UNIVERSITY OF
ARKANSAS

Accelerating DICe on FPGA

Status Update on Honeywell Research

Keaten Stokke & Atiyeh Panahi

Advisor: Dr. David Andrews

May 29th, 2019

Recent Accomplishments

- Migrated to the ZCU104
  - Successfully ported over our design
    - 64x48 image correlation
    - Successfully scaled up to 232x448 (¼ full frame)
  - Upgraded to Vivado 2018.3.1
    - IP upgrades
  - Experience working with Zynq
- Arithmetic Functions
  - Compared with the built in Vivado FP IPs
    - Our FP IPs are still the best option
      - Optimized for 150 MHz
      - Localized within each IP
- FPGA Security
  - A thorough report is being developed
    - Over 30 papers on FPGA security have been used
  - Best practices
    - How the development cycle impacts FPGA security
  - Specific boards
    - Revolving around Zynq security
    - Older Virtex boards have been used to demonstrate attacks
    - Separate presentation if currently interested in the status of this research

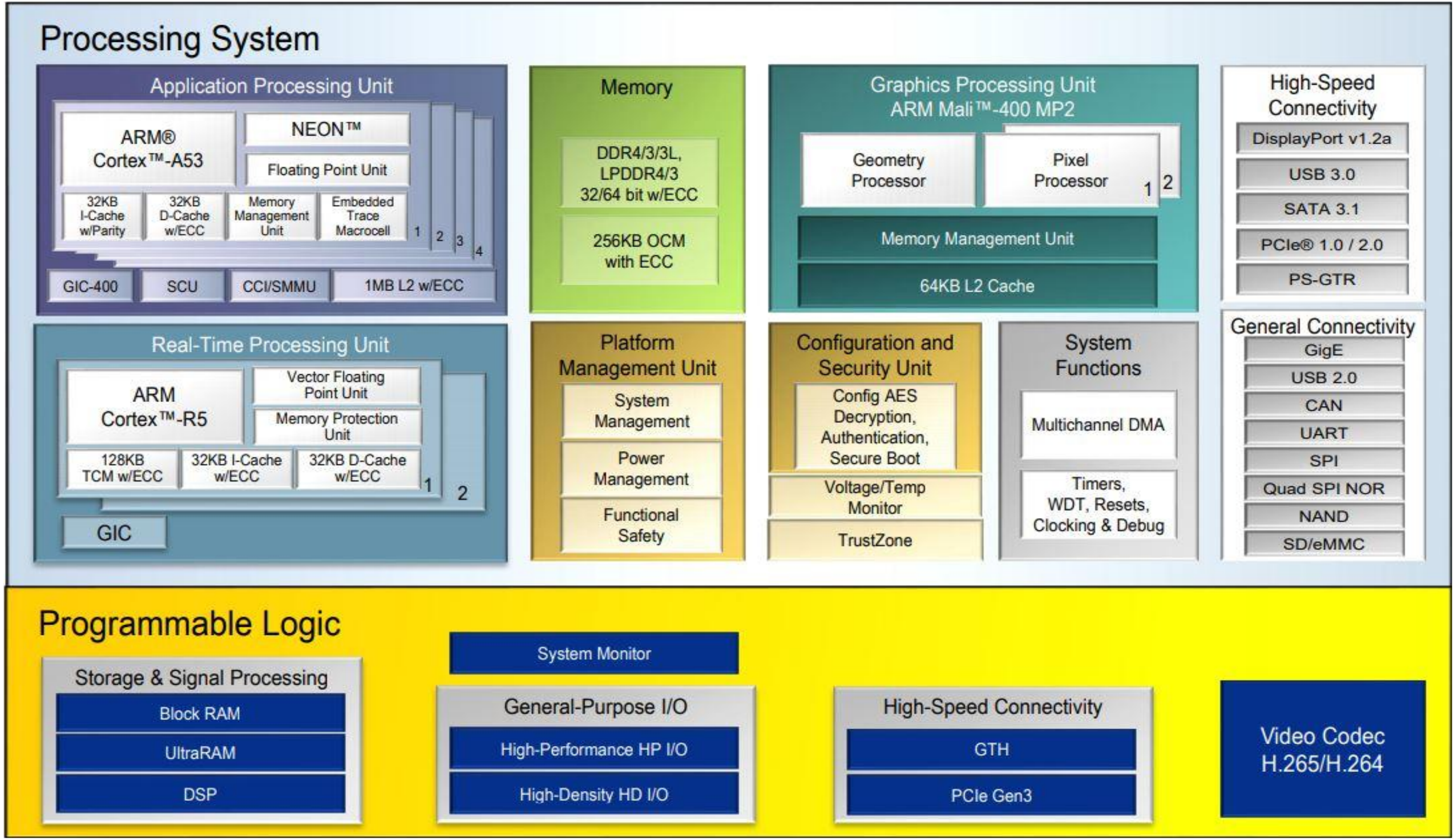
Recent Accomplishments

KC705 vs. ZCU104 Execution Times

Test Case: 64x48 Design	Total Preprocessing Execution Time	Total Transfer Time	Total FPGA Correlation Time	Total GUI Correlation Time	Total FPGA Execution Time	Total GUI Execution Time
KC705	0.21 s	1.25 s	0.0025 s	0.016 s	1.48 s	0.058 s
ZCU104	0.21 s	0.104 s	0.0025 s	0.016 s	0.33 s	0.058 s
Results	No Change	12x faster	No Change	No Change	4.5x faster	No Change

- Total Execution Time (compared to the GUI)
  - KC705: 25x slower
  - ZCU104: 5.6x slower
  - ZCU104 without Python preprocessing: 1.8x slower [Multithreading!!!]
    - Ethernet transfer rate can theoretically be x10 faster [80Mbps → 800Mbps]
    - After design optimizations & parallelizations total FPGA correlation time can be reduced

