



ThalesAlenia
A Thales / Finmeccanica Company *Space*

Dependability related impacts of the utilization of FPGA's in space projects

TRISMAC 2008

M. Sarno; C. Cianci; R. Caterino; Thales Alenia Space (Italy)

THALES

Template reference : 100181670S-EN

Space projects have been increasingly using FPGA devices for the last years. Post programming antifuse failures experienced in the past, demonstrate that programmed antifuse may suffer latent damage during programming leading to infant or earlier-life mortality.

In terms of dependability analysis, this means that reliability established for the blank devices may be compromised through the programming step.

This has triggered the need to analyse and investigate in more details the *dependability related impacts of the utilization of FPGA's in space projects.*

In dependability engineering, the basic assumption is that ***the quantified failure data of the EEE components are only related to the probability of occurrence of random failures.***

- Use of space-approved EEE components is intended to ensure that the systematic failure rate (e.g. infant mortality) is negligible compared to the random failure rate.



This assumption may not be met in the case of MEC FPGAs

The work is intended to identify specific reasons to this statement and propose a dedicated dependability approach able to effectively cope with the issue of FPGA's failure in space projects and identifies the way to enhance the dependability of the design using FPGAs.

- Since 2003, different American factories (e.g. Aerospace, Boeing, JPL) reported that Field Programmable Gate Array Components (FPGA) of the family “SX-S” produced by Actel with technology 0,25 μm M2M at the Matsushita (MEC) facility in Japan, experienced functional failure in laboratory testing.
- A Tiger team (NASA and American Companies) was created to investigate the issue.
- Two types of failures were observed. Both of them are antifuse-related and happen after the programming phase inducing **signal delays** of different amount:
 - **Low Programming Current failure** causes a signal delays in the range of hundreds of pico seconds
 - **High programming Current failure** causes a signal delays of 10 to 100 nano seconds

- As a first solution ACTEL released a **New Programming Algorithm** called “New”, with respect to the previous called “Old”. It slightly reduce the probability of the failure but does not fully solve the problem.
- At the same time, in order to eliminate the occurrence of antifuse failures, **ACTEL developed a new version of these products**. The new products were given a different part number and the new device family (UMC RT54SX-SU) is manufactured in Taiwan facility.
- Test has been performed also on the new SX-SU devices and **no significant number of failures antifuse-related** was detected.

The first phase of this study was structured in the following steps:

- DATA SELECTION, starting from the available reliability test data on programmed FPGAs, to identify FPGA part-type with a sufficient amount of available data

- DATA ANALYSIS, studying the dependence of failures from factors related with the device:
 - Test Conditions
 - Design
 - Temperature
 - Applied Voltage
 - Frequency
 - Technology
 - Programming Algorithm
 - Process to get a programmed FPGA

- UNDERSTANDING of limiting factors by their evaluation

Data collected were used to perform statistical analysis using tools like Weibull distribution.

Weibull plots confirm the hypothesis of “infant mortality” which calls for a suitable screening procedure for the devices.

Analysis of factors limiting FPGAs dependability:

- **test conditions** have obviously a great influence on failure occurrence but available data don't show which are significant conditions on failure occurrence. This topic needs a further investigation;
- **design dependence** of the failures have been verified: test performed by ACTEL (QBI) is a less stressful design with respect to the Tiger Team design and it leads to a low failure rate. “Safe” conditions in FPGA's designing need to be investigated;

- **high temperature** is an accelerating factor: from 25°C to 125°C, $A_f=8$.
The high temperature causes an increase in failure rate but it is not the main accelerating factor;
- **the frequency dependence** of the failure rate was not observed;
- **applied voltage** is an accelerating factor more considerable than temperature:
from 2,5 V to 3.0 V, $A_f=50$.
Taken from JAXA paper, no detailed data are available;
- **the programming algorithm** reduce the probability of the failure but does not fully solve the problem;

- there are also some **factors related to the applied process to get a programmed** FPGA that can cause some kind of failures (like ESD failures or damages during FPGA programming). However this kind of failures, are detected immediately during FPGA programming or verification;
- the **antifuse technology** that characterizes the device is a major influencing factor on failure occurrence: the high-current damages on MEC antifuses don't appear on UMC devices.
 - The manufacturer states that the new technology effectively solves any problems and devices are now dependable.
 - ~ *Is it true?*
 - ~ *Will the failures appear after longer times?*
 - ~ *Will appear other kind of failures?*

