System Board 6156

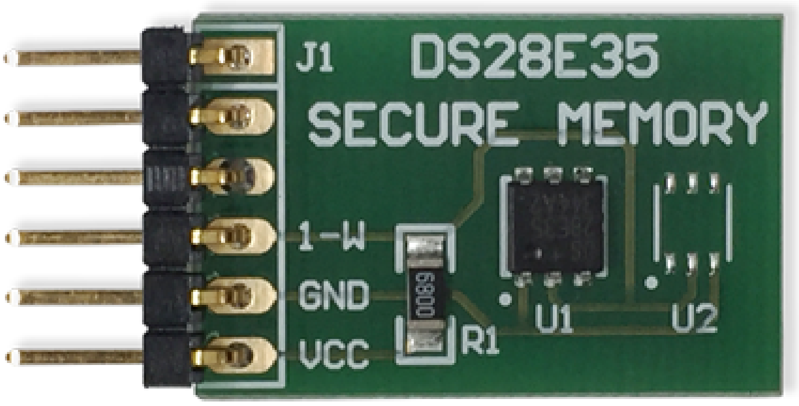
MAXREFDES44#: SECURE AUTHENTICATION DESIGN WITH 1-WIRE ECDSA AND XILINX ZYNQ SOC

Details

Introduction

Smart factories and applications for industrial and medical employ the flexibility and high performance of modern SoCs. As these systems become increasingly connected, security emerges as a paramount feature to protect IP, track product lifetime, and prevent counterfeiting. The MAXREFDES44# is a 1-Wire based asymmetric authentication reference design, built to authenticate peripherals to Xilinx SoCs. The public keys are stored on the Xilinx SoC, relieving the need for a secure secret memory location, while the private key is stored on the DS28E35 using DeepCover® technology. Using the provided example code, the SoC executes a challenge response sequence with the DS28E35 to ensure the authenticity of a module, peripheral, or subsystem. The DS28E35 communicates on a 1-Wire bus, providing a standard communication interface. The MAXREFDES44# hardware, shown in **Figure 1**, is equipped with a Pmod-compatible connector for immediate testing using an Avnet MicroZed evaluation kit. The simplicity of this design enables rapid adoption into any peripheral requiring the heightened security provided by the asymmetric ECDSA algorithm.

MAXREFDES44# System Board



Enlarge+

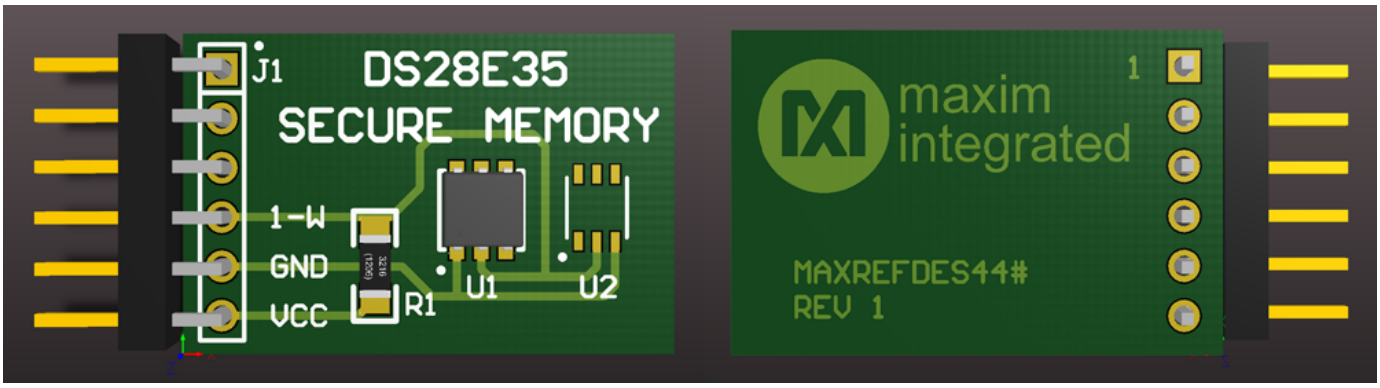


Figure 1. MAXREFDES44 DS28E35 peripheral module (top and bottom).