MPSoC ZCU104 Features



Processing System

Application Processing Unit

ARM® Cortex™-A53

NEON™

Floating Point Unit

32KB I-Cache w/Parity

32KB D-Cache w/ECC

Memory Management Unit

Embedded Trace Macrocell

1 2 3 4

GIC-400

SCU

CCI/SMMU

1MB L2 w/ECC

Memory

DDR4/3/3L, LPDDR4/3 32/64 bit w/ECC

256KB OCM with ECC

Graphics Processing Unit ARM Mali™-400 MP2

Geometry Processor

Pixel Processor

1 2

Memory Management Unit

64KB L2 Cache

High-Speed Connectivity

DisplayPort v1.2a

USB 3.0

SATA 3.1

PCIe® 1.0 / 2.0

PS-GTR

Real-Time Processing Unit

ARM Cortex™-R5

Vector Floating Point Unit

Memory Protection Unit

128KB TCM w/ECC

32KB I-Cache w/ECC

32KB D-Cache w/ECC

1 2

GIC

Platform Management Unit

System Management

Power Management

Functional Safety

Configuration and Security Unit

Config AES Decryption, Authentication, Secure Boot

Voltage/Temp Monitor

TrustZone

System Functions

Multichannel DMA

Timers, WDT, Resets, Clocking & Debug

General Connectivity

GigE

USB 2.0

CAN

UART

SPI

Quad SPI NOR

NAND

SD/eMMC

Programmable Logic

System Monitor

Storage & Signal Processing

Block RAM

UltraRAM

DSP

General-Purpose I/O

High-Performance HP I/O

High-Density HD I/O

High-Speed Connectivity

GTH

PCIe Gen3

Video Codec H.265/H.264

MPSoC ZCU104 Features

- **SoC - Targeting the new chips for speedup**
  - Application Processing Unit (APU)
    - ARM Cortex-A53 (Quad-core)
    - Floating Point Unit
  - Real-Time Processing Unit (RTPU)
    - ARM Cortex-R5 (Dual-core)
    - Vector Floating Point Unit
  - Graphics Processing Unit (GPU)
    - Pixel Processor (x2)
    - Geometry Processor
- Our current design is almost entirely programmable logic (PL); we need to learn how to target these processing cores for a speed up now that we have them

