FPGA Assurance: from Radiation Susceptibility through Trust and Security

Melanie Berg, AS&D Inc. in support of the NEPP Program and NASA/GSFC

Melanie.D.Berg@NASA.gov

Kenneth LaBel: NASA/GSFC

Michael Campola: NASA/GSFC

Acronyms

Acronym	Definition
1MB	1 Megabit
3D	Three Dimensional
3DIC	Three Dimensional Integrated Circuits
ACE	Absolute Contacting Encoder
AHB	Advanced high performance bus
ADC	Analog to Digital Converter
AEC	Automotive Electronics Council
AES	Advanced Encryption Standard
AF	Air Force
AFRL	Air Force Research Laboratory
AMD	Advanced Micro Devices Incorporated
AMS	Agile Mixed Signal
ARM	Acorn Reduced Instruction Set Computer Machine
AXI	Advanced extensible interface
BAE	British Aerospace
BGA	Ball Grid Array
BRAM	Block Random Access Memory
BTMR	Block triple modular redundancy
BYU	Brigham Young University
CAN	Controller Area Network
CBRAM	Conductive Bridging Random Access Memory
CCI	Correct Coding Initiative
CGA	Column Grid Array
CMOS	Complementary Metal Oxide Semiconductor
CN	Xilinx ceramic flip-chip (CF and CN) packages are ceramic column grid array (CCGA) packages
COTS	Commercial Off The Shelf
CRC	Cyclic Redundancy Check
CRÈME	Cosmic Ray Effects on Micro Electronics
CRÈME MC	Cosmic Ray Effects on Micro Electronics Monte Carlo
CSE	Crypto Security Engineer
CU	Control Unit
DC	Direct current
DCU	Distributed Control Unit
DDR	Double Data Rate (DDR3 = Generation 3; DDR4 = Generation 4)
DFF	Flip-flop
DMM	Digital Multimeter
DMA	Direct Memory Access
DSP	Digital Signal Processing
DSPI	Dynamic Signal Processing Instrument
DTMR	Distributed triple modular redundancy
Dual Ch.	Dual Channel
DUT	Device under test
ECC	Error-Correcting Code
EDAC	Error detection and correction
EEE	Electrical, Electronic, and Electromechanical
EMAC	Equipment Monitor And Control
EMIB	Multi-die Interconnect Bridge
EPCS	Extended physical coding layer
ESA	European Space Agency
ETW	Electronics Technology Workshop
FASTIME	Framework for assessing security and trust in microelectronics
FCCU	Fluidized Catalytic Cracking Unit
FeRAM	Ferroelectric Random Access Memory
FinFET	Fin Field Effect Transistor
FIR	Finite impulse response filter
FPGA	Field Programmable Gate Array
FPU	Floating Point Unit
FY	Fiscal Year
Gb	Gigabit
Gbps	Gigabit per second
GCR	Galactic Cosmic Ray
GEO	geostationary equatorial orbit
GIC	Global Industry Classification
GOMACTech	Government Microcircuit Applications and Critical Technology Conference
GPIO	General purpose input/output
GPIB	General purpose interface bus
GPU	Graphics Processing Unit
GRC	NASA Glenn Research Center
GSFC	Goddard Space Flight Center

Acronym	Definition
GSN	Goal Structured Notation
GTH/GTY	Transceiver Type
GTMR	Global TMR
HALT	Highly Accelerated Life Test
HAST	Highly Accelerated Stress Test
HBM	High Bandwidth Memory
HDIO	High Density Digital Input/Output
HDR	High-Dynamic-Range
HiREV	High Reliability Virtual Electronics Center
HMC	Hybrid Memory Cube
HOST	Hardware Oriented Security and Trust
HP Labs	Hewlett-Packard Laboratories
HPIO	High Performance Input/Output
HPS	High Pressure Sodium
HSTL	High speed transceiver logic
I/F	interface
I/O	input/output
I2C	Inter-Integrated Circuit
i2MOS	Microsemi second generation of Rad-Hard MOSFET
IC	Integrated Circuit
I-Cache	independent cache
JFAC	Joint Federated Assurance Center
JPEG	Joint Photographic Experts Group
JPL	Jet propulsion laboratory
JTAG	Joint Test Action Group (FPGAs use JTAG to provide access to their programming debug/emulation functions)
KB	Kilobyte
L2 Cache	independent caches organized as a hierarchy (L1, L2, etc.)
LCDT	NEPP low cost digital tester
LEO	Low Earth Orbit
LET	Linear energy transfer
L-mem	Long-Memory
LANL	Los Alamos National Laboratory
LP	Low Power
LUT	Look-up table
LVCMOS	Low-voltage Complementary Metal Oxide Semiconductor
LVDS	Low-Voltage Differential Signaling
LVTTL	Low –voltage transistor-transistor logic
LTMR	Local triple modular redundancy
LW HPS	Lightwatt High Pressure Sodium
M/L BIST	Memory/Logic Built-In Self-Test
Mil-STD	Military standard
MAPLD	Military Aerospace Programmable Logic Device
MBMA	Model-Based Missions Assurance
MFTF	Mean fluence to failure
μPROM	Micro programmable read-only memory
μSRAM	Micro SRAM
Mil/Aero	Military/Aerospace
MIPI	Mobile Industry Processor Interface
MMC	MultiMediaCard
MOSFET	Metal-Oxide-Semiconductor Field-Effect Transistor
MP	Microprocessor
MP	Multiport
MPFE	Multiport Front-End
MPSoC	Multiprocessor System on a chip
MPU	Microprocessor Unit
Msg	message
MTTF	Mean time to failure
NAND	Negated AND or NOT AND
NASA	National Aeronautics and Space Administration
NASA STMD	NASA's Space Technology Mission Directorate
Navy Crane	Naval Surface Warfare Center, Crane, Indiana
NEPP	NASA Electronic Parts and Packaging
NGSP	Next Generation Space Processor
NOR	Not OR logic gate

Acronym	Definition
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
OCM	On-chip RAM
PC	Personal Computer
PCB	Printed Circuit Board
PCIe	Peripheral Component Interconnect Express
PCIe Gen2	Peripheral Component Interconnect Express Generation 2
Pconfiguration	SEU cross-section of configuration
Pfunctional_logic	SEU cross-section of functional logic
PHY	Physical layer
PLL	Phase Locked Loop
PMA	Physical Medium Attachment
POR	Power on reset
Proc.	Processing
PS-GTR	High Speed Bus Interface
PSEFI	SEU cross-section from single event functional interrupts
Psystem	System SEU cross-section
QDR	quad data rate
QFN	Quad Flat Pack No Lead
QML	Qualified manufactures list
QSPI	Serial Quad Input/Output
RADECS	IEEE Radiation and its Effects on Components and Systems
RC	Resistor capacitor
R&M	Reliability and Maintainability
RAM	Random Access Memory
ReRAM	Resistive Random Access Memory
RGB	Red, Green, and Blue
RH	Radiation Hardened
RT	Radiation Tolerant
SATA	Serial Advanced Technology Attachment
SCU	Secondary Control Unit
SD	Secure Digital
SD/eMMC	Secure Digital embedded MultiMediaCard
SD-HC	Secure Digital High Capacity
SDM	Spatial-Division-Multiplexing
SEE	Single Event Effect
SEFI	Single Event Functional Interrupt
SEL	Single event latchup
SERDES	Serializer/deserializer
SET	Single event transient
SEU	Single event upset
Si	Silicon
SK Hynix	SK Hynix Semiconductor Company
SMDs	Selected Item Descriptions
SMMU	System Memory Management Unit
SNL	Sandia National Laboratories
SOA	Safe Operating Area
SOC	Systems on a Chip
SPI	Serial Peripheral Interface
SSTL	Sub series terminated logic
TBD	To Be Determined
Temp	Temperature
THD+N	Total Harmonic Distortion Plus Noise
TMR	Triple Modular Redundancy
T-Sensor	Temperature-Sensor
TSMC	Taiwan Semiconductor Manufacturing Company
UART	Universal Asynchronous Receiver/Transmitter
UltraRAM	Ultra Random Access Memory
USB	Universal Serial Bus
VNAND	Vertical NAND
WDT	Watchdog Timer
WSR	Windowed shift register
XAUI	Extended 10 Gigabit Media Independent Interface
XGXS	10 Gigabit Ethernet Extended Sublayer
XGMII	10 Gigabit Media Independent Interface)
XWSG	Xilinx Security Working Group

Outline

- Field programmable gate array (FPGA) single event effect (SEE) test guidelines.
- Xilinx Kintex-UltraScale heavy-ion single event upset (SEU).
- Upcoming heavy-ion testing.
- Proton SEE test results.
- Xilinx Kintex-UltraScale Deliverables.
- Challenges: Xilinx Kintex-UltraScale SEE testing.
- NEPP involvement with FPGA security and trust.

NEPP…Providing the following for FPGA driven applications: guidance, radiation SEE data and analysis, mitigation strategies, and government trust/security process development.

FPGA SEU Test Guidelines

DUT: device under test

- **Impact to community:**
  - It can be challenging to compare FPGA SEU data because of differences in test vehicle and test methodology.
  - The FPGA SEU Test Guidelines Document creates standardized test methodologies and provides a means for data comparison across organizations and FPGA types.
  - The FPGA SEU Test Guidelines Document points out best practices for DUT test structures, monitoring DUT functional response, visibility into DUT operation, DUT control, and DUT power.
- **Update of the test guideline best practices will be available by October 2018.**
  - Additional test structures for SEU investigations.
  - Additional "do's" and "should-not-do's."
  - Embedded processor testing techniques.

