SEC Xtractor – Assisted Hardware Analysis Tool

Thomas Weber [1]

SEC Consult Unternehmensberatung GmbH[2]*,*
SEC Consult Vulnerability Lab,
Leopold-Ungar-Platz 2/3/3, 1190, Vienna
Responsible: T. Weber, Classification: Public

December 2, 2019

[1] research@sec-consult.com
[2] https://www.sec-consult.com

Chapter 1

Overview

This chapter gives an overview about the SEC Xtractor tool and its functionalities. The schematics are also located here.

1.1 General Description

The SEC Xtractor Assisted Hardware Analysis Tool was originally designed as internal hardware analysis tool. It was used as all-in-one solution to dump NAND NOR SPI and I2C flash memory chips. Because of different voltage levels of some chips, the SEC Xtractor provides the option to adjust the voltage from 1.8V to 5.3V. Its program code is completely written in standard C which enables any programmer to modify the code without a lot of knowledge about hardware. Custom memory chips can also be added to the firmware in this way. Beside reading flash memory chips, the SEC Xtractor has integrated JTAG-bruteforce functionality with configurable pin count. UART transmit pins can be found with a passive UART identifier module. Another capability of the SEC Xtractor is the directly available FT2232H module that enables the device to use OpenOCD and two serial ports out of the box, also with configurable voltage levels.

1.2 Functional Description

This tool can be used as

- memory chip reader (I2C, SPI, NAND, NOR)
- interface identification gadget (JTAG, UART)
- power supply (5V, 2.7V, 1.8-5.3V)
- UART to USB bridge
- JTAG adapter with OpenOCD

The integrated protection circuit of the level shifters (up to +/-8kV) is the reason why no external diodes were used in the schematics. All commands that can be issued to the integrated SEC Xtractor shell can be sent by using the following UART serial port settings:

- Serial Port: Two serial ports will appear when the device is attached. Take the first port *(mostly ttyUSB0)*.
- Baudrate: 4 MBaud
- Configuration: No flow control, no parity bit, 8 data bit, one stop bit

1.2.1 Memory Reader

The SEC Xtractor can read I2C memory chips by using libmpsse. SPI memory chips can be read by using the `flashrom` project. The ATXmega128A1U is not needed for I2C and SPI.

NAND and NOR memory chips can be read by using the ATXmega128A1U microcontroller. Both actions can be done directly over the tools command line.

1.2.2 Interfaces

A JTAG brute forcer was implemented on a modified version of JTAGenum, originally written by cyphunk aka Nathan Andrew Fain *(see https://deadhacker.com/2010/02/03/jtag-enumeration/)*. To find UART interfaces, another piece of software was implemented with interrupts. This UART scanner detects such interfaces in a passive way by just listening on the specified pins. An RS485 transceiver can be used in a DIL socket for communicating with bus devices. The MAX3471 transceiver is recommended for this purpose. All other pins are protected by the internal diodes of the TXS0108EQ-Q1 level shifters. They are used to shift the IO voltage levels of the ATXmega128A1U microcontroller from 1.8V to 5.3V and the voltage levels of the FT2232H microcontroller from 1.8V to 3.3V.

1.2.3 Power Supply

The board supplies 5.0V, 2.7V and adjustable voltage. The used darlington transistors can deliver several amperes *(depending on the specific model)* It is usually enough for 500mA devices without additional cooling of the transistors.

Note: The power supply is not protected from short circuits!

1.2.4 UART-to-USB

The FT2232H mini module can directly act as UART to USB converter on different voltage levels. This can be used for connecting to a shell of a target device.

1.2.5 JTAG Adapter

The FT2232H mini module can also directly act as hardware JTAG adapter by using the OpenOCD software on different voltage levels.

1.3 Board Revisions

1.3.1 Revision 1.0

Initial revision. Green soldermask.

1.3.2 Revision 1.20

The power supply of the FT2232H mini module and the overall system were merged. This resolved the power supply issues when plugging in the USB port before the power supply. Additional silk text was added to label the SPI pins for the FT2232H chip. Red soldermask.

