Design of Soft Error Tolerance Technique for FPGA Based Soft core Processors

Ishan M Safarulla[1] ,Karthika Manilal[2]
[1]PG Scholar, VLSI & Embedded Systems, [2]Assistant professor,
[1,2]TKM Institute of Technology,Kollam, Kerala, India
[1]ishansafarulla@gmail.com,[2]Karthikamanilal@gmail.com

Abstract— **SRAM-based FPGAs are susceptible to radiation-induced temporary faults called as single-event upsets (SEUs) or Soft errors. Soft errors affects or changes only some logic states of memory elements, but the device itself is not permanently damaged. SEUs may directly alter the logic states of any static memory element or induce changes to configuration memory. A new fault detection system architecture can be incorporated on any SRAM based FPGA with integrated soft core processors. It allows for detection of error in the system and also detects the processor with the error, so that the system can continue execution with the fault free processor. The fault detection system consists of a Lockstep scheme which is based on DWC technique. Lockstep Scheme detects the presence of error in the system but fails to point in which core, error is present. The Faulty core is detected using RESO Method which is based on DWC-CED technique. Once the faulty core is detected, fault tolerance is achieved using Fault tolerant Configuration Engine and by Hamming method. Fault Tolerant Configuration engine built on the basis of the PicoBlaze core, detects the fault location using CRC method and eliminates the error by frame based reconfiguration and is made fault-tolerant using triple modular redundancy (TMR). SEC using hamming method detects and corrects single bit error. Both the cores are synchronized back after fault recovery using CRB. The coding is done in VHDL language, synthesized using Xilinx ISE 13.2 and simulated using ISim.**

Keywords- SRAM, PicoBlaze, CED, Soft errors, TMR, FPGA, DWC, fault.

I. INTRODUCTION

Field Programmable Gate Arrays (FPGA) is well known devices concerning reconfigurable hardware. FPGAs consist of an array of programmable logic blocks surrounded by a programmable routing fabric that allows blocks to be programmably interconnected. The array is surrounded by programmable input/output blocks that connect the chip to the outside world. Every FPGA relies on an underlying programming technology that is used to control the programmable switches that give FPGAs their programmability. SRAM-based FPGA devices are steadily becoming the most suitable platform for implementing modern embedded applications due to their high re-configurability, low cost and availability. Static memory cells are the basis for SRAM programming technology which are distributed throughout the FPGA to provide configurability. The re-programmability feature of SRAM leads to high logic density in terms of SRAM memory cells. Due to high logic density in terms of SRAM memory cells, SRAM based FPGA's are sensitive to radiation and require protection to work in harsh environments. Due to the increasing integration density FPGA chips are getting more prone to faulty behavior caused by cosmic or artificial radiation .Such faults are modeled as Single Event Upsets (SEUs) or Transient faults.

SEU are the major concern in space applications [6].Many techniques have been developed to protect critical systems on SRAM FPGAs against SEU. These techniques are classified as SEU mitigation techniques which prevent SEU to disturb the normal operation of the target design, and SEU recovery techniques that recover the original programmed information in the FPGA configuration memory after an upset. The most common SEU mitigation techniques employ hardware redundancy like Triple Modular Redundancy (TMR), Duplication with Comparison (DWC), Duplication with Comparison with Concurrent Error Detection (DWC-CED) and Error Correcting Codes (ECC) such as Single error correction using Hamming Method.

This paper is organized as follows. Section 2 gives an outline of the paper. In Section 3, proposed method; fault detection using Lockstep scheme and RESO method, Fault tolerance using TMR based Configuration engine and SEC using hamming method along with Cores synchronization after fault tolerance is discussed. In section 4 the simulation results were discussed. Conclusions and on-going works are discussed in section 5.

II. REPORT OUTLINE

A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing. Programmable elements in a FPGA are used to configure the functionality of FPGA. The logic elements and routing switches depends on the programmable elements. Logic element includes LUT's (Look up table), MUX'es and Flip flops. Routing switches connects different logic blocks together and is controlled by programmable elements. There are different technologies for programming an FPGA. The technologies used are SRAM based, Anti-fuse and Flash based.