Detailed Description of Hardware

The system shown in **Figure 2** shows the high-level implementation of the design. The system requires:

- Cheyenne ‘C’ code running on the ARM® Cortex® A9 processor in the Processing System (PS)
- Cryptographically Secure Pseudo Random Number Generator (CSPRNG) running in the Programmable Logic (PL)
- PC connected to a RS-232 port (USB UART)
- MAXREFDES44# with the DS28E35 and a 680Ω pullup resistor

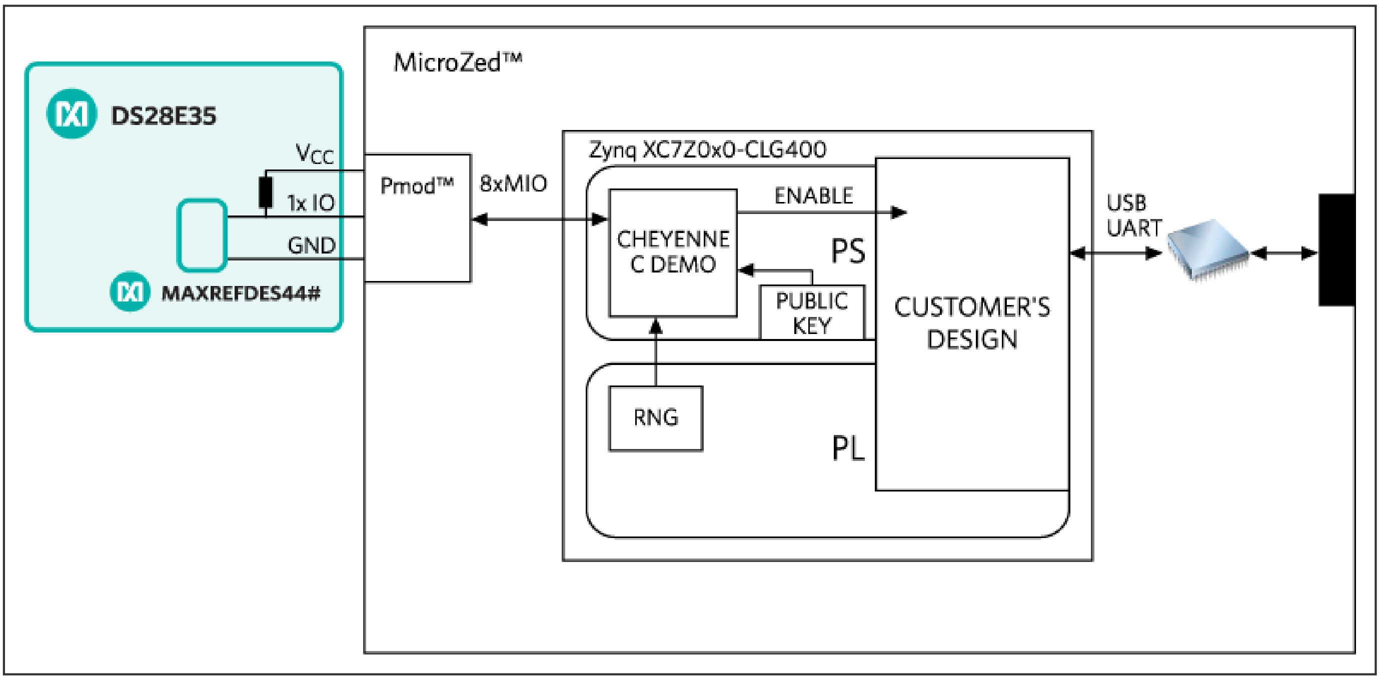


Figure 2. System design block diagram.

Hardware

The hardware setup for this reference design is:

- PC with 1GB RAM
  - www.xilinx.com/design-tools/vivado/memory.htm
- Avnet MicroZed (available by Avnet for purchase separately)
  - http://microzed.org/
- Maxim DS28E35 peripheral module (MAXREFDES44# available for purchase)
  - Available for immediate download on the Design Resources tab is the schematic, BOM, and PCB Gerber
- USB-A to USB-micro B cable
- Xilinx platform cable USB
- DS28E35EVKIT# (2nd generation with DS2475 available for purchase separately) used for programming only

Software

The software requirements for this reference design are:

- Windows 7 OS or newer
- A terminal program such as Tera Term or HyperTerminal®
- Vivado® Design Tools (Vivado 2014.2)
  - www.xilinx.com/support/download/index.htm
- Embedded Design Tools (Xilinx SDK 2014.2)
  - www.xilinx.com/support/download/index.htm
- Firmware Files
  - Available by request on the MAXREFDES44# webpage landing under

Design Resources tab with a nondisclosure agreement (NDA):

- MAXREFDES44_NDA_FW.zip

Detailed Description of Firmware

The archived Vivado project, “MAXREFDES44.xpr.zip”, contains all the details of the PS and PL. The archive has a basic Zynq configuration that contains Avnet’s MicroZed Board Definition for 2014.2 and additional modifications to add a CSPRNG needed for security. Avnet’s MicroZed Board Definition for 2014.2 can be found on their MicroZed website under documentation. **Figure 3** shows the block diagram for the design found under the “\MAXREFDES44.xpr\MZ_Zynq_HW” path and called “MZ_Zynq_HW.xpr”.

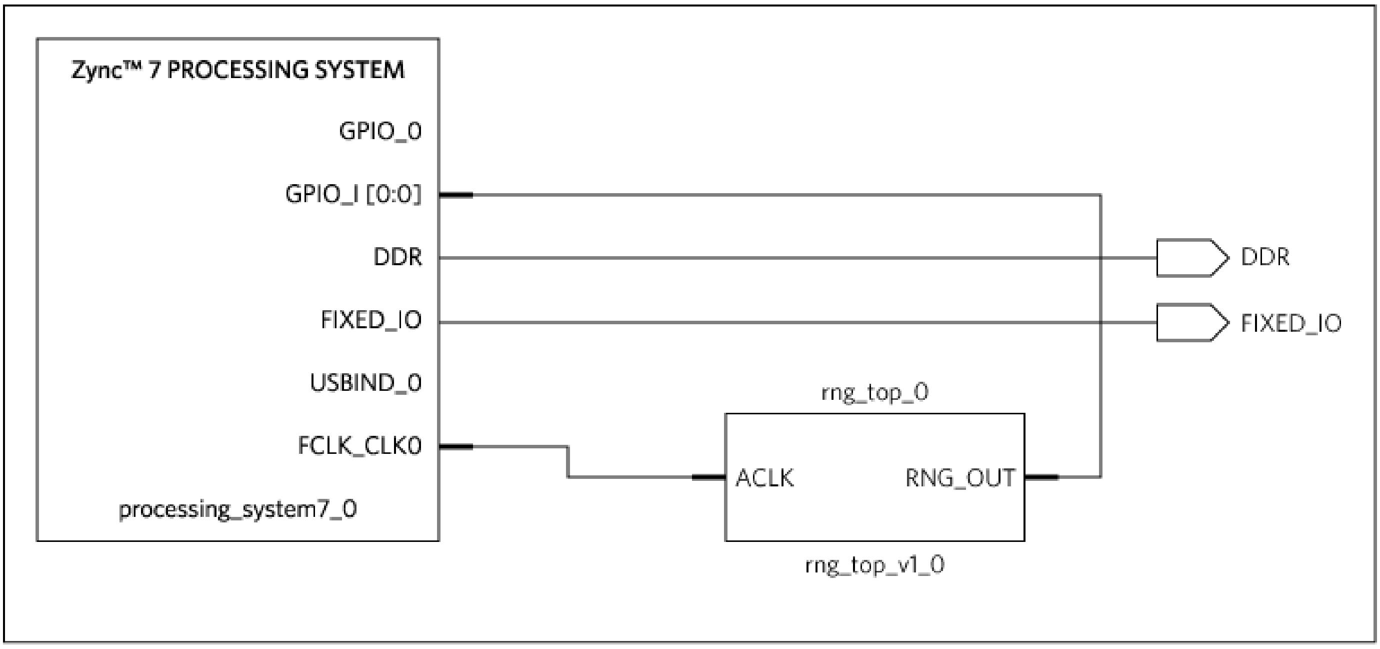


Figure 3. Block diagram of Zynq.

The PS and PL configuration block diagram is shown in **Figure 4**.