1.3.3 Revision 1.31

A boot button and two crystals (32.768kHz and 16MHz) were added to the system. The system voltage level was changed from 3.3 volt to 2.7 volt. Black soldermask.

1.4 Schematics

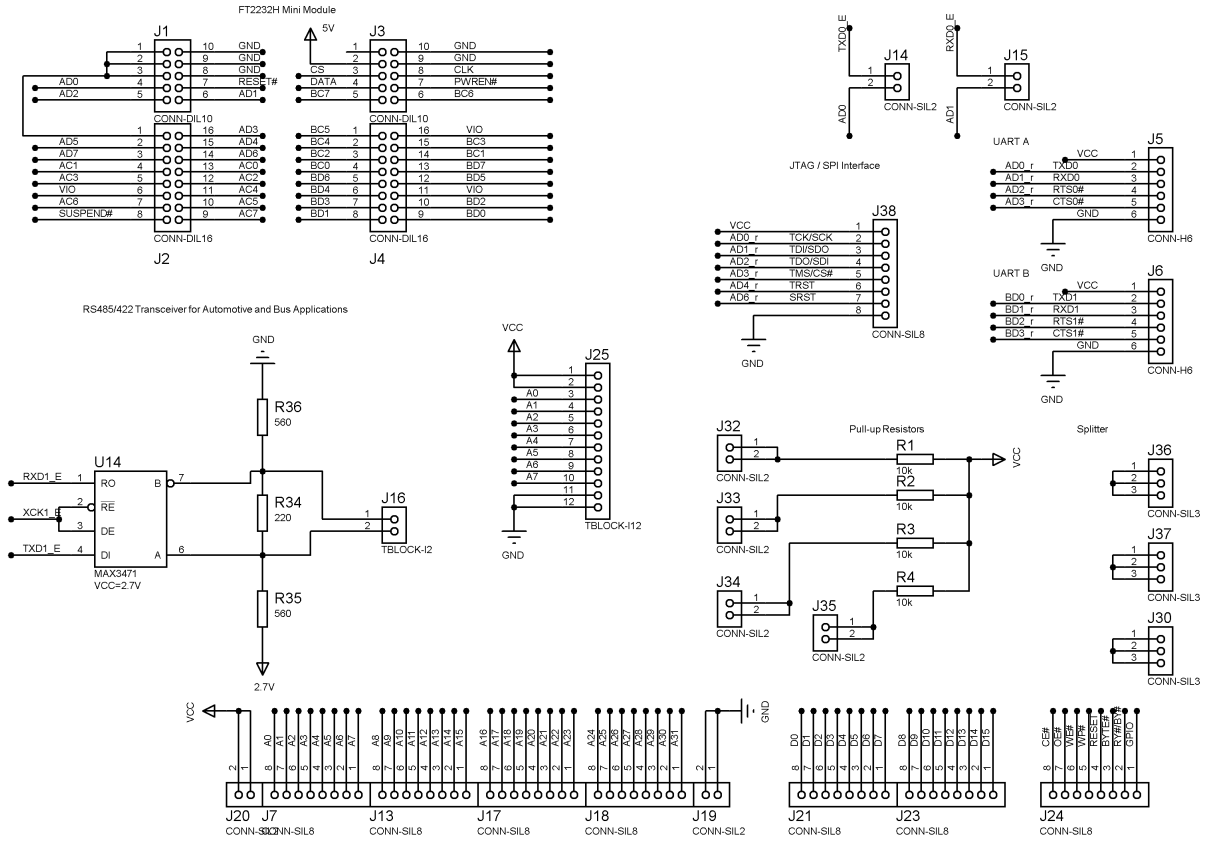

Figure 1.1: Schematics including the FT2232H mini module, the RS485 transceiver, connectors and pull-up resistors.