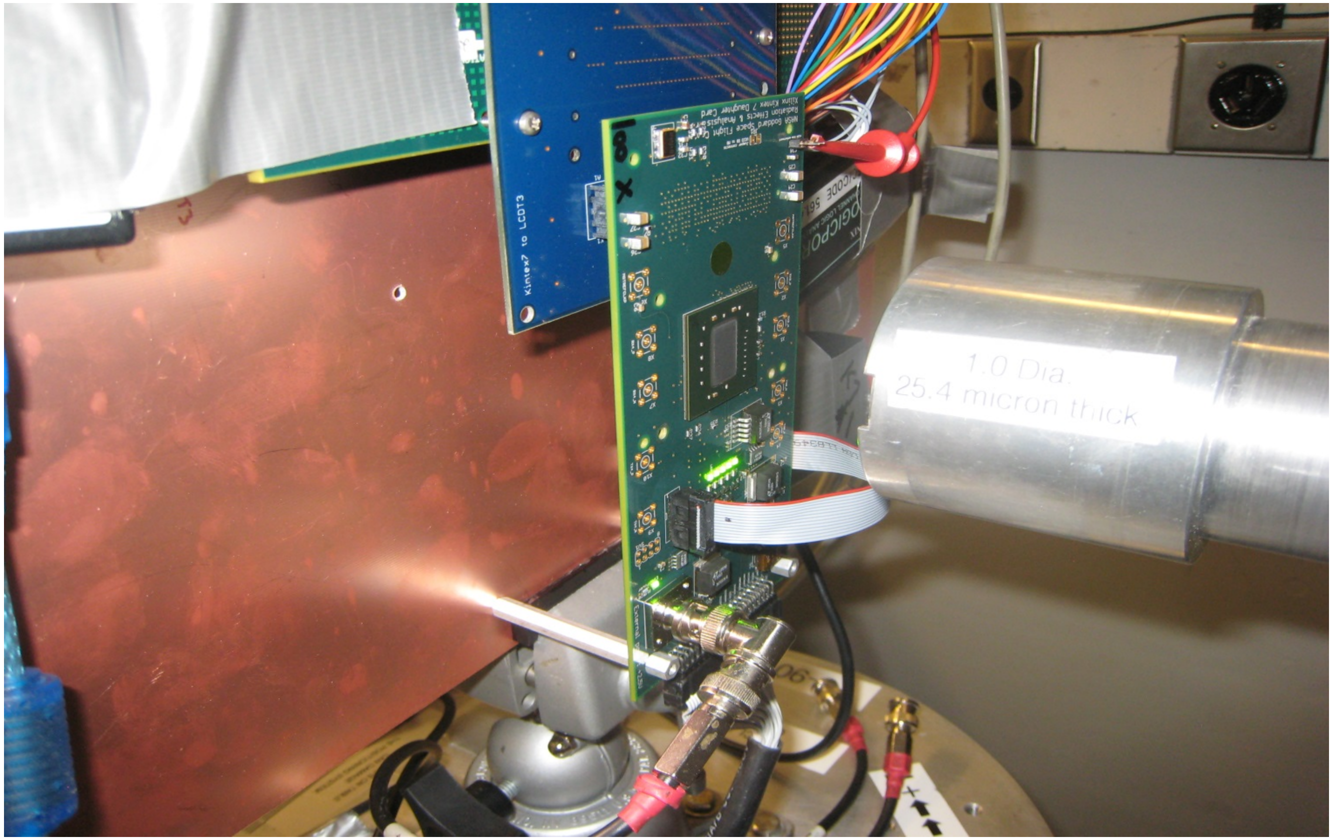
https://nepp.nasa.gov/files/23779/fpga_radiation_test_guidelines_2012.pdf

NEPP FPGA Radiation Testing Is Differentiated From Most Other Organizations

- **Low cost digital tester (LCDT) – board with FPGA that supplies DUT stimulus and monitors DUT response.**
- **Custom built DUT board that connects via high speed interface to the LCDT.**
- **Visibility of DUT response is significantly enhanced versus evaluation boards.**
- **LCDT is state machine based (not processor based). Provides fine grained monitoring and reporting (*ns* versus *s*).**
  - **Hak Kim and the NEPP engineering team built the LCDT board.**
  - **Custom test controls are designed into the LCDT FPGA.**
  - **Custom test structures are designed into the DUT FPGA.**
- **NEPP currently uses evaluation boards for memory testing.**
- **NEPP is investigating the use of evaluation boards for complex FPGA testing.**

SRAM: Static random access memory

SRAM-based FPGA Mitigation Study using Xilinx Kintex-UltraScale (XCKU040-1LFFVA1156I)



Impact to Community
Kintex-UltraScale

σ_{SEU}: SEU Cross-section *SEFI: Single event functional interrupt*

- **Current generation of Xilinx FPGA devices targeted for space applications.**
- **High-speed I/O interfaces are significantly more robust than previous generations.**
- **There are no embedded mitigation circuits in the user fabric. However, higher gate-count allows the user to more efficiently insert mitigation into the design.**
- **There is no embedded processor. However, the user can embed a soft-core.**

$$P(fs)_{system} \propto P_{Configuration} + P(fs)_{functionalLogic} + P_{SEFI}$$

Design σ_{SEU} ***Configuration σ_{SEU}*** ***Functional logic σ_{SEU}*** ***SEFI σ_{SEU}***

NEPP performs an independent study to determine the level of SEU susceptibility for the various FPGA components.

Xilinx Kintex-UltraScale Study Objectives

- This is an independent investigation that evaluates the single event destructive and transient susceptibility of the the Xilinx Kintex-UltraScale device.
- FPGA susceptibility is both design and device dependent.
  - There will be events that are unique to a design.
  - There will be events that are specifically due to device features.
- Design/Device susceptibility is determined by monitoring the DUT for Single Event Transient (SET) and Single Event Upset (SEU) induced faults by exposing the DUT to a heavy ion beam.
- Potential Single Event Latch-up (SEL) is checked throughout heavy-ion testing by monitoring device current and temperature.
- This device does not have embedded mitigation. Hence, user implemented mitigation is investigated using Synopsys mitigation tools.
- FPGA part# XCKU040-1LFFVA1156I.
- Collaboration: Xilinx, Mentor Graphics, and Synopsys.

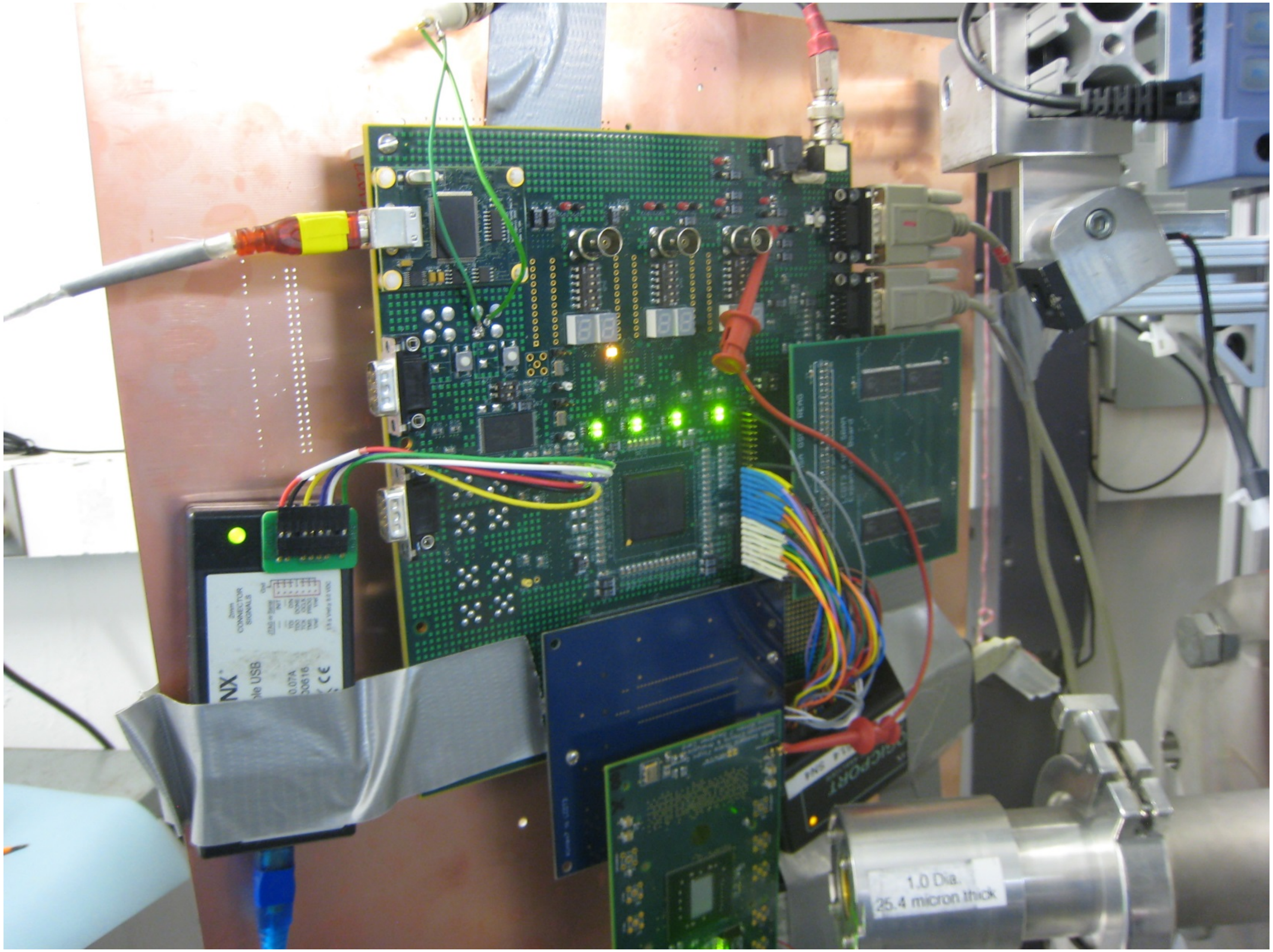
Test Facility Conditions

- Facility: Texas A&M University Cyclotron Single Event Effects Test Facility, 25 MeV/amu tune.
- Flux: 1 x 10^2 to 5 x 10^5 particles/$cm^{2\cdot}$s
- Fluence: All tests were run to 1 x 10^7.. 5 x 10^7 particles/cm^2 or until destructive or functional events occurred.

Ion	Energy (MEV/Nucleon)	LET (MeV*cm^2/mg) 0°	LET (MeV*cm^2/mg) 60 °
He	25	.07	.14
N	25	0.9	.18
Ne	25	1.8	3.6
Ar	25	5.7	11.0
Kr	25	20.4	40.0
Xe**	25	38.9	78.8

We were unable to obtain Kr and Xe during our testing

Kintex-UltraScale DUT And Tester



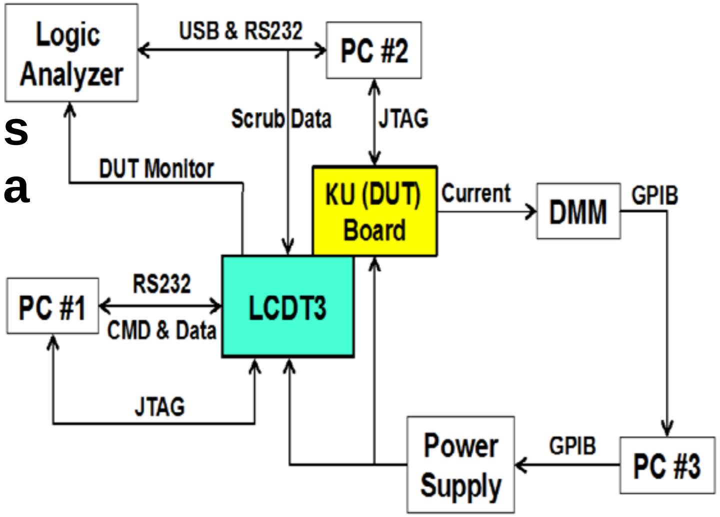
Test Setup Details (1)

- NEPP Low Cost Digital Tester (LCDT3)
  - Control Kintex-UltraScale Operation Modes and Execution.
  - Collect All Data from Kintex-UltraScale Board, analyze data and report the results to PC #1.
- PC #1
  - Configure LCDT3 via JTAG. Send Commands LCDT via RS232. Receive Data from LCDT via RS232.
- PC #2
  - Configure Kintex-UltraScale via JTAG. Readback Kintex-UltraScale configuration data after irradiation.
  - Send Kintex-UltraScale configuration data for DUT configuration scrubbing via USB & RS232.
  - Run and display logic analyzer capture via USB.

