Bus Spider: flexible open source hacker multi-tool

Introduction

Different sensors and controllers are used during development of electronics. In most cases these controllers use serial interfaces (I2C, SPI, UART) for communication. It is useful to test them sending commands and analyzing results. However, in most cases PC does not have corresponding interfaces.

The well-known Bus Pirate v3 (http://dangerousprototypes.com/docs/Bus_Pirate) device developed by Dangerous Prototypes resolves this issue. It's a cheap and universal device. It can be connected to regular PC via USB and provides ability to use several most common serial interfaces. Communication with Bus Pirate is performed through serial console.

Unfortunately, Bus Pirate v3 has several issues:

- low throughput (approximately 10 KB/s);
- interfaces are multiplexed (only one can be used at the same time);
- exit from UART-USB bridge mode requires resetting the device.

These issues are caused by the limited specs of PIC24FJ64GA002 16-bit Microchip microcontroller used in Bus Pirate v3.

There is Bus Pirate v4. It has better throughput than Bus Pirate v3. Unfortunately it seems that Dangerous Prototypes abandoned Bus Pirate v4 firmware development and it never reached stable state.

Bus Spider

This project proposes to create Bus Spider --- a superior device based on the FPGA board. We are using FPGA to implements a SoC with RISC-V compatible core picorv32 (https://github.com/cliffordwolf/picorv32). The SoC is being developed in MIET (https://github.com/miet-riscv-workgroup/rv32-simple-soc).
Embedded software rewritten from scratch will provide the same well-approved serial console interface as the Bus Pirate's.
In our project we will consider the experience of the Bus Pirate creators trying to preserve usability of original device.
We plan to add hardware JTAG controller and a logical analyzer in the future.
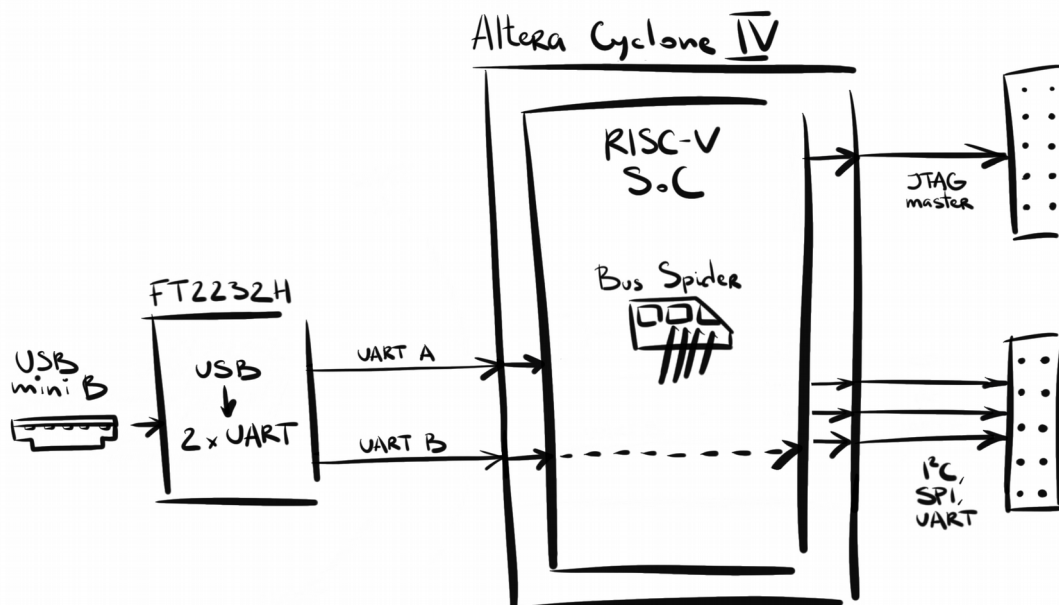
Block Diagrams

Fig. 1

Fig. 1 shows implementation of Bus Spider with basic functionality. This prototype already was created and evaluated (see fig. 1a). Information about it's components can be found here:

- FT2232 breakout board
  (http://dangerousprototypes.com/docs/FT2232_breakout_board);
- CoreEP4CE6 (https://www.waveshare.com/wiki/CoreEP4CE6).