MPSoC ZCU104 Features

- **Configuration Security Unit [CSU]**
  - Secure Boot - Two methods
    1. **Hardware Root of Trust**: Asymmetric authentication and encryption to provide CIA of the boot and configuration files
    2. **Encryption Only**: No asymmetric authentication, but requires all configuration files loaded must be encrypted and authenticated with AES
  - Secure key storage and management
    - **Volatile keys**: operation key, key update register key (KUP)
    - **Non-volatile keys**: eFUSE, BBRAM, family key, PUF key encryption key (KEK)
    - **Encryption key backup**: BBRAM stores AES key even with power loss
  - Ring Oscillator Physically Unclonable Function [RO PUF]
    - Generates a device-unique key for authentication and identification
    - Process variations in manufacturing ensure uniqueness between two identical circuits

MPSoC ZCU104 Features

- **Configuration Security Unit [CSU] (continued)**
  - Encryption & Authentication
    - Configuration files & bitstreams
  - Triple redundant MicroBlaze processor
    - Controls boot operations
  - ARM TrustZone
    - Hardware isolation for trusted software
  - Cryptographic hardware acceleration
    - Crypto-Interface Block (CIB) for AES block ciphers that were adopted for efficiency and performance that provide integrity and confidentiality
    - AES-GCM, DMA, SHA-3, RSA, PCAP
  - Tamper Monitoring & Response
    - Temperature & Voltage alarms
    - I/O Port Monitoring
    - Zeroization of keys and bitstream

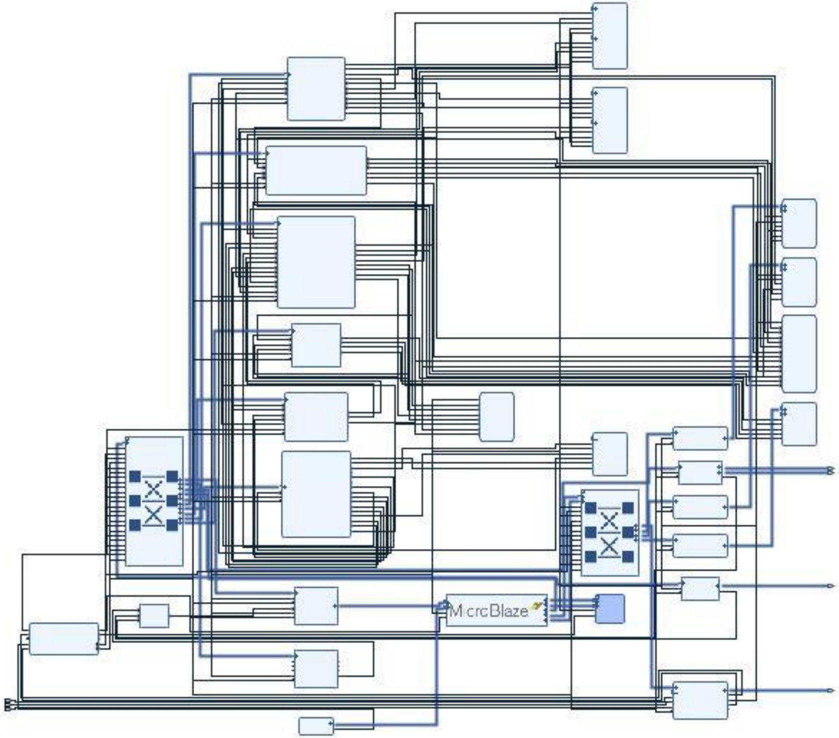
MPSoC ZCU104 Features

- **URAM**
  - 71% of SRAM memory
  - Read is 1 clock cycle (2x faster)
  - Synchronous ports and clock
  - Less power consumption (sleep mode/disable unused cells)
  - Fixed port width (72 bits) (4 x 72 = 288 Kb per cell)
- **BRAM**
  - 29% of SRAM memory
  - Read is 2 clock cycles
  - True dual porting (asynchronous clocks)
  - Ability to initialize with .COE file
  - Configurable port width