JTAG: joint test access group

RS232: Recommended Standard 232

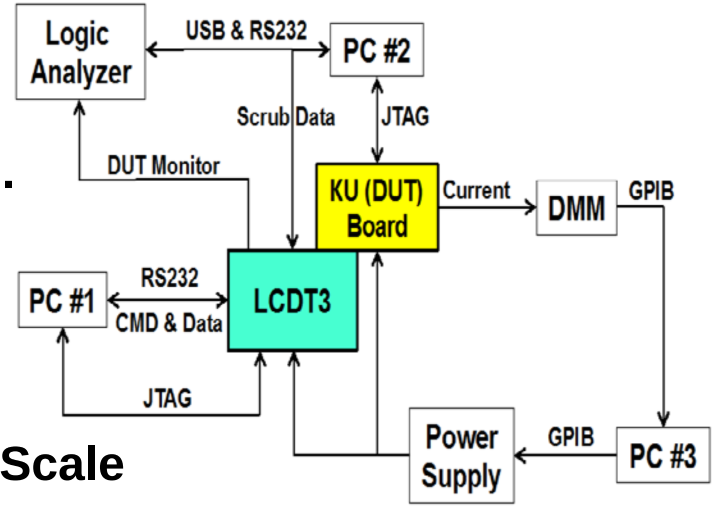
USB: Universal Serial Bus



Test Setup Details (2)

GPIB: general purpose interface bus

- DMM (digital multimeter)
  - Scan Kintex-UltraScale supply current measurement.
  - Measures Xilinx device voltage planes: VCCINT, VCCO, VCCAUX, VCCMGT , VTxRx.
  - Monitors temperature from the on-chip diode.
- PC #3
  - Control DC Power Supply via GPIB.
  - Collect current readings from DMM via GPIB.
- Logic Analyzer
  - Monitor Kintex-UltraScale operation status.
- Power Supply
  - Provide power to both LCDT3 & Kintex-UltraScale board.
- Kintex-UltraScale DUT
  - Although there are various components on this board (as illustrated in Figure 4), only the mounted Kintex-UltraScale device is subjected to the heavy-ion beam.



History of Xilinx and SEL or Latchup-Like Events: Virtex 2 through UltraScale Series

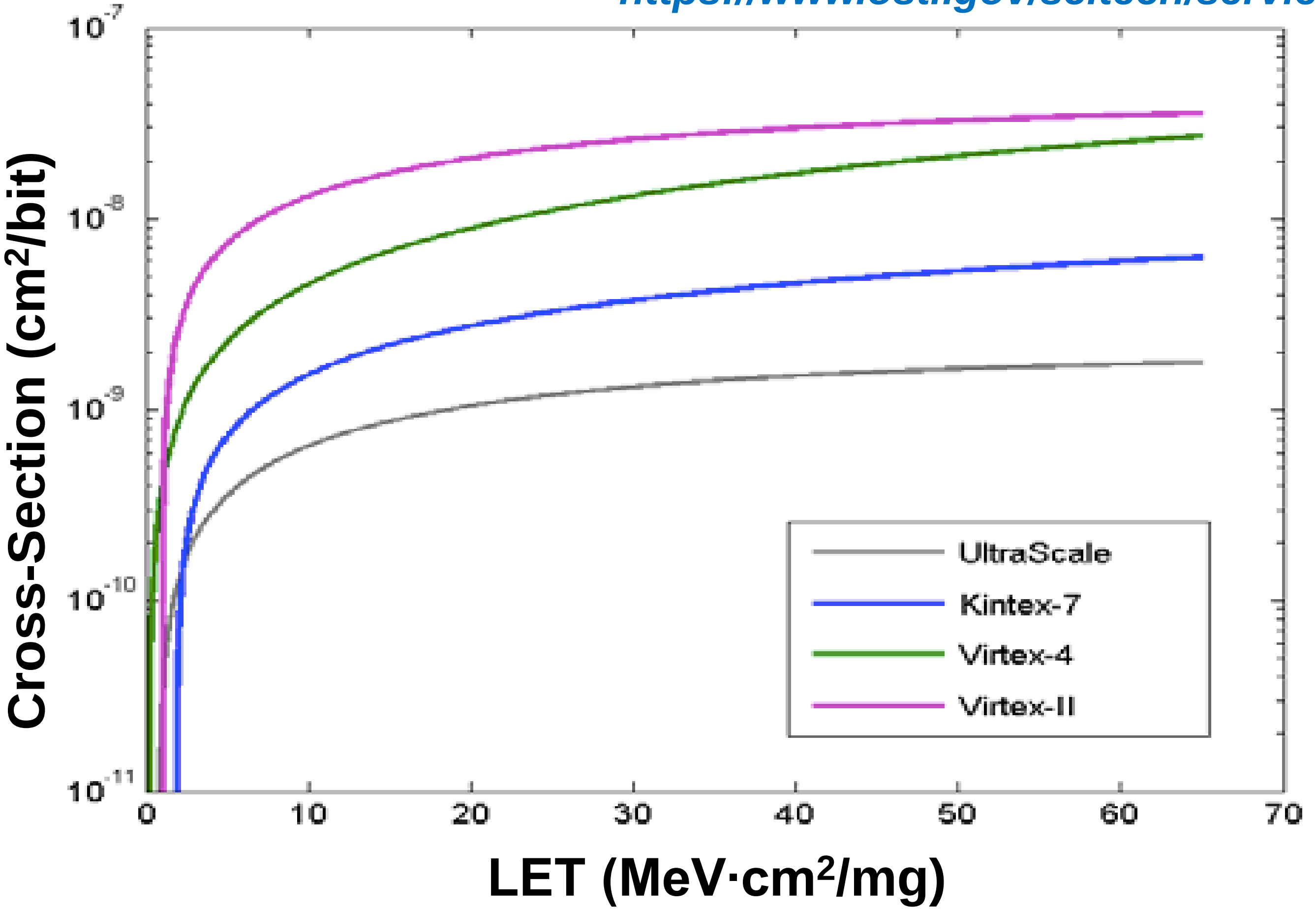
Latchup-like event: A component is affected by an ionizing particle such that current is increased and held. A power-cycle is required for the circuit to release the current.

- **Xilinx Virtex 2: Latchup-like events have been observed in flight. Most likely due to embedded half-latches in the device.**
- **Xilinx Virtex 5: Half-latches were removed. No latchup-like events observed during SEE testing or in flight.**
- **Xilinx 7-series: Is it SEL or latchup-like? Observed only on 7-series devices that contained 3.3V I/O. Devices that do not contain such I/O have no latchup-like events.**
- **Xilinx UltraScale series no latchup-like event observed.**
- **Xilinx UltraScale+ series latchup-like events observed.**

Xilinx Scaling Family Trends for Configuration Bits in Heavy Ions

David Lee et. al. "Single-Event Characterization of the 20 nm Xilinx Kintex-UltraScale Field-Programmable Gate Array under Heavy Ion Irradiation"

https://www.osti.gov/scitech/servlets/purl/1263983



Daily configuration upsets are expected in LEO and GEO.

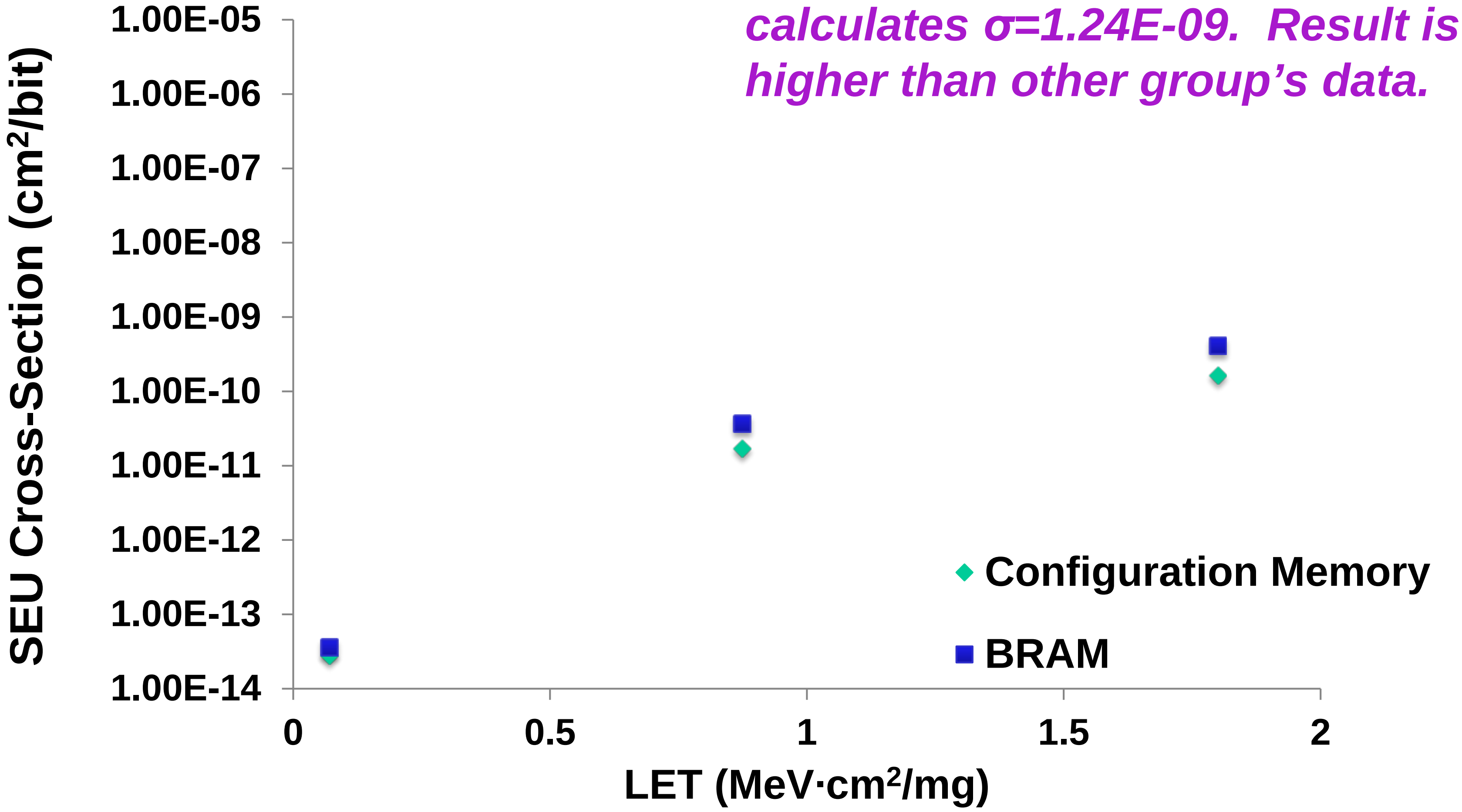
NEPP Kintex-UltraScale Configuration Memory and BRAM SEU versus LET

BRAM: Block Random Access Memory

SEU: single event upset

LET: linear energy transfer

At LET=20.4MeVcm^2/mg, NEPP calculates σ=1.24E-09. Result is higher than other group's data.



