



复杂、分布式电子学系统之 调试、诊断、慢控制接口的探索和实践

On the Shoulder of 100 Gbps

On the Demand of 100 eV

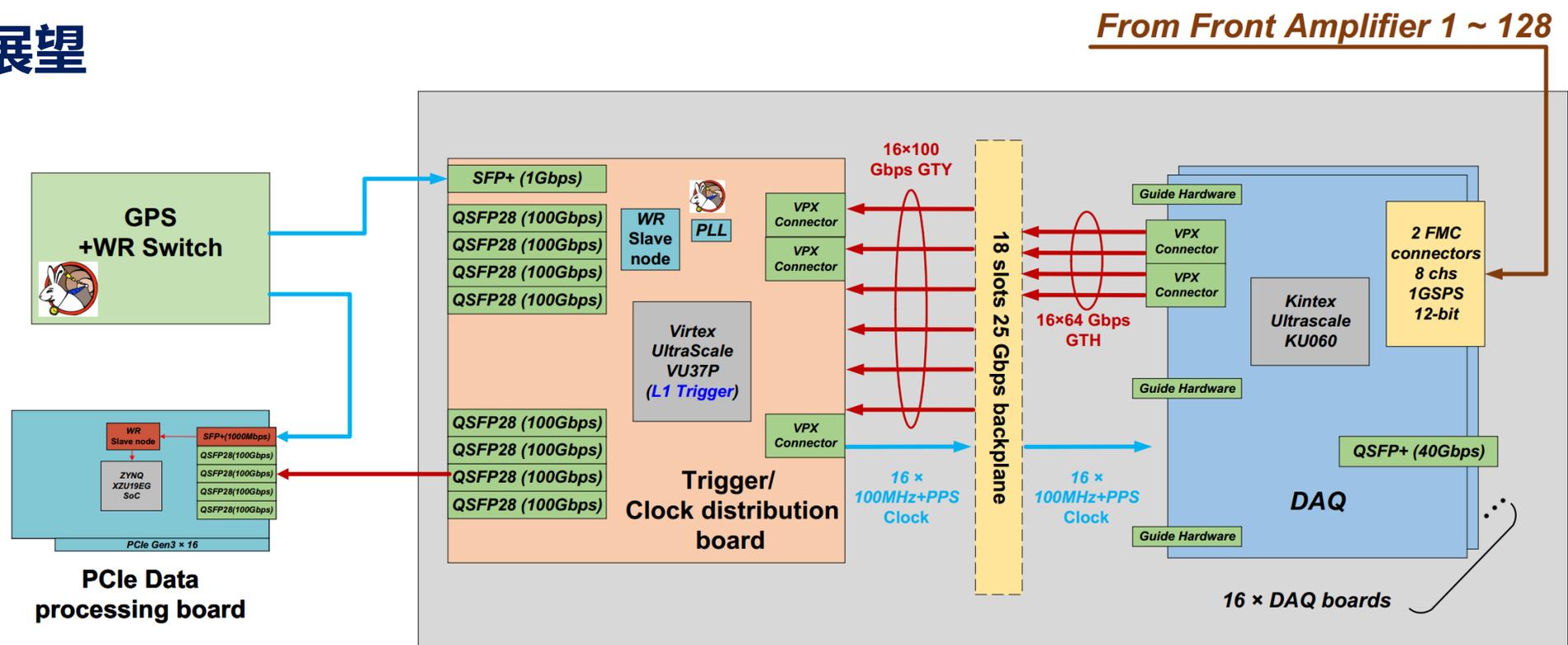
薛涛、文敬君、姜林、杨昊彦、韦亮军、潘秋彤、梁博

李荐民、刘以农

2024.07.16

目录

- Motivation, 从调试接口说起
- 电子学板卡的板载调试接口的实现
- 电子学系统远程调试接口的实现
- 电子学板卡中多个FPGA的互联和慢控制接口的实现
- 实践、总结和展望



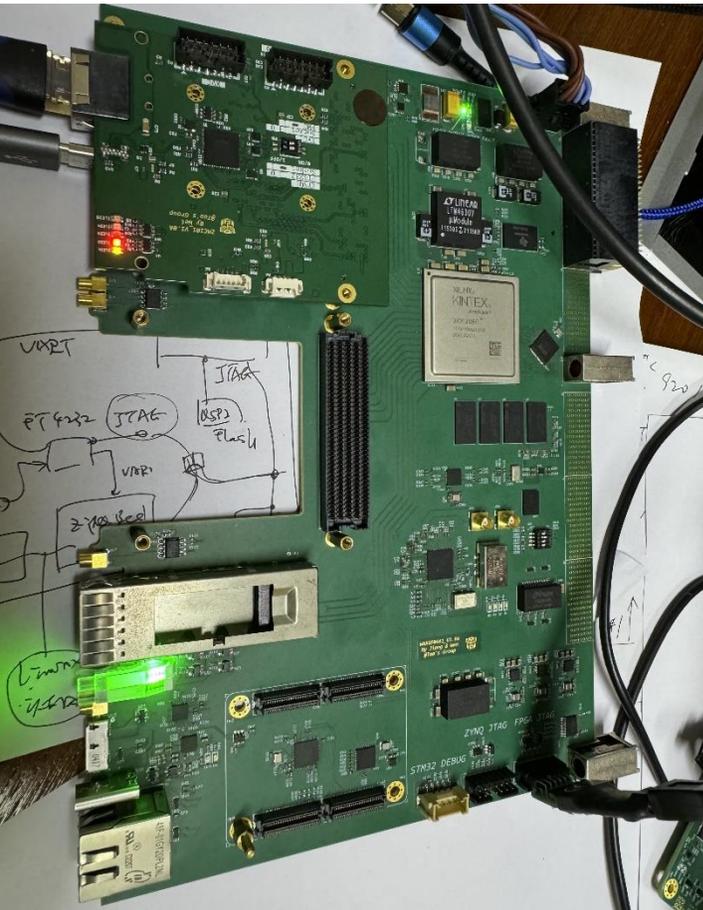
Motivation, 从调试接口说起

- **FPGA调试接口的历史、现状和思路**
 - 最常用的USB-JTAG紧凑型调试器及其局限性
 - 大规模、复杂、分布式电子学系统调试的痛点和需求
 - 从单块板卡，到几百、上千块板子组成系统的调试方法