FPGA Comparisons

Block Design

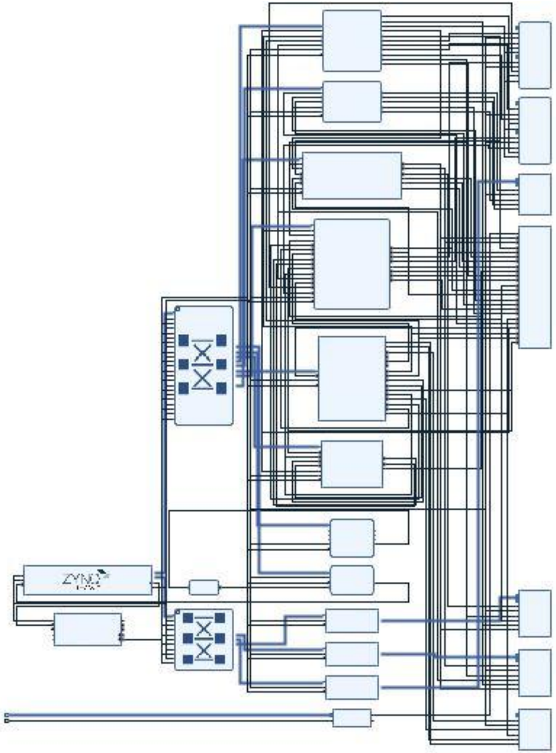
KC705 (MicroBlaze) [29 blocks]



FPGA Comparisons

Block Design

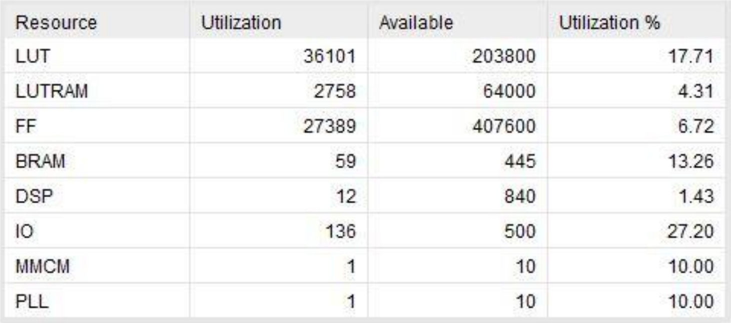
ZCU104 (Zynq) [24 blocks, only 20 required]



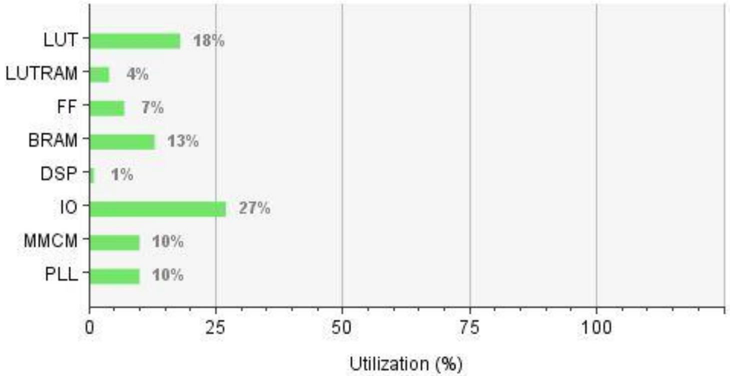
FPGA Comparisons

Resource Utilization

KC705 (MicroBlaze)