To be presented by Melanie Berg at the NASA Electronics Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June18–21, 2018

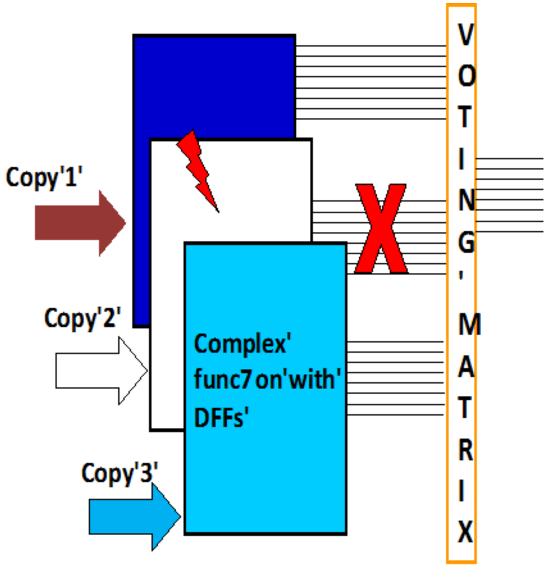
Highlighted Configuration and BRAM Results

- Rumors: Configuration memory (CRAM) is hardened in the Xilinx Kintex-UltraScale and BRAM is not hardened.
- Data suggest otherwise. Relative BRAM versus CRAM SEU-data look similar to other series and do not reflect hardened results.
- At an LET=1.8MeVcm^2/mg, the BRAM experienced a reset SEFI.
  - Static test - MFTF of occurrence is not known.
  - Total fluence of static test was 1.0E+07.
  - CRAM did not seem to be affected at this LET.
- Tests show blockage/shadowing at angle.
  - Occurred at two out of three test trips.
  - Angular results (45° and 60°) have lower SEU cross-sections.
  - Clear view of device in beam. Must be internal shadowing – device orientation.
  - Additional tests will be performed with different orientations.

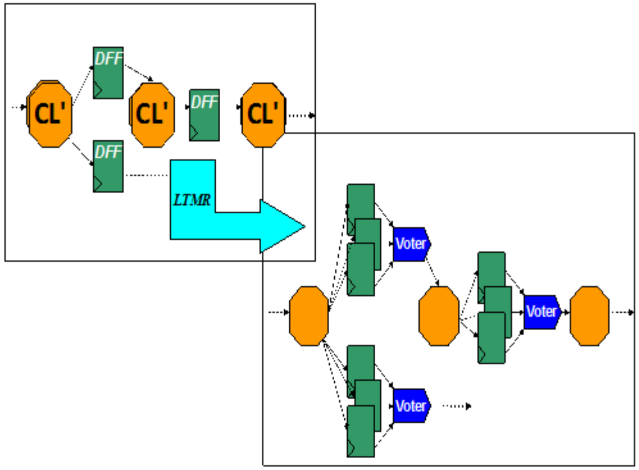
Xilinx Kintex-UltraScale Dynamic SEE Tests

- All dynamic tests are set up prior to beam to include configuration scrubbing:
  - All scrubbing is external to device.
  - One scrub cycle is in the order of ms.
  - Scrubber works in heavy-ion beam. Proven by reading back configuration post DUT exposure.
- A variety of parameters are used for dynamic testing to increase state space traversal during beam exposure.

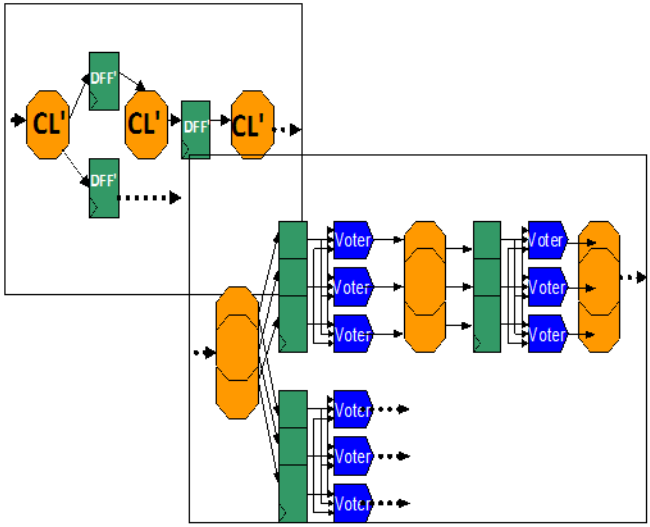
Various Triple Modular Redundant (TMR) Schemes Implemented in FPGA Devices



Block diagram of block TMR (BTMR): a complex function containing combinatorial logic (CL) and flip-flops (DFFs) is triplicated as three black boxes; majority voters are placed at the outputs of the triplet.



Block diagram of local TMR (LTMR): only flip-flops (DFFs) are triplicated and data-paths stay singular; voters are brought into the design and placed in front of the DFFs.



Block Diagram of distributed TMR (DTMR): the entire design is triplicated except for the global routes (e.g., clocks); voters are brought into the design and placed after the flip-flops (DFFs). DTMR masks and corrects most single event upsets (SEUs).

TMR can be embedded in the FPGA or user inserted.

Kintex-UltraScale Designs Tested

Test Structure	Frequency Range
Counter Array No TMR	50MHz
Counter Array DTMR with partitioning	50MHz
Counter Array DTMR no partitioning	50MHz
Counter Array BTMR with partition	50MHz
Counter Array LTMR with partition	50MHz

For the current test set, all counter-array mitigation was inserted using Synopsys Premier .

Currently, NEPP is the only organization with heavy-ion data for the Synopsys and Mentor Graphics mitigation tools.

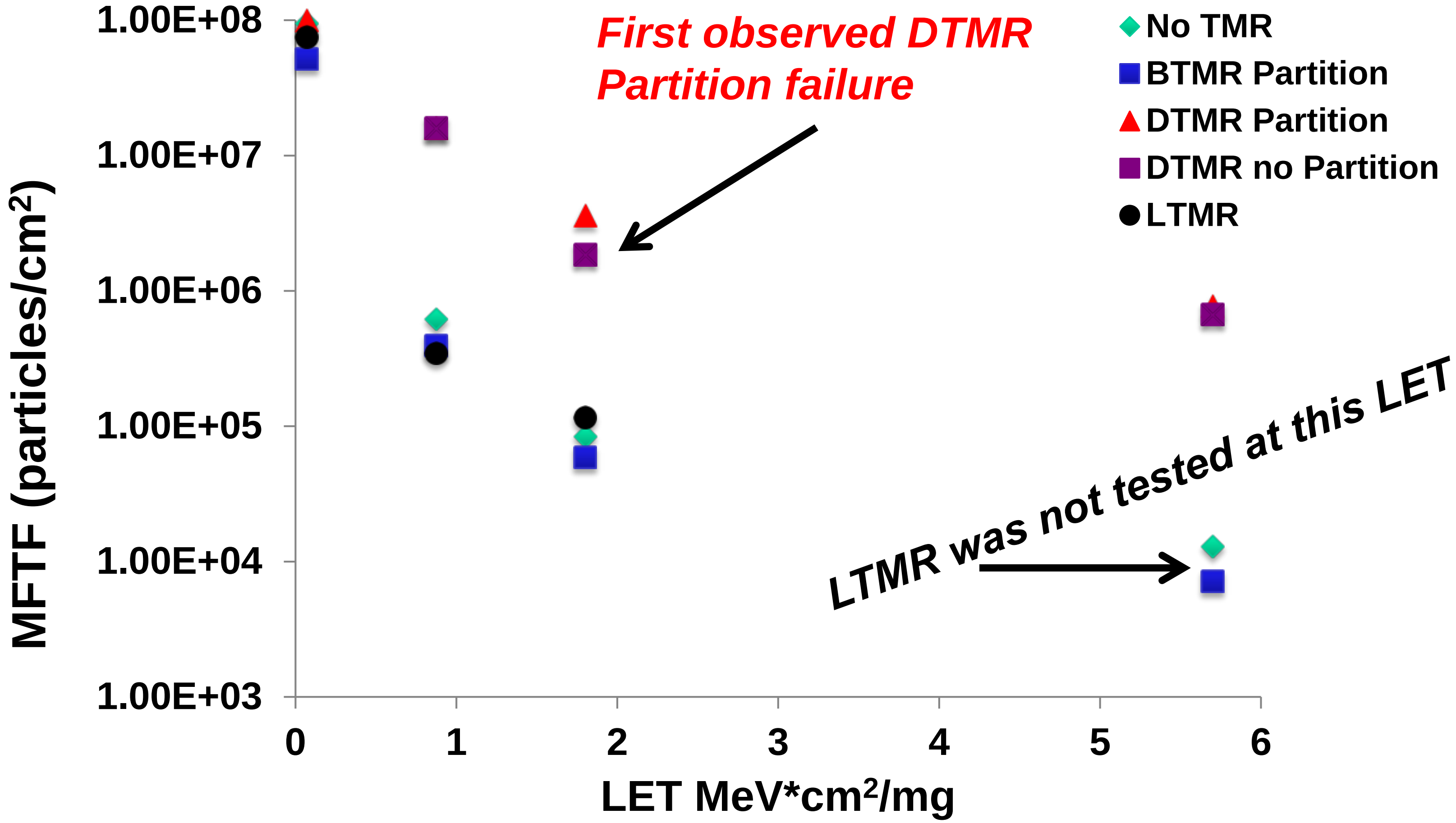
Kintex-UltraScale System Characterization: SEU Cross-Section (σ) and Mean Fluence To Failure (MFTF)

Φ = *particles/cm*^{2}

$$\sigma = \frac{1}{MFTF} = \frac{1}{\Phi}$$

Generally, σ is how SEU data is presented. However, it is becoming more common to use MFTF for system characterization.

