0 or 1 to another ring, typically oscillating all the time. The result sampled to memory is directly the difference between selected 2 ring oscillators. It is suppressing supply voltage and the die temperature variations much better, than in the case when the rings are compared fully separately. Advanced delay-fault detection mode [*44*] can be used. Data from dedicated units like in [*64*] can be internally utilized as well.

3.2 Design of Test Oscillators

Advanced 40 nm technology as well as the newest successful and widely used 28 nm technology is very fast, therefore most of the test ring oscillators were designed as **addressable four-stage rings.** See Figure 19 and Figure 20 with the example of the exact implementation of the rings in Xilinx FPGA. Only 35 selected rings were designed as much longer, allowing generation of frequencies below the sampling frequency *fs*. The extended version of the solution uses programmable number of stages in each ring, however the set of possible lengths of the ring and number of the CLBs in the chain must be specified during the design phase. **Each stage utilizes one LUT** and one flip-flop in the **latch** mode (single SLICE). Only **the last stage** in each ring **inverts** its input in order to create the ring oscillator. Each ring has one **enable signal** and one **special signal**, determining level 0 or 1 across the whole path **when the ring is disabled** (off). The last signal allows a change in the ring structure and can control the total length of the chain.

The output of the ring and dedicated BRAM bit or data stream will be also named a "channel" in this document.

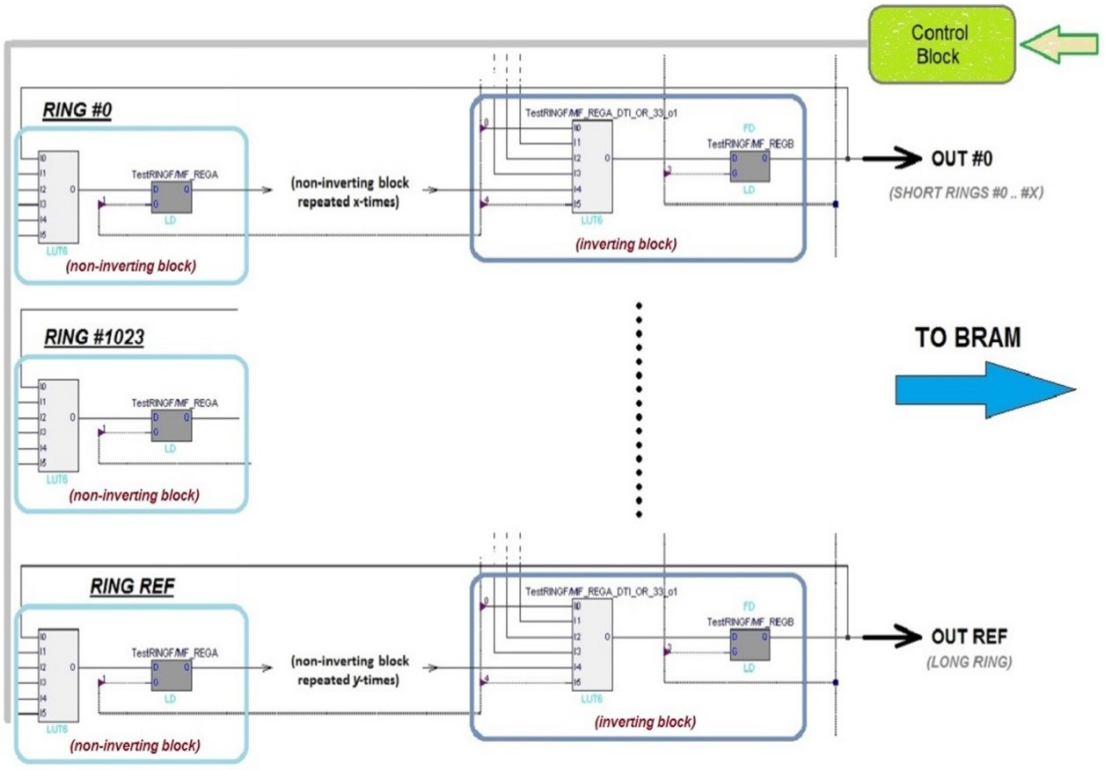


Figure 19. Implementation of test rings and control signals.

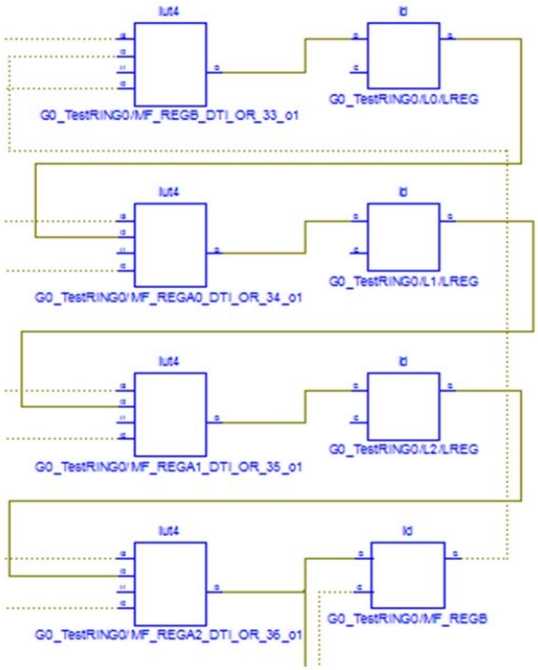


Figure 20. An example of the implemented short ring.

The last version of the test rings has also introduced a programmable length of the rings, where the new signal can change the length of the ring, allowing oscillations generated by various number of the basic logic units while maintaining same location of the measured test structures without special constraints. It enables a completely new dimension of the measurement itself as well as advanced data processing using different data and calculations on same structures, however running in different modes of operations or influencing each other in different ways.

The ring oscillators and their parameters or control signals can be programmed by a separate control chain(s) in most of cases and especially in non-reconfigurable types of FPGA or programmable devices, like Altera or Lattice FPGAs or CPLD (Complex Programmable Logic) devices using e.g. Flash cells or hybrid structures. In reconfigurable types of programmable devices (Xilinx FPGAs), all the ring oscillators and their parameters or control signals can be programmed or read back to the main unit by a special configuration streams. If properly solved at the synthesis levels, the final design will contain more oscillators to be used for the measuring purposes and also the spectrum of the measured parameters can be wider or the overall granularity can be finer.

The whole design, written in Verilog (description in [*70*]) , incorporates an array of up to 1024 addressable two-stage ring oscillators in total, each of them can be separately switched on (enabled) and off (disabled) by its dedicated enable signal. In addition, the off-state can be also fully controlled, as mentioned in the previous subchapter. This feature is used for the **study of aging effects** and change in parameters of PMOS (marked as zero/0/L) or NMOS (marked as one/1/H) state applied for long time to selected set of rings, while others (marked as X) can run for days, weeks or months. In addition, the complexity of the solution results in different final design of each single ring – some are designed utilizing local routings, some as near-by SLICEs or CLBs. In the final set of 1024 rings, subsets of selected rings were identified, based on timing or location constraints or interests, some with near same parameters, each belonging to selected group of always-running rings, or rings with temporary 0/L or 1/H state.

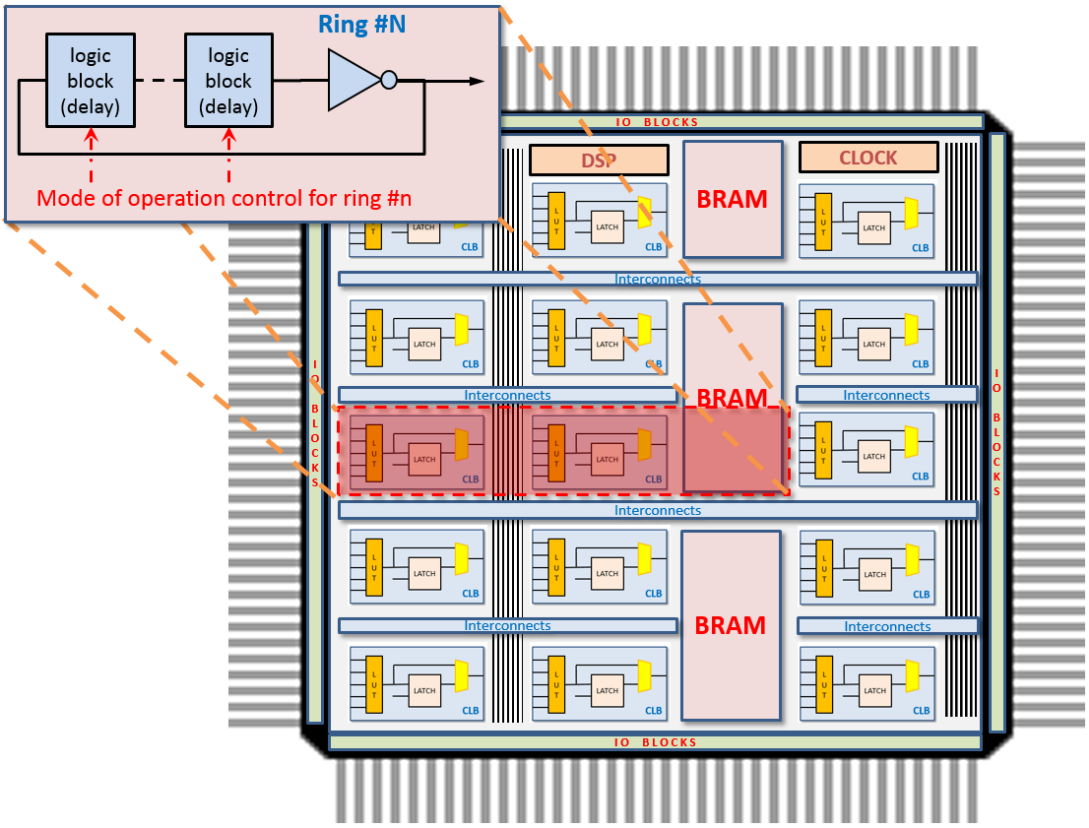


Figure 21. A general implementation in programmable technologies and the general principle in an illustrative way.

3.3 Utilization of BRAMs Becomes a Clear Advantage

The presented approach is new in its background as well as application. However, and in addition to such approach, the overall method simplicity and quality of the results is increased by utilization of Block RAM units (BRAM) in modern FPGA devices. It enables a new dimension of measurements and data acquisition. The Block RAM units implemented in modern devices incorporate true dual-port 8-transistor cells in RAM blocks. In addition, such blocks incorporate perfectly synchronized samplers as a series of D-type flip-flops (DFFs) integrated at all the data and address bit inputs, control signals and optionally at the data outputs (such output flip-flops can be bypassed, while the input ones are fixed in the BRAM functional block).

3.3.1 BRAM structure

Figure 22 shows the very typical block RAM logic diagram used in near all modern FPGA devices. It consists of a memory array, latches and input and optional output registers. This basic (single data bit) unit is implemented in 18 or 36 copies utilizing the same address, clock and mode or enable inputs, while sharing area in the same dedicated locations across the FPGA die. In some types of FPGA, the memory blocks can also be routed in a cascade mode creating a large dual-port 36 Kb block RAM with port widths of up to 72 bits. The length of memory block is configurable with respect to the number of used data bits. The extended size of data bits allows optional error check and correct (ECC) function by implementation of parity or similar memory data content checking and also correction mechanism. The memory block provides one additional data bit per each group of standard 8 data bits. The input data and registers are sampled in all modes of operations, the output register can be used or passed by the output multiplexer. Each memory access, read or write, is controlled by the clock, all inputs, data, address, clock enables, and write enables are registered. Nothing happens without a clock. During a write operation, the data output can reflect either the previously stored data, the newly written data, or can remain unchanged. A programmable FIFO logic is implemented in some FPGA families as well.

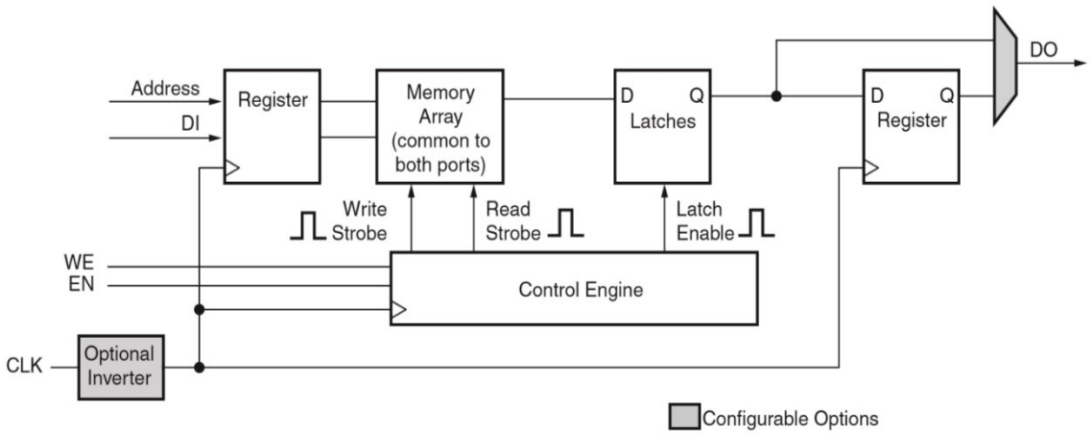


Figure 22. Virtex 6 Block RAM Logic Diagram (One Port Shown, reprinted from [71] – F1-5, and the same in [72] - F5, and the last 7 series Xilinx FPGAs in [73] and Ultrascale families in [74] – F1-5).

3.3.2 BRAM locations

The memory block are populated in high numbers all across the FPGA die. It is obvious that the number of BRAM blocks is much lower than the number of other logic components. Figure 23 shows an example of location of BRAM blocks in 40 nm Virtex 6 FPGAs as it can be seen in Xilinx FPGA editor software tool. It shows how the entire pool of configurable logic blocks (CLBs and SLICEs) is interleaved by BRAM blocks or dedicated DSP (digital signal processing, multiply and accumulate) blocks.

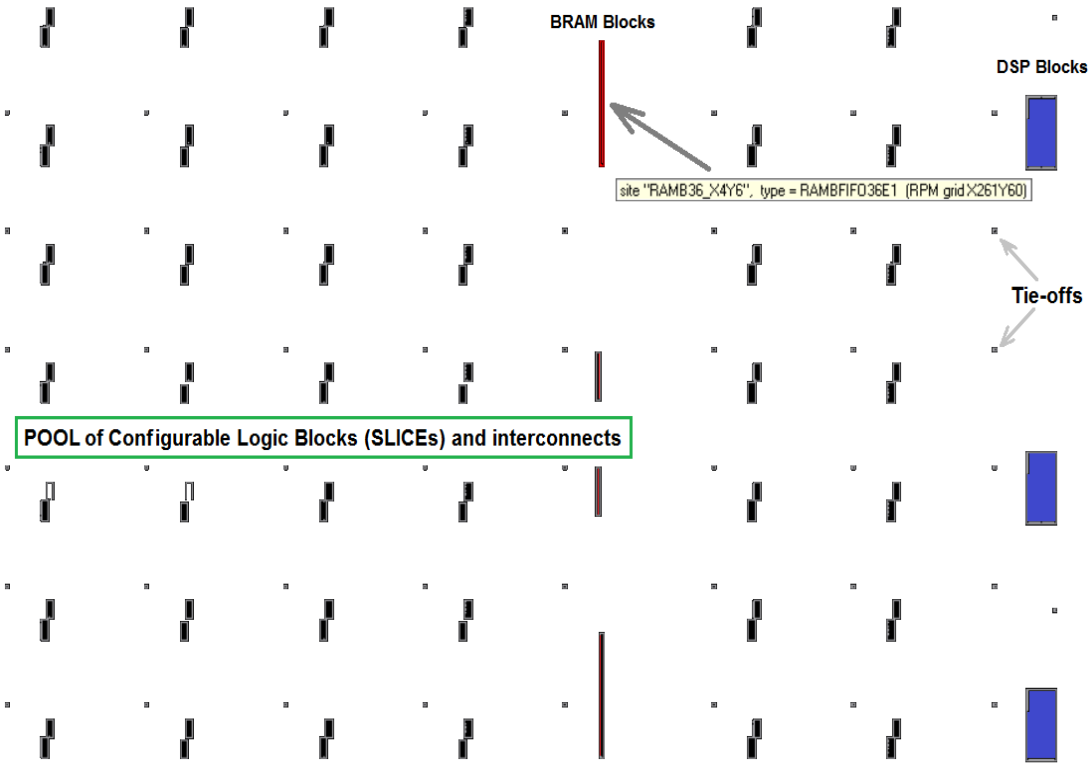


Figure 23. An example with comments of BRAM exact locations in Virtex 6 as shown by Xilinx FPGA editor software tool.

3.3.3 BRAM modes

The Block RAMs circuits can be configured in various modes. Table 1 shows supported modes of BRAM configuration on modern Xilinx FPGA platforms. These modes represent the final data and address configurations and may limit the size of the basic block or a chunk of data in the final data stream.

Table 1. Supported modes of BRAM configuration on modern FPGA platforms.

Port Data Width	*Port Address Width*	*Memory Depth (Max. BRAM cycle size)*	*Ports*	*Note*
1	15	32768	A[14:0], DIO[0]	*A half size on Spartan*
2	14	16384	A[13:0], DIO[1:0]	*A half size on Spartan*
4	13	8192	A[12:0], DIO[3:0]	*A half size on Spartan*
8+1 / 9	12	4096	A[11:0], DIO[8:0]	*A half size on Spartan*
16+2 / 18	11	2048	A[10:0], DIO[17:0]	*A half size on Spartan*
32+4 / 36	10	1024	A[9:0], DIO[35:0]	*Not supported on Spartan*
1	16	65536	A[15:0], DIO[0]	*Cascade mode using 2 BRAM units, not a single BRAM block!*

3.3.4 Changes in BRAM on FPGAs manufactured using 28 nm technology

FPGAs manufactured using 28 nm technology (TSMC) have some new features, like power gating implementation (unused blocks are completely switched off) and also the new external power supply V_{CCBRAM} is used to power the block RAM memory cells.

3.3.5 BRAM sizes

Regarding the required number of memory blocks, the number of BRAM blocks in FPGAs is typically not aligned to 2^n (it means 256, 1024, 4096 blocks) and thank to this reality and typical size of cache memories, some BRAMs stay unused in most of designs. Table 2 shows numbers and total sizes of BRAM blocks available in each modern product line and FPGA families. My measurement blocks and delay-fault detectors can use just such spare blocks. In addition, they can use only interconnect resources or minimal spare logic resources. In most of cases, my aging detectors do not affect the original design the FPGA designs updated of the aging and reliability measurement units.

Table 2. Number of available BRAM blocks present in various Xilinx FPGA families.

Family	*Technology*	*BRAM blocks (min.)*	*BRAM blocks (max.)*	*BRAM Size Total (max.)*	*Source*
Virtex 5	65 nm	36	516	18,6Mb	[*75*] DS174 (v2.0), [*76*] DS192 (v1.3)
Spartan 6	45 nm	12	268	4,8Mb	[*77*] DS160 (v2.0)
Virtex 6	40 nm	156	1064	38Mb	[*78*] DS150 (v2.4)
Artix	28 nm	50	365	13Mb	[*79*] DS180 (v1.15)
Kintex	28 nm	135	955	34Mb	[*79*] DS180 (v1.15)
Kintex Ultrascale	20 nm	540	2160	76Mb	[*80*] DS890 (v1.3), [*81*] UltraScale Architecture Product Selection Guide
Virtex 7	28 nm	795	1880	68Mb	[*79*] DS180 (v1.15)
Virtex Ultrascale	20 nm	1260	3780	136Mb	[*80*] DS890 (v1.3), [*81*] UltraScale Architecture Product Selection Guide

Figure 24 shows an overview of Table 2 in graphical illustrative format and shows also the trend, clearly indicating strongly rising the total number and capacity of BRAM blocks in modern FPGAs.

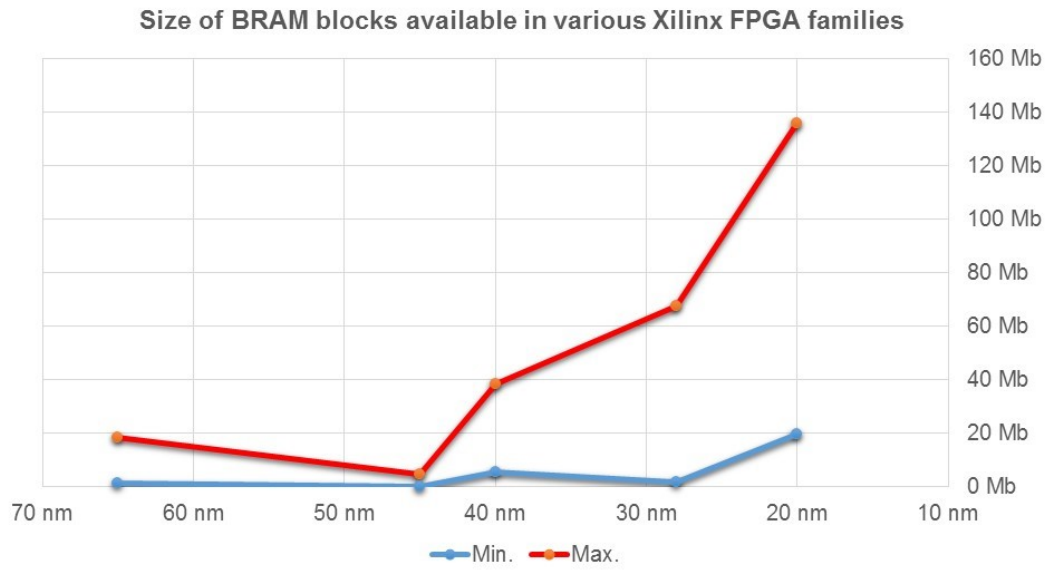


Figure 24. Size of BRAM blocks available in various modern Xilinx FPGA families.

3.3.6 Method and usage of BRAMs in details

Figure 25 illustrates the key part of the method and the usage of BRAMs, where waveforms of ad-hoc created oscillators are streamed and sampled into memory blocks of size n bits. As the main key outputs, duty cycle (shortened as DC) and frequency are calculated, resp. the relative zone frequency (shortened as CH) in active Nyquist zone k of the sampling frequency f_s. The relative zone frequency of all the circuit or delay t_d per one stage of s-stage long ring oscillator can be calculated for given data stream using simple linear formula, very effectively implementable in software or hardware resources.

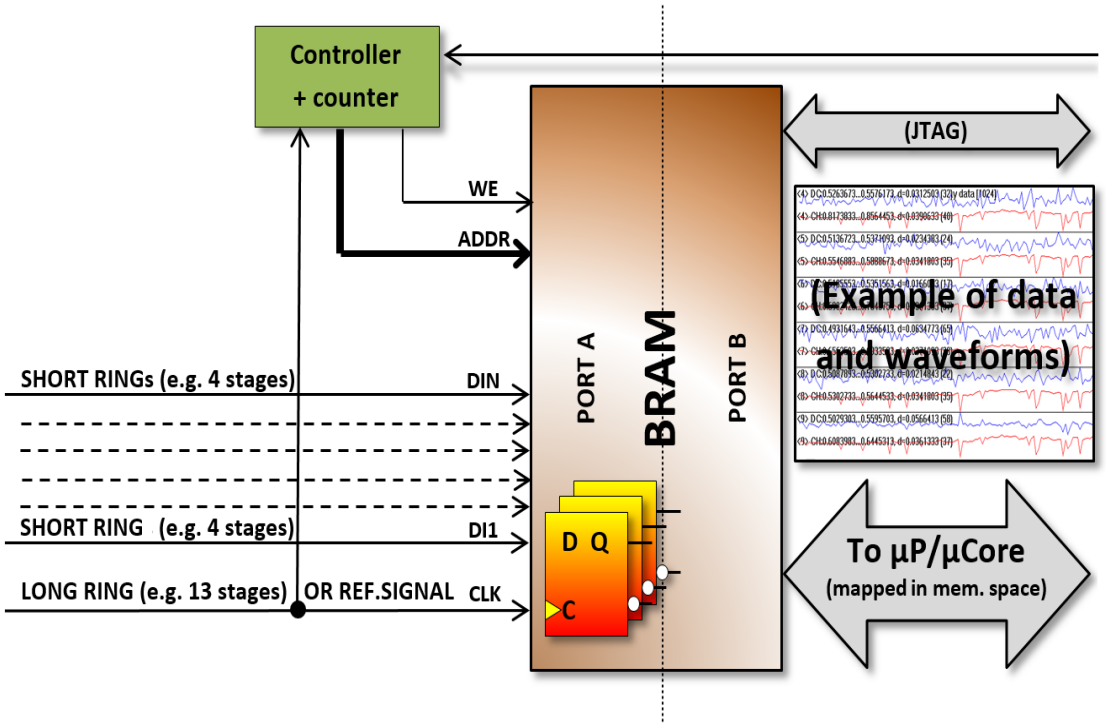


Figure 25. The basic principle of the method and complete on-chip parameter measurements using BRAM blocks.[6]

The method can also be implemented using sets of counters. However, simple design, implementation, extensibility and wide are new and unique advantages of this new method. The design and implementation remain same for all the evaluation processes as well as source of data. In addition, this method allows processing of partial data streams utilizing the same resources. For example, ring oscillator start-up phases as well as steady oscillation phases can be analysed in the same BRAMs and data streams by changing the start and stop addresses. No any special set of programmable counters and logic is required at all – only one tiny and easily implementable fixed set of already presented dedicated resources is connected to already existing designs using interconnect resources

[6] Multiple digital oscillators across the chip and the resulting data streams are sampled in the synchronous memory block. The entire area and circuits of chip can be measured and processed using e.g. partial or dynamic reconfiguration.

only. In addition, such BRAM blocks can be still utilized as a standard RAM memory in processor systems, if the measurement tasks are not in process. Memory segmentation techniques are available as well.

3.4 Nyquist zones and undersampling

When the ring outputs are latched, acquiring bits or data from the ring oscillators and channels and creating the data streams, sampling is performed as the key process of converting a signal into a numeric sequence. The Nyquist–Shannon sampling theorem, named after Harry Nyquist and Claude Shannon, more commonly referred to as the Nyquist sampling theorem or the sampling theorem, is the fundamental result in the field of information theory, and it says that if a function *x(t)* contains no frequencies higher than f_n hertz, it is completely determined by and can be reconstructed giving its ordinates at a series of points equidistantly spaced $1/(2\ f_n)$ apart, or a given band-limited function can be perfectly reconstructed from a countable sequence of samples if the band limit *fs/2,* which is no greater than half the sampling rate *fs* (in Hertz or Samples per second). The half-period from DC (zero frequency) to *fs/2* (half the sampling frequency) is often called the *Nyquist interval* or the *Nyquist region* or the first *Nyquist zone 0*. The *fs/2* is called *Nyquist frequency*. The band from the Nyquist frequency fs*/2* to the sampling frequency *fs is* the *Nyquist zone 1*, and so forth. This key theory is all well-described and referenced in all literature and sources dealing with sampling or signal processing methods or technologies, starting from the key famous paper [***82***], followed by a comprehensive overview presented in [***83***].

Undersampling or bandpass sampling, in general, is a technique where the signal is sampled at a sample rate below its Nyquist rate or twice the upper cut-off frequency, but one is still able to reconstruct the signal. It means that a given signal can be sampled by another, much lower frequency signal, while same parameters of the given signal can be still reconstructed. However, when one undersamples a bandpass signal, the samples are indistinguishable from the samples of a low-frequency alias of the high-frequency signals. Hence, e.g. the frequency of the given signal f_g sampled at the rate of f_s cannot be

determined without previous knowledge of the exact number of its Nyquist zone, because the data sampled and results calculated are de facto invariant to the number of the Nyquist zone, as the general theory shows.

Figure 26 describes it in detail and shows an example of the signal spectrum, Nyquist zones and undersampling.

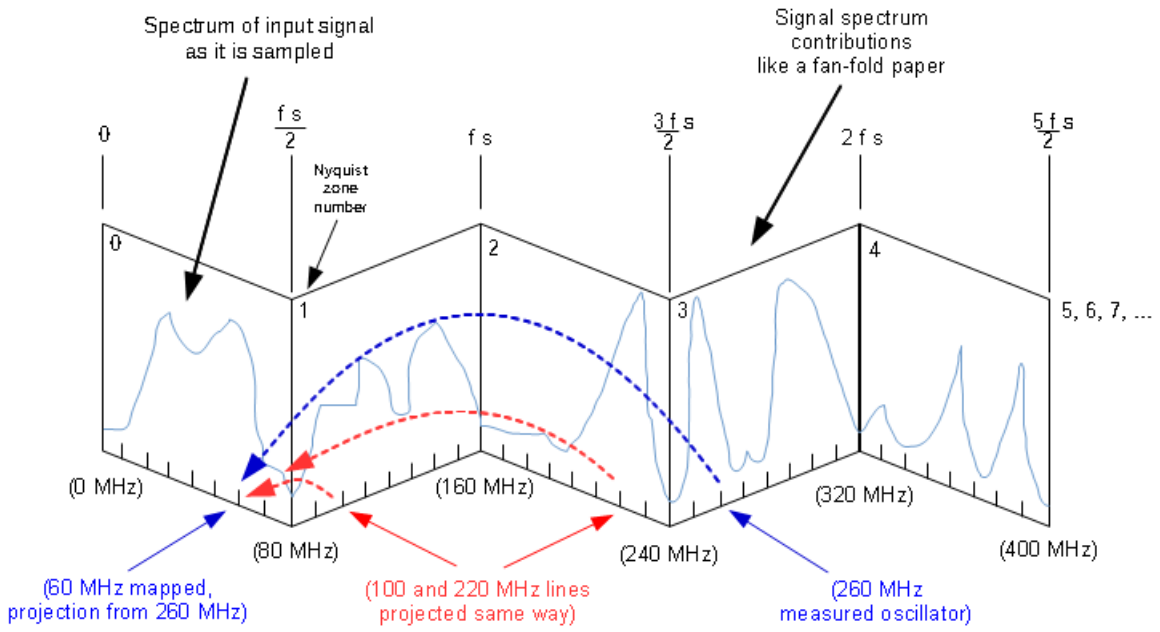


Figure 26. Signal spectrum and an example of undersampled signals

Any purely sine-wave unit signal results in a single solution and just one Fourier coefficient. Periodic functions defined on the unit circle are simply projected by the Fourier transform to the sequence of its Fourier coefficients. A harmonic of a wave is a component frequency of the signal that is an integer multiple of the fundamental frequency. When this fact is simplified to the presented undersampling approach, the Fourier analysis shows that only periodic signals with duty cycle 50% sampled by and ideal signal and equidistant sample points may result in a single unique result. A signal with its duty cycle not equal to 50% (the duration of zero or one in purely digital binary representation) must result in multiple frequencies in term of its absolute fundamental as well as all the spectrum of their harmonic components. Therefore, the frequency of such signals cannot be explicitly determined by the undersampling method and such values of

the duty cycle will result in an error in measurement or even complete impossibility to calculate or determine even basic components of the sampled or signal measured. The following lines show it all in a very illustrative way.

3.5 Evaluating duty cycle

A duty cycle is typically defined as percentage of time that an entity spends in an active state as a fraction of the total time under consideration. A standard formula can be used to calculate the Duty Cycle (DC) of the selected signals as follows:

$$Duty\ Cycle = \frac{\tau}{T} \tag{3-1}$$

where

τ is the duration of 1 (is active state H or logic 1),

T is the period.

Using a probabilistic approach and sampling the signal at random uniformly distributed time points as well as sampling the data signals asynchronously - it means the sampling signal is different from its component in the Nyquist interval in its frequency, allowing to sweep the sampling point along the basic signal interval - we get:

$$Duty\ Cycle = \lim_{n\to\infty} \frac{\sum_{j=1}^{n} x_j}{n} \approx \frac{\sum_{j=1}^{n} x_j}{n}; \forall n \gg 1 \tag{3-2}$$

or

$$DC = \frac{\sum_{j=1}^{n} x_j}{n} \tag{3-3}$$

where

n is the number of samples in BRAM,

x_j is the j-sample (sampled 0 or 1),

and DC is in the range of <0,1>.