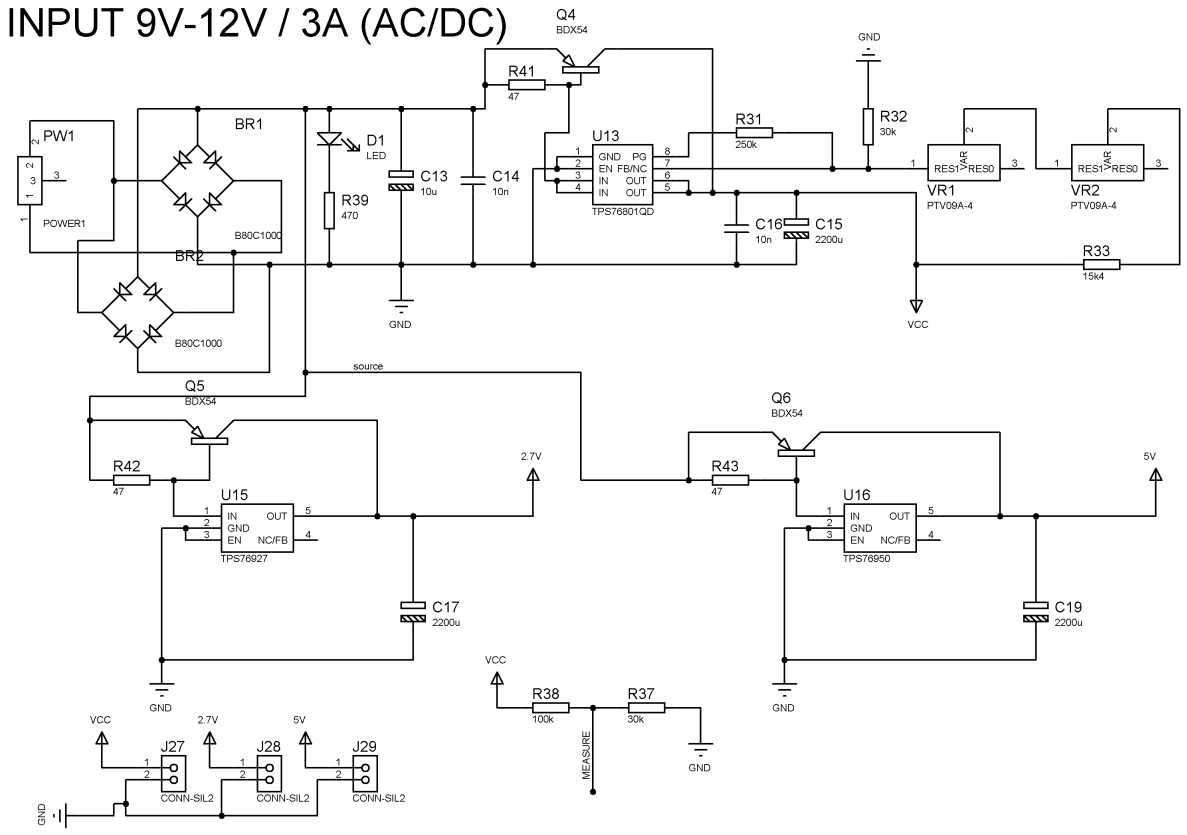

Figure 1.2: Power supply schematics of the whole board. The voltage divider for the analogue measurement is included.