Kintex-UltraScale Mitigation Study: Counter Array MFTF versus LET



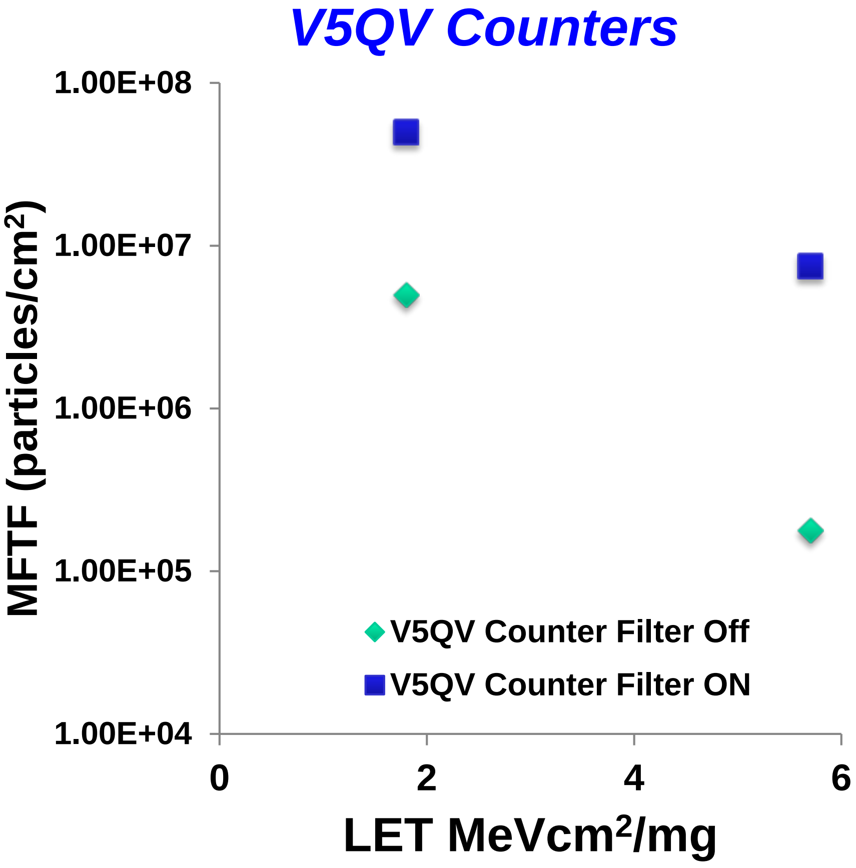
First observed DTMR Partition failure

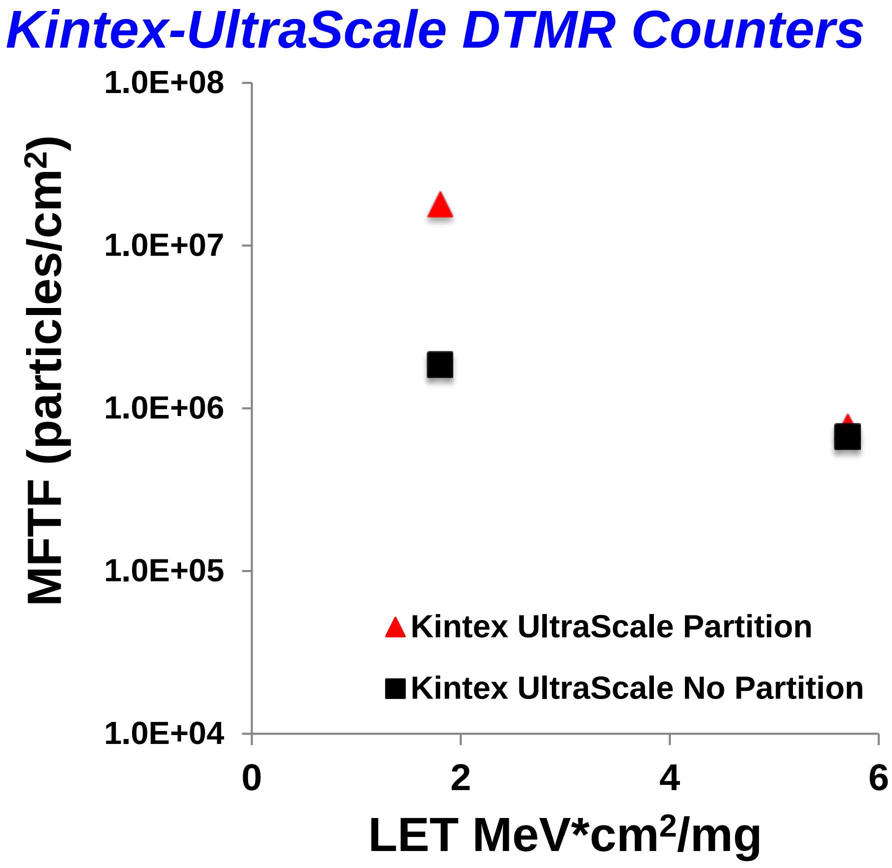
LTMR was not tested at this LET

Kintex-UltraScale Data drops off quicker than radiation hardened Xilinx Virtex (V5QV).

More SEU testing should be performed for more detailed comparisons.

Comparison of Xilinx V5QV and Kintex-UltraScale with Mitigation





Complex Kintex-UltraScale Designs Tested

Test Structure	Frequency Range
Xilinx MicroBlaze No TMR No Cache and with Cache	25MHz
Xilinx MicroBlaze BTMR No Cache and with Cache	25MHz
Xilinx MicroBlaze DTMR No Cache and with Cache	25MHz

- ***All tests that use cache have error correction code (ECC).***
- ***All tests have internal instruction and data BRAM***

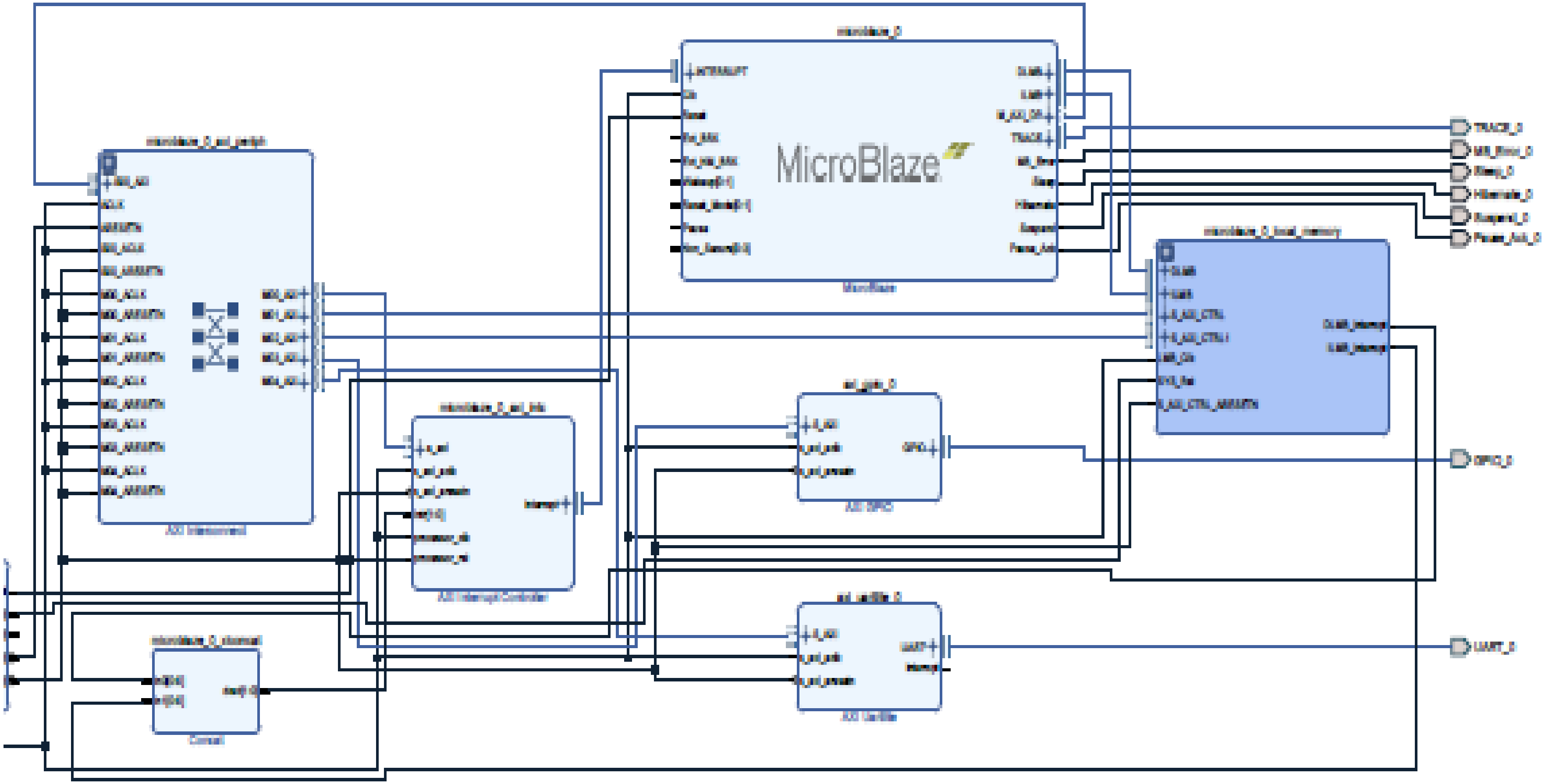
For the current test set, all MicroBlaze mitigation was inserted using Mentor Graphics Precision Hi-Rel

Currently, NEPP has the only heavy-ion data for the Xilinx Kintex-UltraScale embedded MicroBlaze.

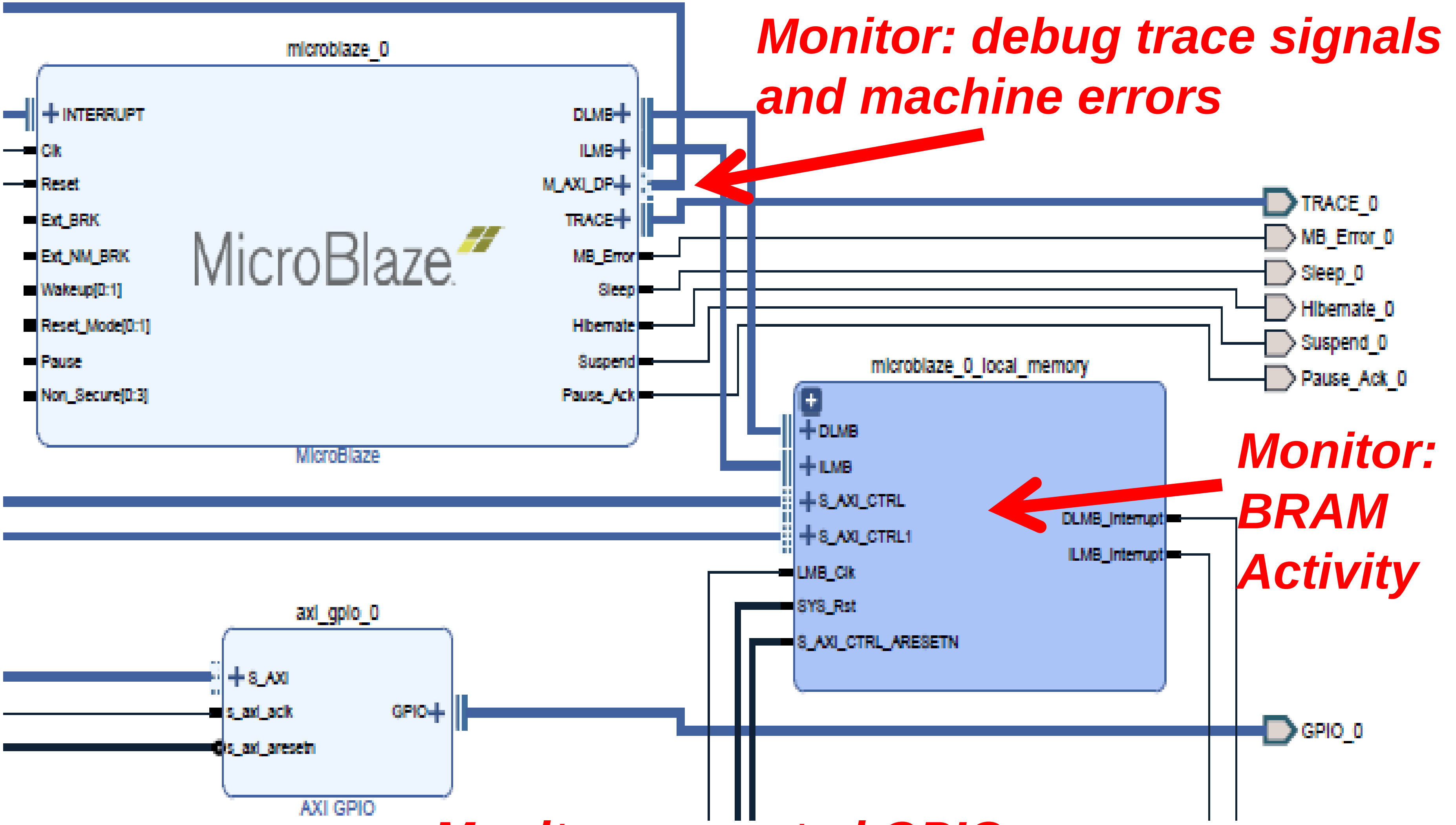
MicroBlaze Block Diagram

DTMR is internal to Blocks.

BTMR triplicates the entire design except for clocks and resets.