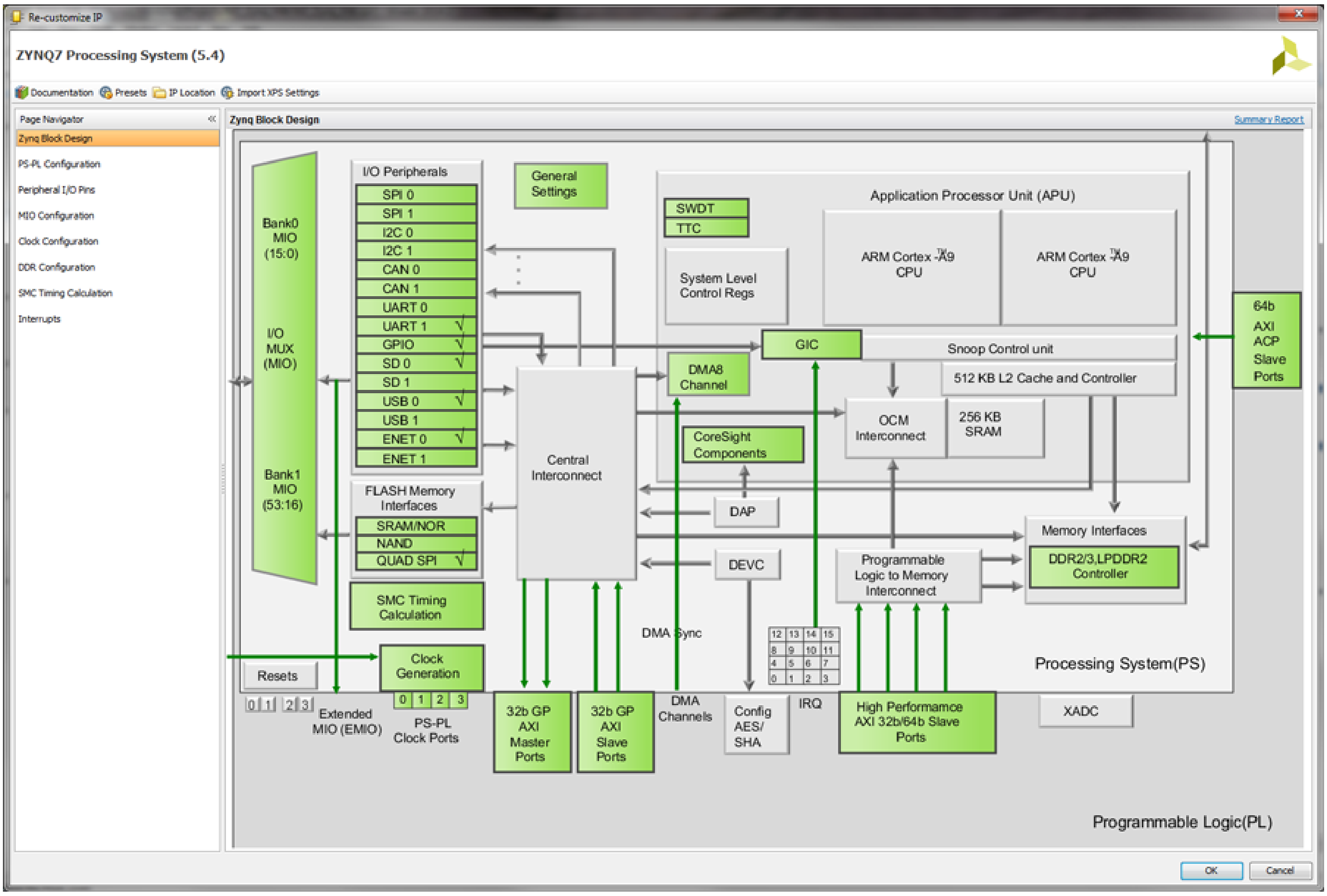