SRAM based FPGA's utilizes SRAM for expressing routing and core computational functions, through the use of LUT and MUX's. It uses SRAM switch as the programmable element which is a thin oxide pass transistor. Depending on the value of

switch gate voltage, switch can either allow data to pass from switch input or break connection between them. Switch gate voltage is controlled by output of SRAM. Logic cell configuration data is stored in the static memory which is organized as array of latches. SRAM technology uses bistable latching circuitry to store each bit. Features of SRAM technology includes Volatile, Fast re-programmability , Large area and more power consumption, High speed and do not need periodic refreshments etc.

Single event upset (SEU) is defined as radiation-induced errors in microelectronic circuits caused when charged particles (from radiation belts or from cosmic rays) lose energy by ionizing the medium through which they pass, leaving behind a wake of electron hole pairs. When a charged particle strikes a memory cells sensitive nodes, it generates a transient current pulse that can mistakenly turn on the opposite transistors gate[6]. The effect can produce a bit flip in the memory cell. This effect is called SEU. SEUs are non-destructive. SEUs are also called as soft errors, since it can be corrected by resetting the device and also only some logic state(s) of memory element(s) are changed but the circuit/device itself is not permanently damaged.

In FPGAs, SEUs may directly corrupt computation results or induce changes to configuration memory. Upsets need to be corrected only to ensure that errors do not accumulate. Charged particles can also change the logic function of the mapped circuit when they hit the on-chip configuration [6]. Transient faults occur because of radiations, electromagnetic interference, and power glitches. SEUs can affect both combinational and sequential circuits. It cause transient pulses in combinational logic paths. SEUs in configuration memory may result in modifications of the functionalities of the application design the FPGA implements. All configuration memory bits can be classified as being sensitive (whose upset induces errors) and non-sensitive[1]. The sensitive bits can be further categorized into two following categories:

Non persistent bits are those configuration bits which, when upset, may induce non persistent functional errors which disappear once the device is reconfigured.

Persistent bits are those configuration bits which, when upset, induce persistent functional errors, which do not disappear even after the device is reconfigured.

Soft-core processors are pretested and predesigned intellectual property microprocessors whose architecture and behavior are fully described using a synthesizable subset of a hardware description language (HDL) [2]. It can be designed for a reprogrammable fabric such as an FPGA [5]. PicoBlaze is a soft processor cores since they are synthesized from an HDL and use the programmable logic and routing resources of an FPGA for their implementation [10]. It is an 8-bit microcontroller architecture which can be synthesized in Spartan 3. PicoBlaze consists of two parts: 1) the processor core KCPSM3 (Ken Chapman Programmable State Machine version 3) and 2) the program memory from which instructions are fetched and executed by the processor core. There are also two VHDL files that are used to construct the complete PicoBlaze with program. The KCPSM3.vhd file is optimized for Spartan 3[10].The program memory is a VHDL file specific to the user's desired program to be executed by the PicoBlaze core and is generated automatically by the assembler (KCPSM3.exe) from assembly language program, titled name.psm. The program to be executed is initialized in the Block RAM and is assembled prior to synthesis. PicoBlaze and the KCPSM3 assembler support a total of 57 instructions.

Mitigation Technique is a process of applying design techniques to strengthen the functional integrity of the circuit, and protect it from the effect of any SEU [9]. Fault-tolerant methods used to mitigate logic errors in FPGA based on redundancy technique are as follows. Duplication with Comparison (DWC) for detecting the presence of faults in the system, Duplication with comparison with Concurrent Error Detection (DWC-CED) for detecting the faulty module in the system, Triple Modular Redundancy (TMR), SEC(Single Error Correction) using Hamming method for masking and tolerating faults.

A SEU immune circuit may be accomplished through a variety of mitigation techniques [7]. Redundancy is provided by extra components (hardware redundancy), by extra execution time (time redundancy), or by a combination of both. DWC is a simple hardware redundancy to detect errors in the circuit in which the circuit is replicated twice and the results produced by the original circuit and the replicated circuits are compared to detect faults. DWC is able to detect but not to correct errors and also fails to indicate the fault location. DWC offers so many advantages such as easy to apply to any circuit, detect a variety of errors, can detect errors immediately etc. DWC-CED combines DWC method with a CED (Concurrent Error Detection) based on time redundancy that work as a self-checking block [8]. DWC detects the faults in the system and CED detects which block is fault free. This mechanism is able to detect the faulty module and select the correct output of the two. The basic concept of time redundancy is the repetition of computation in a different way that allows the errors to be detected. During the first computation, the operands are used directly and the result is stored. During the second computation, the operands are modified, prior to use, so that errors due to faults in the combinational logic are different in the first calculation than in the second and can be detected when results are compared. TMR technique is a hardware redundancy technique in which, a circuit can be hardened to SEUs by making three copies and performing majority vote on the output [9]. If any one of the three systems fails, the other two systems can correct and mask the fault. Single Error Correction using Hamming method is an information redundancy method of fault tolerance by adding extra bits to the original data. Hamming codes are a family of linear error correcting codes. Hamming