The NEPP Difference: MicroBlaze Real-time Traceability and Watchdog Monitoring



Monitor: debug trace signals and machine errors

Monitor: BRAM Activity

Monitor: expected GPIO

BTMR Study: Example When All Malfunction Simultaneously; LET = 0.9MeV·cm^2/mg(1)

TIME: Tester clock cycles

MBnData: Output of MicroBlazen

ClkErrn: Heart beat for MicroBlazen (MBn)

TIME	Status	ClkErr2	MB2Data	ClkErr1	MB1Data	ClkErr0	MB0Data
1004	0	1	0	1	0	1	0
1.37E+09	6	0	9d	0	9d	0	9d
1.42E+09	0	1	5f	0	87	0	7
1.51E+09	0	0	5f	0	20	0	5
1.51E+09	0	0	5f	0	91	0	5
2.58E+09	0	1	0	0	0	0	40
2.59E+09	0	1	0	0	e4	0	40

Tester checks MBnData every clock cycle.

Tester also has watchdogs on all MicroBlaze debug signals (not shown).

Interesting: Most BTMR tests all go out of sync (with and without cache).

BTMR Study: Example When All Malfunction Simultaneously; LET = 0.9MeV·cm^2/mg(2)

🟨 *Beam Turns on*

🟥 *Error occurs*

TIME =tester clock cycles. Tester runs a 50MHz.

At start of beam, all MicroBlaze data are equal.

Start of beam synchronization is unique to NEPP.

TIME	Status	ClkErr2	MB2Data	ClkErr1	MB1Data	ClkErr0	MB0Data
1004	0	1	0	1	0	1	0
1.37E+09	6	0	9d	0	9d	0	9d
1.42E+09	0	1	5f	0	87	0	7
1.51E+09	0	0	5f	0	20	0	5
1.51E+09	0	0	5f	0	91	0	5
2.58E+09	0	1	0	0	0	0	40
2.59E+09	0	1	0	0	e4	0	40

Notice, MB2 indicates a clock error (loss of heartbeat). MB0 has malfunction with active heartbeat… misleading.

BTMR Study: Example When All Malfunction Simultaneously; LET = 0.9MeV·cm^2/mg(3)

🟨 ***Beam Turns on***

🟥 ***Error occurs***

MFTF calculation shows the importance of the NEPP beam synchronizer. Other groups usually handle this manually.

TIME	Status	ClkErr2	MB2Data	ClkErr1	MB1Data	ClkErr0	MB0Data
1004	0	1	0	1	0	1	0
1.37E+09	6	0	9d	0	9d	0	9d
1.42E+09	0	1	5f	0	87	0	7
1.51E+09	0	0	5f	0	20	0	5
1.51E+09	0	0	5f	0	91	0	5
2.58E+09	0	1	0	0	0	0	40
2.59E+09	0	1	0	0	e4	0	40

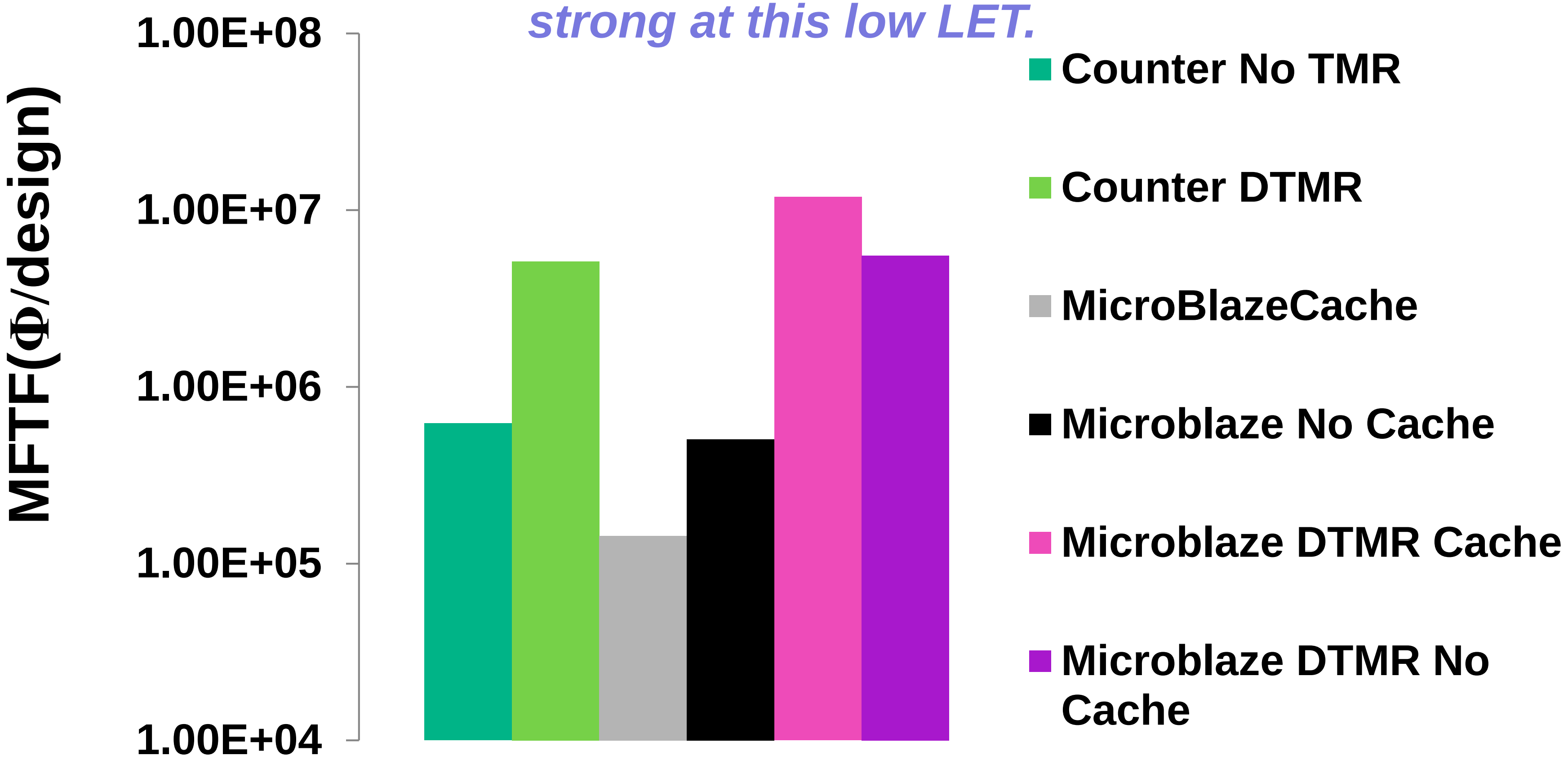
TIME = 1.42E+09cycles − 1.37E+09cycles = 4.98E+07 cycles

$$\Phi = \textit{flux} * s = (3.09\times10^{5}(\Phi/s))*(\textit{TIME(cycles)/50MHz}) = \textit{2.07E+05 particles/cm}^{2}$$

Comparison of Kintex-UltraScale Counters and MicroBlaze MFTF (1)

Data Points were obtained at LET=0.9MeV·cm^2/mg, normal incidence.

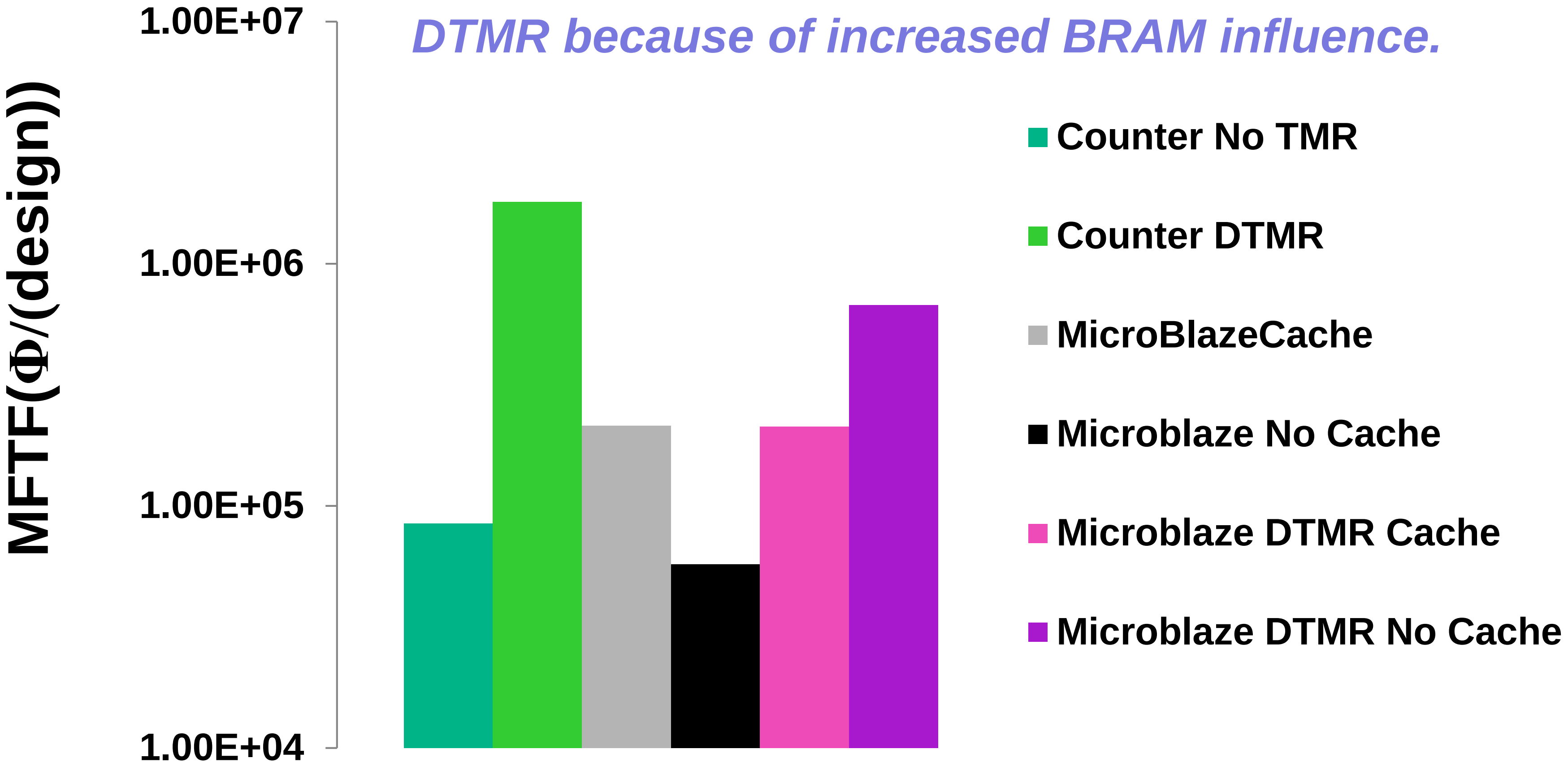
Counter and Microblaze DTMR are relatively strong at this low LET.



Comparison of Kintex-UltraScale Counters and MicroBlaze MFTF (2)

Data Points were obtained at LET=1.8MeV·cm^2/mg, normal incidence.

