Technical University of Košice
Faculty of Electrical Engineering and Informatics

Development tools for evaluation of cryptographic primitives implemented in reconfigurable hardware

Master's Thesis

2016 Marek Laban

Technical University of Košice
Faculty of Electrical Engineering and Informatics

Development tools for evaluation of cryptographic primitives implemented in reconfigurable hardware

Master's Thesis

Study Programme:	Smart Electronics
Field of study:	5.2.13 Electronics
Department:	Department of Electronics and Multimedia Communications (KEMT)
Supervisor:	Ing. Michal Varchola PhD.
Consultant:	doc. Ing. Miloš Drutarovský, CSc.

Košice 2016 **Marek Laban**

Errata

Development tools for evaluation of cryptographic primitives implemented in reconfigurable hardware

Marek Laban

Košice 2016

Abstract

This master thesis describes the software and hardware design of a platform designed for the HECTOR project. The platform consists of a mother board and daughter modules, which constitute a modular system. It is aimed at testing and evaluation of cryptographic primitives like true random number generators (TRNGs) or physical unclonable functions (PUFs) across different FPGA and ASIC families. Software is optimized for evaluation of TRNGs. It allows to collect data from random number generator located in the daughter module and read it using a USB interface. At the end of master thesis, the author demonstrates the use of the designed platform on a suitable case study - design and implementation of a TRNG.

Keywords

HECTOR, FPGA, evaluation platform, true random number generator

Abstrakt

Diplomová práca opisuje návrh softvérovej a hardvérovej platformy určenej pre projekt HECTOR. Platforma pozostáva z materskej dosky a dcérskych modulov, ktoré tvoria modulárny systém. Tá je zameraná na testovanie a vyhodnocovanie kryptografických primitívov akými sú skutočné generátory náhodných čísel (TRNGs) alebo fyzicky neklonovateľné funkcie (PUFs) naprieč rôznymi rodinami FPGA a ASIC obvodov. Navrhnutý softvér je optimalizovaný pre vyhodnocovanie TRNGs. Umožňuje zber dát z TRNG umiestneného v dcérskom module a nazbierané dáta vyčítať prostredníctvom USB rozhrania. V závere práce autor demonštruje využitie navrhnutej platformy implementáciou TRNG.

Kľúčové slová

HECTOR, FPGA, vyhodnocovacia platforma, generátor skutočne náhodných čísel

TECHNICAL UNIVERSITY OF KOŠICE

FACULTY OF ELECTRICAL ENGINEERING AND INFORMATICS

Department of Electronics and Multimedia Communications

DIPLOMA THESIS ASSIGNMENT

Field of study: **5.2.13 Electronics**

Study programme: **Smart Electronics**

Thesis title:

Development tools for evaluation of cryptographic primitives implemented in reconfigurable hardware

Vývojové nástroje pre testovanie kryptografických primitívov implementovaných v rekonfigurovateľnom hardvéri

Student: **Bc. Marek Laban**

Supervisor:	**Ing. Michal Varchola, PhD.**
Supervising department:	**Department of Electronics and Multimedia Communications**
Consultant:	**doc. Ing. Miloš Drutarovský, CSc.**
Consultant`s affiliation:	**Department of Electronics and Multimedia Communications**

Thesis preparation instructions:

Design and implement modular hardware platform and associated software tools aimed at testing of cryptographic primitives implemented in various target FPGA devices to be used within the H2020 HECTOR project.
The implemented reconfigurable hardware platform must support connection to the PC computer via fast communication USB interface. The software tools must demonstrate all the relevant features of the implemented hardware platform. As a target cryptographic primitive, use a secured TRNG design and evaluate its robustness in various environmental conditions (Vcc, ambient temperature, etc.). The hardware must be designed using the Altium Designer CAE software.
The final documentation of the hardware design must contain complete documentation needed for the industrial production of the hardware, including printed circuit board. The hardware Intellectual Property (IP) functions must be written in VHDL and simulated in the Modelsim CAE environment.