As mentioned above in the theory subchapter, the duty cycle information is important information in determining the frequency of a signal. However, changes in the duty cycle may be efficiently used in an analysis of the signal path and determining for example NMOS or PMOS field-effect transistor gate threshold values. In an ideal case, if the threshold is set at a half of the circuit power supply voltage, and the delays in the circuit are the same for both L to H and H to L (the circuit and entire path has sufficient bandwidth and it transports a signal transition in exactly the same way), the duty cycle of such a signal sampled by an ideal sampler with zero jitter and the same threshold value will result in the same number of zeroes and ones in a sufficiently high even number of samples in sampled data streams. The even number of samples is already ensured by the length of the memory blocks, typically 2^{bn}, where *bn* is typically 10 in modern FPGA devices, enabling typically 1024 memory rows and 18 or 36 data streams per each single BRAM unit.

3.6 Evaluating frequency

If sampling periodic signals with a duty cycle very close to 50 % (H:L levels of the digital signal in their length close to 1:1), the following evaluated formula for undersampling and the corresponding Nyquist zone can be used and the frequency calculated easily from the data, using a linear or hyperbolic format and corresponding algorithm. However, precise measurement of the frequency in terms of its absolute value is not required at all. In fact, the only parameter measured is the change of frequency within a Nyquist zone. Therefore, in the following linear formula, only the value of *CH* is to be evaluated as a relative number of transitions in the sampled data streams, such as:

$$CH = \frac{\sum_{j=2}^{n} |x_j - x_{j-1}|}{n} \tag{3-4}$$

where

n is number of samples.

x_j is the j-sample (sampled 0 or 1),

and *CH* is in the range of $\langle 0,1)$.

In this case, the subtraction and the absolute value can be calculated using the XOR (eXclusive-OR, symbol ⊕) logic operation. This logic operation, as a logic gate, is already present in high amount in the configuration logic blocks in programmable logic devices, including FPGAs and CPLDs. Using this XOR-gate already present in the chips, **no** any special or any intensive logic resources are required at all. It also is one of the very basic operations supported by all ALU (Arithmetic Logic Unit) in processor systems.

Using the XOR operation, we get the following formula:

$$CH = \frac{\sum_{j=2}^{n}(x_j \oplus x_{j-1})}{n} \tag{3-5}$$

If *DC* is 50%, the frequency (linear formula) can be calculated as follows:

$$f = \frac{f_S}{2}(k+m) - \frac{f_S}{2}\left(sgn(\mathrm{m}-1)\right)\left(\frac{\sum_{j=2}^{n}|x_j - x_{j-1}|}{n}\right) = \tag{3-6}$$

$$= \frac{f_S}{2}\left(k + m - sgn(m-1).\left(\frac{\sum_{j=2}^{n}|x_j - x_{j-1}|}{n}\right)\right); n \gg 1 \tag{3-7}$$

Hence, the average delay of each single stage can be calculated as:

$$t_d = \frac{1}{S.f_S.\left(k+m-sgn(m-1).\left(\frac{\sum_{j=2}^{n}|x_j - x_{j-1}|}{n}\right)\right)}; n \gg 1 \tag{3-8}$$

where

fs is the sampling frequency,

k is the active Nyquist zone number (0,1,2,3, …), while the first Nyquist zone (here starting from number zero) is 0 Hz to *fs/2*,

m is *k* modulo 2,

S is the number of stages in the ring oscillator.

3.7 Undersampling under limitations

As mentioned in the theory subchapter above, in order to exactly determine or calculate the frequency of the digital signal, its duty cycle must be equal to 50 % and also the sampler (sampling unit) has to have ideal parameters. Figure 27 shows the impact of the duty cycle ratio on determining the frequency as it was introduced above.

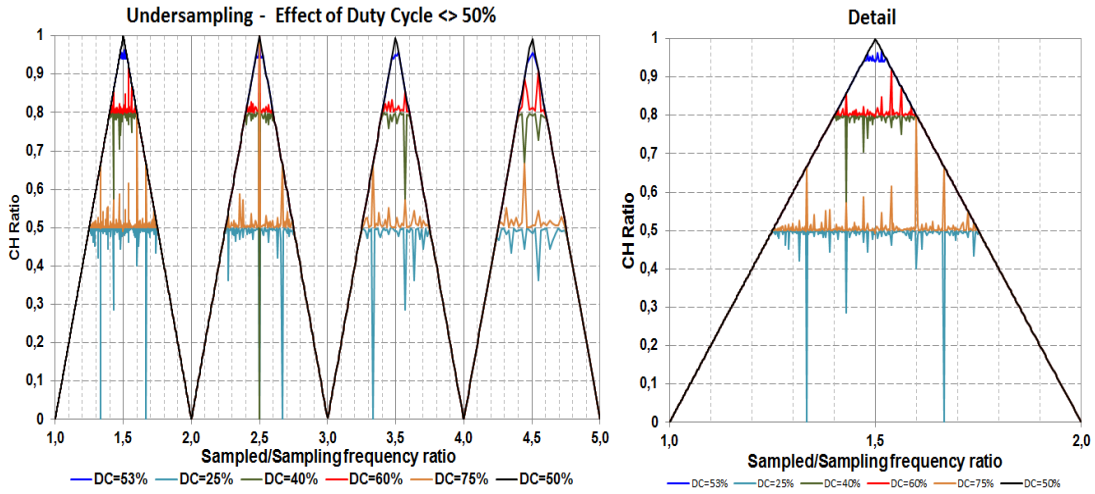


Figure 27. Simulated effect of duty cycle on frequency evaluation (with detail).

Not only the theory, but also the simulations performed as well as real tests show, that duty cycle DC of 50±3 % as well as the typical jitter in the range of picoseconds causes acceptable error below 10%, while the results can be finally adjusted under certain conditions. In case of changes in DC while CH stays the same, it is obvious, that we are facing some change of the circuit or FET transistor threshold levels. Any changes in the frequency are caused by variations in voltage of internal power supply rails or die temperature.

3.8 Absolute and differential method

The new proposed methodology allows implementation of two key methods, called *absolute* and *differential*. The absolute method uses an external signal as the clock signal of the sampler unit or the BRAM clock input. It utilizes typically 100 MHz clock signal as the source of sampling frequency from the on-board crystal oscillator unit already present on most of development boards and kits. If the stability and quality of the oscillator and all the signal path is high, the method is surprisingly sensitive to detect very tiny changes in temperature or power supply voltages, and the resolution is sufficient enough to detect a human finger is touching the FPGA package (the sensitivity is approximately 0.7 ps/K in case of 45 nm low-power Samsung technology [***84***]) as well as stress effects in the FPGA silicon substrate due to e.g. torque, moment of force applied to the FPGA package or the whole PCB board. Random telegraph noise (RTN) exhibited by deep-submicrometer metal-oxide-semiconductor metal–oxide–semiconductor field-effect transistors can be detected as well. **The absolute method is used mainly for measurement of parameters of the basic units of the devices, delays, strong crosstalk, mutual changes in threshold values and dependencies of the internal structures to e.g. temperature or voltage absolute values or variations.**

The new differential method is a completely new method invented. In this case, the clock source of the sampling unit or the BRAM clock input is connected to another selected ring oscillator output, typically much longer in its number of chain units, or in having specific parameters. This solution creates **completely in-situ method**, because the measured objects, the measuring unit, data acquisition and data storage unit as well as the data processing units are on the same chip, device or in the same package. Owing to this fact, all the parts of the solution do have same or very similar environmental conditions, while utilizing different sets of transistors or basic circuits, paths and logic blocks. This solution suppresses the effects of temperature changes to acceptable minimum levels (an increase in temperature by 40 degree of Kelvin represents typically only about 10 % of measured aging effects per month) even on its very basic data processing level. **The differential method is used especially for aging and device degradation processes measurement and analysis purposes. If combining advanced matrix operations and**

data from measurements using also the absolute method, electromigration effects, various crosstalks and other mutual effects as well as tiny changes in the device can be detected at much higher sensitivity levels.

3.9 Method's sensitivity and resolution aspects

In case of the absolute method, the overall quality of the outputs generated by the method presented is determined by the external clock sources and quality of the signal paths to the device. In both cases, both mentioned key parameters of the method are directly affected by the amount of data available in the data streams. However, the maximum BRAM sampling frequency is limited to those around 300 MHz in low-power or 600 MHz in high-performance modern FPGA devices. Also the jitter caused by the BRAM input units, crosstalk, interconnections, and consequently data samples, creates additional errors in the measurement. Figure 28 shows the results of experiment, where the sampler shows uniformly distributed jitter at various levels. The results clearly show that the error caused in measurement of the signal frequency is below 2 % in the first Nyquist zone and the number of stages used in the ring oscillators. It is highly limited close to the limits of the frequency band, while the measurements at the centre frequency are nearly unaffected.

The length of a data block obtained per one cycle is in MB (4Kb to 64Kb per channel). In case of higher number of rings, each data path consists of 1024 bits. During the tests, the length of data in 1 kbit per channel was observed as the minimum to get some reasonable outputs. Arrays larger than 64 Kb provide no significant improvement in final results. The raw data can be extremely easily compressed by a simple lossless compression method (for example run-length), or advanced compression method like Huffman compression, LZW, etc.). The data can be processed by the internal processor (typically ARM cores on modern FPGA devices, or any type of soft-core processor solutions, such as Microblaze in my case) or sent out of the chip via USB or JTAG to a PC and processed there. The way of utilization of BRAM and the presented algorithms are suitable for multicore systems and multiprocessing as well.

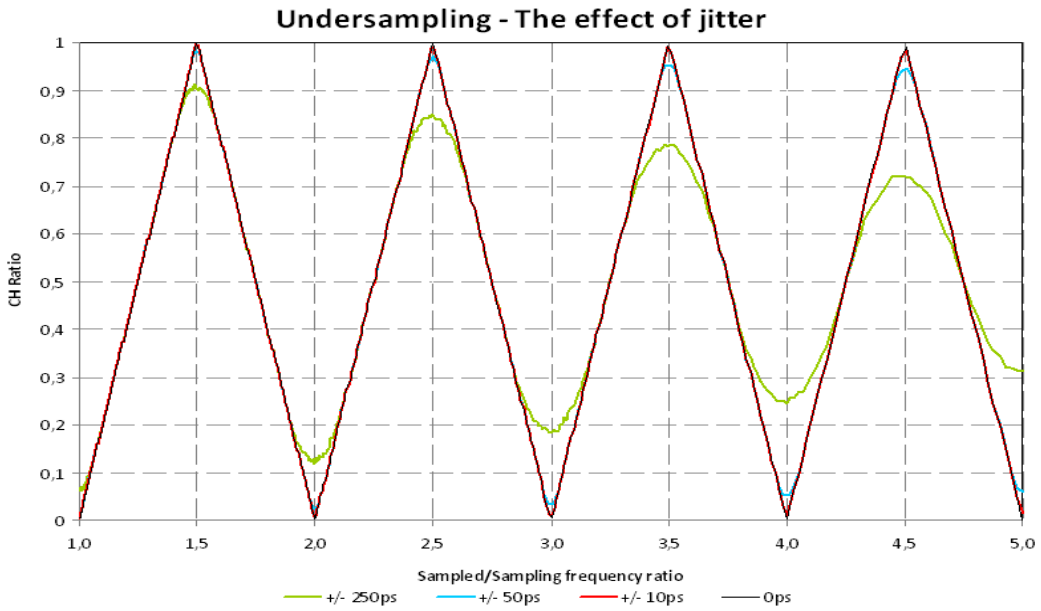


Figure 28. Simulated impact of jitter of sampler on frequency evaluation.

For the absolute measurement mode, just one precise on-board crystal oscillator is utilized as the base clock frequency, typically 100 MHz or 200 MHz. This value was selected because of its simplicity and also because it is selectable all across the main development kits and platform. Theoretical resolution of the method is limited by the maximum sampling frequency and length of the sampled data block. Theoretical resolution of the method is obviously limited by detection of at least one difference in two data streams of two sampled frequency sources or outputs of ring oscillators. Table 3 shows selected details from modern FPGA families including the maximum time resolution of the method on the selected platforms.

The real usable and stable values of the method's resolution, on real structures and using full BRAM data width, are typically in the range of tens of picoseconds, also due to jitters, wider aperture window and lower BRAM clock frequencies used in most of designs. Table 4 shows the typical resolution of the method within the first Nyquist zone and with respect to the non-ideal parameters of the samplers and BRAM blocks, all across the FPGA die. Resolution of the method is also limited by the Nyquist frequency and operating Nyquist zone. Operating in the sixth (and higher) Nyquist zone at high frequencies gives noisy results, as well as BRAM working close to its maximum clock

frequency. The optimal solution operating close to the limits is clearly a trade-off. However due to various noise sources and crosstalk present in real FPGA designs and systems, dithering and averaging methods can be effectively used and applied to an FPGA system and the partial data in order to increase the final resolution of the method

Table 3. Maximum resolution of the method on FPGAs from selected modern Xilinx FPGA families

FPGA Family	Technology	$f_{BRAMmax}$	$t_{BRAMmin}$	t_{resCH1}	t_{resCHm}	Source
Spartan 6	LP 45 nm	320 MHz	3,13 ns	3,1 ps	190 fs	[85] DS162 (v3.0)
Virtex 6	HP 40 nm	600 MHz	1,67 ns	1,6 ps	50 fs	[86] DS152 (v3.6)
Zynq 7	LP 28 nm	510 MHz	1,96 ns	1,9 ps	60 fs	[87] DS187 (v1.11)
Kintex 7	HP 28 nm	601 MHz	1,66 ns	1,6 ps	50 fs	[88] DS182 (v2.8)
Ultrascale	HP 20 nm	660 MHz	1,52 nm	1,5 ps	45 ps	[89] DS892 (v1.2)

Legend:

$f_{BRAMmax}$ is the maximum BRAM clock frequency according to the FPGAs' product specification datasheets

$t_{BRAMmin}$ is the minimum BRAM cycle time

t_{resCH1} is the minimal time resolution of the method per BRAM cycle, without averaging, using all channels in given BRAM block

t_{resCHm} is the minimal time resolution of the method per BRAM cycle, without averaging, using given BRAM block configured with one channel only, for a single BRAM block and without any cascade mode, supported by some FPGA families

The method and its sensitivity and resolution was validated on many platform. Please see chapter 4.6.1 - Basic Statistics at page 86 for more results regarding basic statistic results and data processing of the raw BRAM data streams.

Table 4. Typical resolution of the method on FPGAs from selected modern Xilinx FPGA families

FPGA Family	Technology	t_{awm}	$t_{resTyp100MCH1}$	$t_{resTypMAXCH1}$	Source
Spartan 6	LP 45 nm	0,40 ns	10 ps	3 ps	[*85*] DS162 (v3.0)
Virtex 6	HP 40 nm	1,14 ns	11 ps	5 ps	[*86*] DS152 (v3.6)
Zynq 7	LP 28 nm	0,49 ns	10 ps	3 ps	[*87*] DS187 (v1.11)
Kintex 7	HP 28 nm	0,42 ns	10 ps	2 ps	[*88*] DS182 (v2.8)

Legend:

t_{awm} is the maximum aperture window across all the BRAM blocks and devices according to the FPGAs' product specification datasheets

$t_{resTyp100MCH1}$ is the typical resolution of the method for the most used 100MHz clock source frequency and all BRAM channels, for a single BRAM block and without any cascade mode, supported by some FPGA families, without averaging

$t_{resTypMAXCH1}$ is the typical resolution of the method for the maximal BRAM clock frequency and all BRAM channels, again for a single BRAM block and without any cascade mode, supported by some FPGA families, without averaging.

Note: Ultrascale estimations (20 nm) are not provided due to insufficient data provided by the FPGA manufacturer up to the final date of publication of this document.

3.10 Oscillator start-up phase and noise

The ring oscillator theory is very complex in its nature. The basics related to this area can be found in [*90*], [*91*] or [*92*]. However the exact case absolutely same to my proposed method is not published yet. My approach doesn't contain series of inverters, but one inverter only, followed by a series of delay stages. It is obvious that my approach lower the frequency and also noise of the ring oscillators or generated by the ring oscillator circuit.

The initial period of deterministic oscillation contain a noise, as it was also reported in [*93*]. This phase is used for cryptographic purposes. The principles and observed waveforms are discussed or reported in [*94*], [*95*], [*96*], [*97*], or [*98*], [*99*], [*100*] and [*101*].

Figure 29 shows all the phases available in measurement of degradation processes and in the proposed method. The exact time can be adjusted both by fixed counter design as well as much more convenient way by a selection of suitable address ranges in BRAMs and adjusting the amount of usable data. The oscillation phase (in green) is also kept at the required minimum, because any oscillation causes a relaxation of the aged parts of the circuit and recovers some non-zero portion of the original or initial state and parameters of the employed transistors and nanostructures.

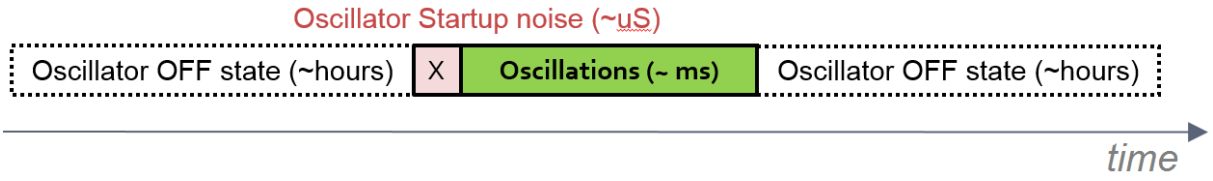


Figure 29. Ring oscillator start-up phase and measurement of BTI processes.

I have performed many measurements to validate the method and in order to study the start-up phases in more details at least on selected platforms. However, it is very difficult to route the internal signals and ring oscillator outputs out of the FPGA package, especially in case of the fastest rings and general I/O pins. There are many factors influencing the quality of the final signal measured out of the package and it may also have a direct negative impact to the originally designed circuit. In case of measured signal with higher frequencies in the range of hundred MHz and GHz bands, the best results can be achieved only by direct measurement methods or when using differential I/O ports and differential active GHz probes. In my case, it was not possible to use probes connected directly to the chip (wafer), but many tests were performed using a new advanced oscilloscope – Agilent 9000k – with very long acquisition memory of 1 GSa per channel at 20 GSa/s maximum sampling frequency capability.

Figure 30 shows an example of measured waveform of the output signal of very long ring oscillator (frequency about 25 MHz) sampled by the new Agilent 9k oscilloscope and using only passive probes. he oscillator output was routed to a general FPGA I/O pin and on the JA connector at Zedboard development kit. The I/O signals are routed from the FPGA package to the physical connector pin via a small, spatially very tiny serial resistors. The Zedboard contains 28 nm FPGA chip - Zynq®-7000 family All Programmable SoC - XC7Z020 in CLG484 BGA package. The oscillator output frequency can be evaluated in each cycle with sufficient precision only in the case, if very high sampling frequency and high-quality signal paths are used. However any effective usability of this simple approach for higher frequencies of shorter ring oscillators is very low. It is also possible to make an observation when comparing experiences with available FPGA boards, that the latest 28 nm technologies offer generally better signal quality than the most of their low-power predecessors. The observed start-up transitions lasts typically for hundreds of the signal periods and up to 5% in its magnitude for all the measuring path chain.

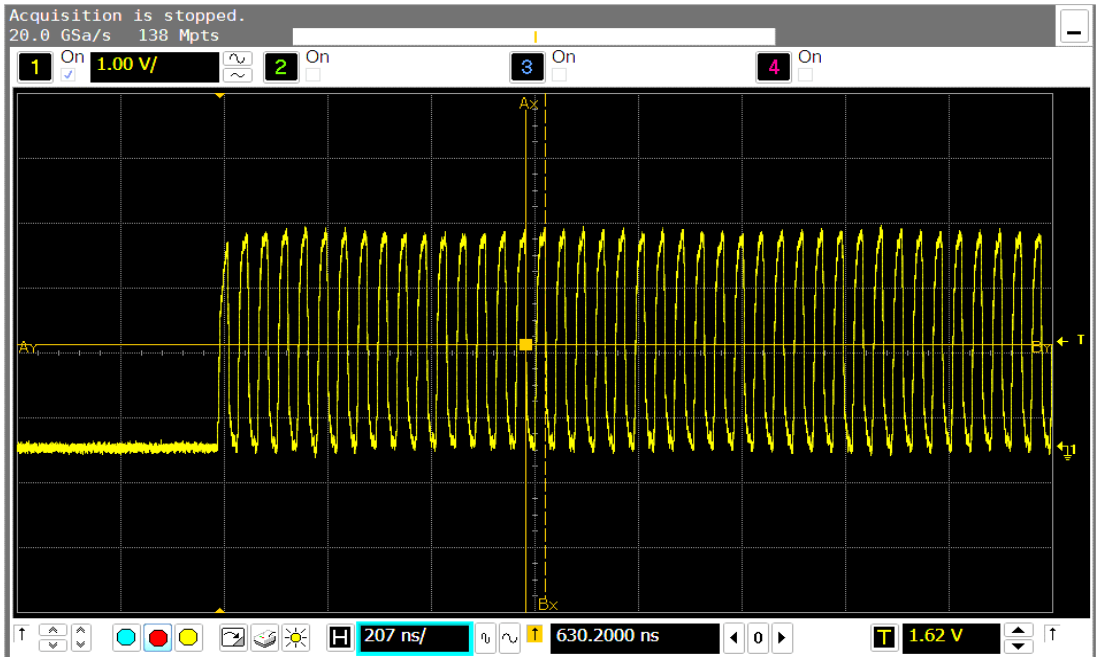


Figure 30. An example of externally measured ring oscillator start-up phase of a long ring.

Chapter 4

4 Experiments and Results

An experiment is a procedure carried out in order to verify the validity of a hypothesis. It has to be clearly mentioned here, that I have performed close to hundred different tests on many platforms, environmental conditions and configurations. I have generated more than 1000 GB of raw data logged during all the tests.

4.1 Test Platforms, Tools and FPGA Types Used

The main advantage of the experiments described in this chapter is in **utilization of** the **standard tools only** and generally available development kits, no other tools or expensive equipment (oscilloscope, logic analyser, etc.) is required at all. The method is based on a simple core design. It is easily scalable thanks to the flexible key part of the design. The design can utilize also programmable internal matrixes for dynamic scaling of the rings.

4.1.1 65 nm FPGA device and platform

The first test board and the FPGA type used for the first test purposes were Xilinx ML506 board[7] with 65nm Virtex 5 FPGA XC5VSX50T-FFG1136 manufactured using 65 nm copper CMOS process technology (1.0V core voltage). The device has about 8160 slices, 780 Kb of distributed RAM and 4752 Kb of Block RAM employing 132 blocks, each 36 Kb in each true dual-port RAM block. There is also a socket populated with a 100-MHz oscillator. The programmable clock generator provides 33 MHz, 27 MHz, and

[7] http://www.xilinx.com/products/boards-and-kits/HW-V5-ML506-UNI-G.htm

a differential 200 MHz clock to the Xilinx FPGA. Please see [*102*], [*103*] and [*104*] for more details about this platform.

4.1.2 45 nm low-power FPGA device and platform

Regarding 45nm test platform, Digilent's Atlys Spartan FPGA Development board[8] was used for the test purposes, having one Xilinx Spartan®-6 LX45 FPGA on the board, (in my case and FPGA type a chip having approximately 44K logic cells, 6822 slices with look-up tables (LUT), 54576 flip-flops, 172 pieces of 18Kb true dual-port RAM blocks of 2088Kb block memory, etc.). The die is manufactured using a 45nm Samsung low-power copper process technology [*84*] and assembled on the board in a 324-pin BGA package. There is also a single 100MHz clock source on the board. Please see [*77*] for details about Spartan Xilinx FPGA family and about Atlys board in [*105*].

4.1.3 40 nm high-performance FPGA device and platform

Some tests were done also on ML605[9] development board utilizing Virtex®-6 XC6VLX240T-1FFG1156 FPGA device manufactured using 40nm process. This device has 241152 logic cells, 37680 slices and 416 pieces of 36Kb true dual-port RAM blocks (14976 Kb in total in BRAMs only). There is also a differential 200MHz and a single-ended 66 MHz socketed clock source present on the board. Please see [*78*], [*86*] , [*106*] and [*107*] for more details about this platform.

4.1.4 28 nm low-power and high-performance FPGA devices and platforms

Two samples of Digilent's low-cost ZedBoard™ Field Programmable Gate Array (FPGA) Development board[10] were used for the test and measurement purposes, having one Xilinx Zynq™-7000 SoC (All Programmable System on Chip) FPGA type

[8] http://www.digilentinc.com/Products/Detail.cfm?Prod=ATLYS

[9] http://www.xilinx.com/products/boards-and-kits/EK-V6-ML605-G.htm

[10] http://www.digilentinc.com/Products/Detail.cfm?Prod=ZEDBOARD

XC7Z020-1CLG484 on the board. The FPGA device is a member of the Artix™-7 low-cost Xilinx FPGA product family, intended for the application segment similar to previous Spartan© product families[11] (see Xilinx press release from July 17, 2012). The die is manufactured using TSMC's advanced 28 nm high-performance, low-power copper process technology, incorporating dual-core ARM® Cortex™-A9 based application processor unit (APU), programmable logic (in my case an FPGA type having approximately 85K logic cells, 53200 look-up tables (LUT), 106400 flip-flops, 140 pieces of 36Kb true dual-port RAM blocks of 560 KB block memory, etc.), cache or other memories, interfaces, DSP blocks, etc. Please see e.g. Xilinx datasheets [*79*], [*108*], [*87*] and [*109*] for more details about the FPGA families, including all the detailed information mentioned in the WP423 in [*110*]. The Kintex family details can be found in [*88*]. The FPGA is assembled on the board in a 484-pin BGA package. There is also a single 100MHz clock source available on the board. Please see [*111*] and [*112*] for more details, as well as the ZedBoard community web [*113*] for additional information and support.

4.1.5 Notes

The data mentioned above shows that the 45nm Spartan is approximately a half of the 28 nm Zynq in terms of size of the programmable logic cells as well as the total block memory cells available.

Some tests were performed also on 90 nm FPGA using Spartan 3 platform. However the results are not significantly different to the results obtained on 65 nm FPGA device and platform. Hence, such results are not presented in this document.

4.2 Software Tools Used

Only a standard software set of tools from Xilinx, ISE Design Suite 14.x in the 64bit version was used. The proprietary data processing software was written in GNU C. This my new software pack is a part of a new Open-Source data processing toolbox, used

[11] see e.g. Xilinx press release from July 17, 2012, SAN JOSE, California

especially for devices parameter measurement, mapping, optimum parameter-aware placement and routing, up to a final project testing and reliability assessment purposes.

4.3 Connections and interfaces to PC

The boards were connected to a PC via USB using serial line or JTAG, no other devices, tools or any special or expensive equipment were utilized, necessary or required. The UART was set at 115200 bauds and the JTAG clock speed was set to the maximum frequency all the time.

4.4 Measuring and Controlling FPGA Core Voltage

Modern programmable chips, including 28 nm Zynq™ devices, incorporate a dedicated XADC block [*108*], typically based on dual 12-Bit 1 MSPS Analog-to-Digital (A/D) Converter. This dedicated unit is capable of measuring various internal and external voltages and also the die temperature. Therefore, there is no problem in case of all 28 nm devices. The only problem was with measurement of the FPGA power consumption. In case of 28 nm low-power Zynq devices, the ZedBoard™ was slightly modified adding small 0.01 Ω resistors, allowing the measurement of the currents at power rails. The voltages measured by the internal XADC unit were measured and checked externally with sensitive multimeters, while the measurement error was mostly of the additive type, with errors below acceptable 2%.

In case of a 45nm Spartan device and the Digilent Atlys board, measurement of both the voltage as well as the current on 0.010 Ω resistor shunts is performed using already incorporated sensitive I^2C interfaced 16-bit plus sign on-chip programmable gain ΔΣ A/D converters LTC2481 [*114*], placed on the board off the FPGA chip and close to the DC/DC supplies. Digilent Adept software was used to perform the complete control and data logging or storage. The measurement of the die temperature was achieved using an external temperature sensor attached to the heatsink on the FPGA package.

In case of complex and expensive development boards, including Virtex 7 ones, the board power management units typically utilize advanced DC/DC controllers, such as AVS systems from Texas Instruments in [*115*] or [*116*] for low-power systems. Such fully programmable advanced power management systems allow on-line changes in many parameters of the power supply generated output voltage and other signals, e.g. through I2C bus or similar System Management bus. FPGA core voltage adjustment can be performed in very rich way, however it typically requires special software or dedicated hardware IPs. One can find also some other information in [*117*] and [*118*].

In case of low-cost development boards, the power supply voltage has to be adjusted with special external components or modifying parts of the power supply circuits. In case of both Digilent Atlys and ZedBoard™ low-cost boards, the FPGA core power supply voltage was regulated with multi-turn miniature potentiometers added to the original DC/DC power supply circuit, allowing easily adjustable voltage steps below desired resolution of 0.5 mV. The power supply outputs were monitored all the time and very high stability of the conditions desired was achieved. The change in temperature of the die will be discussed and is corrected in the final data.

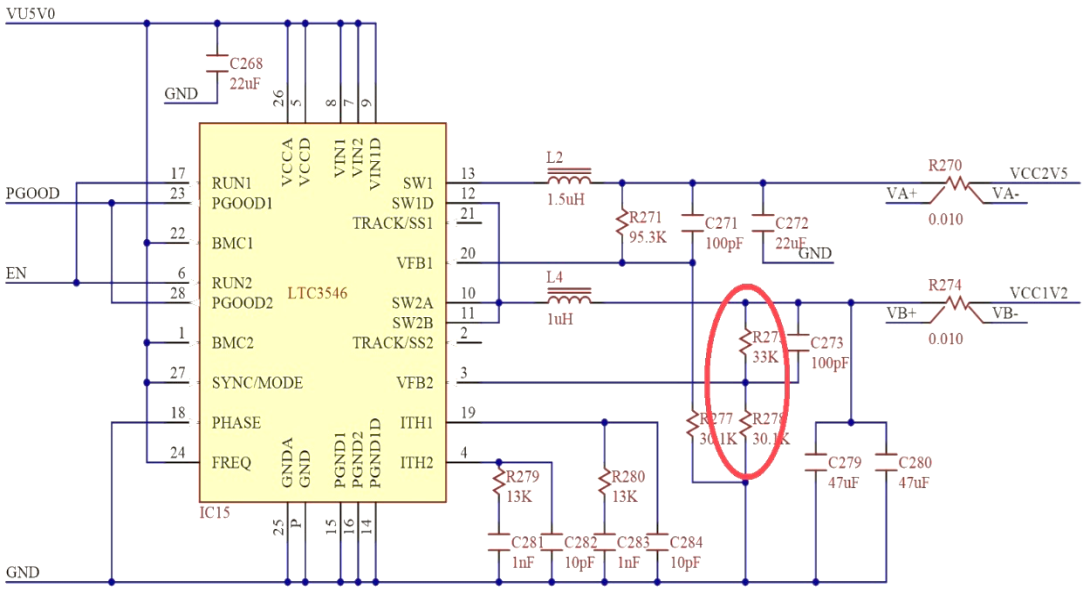


Figure 31. Schematic of the DC/DC 45 nm FPGA core power supply unit on Digilent Atlys board (adjusted from [*119*] page 12).

The core supply voltage of 45 nm Spartan FPGA in Digilent Atlys development board was adjusted using a 50 kΩ multi-turn miniature trimming potentiometer added in parallel to resistors R275 and R278 in the original DC/DC power supply circuit, close to LTC3546 switched DC/DC combined 1.2 V and 2.5 V power supply controller. Figure 31 shows the details about the modified part in the board's schematic. Figure 32 shows one of the modified Digilent Atlys board in detail. Please see [*120*] for more details.