Xilinx Parallel Cable IV



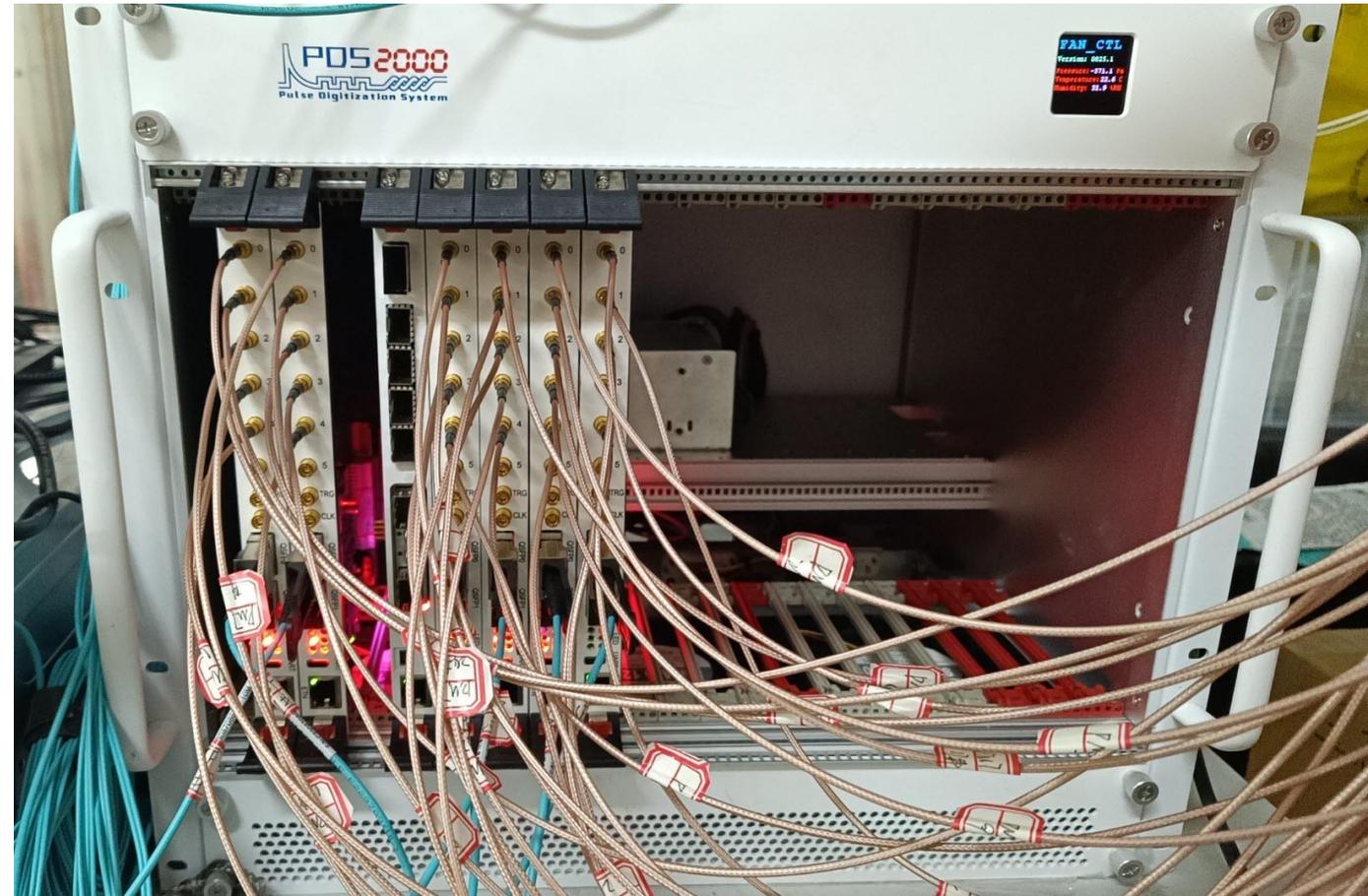
Xilinx Platform Cable USB II



Digilent JTAG-SMT2

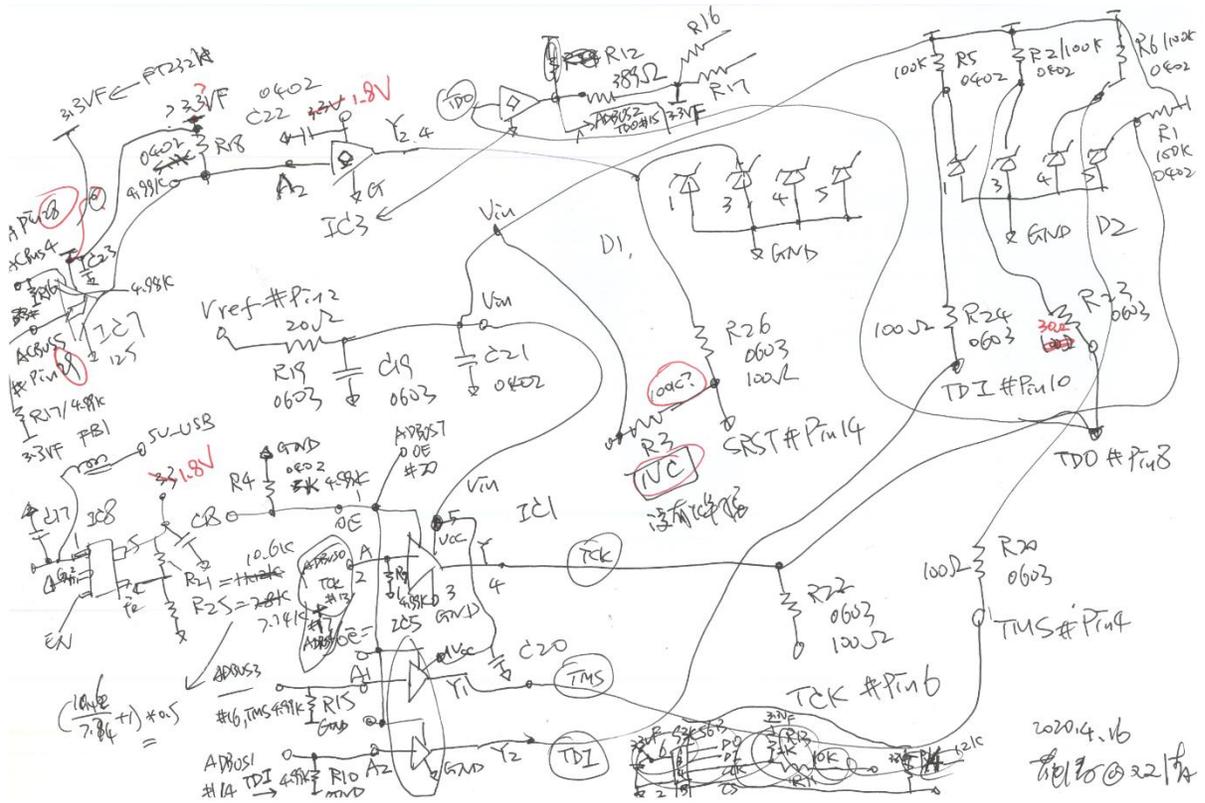
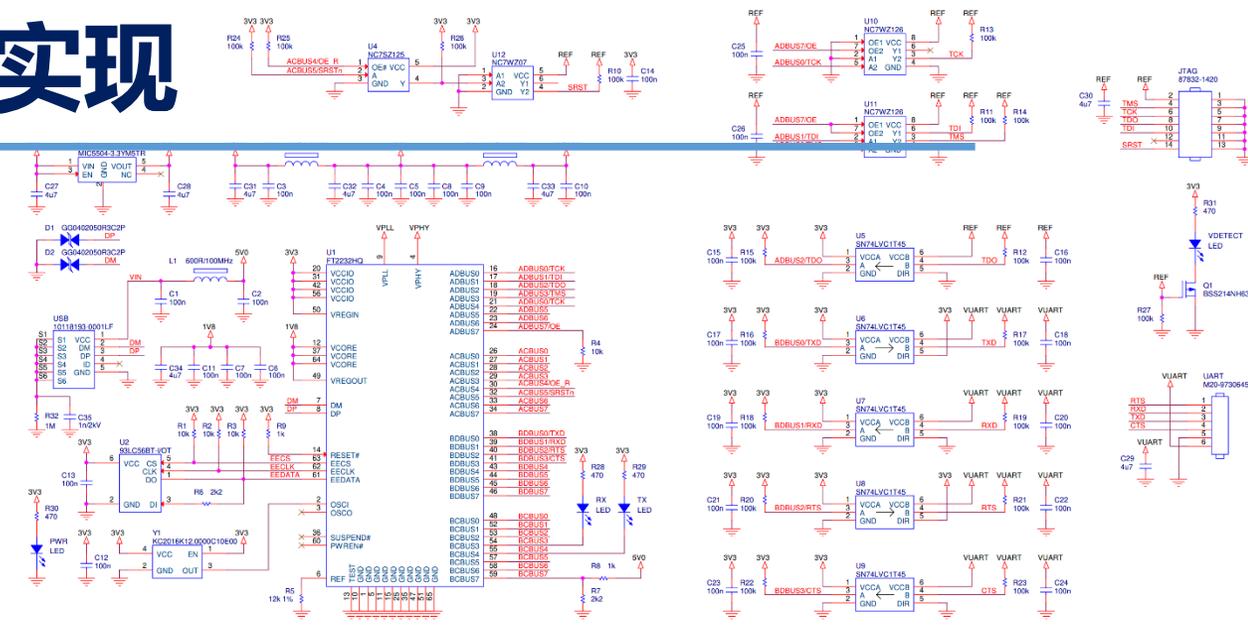


Digilent JTAG-HS3



电子学板卡的板载调试接口的实现

- **USB-JTAG/UART调试接口的实现思路**
- **使用FTDI公司的FT232HQ和FT4232HQ**
 - FT232HQ包含2个Channel, 可以实现JTAG+UART
 - FT4232HQ包含4个Channel, 可以实现JTAG+3×UART
 - 推荐使用TMUX1574做为JTAG二选一MUX
 - 推荐使用SN74AHC4T774做为JTAG电平转换
- <https://ieeexplore.ieee.org/abstract/document/8977100>



An Example of PCB Reverse Engineering – Reconstruction of Digilent JTAG SMT3 Schematic

Matěj Bartík CTU FIT matěj.bartík@fit.cvut.cz
 Tomáš Beneš CTU FIT benešto3@fit.cvut.cz
 Karel Hynek CTU FIT hynekkar@fit.cvut.cz

Abstract—This paper presents a successful reverse engineering process of Digilent JTAG-SMT3-NC module, revealing the identity of all key components. The reconstruction required a deep knowledge of PCB (Printed Circuit Board) design and manufacturing process and knowledge of (elementary) function principles and behavior of the examined device. We were able to reveal 80% of schematic via analysis of publicly available resources such as original high-resolution images and BOM (Bill of Material) fragments. The remaining 20% were obtained by non-invasive test equipment such as multi-meter and microscope. The reconstructed schematic has been verified by designing our own PCB implementing the original SMT3 function.