Language of the thesis: English

Thesis submission deadline: 29.04.2016

Assigned on: 31.10.2015

.....
prof. Ing. Jozef Juhár, CSc.
Head of the Department

TECHNICKÁ UNIVERZITA V KOŠICIACH FAKULTA ELEKTROTECHNIKY A INFORMATIKY -10-

.....
prof. Ing. Liberios Vokorokos, PhD.
Dean of the Faculty

Declaration

I hereby declare that this thesis is my own work and effort. Where other sources of information have been used, they have been acknowledged.

Košice, April 29, 2016 .....

Signature

Acknowledgement

I wish to express my sincere thanks to Michal Varchola, PhD. the main supervisor, who helped me much with his valuable skills and expertise. I would also like to thank Ladislav Cechlár, Ladislav Tóth, Peter Husnaj and Marcel Kleja from Micronic a.s. for their guidance and support. I thank also remaining colleagues from this company for their help.

My sincere thanks also go to prof. Viktor Fischer and Oto Peťura for offering me the internship, leading my work there and their thesis review. Special mention should go to assoc. prof. Miloš Drutarovský, for his constant, and constructive guidance and help throughout the study. To all other who gave me a hand, I say thank you very much.

This work was performed in the framework of the HECTOR research project, which is founded by the European Union under grant agreement number 644052.

Contents

Introduction **1**

1 Cryptography and randomness **3**

1.1 Random number generators 3

1.2 Physically unclonable functions 4

1.3 Hardware dependence of TRNGs and PUFs 5

1.4 HECTOR project 5

2 HECTOR evaluation platform **6**

2.1 Evaluation platform specifications 6

2.2 Required cryptographic primitives 7

2.3 Objectives of the diploma thesis 8

3 Hardware design **9**

3.1 SmartFusion 2 10

3.1.1 Device programming 10

3.1.2 System reset 11

3.1.3 Clocking of the device 11

3.1.4 SF2 banks voltage 12

3.2 Motherboard power supply 12

3.2.1 Filtering 13

3.2.2 Power protection 14

3.2.3 Side channel measurements 14

3.2.4 Daughter boards power management 15

3.3 SD cards 18

3.4 External RAM 19

3.5 USB connection 19

3.5.1 FTDI RS232RL drivers 20

3.6 Daughter boards connection 21

3.6.1 SATA connector 21
3.6.2 HDMI connector 22
3.6.3 ZIF connector 23
3.7 Manufacturing of the printed circuit printed boards 24
3.7.1 Motherboard releases notes 25
3.8 Daughter board featuring SmartFusion 2 device 26
3.9 Daughter board featuring the Spartan 6 device 28

4 Design of the software tools and functions 30
4.1 Motherboard software requirements 30
4.2 PC application requirements 32
4.3 Data acquisition from a TRNG 32
4.3.1 UART packets 34
4.3.2 MSS instructions 36
4.3.3 RAM and USB mass storage 38
4.3.4 MSS - FPGA interface 38
4.3.5 External RAM write interface 39
4.3.6 Serial to parallel converter 40
4.3.7 Control block implementation 41
4.3.8 Testing 42
4.3.9 Host PC software for TRNG data acquisition 42
4.4 Software tools for development of hardware and software embedded system 43