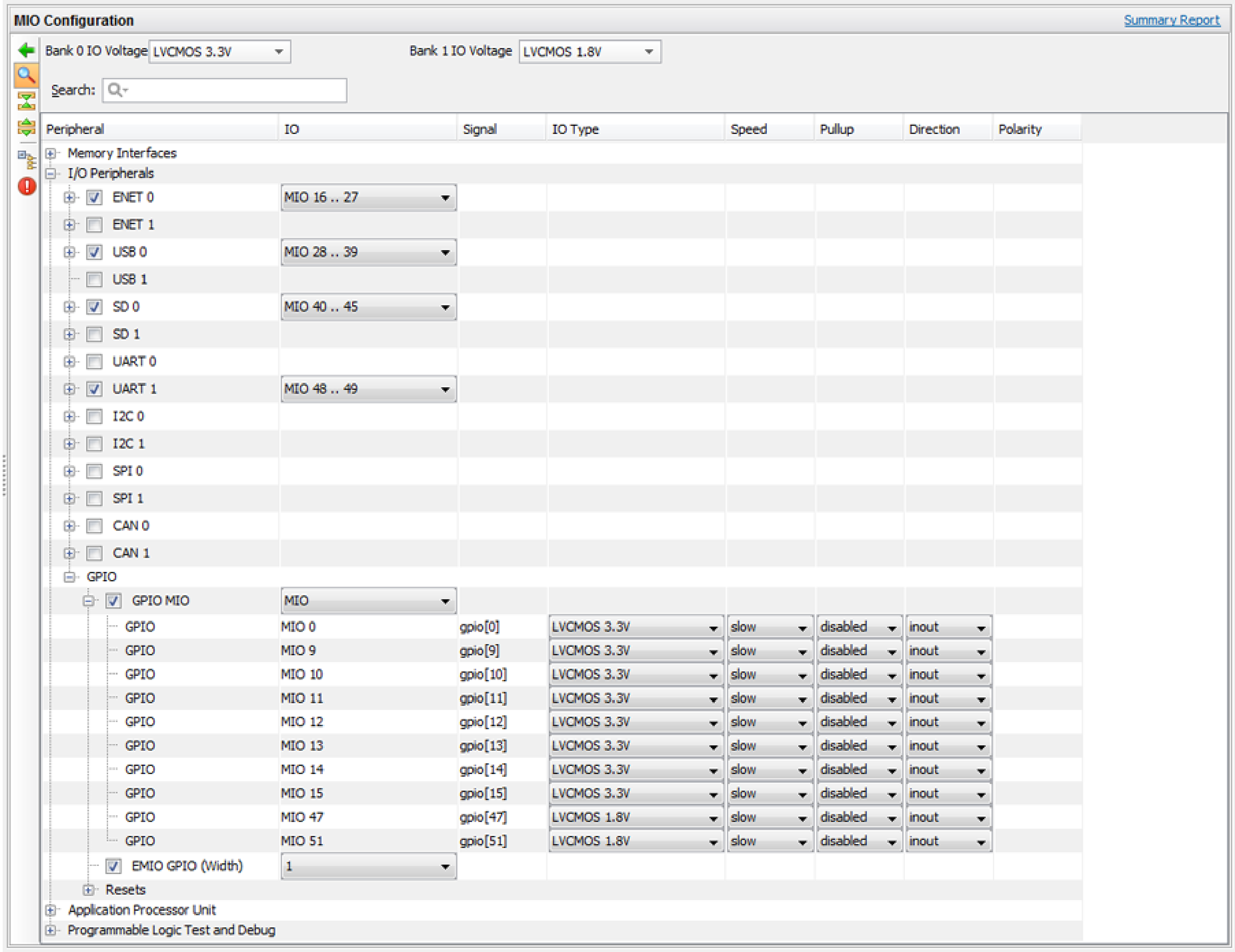