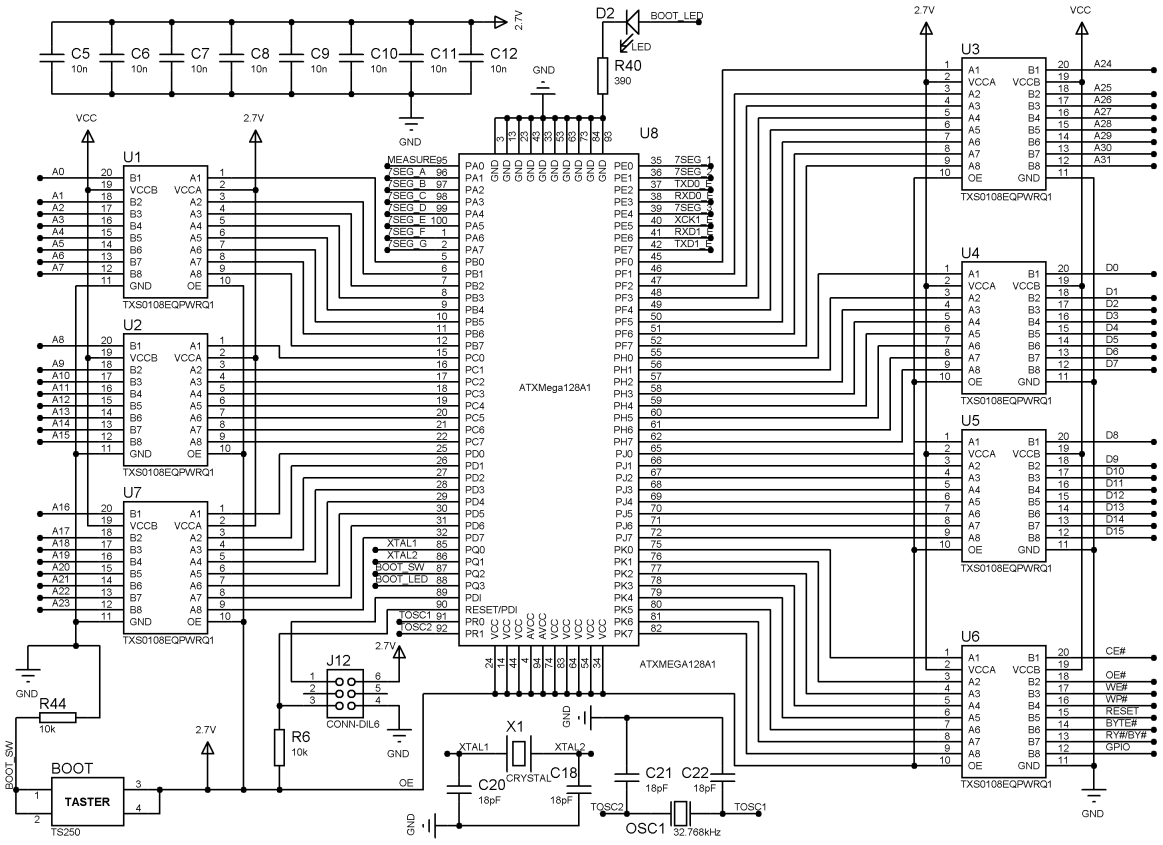

Figure 1.3: This schematic sheet includes the core of the tool. The main microcontroller including peripheral components like the level shifters are depicted here.