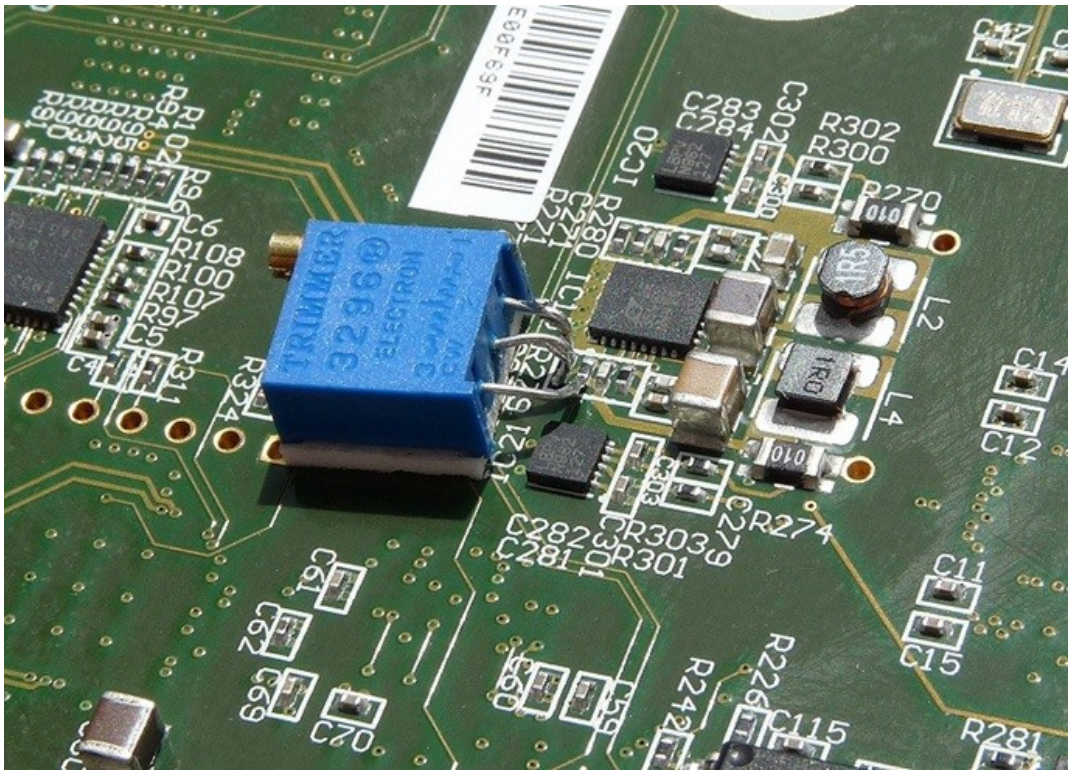


Figure 32. Modified Digilent Atlys Spartan 6 board with a 50 kΩ multi-turn miniature trimming potentiometer added to the original DC/DC circuit.

ZedBoard's FPGA core supply voltage, equipped with 28 nm low-power Zynq programmable system-on-chip, was adjusted using a 20 kΩ multi-turn miniature trimming potentiometer added in parallel to resistors R253 and R256 in the original switched DC/DC power supply circuit, close to MAX15021A switched DC/DC combined 1.0 V and 1.5 V power supply controller. Figure 33 shows details about the modified part in the board's schematic original file. Please see [*120*] for more details. Figure 34 shows the key detail of one of the modified ZedBoard.

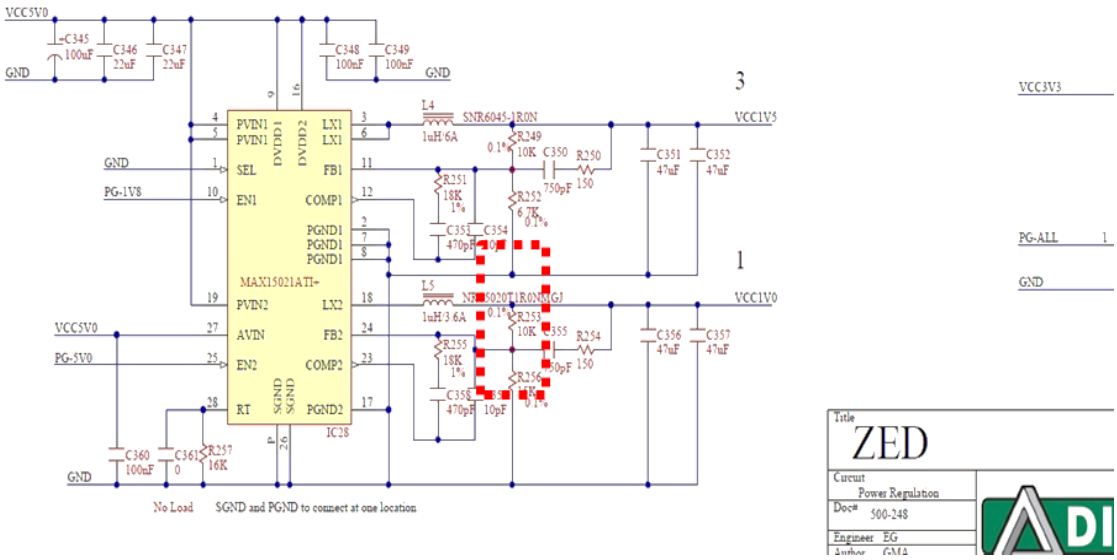


Figure 33. Schematic of the DC/DC 28 nm FPGA core power supply unit on Digilent ZedBoard (adjusted from [*120*]).

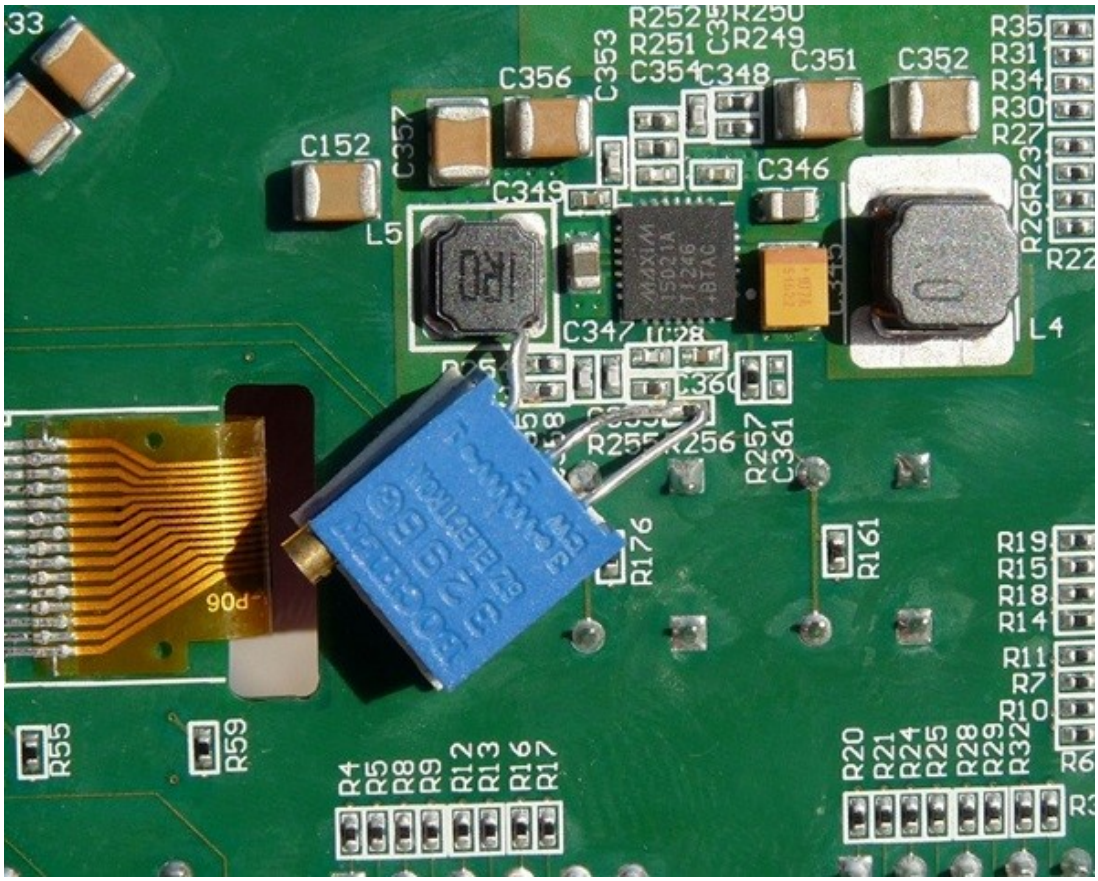


Figure 34. Modified Zynq ZedBoard™ with a 20 kΩ multi-turn miniature trimming potentiometer added to the original DC/DC circuit.

4.5 Measuring and Controlling FPGA Die Temperature

Measurement of die temperature and also a way of control of the FPGA die temperature in order to reach desired temperature levels and study behaviour and parameters of the system under such changed conditions in one of very important part of all serious research and experiment activities. It is possible to find very high number of sources they implement and study temperature measurement control and study, starting from [*121*], study of FPGA behaviour in [*94*], and introducing various toolsets like the one presented in [*122*]. Paper [*123*] deals with operation of Xilinx FPGAs ate extremely low temperatures. A suitable type of temperature chamber is used in most of such experiments and applications. However, is this approach really the best and easiest way to study behaviour of complex systems? Probably not in all cases. Using a climate or a temperature chamber can be very expensive and difficult task. It is important to mention that a special board must be designed or all the development board inserted in the chamber. However, in this case not only FPGA chip is influenced by the temperature and environment, but also the power supply blocks and circuits present on any FPGA development board. Power supply blocks and circuits are very complex systems today and they are subjects to temperature variations as well. Hence, the parameters of such real FPGA chip structures will be influenced not only by the temperature and environmental conditions itself, but also by changes in the power supply rails. It also is why I decided to develop a different approach and in order to try to influence just and only the FPGA die. This approach has some limitations, but it is fully working the desired range of temperatures.

During some of the tests, the **FPGA devices were cooled down or warmed up using a small low-cost thermoelectric element type** TEC1, powered by a 5 A regulated power supply. Due to this fact, it was difficult to reach lower temperature values below 0 °C. On the other hand, thanks to this point-type temperature control, **no other devices were significantly influenced** by the temperature changes and big temperature gradients, including the power supply circuits (no any integrated circuits and devices except

capacitors are located close to the FPGA chip, please see the board layout files for more information). Figure 35 shows a photo of one of the modified 28 nm FPGA platform, including one computer fan mounted on top of the temperature control system. The FOGA die temperature was measured using XADC block [*108*].

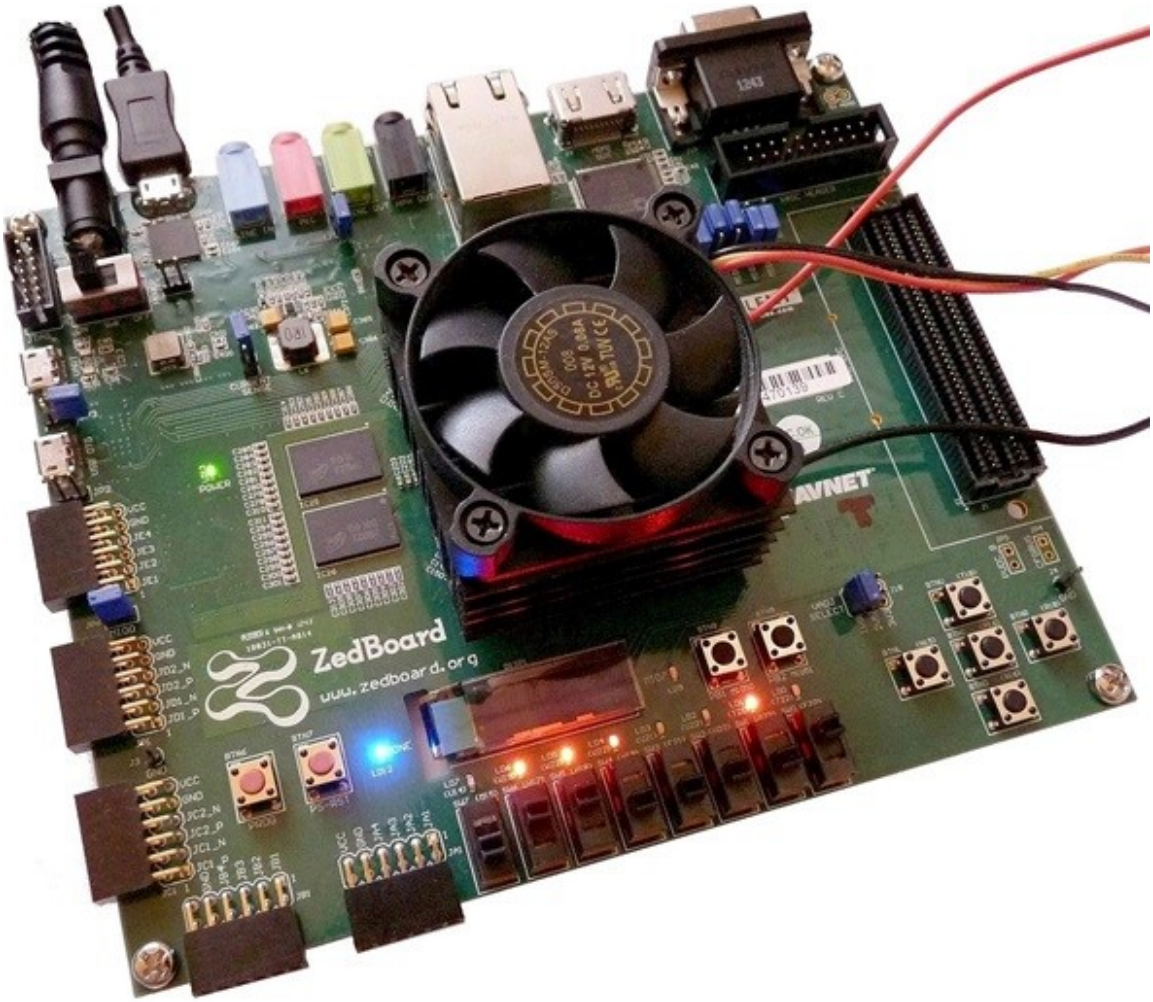


Figure 35. A photo of one of the modified ZedBoard ready for temperature testing.

Figure 36 shows a detail of this the modified ZedBoard™ with both the TEC1 thermoelectric element with silicone grease (thermal compound) and a large heatsink with a fan on it.

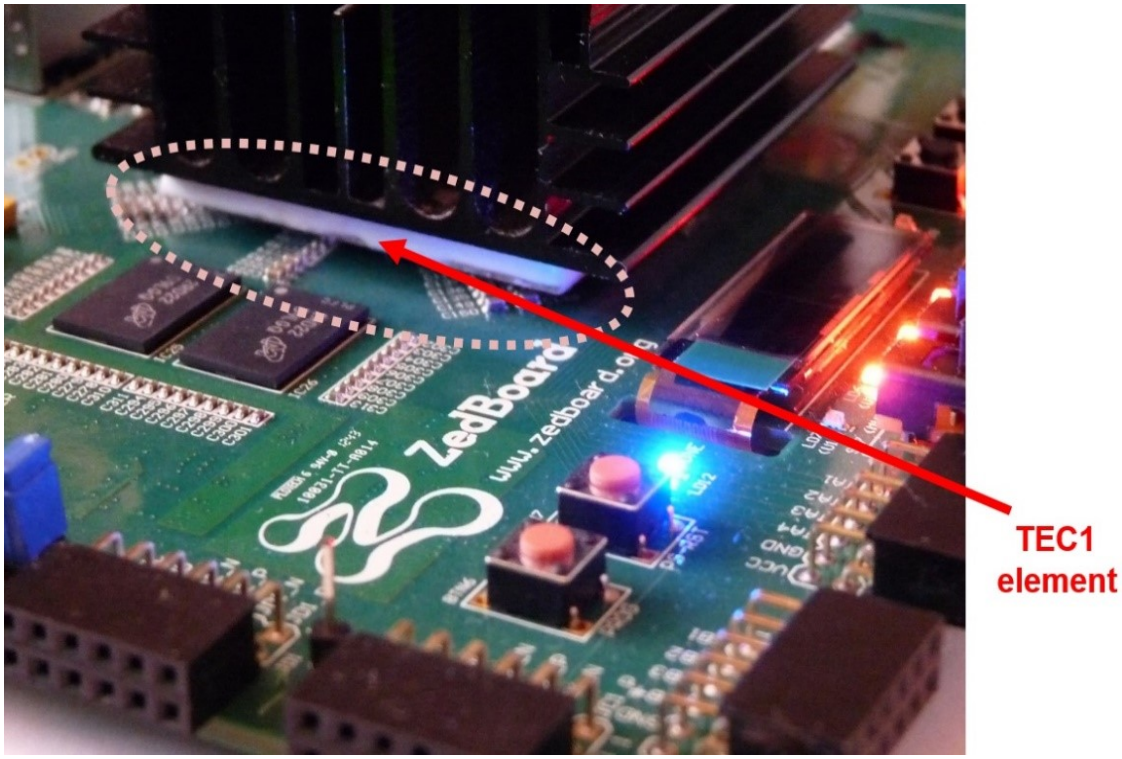


Figure 36. Modified Zynq ZedBoard with a thermoelectric element mounted on FPGA package.

4.6 Selected results

This chapter and all the following figures show selected results from a very high number of performed tests and measurements, including measurements of delays, under various stress conditions and also measurement of aging effects and degradation processes. Some of them have used the so-called absolute method (oscillators running at frequencies from 50 to 300 MHz) and external MEMS resonators. Other figures illustrate availability of measurements of degradation processes in FPGAs. During all the tests, also auxiliary data were logged and analysed.

4.6.1 Basic Statistics

As discussed in one of the previous chapter and subchapter 3.9 - Method's sensitivity and resolution aspects – the method presented in this document allows very high resolution and relatively low noise measurements. This can be validated using very basic statistic processing methods applied to the results and data processing of the raw BRAM data streams.

Figure 37 shows an example of generated histograms - probability distribution of frequency measurement results as CH values, measured on high-performance 28 nm Kintex FPGA. It represents the worst-case results using the shortest BRAM block and data stream length of 1024 bits per channel only. It represents 350 samples sampled in the 3rd Nyquist zone using only a short 1024 bits memory depth, with the average CH value 0.50798 very close to the zone centre frequency. It includes a small change of ± 2 °C in the die temperature around the average value of 41 °C, and also the FPGA core voltage values from 1.003 V to 1.006 V.

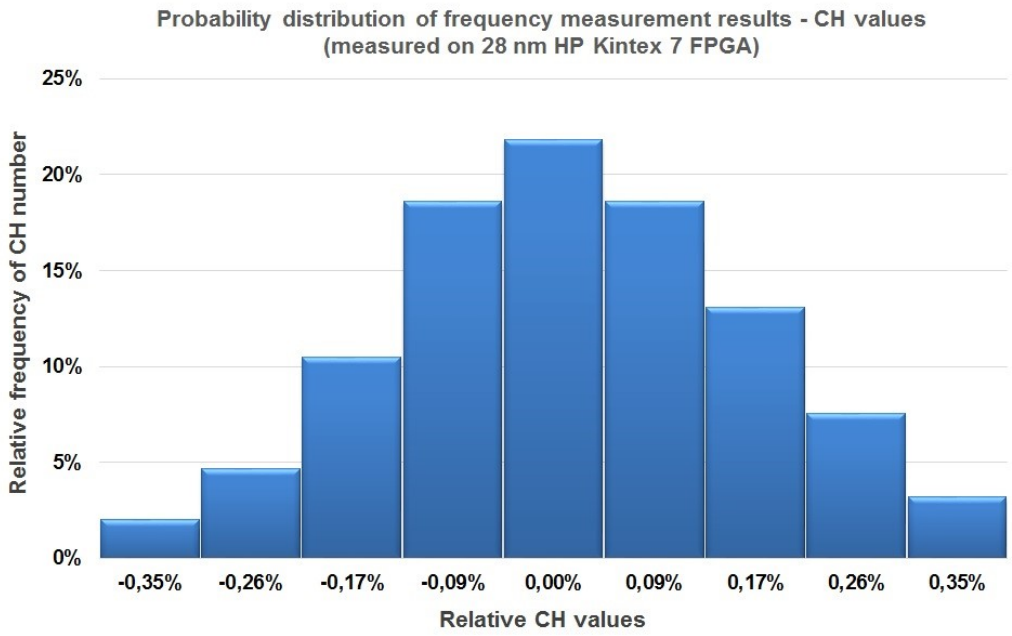


Figure 37. An example of histogram - probability distribution of CH values of frequency measurement results.

The discussed probability distribution of frequency measurement results as CH values is not the ideal one. However the frequencies are close to the normal distribution and obviously in very narrow band ± 0.35 % even under the above mentioned noise conditions. This example represents the typical worst-case result on the platform and using very short BRAM blocks. Figure 38 shows both the environmental conditions logged during this test.

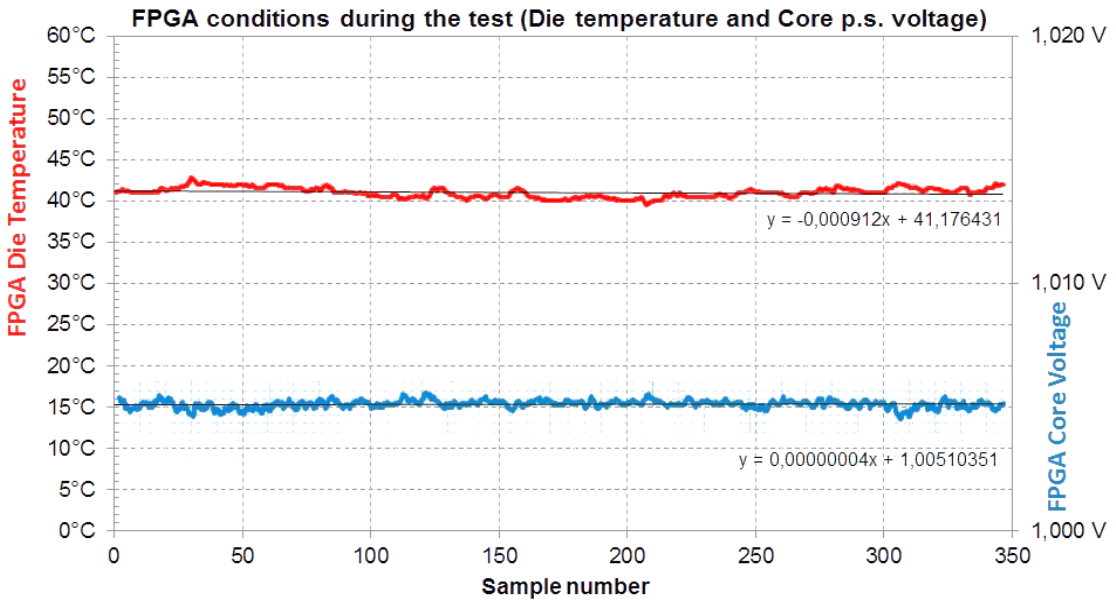


Figure 38. Die temperature and core voltage logged during the discussed test

4.6.2 Measuring Mutual Impact and Crosstalk

The presented method allows many other types of measurement of various parameters and under various conditions using physically the same design and BRAM blocks. Relationship between the die temperature and SLICE (or any other part of ring oscillator) is one of the most important and the very first task measured in a new technology or type of FPGA. Such temperature coefficients can be rarely found and are typically common for each technology line. However, for example crosstalk and mutual impact of workload or utilization of far or neighbouring logic units and circuits is important information, which is not enclosed in datasheets or papers. Figure 39 shows an example of results of my measurements in this area, results of measurements of internal FPGA delays (look-up

tables - LUT - plus latch delay, *An* input to *DQ* output, plus interconnects - NET). It is based on evaluation of the output frequency of each ring oscillator using the absolute method presented in this document. It shows measurable and clearly detectable mutual impact and changes in ring oscillator frequency and delays in the logic, if selected set of oscillators is switched on and off. Ring #30 has visible immediate impact to frequency (delays) of ring #31. Ring #17 influences ring #30 in much lower way. Ring #1 is located completely out of the previous set of ring oscillators. This ring is obviously not significantly affected by work mode or workload of any other ring oscillator. It was observed during the tests, that the final delay change can be up to 10 picoseconds for approximately 50 % loaded cells in 45 nm Spartan 6 FPGA. Under some conditions, it can be close to MUX delay in faster devices. High-performance Virtex lines are more immune to such effects that low-power low-cost Spartan FPGAs. Figure 39 also shows an impact of die temperature; the internal temperature of Spartan FPGA chip has increased during the test, obviously due to increased power dissipation. This fact is illustrated by small, 2 picoseconds delay at begin and end of the test, visible clearly on ring oscillator #1. The new method presented in this document allows analyses of oscillation start-up phases as well as steady oscillation phases using the same physical resources.

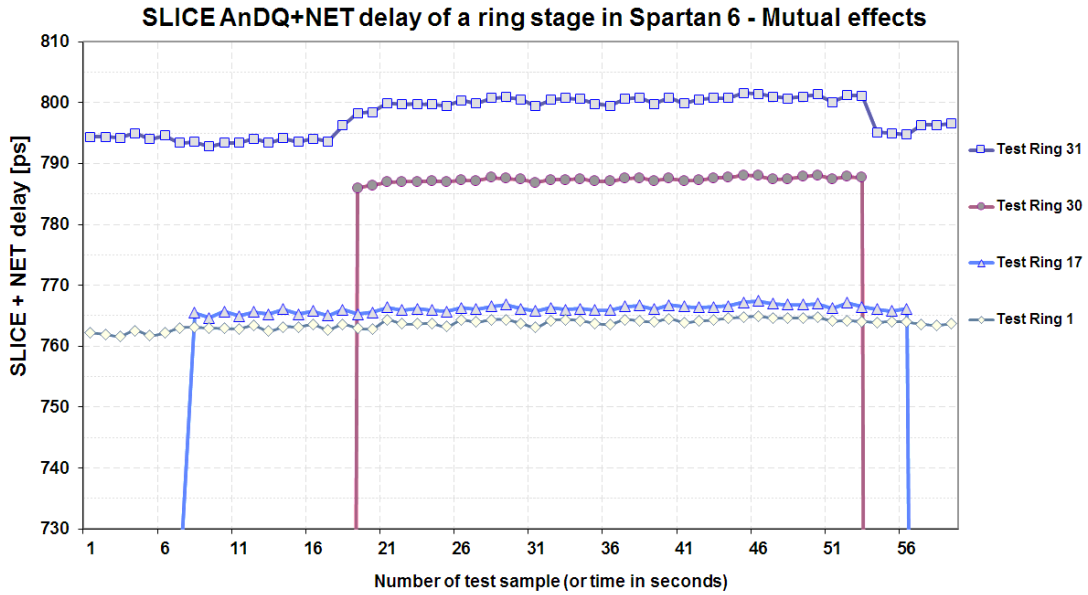


Figure 39. Example of mutual impact and crosstalk and the temperature impact on delays in selected SLICEs and ring oscillators.

It has to be noted here, that both the 28 nm and 45 nm low-power platforms and development boards mentioned do incorporate 100 MHz oscillators and FPGA design was also absolutely the same, only the constraint files were updated in accordance with selected platform and actual board and FPGA pin functions. Crystal or MEMS oscillators are located far away from FPGA chip location and powered from completely different power rails. The crystal oscillators were checked and their frequencies were extremely precise, well below 1 % of the acceptable overall error. Therefore, the results can be considered to be fully corresponding to each other in terms of the absolute as well as relative values points of view. The obtained data and results are fully comparable at least between the technology nodes and devices.

Compared to the situation experienced with 45 nm Spartan® 6 FPGAs, the difference in two neighbouring bands in 28nm device is much lower. There is not such a significant difference between the local and global interconnects, compared to the timing variations within the LUTs and Flip-Flops in the rings.

4.6.3 Measuring Frequency and Delay in Hard Environment

Figure 40 shows the duty cycle results for the 45 nm Spartan device under various core voltage conditions. The two curves for each sub-chart (ring) represent both modes of the core voltage change, when the voltage went up and when it changed back or below its nominal value afterwards. It shows that the device faces absolutely no problems above the recommended working condition range up to 1.50 V of the core voltage, but there are some minor problems with all the members of the set of rings below 0.80 V. This is clearly indicated by standard deviation calculated across all the oscillators and data streams. A change in this value indicates a change in the parameters of some member of the analysed set of oscillators. Therefore, the device works somehow, but not in a fully reliable way. This level represents 66 %, or at least 125 % respectively, portion of the recommended nominal working conditions, it means 1.20 V. The sensitivity coefficient or slope for the linear regression model of the fastest rings is approximately 0.04, at a negative proportion to the voltage. It consists of many factors, including the gate threshold values, etc.

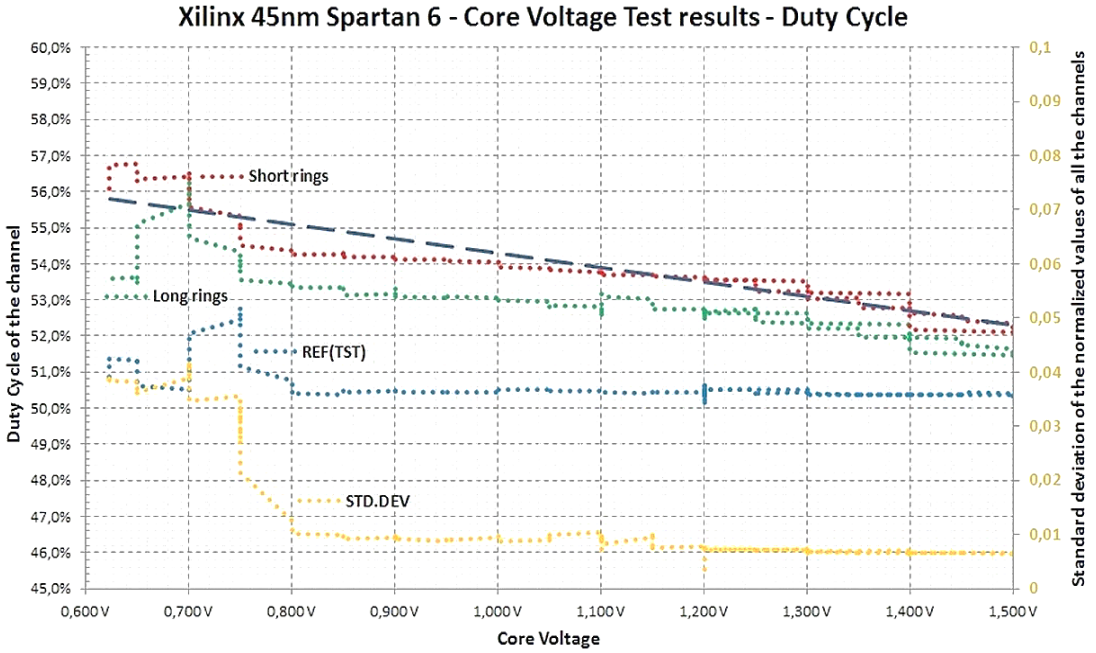


Figure 40. Measurement results of the duty cycle to core voltage change for 45 nm Spartan6.

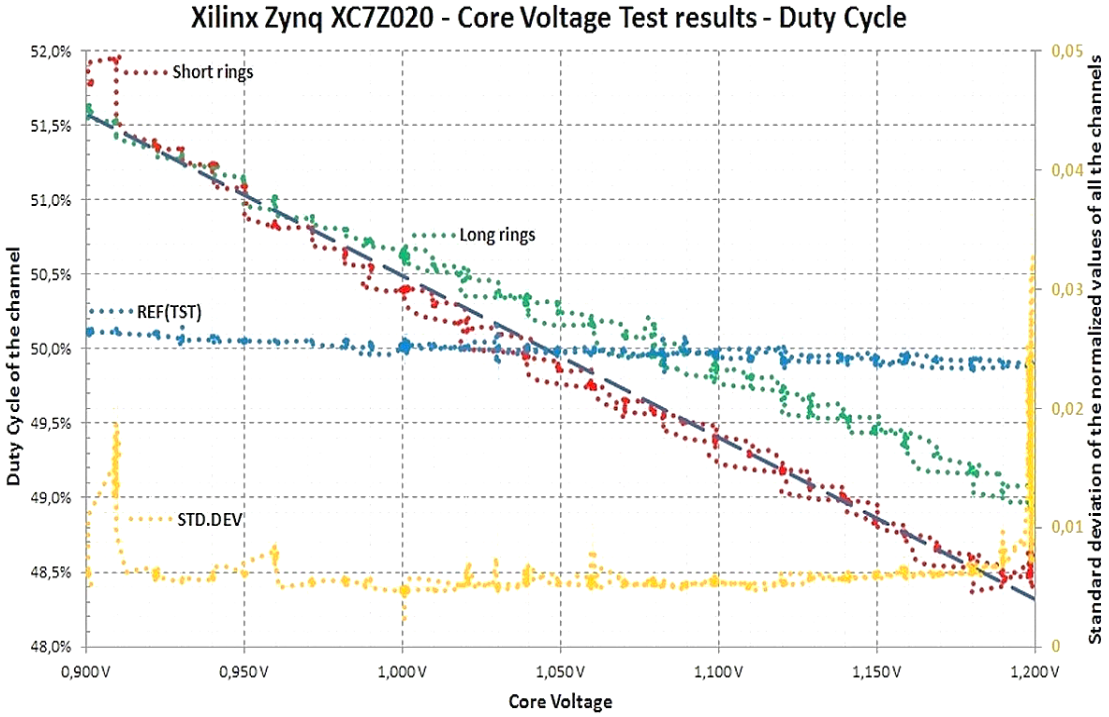


Figure 41. Duty cycle and detailed core voltage change results for 28 nm Zynq device.