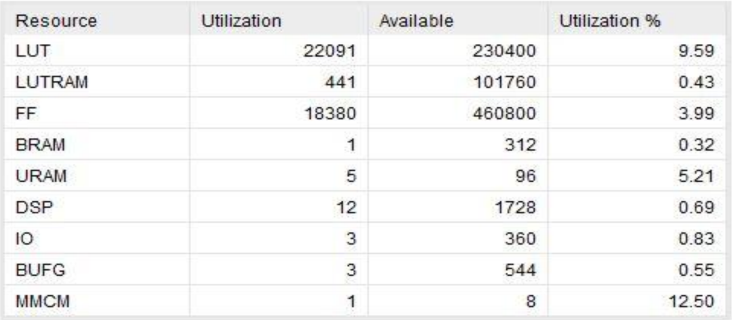
Resource	Utilization	Available	Utilization %
LUT	36101	203800	17.71
LUTRAM	2758	64000	4.31
FF	27389	407600	6.72
BRAM	59	445	13.26
DSP	12	840	1.43
IO	136	500	27.20
MMCM	1	10	10.00
PLL	1	10	10.00



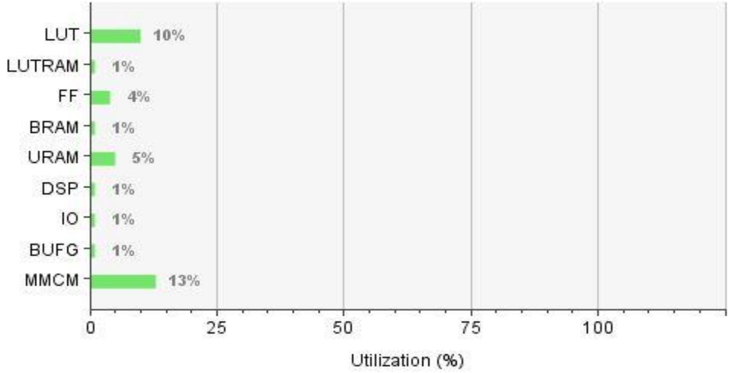
FPGA Comparisons

Resource Utilization

ZCU104 (Zynq)



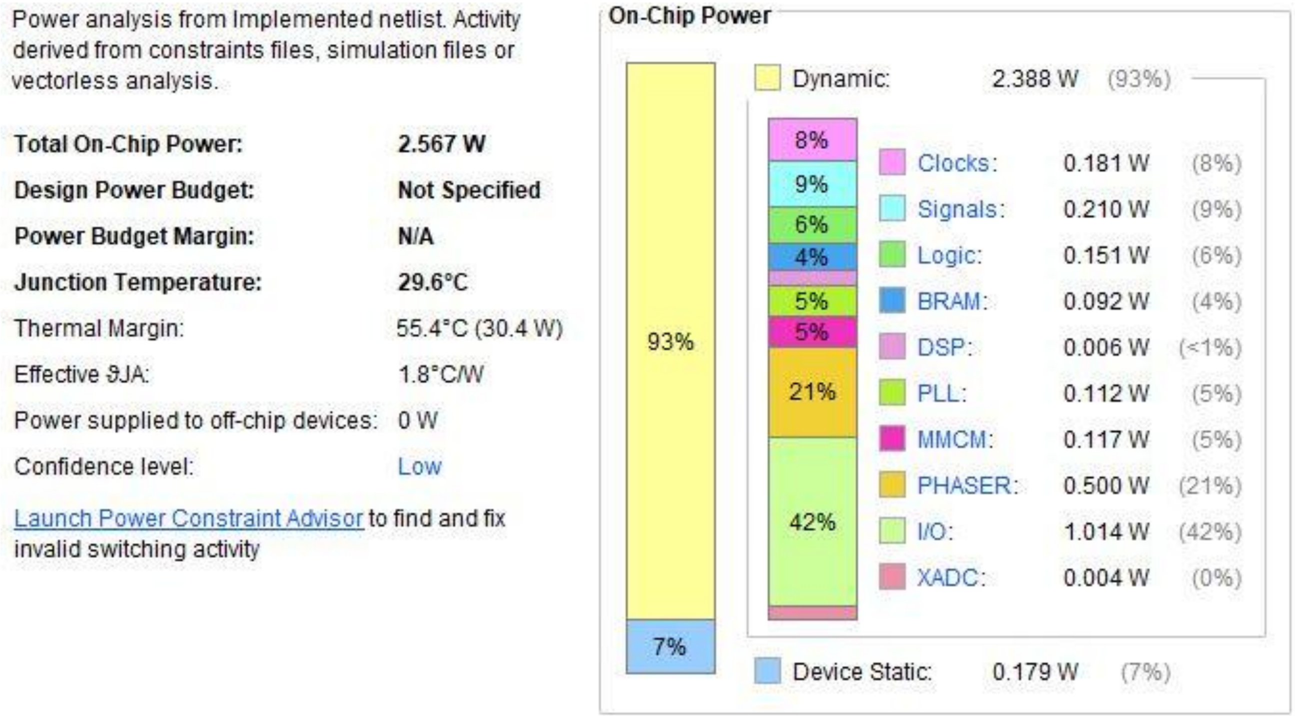
Resource	Utilization	Available	Utilization %
LUT	22091	230400	9.59
LUTRAM	441	101760	0.43
FF	18380	460800	3.99
BRAM	1	312	0.32
URAM	5	96	5.21
DSP	12	1728	0.69
IO	3	360	0.83
BUFG	3	544	0.55
MMCM	1	8	12.50