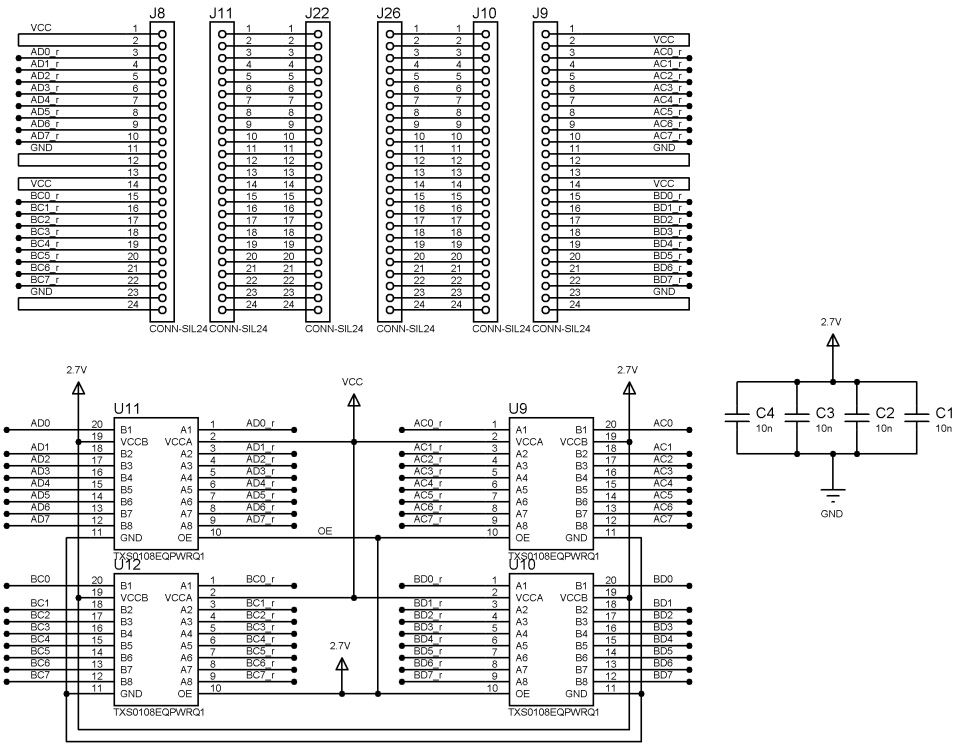

Figure 1.4: The ZIF adapter and level shifters are included on this schematic sheet.

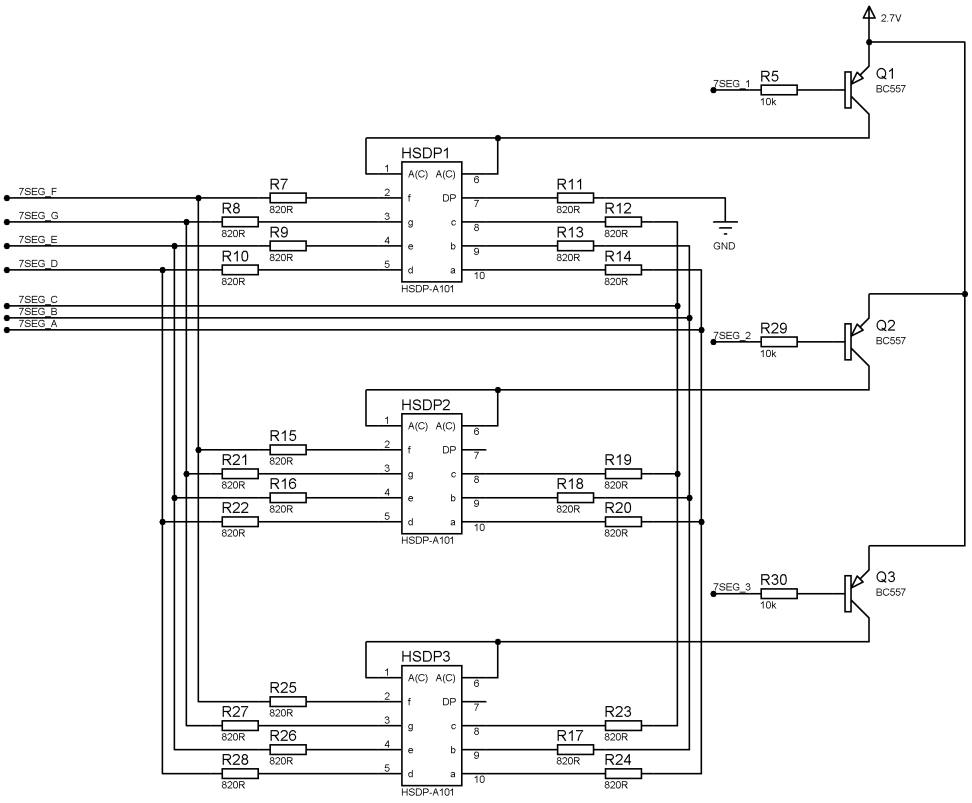

Figure 1.5: The seven-segment displays are included in this schematic sheet.

Chapter 2

Memory Reading

The usage of the SEC Xtractor for reading memory chips is explained in this chapter.