codes can detect two and correct up to one bit errors. Hamming codes are widely used due to its simplicity. Adding one extra parity bit makes the code an extended hamming code. Extended hamming codes are single error correcting and double-error detecting (SECDED).

III. SYSYTEM ARCHITECTURE

The proposed system architecture consists of fault detection and Fault tolerance sections. Fault detection part detects the presence of error and identifies the faulty core in the system. Fault tolerance system localizes the fault location and recovers the system from the error. Figure 1 shows the system architecture.

A. Fault Detection

Fault Detection consists of Lockstep scheme, and RESO method. The Lockstep scheme based on DWC, detects the presence of fault in the system [1].Figure 2 shows the lockstep scheme.

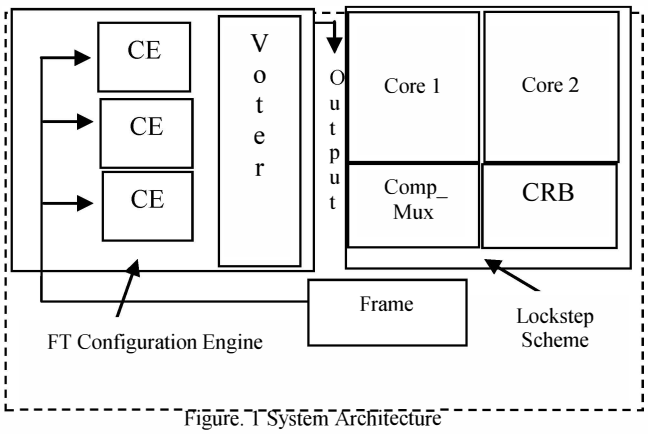

Figure. 1 System Architecture

Lockstep scheme consists of a Pair of PicoBlaze cores with one faulty, comparator and a multiplexer. Two identical PicoBlaze cores are provided with the same input. Their outputs are identical during fault-free functioning.

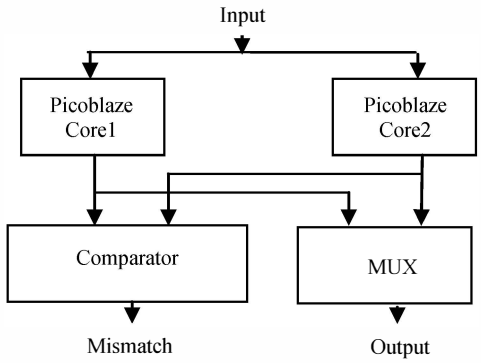

Figure. 2 Lockstep Scheme

Comparator indicates any mismatch between the outputs of cores. MUX connects one of the cores to the system output, so that if one is faulty, the other is switched on.

The RESO method based on DWC-CED technique detects the faulty core in the system and switches the correct core to output. Re-computing with shifted operands (RESO) is one of methods of Concurrent error detection (CED). The basic idea is to modify the operands before performing the re-computation so that an error affects different parts of the circuits. Here the computations are carried out twice, once on the basic input and once on the shifted input. Result from these two operations is compared to detect an error. Figure 3 shows the DWC-CED technique using RESO method [8].