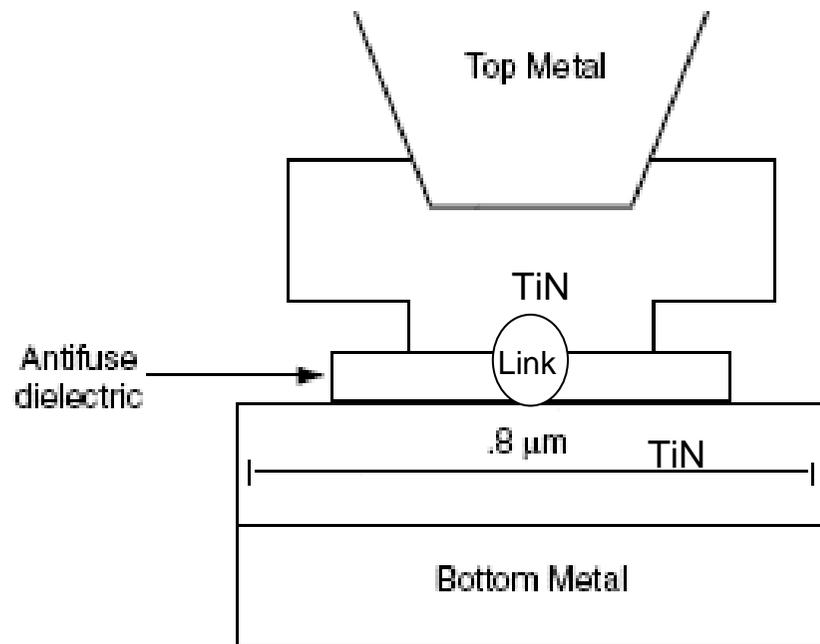
The proposal of methods to enhance FPGAs dependability involved the analysis of:

- **FAILURE MECHANISM** in antifuse-related device. Starting from the failure mechanism analysis performed by Actel, a numerical simulation has been performed as a further investigation on the causes of antifuse-related failures
- **DEPENDABILITY ENGINEERING RULES** (e.g. diversification, redundancy) & **ANALYSES** (e.g. FMECA, Derating) in presence of systematic failures. Proposal of new or completed analysis to enhance dependability
- **NEW POST PROGRAMING SCREENING** with proposal for future studies

The physical characteristics of the FPGA have been investigated to understand the FPGA's failure mechanism and how to improve the actual reliability program.

The understanding of the antifuse formation process and failure mechanism was necessary in order to propose additional and improved practices as specific countermeasures to the identified limiting factors.

Programming process



- A **current pulse is applied** to each antifuse in order to cause localized mass transfer in proximity of the amorphous silicon dielectric layer.
- The combination of high temperature and high electric field **causes the TiN barrier metal to flow through the dielectric**, making electric contact with the TiN barrier on the other side of the dielectric.
- As the conducting filament forms, the **resistance in the antifuse drops** from GΩ to several tens of Ω.

An electrostatic simulation have been performed with the aim of reaching a deeper knowledge on antifuse failure mechanism.

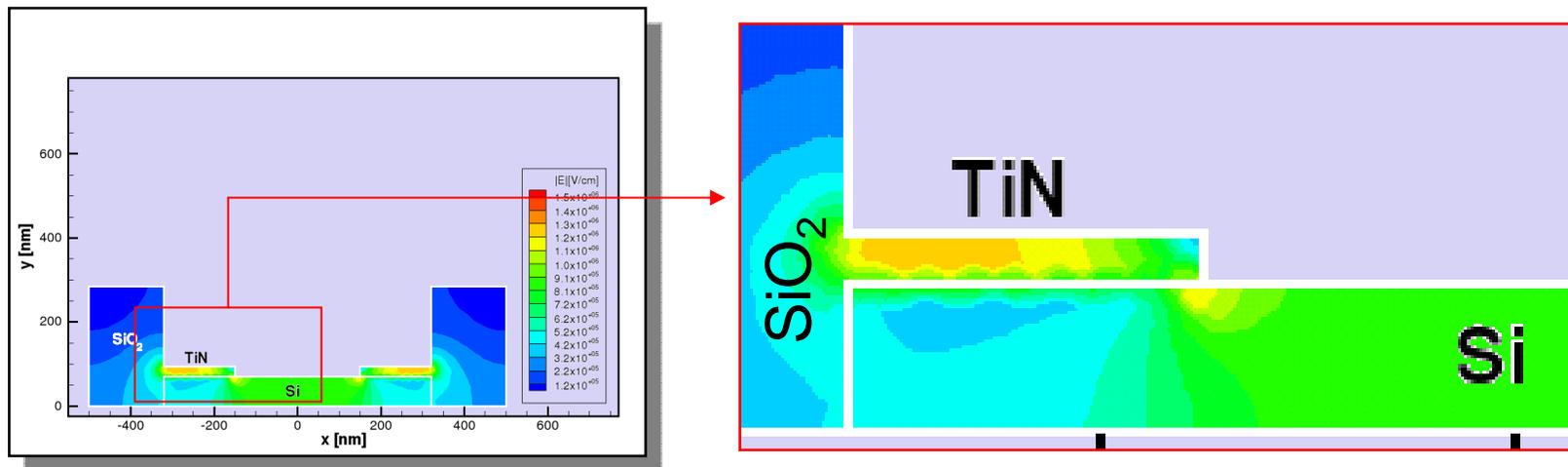
The simulation takes into account electrostatic effects of a 6.0 V voltage applied at the un-programmed antifuse ends and it allows us to see the values of electric field in the area where the conductive link will appear.