2.1 SPI

For reading SPI flash memory chips, the SEC Xtractors ZIF socket in the center of the PCB *(see Figure 2.1)* is intended to be used. By attaching an appropriate DIL adapter to the socket *(see Figure 2.2)*, a

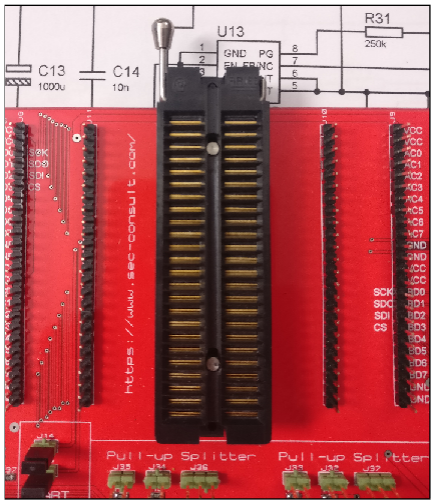

Figure 2.1: ZIF socket in the center of the SEC Xtractor tool.

broad range of SMD chips can be read. It is important to open the UART bridge of the ATXmega128A1U when reading from channel A of the FT2232H chip as both ICs would be attached at the same time in this case. This can result in interferences which disrupts the communication. Channel B can be used without any jumper changes. The project `flashrom` *(see https://flashrom.org/)* can be used to dump SPI memory chips. Because of the propagation delay, that comes form the level shifters, a clock divisor

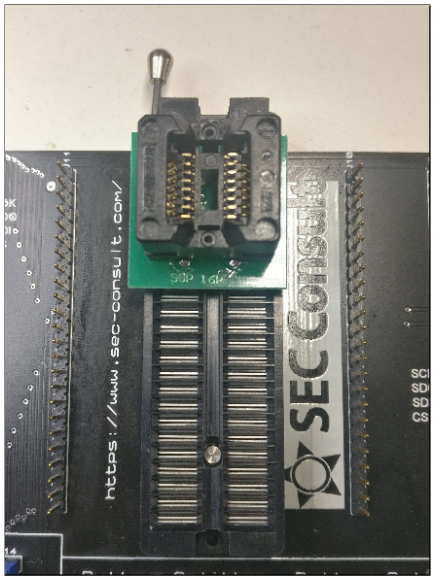

Figure 2.2: Mounted DIL adapter for SOP16 packages.

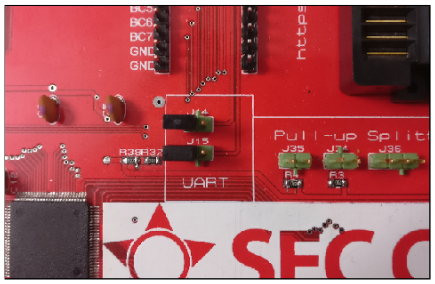

Figure 2.3: UART jumper bridge to the ATXmega128A1U.

for the read and write command should be used. A normal read operation can be started by issuing the following command:

```
flashrom -p ft2232_spi:type=2232H,port=A,divisor=10 -r dump.bin
```

To connect a SPI memory chip for reading purpose, the circuitry depicted in Figure 2.4 can be used. To create this circuit on the SEC Xtractor board, connection wires like on prototyping boards can be used.

2.2 I2C

For reading I2C flash memory chips, the SEC Xtractors ZIF socket in the center of the PCB *(see 2.1)* is intended to be used *(like for SPI)*. The implication for the UART bridge, described in the previous section, is the same. Therefore, it should be opened. To read I2C memory chips, `libmpsse` can be used.

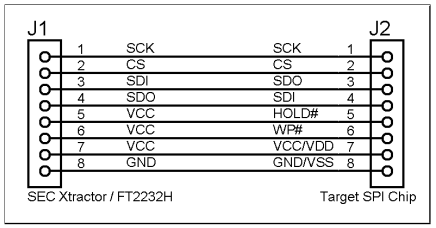

Figure 2.4: SPI flash memory connection circuit.