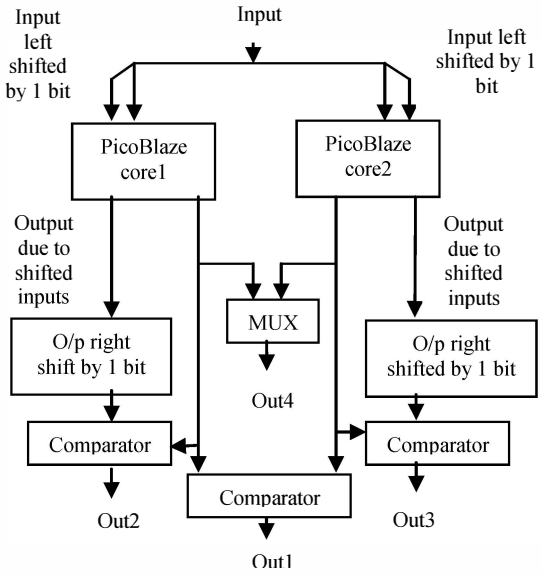

Figure. 3 RESO Method

The two identical PicoBlaze cores are provided with same inputs. The input is then left shifted by 1 bit and provided to the PicoBlaze cores along with the actual input. The output due to actual inputs from both cores is then compared. If it shows a mismatch it indicates that one of the cores is faulty. Now to determine the faulty core, the output due to left shifted inputs from each core is right shifted by 1 bit and then compared with the actual output of the corresponding core. If the comparator shows a mismatch, it indicates the corresponding core is the faulty one. Now the correct core is switched to output by using MUX module.

B. Fault Correction

Once the Faulty core is identified in the system, the faulty core has to be recovered. Fault tolerance is achieved through Fault tolerant Configuration Engine and by SEC (Single error correction) using Hamming Method.

A Fault tolerant configuration engine which is made fault tolerant using TMR technique locates the position of single bit

error in the faulty core and recovers the core from fault [1] .The configuration engine consists of a CRC generator, CRC checker and a PicoBlaze core. Figure 4 shows the Configuration engine based on TMR technique.

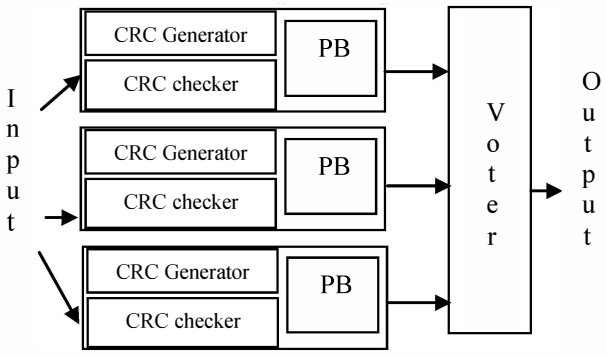

Figure. 4 TMR based Configuration Engine

Initially the Configuration memory data of both cores are read in the form of 8 bit frames. Cyclic Redundancy Check (CRC) based on binary division is a powerful technique for error detection [4]. Each Frames of core 1 is read and is provided to a CRC Generator one by one. CRC Generator performs binary division of the frame data by a predetermined binary number (divisor) to obtain redundant bits (remainder). This remainder is then concatenated with the corresponding frame of core 2 and performs the binary division again using the same divisor. If the remainder then obtained is zero, it indicates that both the frames (i.e. from core1 and core2) are same. If not, the corresponding frame has error. Then along with that frame, the corresponding correct frame from correct core is given to PicoBlaze core for fault recovery.Fault recovery is done by PicoBlaze core using partial reconfiguration concept. The PicoBlaze core copies the correct frame from the correct core (core1) and writes it to faulty frame location of core 2(faulty frame). Here instead of copying the entire frames, only faulty frame is replaced by corresponding correct frame, hence the name partial reconfiguration. The CE is made fault tolerant using TMR technique [1]. So if any one of the CE fails output will not get affected by the fault.SEC using Hamming method uses the concept of Extended Hamming method for error detection and correction [3]. Hamming encoder section takes 8 bit frame data from correct core and compute hamming bits and a parity bit. These redundant bits are then inserted into the corresponding frame of the core 2.In hamming decoder section, hamming bits and parity bit are again computed for the frame of core 2(with redundant bits).

The encoder has a 'k' bit input data in (D) and one output data out (n+k+1).For a word having k bit length, hamming code length of n bit is used[3]. The n value can be calculated by equation $2^n \geq n+k+1$. Let 8 bit word be (D8 to D1) each D represent each bit (1 or 0).

R1 = (D1 xor D2 xor D4 xor D5 xor D7)
R2 = (D1 xor D3 xor D4 xor D6 xor D7)
R3 = (D2 xor D3 xor D4 xor D8)
R4 = (D5 xor D6 xor D7 xor D8)

These hamming bits are to be interspersed at bit positions 2^n (n = 0, 1, 2, 3) with the original data bits. The parity bit, P1 is (D1 xor D2 xor D3 xor D4 xor D5 xor D6 xor D7xorD8 xor r1 xor r2 xor r3 xor r4).These 13 bits are transmitted as Data out. Figure 5 shows the encoded data format.