Index Terms—Xilinx FPGA; JTAG; Digilent; SMT3; Reverse Engineering; PCB; FTDI.

I. INTRODUCTION

A JTAG (Joint Test Action Group) [1] adapter is probably the most popular way for uploading a user code into a programmed device such as processors or any other programmable logic. It is nearly 30 years, when FPGAs/CPLDs development boards were used for education of the new generation of digital logic engineers, making a solderless breadboard and 74xx logic gates outdated and obsolete. However, these development boards were supplied without on-board JTAG adapter (as is common in the present) which has to be bought separately. That was the era of Xilinx Parallel Platform Cable III (DLC9) [2], which was connected to a PC via a parallel port, and much cheaper homemade DLC9 clones.



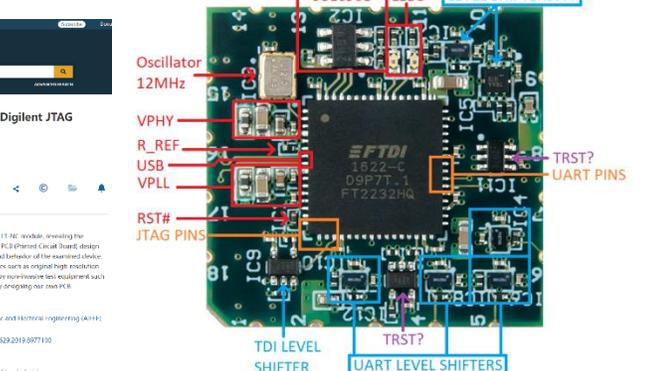
Fig. 1. Xilinx Platform Cable USB (DLC9)

The scenario became the same for DLC9 successors such as Xilinx Platform Cable USB I [3] (see Fig. 1) and II [4] (DLC9 and DLC10 respectively). The schematic and other resources of the DLC9 lacked nearly ten years ago [5] which allows to produce significantly cheaper clones (approximately 30 USD) compared to genuine DLC10 (225 USD). The price of a DLC9 clone [5] cannot be lowered further regarding two

Device Output

Word	MSB	0000	8801	0403	6010	0700	00C0	0008	0000	129AV.....
0000:	34AC	1AE0	0000	0000	0056	0001	92C7	356A	4.....V.....5j		
0010:	0157	3120	744A	6761	6D53	3374	0000	0000	...Wl tJgsm3...		
0018:	0000	0000	4400	6769	6C69	6E65	2074	544A	...D.giline tTJ		
0020:	4741	532D	544D	0033	0000	0000	0000	0000	GAS-IM.3.....		
0028:	0000	0001	0000	0000	0000	0000	0000	0000D.i		
0030:	0000	0000	0000	0000	0000	0000	0000	0000	.g.i.l.e.n.t.4.D		
0038:	0000	0000	0000	0000	0000	0000	0000	0000	i.g.i.l.e.n.t.		
0040:	0000	0000	0000	0000	0000	0000	0000	0000	.A.d.e.p.t..U.S		
0048:	0000	0000	0000	0000	0000	0312	0044	0069	.B..D.e.v.i.c.e		
0050:	0067	0069	006C	0065	006E	0074	0334	0044	...2.1.0.3.5.7.A		
0058:	0069	0067	0069	006C	0065	006E	0074	0020	.7.D.0.0.E.....f.		
0060:	0041	0064	0065	0070	0074	0020	0055	0053			
0068:	0042	0020	0044	0065	0076	0069	0063	0065			
0070:	031A	0032	0031	0030	0033	0035	0037	0041			
0078:	0037	0044	0030	0030	0045	0030	0000	7882			

User I



电子学板卡的板载调试接口的实现

- **Vivado的支持: 将FT232HQ/FT2232HQ/FT4232HQ配置为USB-JTAG/UART调试器**

- **Vivado从2022.1版本开始支持 program_ftdi 将FTDI公司的FT2232HQ和FT4232HQ变成USB-JTAG调试器**

- FT2232HQ包含2个Channel, 可以实现JTAG+UART。Vivado将其 Channel A 编程为JTAG接口, Channel B 默认为UART接口。
- FT4232HQ包含4个Channel, 可以实现JTAG+3×UART。Vivado将其 Channel A 编程为JTAG接口, Channel B/C/D 默认为UART接口。可以修订EEPROM将 Channel B 配置为SWD/JTAG接口用于板载底层控制器/STM32的编程接口。

AMD Technical Information Portal

Vivado Design Suite User Guide: Programming and Debugging (UG908) UG908 2022-04-26 2022.1 English

在文档中搜索
关键字

目录

- + Vivado Lab Edition
- + Generating the Bitstream or Device Image
- + Programming the Device
- + Remote Debugging in Vivado
- + Programming Configuration Memory Devices
- + Advanced Programming Features
- + Serial Vector Format (SVF) File Programming
- + Debugging the Design
- + In-System Logic Design Debugging Flows
- + Debugging Logic Designs in Hardware
- + Viewing ILA Probe Data in the Waveform Viewer
- + Debugging Designs Post Implementation
- + Serial I/O Hardware Debugging Flows
- + Versal Serial I/O Hardware Debugging Flows
- + Debugging the Serial I/O Design in Hardware
- + Device Configuration Bitstream or PDI Settings
- + Trigger State Machine Language Description
- + Low Level SVF JTAG Commands
- + JTAG Cables and Devices Supported by hw_server
- **Programming FTDI Devices for Vivado Hardware Manager Support**

Programming FTDI Devices for Vivado Hardware Manager Support

For FTDI devices to be recognized as a USB-to-JTAG interface in Xilinx® JTAG software tools such as XSDB or the Vivado® Hardware Manager the EEPROM on the FTDI device must be programmed with a custom firmware provided by Xilinx. Programming the FTDI is accomplished by using the `program_ftdi` utility included in the Vivado install as a Tcl command. Once programmed, the FTDI device will be recognized as a valid programming cable in Vivado.

Note: For on-board implementation details including FTDI connectivity, please reference the Xilinx VCK190 Schematics available in XTP610 on <https://www.xilinx.com/products/boards-and-kits/vck190.html>

The `program_ftdi` utility supports the following FTDI devices:

- FT232H
- FT2232H
- FT4232H

Command Reference:

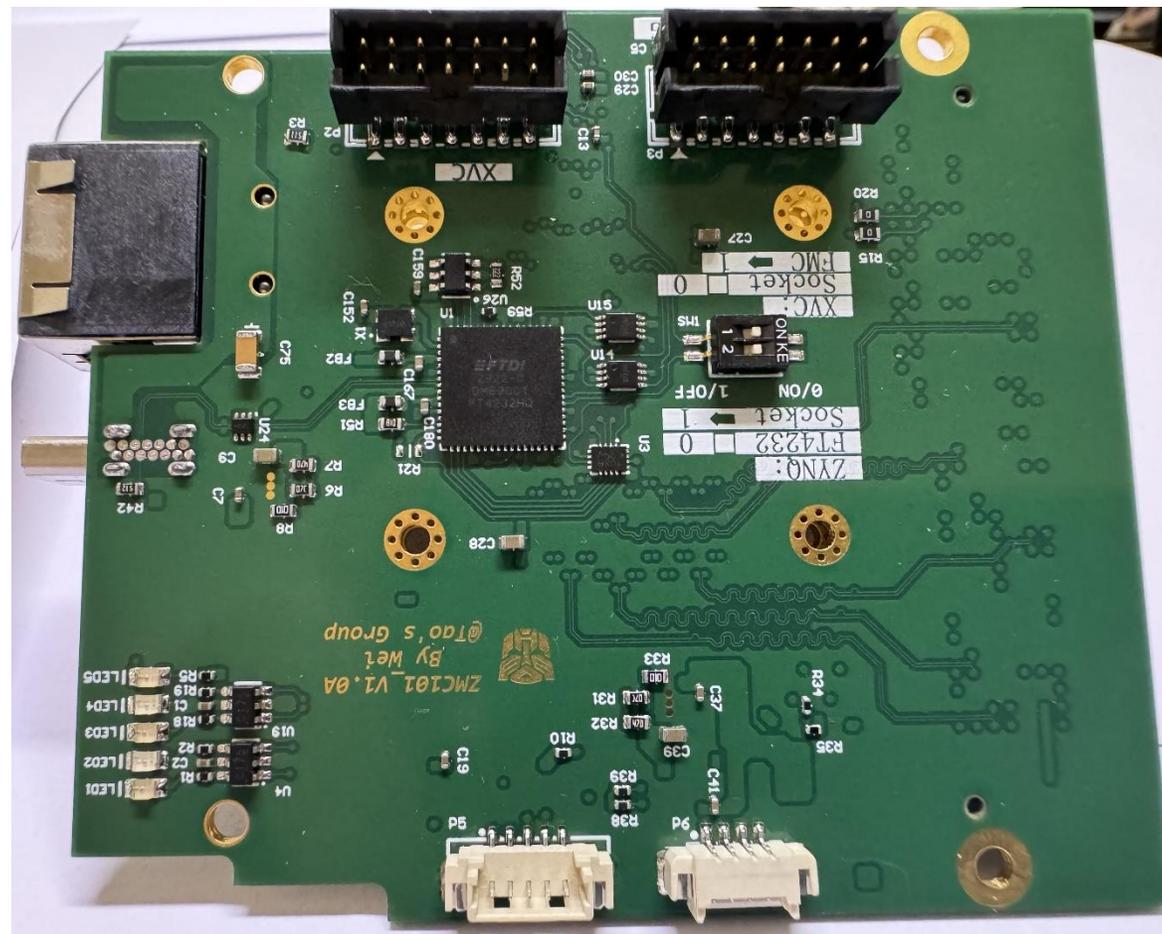
```
program_ftdi
```

Short Description
Write/Read to FTDI EEPROM for Xilinx JTAG Tools support

Syntax:
`program_ftdi [-write -ftdi=<ftdi_part> -serial=<serial_number> [-vendor=<vendor_name>] [-board=<board_name>]] [-m=<manufacturer>] [-desc=<description>] | [-write -filein=<cfg_filein>] | [-read [-fileout=<cfg_fileout>]] [-help] [-longhelp]`

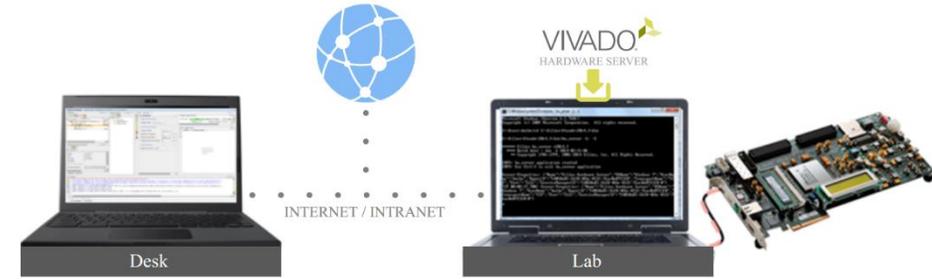
Usage:

Name	Description
-ftdi	Specify the ftdi device to be programmed <FT232H FT2232H FT4232H>
-serial	Serial number to be written into the EEPROM

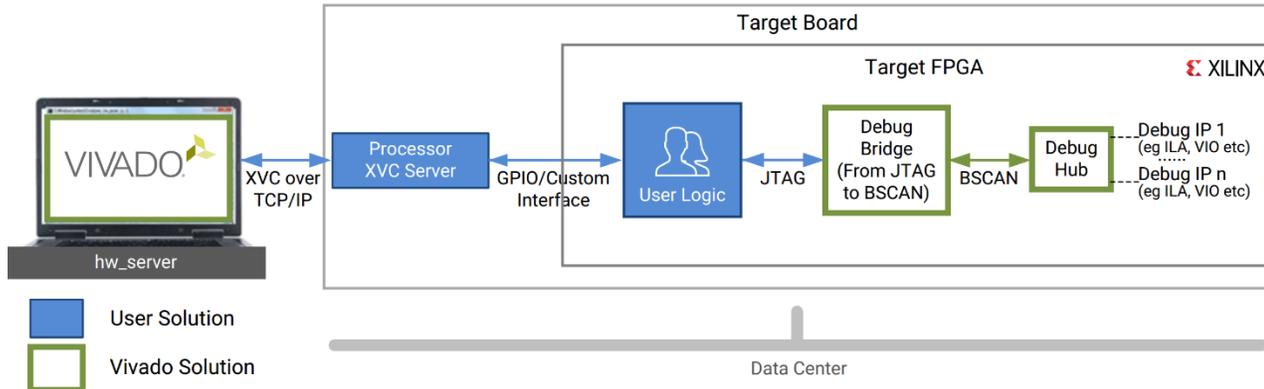


电子学系统远程调试接口的实现

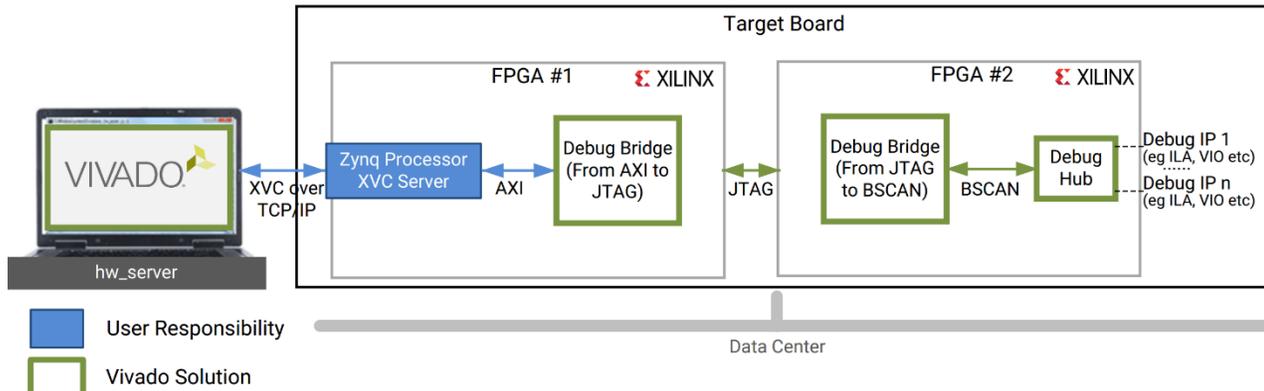
- XVC (Xilinx Virtual Cable) 通过以太网进行远程调试的JTAG接口
 - 使用Debug Bridge IP核及运行与Embedded Linux上的 xvcServer
 - <https://github.com/Xilinx/XilinxVirtualCable>
 - https://support.xilinx.com/s/article/974879?language=en_US