Simulation Constraints: a static simulation has been performed. It doesn't take into account any effects due to current flowing and matter percolation

Simulation software: TiberCAD

See www.tibercad.org for references

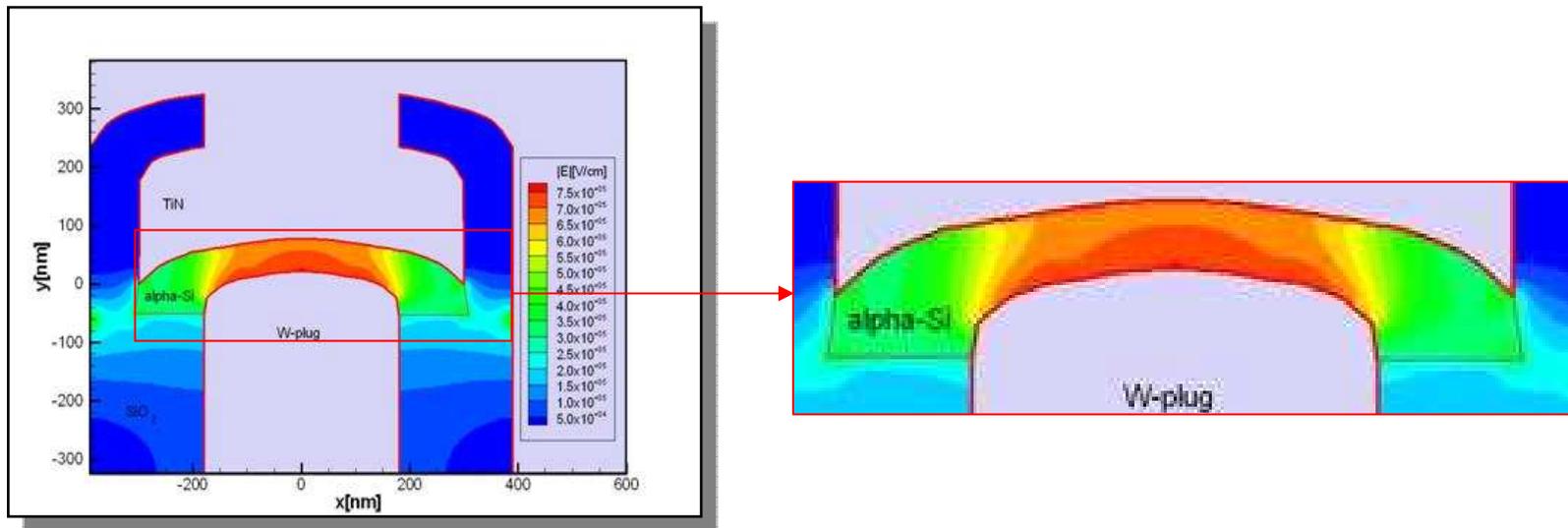
Simulation of electric field in device supporting MEC technology evidences a central area of high field and two areas of maximum field at the corner of the titanium nitride layer, in proximity of the silicon dioxide layer.



The corners are near to the silicon dioxide layer and the strong field in those areas enables the oxide's inclusion in conductive filament

The oxide compromises the filament's electrical conductivity, causing signal delay also if the TiN layers are linked by the conducting filament

The UMC technology solves this issue with a new antifuse geometry. Simulation in ACTEL UMC antifuse shows that the electrostatic field, at 6.0 V voltage applied at the antifuse ends, reaches its maximum values in the central area of the amorphous silicon layer.