In decoder, 13 bit word is taken as Data in and decoded.

13	12	11	10	9	8	7	6	5	4	3	2	1
P1	D8	D7	D6	D5	R4	D4	D3	D2	R3	D1	R2	R1

Figure. 5 Encoded data format

For this 13 bit code, hamming bits and parity bit are calculated (as done in encoder).

R1=D1 xor D3 xor D5 xor D7 xor D9 xor D11
R2=D2 xor D3 xor D6 xor D7 xor D10 xor D11
R3=D4 xor D5 xor D6 xor D7 xor D12
R4=D8 xor D9 xor D10 xor D11 xor D12
Parity=D1 xor D2 xor D3 xor D4 xor D5 xor D6 xor D7 xor D8 xor D9 xor D10 xor D11 xor D12 xor D13

If the calculated hamming bit (in R4 R3 R2 R1) is 0000 and parity bit is 0, then the corresponding frames from both cores are same. If the calculated hamming bit is a non-zero value and parity is 1, then there is an error occurred in bit position indicated by the hamming code. Therefore the corresponding frames from both cores are different. Now by inverting the bit pointed by the hamming code, in the frame of core 2(Faulty core) the correct frame can be retrieve.Once the faulty core is recovered from the fault, both the cores has to be synchronized back to perform the functions together, which is carried out by Context recovery block (CRB) [1]. CRB copies the context of correct core to the recovered core. Figure 6 explains the context recovery. A context is the contents of a CPU's register and program counter value at any point in time. The context values of core 1 are transferred to core 2, and this process is controlled by control logic. Control logic acts as state machine, constructed using eight states, in which each states control the data transfer. During the first four states, data is transferred from core 1 to core 2 and in the next 4, these data's are outed from core 2.

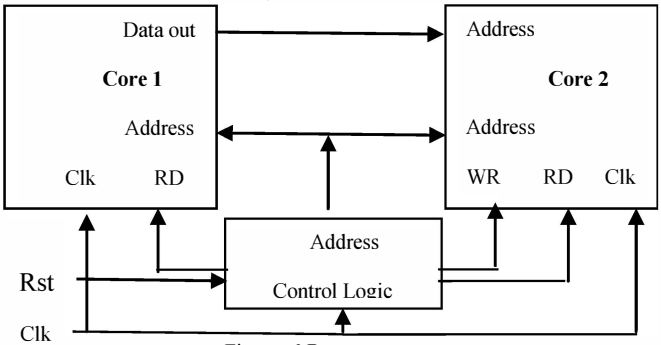

Figure. 6 Recovery process

IV. SIMULATION RESULTS

The design entry is modelled using VHDL and simulation using Isim using Xilinx ISE Design Suite 13.

Lockstep scheme detects the error presence in the system.

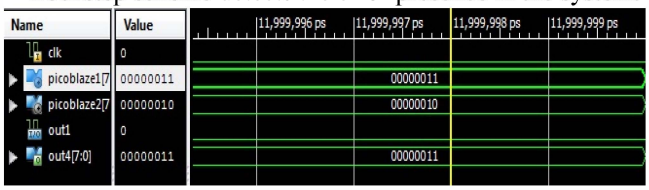

Figure. 7 Lockstep Scheme

The out1 and out4 port shows the Comparator and MUX outputs. RESO Method identifies the faulty core. The out1 and out4 shows the main comparator and MUX output.Out2 shows the comparator output for core1 and Out3 for core2..

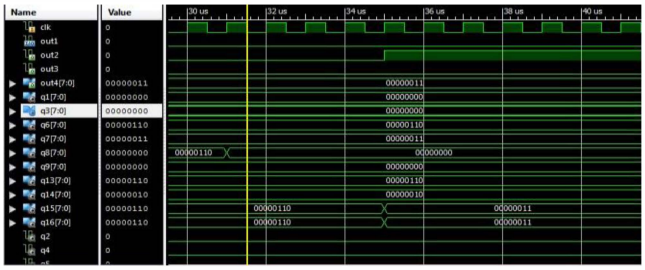

Figure. 8 RESO Method

Fault tolerant configuration engine for fault tolerance, recovers the system from fault.