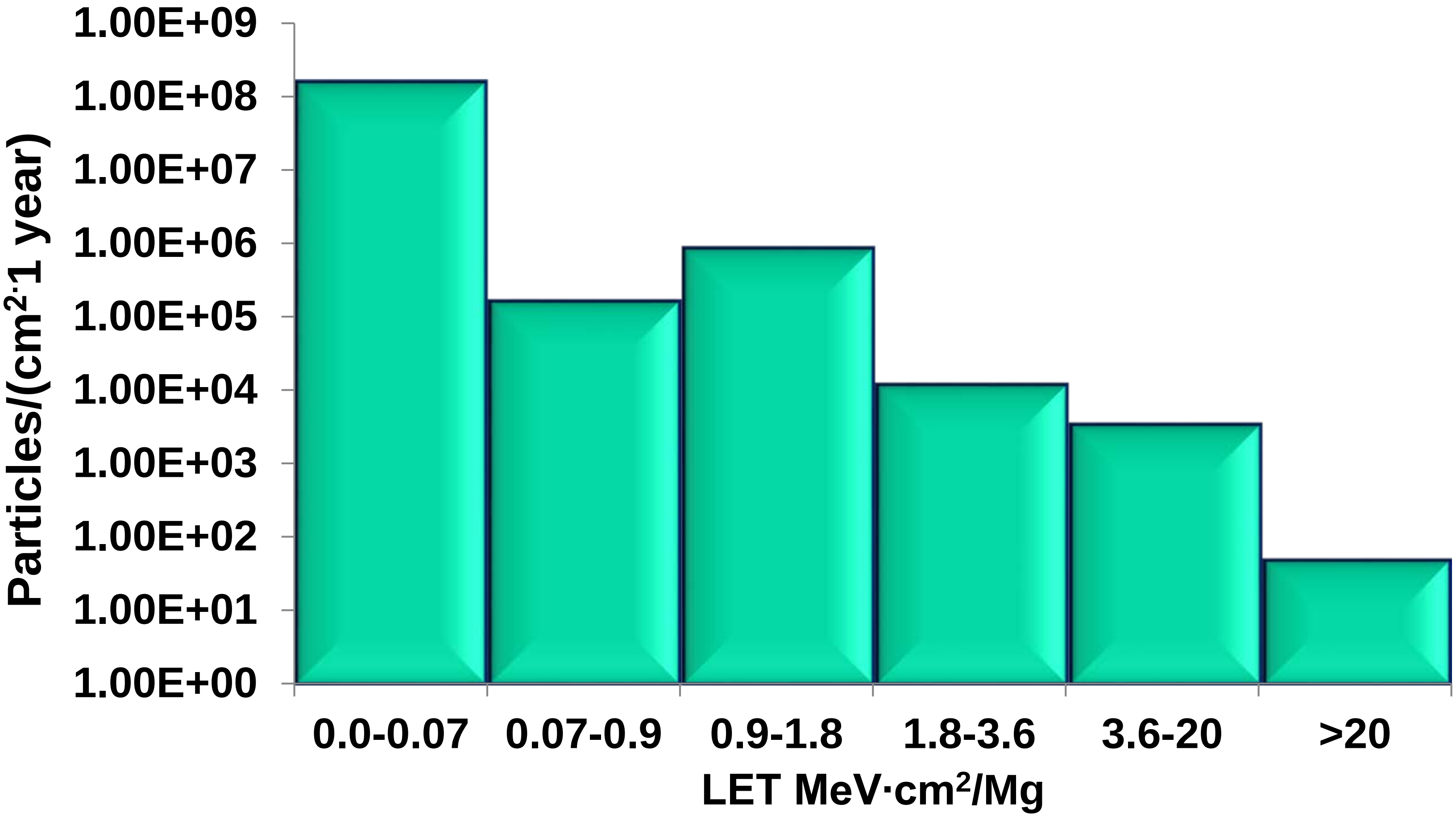
MicroBlaze DTMR is weaker than counter DTMR because of increased BRAM influence.



To be presented by Melanie Berg at the NASA Electronics Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June18–21, 2018

Binned Space-Environment Data: One Year

- Bins do not take into account particle incidence. This is a quick look.
- Taking into account angle has been performed; but is out of scope of this presentation.



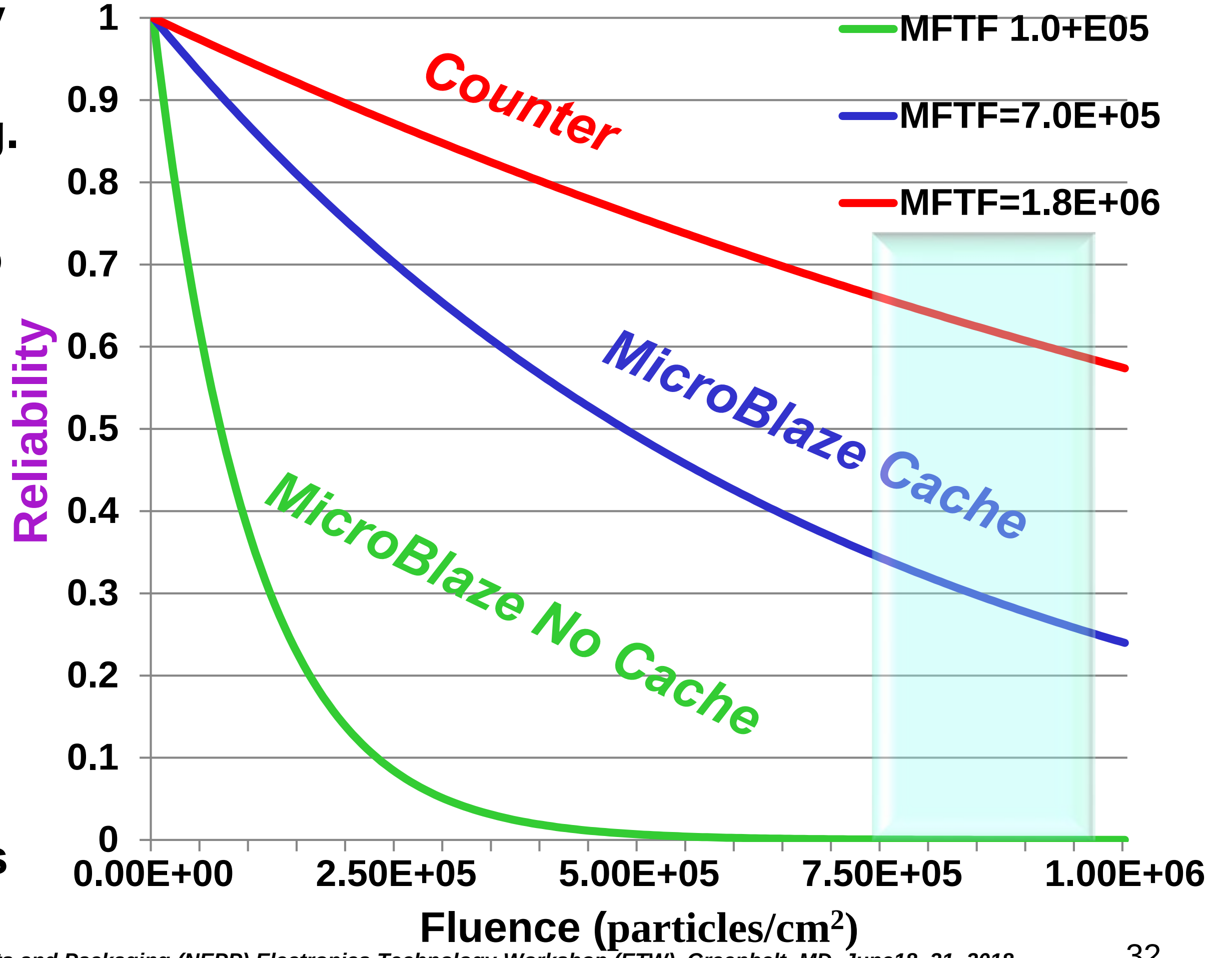
To be presented by Melanie Berg at the NASA Electronics Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June18–21, 2018

System Reliability Pertaining to Space Particles Bin:$0.9MeVcm^2<LET<1.8MeVcm^2$

$$Reliability = e^{\frac{-\Phi}{MFTF}}$$

Quick look for one bin: a system is as strong as its weakest link.

- **Graph illustrates reliability for three different MFTFs with LET = 1.8MeV·cm^2/mg.**
- **In one year, the system is expected to be exposed to approximately 8.0E+05 particles within the specified LET range.**
- **None of the DTMR'd systems are expected to reliably operate without interruption for a full year.**
- **A system flush or reset would need to be anticipated during a year's time.**



To be presented by Melanie Berg at the NASA Electronics Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June18–21, 2018

Summary of Mitigation Application to Kintex-UltraScale during SEU-Heavy-Ion Testing

- **Mitigation study proves DTMR is the strongest mitigation scheme implemented in an SRAM-based FPGA.**
  - **However, for flushable designs BTMR might be acceptable.**
  - **LTMR is not acceptable in SRAM-based FPGAs for any design.**
  - **Partitioning may not be necessary.**
- **During testing, BTMR MicroBlaze has unexpected behavior where all three processors malfunction at the same or similar clock cycle.**
- **Although GTMR has been implemented in V5 families and earlier Xilinx device families, NEPP has suggested to avoid GTMR because clock skew is difficult to control.**
  - **In 2015-2016, via heavy-ion SEU testing, It has been observed in the Xilinx 7-series, that race conditions due to clock skew are unavoidable.**
  - **This is due to the speed of combinatorial logic and route delays in the 7-series versus earlier Xilinx FPGA device families.**
- **Automated mitigation tools have improved for simple designs. They are still working on IP core instantiations and other challenges.**
- **Mitigation and IP cores are still a major concern!!!!!!!!!!!!!!!**

Deliverables: Xilinx Kintex-UltraScale Test Report

- **First Kintex-UltraScale SEE test report was submitted July of 2017.**
- **Second Kintex-UltraScale SEE test report will be submitted July/August 2018. Will include MicroBlaze data.**
- **As a summary:**
  - **NEPP has provided insight into Xilinx potential latchup-like events.**
  - **Through previous heavy-ion studies and design experience, NEPP has provided Synopsys and Mentor graphics information for sufficient mitigation strategies per FPGA type.**
  - **NEPP is providing leading edge SEE data and SEE test guidance for the Kintex UltraScale.**
  - **TBD for NEPP to perform more testing.**

Upcoming Heavy-Ion Tests:

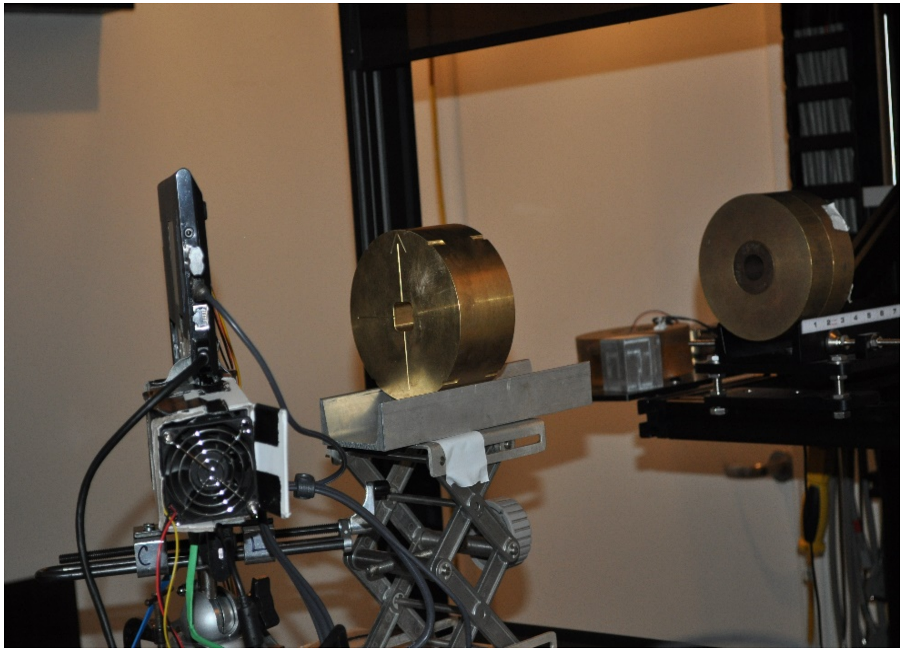
- Xilinx Kintex UltraScale tests:
  - Additional LET test points.
  - MicroBlaze mitigation with external instruction and data memory.
  - Digital signal processor blocks (DSPs).
- Intel Cyclone-10 tests:
  - Shift registers
  - Counters
  - DSP blocks

Test dates TBD

Tests will be conducted at Texas A&M University Cyclotron Single Event Effects Test Facility, 25 MeV/amu tune.