Figure 41 shows the duty cycle results for the 28 nm Zynq device. The two curves for each sub-chart (ring) represent both modes of the core voltage change, when the voltage went up and when it changed back or below its nominal value. It shows that the device faces problems at voltages close to 1.20 V, which is above the recommended working condition range of the core voltage. There are also some minor problems with all the members of a set of rings close to 0.9 V. The board has disconnected when the 0.890 V level was reached. The FPGA device and the development board, or one of its key parts, obviously does not work below 0.900 V and does not work in entirely reliable way close to 1.2 V. These levels represent 90 %, or 120 % respectively, portion of the recommended nominal working power supply conditions, it means 1.0 V. It is a much, much narrower voltage band, than it was in case of the 45 nm Spartan device. The sensitivity coefficient or slope for the linear regression model of the fastest rings is approximately 0.1, with a negative proportionality to the core power supply voltage. It consists of many factors, including the gate threshold values, etc.

Figure 42 shows results of measurement of SLICE delays (device performance) within selected voltage ranges and for both platforms. The 28 nm Zynq device and the delay of its internal circuits is clearly more sensitive to FPGA core voltage variations than the previous Spartan 45nm technology node. In addition, the 2^{nd} order regression models and extrapolations indicate the limits of the devices. The real values of the limits were not tested due to the possible non-reversible effects and negative impact on the devices. However, the tests performed within the presented ranges show nearly fully reversible processes, where a short voltage stress lasting few minutes had a negligible impact on the FPGA devices measured.

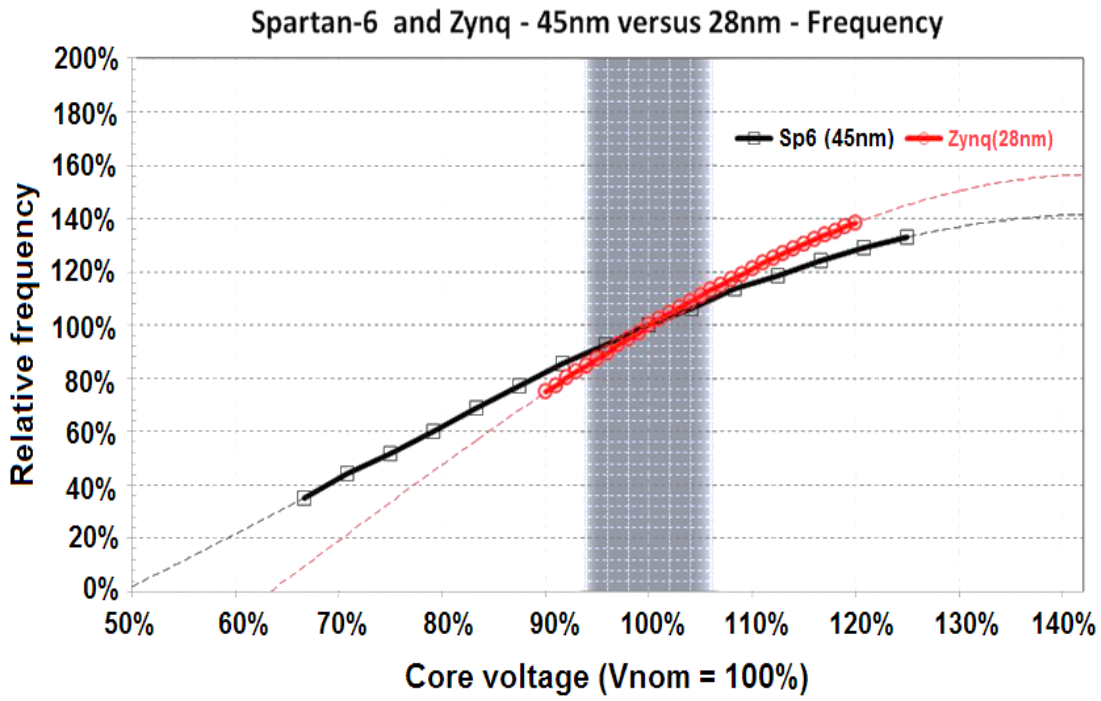


Figure 42. Comparison of both platforms for maximum working frequency with respect to the core voltage (the area in grey indicates the recommended working range by the FPGA manufacturer).

Figure 42 shows clearly linear models, applicable very easily within the recommended voltage working ranges according to the Xilinx datasheets. This 28 nm Zynq device is clearly more sensitive to voltage variations than the previous Spartan 45 nm technology node.

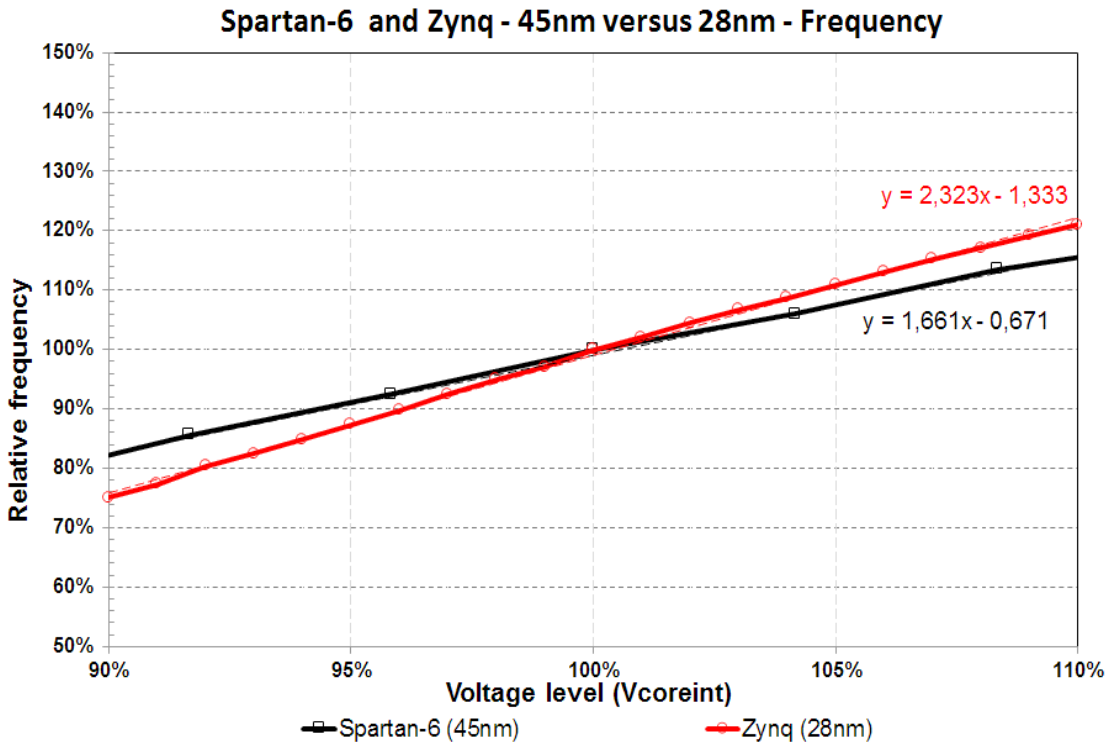


Figure 43. Comparison of both platforms with respect to the recommended working conditions in Xilinx specifications.

Figure 44 shows a comparison of both 28 nm and 45 nm low-power platforms for the overall design power consumption, however measured only at the core voltage power rails (V_{core} or V_{int}). One important fact has to be noted here, that the core voltage rail is not routed only to the FPGA device (please see the schematic diagram and other related documents), but also to one external device. Based on the modifications made to one board (the external devices were physically disconnected from the power rails), the measurement error caused by the mentioned fact was evaluated below 12 % of the total values. This is considered to be not significantly affecting the data and results presented in this document. The experiments were performed on 2 pieces of the boards for each technology (4 development boards in total) with measured differences below acceptable 10 % overall error.

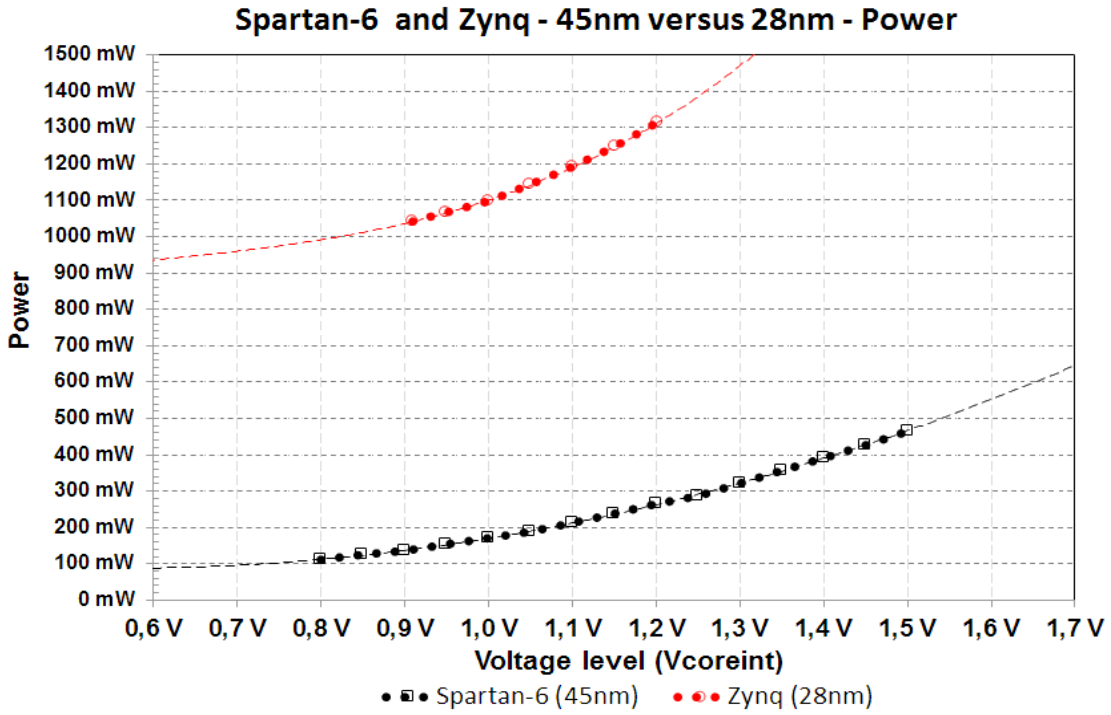


Figure 44. Comparison of both platforms for overall design power consumption.

It has to be pointed out that the ARM cores in the 28 nm Zynq were switched off during the test, ensuring measurement of the configurable logic part of the die at the maximum possible level. Also, the 45 nm Spartan is approximately a half of the 28 nm Zynq in term of the size of the programmable logic cells as well as all block memory cells available. Therefore the overall higher power consumption of the 28 nm Zynq device is not a problem. Also, the designs are not considered to be really typical ones in term of the device utilizations or design complexities. However, it shows the key result that the 45nm Spartan device is consuming much less power in a wider working voltage range and the 28 nm technology is more sensitive to voltage variations, as indicated by the charts in Figure 45.

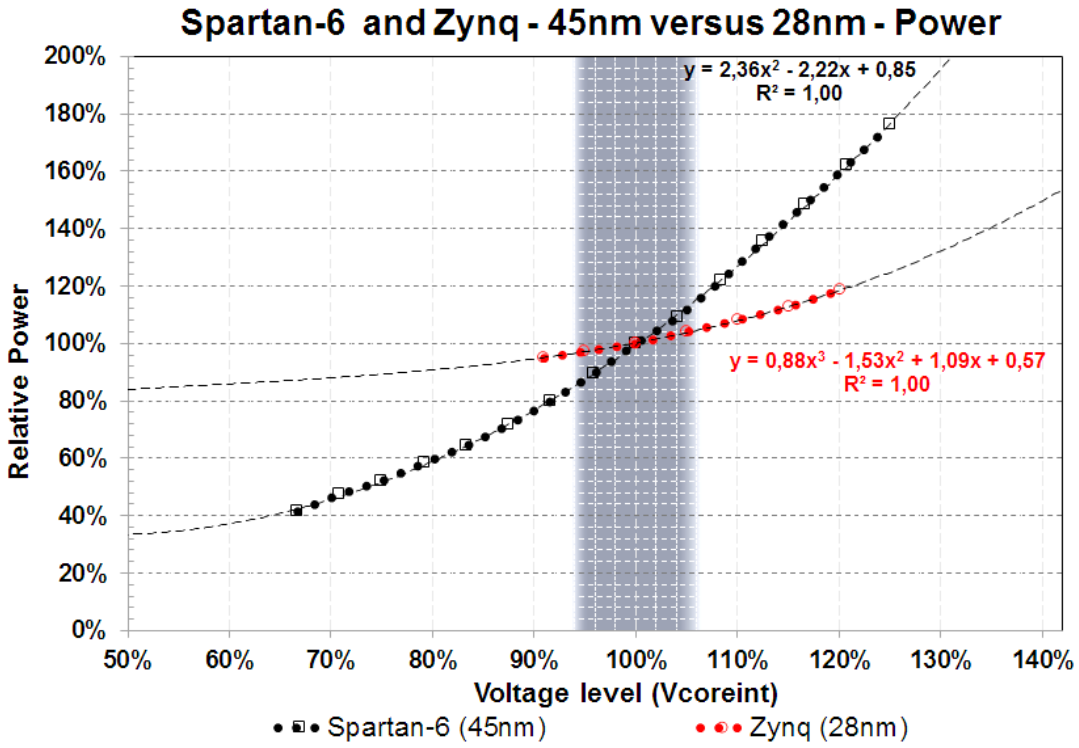


Figure 45. Comparison of both platforms for the overall design power consumption (relative measures).

The figure above shows also the models that can be used for behaviour modelling of such devices. It is obvious that 2nd order of regression model is fully sufficient to create very accurate models.

The next figure in this chapter shows one important result: running the 28 nm device at the initial core voltage value of 0.95 V can create key 30 % spare margin for future increase in the core voltage, in order to mitigate or compensate the aging effects in the FPGA structures and maintain the same device performance and speed of the design, internal structures and circuits. The corrected curve represents the original measurement data calculated back to the same temperature; the other one shows the original data and results including a small increase in the die temperature (see Figure 53).

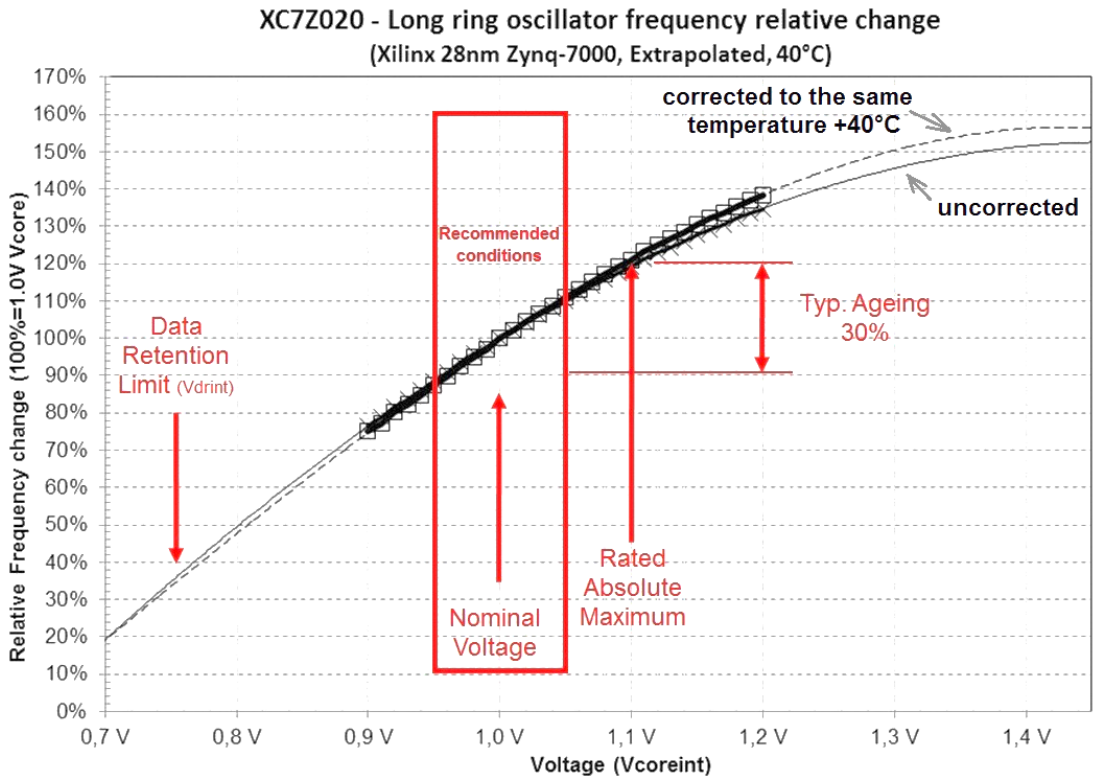


Figure 46. The maximum frequency relative change and key space available for mitigation of aging effects.

4.6.4 Measuring Degradation Processes and Aging in Nanostructures

The following lines show results from measurements performed under accelerating extreme conditions. As already discussed, temperature and voltage are the two basic acceleration factors, that can be applied to the integrated circuit and FPGAs in general very easily. It is obvious that the degradation and aging processes can be accelerated by these environmental conditions and therefore detectable or measurable within typically much shorter timeframe. This works well in case of older technologies [*14*]. However no similar tests and results are available for 28 n technologies.

During the tests, the device was cooled down or warmed up by a small low-cost thermoelectric element type TEC1, powered by a 5 A regulated power supply. Due to this

fact, it was difficult to reach lower temperature values below 0 °C. On the other hand, thanks to this point-type temperature control, no other devices were significantly influenced by the temperature changes and big temperature gradients, including the power supply circuits (please see the board layout files for more information).

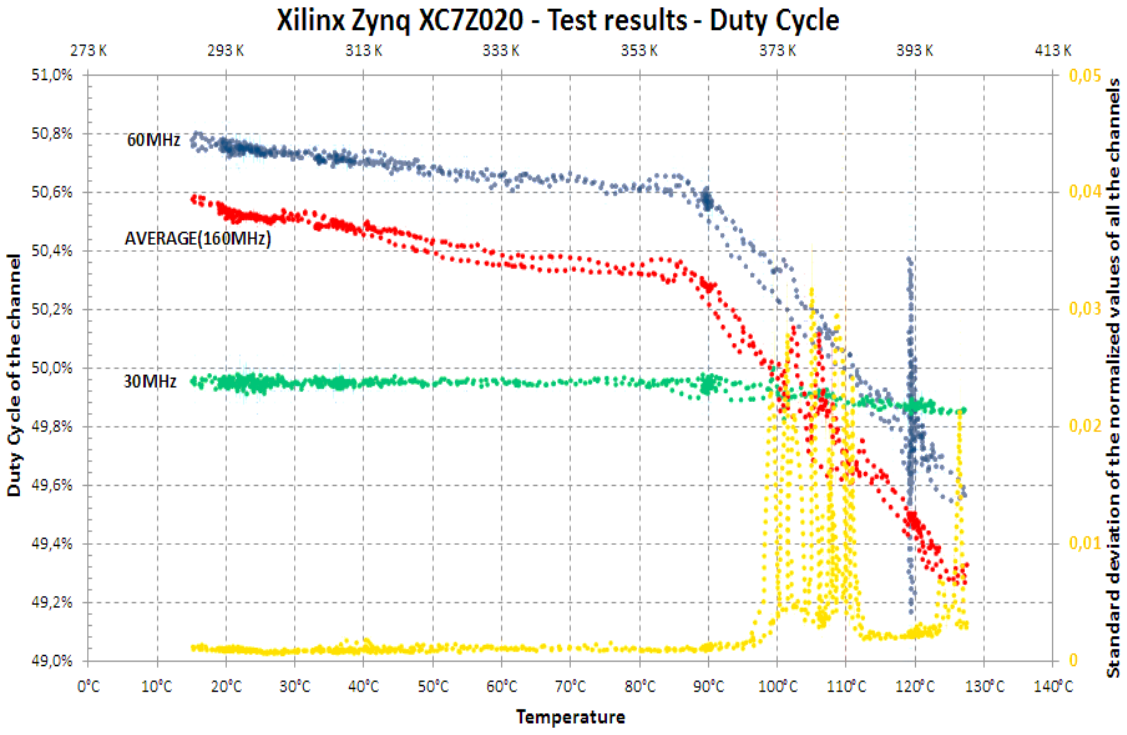


Figure 47. Duty cycle of ring oscillators with various lengths to the die temperature measured by BRAMs.

Figure 47 represents the results of measurement of duty cycle of the ring oscillators. The device used during the test is qualified for commercial temperature operating range from 0 °C to 85 °C. It is one the very interesting results the first problems start just at the temperature around 90 °C (360 Kelvin). The test were performed twice with different designs (running different set of rings) and only up to 115 °C. The result are very similar, problems start again at around 90 °C, only the duty cycle and frequency values are slightly different (the difference of the average values is below 0.05 %), because the rings consist of physically different cells at physically different location on the FPGA die. The chart

includes the stage delay value as well as the standard deviation all across the active channels.

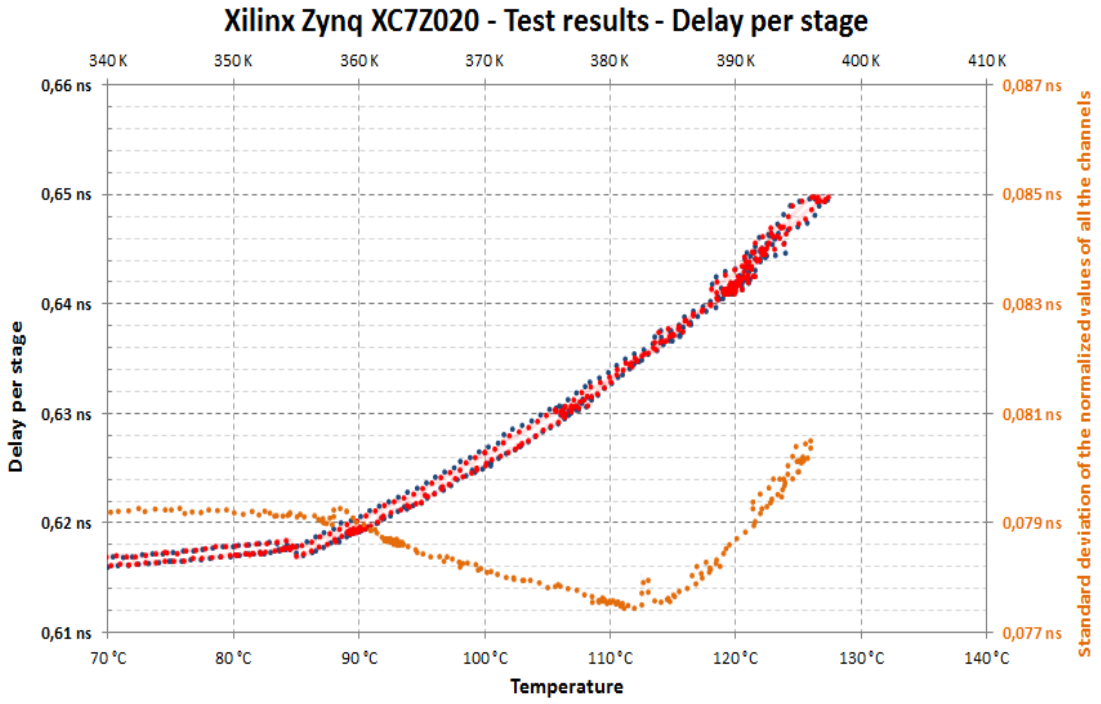


Figure 48. Delay per single stage of the ring oscillators to the die temperature.

Figure 48 represents the measurement of the SLICE delays with respect to the temperature. It shows average SLICE delays and hence frequencies of the longer ring oscillators with respect to the FPGA die temperature. It was found that the delay has increased in the range of 5 % of the base value within the device temperature range, and within 9 % within the extended temperature range. A very remarkable result is the change in the circuit behaviour above 85 °C. The chart again includes the stage delay value as well as the standard deviation all across the active fast channels. The standard deviation of the delays significantly increases above 110 °C. However the temporarily lowered value from 90 °C to 110 °C is difficult to understand. Anyway, in the case of lower frequencies, the delay of the stages goes up much faster from the temperature of 85 °C.

The test has fully validated the proper functionality of the device within the permitted device temperature range. However, it is obviously not possible to utilize such devices for measurements of aging effects under higher temperature as one of the two key acceleration factors (temperature and voltage). According to the Arrhenius law, only the acceleration factor of 2 or 3 can be safely reached with this device. When the power supply voltage is increased, much higher acceleration factors in the range of tens can be achieved.

It is obvious, that the duty cycle ratio below 85 °C goes down with the slope of approximately 0.01 % of the duty cycle ratio per degree of Celsius for the pure rings and higher frequencies. This rapidly changes for higher temperatures to the value of 0.025 %. The internal FPGA circuit faces serious problems with faster rings at 85 °C up, while slower 60 MHz rings were significantly affected at 120 °C. The lowest-speed rings at 30 MHz are somehow functional up to 125 °C. It also looks from the results that the problem is not in JTAG or BRAMs, because the data streams were consistent also in the blocks with shared low-speed and high-speed ring data streams.

As mentioned in the theory and description above, the novel differential method and approach presented brings completely new dimensions to measurements of extremely small changes caused by degradation processes in modern nanotechnologies and devices utilizing either high-power circuits or small feature size technologies. An example of measured aging in 40 nm and 28 nm FPGA nanostructures follows. Only the method presented allows measurement and determination of both the duty cycle and frequency of the differential signal between selected types of circuits. It includes NBTI and PBTI effects as well as relaxation effects in the paths. Figure 49 shows one of the first measurements performed on Virtex 5 family using 65 nm technology. Figure 50 shows the change in duty cycle measured on the 40 nm high-performance technology (Virtex-6 FPGA), representing a small shift in the transistor threshold levels. Figure 51 is related to a high-performance 28 nm technology (Virtex-7 FPGA) and it shows a change in relative frequency of ring oscillators running in different modes. It clearly shows that also the frequency of continuously running oscillators remains nearly the same (according to the linear regression model, a change of 10 % has to be reached in a period close to 10 years), while the rings held at level 0 (L) slow down much faster, reaching the 10 % decrease in performance within approximately 3 years.

Measurement of the duty cycle is omitted in most papers and methods, but is has direct relation to the threshold level. No similar results from 28 nm technologies have yet been published, but the models show results similar to the numbers available from manufacturers and other research works on purely transistor-based structures (e.g. works performed in imec, Belgium).

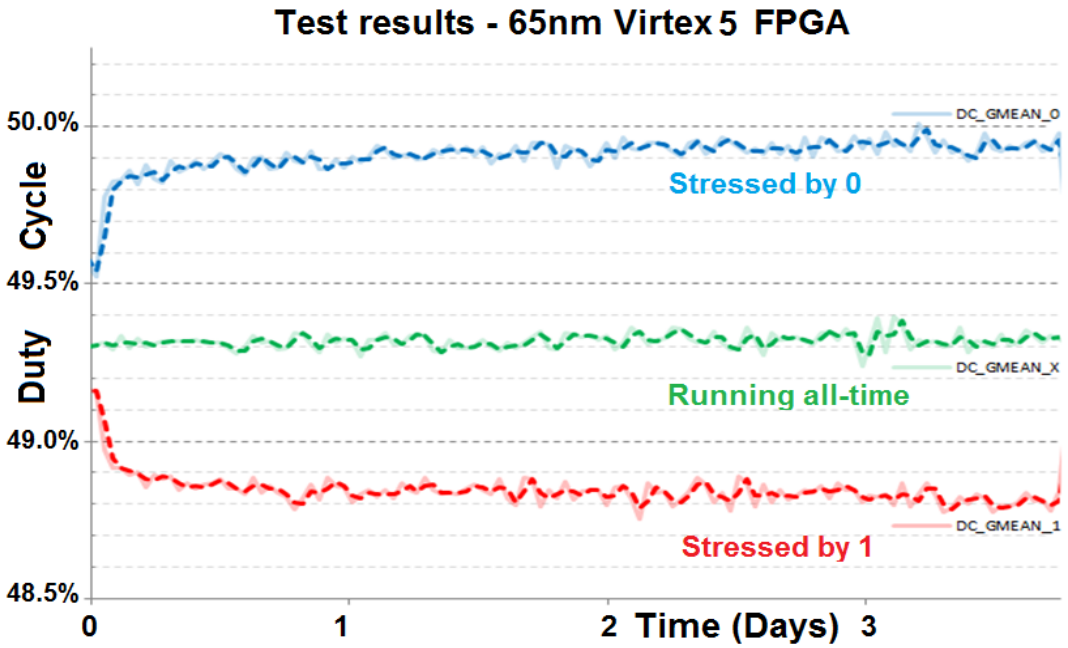


Figure 49. An example of the application of the reliability lab-on-chip methodology - BTI in 65 nm FPGA with V_{th} changes projected to duty cycle.

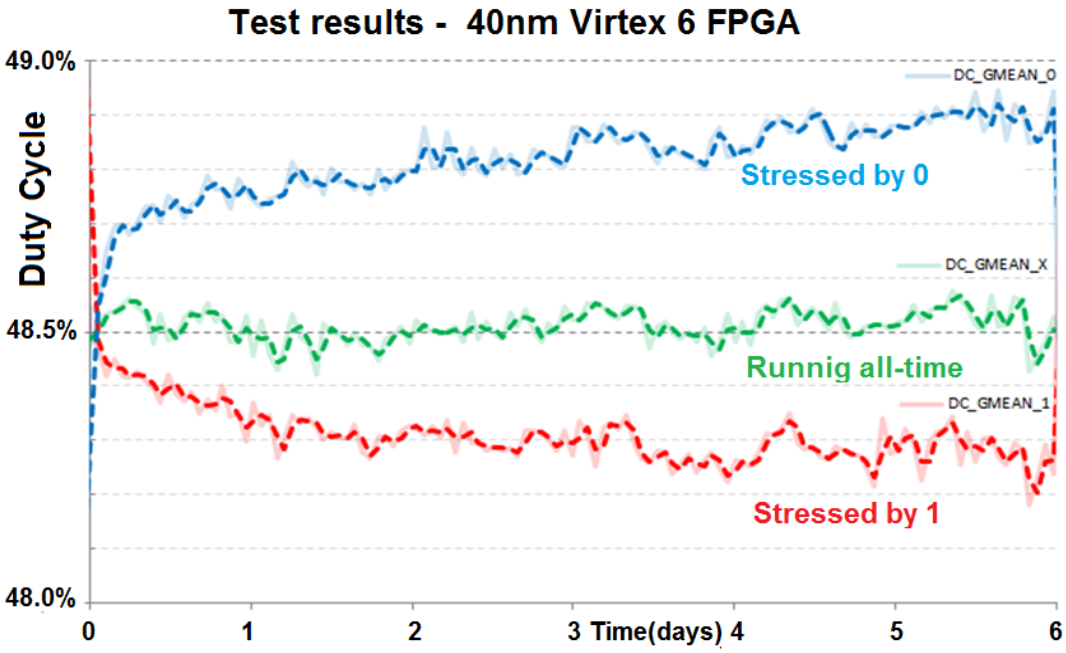


Figure 50. An example of degradation processes measured in 40 nm technology – change in the duty cycle.