Fig. 1a

②

Altera Cyclone **IV**

Raspberry Pi 3

SPI

SPI
↓
×2 UART

UART A

UART B

RISC-V
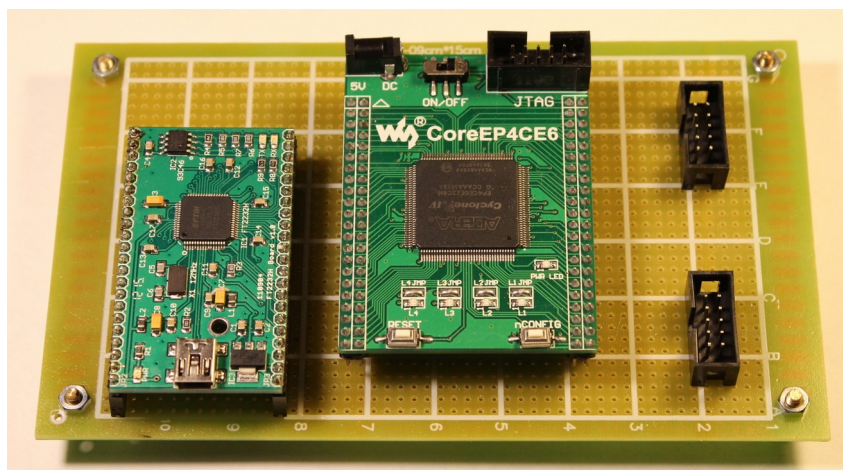SoC

Bus Spider

Wi-Fi Ethernet
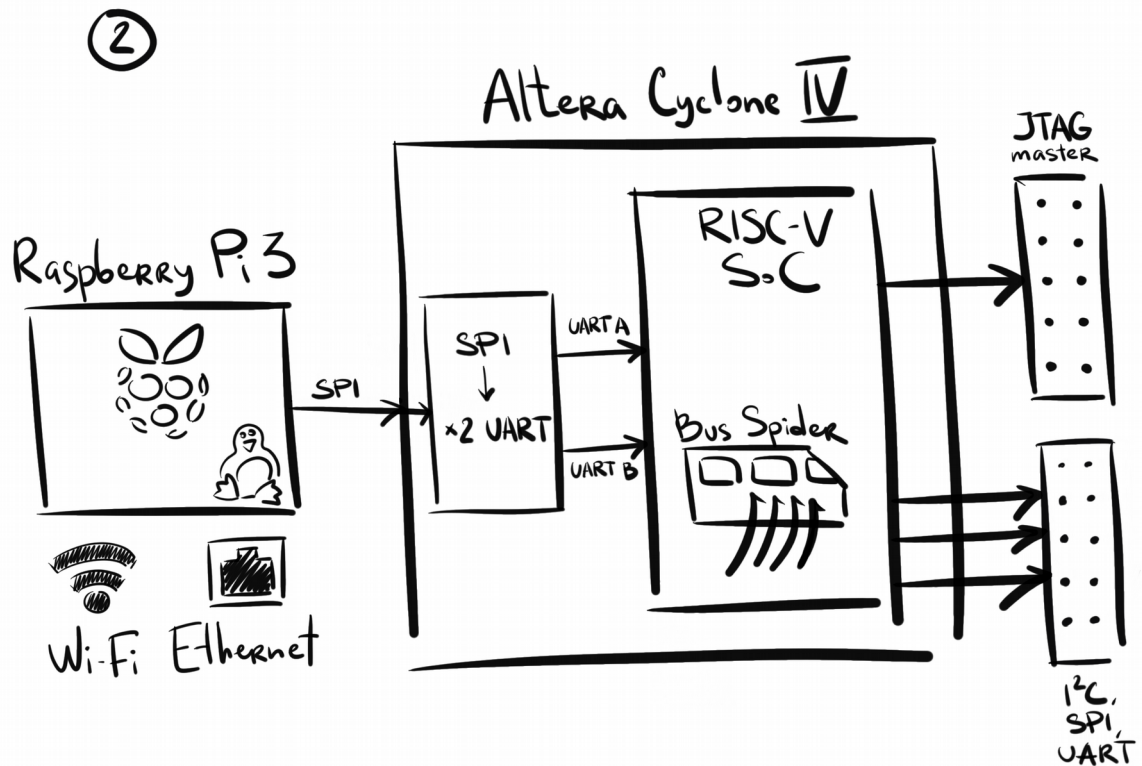
JTAG
master

I²C,
SPI,
UART

Fig. 2

Fig. 2 shows Bus Spider working in conjunction with Raspberry Pi 3 to provide network accessibility. This implementation uses SPI to speed up data transfers.
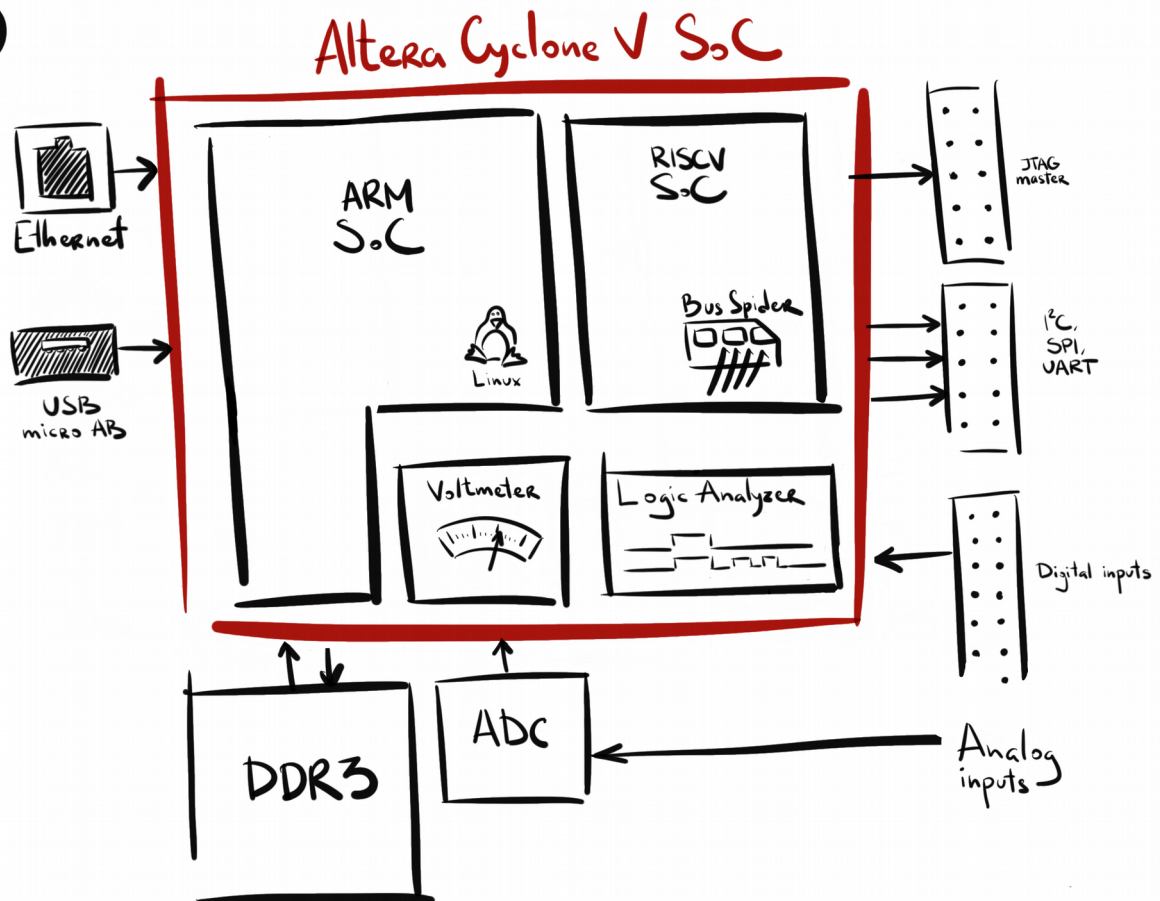
Fig. 3

Fig. 3 demonstrates implementation of Linux host and Bus Spider controller on the same FPGA chip, using Cyclone V SoC ARM core. External fast RAM can be used to implement logic analyzer functionality.

Features

1. Bus Spider preserves mature Bus Pirate protocol: software for Bus Pirate can be used with Bus Spider;
2. Higher throughput of host interface: much higher than 10 KB/s of Bus Pirate v3;
3. FPGA makes Bus Spider expandable: user can add specific interface if necessary;
4. FPGA permits achieving higher level of system integration: Linux host and Bus Spider can be implemented in the same FPGA device;
5. FPGA makes it possible to add logic analyzer functionality.