The conductive link will appear in an area far from the silicon dioxide.

The simplified simulation we performed, would have had permitted to foresee a possible bad antifuse formation in the MEC antifuse.

- **An high supply voltage (i.e. biasing voltage) can shorten the device life by accelerating the failure mechanism more than temperature.**
 - JAXA experiments and their statistical processing on ACTEL MEC FPGA.
- *ACTEL states that **the root cause of the antifuse-related failures is the oxide involvement** in the conductive filament due to MEC antifuse structure that happen during the programming phase*
 - There is no data supporting the hypothesis that over-stressed application conditions can cause failure mechanism with oxide involvement
- Simulation outcomes: the role of geometry with high electric field (high programming voltage) is confirmed: MEC structure allows the formation of a conductive link through the oxide layer.

The antifuse will be bad programmed or well-programmed during the programming phase but undershoots and over-stress, especially an high supply voltage, could accelerate the failure detection

It has been assessed both the adequacy of the dependability engineering rules and reliability analysis application as countermeasures:

FPGA derating

It is effective because the failure rate of most part decrease as the applied stress level are decreased below their rated value.

Derating must be cost-effective.

- The derated voltage as specified in ECSS-Q-30-11A is very close to the manufacturer's recommended operating voltage

It is not possible to establish a further derating requirement for the supply voltage.

FPGA redundancy

Redundancy is an effective countermeasures in presence of random failure.

- Redundancy actually can not be considered an effective countermeasure for antifuse related failure until failure mechanism is not definitively excluded as systematic

FPGA FMECA

It's a current practice to perform a unit-level FMECA (design-FMECA) that consider FPGAs as black boxes.

- **A detailed FPGA-level FMECA** can contribute to a better evaluation of the failure risk. It can take into account the FPGA characteristics that can increase the failure risk
 - the **number of critical programmed antifuse in FPGAs**.
 - The use of a **routed clock** in the designs. ACTEL recommends to use the HCLK as the main clock of the design because it doesn't use antifuse and thus it can not fail.

- **A process FMECA** can be performed on the FPGA. Process FMECA is the application of the FMECA methodology to the manufacturing, integration and test processes to identify weak points and to determine their effects on the product and on the process itself.

FPGA diversification

For safety critical function, the required failure tolerance can be implemented in redundant equipment utilizing both different FPGA devices and software diversification.

- **Hardware diversification**: the main unit and the redundant one can be FPGAs from **different manufacturer** (e.g. ACTEL and ATMEL or AEROFLEX)
 - only if their reliability is proved to be at the same level-
- **Software diversification**: the same function can be implemented on two FPGAs by means of **two different design**.

Implementing diversification on two redundant devices can make effective the redundancy. Both manufacturer and design diversification have a very high cost impact

Post Programming screening based on Voltage Acceleration could be more effective than screening based on Temperature Acceleration (usually indicated as Post Programming Burn In)

- This is supported by the JAXA results, presented before, about voltage acceleration on failure's detection. (The detailed test data are not available)

The role of biasing voltage and current in antifuse-related failures is still to be investigated.

- The study provides considerations in order to propose a **dedicated dependability approach** able to deal with the issue of FPGA's failure and identifies the way to enhance the dependability of the design using FPGAs;
- it has been assessed both the adequacy of the dependability **engineering rules** and **reliability analyses** application as countermeasures;
- the **physical characteristics of the FPGA** have been investigated to understand the FPGA's failure mechanism performing a **static simulation** of electrostatic field inside the antifuse, before the programming phase. This **simplified simulation** would have had permitted to foresee a possible bad antifuse formation in the MEC antifuse;
- the antifuse will be bad programmed or well-programmed during the programming phase but high **biasing voltage** could accelerate the failure detection. The role of **biasing voltage** as accelerating factor need to be further investigated;

- dedicated **dynamic simulations** able to reproduce the process of antifuse programming with the percolation of the conductive link, could be very useful both to verify the effect of accelerated biasing voltage versus time on programmed antifuse and to evaluate *a priori* any failure-mechanisms in antifuse-based devices;
- for new FPGA's type a **process FMECA** should be suitable to analyse the whole process of productions phase;
- in future, before using new type of devices, in order to perform the above simulation/analysis it is necessary **a more cooperative relationship with the manufacturer** to receive FPGA physical characteristic and technical information. (e.g. programming parameters, etc...).