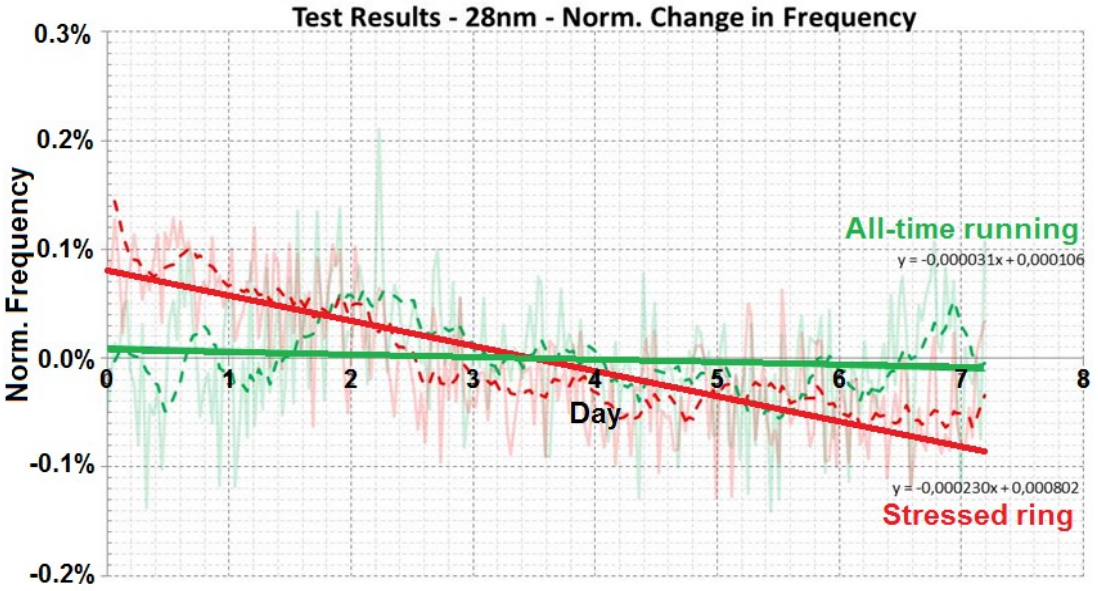


Figure 51. An example of degradation processes measured in high-performance 28 nm Virtex technology, showing relative frequency of ring oscillators working in different modes.

4.6.5 Other Results and Data Collected in Measurements and Experiments

The overall results are typically presented as the average, or mean value, calculated across the members of the set of ring oscillators in the same mode. There are typically 3 basic sets of ring oscillators: continuously running ring oscillators, rings held at L level and rings held at H levels for most of the time and measured momentarily once an hour. Any rings oscillations or fast level changes in circuits act as a kind of relaxation process to the nanostructures, field-effect transistors and related paths. Therefore the measurement processes must be very short, typically only 1 ms in most of my measurements. The charts Figure 52 show the key and important fact that all members of the 3 basic sets of ring oscillators and paths behave in the same way; no exceptions even after changing the mode or after a relaxation event were observed. It also validates the new method presented in this document. Such behaviour of all sets of ring oscillators is checked in all measurements.

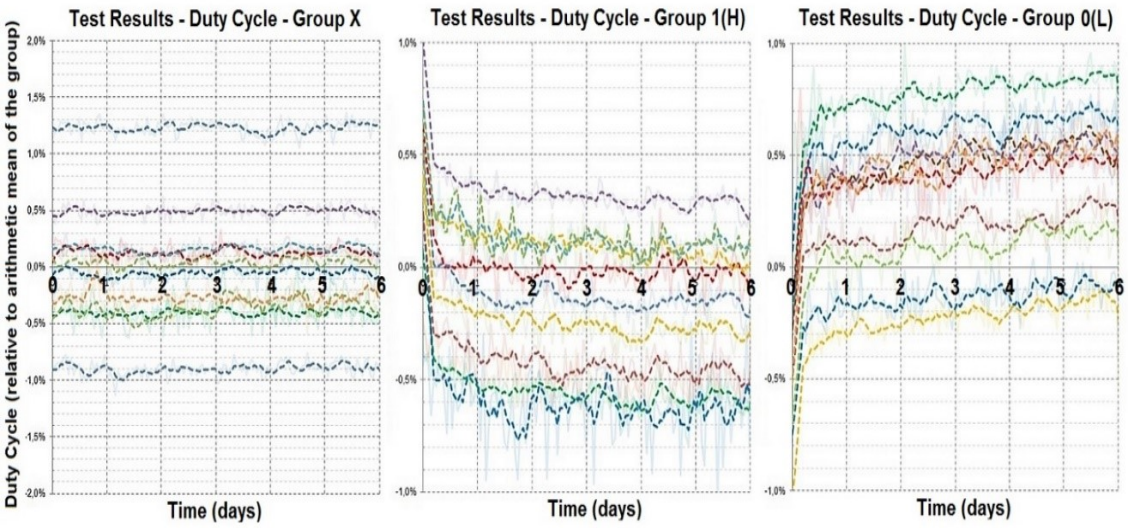


Figure 52. An example of unrolled results of members of the measured groups of ring oscillators – all rings in the group behave in the same way.

As mentioned above, the measurement results also consist of core voltage, currents, and die temperature measured as well as processed data from BRAMs, available as CSV files. Also actual date, time, duty cycle and frequency ratio values are included in the files. Figure 53 shows an example of the collected data from one of my experiments.

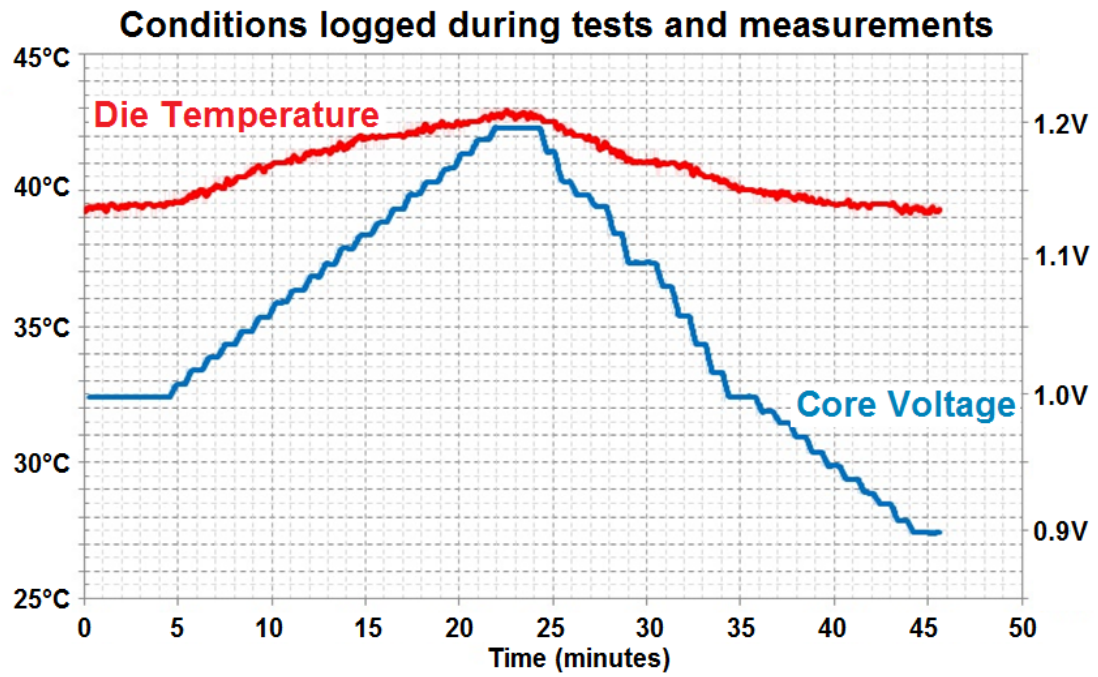


Figure 53. An example of the log data during the measurements and experiments.

Figure 54 shows the relation between the internal core voltage and temperature measured, based on data available from the XADC block. The experiment was carried out within a wide temperature range from 15 °C to 130 °C. This experiment has shown, what the real "quality" of the XADC block is, and how wide the usable temperature range is in case of the key temperature measurements. One can clearly see that the relationship is not fully linear, as it should be according purely to the theory. It is caused mainly by increasing leakage currents. However, the results are fully within the device specification range as mentioned in the Zynq-7000 All Programmable SoC datasheet, a ±2 % error for the extended temperature range is shown.

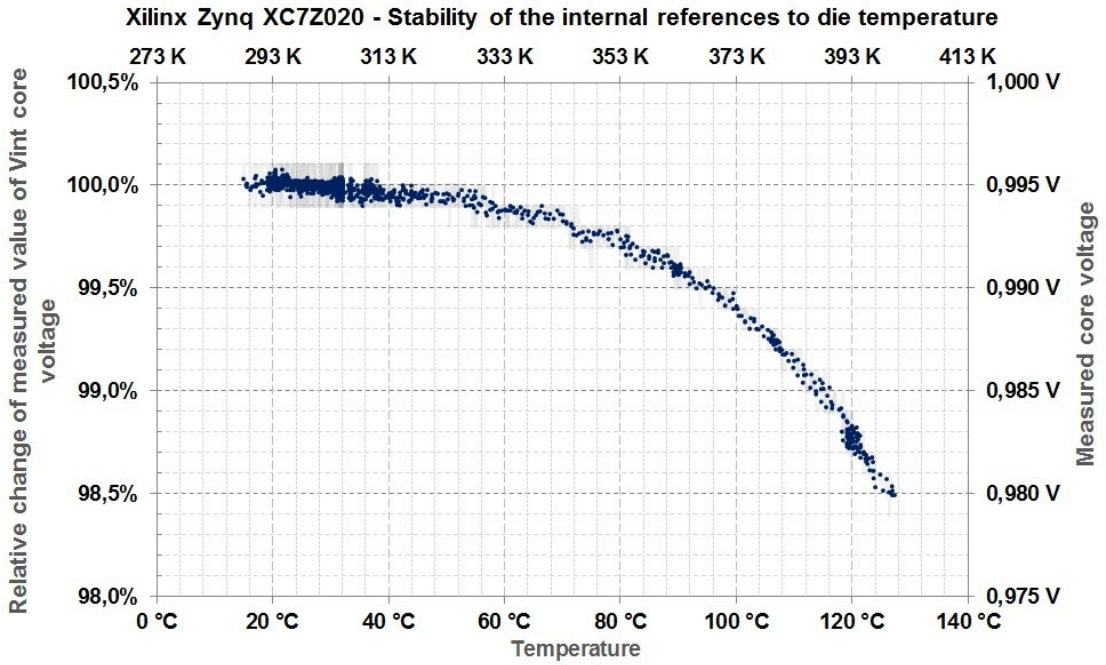


Figure 54. An example of leakage measured in one of my previous temperature-related experiments.

4.6.6 Conclusions

The results show that the 45 nm Spartan allows lower power consumption under acceptable performance, compared to 28 nm Zynq device. On the other hand, the latest 28 nm Zynq device incorporates also two ARM processor cores, while this part of the chip can control the rest of the chip and the programmable part can be completely switch off. It can result in better overall power-consumption results, while the device offers higher peak performance of the programmable part, while saving FPGA resources, required for a standard implementation of a selected soft core. The results also show important voltage ranges for each technology, which can be used in other experiments or designs, while presenting corresponding values in terms of FPGA device performance and power consumption.

The original idea was to better understand the real internal structures including the latest generally available 28 nm FPGA technology and their parameters including changes under various conditions. The comparison to the previous 45 nm technology node is also unusual information. The values obtained are important for proper simulations and modelling or estimations of the design parameters in FPGAs and other VLSI products utilizing similar technology and nanostructures. The results presented can also be used for evaluation of the impact of aging, degradation and electromigration processes on the final design. Aging effects - aging (bias temperature instability, time-dependent dielectric breakdown, etc.) and the models can be supported by the new data presented on the low-power platforms. They can also be utilized in reliability estimation processes and λ or design's final reliability evaluation phases of MTBF (Mean Time Between Failures) or MTTF (Mean Time To Failure) parameters. The results further be used for various purposes in performance optimizations, not only in dependable, automotive, transportation, medical or security systems, but also for example to suppress security threats, where the detailed knowledge of system delays and behaviour under various conditions, such as temperature, voltage and load, can re-create some of the internal structures, even if the configuration stream is encrypted. The results presented in this document also clearly show the limits of the technologies and the impact on the useful range of the accelerating factors.

The results presented confirm the information rarely presented by the manufacturer: The on-chip FPGA temperature measurement by the XADC unit is used for critical temperature warnings and also supports automatic shutdown to help prevent the device from being permanently damaged. The on-chip temperature measurements record the junction temperatures continuously during pre-configuration and automatic shutdown. For configured devices, the on-chip temperature measurements are enabled and on by default. There is a user alarm signal available: the alarm signal ALM [0] is high when the device temperature exceeds the limit in the temperature upper control register 50h (80 °C default). The alarm signal ALM remains high until the temperature falls below the lower threshold, temperature lower (54h) (70 °C default).The fixed internal signal is used by

the FPGA internal HW units and circuits and it is active starting from the maximal permitted working condition temperature level (85 °C default).

The results presented in this document have obviously and fully validated the new proposed methodology and demonstrated its desired quality. The clear advantages of the presented method and solutions in modern designs have been shown as well. The method itself, ways of utilization of dual-port BRAMs as well as data processing algorithms are suitable for applications in modern processor or multicore systems. The method presented is continuously being improved and some of the technology derivatives are protected (patents pending). Please contact the first author for more details. However, the main framework for the basic easy measurements and tests is to be developed as an open source project with a broad availability to as much as widest range of research as well as industry applications and use.

Chapter 5

5 Delay-Fault Run-Time XOR-less Aging Detection Unit using BRAM in modern FPGAs

The reliability issue, including aging processes in modern devices with very fine structures and utilizing programmable technologies, being applied in high-performance or dependable systems in various safety, automotive or space applications, is sometimes very difficult to predict, measure or watch. The task is well-mastered in the world of ASIC, the situation is slightly different for FPGA devices. Modern FPGA devices incorporate number of true dual-port memory blocks with 8-T cells, hence offering new options. However, such blocks are typically used for data storage and processing purposes. This chapter presents my completely new solution as a new way of utilization of the RAM block (BRAM) for the delay fault detection purposes. The BRAM and a simple controller log risky transitions or delay fault events and may positively affect the overall reliability of the device as well as all the system.

5.1 Introduction

The aging of the electronic nanostructures, as well as the most of the generally negative internal changes due to various physical mechanisms, causes changes in parameters of CMOS structures; PMOS transistors are more sensitive than NMOS. It typically results in changes in the gate threshold levels or interconnects (electro-migration). These changes also result in lowering of the maximal drain current and cut-off frequency, elongating the processing delays in the aging-affected circuits (compared to the original design). An overview of the aging issue and solutions in FPGA can be found e.g. in [*124*], the degradation analysis can be found in [*14*], interconnects delay issue is described in [*125*]. In case of dependable systems, the key parameter lies in the negative changes in delays

of critical paths. The system failures due to such negative effects must be avoided. Hence, all the critical changes have to be detected, in the ideal case the given or sufficient time before it results in the system failure.

One of the possible solutions is to measure changes in internal structures, typically propagation delays of selected signals with automatic detection of events above given limits. As long as the timing requirements of all paths are correct, lowering maximal working frequency of transistors or structures doesn't affect the overall reliability of the circuit or system. Aging stays visible and causes problem only if the propagation delays in implemented logic path exceed the given values.

The usually used technique of detection of the timing violations is to generate another auxiliary clock signal and sample the end of the critical logic path twice with a short mutual delay. It means to sample the output of latches or D-Flip Flops (DFF) of selected paths at two (or more) time points around the original (global) clock rising (or falling) edge, and compare all the output values, typically by XOR gates. In critical paths and during work of dependable systems along their lifetime, no any change of the output of the logic part of the design (routed to the DFFs input) is permitted within the given setup and hold timing constraints [*85*] and [*86*]. When the output values differ, one (or more) of the first in line latches or other DFF has probably sampled a wrong value. It means that a metastability or SET/SEU (Single-Event Transition/ Upset) has occurred. If signals with those wrong parameters are propagated in the system or processed by following circuits, it may cause wrong functionality of the circuits or device. It directly influences the internal functionality and reliability of the dependable system.

In order to prevent such negative system behaviour, many special or auxiliary circuits can be designed in ASIC. However, the exact implementation of such circuits in FPGA (i.e. devices with already fixed set of basic or available structures) can be very difficult, not only due to the complexity of the internal interconnect mesh, but also due to many internal structural or timing limitations (e.g. low-order filters implemented in the FPGAs).

5.2 Description of the Proposed Solution

It is very difficult to find papers or previous work about aging detectors using BRAMs, as well as other results from this area in FPGAs. However, the work described in [*126*]

shows sufficient stability of the internal FPGA structures, including the front DFFs of the BRAM blocks (see [*72*] or [*71*] for all details). As mentioned, the BRAMs are typically used for data storage or processing purposes. However, the BRAMs in modern FPGAs offer many new options, they have been improved (see [*72*], [*71*], and [*127*], and their reliability is similar to the rest of the chip area of devices nowadays, for example [*43*]). In addition, high-quality externally-inducted-SEU-free devices (Actel, BAE, and other military grade devices) already exist, while one of the biggest issue – aging effects – remains and gains with lowering of lithography technologies.

Figure 55 shows the basic idea of my new solution. It is obvious, that it is only an extension of the standard solution, while the delay-fault detection DFF is replaced by the BRAM resources, already containing very well synchronized DFFs in the front stage unit (described in [*71*], [*72*], [*85*] and [*86*]). Moreover, this my solution doesn't incorporate any XOR gate to be added to the original design. During the implementation of the presented solution, it was found that the interconnect network delays (NET), in the CLBs and crossbar switch arrays, are in the desired time range. The clock distribution network and paths are quite well designed. And in some cases, only the delays of interconnect paths can be utilized. The final solution should avoid a must of processing of data stored at different rows (memory address or sampling time). The already latched signal (output of the BRAM) is routed back to the BRAM and latched again in the next cycle. It ensures the desired time independence of rows in the memory. It is obvious, that this approach and way of implementation in fact completely isolates all the events. Each memory address location (row) and data in the BRAM can be processed as fully separated events. The XOR operation is performed by the CPU operation. However, the memory locations can be written and read fully asynchronously, while no any extra read cycle or existence of the previous corresponding data is required.

The detailed timing parameters of the final design can be obtained from the design analyses, or results from PlanAhead (or any other tool), or it can be measured as well. For the direct measurement purposes, it is required to implement only one diagnostic signal, in the best case allowing generation of periodical signals in the critical path. Some systems already incorporate such feature for self-checking purposes; thus no any other signals are required. The signal must be generated fully asynchronously to the clock signal, or synchronously with well-defined L and H widths, jitter or time delays, allowing

calculation of the aging detector unit parameters. The tests performed with fully asynchronous signals clearly showed, that the results are surprisingly very stable, and in the required range of tens or hundreds of picoseconds.

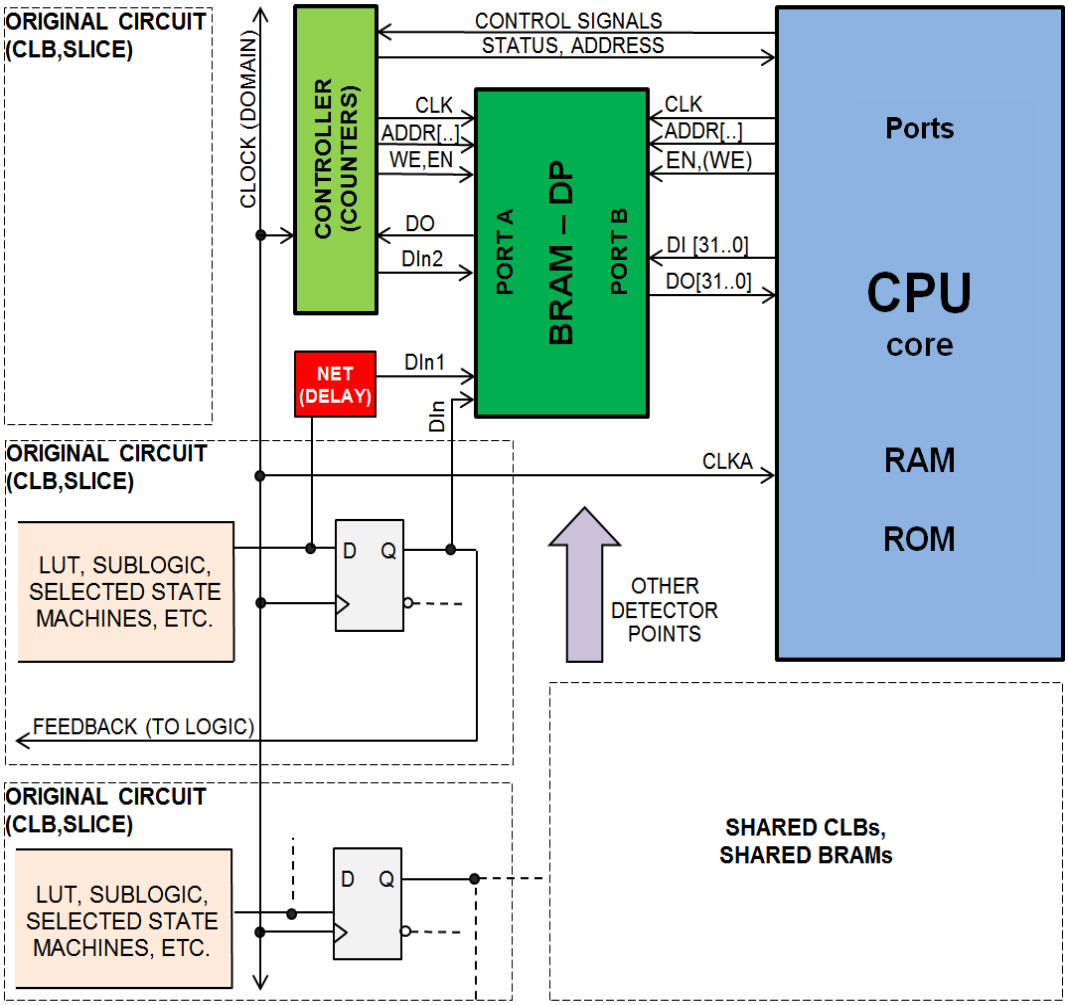


Figure 55. Main idea of the new solution (no XOR gate is required)

5.3 *An Example of Implementation*

Figure 56 shows the simplest implementation of the solution. It presents only the main idea. The virtual zero delays are never present in any real system. The simplest solution gains just from the existence of significant interconnect delays. The delays must be determined or designed in order to setup required delay sensitivity. This complex solution can be insufficient in some systems, but many systems can utilize just this simplest solution. It was previously validated on the test systems (with Xilinx Spartan 6 and Virtex 6 FPGAs), that the interconnect delays can be quite short in the range of hundreds of

picoseconds (with subsets in tens of picoseconds), depending on the type and length of interconnect. These delays are fully sufficient to cover setup/hold times.

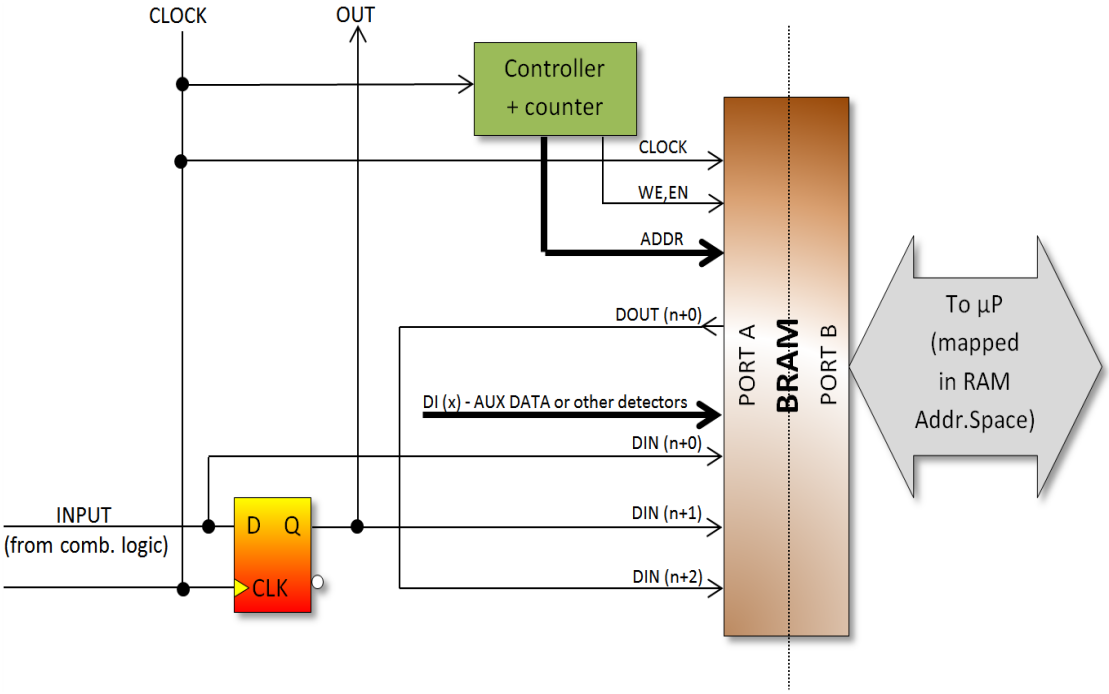


Figure 56. The very minimal version of the proposed detector – no any SLICE or CLB resources are used for XORs

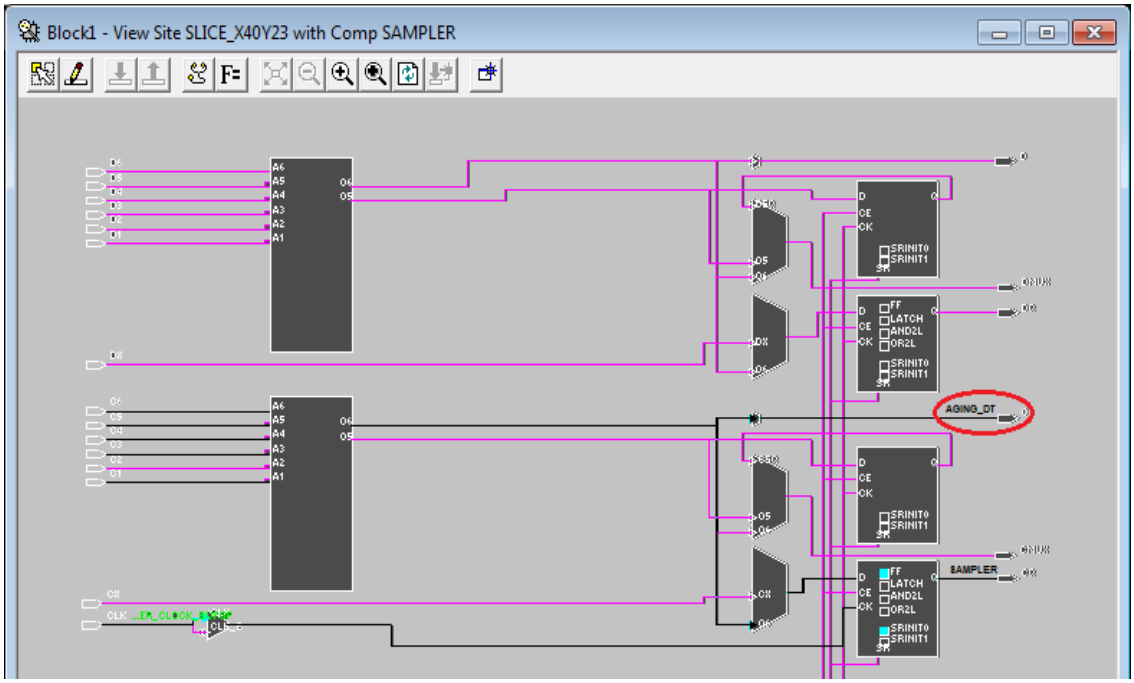


Figure 57. The proposed aging detector can be easily implemented into already existing designs in Xilinx FPGAs

Figure 57 shows an example of the real implementation of the presented solution in a standard design. In the following test and its description, the end of the critical path is named AGING_DT and the final DFF is named SAMPLER. The example in Verilog (this language description can be found in [*70*]) utilizes one BRAM block in the 4Kx4 BRAM in the true dual-port configuration and WRITE_FIRST mode, as follows:

```
reg [3:0] memory [4095:0];

reg [3:0] DOA;
reg [3:0] DOB;
always @(posedge CLOCK)
 begin
  memory[ADDRA]={0, DOA[0], SAMPLER, AGING_DT};
  ADDRA = ADDRA + 1;
  DOA = memory[ADDRA];
  if (CPU_WRITE_ENn == 0)
                memory[ADDRB]= CPU_DB[3:0];
  DOB = memory[ADDRB];
 End
```

`ADDRA` (port A) is reserved for the aging detection block and it is expected, that the address of the stored data will be only incremented. It results in very simple implementation of the solution. In another design, now under testing, it allows memory segmentation techniques, it means a way of data pre-processing, based on the previous results calculated by the CPU unit. The port A can be synchronized with Port B in some (optimal) case. `ADDRB` denotes the CPU side of the dual-port RAM.

5.4 Results

The proposed solution was tested and validated on Xilinx FPGAs: Digilent's Atlys Spartan FPGA Development board, incorporating a 45 nm Xilinx Spartan®-6 LX45 FPGA device in a 324-pin BGA package on the board, and a single 100MHz clock source[12]. In addition, some tests were done on a ML605[13] board with a 40 nm Virtex-6 device. The boards were connected to a standard PC via USB (JTAG). No any other device or special equipment was utilized or required. The standard ISE Design Suite 13.4

[12] http://www.digilentinc.com/Products/Detail.cfm?Prod=ATLYS

[13] http://www.xilinx.com/products/boards-and-kits/EK-V6-ML605-G.htm

(64bit version) from Xilinx was used. A set of short supporting software for the final data processing was written in GNU C/C++.

Table 5 shows an example of data obtained during the tests. *AGING_DT* column is the sampled aging output, *SAMPLER* is the sampled output of D-Flip-Flop or the output latch, already existing in the original design.

Table 5. An example of the detected risky transitions by my proposed XOR-less aging detector

Address @	AGING_DT @n	SAMPLER @n	AGINT_DT @n-1
n+0	1	1	1
n+1	**0**	**0**	**1**
n+2	0	0	0
n+3	0	0	0
n+4	**1**	**1**	**0**
n+5	1	1	1
n+6	0	1	1
n+7	0	0	0

The key point of the solution is that the CPU has to check only the data consistency of the last two columns – both must be identical. This is fully asynchronous to the CPU performance; the columns must be same at the same memory address location and at any sample time for years; otherwise a delay fault is detected. The data consistency between the *AGING_DT* column at *(n-1)* and at *(n)* position (the first and the third column) should be also kept at any time, naturally only when the logging is off. Data inconsistency may occur very often during asynchronous access of the detector unit and CPU (<1% in my test system). Finally, the table shows two examples of the suspected changes, when the data has changed very close to the clock domain. It is obvious, that the *AGING_DT* signal has changed or was not stable a short time (<1ns) close to the previous clock edge [n+0],

during 1→0 transition, resp. 0→1 transition in the 2nd case. The parameters of the implemented solution (in the steps set by the used architecture) can be adjusted by special constrains, put on the optimal placement of the utilized BRAM, while only interconnects can be rerouted.

5.5 Conclusions

This proposed novel and unusual delay-fault detection unit with extended analysis and pre-processing purposes was presented during 13th Biennial Baltic Electronics Conference BEC2012 in October 2012 in Tallinn, Estonia. This XOR-less aging detector uses the standard approach for detection of delay faults, but by the innovative exploitation of the very standard part of modern FPGAs. The presented solution has obvious advantages, like easy implementation to an existing design, where a CPU core is already used (actually very often in modern designs), and the CPU address space can be very easily extended of the block RAM detector unit. The CPU can analyse the data in background, during its spare time, with no hazard states with respect to the CPU read/write cycles (both sides can be synchronized with same clock domain). The memory address of the event allows determination or estimation of the time, an equivalent of timestamps, and hence estimation of the event occurrence. The Duty Cycle (or 1/0 ratio) can be very simply calculated from the data, also the impact to the PMOS/NMOS or other structures can be estimated (aging). In addition, all the DFFs in BRAM are optimally synchronized. On the other hand, the usage of BRAM has also obvious disadvantages, like increase in the overall power consumption and suitability preferably for long critical paths; too short paths can be too fast to fulfil the BRAM timing requirements.