From AXI to BSCAN

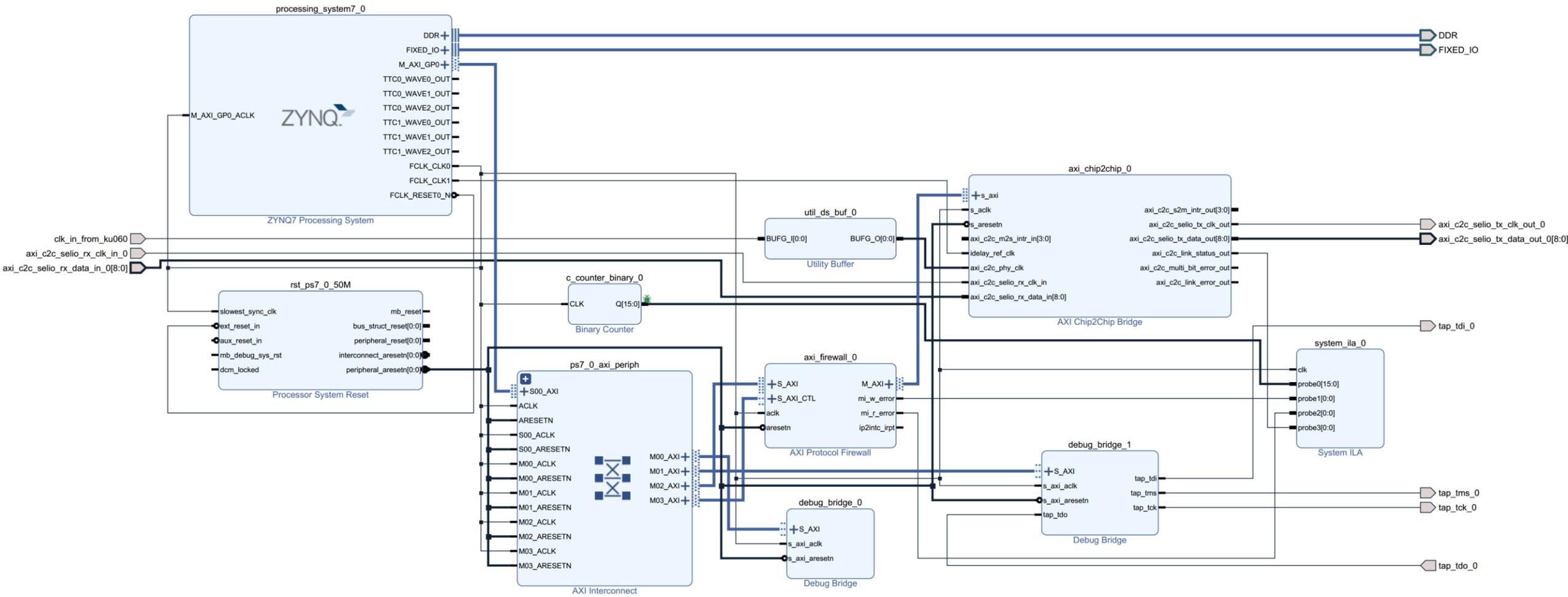


AXI to JTAG Debug Bridge



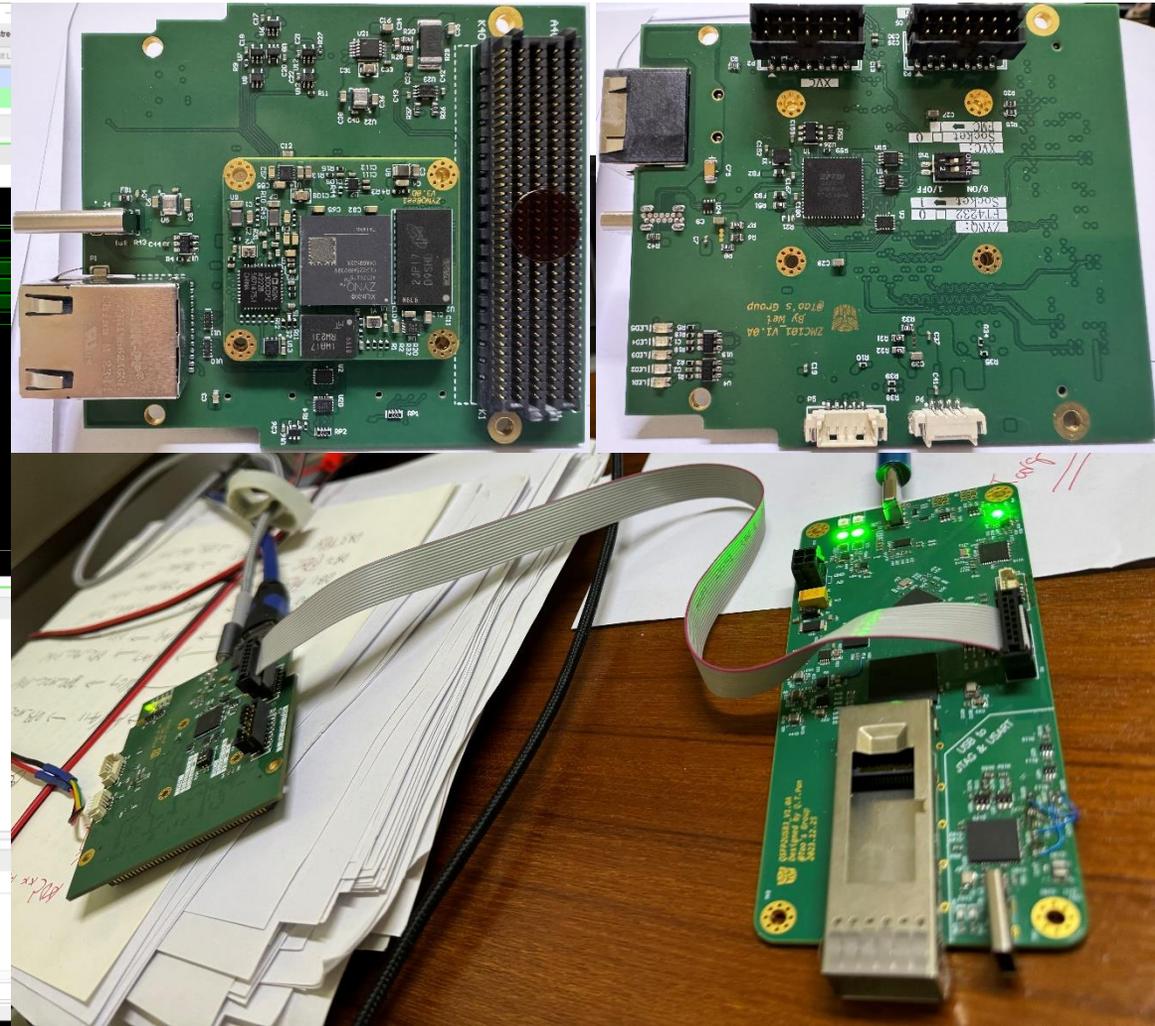
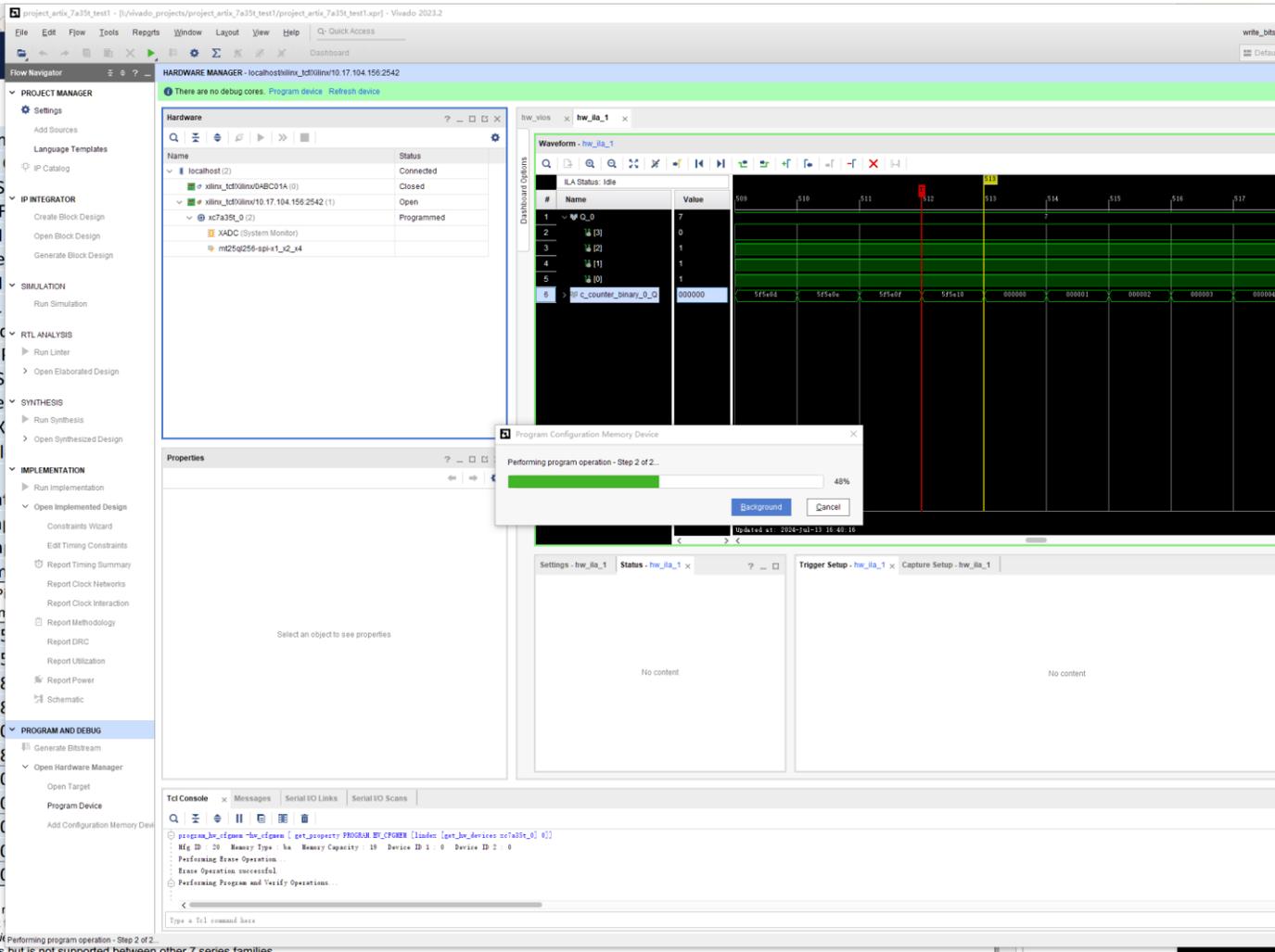
电子学系统远程调试接口的实现