FPGA Comparisons

Power

KC705 (MicroBlaze)



Power analysis from Implemented netlist. Activity derived from constraints files, simulation files or vectorless analysis.

Total On-Chip Power:	**2.567 W**
Design Power Budget:	**Not Specified**
Power Budget Margin:	**N/A**
Junction Temperature:	**29.6°C**
Thermal Margin:	55.4°C (30.4 W)
Effective ϑJA:	1.8°C/W
Power supplied to off-chip devices:	0 W
Confidence level:	Low

Launch Power Constraint Advisor to find and fix invalid switching activity

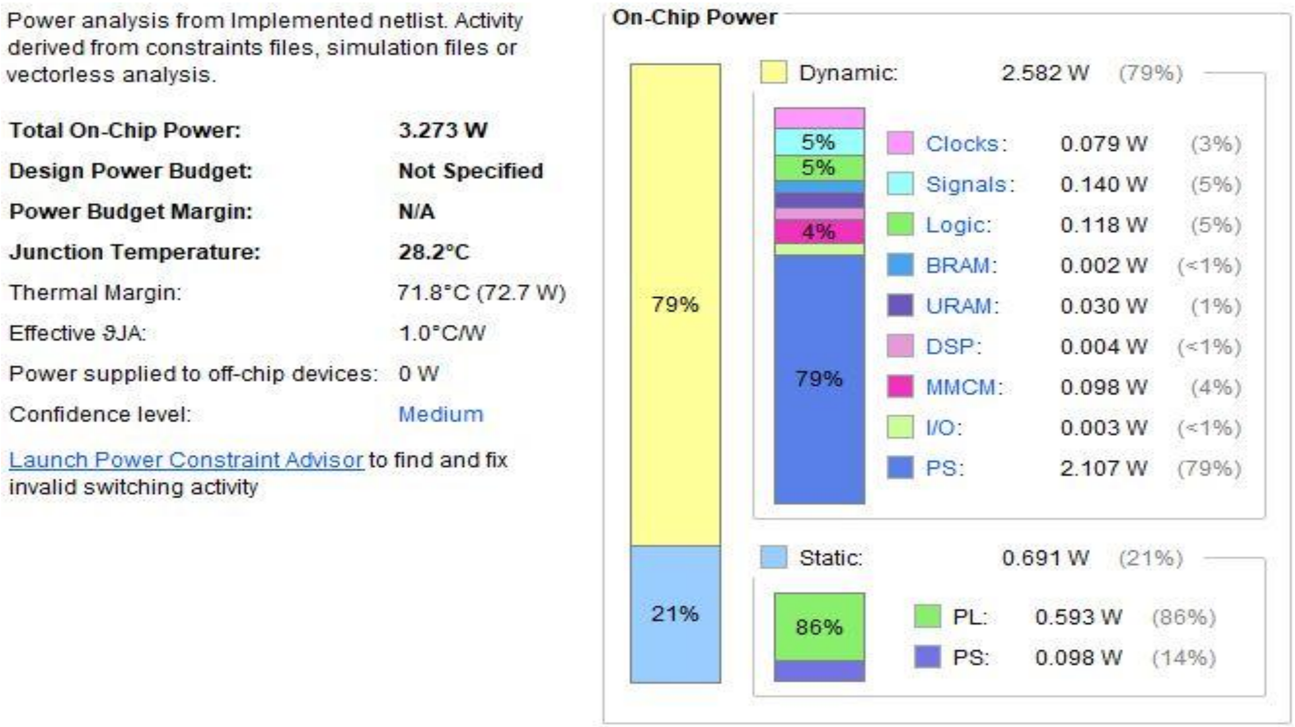
On-Chip Power

Dynamic:	2.388 W	(93%)
Clocks:	0.181 W	(8%)
Signals:	0.210 W	(9%)
Logic:	0.151 W	(6%)
BRAM:	0.092 W	(4%)
DSP:	0.006 W	(<1%)
PLL:	0.112 W	(5%)
MMCM:	0.117 W	(5%)
PHASER:	0.500 W	(21%)
I/O:	1.014 W	(42%)
XADC:	0.004 W	(0%)
Device Static:	0.179 W	(7%)

FPGA Comparisons

Power

ZCU104 (Zynq)



Power analysis from Implemented netlist. Activity derived from constraints files, simulation files or vectorless analysis.

Total On-Chip Power:	**3.273 W**
Design Power Budget:	**Not Specified**
Power Budget Margin:	**N/A**
Junction Temperature:	**28.2°C**
Thermal Margin:	71.8°C (72.7 W)
Effective ϑJA:	1.0°C/W
Power supplied to off-chip devices:	0 W
Confidence level:	Medium