The future work lies chiefly in detailed tests of my solution under various temperature and chiefly voltage variations, testing of the solution with various processor cores, covering also optimal applications in special CPU cores, VLIW cores and multicore solutions.

Chapter 6

6 Integration of the Solutions in Complex Systems

This chapter shows a ways of utilization of the methodology a solutions developed and presented above in this document into various complex systems. This chapter contains partly and is also based on a very wide work performed in strong cooperation with my colleagues from other international research teams, especially the one in Germany.

6.1 Memory Segmentation

Various methods of memory segmentation creates a perfect base for an efficient incorporation of this new solution into existing processor systems. Figure 58 shows an example of it. A processor system uses 4 memory blocks of memory (16KB in total) for RAM purposes. Two upper blocks are used purely for RAM and data storage. The two lower blocks are used wither for data or for measurement of internal circuit parameters. The block selection signal enables one of two used blocks for the measurement activities. In addition, the block can be selected automatically when a fault or any special condition is detected. The processor system typically analyses the other block to the one used for the measurement purposes at a given time.

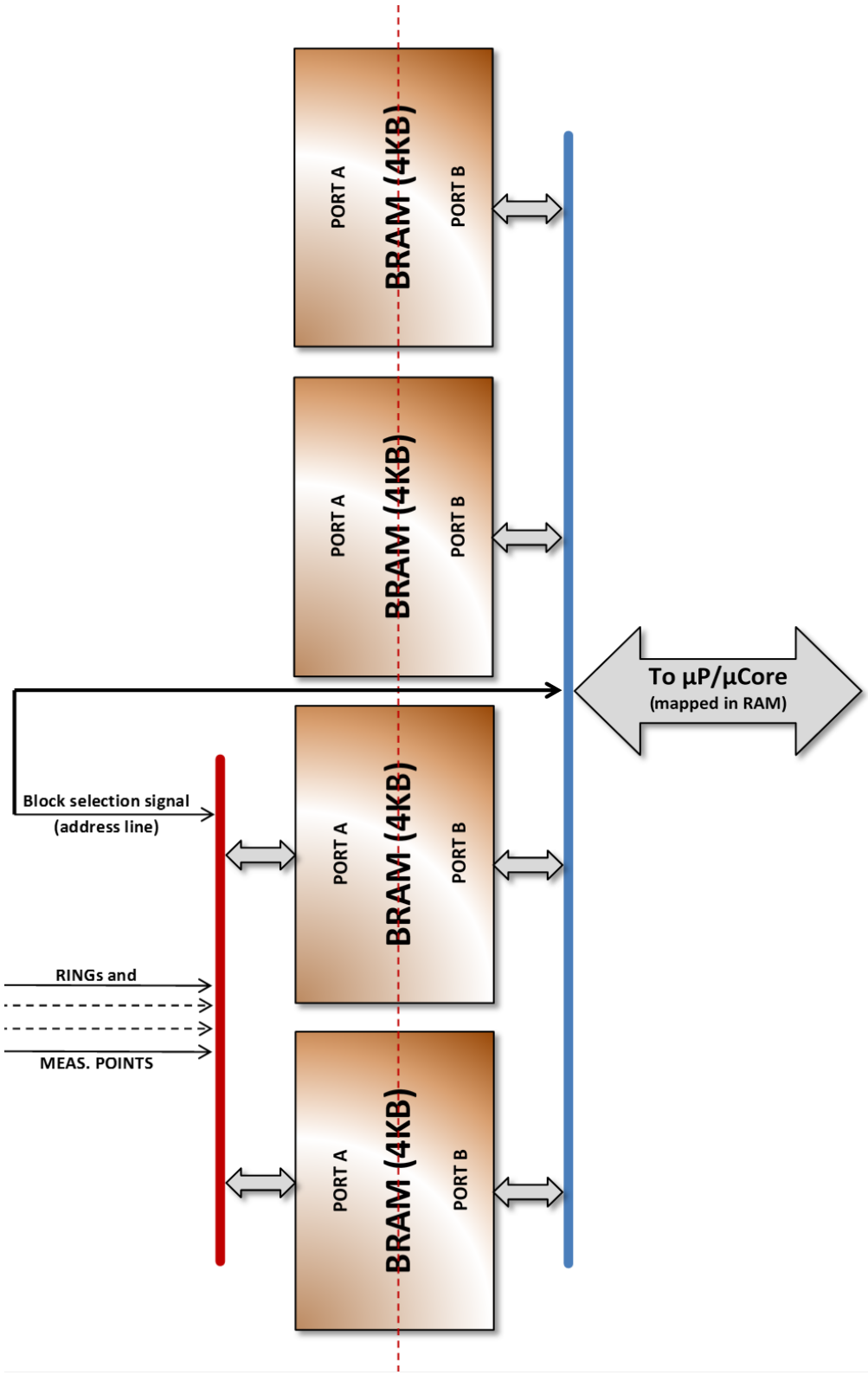


Figure 58. An example of an efficient memory segmentation scheme

6.2 Fitting FPGAs under Constraints

Test result, circuit and logic configuration reproducibility and detailed structural analysis is an important requirement. Therefore, **constraints and placement directives are used in FPGA development systems in order to specify the exact circuit and transistor layout** of a given test configuration and ensure test circuit exact reproducibility.

6.3 Parameter-aware Placement

One of key aging mitigation technique lies in better analysis of a given architecture, solution, design and the exact implementation in a selected microelectronic device or system. The very basic idea is that one can detect the critical paths that will age faster than the rest of the system and such paths are also crucial components of the system or the ones influencing the overall dependability of the system. After this key analysis and identification of the key circuit, paths and components, the final platform and chip is analysed completely. As one of the delivered results, a list or a matrix of delay of CLB or SLICEs in each single given chip is evaluated. The final implementation and/or data can also be adjusted in order to analyse exactly the crucial components of the path as they is to be implemented or fitted in the final design and FPGA. After such measurements and analysis, a set of constrains for a given FPGA device is generated and the system fitted and placed into the final product in the way that the crucial parts will be located in the fastest structures or locations of the die. The rest of the system is fitted and placed into remaining areas in order to fulfil rest of given timing and other requirements. One can expect that such optimized parameter-aware placement will result in longer lifetime and positively impacts the overall reliability of dependable systems.

6.4 Configuring and Utilizing Programmable Chips in Details

The following ones are the main approaches and ways of utilization of the programmable circuits and FPGAs with respect to the chip life time (the ideas are applicable to any fully programmable structure):

1) The chip is configured and utilized entirely during the production phase of the equipment, or during special service short time-frames. The ring oscillators are spread across all the chip utilizing all or near all logic resources. After this step, the chip is filled with a fixed or optimized configuration bit stream in order to create the desired original equipment functionalities. The optimized configuration stream can be generated in order to place the most design critical parts at the fastest chip locations and hence to create timing spaces for aging or other reliability assessment purposes.

2) The case (1) can be executed on demand or during specified equipment maintenance time frames. In this case, the following principle in Figure 59can be effectively used; during the design phase, the entire chip is utilized in more different modes in such a way, that the first part performs desired function, while the second one can be configured and measured. At specified time, these two areas simply exchange their functionalities, or the measuring subpart travels around the chip configuration area. In real application and in chips allowing partial reconfiguration, this feature can be realized by a set of already prepared configuration streams for the desired programmable areas.

3) The chip is configured and performs its desired function. The measuring parts and detectors are directly incorporated into the entire design at selected key or critical places. This new approach and solution enables the key feature: the original design stays completely untouched and the new measuring parts are routed utilizing only the interconnection resources to BRAMs. However, the final measurement or detection capabilities can be limited by the original design.

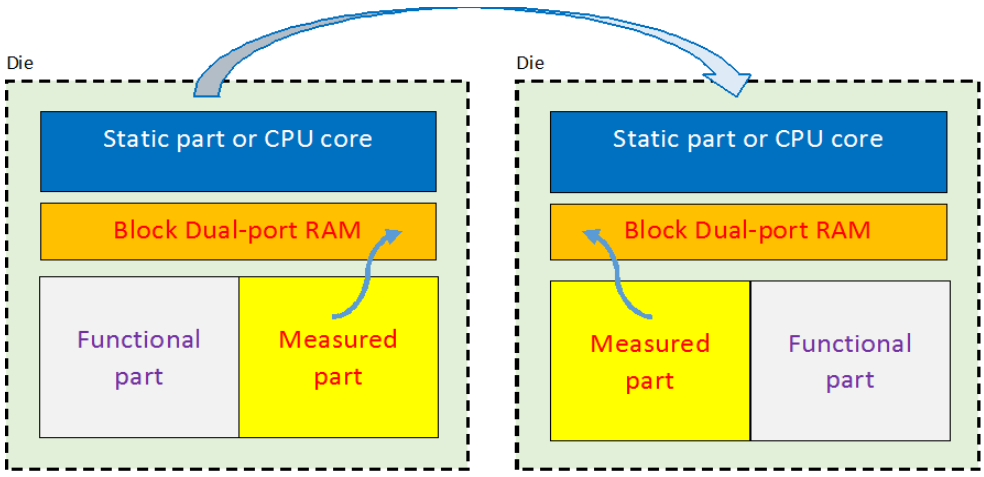


Figure 59. The entire area and circuits of chip can be measured using partial or dynamic reconfiguration.

6.5 *Altera and Xilinx FPGAs in Complex Systems*

Very long instruction word (VLIW) processors have some properties that make them attractive for the use in embedded systems. Although such cores have simple control logic, they provide relative high performance thanks to the burden of parallelizing the code is shifted into the compiler. It was my pleasure to stay in our partner university site in Germany, where me and my colleagues from BTU Cottbus have performed many interesting experiments. We have already presented a VARP VLIW solution in [*66*] and [*67*], allowing complete, extremely easy and low-cost implementation of the method into soft-cores on many Xilinx and Altera platforms. We have used the VARP-Architecture (VLIW Architecture for Research Purposes). This is a simple and scalable VLIW core with a 16 bit data path.

The following experiment is intended to the study of implementation of complex systems and impact to the overall system performance, when implemented in different configurations or platforms.

Tables and figures below show the results of the post-routing (final) timing models at 85 °C and the fastest FPGA grades. The low-cost FPGAs are shown in different locations, because these types were not designed at same technology nodes, except the 90 nm and the last 28 nm ones.

6.6 Technology Scaling Experiment

In this experiment, the VLIW processor is designed as exactly 4 issue slot and 4 execution unit core. The following table shows the main results for both the key platforms - Xilinx and Altera FPGAs.

Table 6. The maximal frequency of the VLIW processor (4 issue slots and execution units) in XILINX and ALTERA.

Technology	XILINX Virtex	ALTERA Stratix	Xilinx to Altera
90 nm	119 MHz	105 MHz	+ 13%
65 nm	154 MHz	151 MHz	+ 2 %
40 nm	193 MHz	147 MHz	+ 31 %
28 nm	197 MHz	171 MHz	+ 15%

The following figure shows the table data in a better way and also for the low-power low-cost FPGAs, where the technology nodes do not match between both Altera and Xilinx FPGA manufacturers.

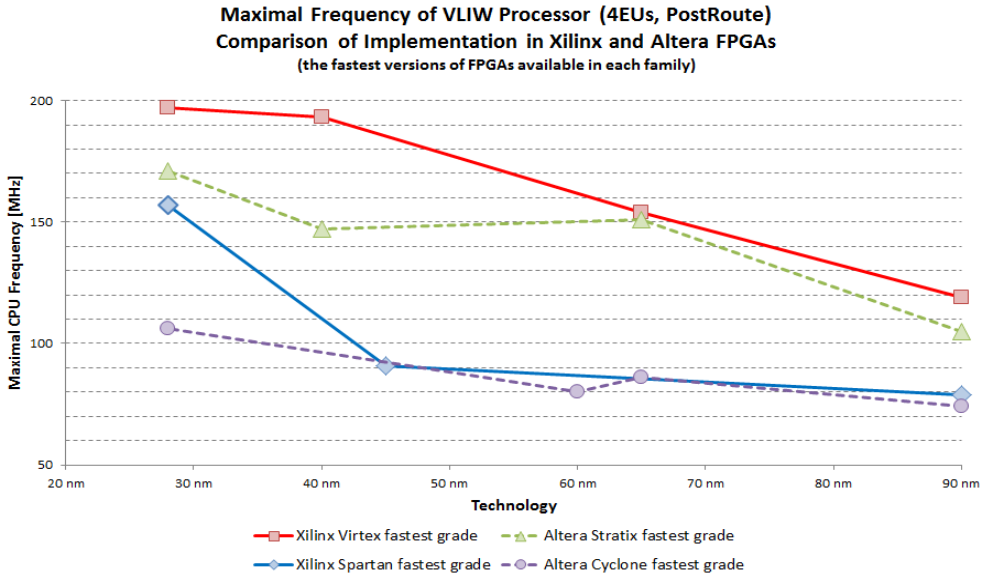


Figure 60. The maximal frequency of VLIW processor with 4 issue slots and execution units in selected XILINX and ALTERA FPGAs with respect to the technology node.

6.7 Core Scaling Experiment

The FPGAs selected for the core scaling benchmark purposes were Virtex device XC6VLX240T-3-FF1156 and Altera device EP4SGX70HF35C2. The 40 nm technology node was selected because of its excellent performance across the portfolio including the latest 28 nm technologies.

Table 7. Performance results of core scaling –the maximal frequency and delays - post-routing data at 85 °C.

Number of Issue Slots	Delay Stratix	Maximal frequency Stratix IV	Delay Virtex	Maximal frequency Virtex 6	Virtex /Stratix
1	6,0 ns	167 MHz	5,2 ns	192 MHz	87%
2	5,9 ns	169 MHz	5,2 ns	193 MHz	88%
3	6,1 ns	164 MHz	5,5 ns	182 MHz	90%
4	6,8 ns	147 MHz	5,2 ns	193 MHz	76%
5	6,8 ns	146 MHz	6,2 ns	161 MHz	91%
6	6,9 ns	144 MHz	6,2 ns	161 MHz	89%
7	7,4 ns	136 MHz	6,7 ns	150 MHz	91%
8	7,4 ns	135 MHz	6,7 ns	150 MHz	90%
9	7,3 ns	137 MHz	9,0 ns	111 MHz	**124%**
10	7,8 ns	128 MHz	11,4 ns	88 MHz	**146%**
11	7,9 ns	127 MHz	9,7 ns	104 MHz	**123%**
12	7,6 ns	131 MHz	9,8 ns	102 MHz	**128%**

Figure 61 shows the performance results of the CPU for Xilinx Virtex 6 line and Altera Stratix IV and selected number of execution units and issue slots implemented in the VLIW processor core.

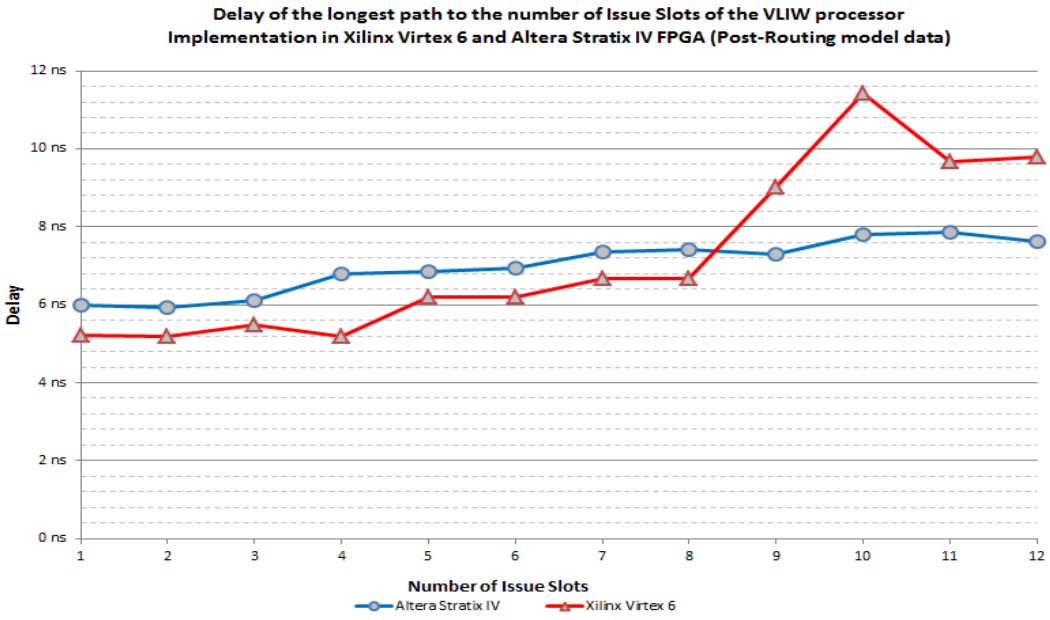


Figure 61. The maximal delay at the longest path of the VLIW processor units in the selected Xilinx Virtex 6 and Altera Stratix IV 40nm FPGAs and with respect to the number of issue slots.

6.8 Discussion

It has to be noted first that we have observed a significant gap between ISE and Quartus tools regarding the time spent on synthesis and implementation of the VHDL design. Xilinx ISE was slower in most of cases. In few cases, ISE was significantly slower in tens of minutes or even hours. The results show that the latest 28nm technology in fact no longer creates any significant gap between low-cost and high-end Xilinx FPGAs. The difference in performance is very low. In fact the fastest low-power device has similar

performance in my tests as the slowest high-end device. **The performance of the low-cost 28 nm devices has increased significantly.** It is due the fact that the three new Xilinx families (named Artix-7, Kintex-7 and Virtex-7) are manufactured in the same process, TSMC's high-k metal gate (HKMG) 28 nm technology. On the other hand, the performance increase between the Virtex 6 and 7 lines is surprisingly low, lower than expected from the results of the technology predecessors. It means that Virtex 6 is already pretty well-designed, or the latest 28nm process or technology and design of the fastest Virtex 7 devices is probably not optimized as well as in the case of the technology predecessor. However, the detailed analysis shows that the problem can lie in the network or routing resources, as it is indicated by the difference in synthesis and post-route timing results. This seems to be a significant change in the technology.

It is clearly visible that the total delay (logic plus interconnections) is lower in case of Xilinx FPGA for VLIW processor, or that Xilinx is faster in designs containing a lower number of execution units. But this situation changes rapidly for designs with 9 and more execution units, where the key delays lie in the FPGA routing resources. Please see more details in the paper [*66*] on the distribution of logic and routing delays. Generally speaking, the results from the scaling of the core show that the difference in performance is approximately same for smaller designs, but Altera clearly wins in complex designs with huge requirements put on routing resources. The previous detailed investigation in [*66*] shows that the delay in logic resources in Xilinx FPGA is nearly the same; hence the problem is in the routing resources. It points to the fact that the logic resources in Xilinx FPGAs are very good, but the overall performance is limited by the system of interconnections. Altera is probably stronger in the routing resources. The following figure shows the key overview expressed as the overall performance in Million Operations Per Second (MOPS). All the results are important for the future work and selection of FPGA devices or platform for given type of simple or complex designs.

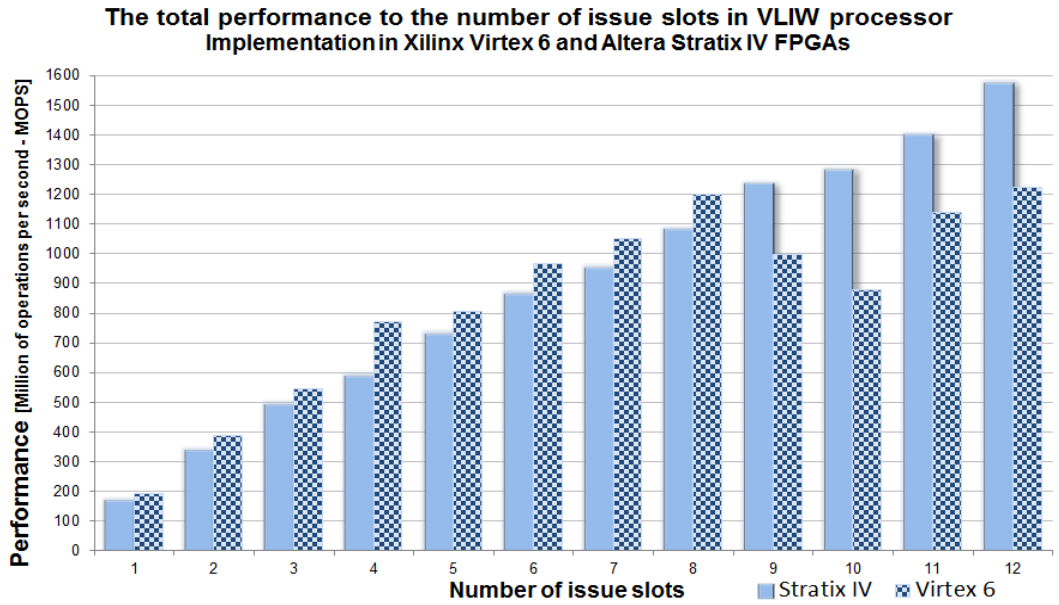


Figure 62. Performance in Million Operations Per Second (MOPS) of various FPGA and VLIW architectures (number of issue slots ranges from k = 1 to k = 12)

Chapter 7

7 Conclusions

New reliability methodology and also its key theory background has been presented in this document. The reconfigurable lab-on-chip concept based on undersampling and on-chip generated and analysed BRAM data streams is presented as well, including the underlying method and selected results from in-situ measurements. The method allows extremely easy and precise way of measurement of parameters and parameter shifts in devices and circuits, reliability testing, better estimation of reliability parameters and their initial or periodic assessment. Is also includes all the developed multi-platform solutions, new equations, XOR-less aging detection unit and also the key differential aging measurement mode using BRAMs. A lot of new, sometimes also previously unpublished data and results from measurements and experiments on various technologies down to very popular 28 nm were included and discussed as well. The area of research itself seems to be also a new one. For example Google Scholar webpage shows, when looking for the search results of the keywords “FPGA, aging, undersampling”, the obvious exclusivity of the research presented in this document, that it is obviously unique in its topic as well as results, volume and set of activities. It is also very difficult to find any other paper dealing with BRAM utilization for the purpose and in the way presented in this document.

7.1 Contributions of the Work

This document has also presented a number of results from many experiments and measurements in this document, utilizing the new method presented. The experiments were performed mainly on the modern Xilinx FPGA devices and platforms using selected development boards. The experiments presented and their results have clearly proved the theory as well as the theoretical results. The frequency of ring oscillators can be measured

in an extremely precise way and completely in-situ, including the data acquisition and processing tasks using a low-cost easily-implementable method. Utilization of BRAMs is the new and clear advantage of the proposed methodology and creates new easily extensible ways of measurements, analyses and data processing, while maintaining the same physical resources on the chip. The original designs do not require any new logic and modification of CLB structures. In majority of designs, all the measurement and data processing circuits and structures are connected to the original design using interconnect resources only.

The presented results show and also confirm generally observed important trends in microelectronics and the modern nanotechnologies. The method is applicable to general as well as complex systems. The method has been implemented and it has validated the method and trends on complex systems. The presented solution enables additional reliability enhancements with extremely low added costs, positively affecting the design's final MTBF or MTTF parameters.

7.2 Critical Assessment of the Work

The presented work and methodology is definitely based on modern solutions and technologies. The results shows in this document validates the required and sufficient sensitivity and easy implement ability in modern systems and measurement of various parameters of circuits and devices. However, the experiment and measurements were not performed on larger amount of various products and pieces of FPGA devices, chips and programmable circuits. In the microelectronic industry, 50 to 200 pieces are typically used for general information and technology qualification, Intel has presented a data from millions of pieces shipped to customers. Any such a volume is not reachable at all in my conditions. At our university, I had a possibility to test really extensively a one piece of the board only, or a few pieces from approximately 10 boards used for teaching purposes. However, it is not possible to make any piece of so expensive hardware unusable for students and teaching processes, damage it, or lose the warranty in case of the very new development boards and other products. Therefore, the future work is intended to application of the presented methodology and implementation of the presented or similar

new solutions in higher volumes and systems and also thanks to a closer cooperation with our existing or new partners.

7.3 Future Work and Possibilities of Future Research

The future is intended for detailed study of the already implemented as well as many new solutions and mechanism, their analyses, description, modelling, and better understanding. The growing reliability data bank is an important part of the final methodology and toolbox, allowing complete measurement of most of the today's internal structures, their usage for special parameter-aware placement and routing in critical designs, evaluation or estimation of the key reliability parameters with respect to the initial values or points, up to the key simple or complex continuous or on-demand reliability assessments tasks.

References

This chapter contains list details only of those works cited in the text of this document.

[1] G. Moore, "Progress in digital integrated electronics [Technical literature, Copyright 1975 IEEE. Reprinted, with permission. Technical Digest. International Electron Devices Meeting, IEEE, 1975, pp. 11-13.]," *Solid-State Circuits Society Newsletter, IEEE*, pp. 36-37, Sept. 2006. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4804410

[2] Intel Corporation. (1975) 4004 Single Chip 4-bit P-Channel Microprocessor. [Online]. http://www.intel.com/Assets/PDF/DataSheet/4004_datasheet.pdf

[3] Intel Corporation. (2012) Intel Xeon Phi Coprocessors. [Online]. http://ark.intel.com/products/family/71840/Intel-Xeon-Phi-Coprocessors

[4] Intel Corporation. (2013) Chip Shot: Intel Reveals More Details of Its Next Generation Intel Xeon Phi Processor at SC'13. [Online]. http://newsroom.intel.com/community/intel_newsroom/blog/2013/11/19/chip-shot-at-sc13-intel-reveals-more-details-of-its-next-generation-intelr-xeon-phi-tm-processor

[5] NVIDIA Corporation. (2014) NVIDIA's Next Generation CUDA Compute Architecture: Kepler GK110 The Fastest, Most Efficient HPC Architecture Ever Built - White Paper. [Online]. http://www.nvidia.com/content/PDF/kepler/NVIDIA-Kepler-GK110-Architecture-Whitepaper.pdf

[6] Taiwan Semiconductor Manufacturing Company. (2014) 28nm Technology Overview. [Online]. http://www.tsmc.com/english/dedicatedFoundry/technology/28nm.htm

[7] Xilinx. (2014) Virtex-7 FPGA Family. [Online]. http://www.xilinx.com/products/silicon-devices/fpga/virtex-7/index.htm

[8] Taiwan Semiconductor Manufacturing Company. (2014) 20nm Technology Overview. [Online]. http://www.tsmc.com/english/dedicatedFoundry/technology/20nm.htm

[9] Intel Corporation. (2014, March) Intel Custom Foundry Demonstrates Industry-Leading General Purpose SerDes on 14nm Process. [Online]. http://newsroom.intel.com/community/intel_newsroom/blog/2014/03/20/intel-custom-foundry-demonstrates-industry-leading-general-purpose-serdes-on-14nm-process

[10] Toshiba. (2014, April) Toshiba Starts Mass Production of World's First 15nm NAND Flash Memories. [Online]. http://www.toshiba.co.jp/about/press/2014_04/pr2301.htm

[11] Kaizad Mistry. (2011) Tri-Gate Transistors: Enabling Moore's Law at 22nm and Beyond, Intel Technology & Research page. [Online]. www.intel.com/technology

[12] J. Levine, E. Stott, G. Constantinides, and P. Cheung, "Online Measurement of Timing in Circuits: For Health Monitoring and Dynamic Voltage and Frequency Scaling," in *Field-Programmable Custom Computing Machines (FCCM), 2012 IEEE 20th Annual International Symposium on*, Toronto, ON, Canada, Jan. 2012, pp. 109-116. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6239800

[13] E. Stott and P. Cheung, "Improving FPGA Reliability with Wear-Levelling," in *Field Programmable Logic and Applications (FPL), 2011 International Conference on*, Chania, Crete, Greece, September 2011, pp. 323-328. [Online]. http://ieeexplore.ieee.org/xpl/login.jsp?arnumber=6044838

[14] E. Stott, J. Wong, P. Sedcole, and P. Cheung, "Degradation in FPGAs: Measurement and modelling," in *Proceedings of the 18th Annual ACM/SIGDA International Symposium on Field Programmable Gate Arrays*, Monterey, California, USA, February 2010, pp. 229-238. [Online]. http://dl.acm.org/citation.cfm?id=1723152

[15] E. Stott, P. Sedcole, and P. Cheung, "Modelling degradation in FPGA lookup tables," in *Field-Programmable Technology, 2009. FPT 2009. International Conference on*, Sydney, NSW, December 2009, pp. 443-446. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5377640

[16] E. Stott, J. Wong, and P. Cheung, "Degradation Analysis and Mitigation in FPGAs," in *Field Programmable Logic and Applications (FPL), 2010 International Conference on*, Milano, Italy, August 2010, pp. 428-433. [Online]. http://ieeexplore.ieee.org/xpl/login.jsp?arnumber=5694288

[17] J. Smith and J. Vaccaro, "Failure Mechanisms and Device Reliability," in *Reliability Physics Symposium, 1967. Sixth Annual*, Los Angeles, CA, USA, Nov. 1967, pp. 1-9. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4207750

[18] R. Stewart, "Causal Basis for System Failure Rate Calculations," in *Reliability Physics Symposium, 1967. Sixth Annual*, Los Angeles, CA, USA, Nov. 1967, pp. 166-169. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4207773

[19] C. Ryerson, "Mathematical Modeling for Predicting Failure Rates of Component Parts," in *Reliability Physics Symposium, 1967. Sixth Annual*, Los Angeles, CA, USA, Nov. 1967, pp. 10-15. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4207751

[20] M. Botzler, P. Zeiler, and B. Bertsche, "Failure prediction by means of advanced usage data analysis," in *Reliability and Maintainability Symposium (RAMS), 2014 Annual*, Colorado Springs, CO, USA, Jan. 2014, pp. 1-6. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6798508

[21] B. Zhihong LiuMcGaughy and J. Ma, "Design tools for reliability analysis," in *Design Automation Conference, 2006 43rd ACM/IEEE*, San Francisco, CA, USA, 2006, pp. 182-187. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1688786

[22] v. Dam and M. Hauser, "Ring oscillator reliability model to hardware correlation in 45nm SOI," in *Reliability Physics Symposium (IRPS), 2013 IEEE International*, Anaheim, CA, April 2013, pp. CM.1.1-CM.1.5. [Online]. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6532061

[23] A. Ghetti, C. Monzio Compagnoni, A. Spinelli, and A. Visconti, "Comprehensive Analysis of Random Telegraph Noise Instability and Its Scaling in Deca–Nanometer Flash Memories," *Electron Devices, IEEE Transactions on*, pp. 1746-1752, Aug. 2009. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5159507

[24] P. Hyuk-Min KwonIn-Shik HanJung-Deuk BokSang-Uk ParkYi-Jung JungGa-Won LeeYi-Sun ChungJung-Hwan LeeChang Yong KangKirsch and R. Jammy, "Characterization of Random Telegraph Signal Noise of High-Performance p-MOSFETs With a High-<formula formulatype="inline"> <img src="/images/tex/348.gif" alt="k"> </formula> Dielectric/Metal Gate," *Electron Device Letters, IEEE*, pp. 686-688, May 2011. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5735182

[25] D. Fugazza, D. Ielmini, S. Lavizzari, and A. Lacaita, "Random telegraph signal noise in phase change memory devices," in *Reliability Physics Symposium (IRPS), 2010 IEEE International*, Anaheim, CA, May 2010, pp. 743-749. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5488741

[26] J. Black, "Electromigration - A brief survey and some recent results," *Electron Devices, IEEE Transactions on*, pp. 338-347, Apr 1969. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1475796

[27] J. Black, "Mass Transport of Aluminum by Momentum Exchange with Conducting Electrons," in *Reliability Physics Symposium, 1967. Sixth Annual*, Los Angeles, CA, USA, Nov. 1967, pp. 148-159. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4207771

[28] J. Black, "Physics of Electromigration," in *Reliability Physics Symposium, 1974. 12th Annual*, Las Vegas, NV, USA, USA, April 1974, pp. 142-149. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4208018

[29] J. Bukowski and W. Goble, "Validation of a mechanical component constant failure rate database," in *Reliability and Maintainability Symposium, 2009. RAMS 2009. Annual*, Fort Worth, TX, USA, Jan. 2009, pp. 338-343. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4914699

[30] H. Mine, "Reliability of a Physical System," *Circuit Theory, IRE Transactions on*, pp. 138-151, May 1959. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1086604

[31] J. Suran, "Effect of Circuit Design on System Reliability," *Reliability and Quality Control, IRE Transactions on*, pp. 12-18, March 1961. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5007249

[32] L. Hellerman and M. Racite, "Reliabllity Techniques for Electronic Circuit Design," *Reliability and Quality Control, IRE Transactions on*, pp. 9-16, Sept. 1958. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5007177

[33] H. Mine, "Reliability of physical system," *Information Theory, IRE Transactions on*, pp. 138-151, May 1959. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1057526

[34] Y Miura and Y. Matukura, "Investigation of Silicon-Silicon Dioxide Interface Using MOS Structure," *Japan Journal of Appllied Physics*, vol. 5, p. 180, 1966.