Proton SEE Testing of Kintex-UltraScale

- Tests were performed at Massachusetts General Hospital (MGH) Francis H. Burr Proton Therapy Center.
- 200MeV protons.
- SEU cross-section of configuration: 2.3E-15 (cm^2/bit).
- Cheers to Ethan!



Challenges: Xilinx Kintex-UltraScale SEE Testing (1)

- **Each test takes too long:**
  - **Set up of parameters is easy. We have been doing this for about 13 years.**
  - **Configuration takes minutes. Read-back of configuration takes at least 5 minutes.**
- **New LCDT or evaluation board:**
  - **The current LCDT is over 10 years old and is based around a Xilinx Spartan 6.**
  - **Evaluation boards are promising because they have many more I/O than they used to (necessary for visibility during testing).**
  - **However, we are not sure how well the evaluation boards will hold up during proton testing.**

To be presented by Melanie Berg at the NASA Electronics Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June18–21, 2018

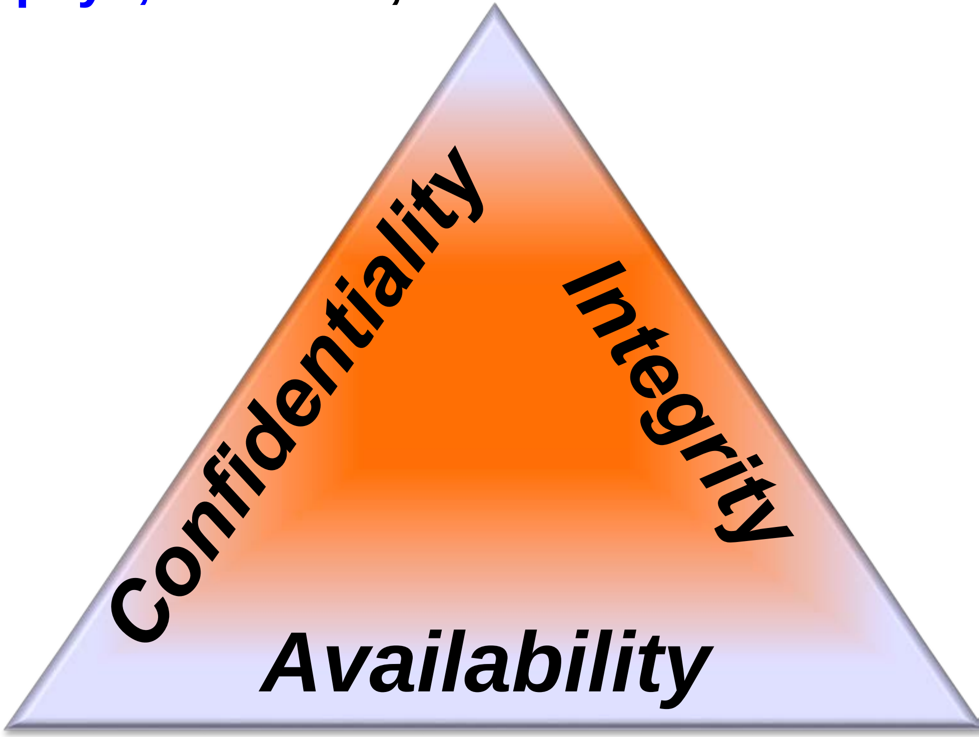
Challenges: Xilinx Kintex-UltraScale SEE Testing(2)

- Scrubbing during proton SEE testing:
  - Tester holds the entire configuration in onboard SRAM.
  - Configuration is near 1Gb and gets corrupted while being held by tester.
  - Currently LCDT cannot accommodate redundancy in SRAM.
  - Will need a new tester with larger onboard memory for scrubber configuration storage.
  - Will also look into better shielding techniques.
- Penetration problem… is it an orientation issue? A setup issue?

To be presented by Melanie Berg at the NASA Electronics Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June18–21, 2018

FPGA Security and Trust

- Goal: Support the United States government regarding FPGA security and trust. Enhancement to conventional assurance procedures.
- Collaboration with: Aerospace Corporation, Ball Aerospace, SEAKR, Sandia National Laboratories, Air Force Research Laboratory, Naval Surface Warfare Center – Crane, JFAC, OneSpin, Mentor Graphics, Synopsys, Cadence, and other agencies.
  - Meetings,
  - consultations,
  - brain storming,
  - reviews,
  - and presentations.

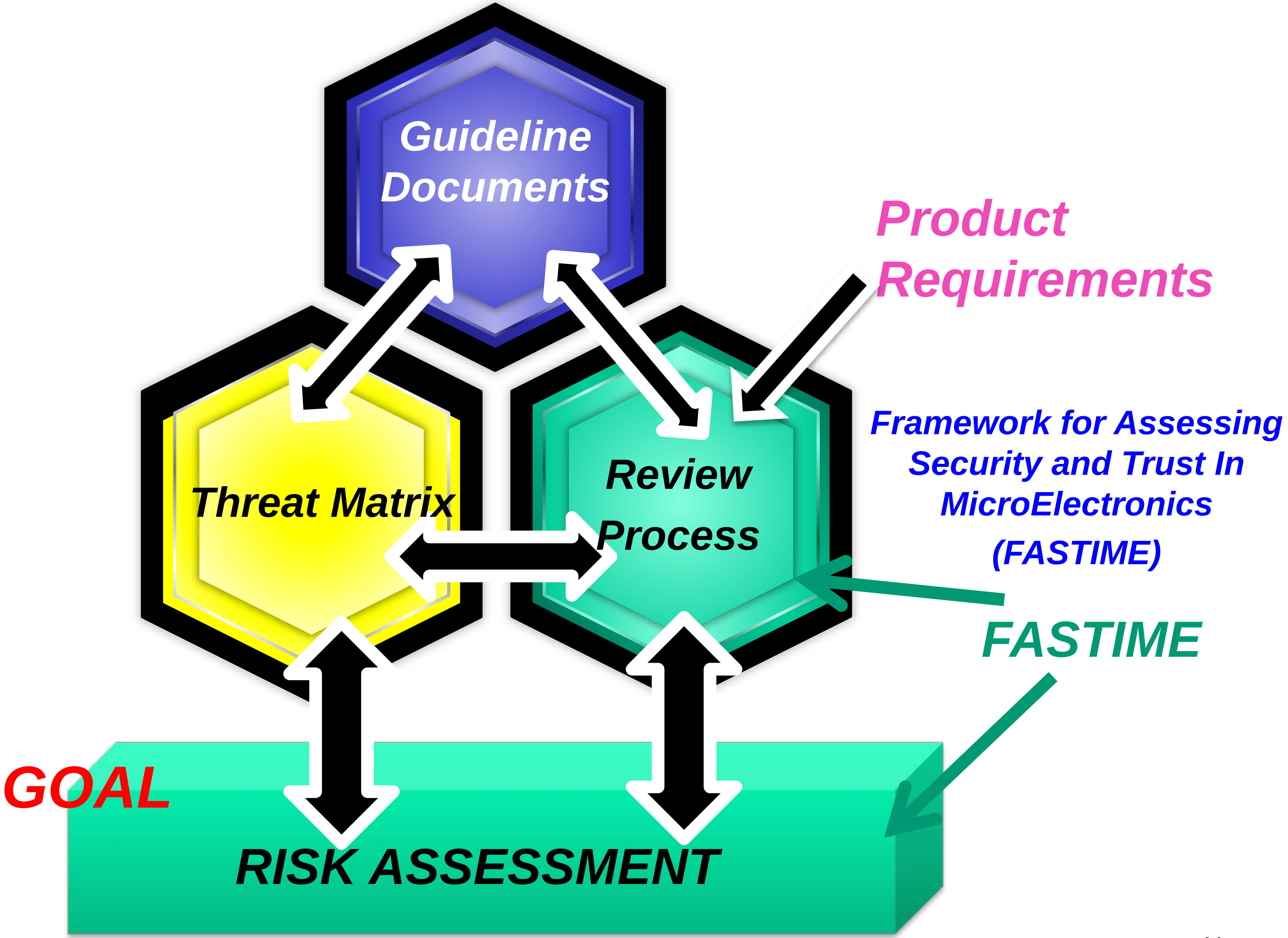


To be presented by Melanie Berg at the NASA Electronics Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June18–21, 2018

Synopsis of Assurance Plan

- The government is developing a systematic framework for practicing security and trust in ASIC and FPGA applications.
- User is provided guidance in mitigation best practices; correspondingly, missions are expected to follow guidelines to the best of their abilities; and risk assessments are performed on implementation.
- There are three flows:
  - (1) FPGA designer flow; (2) ASIC designer flow; and (3) FPGA supplier flow.
  - Separate with unique assurance approaches yet many similarities.
- Activity and Support:
  - Government process established under Defense Production Act Title III
  - Process is currently being beta-tested by targeting two critical missions' FPGA designer flows.

Government Microelectronics Assessment for Trust: GOMAT



To be presented by Melanie Berg at the NASA Electronics Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June18–21, 2018

FASTIME Strengths (1)

V&V: Verification and Validation

IT: Information Technology

- Differentiation between user flow and assessor flow:
  - Guidelines and requirements are provided to the target team and are used as references for the review process (what should be done).
  - Actual implementation is reviewed.
- Framework takes into account:
  - Observed gaps.
  - Potential gaps (unobtainable information, lack in V&V coverage, not vetted personnel).
  - Multiple layers of mitigation (co-dependencies).
  - Potential for adversary's learning process as it pertains to the actual implementation of mitigation.
  - Full ecosystem (personnel, IT, tools, design process, data handling, etc.)

FASTIME Strengths (2)

V&V: Verification and Validation

- Risk analysis is robust:
  - Includes V&V coverage… coverage is not the only element that defines risk.
  - Risk metrics are more than colors or simple strength descriptions.
  - Risk metrics are based on time-to-infiltration and weighted outcome.
  - Risk items can be red-lined for immediate attention.
- Eventual integration with model based system engineering tools.

Vulnerabilities are determined by coverage of guidance, requirements, and implementation discrepancies.

Questions?