Figure 4. PS-PL configuration block diagram.

The essential MIO configurations used in this reference design are the UART and GPIO interfaces shown in **Figure 5**. UART 1 is used to communicate to a terminal program for external print statements to be outputted on MIO48(tx) and MIO49(rx). GPIO has connections to MIO15 (1-Wire) and the EMIO GPIO with a width of one used for an internal connection to the CSPRNG (rng_top_0). All the other MIO configurations are the default settings from the Avnet’s MicroZed Board Definition, which are not used for this reference design.



MIO Configuration

Bank 0 IO Voltage LVCMOS 3.3V

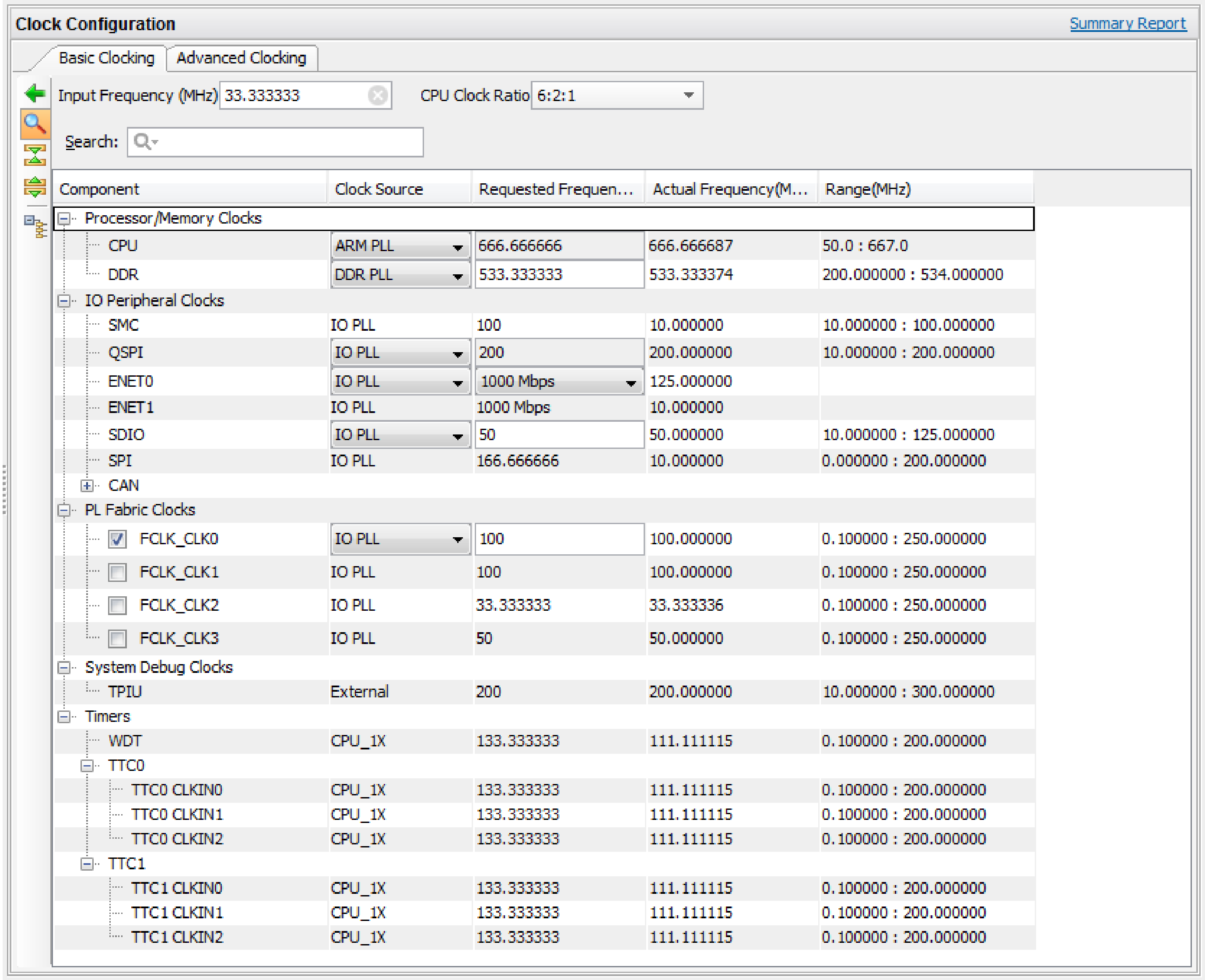
Bank 1 IO Voltage LVCMOS 1.8V

Search:

Peripheral	IO	Signal	IO Type	Speed	Pullup	Direction	Polarity
Memory Interfaces							
I/O Peripherals							
☑ ENET 0	MIO 16 .. 27						
□ ENET 1							
☑ USB 0	MIO 28 .. 39						
□ USB 1							
☑ SD 0	MIO 40 .. 45						
□ SD 1							
□ UART 0							
☑ UART 1	MIO 48 .. 49						
□ I2C 0							
□ I2C 1							
□ SPI 0							
□ SPI 1							
□ CAN 0							
□ CAN 1							
GPIO							
☑ GPIO MIO	MIO						
GPIO	MIO 0	gpio[0]	LVCMOS 3.3V	slow	disabled	inout	
GPIO	MIO 9	gpio[9]	LVCMOS 3.3V	slow	disabled	inout	
GPIO	MIO 10	gpio[10]	LVCMOS 3.3V	slow	disabled	inout	
GPIO	MIO 11	gpio[11]	LVCMOS 3.3V	slow	disabled	inout	
GPIO	MIO 12	gpio[12]	LVCMOS 3.3V	slow	disabled	inout	
GPIO	MIO 13	gpio[13]	LVCMOS 3.3V	slow	disabled	inout	
GPIO	MIO 14	gpio[14]	LVCMOS 3.3V	slow	disabled	inout	
GPIO	MIO 15	gpio[15]	LVCMOS 3.3V	slow	disabled	inout	
GPIO	MIO 47	gpio[47]	LVCMOS 1.8V	slow	disabled	inout	
GPIO	MIO 51	gpio[51]	LVCMOS 1.8V	slow	disabled	inout	
☑ EMIO GPIO (Width)	1						
Resets							
Application Processor Unit							
Programmable Logic Test and Debug							

Figure 5. Block diagram of the Zynq MIO configuration.

The clock configuration is set to use Avnet's MicroZed board definition defaults with the exception being that the FCLK_CLK0 signal is enabled and used to source the CSPRNG as shown in **Figure 6**.



Clock Configuration

Input Frequency (MHz) 33.333333

CPU Clock Ratio 6:2:1

Search:

Component	Clock Source	Requested Frequen...	Actual Frequency(M...	Range(MHz)
Processor/Memory Clocks				
CPU	ARM PLL	666.666666	666.666687	50.0 : 667.0
DDR	DDR PLL	533.333333	533.333374	200.000000 : 534.000000
IO Peripheral Clocks				
SMC	IO PLL	100	10.000000	10.000000 : 100.000000
QSPI	IO PLL	200	200.000000	10.000000 : 200.000000
ENET0	IO PLL	1000 Mbps	125.000000	
ENET1	IO PLL	1000 Mbps	10.000000	
SDIO	IO PLL	50	50.000000	10.000000 : 125.000000
SPI	IO PLL	166.666666	10.000000	0.000000 : 200.000000
CAN				
PL Fabric Clocks				
☑ FCLK_CLK0	IO PLL	100	100.000000	0.100000 : 250.000000
□ FCLK_CLK1	IO PLL	100	100.000000	0.100000 : 250.000000
□ FCLK_CLK2	IO PLL	33.333333	33.333336	0.100000 : 250.000000
□ FCLK_CLK3	IO PLL	50	50.000000	0.100000 : 250.000000
System Debug Clocks				
TPIU	External	200	200.000000	10.000000 : 300.000000
Timers				
WDT	CPU_1X	133.333333	111.111115	0.100000 : 200.000000
TTC0				
TTC0 CLKIN0	CPU_1X	133.333333	111.111115	0.100000 : 200.000000
TTC0 CLKIN1	CPU_1X	133.333333	111.111115	0.100000 : 200.000000
TTC0 CLKIN2	CPU_1X	133.333333	111.111115	0.100000 : 200.000000
TTC1				
TTC1 CLKIN0	CPU_1X	133.333333	111.111115	0.100000 : 200.000000
TTC1 CLKIN1	CPU_1X	133.333333	111.111115	0.100000 : 200.000000
TTC1 CLKIN2	CPU_1X	133.333333	111.111115	0.100000 : 200.000000

Figure 6. Block diagram of the Zynq clock configuration.

The CSPRNG is an exclusive-or of the outputs of two ring oscillators with two different periods and is sampled by the FCLK_CLK0 signal to make random numbers. Because of the two ring oscillators, this creates a combinatorial loop in the PL which usually creates an error when building the design. To overcome the error and make it a warning, the tcl file “project_setup.tcl” is to be run in the tcl console before running the full build. The file can be found under the “/MAXREFDES44/MZ_Zynq_HW” path.

Quick Start

Required Equipment:

- Windows® PC with two USB ports
- MAXREFDES44# board
- MAXREFDES44# supported platform (i.e., the MicroZed kit)
- Programming cable (i.e., the platform cable USB II or equivalent)
- DS28E35EVKIT# (2nd generation with DS2475)

Download, read, and carefully follow each step in the appropriate MAXREFDES44# Quick Start Guide.