[35] L. Tsetseris, X. Zhou, D. Fleetwood, D. Schrimpf, and S. Pantelides, "Physical Mechanisms of Negative-Bias Temperature Instability," *Applied Physics Letters*, vol. vol. 86, pp. pp.1-3, 2005.

[36] T. Grasser et al., "Recent advances in understanding the bias temperature instability," in *Electron Devices Meeting (IEDM), 2010 IEEE International*, San Francisco, CA, USA, Dec. 2010, pp. 4.4.1-4.4.4. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5703295

[37] T. Grasser et al., "Advanced characterization of oxide traps: The dynamic time-dependent defect spectroscopy," in *Reliability Physics Symposium (IRPS), 2013 IEEE International*, Anaheim, CA, USA, April 2013, pp. 2D.2.1-2D.2.7. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6531957

[38] T. Grasser et al., "Analytic modeling of the bias temperature instability using capture/emission time maps," in *Electron Devices Meeting (IEDM), 2011 IEEE International*, Washington, DC, USA, Dec. 2011, pp. 27.4.1-27.4.4. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6131624

[39] B. Kaczer et al., "Origin of NBTI variability in deeply scaled pFETs," in *Reliability Physics Symposium (IRPS), 2010 IEEE International*, Anaheim, CA, USA, May 2010, pp. 26-32. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5488856

[40] R. Wittmann et al., "Impact of NBTI-driven parameter degradation on lifetime of a 90nm p-MOSFET," in *Integrated Reliability Workshop Final Report, 2005 IEEE International*, Oct. 2005, p. 4 pp. [Online]. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1609573

[41] Hong LuoYu WangKu HeRong LuoHuazhong YangYuan Xie, "Modeling of PMOS NBTI Effect Considering Temperature Variation," in *Quality Electronic Design, 2007. ISQED '07. 8th International Symposium on*, San Jose, CA, March 2007, pp. 139-144. [Online]. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4149025

[42] C. Lei JinMingzhen XuTan, "An Investigation on the Permanent Component of NBTI Degradation in a 90nm CMOS Technology," in *Solid-State and Integrated Circuit Technology, 2006. ICSICT '06. 8th International Conference on*, Shanghai, Oct. 2006, pp. 1147-1149. [Online]. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4098349

[43] Xilinx. (2014, March) UG116 (v9.8) : Device Reliability Report - Fourth Quarter 2013. [Online]. http://www.xilinx.com/support/documentation/user_guides/ug116.pdf

[44] P. Pfeifer and Z. Pliva, "Delay-fault run-time XOR-less aging detection unit using BRAM in modern FPGAs," in *Electronics Conference (BEC), 2012 13th Biennial Baltic*, Tallinn, Estonia, October 2012, pp. 81-84, IEEE Catalog Number: CFP12BEC-ART. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6376820

[45] Douglas Sheldon. (2011) FPGA - Overview of JPL Efforts under NEPP, Jet Propulsion Laboratory California Institute of Technology. [Online]. http://nepp.nasa.gov/workshops/etw2011/submissions/talks/Tuesday/0930%20

-%20FPGA%20-%20Overview%20of%20JPL%20Efforts%20under%20NEPP.pdf

[46] Altera. (2014, May) About Altera's Cyclone FPGA Series. [Online]. http://www.altera.com/devices/fpga/cyclone-about/cyc-about.html

[47] Altera. (2007, April) Achieving Low Power in 65-nm Cyclone III FPGAs - White Paper. [Online]. http://www.altera.com/literature/wp/wp-01016.pdf

[48] Jacopo Franco, Ben Kaczer, and Guido Groeseneken, *Reliability of High Mobility SiGe Channel MOSFETs for Future CMOS Applications*. Dordrecht: Springer Science+Business Media, 2014.

[49] Prashant Singh, *On-chip NBTI and Gate-Oxide-Degradation Sensing and Dynamic Management in VLSI circuits*, 3476814th ed. Ann Arbor, MI, USA: ProQuest, 2011.

[50] H.E. Neil Weste and Money David Harris, *Integrated Circuit Design*, Fourth Edition ed. Boston, MA, USA: Pearson Education, Inc., publishing as Addison-Wesley, 2011.

[51] Elie Maricau and Georges Gielen, *Analog IC Realiability in Nanometer CMOS*. New York, USA: Springer Science+Business Media, 2013.

[52] K. Saluja, S. Vijayakumar, and W. Sootkaneung, "NBTI Degradation: A Problem or a Scare?," in *VLSI Design, 2008. VLSID 2008. 21st International Conference on*, Hyderabad, India, Jan. 2008, pp. 137-142. [Online]. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4450493

[53] A. Asenov, R. Balasubramaniam, A. Brown, and J. Davies, "RTS amplitudes in decananometer MOSFETs: 3-D simulation study," *Electron Devices, IEEE Transactions on*, pp. 839-845, March 2003. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1202636

[54] V. Huard et al., "NBTI degradation: From transistor to SRAM arrays," in *Reliability Physics Symposium, 2008. IRPS 2008. IEEE International*, Phoenix, AZ, USA, Jan. 2008, pp. 289-300. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4558900

[55] J. Franco et al., "Reduction of the BTI time-dependent variability in nanoscaled MOSFETs by body bias," in *Reliability Physics Symposium (IRPS), 2013 IEEE International*, Anaheim, CA, April 2013, pp. 2D.3.1-2D.3.6. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6531958

[56] M. Li WangQiuyi YeRobert WongLiehr, "Product Burn-in Stress Impacts on SRAM Array Performance," in *Reliability physics symposium, 2007. proceedings. 45th annual. ieee international*, Phoenix, AZ, USA, April 2007,

pp. 666-667. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4227744

[57] M. Toledano-Luque et al., "Response of a single trap to AC negative Bias Temperature stress," in *Reliability Physics Symposium (IRPS), 2011 IEEE International*, Monterey, CA, April 2011, pp. 4A.2.1-4A.2.8. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5784501

[58] F. Schanovsky, O. Baumgartner, W. Goes, and T. Grasser, "A detailed evaluation of model defects as candidates for the bias temperature instability," in *Simulation of Semiconductor Processes and Devices (SISPAD), 2013 International Conference on*, Glasgow, Sept. 2013, pp. 1-4. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6650559

[59] P. Weckx et al., "Defect-based methodology for workload-dependent circuit lifetime projections - Application to SRAM," in *Reliability Physics Symposium (IRPS), 2013 IEEE International*, Anaheim, CA, April 2013, pp. 3A.4.1-3A.4.7. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6531974

[60] J. Franco et al., "Impact of single charged gate oxide defects on the performance and scaling of nanoscaled FETs," in *Reliability Physics Symposium (IRPS), 2012 IEEE International*, Anaheim, CA, April 2012, pp. 5A.4.1-5A.4.6. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6241841

[61] C. Young et al., "Detection of Trap Generation in High-k Gate Stacks due to Constant Voltage Stress," in *VLSI Technology, Systems, and Applications, 2006 International Symposium on*, Hsinchu, April 2006, pp. 1-2. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4016625

[62] B. Kaczer et al., "The relevance of deeply-scaled FET threshold voltage shifts for operation lifetimes," in *Reliability Physics Symposium (IRPS), 2012 IEEE International*, Anaheim, CA, USA, April 2012, pp. 5A.2.1-5A.2.6. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6241839

[63] A. Hokazono, S. Balasubramanian, K. Ishimaru, and H. Ishiuchi, "Forward Body Biasing as a Bulk-Si CMOS Technology Scaling Strategy," *Electron Devices, IEEE Transactions on*, pp. 2657-2664, Oct. 2008. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4631378

[64] M. Ruffoni and A. Bogliolo, "Direct Measures of Path Delays on Commercial FPGA Chips," in *Signal Propagation on Interconnects, 6th IEEE Workshop on. Proceedings*, Pisa, Italy, May 2002, pp. 157-159. [Online]. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4027685

[65] T. Karnik and K. Sung-Mo, "An empirical model for accurate estimation of routing delay in FPGAs," in *Computer-Aided Design, 1995. ICCAD-95. Digest*

of Technical Papers., 1995 IEEE/ACM International Conference on, San Jose, CA, USA, Nov. 1995, pp. 328-331. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=480136

[66] P. Pfeifer, Z. Pliva, M. Scholzel, T. Koal, and H. Vierhaus, "On performance estimation of a scalable VLIW soft-core in XILINX FPGAs," in *Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2013 IEEE 16th International Symposium on*, Karlovy Vary, Czech Republic, April 2013, pp. 181-186, IEEE Catalog Number: CFP13DDE-ART, Brno University of Technology. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6549813

[67] P. Pfeifer, Z. Pliva, M. Scholzel, T. Koal, and H. Vierhaus, "On performance estimation of a scalable VLIW soft-core on ALTERA and XILINX FPGA platforms," in *Applied Electronics (AE), 2013 International Conference on*, Pilsen, Czech Republic, September 2013, pp. 1-4, IEEE Catalog Number: CFP1369A-PRT, University of West Bohemia. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6636515

[68] J. Keane and C. Wei ZhangKim, "An Array-Based Odometer System for Statistically Significant Circuit Aging Characterization," *Solid-State Circuits, IEEE Journal of*, pp. 2374-2385, Oct. 2011. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5959997

[69] L. Pong-Fei and K. Jenkins, "A built-in BTI monitor for long-term data collection in IBM microprocessors," in *Reliability Physics Symposium (IRPS), 2013 IEEE International*, Anaheim, CA, USA, April 2013, pp. 4A.1.1-4A.1.6. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6532003

[70] IEEE, "IEC/IEEE Behavioural Languages - Part 4: Verilog Hardware Description Language (Adoption of IEEE Std 1364-2001)," pp. 0_1-860, March 2005. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1406532

[71] Xilinx. (2014, February) UG363 (v1.8) : Virtex-6 FPGA Memory Resources - User Guide. [Online]. http://www.xilinx.com/support/documentation/user_guides/ug363.pdf

[72] Xilinx. (2011, July) UG383 (v1.5) : Spartan-6 FPGA Block RAM Resources - User Guide. [Online]. http://www.xilinx.com/support/documentation/user_guides/ug383.pdf

[73] Xilinx. (2014, January) UG473 (v.1.10) : 7 Series FPGAs Memory Resources - User Guide. [Online]. http://www.xilinx.com/support/documentation/user_guides/ug473_7Series_Memory_Resources.pdf

[74] Xilinx. (2013, December) UG573 (v1.0) : UltraScale Architecture Memory Resources - Advance Specification User Guide. [Online]. http://www.xilinx.com/support/documentation/user_guides/ug573-ultrascale-memory-resources.pdf

[75] Xilinx. (2010, March) DS174 (v2.0) : Virtex-5Q Family Overview - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds174.pdf

[76] Xilinx. (2012, March) DS192 (v1.3) : Radiation-Hardened, Space-Grade Virtex-5QV Family Overview - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds192_V5QV_Device_Overview.pdf

[77] Xilinx. (2011, October) DS160 (v2.0) : Spartan-6 Family Overview - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds160.pdf

[78] Xilinx. (2012, January) DS150 (v2.4): Virtex-6 Family Overview - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds150.pdf

[79] Xilinx. (2014, February) DS180 (v1.15) : 7 Series FPGAs Overview - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds180_7Series_Overview.pdf

[80] Xilinx. (2014, May) DS890 (v1.3) : UltraScale Architecture and Product Overview - Advance Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds890-ultrascale-overview.pdf

[81] Xilinx. (2014, May) UltraScale Architecture Product Selection Guide. [Online]. http://www.xilinx.com/publications/prod_mktg/ultrascale_product_selection_guide.pdf

[82] C. Shannon, "Communication in the Presence of Noise," *Proceedings of the IRE*, vol. 37, no. 1, pp. 10-21, January 1949. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1697831

[83] Z. Song and D. Sarwate, "The frequency spectrum of pulse width modulated signals," *Signal Processing*, vol. 83, no. 10, October 2003. [Online]. http://dl.acm.org/citation.cfm?id=950459

[84] Samsung. (2014) 45nm Technology Overview. [Online]. http://www.samsung.com/global/business/semiconductor/foundry/process-technology/40-45nm

[85] Xilinx. (2011, October) DS162 (v3.0) : Spartan-6 FPGA Data Sheet: DC and Switching Characteristics - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds162.pdf

[86] Xilinx. (2014, March) DS152 (v3.6) : Virtex-6 FPGA Data Sheet: DC and Switching Characteristics - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds152.pdf

[87] Xilinx. (2014, February) DS187 (v1.11) : Zynq-7000 All Programmable SoC (Z-7010, Z-7015, and Z-7020): DC and AC Switching Characteristics - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds187-XC7Z010-XC7Z020-Data-Sheet.pdf

[88] Xilinx. (2014, March) DS182 (v2.8) : Kintex-7 FPGAs Data Sheet: DC and AC Switching Characteristics - Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds182_Kintex_7_Data_Sheet.pdf

[89] Xilinx. (2014, May) DS892 (v1.2) : Kintex UltraScale Architecture Data Sheet: DC and AC Switching Characteristics - Advance Product Specification. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds892-kintex-ultrascale-data-sheet.pdf

[90] U. Guler and G. Dundar, "Maximizing randomness in ring oscillators for security applications," in *Circuit Theory and Design (ECCTD), 2011 20th European Conference on*, Linkoping, Aug. 2011, pp. 118-121. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6043291

[91] D. Qingqi and J. Abraham, "Jitter decomposition in ring oscillators," in *Design Automation, 2006. Asia and South Pacific Conference on*, Yokohama, Jan. 2006, p. 6 pp. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1594696

[92] Y. Hirakawa, A. Motomura, K. Ota, N. Mimura, and K. Nakamura, "A universal test structure for the direct measurement of the design margin of even-stage ring oscillators with CMOS latch," in *Microelectronic Test Structures (ICMTS), 2012 IEEE International Conference on*, San Diego, CA, March 2012, pp. 18-22. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6190605

[93] C. Hochberger, M. Changgong LiRaitza, and M. Vogt, "Influence of operating conditions on ring oscillator-based entropy sources in FPGAs," in *Field Programmable Logic and Applications (FPL), 2012 22nd International Conference on*, Oslo, Norway, Aug. 2012, pp. 555-558. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6339378

[94] M. Gag, T. Wegner, A. Waschki, and D. Timmermann, "Temperature and on-chip crosstalk measurement using ring oscillators in FPGA," in *Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2012 IEEE 15th International Symposium on*, Tallinn, Estonia, April 2012, pp. 201-204. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6219057

[95] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," *Computers, IEEE Transactions on*, pp. 403-409, April 2003. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1190581

[96] Z. Xuan and A. Apsel, "A Low-Power, Process-and- Temperature-Compensated Ring Oscillator With Addition-Based Current Source," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, pp. 868-878, May 2011. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5671512

[97] Z. Hui, "Start-up analysis for differential ring oscillator with even number of stages," in *Circuits and Systems (APCCAS), 2010 IEEE Asia Pacific Conference on*, Kuala Lumpur, Dec. 2010, pp. 636-639. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5774827

[98] T. Nakura, M. Ikeda, and K. Asada, "Ring oscillator based random number generator utilizing wake-up time uncertainty," in *Solid-State Circuits Conference, 2009. A-SSCC 2009. IEEE Asian*, Taipei, Nov. 2009, pp. 121-124. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5357194

[99] K. Wold, "Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings," in *Reconfigurable Computing and FPGAs, 2008. ReConFig '08. International Conference on*, Cancun, Dec. 2008, pp. 385-390. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4731825

[100] Y. Haile and P. Leong, "An FPGA Chip Identification Generator Using Configurable Ring Oscillators," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, pp. 2198-2207, Dec. 2012. [Online]. http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6087303

[101] A. Maiti, L. McDougall, and P. Schaumont, "The Impact of Aging on an FPGA-Based Physical Unclonable Function," in *Field Programmable Logic and Applications (FPL), 2011 International Conference on*, Chania, Sept. 2011, pp. 151-156. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6044799

[102] Xilinx. (2009, June) UG348 (v3.0.3): ML505/ML506/ML507 Getting Started Tutorial. [Online]. http://www.xilinx.com/support/documentation/boards_and_kits/ug348.pdf

[103] Xilinx. (2011, May) UG347 (v3.1.2): ML505/ML506/ML507 Evaluation Platform - User Guide. [Online]. http://www.xilinx.com/support/documentation/boards_and_kits/ug347.pdf

[104] Xilinx. (2009, June) UG349 (v3.1): ML505/ML506/ML507 Reference Design - User Guide. [Online]. http://www.xilinx.com/support/documentation/boards_and_kits/ug349.pdf

[105] Digilent. (2013, August) Atlys Board Reference Manual. [Online]. http://www.digilentinc.com/Data/Products/ATLYS/Atlys_rm_V2.pdf

[106] Xilinx. (2011, October) UG533 (v1.5): Getting Started with the Xilinx Virtex-6 FPGA ML605 Evaluation Kit. [Online]. http://www.xilinx.com/support/documentation/boards_and_kits/ug533.pdf

[107] Xilinx. (2012, October) UG534 (v1.8): ML605 Hardware - User Guide. [Online]. http://www.xilinx.com/support/documentation/boards_and_kits/ug534.pdf

[108] Xilinx. (2014, April) UG480 (v1.3.1) : 7 Series FPGAs and Zynq-7000 All Programmable SoC XADC Dual 12-Bit 1 MSPS Analog-to-Digital Converter - User Guide. [Online]. http://www.xilinx.com/support/documentation/user_guides/ug480_7Series_XADC.pdf

[109] Xilinx. (2013, December) DS190 (v1.6) : Zynq-7000 All Programmable SoC Overview. [Online]. http://www.xilinx.com/support/documentation/data_sheets/ds190-Zynq-7000-Overview.pdf

[110] E. Mohsen. (2013, July) WP423 (v2.2) : Reducing System Power and Costwith Artix-7 FPGAs. [Online]. http://www.xilinx.com/support/documentation/white_papers/wp423-Reducing-Sys-Power-Cost-28nm.pdf

[111] Zedboard.org. (2014) Digilent's ZedBoard Zynq FPGA Dev.board documentation. [Online]. http://www.digilentinc.com/Products/Detail.cfm?Prod=ZEDBOARD

[112] AVNET. (2012, August) ZedBoard (Zynq TM Evaluation and Development) - Hardware User's Guide v1.1. [Online]. http://www.zedboard.org/sites/default/files/ZedBoard_HW_UG_v1_1.pdf

[113] Zedboard.org. (2014) ZedBoard commumity dedicated webpage. [Online]. http://www.zedboard.org/

[114] LINEAR Technology. (2010, June) LTC2481 - 16-Bit SD ADC with Easy Drive Input Current Cancellation and I2C Interface (REV.C). [Online]. http://cds.linear.com/docs/en/datasheet/2481fc.pdf

[115] Texas Instruments. (2004, October) Small, Dynamic Voltage Management Solution Based on TPS62300 High-Frequency Buck Converter and DAC6571 - Application Report SLVA196. [Online]. http://www.ti.com/lit/an/slva196/slva196.pdf

[116] Texas Instruments. (2014, March) LM10500 5A Step-Down Energy Management Unit (EMU) With PowerWise Adaptive Voltage Scaling (AVS). [Online]. http://www.ti.com/lit/ds/symlink/lm10500.pdf

[117] LINEAR Technology. (2008, April) Application Note 119A: Powering Complex FPGA-Based Systems Using Highly Integrated DC/DC uModule Regulator Systems; Part 1 of 2 - Circuit and Electrical Performance. [Online]. http://cds.linear.com/docs/en/application-note/an119afb.pdf

[118] LINEAR Technology. (2008, April) Application Note 119B: Powering Complex FPGA-Based Systems Using Highly Integrated DC/DC uModule Regulator Systems; Part 2 of 2 - Thermal Performance and Layout. [Online]. http://cds.linear.com/docs/en/application-note/an119bfb.pdf

[119] Digilent. (2010, June) Atlys Schematics. [Online]. http://www.digilentinc.com/Data/Products/ATLYS/Atlys_C2_sch.pdf

[120] Digilent. (2012, June) ZedBoard Documentation - Schematic (REV C.1). [Online]. http://www.zedboard.org/sites/default/files/documentations/ZedBoard_RevC.1_Schematic_130129.pdf

[121] P. Mangalagiri, R. Sungmin BaeKrishnan, and V. Yuan XieNarayanan, "Thermal-aware reliability analysis for Platform FPGAs," in *Computer-Aided Design, 2008. ICCAD 2008. IEEE/ACM International Conference on*, San Jose, CA, USA, Nov. 2008, pp. 722-727. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4681656

[122] P. Weber et al., "Toolset for measuring thermal behavior of FPGA devices," in *Thermal Investigations of ICs and Systems (THERMINIC), 2013 19th International Workshop on*, Berlin, Germany, Sept. 2013, pp. 48-53. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6675251

[123] G. Burke et al. (2004) Operation of FPGAs at Extremely Low Temperatures. [Online]. http://www.baengineering.com/b159_burke_p-1.pdf

[124] A. Amouri and M. Tahoori, "A Low-Cost Sensor for Aging and Late Transitions Detection in Modern FPGAs," in *Field Programmable Logic and Applications (FPL), 2011 International Conference on*, Chania, Greece, September 2011, pp. 329-335. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6044839

[125] E. Chmelar, "FPGA interconnect delay fault testing," in *Test Conference, 2003. Proceedings. ITC 2003. International*, September 2003, pp. 1239-1247. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1271113

[126] P. Pfeifer and Z. Pliva, "On measurement of impact of the metallization and FPGA design to the changes of slice parameters and generation of delay faults," in *Field Programmable Logic and Applications (FPL), 2012 22nd International Conference on*, Oslo, Norway, August 2012, pp. 743-746. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6339167

[127] C. Hu and S. Zain. (2010, May) NSEU Mitigation in Avionics Applications. [Online]. http://www.xilinx.com/support/documentation/application_notes/xapp1073_NSEU_Mitigation_Avionics.pdf

[128] Douglas L. Perry, *VHDL: Programming by Example*, 4th ed.: McGraw-Hill, 2002.

[129] M. Sung-Man ChoJeong-Hyun LeeChang et al., "High Pressure Deuterium Annealing Effect on Nano-Scale Strained CMOS Devices," in *Reliability physics symposium, 2007. proceedings. 45th annual. ieee international*, Phoenix, AZ, April 2007, pp. 674-675. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4227748

[130] E. Stott, P. Sedcole, and P. Cheung, "Fault tolerant methods for reliability in FPGAs," in *Field Programmable Logic and Applications, 2008. FPL 2008. International Conference on*, Heidelberg, Germany, September 2008, pp. 415-420. [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4629973

Quoted Standards and Other Similar Documents

This chapter contains a separate list from the reference list. This is a list of standards not directly cited in this document, however in close relationship to the area solved in it.

MIL-HDBK-217F Reliability Prediction of Electronic Equipment, 1991. Notice 1 (1992) and Notice 2 (1995).

SR-332, Issue 1 Reliability Prediction Procedure for Electronic Equipment, Telcordia, May 2001.

SR-332, Issue 2 Reliability Prediction Procedure for Electronic Equipment, Telcordia, September 2006.

IEC 61508 and related standards

IEC 61511 and related standards

1364-2001, replaced by IEC 61691-4 First edition 2004-10; IEEE 1364 - IEEE Standard Verilog Hardware Description Language

Mil-Hdbk-338B (Active) Electronic Reliability Design Handbook, October 1998

GEIA-STD-0009 Reliability Program Standard for Systems Design, Development, and Manufacturing

SAE JA-1000 1998-06 Reliability Program Standard

DOD Guide for Achieving Reliability, Availability and Maintainability, August 2005

Mil-Std-704 Aircraft Electric Power Characteristics

IEC 60050 (191) A1 – Electromechanical vocabulary – chapter 191: operating dependability and service quality

UTE C 80-810 Reliability Data Handbook: RDF 2000 - A universal model for reliability prediction calculations for components, electronic boards and equipment

IEC 61709 – Electronic components – Reliability – Reference conditions for failure rates and stress influence models for conversion

IEC 62308:2006 Equipment reliability – Reliability assessment methods

SSB-1.003 – EIA Engineering Bulletin – Acceleration factors

JEDEC JEP122C Failure Mechanism and Models for Semiconductor Devices

Bibliography

This chapter contains a separate list from the reference list. This is a list of sources not directly cited in this document, however in close relationship to the area solved in it.

[1] M. Talmor and S. Arueti, "Reliability Prediction: The Turnover Point," 1997 *Proc. Ann. Reliability and Maintainability Symp*., 1997, pp. 254-262.

[2] W. Denson, "The History of Reliability Prediction," *IEEE Trans. On Reliability*, vol. 47, no. 3-SP, September 1998.

[3] D. Hirschmann, D. Tissen, S. Schroder and R.W. de Doncker, "Reliability Prediction for Inverters in Hybrid Electrical Vehicles," *IEEE Trans. on Power Electronics*, vol. 22, no. 6, November 2007, pp. 2511-2517.

[4] NIST Information Technology Library.

[5] SEmatech, Semiconductor Device Reliability Failure Models.

[6] Johnson, B., W.: Design and analysis of fault-tolerant digital system.,Addison-Wesley, 1989

[7] Hlavička, J., a kolektiv: Číslicové systémy odolné proti poruchám. ČVUT, 1992

[8] Walker, N., W.: The Design Analysis Handbook.Butterworth-Heinemann,1998

[9] Koren, I., Krishna, C., M.: Fault-Tolerant Systems. Morgan Kaufmann, 2007

[10] Douglass, B., P.: Doing Hard Time. Addison-Wesley Professional, 1999

[11] Novak, Ondrej, Gramatova, Elena Ubar, Raimund, et al. : Handbook of Testing Electronic Systems, CTU Prague, 2005, ISBN 80-01-03318-X

[12] Kastensmidt, Fernanda L., Carro, Luigi, Reis, Ricardo: Fault-Tolerance Techniques for SRAM-based FPGAs, Springer, 2006, ISBN 0-387-31068-1

[13] Ciappa, Mauro, Carbognani, Flavio, Fichtner, Wolfgang: Lifetime Prediction and Design of Reliability Tests for High-Power Devices in Automotive Applications, IEEE Transactions On Device And Materials Reliability, Vol. 3, No. 4, December 2003, page 191

[14] White Mark, Bernstein, Joseph B. : Microelectronics Reliability: Physics-of-Failure Based Modeling and Lifetime Evaluation, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, 2008

[15] Jervan, Gert, Steininger, Andreas, Hollstein, Thomas, Ellervee, Peeter, Vierhaus, Heinrich Theodor, Scholzel, Mario, Ubar, Raimund, Raik, Jaan: Dependadble Systems Design - handouts, CREDES Summer School, Tallinn 2011

[16] Nourani, Mehrdad, Namazi, Ali, Askari, Syed, Fault Tolerant Circuits for Highly Reliable Systems,IEEEAC Paper #1746, 2008

[17] ITEM Software and ReliaSoft Corporation, RS 490 Course Notes: Introduction to Standards Based Reliability Prediction and Lambda Predict, 2006.

[18] B. Foucher, J. Boullie, B. Meslet and D. Das, "A Review of Reliability Prediction Methods for Electronic Devices," Microelectron. Wearout., vol. 42, no. 8, August 2002, pp. 1155-1162.

[19] M. Pecht, D. Das and A. Ramarkrishnan, "The IEEE Standards on Reliability Program and Reliability Prediction Methods for Electronic Equipment," Microelectron. Wearout., vol. 42, 2002, pp. 1259-1266.

List of Publications and Presentations of the Author

This chapter contains a list of author's papers, journals, presentations and other publications. The main author is mentioned first, my name is in **BOLD.**

My IEEE papers can be found in SCOPUS (Pfeifer Petr, Author ID: 55513243800), ORCID (Pfeifer Petr, Author ID: 0000-0001-7661-0778), ResearcherID (D-3727-2014) or ResearchGate (http://www.researchgate.net/profile/Petr_Pfeifer) and Google scholar (http://scholar.google.com/citations?user=jcpilXQAAAAJ).

[1] **PFEIFER**, P., PLIVA, Z.: A New Method for In-Situ Measurement of Parameters and Degradation Processes in Modern Nanoscale Programmable Devices. **Journal Microprocessors and Microsystems**, Special Issue, MICPRO2135, Volume 38, Issue 6, Elsevier B.V., ISSN 0141-9331, August 2014 (received 16/10/2013, accepted 27/4/2014, available online 22/5/2014), pp 605-619, DOI: 10.1016/j.micpro.2014.04.008

[2] **PFEIFER** P.: Reliability Assessment and Advanced Measurements In Modern Nanoscale Programmable Technologies: 28nm FPGAs Under Extreme Conditions, ZUSYS, Cottbus, Germany, November 2014

[3] **PFEIFER**, P.: Towards Increased Reliability and Hardware Security using Advanced Measurements and Data Processing on Modern Nanoscale FPGAs, Joint MEDIAN&TRUDEVICE Open Forum, September 2014, Amsterdam, The Netherlands

[4] **PFEIFER**, P., KACZER, B., PLIVA, Z.: A Reliability Lab-on-chip Using Programmable Arrays, 52nd IEEE International Reliability Physics Symposium, Hawaii, USA, June 2014, DOI: 10.1109/IRPS.2014.6861123

[5] **PFEIFER**, P., PLIVA, Z.: On Reliability Enhancement Using Adaptive Core Voltage Scaling and Variations on TSMC 28nm LP process FPGAs, The Third Workshop on Manufacturable and Dependable Multicore Architectures at Nanoscale (MEDIAN'14) Dresden, Germany, March 28, 2014

[6] **PFEIFER**, P., KACZER, B., WECKX, P., PLIVA, Z.: On Reliability Enhancement Using Adaptive Core Voltage Scaling And Variations On Nanoscale FPGAs, 15th IEEE Latin American Test Workshop, Fortaleza, Brazil, March 2014, DOI: 10.1109/LATW.2014.6841917

[7] **PFEIFER**, P., PLIVA, Z.: Advanced design methods – lectures for a new course at TUL, ESF 2014

[8] **PFEIFER**, P., PLIVA, Z.: Advanced design methods – lessons for a new course at TUL, ESF 2014

[9] Co-author of Dolezal, I., et al,: AEL (Analogue Electronics) lectures, TUL, ESF 2014/2015 (under prep.), ISBN 978-80-7494-136-8, DOI:10.15240/tul/002/2014-11-003

[10] Novak, O., et al, **PFEIFER, P.**: CIE (Digital Electronics) lectures, TUL, ESF 2014/2015 (under prep.), ISBN 978-80-7494-049-1

[11] **PFEIFER**, P., PLIVA, Z., SCHOLZEL, M., KOAL, T., VIERHAUS, H.T.: On Performance Estimation of a Scalable VLIW Soft-Core on Altera and Xilinx FPGA platforms. In: Proceedings of the 18th International Conference Applied Electronics 2013 (AE2013). Pilsen, Czech Republic, September 2013, IEEE Conference Record #30244, IEEE Catalog Number CFP1369A-PRT (Print), CFP1369A-ART (Online), ISBN 978-80-261-0166-6 (Print), ISBN 978-80-261-0165-9 (Online), ISSN 1803-7232 (Print), ISSN 1805-9597 (Online), pp. 209-212.

[12] **PFEIFER**, P., PLIVA, Z.: On Measurement of Parameters of Programmable Microelectronic Nanostructures Under Accelerating Extreme Conditions. In: 3rd International Conference on Field Programmable Logic and Applications (FPL'13), ISBN 978-1-4799-0004-6/13, IEEE Catalog Number CFP13623-ART, DOI 10.1109/FPL.2013.6645584, Porto, Portugal, September 2013, pp.1-4

[13] **PFEIFER**, P., PLIVA, Z.: Investigating Diachrony of Programmable Microelectronic Nanostructures. In: Proceedings of the 11th IEEE International workshop on Electronics, Control, Measurement and Signals (ECMSM2013). Toulouse, France, June 2013, IEEE Catalog Number: CFP13ECN-USB ISBN 978-1-14673-6297-9, DOI: 10.1109/ECMSM.2013.6648931, pp.26-28.