- 使用XVC/Debug Bridge实现ZYNQ/ZYNQMP上复杂PL端固件的远程调试
 - 使用Debug Bridge IP核 (AXI to BSCAN) 及运行与Embedded Linux上的 xvcServer
 - 配合ILA/VIO实现ZYNQ/ZYNQMP正常运行Embedded Linux并调试PL端固件



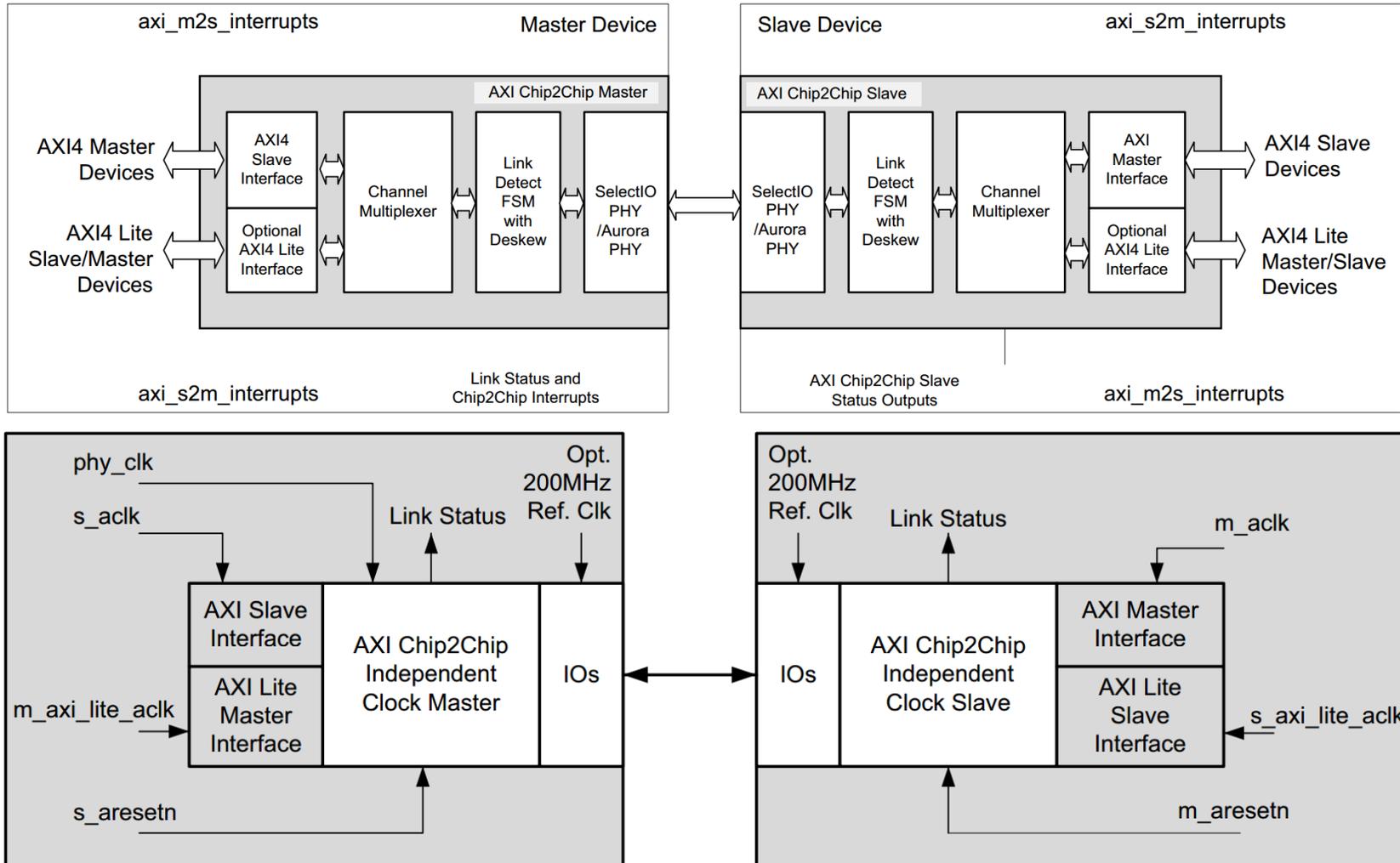
电子学系统远程调试接口的实现

- 使用XVC/Debug Bridge实现ZYNQ/ZYNQMP上复杂PL端固件的远程调试
 - 使用Debug Bridge IP核 (AXI to JTAG) 及运行与Embedded Linux上的 xvcServer
 - 配合ILA/VIO实现正常使用Vivado远程调试连接到ZYNQ/ZYNQMP XVC接口上其他FPGA



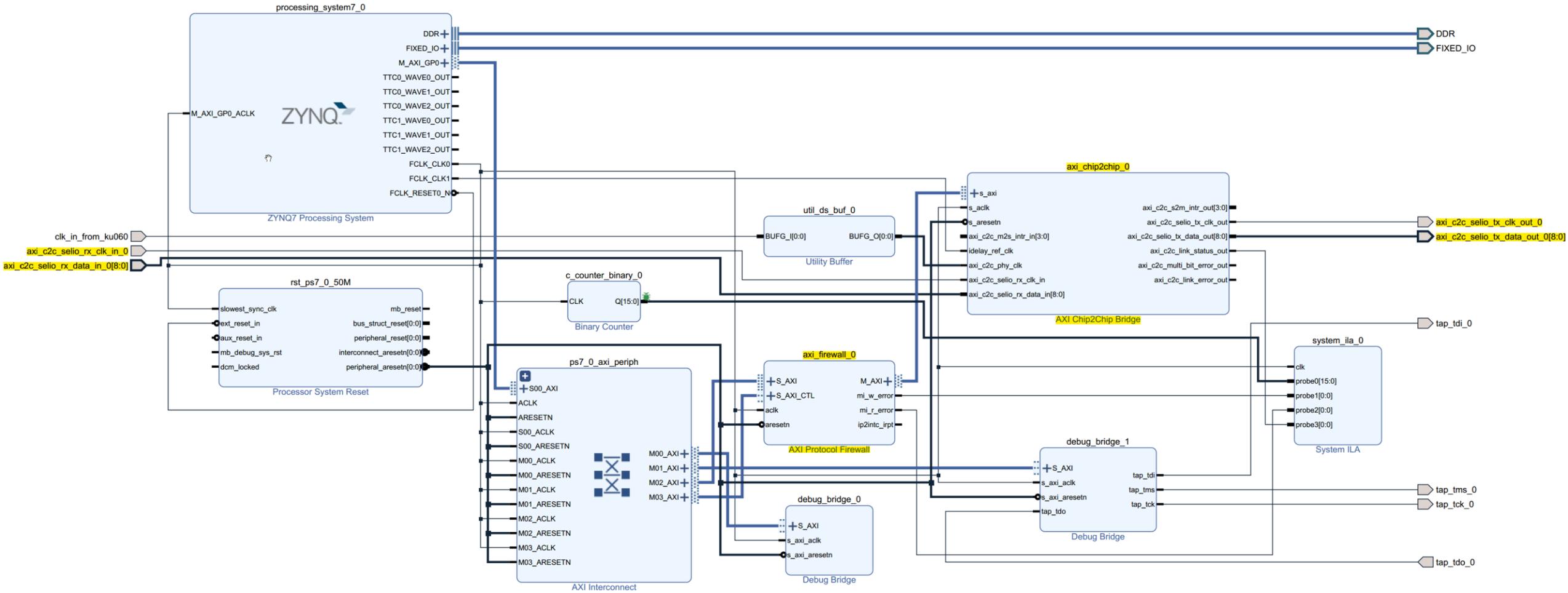
电子学板卡中多个FPGA的互联和慢控制接口的实现

- 使用Chip2Chip (SelectIO/Aurora) 实现ZYNQ/ZYNQMP与大规模FPGA的互联和慢控制
 - 使用c2c, 经过SelectIO (Single Ended/LVDS) 或者Aurora (GT) 将两个或者多个FPGA高速互联
 - 至少需要20跟/对IO或者LVDS, 或者1对GT (RX+TX)