Repositories are available under the following links:

https://www.ftdichip.com/Support/SoftwareExamples/MPSSE/LibMPSSE-I2C.htm

https://github.com/devttys0/libmpsse

To connect an I2C memory for reading purpose, the circuitry depicted in Figure 2.5 can be used. The depicted circuit is more complex than the SPI circuit in the previous section. It can be created

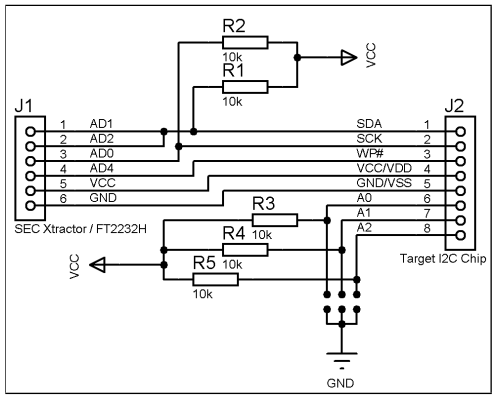

Figure 2.5: I2C flash memory connection circuit.

with prototyping wires too, but this time the ‘‘`pull-up splitter`’’ resistors and connectors on the SEC Xtractor *(see Figure 2.1)* must be used. The address pins A0-A2 can be configured to fit to the corresponding application that reads the memory content.

2.3 NOR

For reading NOR flash memory chips, the SEC Xtractor's socket adapter can be used. It is located on the edge where the ATXmega128A1U resides *(see Figure 2.6)*. The pins marked with `A0-A31` are the address pins, the pins marked with `D0-D15` are the data pins. The remaining pins like `CE#` or `RESET` are control pins. Therefore, a maximum of 32 address bits and 16 data bits can be handled which is equal to a maximum of 68719476736 bits or 8589934592 bytes memory size.

For this purpose, the UART bridge on the board must be closed *(see Figure 2.3)*. The command "dump nor" can be used to read out NOR flash memory content. The resulting output must be converted with "xxd -r" to a readable binary file.

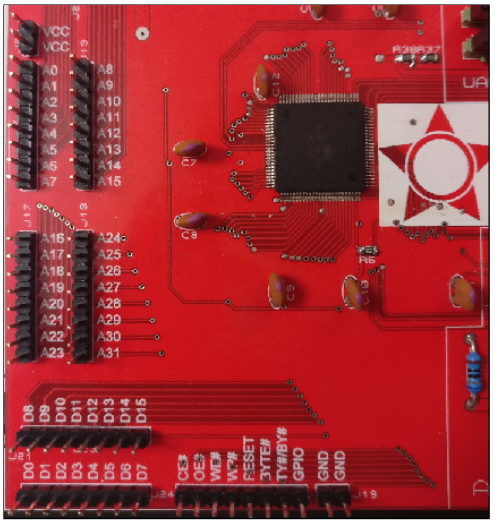

Figure 2.6: Pins that can be used for NOR and NAND flash memory chips.

The additional adapter for NOR flash memory chips is depicted in Figure 2.7. An example how it can be mounted is depicted on Figure 2.8. A standard Xeltex SA247 TSOP-48 adapter was mounted directly with the corresponding memory chip.

2.4 NAND

Reading NAND flash memory chips can be done with the same hardware interface *(see Figure 2.9)* in a similar way like NOR flash memory chips, explained in the previous section. A significant difference is the fact that the NAND interface, called ONFI, sends address and data commands on the same wires. The pins marked with `D0-D15` are used for this purpose while the control pins on the SEC Xtractor are the same. Reading out NAND memory chips can be done with the command "dump nand" *(see Figure 2.10)*. The resulting output must be converted with "xxd -r" to a readable binary file, as mentioned for NOR in the last section.