[14] **PFEIFER**, P., PLIVA, Z., SCHOLZEL, M., KOAL, T., VIERHAUS, H.T.: On Performance Estimation of a Scalable VLIW Soft-Core in XILINX FPGAs. In: Proceedings of the 2013 IEEE 16th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS). Karlovy Vary, Czech Republic, April 2013, IEEE Catalog Number: CFP13DDE-USB, ISBN 978-1-4673-6134-7, DOI: 10.1109/DDECS.2013.6549813, pp. 181-186.

[15] **PFEIFER**, P.: Using digital oscilloscopes for measurement purposes in AP9 classroom for measurement of low signals, ESF, TUL 2012

[16] **PFEIFER**, P.: An Intelligent classroom and measurement workplace – Remote control of oscilloscopes in AP9 classroom, ESF, TUL 2012

[17] **PFEIFER**, P., PLIVA, Z.: Delay-Fault Run-Time XOR-less Aging Detection Unit Using BRAM in modern FPGAs. In: 13th Biennial Baltic Electronics Conference, Tallinn, Estonia, October 2012, IEEE Catalog Number: CFP12BEC-CDR, ISBN: 978-1-4673-2772-5 Proceedings,book), ISBN 978-

1-4673-2773-2 (CDR), ISSN: 1736-3705, DOI: 10.1109/BEC.2012.6376820, p.81-84.

[18] **PFEIFER**, P., PLIVA, Z.: Diachrony of programmable nanostructures. In: proceedings of the ZUSYS Dependable Systems workshop, Cottbus, Germany, October 2012, p.78-83.

[19] **PFEIFER**, P., PLÍVA, Z.: Diachrony of programmable nanostructures. In: Počítačové architektury & diagnostika (PAD2012), Milovy, Czech Republic, ISBN 978-80-01-05106-1, September 2012, p.121-126.

[20] **PFEIFER**, P., PLÍVA, Z.: On measurement of impact of the metallization and FPGA design to the changes of slice parameters and generation of delay faults. In: 22nd International Conference on Field Programmable Logic and Applications (FPL), 2012, Oslo, Norway, August 2012, E-ISBN: 978-1-4673-2255-3, Print ISBN: 978-1-4673-2257-7, DOI: 10.1109/FPL.2012.6339167, p.743-746

[21] **PFEIFER**, P.: Fault-tolerance and testability of programmable devices in safety applications with increased lifetime and reliability requirements", Počítačové architektury & diagnostika (PAD), September 2011, Stará Lesná, Slovakia, ISBN 978-80-227-3552-0, pp.14-19

[22] **PFEIFER**, P. "Fire detection safety system communication loop card with link layer coprocessor, A crossplatform version for EN54/UL864 safety systems with power and communication control signals distributed over the same pair of wires.", 10th International Workshop on Electronics, Control, Measurement and Signal (ECMS) 2011, ISBN: 978-80-7372-781-9, pp. 87-92

[23] KNAPEK, Alexandr, HUTAR, Otakar, **PFEIFER**, Petr, GRMELA, Lubomir: Wide-band low noise preamplifier design for the purposes of flame detectors testing. VUT/Tyco, Journal JMO-Jemná mechanika a optika-Fine

Mechanics And Optics, Volume 53, 3/2008, pages 90-92,
link: http://jmo.fzu.cz/2008/Jmo-03/JMO-200803.pdf

[24] KNAPEK, Alexandr, HUTAR, Otakar, **PFEIFER**, Petr: The measurement of pyroelectric sensor signal using low-noise wideband measurement preamplifier. VUT/Tyco, Journal JMO-Jemná mechanika a optika-Fine Mechanics And Optics, Volume 53, 10/2008, pages 276-278,
link: http://jmo.fzu.cz/2008/Jmo-10/JMO-200810.pdf

[25] SMETANA, Martin, SAJDL, Ondřej, **PFEIFER**, Petr: Universal test SW for Fire Panel Tester. VUT/Tyco, EEICT2009,
link: http://www.feec.vutbr.cz/EEICT/2009/sbornik/02-Magisterske%20projekty/06-Mikroelektronika%20a%20technologie/10-xsmeta00.pdf

[26] VITEK, Ladislav, ŠTEFAN, Pavel, **PFEIFER**, Petr: Universal Fire Panel Tester. VUT/Tyco, EEICT2009, link:
http://www.feec.vutbr.cz/EEICT/2009/sbornik/02-Magisterske%20projekty/06-Mikroelektronika%20a%20technologie/13-dromy.pdf

[27] **PFEIFER**, P.: *NOR FLASH USB key design with Turbo uPSD Plus*, STMicroelectronics 2005

[28] **PFEIFER**, P.: *Full-speed USB design using Turbo uPSD Plus*, STMicroelectronics 2005

[29] **PFEIFER**, P.: *Designing Mass Storage Class (Bulk-Only Transport) USB devices using Turbo uPSD Plus*, STMicroelectronics 2005

[30] **PFEIFER**, P.: *AN2007_Sound Generation using the uPSD Sound Studio On uPSD32xx and Turbo uPSD33xx*, STMicroelectronics 2004, *link:*

[31] **PFEIFER**, P.: *AN1815_USB Device Disconnect-On-Demand with uPSD32xx*, STMicroelectronics 2004

[32] **PFEIFER**, P.: *AN1843_Designing the Oscillator for Use with uPSD*, STMicroelectronics 2004

[33] **PFEIFER**, P.: *AN1886_Low Speed USB Design Using uPSD*, STMicroelectronics 2004

[34] **PFEIFER**, P: *A new PCI local bus analysis and test program*, Poster 2003, CVUT FEE Prague, 2003 ***(best paper award)***
link: http://www3.fs.cvut.cz/web/fileadmin/documents/12241-BOZEK/publikace/2002/PfeiferPoster2002.pdf

[35] **PFEIFER**,P., PITELKA, J. : *Universal Processor Module for Intelligent Mobile Sensor System for Monitoring of Physical Quantities in Environment*, Workshop, CTU Prague, 2003, page 476

[36] **PFEIFER**,P., SURA, A: *Monitoring Station Main Unit of Intelligent Mobile Sensor System for Monitoring of Physical Quantities in Environment*, Workshop, CTU Prague, 2003, page 478

[37] **PFEIFER**, P.: *One-Wire Bus Using FPGA,* In: Proceedings of Workshop 2002, Prague : CTU, 2002, vol. A, p.436-437. ISBN 80-01-02511-X

[38] **PFEIFER**, P: *MATLAB Simulink Accelerator (in Czech)*, Proceedings of MATLAB2002 , Humusoft 2002, ISBN 80-7080-500-5, p.448-450

[39] **PFEIFER**, P: *Universal Data Exchange Server (in Czech)*, Proceedings of MATLAB2002, Humusoft 2002, ISBN 80-7080-500-5, p.451-457

[40] **PFEIFER**,P.: *Fast Simulation System for Simulation and Improvement of Digital Communication Systems in Transportation*, 6th World Multi-Conference on Systemics, Cybernetics and Informatics SCI2002, Orlando, Florida, USA, 2002, ISBN: 980-07-8150-1, Volume IV, p.379-384 ***(best***

paper *in section Broadband Networks and Network Architectures, Topologies and Protocols**)***

[41] **PFEIFER**,P., KOCOUREK, P., NOVAK,J.: *Intelligent Mobile Sensor System for Monitoring of Physical Quantities in Environment*, Proceedings of Applied Electronics 2002, Pilsen 11-12 September 2002, ISBN: 80-7082-881-1, p.136-139

[42] **PFEIFER**, P. : *PCI Local Bus Analysis And Test Program*, Poster2002, CVUT FEE Prague, 2002

[43] **PFEIFER**, P. : *Simulation Of Fieldbus System,* Proceedings of Applied Electronics 2001, ISBN 80-7082-758-0, Pilsen 2001, p.200-203

[44] **PFEIFER**, P. : *Measurement BUS and its virtual interference simulation, implementation of improvement and simulation results*, Poster2001, CTU Prague, 2001

[45] **PFEIFER**, P. : *Fast Simulator of Digital Systems*, Proceedings of Workshop2001, ISBN 80-01-02335-4, p.390, CTU Prague 2001

[46] **PFEIFER**, P., NOVAK, J. : *Simulation of disturbance of Measurement Bus using MATLAB (in Czech)*, Proceedings of MATLAB2000 conference, ISBN 80-7080-401-7, Humusoft 2000, p. 287-292

[47] **PFEIFER**, P., BOHACEK, J., Smid, R: *Statistical processing of measured data using MATLAB (in Czech)*, Proceedings of MATLAB2000 conference, ISBN 80-7080-401-7, Humusoft 2000, p. 55-60

[48] **PFEIFER**, P. : *Multifunctional Programmable Single-Board CAN monitoring Module*, 10th International Conference, FPL2000 Proceedings, Villach, Austria, August 2000, ISBN 3-540-67899-9, DOI: 10.1007/3-540-44614-1_18, Springer-Verlag Berlin Heidelberg 2000, p.163-168

[49] **PFEIFER**, P. *: Multifunctional card with GPIB (IEEE-488) (In Czech, Journal),* Electus Special 2000,
link: http://www.volny.cz/ok1spc/Projects/1999%20-%20GPIB%20Multifunctional%20card/index.html

[50] **PFEIFER**, P. : *Intelligent accupack and power supply for handhelds (In Czech, Journal)*, Amateur Radio 7/1999,
link: http://www.volny.cz/ok1spc/Projects/1996%20-%20Intelligent%20Accupack%20for%20handhelds/index.html

Other Presentations (since 2012 only)

[1] **PFEIFER**, P.: MTBF alias reliability analysis/assessment, models, failure rate estimation methods and standards, Czech Technical University Praha (CVUT), invited talk, February 2012

[2] **PFEIFER**, P.: Reliability of microelectronic circuits and nanostructures (Spolehlivost mikroelektronických obvodů a nanostruktur), CVUT Praha, February 2012 (invited talk)

[3] **PFEIFER**, P.: FPGA aging measurement and results, TUT Tallinn, Estonia, February 2013, supported by COST Action MEDIAN STSM grant

[4] **PFEIFER**, P.: "Diachrony of Programmable Nanostructures: Aging effect on FPGAs down to 28nm", TUL&BTU ZUSYS seminar Dependable Systems on FPGAs, Liberec, September 2013

[5] **PFEIFER**, P., PLIVA, Z.: "Diachrony of Programmable Nanostructures: Investigating Aging of FPGAs down to 28 nm", 26th IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, invited paper, poster, New York city, NY, USA, October 2013

[6] **PFEIFER**, P., PLIVA, Z.: "Aging effect in New Technologies: Investigating 28nm and below", Centre for Integrated Electronic Systems and Biomedical Engineering - CEBE, Electronics Aging session, Tallinn, Estonia, October 2013, av. here http://cebe.ttu.ee/index.php?page=88

[7] **PFEIFER**, P.: Investigating diachrony of modern technologies – A new In-Situ method for complex measurements using programmable gate arrays ", IMEC, Leuven, Belgium, November 2013, supported by COST Action MEDIAN STSM grant

List of Supervised Students

Direct advisor (leader):

L.Sieber, "An intelligent measurement workplace with remote control and data processing framework", (Master, TUL, in progress)

J.Hadač, "Laboratory lessons using the intelligent measurement workplace platform", (Bachelor, TUL, in progress)

P.Vošta, "I2C bus data analysis tool" (Bachelor, TUL, finished)

A.Sůra, "Monitoring Station Main Unit of Intelligent Mobile Sensor System for Monitoring of Physical Quantities in Environment" (Master, CVUT, finished)

J.Pitelka, "Universal Processor Module for Intelligent Mobile Sensor System for Monitoring of Physical Quantities in Environment" (Master, CVUT, finished)

Indirect advisor:

L. Vítek, "Universal Fire Panel Tester", (Master, Tyco/VUT)

M. Smetana, "Universal test SW for Fire Panel Tester", (Master, Tyco/VUT)

A. Knápek, (Master, Tyco/VUT)

M. Hasal, (Master, CVUT)

Glossary

1/f noise: A type of random noise that increases in amplitude at lower frequencies. It is widely observable in physical systems, but not well understood. See *white noise* for comparison.

3-state buffer: A buffer that places an output signal in a high-impedance state to prevent it from contending with another output signal.

A

AC: Alternating Current. Electrical term for the portion of a signal that fluctuates around the average (DC) value.

ASCII: A method of representing letters and numbers in binary form. Each character is assigned a number between 0 and 127. Very widely used in computers and communication.

ASIC: An application-specific integrated circuit is an integrated circuit customized for a special or particular use, typically not intended for general-purpose uses.

Assembly: Low-level programming language that directly manipulates the registers and internal hardware of a microprocessor. See high-level language for comparison.

Attenuation: A decrease in magnitude of current, voltage, or electrical or optical power of a signal in transmission between points. It may be expressed in decibels or nepers.

Availability: It is the proportion of time a system is in a functioning condition, the total time a functional unit is capable of being used during a given interval to the length of the interval.

B

Basic state: Specific state of a system for use as a base for the evaluation of actual states of the system.

Binning: Method of forming a histogram when the data (or signal) has numerous quantization levels, such as in floating point numbers.

Bonding: A wire bonding is a manufacturing process of complete integrated circuit, in which the chip is mounted upright and wires are used to interconnect the chip pads to external circuitry. Today and in modern nanoscale technologies, typically copper material is used in both the chip metal layers as well as bonding wires (no gold wires are used anymore). Aluminium metal layers and wires (thickness about 250 to 400 μm) are used in other standard or older technologies.

Bump: Solder bumps are deposited on the chip pads on the top side of the wafer during the final wafer processing step in order to mount the chip to some external circuitry, like another chip or wafer, or circuit board. The chip is flipped over and the solder is reflowed to complete the interconnects.

Bus: (1) In a processor, a physical facility on which data is transferred to all destinations, but from which only addressed destinations may read in accordance with appropriate conventions. (2) A network configuration in which nodes are

interconnected through a bidirectional transmission medium. (3) One or more conductors used for transmitting signals or power.

Bus network: A network configuration that provides a bidirectional transmission facility to which all nodes are attached. A sending node transmits in both directions to the ends of the bus. All nodes in the path examine and may copy the message as it passes.

C

C: Common programming language used in science, engineering and DSP. Also comes in the more advanced C++.

C4: A flip chip technology, abbreviated also as Controlled Collapse Chip Connection, is a method for interconnecting semiconductor devices, such as IC chips.

CMOS: A technology for constructing integrated circuits by using complementary and typically symmetrical pairs of p-type and n-type metal oxide semiconductor field effect transistors (MOSFETs) for logic functions.

Configurable Logic Block (CLB): The basic FPGA cell, it includes function generators (lookup tables, or LUTs), registers (flip-flops or latches), and reprogrammable routing controls (multiplexers). CLBs implement macros and other designed functions. CLB provides the physical support for an implemented and downloaded design. CLBs have inputs on each side, and this versatility makes them flexible for the mapping and partitioning of logic.

Controller: A unit that controls input/output operations for one or more devices.

CPU: A central processing unit is the hardware within a computer system that carries out the instructions of a computer program by performing the basic arithmetical, logical, and input/output operations.

Crosstalk: The disturbance caused in a circuit by an unwanted transfer of energy from another circuit.

Cyclic redundancy check (CRC): Synonym for frame check sequence (FCS).

D

Datagram: A particular type of information encapsulation at the network layer of the adapter protocol. No explicit acknowledgment for the information is sent by the receiver. Instead, transmission relies on the “best effort” of the link layer.

DC: Direct Current. Electrical term for the portion of the signal that does not change with time; the average value or mean. See *AC* for comparison.

Dependability: It is a measure of a system's availability, reliability, and its maintainability.

Dependent variable: In a signal, the dependent variable depends on the value of the independent variable.

Destination: Any point or location, such as a node, station, or particular terminal, to which information is to be sent.

Die: A die is a small block or piece of semiconducting material, on which a given functional circuit is fabricated. Integrated circuits are produced in large batches on a single wafer, it is cut (“diced”) into many pieces, each containing typically the same one copy of given circuit.

Drain: A terminal (D) of the Field-Effect Transistor (FET) through which the carriers leave the channel. Drain-to-source voltage is V_{DS}.

E

Electromagnetic interference (EMI): A disturbance in a system or transmission of data on a network resulting from the magnetism created by a current of electricity.

EOT: An Equivalent Oxide Thickness is a distance in nanometers (nm), which indicates thickness of a silicon oxide film that would need to be to produce the same effect using given high-k material.

F

FET: The field-effect transistor is a transistor that uses an electric field to control the conductivity of a channel of one type of charge carrier in a semiconductor material.

Flip-flop: A bistable (trigger) circuits, a trigger circuit that has two *stable states.*

G

Gaussian: A bell shaped curve of the form e^{x^2}. The Gaussian has many unique properties. Also called the *normal distribution*.

Gate: A terminal (G) of the Field-Effect Transistor (FET) that modulates the channel conductivity. By applying voltage to G, one can also control Drain current.

GPU: A graphics processing unit - a specialized electronic circuit in computer systems designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display.

H

Hard error: An error condition on a network that requires that the source of the error be removed or that the network be reconfigured before the network can resume reliable operation. See also beaconing. Contrast with soft error.

Hertz (Hz): A unit of frequency equal to one cycle per second.

Huffman encoding: Data compression method that assigns frequently encountered characters fewer bits than seldom-used characters.

I

Impulse: See *pulse.*

Integers: Whole numbers: ⋯ -3, -2, -1, 0, 1, 2, 3, ⋯.

Integrated Circuit: A set of electronic circuits on one small plate (a "chip") of semiconductor material, typically silicon.

Interposer: An electrical interface routing between one socket, chip or connection to another. In microelectronics, an intermediate chip and layer that is often fabricated using much cheaper technologies (typically 65 nm interposer for 28 nm die) and metal layers only. It is used only for interconnection routing or as a ground/power plane.

J

Jitter: Undesirable variations in the time of a given event (sampling point, data arrival time, etc.).

K

κ: "low-k" (low-kay) or "low-κ" (low-kappa) is referred to a dielectric as a material with a small dielectric constant relative to silicon dioxide.

L

Layer: (1) One of the seven levels of the Open Systems Interconnection reference model. (2) In open systems architecture, a collection of related functions that comprise one level of hierarchy of functions. Each layer specifies its own functions and assumes that lower level functions are provided. (3) In SNA, a grouping of related functions that are logically separate from the functions of other layers. Implementation of the functions in one layer can be changed without affecting functions in other layers.

Linear system: By definition, a system that has the properties of additivity and homogeneity.

Link: (1) The logical connection between nodes including the end-to-end link control procedures. (2) The combination of physical media, protocols, and programming that connects devices on a network. (3) In computer programming, the part of a program, in some cases a single instruction or an address, that passes control and parameters

between separate portions of the computer program. (4) To interconnect items of data or portions of one or more computer programs. (5) In SNA, the combination of the link connection and link stations joining network nodes.

Logical connection: In a network, devices that can communicate or work with one another because they share the same protocol. See also physical connection.

Logical link control protocol (LLC protocol): In a local area network, the protocol that governs the exchange of frames between data stations independently of how the transmission medium is shared.

Lossless compression: Data compression technique that exactly reconstructs the original data, such as LZW compression.

M

Macrocell: A logic cell, which is made of gates only. A macrocell can implement both combinatorial and registered equations.

Maintainability: It is the ease or of the probability that a failed equipment, machine, or system can be restored to its normal operable state within a given timeframe.

Mapping: The process of assigning a design's logic elements to the specific physical elements that actually implement logic functions in a device.

Mean: The average value of a signal or other group of data.

Metastable state: see *unstable state.*

Multiplexer: A reprogrammable routing control. This component selects one input wire as output from a selection of wires.

N

Net: A logical connection between two or more symbol instance pins. After routing operations, the abstract concept of a net is transformed to a physical connection called a wire. It is used also as an electrical connection between components or nets. It can also be a connection from a single component (in this case the same as a wire or a signal).

Network layer: (1) In the Open Systems Interconnection reference model, the layer that provides for the entities in the transport layer the means for routing and switching blocks of data through the network between the open systems in which those entities reside. (2) The layer that provides services to establish a path between systems with a predictable quality of service. See Open Systems Interconnection (OSI).

Noise: (1) A disturbance that affects a signal and that can distort the information carried by the signal. (2) Random variations of one or more characteristics of any entity, such as voltage, current, or data. (3) Loosely, any disturbance tending to interfere with normal operation of a device or system.

Normal distribution: A bell shaped curve of the form e^{x^2}. Also called a Gaussian.

O

Open Systems Interconnection (OSI): (1) The interconnection of open systems in accordance with specific ISO standards. (2) The use of standardized procedures to enable the interconnection of data processing systems. *Note:* OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

Open Systems Interconnection (OSI) architecture: Network architecture that adheres to a particular set of ISO standards that relates to Open Systems Interconnection.

Open Systems Interconnection (OSI) reference model: A model that represents the hierarchical arrangement of the seven layers described by the Open Systems Interconnection architecture.

P

Path: A connected series of nets and logic elements. A path has a start point and an end point that are different depending on the type of path.

Path delay: The time it takes for a signal to propagate through a path.

Packet: In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. Synonymous with data frame.

Parameter space: One parameter can be graphically interpreted as a line, two parameters a plane, three parameters a space, and more than three parameters a hyperspace.

Patterning: It is the transfer of a pattern into a material in microelectronics.

Photolithography: It is a process of transferring geometric shapes (representing devices, circuits, wires and interconnections, etc.) on a mask to the surface of a silicon wafer.

Physical connection: The ability of two connectors to mate and make electrical contact. In a network, devices that are physically connected can communicate only if they share the same protocol. See also logical connection.

Physical layer: In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain, and release physical connections over the transmission medium.

Pointer: A variable whose value is the address of another variable.

Poisson statistics: Variations in a signal's value resulting from it being represented by a finite number of particles, such as: x-rays, light photons or electrons. Also called *Poisson noise* and *statistical noise.*

Port: (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. Synonymous with socket.

Precision: The error in a measurement or prediction that is not repeatable from trial to trial. Precision is determined by random errors. See *accuracy* for comparison.

Probability distribution function (pdf): Gives the probability that a *continuous* variable will take on a certain value. See *pmf* for comparison.

Probability mass function (pmf): Gives the probability that a *discrete* variable will take on a certain value. See *pdf* for comparison.

Propagation: The transmission of signal from one point in a design to other points.

Protocol: A set of semantic and syntactic rules that determines the behaviour of functional units in achieving communication, the sequencing rules for requests and responses used for managing the network, transferring data, and synchronizing the states of network components, a specification for the format and relative timing of information exchanged between communicating parties.

Prototyping: The first full-scale functional model of a new device, or the use of a model prior to the generation of a final version of a chip.

Pulse: A variation in the value of a magnitude, short in relation to the time schedule of interest, the final value being the same as the initial value.

Pull-down: A device or circuit used to reduce the output impedance of a device, often a resistor network that holds a device or circuit output at or less than the zero input level of a subsequent digital device in a system.

Pull-up: A device or method used to keep the output voltage of a device at a high level, often a resistor network connected to a positive supply voltage.

Pulse train: A series of *pulses* having similar characteristics.

Pulse string: see *pulse train*.

Q

Quantization error: The error introduced when a signal is quantized. In most cases, this results in a maximum error of ±½ LSB, and an rms error of 1/√12 LSB. Also called *quantization noise*.

Quasistable state: see *unstable state.*

QWORD: A Quad Word. Eight bytes.

R

RAM-based FPGA: An FPGA whose configuration data is programmed into random access memory. These devices are re-programmable. Some FPGAs allow also partial re-programmability or reconfiguration.

Random error: Error in a measurement or prediction, that it not repeatable from trial to trial. Determines *precision.* See *systematic error* for comparison.

Random access memory (RAM): A computer's or
adapter's volatile storage area into which data may
be entered and retrieved in a nonsequential manner.

Read-only memory (ROM): A computer's or adapter's storage area whose contents cannot be modified by the user except under special circumstances.

Reconfigurability, Reconfigurable Computing: Ability or a methodology of using programmable logic devices in a system design such that the hardware-based logic can be changed to perform various tasks. It may result in the use of fewer components, less power, and the flexibility that bring about. In a general meaning, it is used in remote control systems or system allowing external access to it, then it allows networked equipment in the field to be upgraded or repaired remotely.

Reliability: The ability of a system or component to perform its required functions under stated conditions for a specified period of time, ensuring a continuity of correct service.

Reparability: ease of restoring service after a failure.
Resistance: The property based on material, dimensions, and temperature of conductors determining the amount of current flowed or produced at a given difference in potential, while a material's current impedance that dissipates power in the form of heat. It is used also in the meaning of the drive of the output pins on a network.

Routing: Routing is the process of assigning logical nets to physical wire segments in the FPGA that interconnect logic cells.

Routing layer: A routing layer is a conductive layer used for interconnections.

Run-length encoding: Simple data compression technique with many variations. Characters that are repeated many times in succession are replaced by codes indicating the character and the length of the run.

S

Serviceability: It is the ease of conducting scheduled inspections and servicing.

Setup time: The amount of time required for a data input to be stable prior to the triggering edge of a clock device.

Signal: A description of how one parameter varies with another parameter. Example: a current that varies with time. It is also used for a wire or a net.

Silicon on insulator (SOI): It is a technology using a layered silicon-insulator-silicon substrate in place of conventional silicon substrates in semiconductor manufacturing and microelectronics, in order to reduce parasitic device capacitance and improvement of performance. It is used in industry since 1998.

Skew: It is defined as a Clock to signal delay in synchronous circuits.

Slack: The difference between the constraint and the analysed value. A negative slack indicates an error condition.

Slew Rate: The speed with which the output voltage level transitions from high to low or vice-versa. The slew rate determines how fast the transistors on the outputs change states.

SLICE: A fundamental building block of the FPGA, containing LUTs and registers. In Xilinx FPGAs, there are two slices in each Configurable Logic Block (CLB), though the specific contents

of the slice may vary with the device family. There are three types of slices: SLICEM, SLICEL, and SLICEX.

Soft error: An intermittent error in a circuit or on a network that causes information or data to have to be transmitted more than once to be received or processed. A soft error affects the system's performance but does not, by itself, affect the system's overall reliability. If the number of soft errors becomes excessive, reliability is affected. Contrast with hard error.

Source: A terminal (S) of the Field-Effect Transistor (FET) through which the carriers enter the channel**.**

Source code: A computer program in the form written by the programmer; distinguished from *executable code*, a form that can be directly run on a computer.

SRAM: Static Random Access Memory or volatile memory. SRAM holds a value as long as power is continually supplied. It loses its contents when the power is turned off

Stable state: In a trigger circuit, a state in which the circuit remains until the application of a suitable *pulse.*

State variable: Quantity describing the state of system.

Statistical noise: Variations in a signal's value resulting from it being represented by a finite number of particles, such as: x-rays, electrons, or light photons. Also called *Poisson statistics* and *Poisson noise*.

System: Any process that produces an output signal in response to an input signal.

Systematic error: Error in a measurement or prediction that are repeatable from trial to trial. Systematic errors determine *accuracy*.

Switch matrix: A collection of transistors located between configurable logic blocks that enables the connection of two interconnect lines. Place and Route phase and utilities use the switch matrices and interconnects to connect CLB inputs and outputs. Switch matrices reduce some of the net delay and the may have the three possible directions top, bottom, and left.

T

Thermal Design Power: A maximum amount of heat generated by the system or CPU, which the cooling system is required to dissipate in typical operation.

Tie-off cell or sites: In FPGAs, tie-off cells provide ESD protected logic levels '1' and '0' to be used for connecting transistor gates. The transistor gates in a design may be required to connect logic '1' and logic '0' permanently. It is represented by power supply V_{DD} (tie high cells) and common V_{SS} (tie low cells) logic levels, and it is usually tapped from near-by power lines. The Tie-off cells are placed between gates and power lines in order to ensure the transistor gate receives only ESD protected signals (tie HI/LO is usually one ESD protection diode preventing input poly oxide be stroking by electro-static current).

Topology: The physical or logical arrangement of nodes in a computer network. Examples include ring topology and bus topology.

Transceiver: Any device that can transmit and receive traffic.

Transmission speed: The number of signal changes transmitted per unit of time is called the data rate. That rate is usually expressed in terms of a unit known as a baud. The baud is the number of times per second the line condition can switch from "1" to "0". Data rate and transmission speed, which is expressed in terms of bits per second, usually are not the same, as several bits may be transmitted through the channel by the modem in each signal change (a few bits can be transmitted as one symbol).

Transform: A procedure, equation or algorithm that changes one group of data into another group of data.

Trigger circuit: A circuit that has a number of *stable states* or *unstable states*, at least one being stable, and is designed so that a desired transition can be initiated by application of suitable *pulse*.

Through-silicon via (TSV): A high-performance technique of vertical electrical connection passing completely through a silicon wafer or die.

Twisted pair: A transmission medium that consists of two insulated conductors twisted together to reduce noise.

U

UIM: Universal Interconnect Matrix - the routing matrix for CPLD or some programable devices. This fully populated switching matrix allows any output to be routed to any input, guaranteeing 100% routability of all designs. The UIM can also function as a very wide AND gate, which can allow more logic to be placed in macrocells.

Unique Word: a special codeword, generally used as synchronizing word

Unshielded twisted pair (UTP): Like as telephone twisted pair. One or more twisted pairs of copper wire in the unshielded voice-grade cable commonly used to connect a telephone to its wall jack. Also referred to as "unshielded twisted pair"

Unstable state: In a trigger circuit, a state in which a circuit remains for a finite period of time at the end of which it returns to a *stable state* without the application of a *pulse.*

V

Verilog: A hardware description language (HDL) used to model electronic systems, most commonly used in the design and verification of digital circuits at the register-transfer level of abstraction. It supports the verification of analogue circuits and mixed-signal circuits as well. Appeared in 1984, standardized as IEEE P1364-2005.

Via: A path or a way, a vertical interconnect access, an electrical connection between layers in an electronic circuit that allows a conductive connection between different layers. I goes through the plane of one or more adjacent layers. A small hole in an insulating oxide layer in integrated circuits.

VHDL: Since 1980, a hardware description language used in electronic design automation to describe digital and mixed-signal systems. Widely used in field-programmable gate arrays and integrated circuits, it can also be used as a general purpose parallel programming language [*128*]. Standardized as IEEE 1076 and IEEE 1164.

Von Neumann Architecture: Internal computer layout where both the program and data reside in a single memory; very common.

W

Wafer: A thin slice or substrate of semiconductor material, used in the fabrication of integrated circuits and other microdevices, containing a high number of a die on each single wafer.

Wire segment: A metal interconnect track that is physically located on the surface of the chip. Typically connections between two cells use multiple wire segments that are connected together to form an electrical connection.

wired-AND functions: AND gates and their DeMorgan equivalents produced by the inherent structure of the UIM.

wired-AND gate: A symbol, as opposed to a physical gate, representing a function generated from a wired connection of two NAND gates, for example.

wired logic: A wire connection between two gate outputs that provides a specific logic function.

Wireload: The maximum number of specified unit loads that a specified output can drive.

White noise: Random noise that has a flat frequency spectrum. Occurs when each sample in the time domain contains no information about the other samples. See *1/f noise* for comparison.

X

XADC: The XADC block, provided in Xilinx® 7 series FPGAs, includes a dual 12-bit, 1 Mega sample per second (MSPS) analog-to-digital converter and on-chip sensors.

XCF: The XCF (XST Constraint File) syntax allows you to specify a specific constraint for the entire device (globally) or for specific modules in your design.

XOR: A logical operation or a gate that forms exclusive disjunction or exclusive "or" where output is true whenever both inputs differ (one is true, the other is false).

Y

Yield: The proportion of devices or chips on the wafer which are found to perform all required functions properly. It is also is the percentage of defect-free (usable) die on a silicon wafer.

Z

Z-RAM: Zero-capacitor dynamic random-access memory technology based on the floating body effect of silicon on insulator (SOI) process technology.

Index

This page is intentionally left blank.