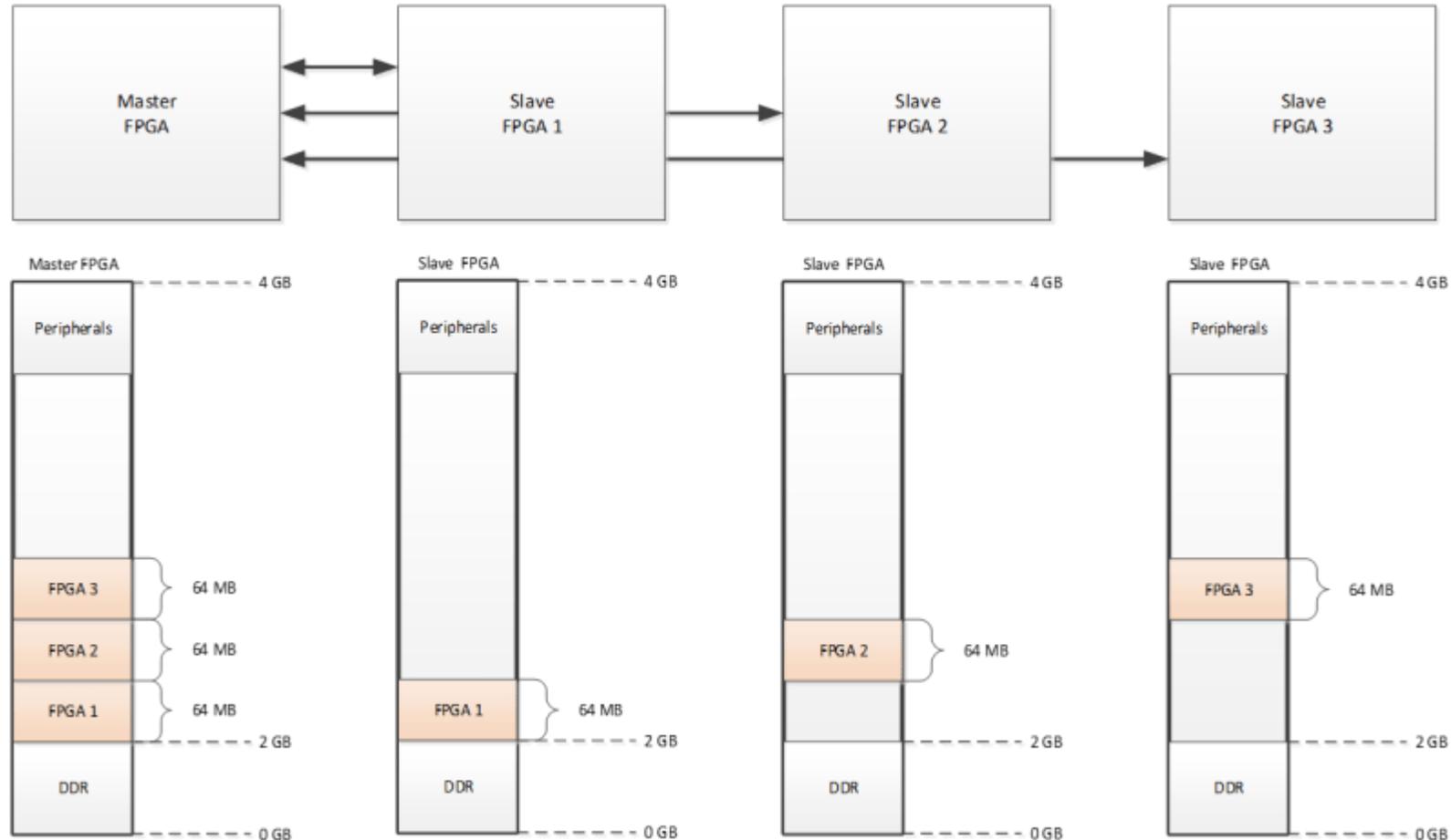
电子学板卡中多个FPGA的互联和慢控制接口的实现

- 使用Chip2Chip (SelectIO/Aurora) 实现ZYNQ/ZYNQMP与大规模FPGA的互联和慢控制
 - 可以使用 AXI Protocol Firewall 有效隔离c2c和系统AXI BUS, 并保证调试阶段不被 hang



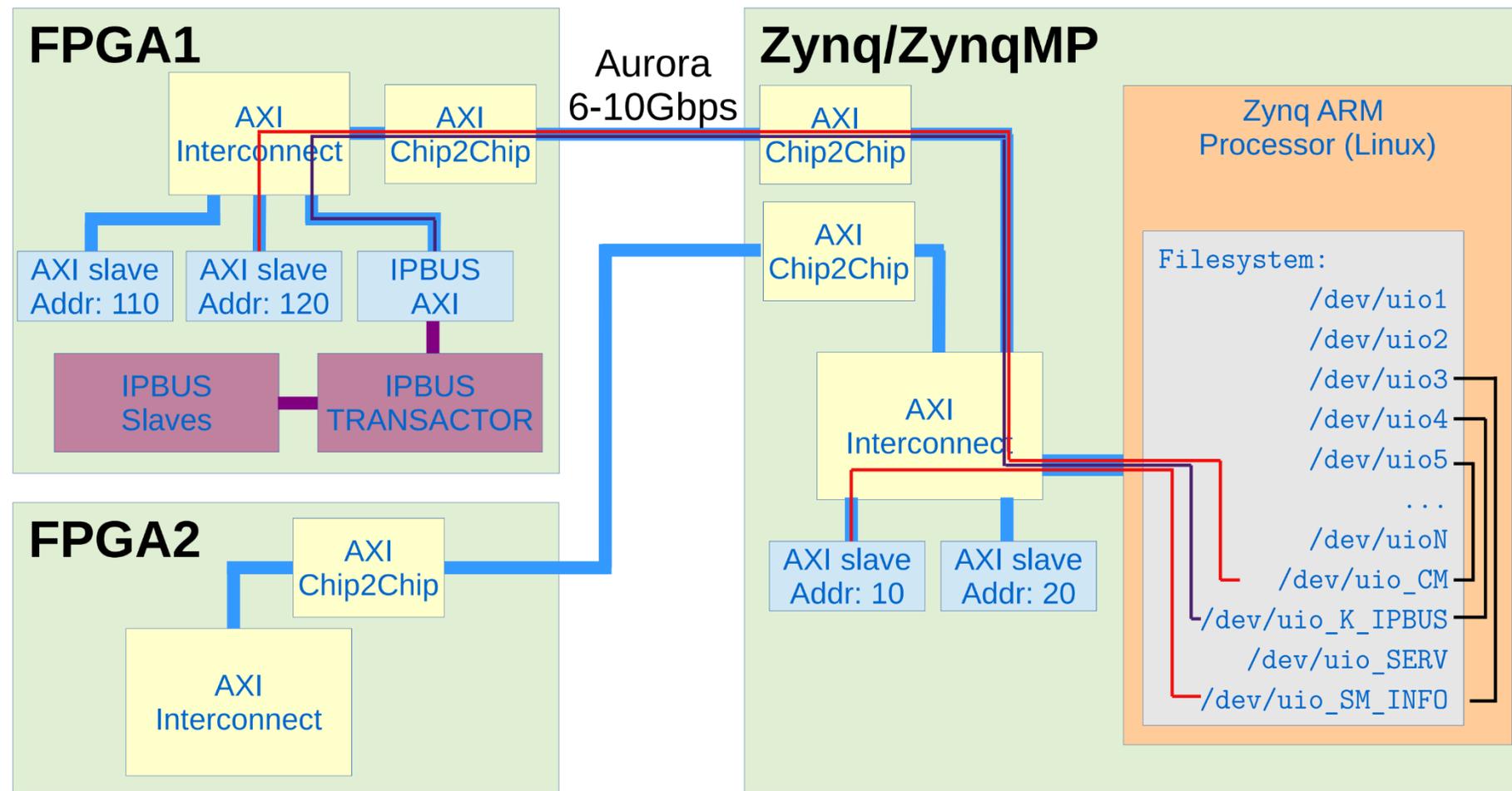
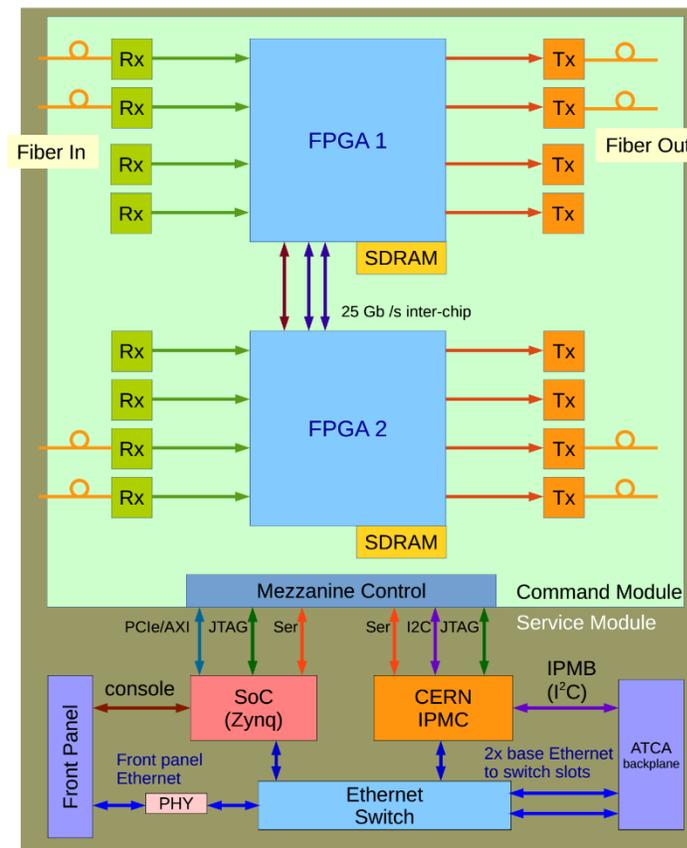
电子学板卡中多个FPGA的互联和慢控制接口的实现