Figure 9. Simulation of FT Configuration engine using TMR

SEC using Hamming Method for correcting single bit error consists of a hamming encoder and decoder section.

Figure 10. Simulation of Hamming Encoder

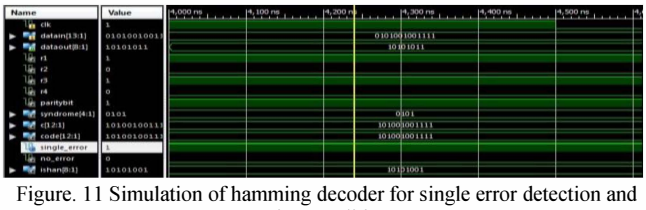

Figure. 11 Simulation of hamming decoder for single error detection and correction conditions

After the fault is removed from system, both cores are synchronized back using CRB.

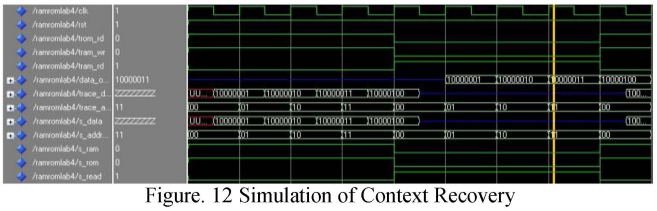

Figure. 12 Simulation of Context Recovery

V. CONCLUSIONS

SRAM based FPGA's are sensitive to radiation induced faults and require protection to work in harsh environments due to it's to high logic density in terms of SRAM memory cells. SRAM based FPGAs are affected by radiation induced temporary faults called as single event upsets (SEUs) or soft errors. That may alter the logic states of any static memory elements. The paper is intended to design a new architecture for soft error detection technique which can be incorporated on any SRAM based FPGA with integrated Soft-core processors. PicoBlaze is used as the Soft-core processor, which is a compact, capable, and cost-effective fully embedded 8-bit RISC virtual soft core optimized for the Xilinx FPGA families. Lockstep scheme based on DWC technique used to detect the presence of error in the system and RE-computing with Shifted Operand (RESO) method based on DWC-CED to detect the core with error are designed and simulated. Fault tolerance using TMR based configuration engine, by hamming method and cores synchronization using CRB are designed and simulated.

REFERENCES

[1] Hung-Manh Pham, SebastienPillement, Stanisław J. Piestrak "Low-Overhead Fault Tolerance Technique for a Dynamically Reconfigurable Soft-core Processor", IEEE transactions on computers, vol. 62, no. 6, June 2013

[2] Bertrand Le Gal and Christophe Jego "Soft core Processor Optimization According to Real-Application Requirements" IEEE embedded systems letters vol. 5, no.1, pp 4-7. March 2013

[3] Ajilesh R.K, Anand, Nandakumar.r & Sreejeesh.s.g"Design of configurable ip core for error detection and correction", Int. J. Comp. Science & Informatics, Vol 4 , 2231-5292 June 2012

[4] Wael M El Medany"FPGA Implementation of CRC", Int. Conf. Wireless and Mobile Commuinication, Sep. 2012

[5] P. Yiannacouras, J. G. Steffan, and J. Rose, "Exploration and customization of FPGA-based soft processors," IEEE Trans. Comp.-Aided Design. Circuit.,vol. 26, pp. 266–277, Feb.2007.

[6] DirettoredellaScuolaand Andrea Manuzzato"SINGLE EVENT EFFECTS ON FPGAs", Vol 3, December 2006

[7] Jonathan Johnson andWilliam Hower "Using Duplication with Compare for On-line Error Detection in FPGA,"December 2007

[8] Vatsya Tiwari , Pratap Singh Patwal " Design and analysis of software fault-tolerant techniques for soft-core processors in reliable sram-based fpga"pratap Singh Patwal , Int. J. Comp. Tech. Appl., Vol 2 (6), 1812-1819 June 2006

[9] Xilinx "Error detection and correction Techniques for Virtex FPGAs" February 2005.

[10] PicoBlaze 8-bit Embedded Microcontroller User Guide for Extended Spartan®-3 and Virtex®-5 FPGAs Introducing PicoBlaze for Spartan-6, Virtex-6 and 7 Series FPGAs, UG129 June 22, 2011