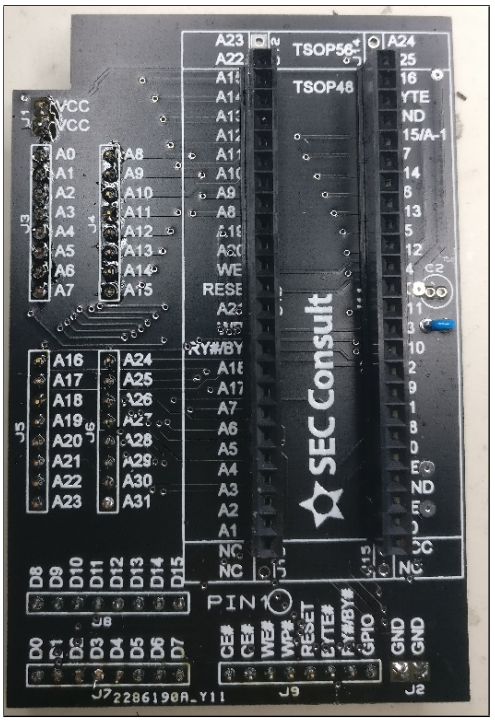

Figure 2.7: Adapter PCB to use NOR flash memory chips with a DIL socket.

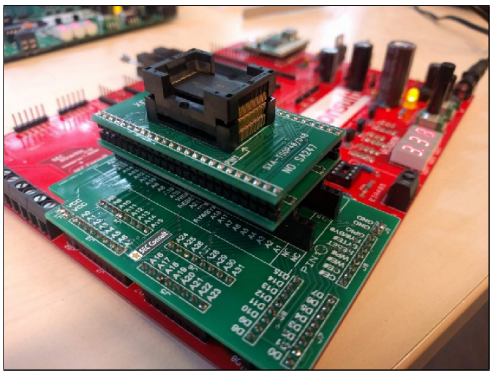

Figure 2.8: Mounted NOR flash memory adapter with ZIF socket.

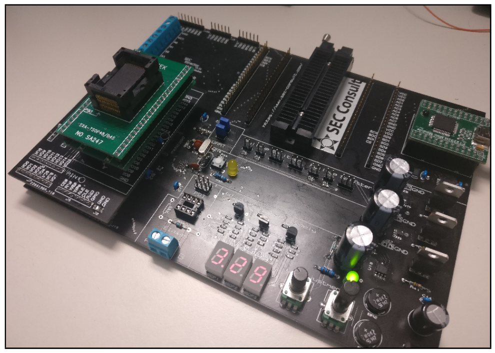

Figure 2.9: Mounted NAND adapter on the SEC Xtractor.

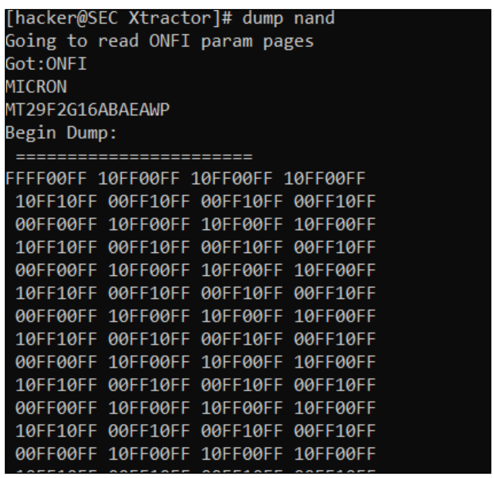

Figure 2.10: Terminal output during read operation.

Chapter 3

Interface Identification

The interface identification functionalities are covered in this chapter. A general command that can be issued on the SEC Xtractor shell for configuring the pin count is “pinlen set”. Setting the pin count of 16 for example will activate the pins “A0”-“A15”.

3.1 JTAG Identification

JTAG can be found by connecting the corresponding wires to the target device and type “pattern scan”, like implemented in JTAGenum.

3.2 UART Detection

The passive UART scan can be started by issuing the command “uart scan” in the console. It counts the pin changes and let you determine where UART TX pins may be located.

Chapter 4

Firmware Development

4.1 Program the Device

There are two ways to program the SEC Xtractor's flash memory. The first is the classic way via the PDI port, the second way is the bootloader over the serial port.

The PDI socket can be used with all fitting AVR programmers. The AVRISPMKII is set as programmer in the Makefile. This must be changed when another programmer is used.

The bootloader mode can be initialized when the button "BOOT" is pressed on the PCB down during power-up and programming. The bootloader can handle input from avrdude when the programmer "avr911" is set in the Makefile. This is the case when the command "make flash-main-serial" is issued.