- 使用Chip2Chip (SelectIO/Aurora) 实现ZYNQ/ZYNQMP与大规模FPGA的互联和慢控制
 - 实现c2c之后, 其他FPGA就像内存映射一样, 可以将其一段Memory映射到主FPGA (ZYNQ/ZYNQMP) 的地址空间



实践：CERN

- CERN, Apollo Blade Platform Team build APOLLO Platform for CMS and ATLAS



非常棒的设计。不但有硬件设计思路，还包含 Embedded Linux 上的软件设计思路。

https://indico.cern.ch/event/799275/contributions/3413769/attachments/1861634/3059771/DGastler_SoCWS_2019-06-13.pdf

<https://indico.cern.ch/event/996093/contributions/4376632/attachments/2260716/3837066/Dgastler-2021-06-09-ApolloUpdate.pdf>

实践：我们

- 在锦屏暗物质探测实验和锦屏中微子观测实验中，读出电子学系统的核心，2×FMC载板WRX602使用了自主研制的ZYNQBee1 V3.0D模块通过XVC和Chip2Chip，实现ZYNQ与大规模FPGA (XCKU060) 的互联和慢控制

- FT4232HQ用于单板调试接口**

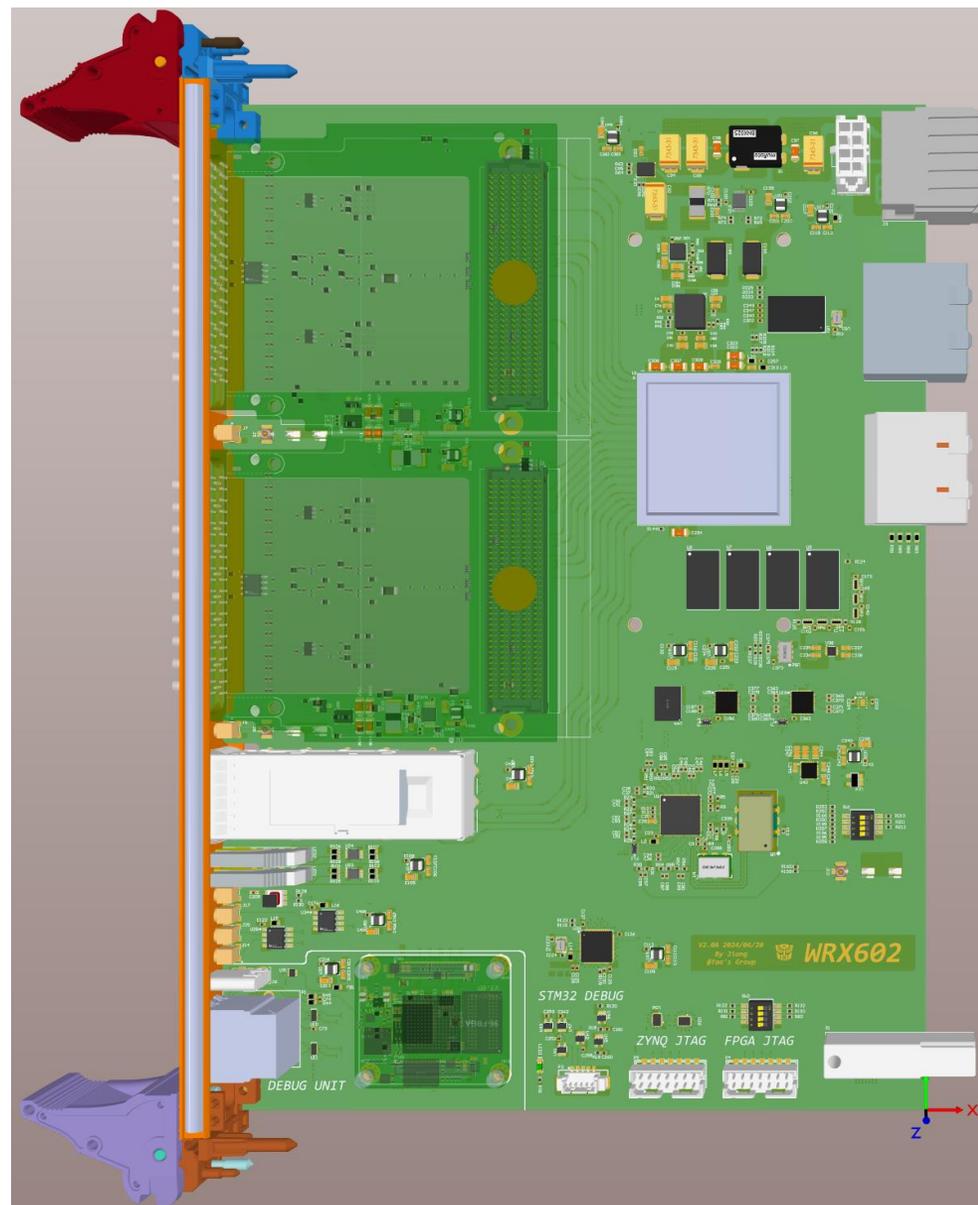
- 前面板使用TypeC接口，Channel A实现JTAG，经过电平转换和MUX，可选直接连接到ZYNQ或者KU060
- FT4232HQ的Channel B实现SWD，连接到底层控制的STM32
- FT4232HQ的Channel C/D实现UART，分别连接到ZYNQ和STM32

- ZYNQBee1 V3.0D**

- 512MB DDR3 SDRAM
- 64MB QSPI Flash
- 16GB eMMC
- Ethernet PHY
- 尺寸为 30mm×35mm
- 运行Embedded Linux 和 xvcServer，支持SSH远程

- 2×FMC接口，均支持LA/HA及8 Lanes，板载时钟 LMK04828

- 前面板QSFP光纤接口和背板8 Lanes/16 Gbps Serdes接口



总结和展望

- 使用FTDI公司的FT2232HQ和FT4232HQ，配合Vivado开发环境，能够有效解决单板电子学板卡的板载调试接口需求；
- 使用ZYNQBee1 V3.0D运行Embedded Linux，实现Debug Bridge，能够实现远程JTAG调试、编程接口。实现大规模、复杂、分布式电子学系统的调试；
- 使用Chip2Chip，能够将其他大型FPGA的控制、数据接口映射到ZYNQBee1 V3.0D运行的Embedded Linux中，非常有利于大规模、复杂、分布式电子学系统控制和维护。
- 未来在锦屏暗物质探测实验和锦屏中微子观测实验中使用上述技术来满足大规模电子学系统的各项需求。



谢谢!