Launch Power Constraint Advisor to find and fix invalid switching activity

On-Chip Power

🟨 Dynamic:	2.582 W	(79%)
🟪 Clocks:	0.079 W	(3%)
🟦 Signals:	0.140 W	(5%)
🟩 Logic:	0.118 W	(5%)
🟦 BRAM:	0.002 W	(<1%)
🟪 URAM:	0.030 W	(1%)
🟪 DSP:	0.004 W	(<1%)
🟥 MMCM:	0.098 W	(4%)
🟩 I/O:	0.003 W	(<1%)
🟦 PS:	2.107 W	(79%)
🟦 Static:	0.691 W	(21%)
🟩 PL:	0.593 W	(86%)
🟦 PS:	0.098 W	(14%)

Next Steps

- Going back to the DICe Correlation IPs
  - Validating the results
    - Verify that each IP operates correctly
    - Compare image correlation between DICe GUI and FPGA
  - Scale up
    - Support for more than two frames
    - Larger image sizes (< 896x464)
      - We now have the URAM/BRAM resources to scale up
      - Currently scaling up to 464x448 (½ full frame)
  - Adding more DICe features
    - Unique subset shapes
      - Currently working on circle subsets
    - Dynamic subsets
      - Exclusions inside the area of interest (AOI)
      - Multiple subsets (< 14)
    - Image obstructions
    - Simplex & robust correlation
  - Optimize and parallelize
    - Target all of the processors cores
    - With URAM we can cut clock cycles in half for reads
    - We've identified sections of code that can be parallelized

Conclusion

Questions?