5 Evaluation of PLL-Based TRNG 45
5.1 Design and principle 45
5.2 Testing and results 46

6 Conclusion 49

Bibliography 50

Appendices **56**

Appendix A **57**

Appendix B **58**

List of Figures

2 - 1 Block diagram of required daughter board connections 7
2 - 2 Flow chart of description in following sections 8
3 - 1 Hardware design block diagram 9
3 - 2 System Reset Interface 11
3 - 3 Motherboard power line block diagram 13
3 - 4 Motherboard power protection 14
3 - 5 Schematic of SmartFusion 2 SoC CORE side channel measurement connection 15
3 - 6 Replaceable resistor between SMA connectors 15
3 - 7 Daughter boards power supply block diagram 16
3 - 8 XK5 and XK2 jumper position 16
3 - 9 XK6 jumper position - set to ADJ1 16
3 - 10 SATA connector dedicated to the daughter board connection 17
3 - 11 USB devices block diagram 20
3 - 12 Motherboard description 24
3 - 13 Description of the daughter board featuring the SmartFusion 2 device 26
3 - 14 Daughter board Spartan 6 description 28
3 - 15 Daughter board Spartan 6 programming reduction 29
4 - 1 Motherboard software design block diagram 31
4 - 2 Design of TRNG acquisition system 33
4 - 3 Functional diagram of MSS packet manipulation 34
4 - 4 Format of the command packet 35
4 - 5 Format of the status packet 36
4 - 6 Format of read data packet 36
4 - 7 External RAM write interface (AHB Fabric Master) 39
4 - 8 S/P converter data output (32-bit words) 40
4 - 9 Serial to parallel converter 41

4 - 10 Shifting of a 32-bit word 42
5 - 1 Principle of Phase-locked loop-based TRNG [38] 46
5 - 2 Connection of the evaluation platform during testing 48
6 - 1 Schematic of mother board page 1/10 59
6 - 2 Schematic of mother board page 2/10 60
6 - 3 Schematic of mother board page 3/10 61
6 - 4 Schematic of mother board page 4/10 62
6 - 5 Schematic of mother board page 5/10 63
6 - 6 Schematic of mother board page 6/10 64
6 - 7 Schematic of mother board page 7/10 65
6 - 8 Schematic of mother board page 8/10 66
6 - 9 Schematic of mother board page 9/10 67
6 - 10 Schematic of mother board page 10/10 68
6 - 11 Mother board final artwork prints - 1. Top layer 69
6 - 12 Mother board final artwork prints - 2. Signal layer 70
6 - 13 Mother board final artwork prints - 3. GND layer 71
6 - 14 Mother board final artwork prints - 4. VCC layer 72
6 - 15 Mother board final artwork prints - 5. Signal layer 73
6 - 16 Mother board final artwork prints - 5. Signal layer 74
6 - 17 Mother board composite drawing - Top layer 75
6 - 18 Mother board composite drawing - Bottom layer 76
6 - 19 Schematic of daughter board SF2 page 1/4 77
6 - 20 Schematic of daughter board SF2 page 2/4 78
6 - 21 Schematic of daughter board SF2 page 3/4 79
6 - 22 Schematic of daughter board SF2 page 4/4 80
6 - 23 Daughter board SF2 final artwork prints - 1. Top layer 81
6 - 24 Daughter board SF2 final artwork prints - 2. GND layer 81
6 - 25 Daughter board SF2 artwork prints - 3. VCC layer 82
6 - 26 Daughter board SF2 artwork prints - 4. Bottom layer 82

6 - 27 Daughter board SF2 composite drawing - Top layer 83
6 - 28 Daughter board SF2 composite drawing - Bottom layer 84
6 - 29 Schematic of daughter board S6 page 1/3 85
6 - 30 Schematic of daughter board S6 page 2/3 86
6 - 31 Schematic of daughter board S6 page 3/3 87
6 - 32 Daughter board S6 final artwork prints - 1. Top layer 88
6 - 33 Daughter board S6 final artwork prints - 2. GND layer 88
6 - 34 Daughter board S6 artwork prints - 3. VCC layer 89
6 - 35 Daughter board S6 artwork prints - 4. Bottom layer 89
6 - 36 Daughter board S6 composite drawing - Top layer 90
6 - 37 Daughter board S6 composite drawing - Bottom layer 91

List of Tables

3 – 1 Used SmartFusion 2 IO bank supplies 12
3 – 2 U22 regulator options configured by the SW1 switch 17
3 – 3 U18 (U19) regulators option configured by the SW3 (SW2) switch . . 17
3 – 4 ZIF connector power supply pins 18
3 – 5 SmartFusion 2 - SD cards pinout 18
3 – 6 SmartFusion 2 pins connected to SATA connector. 22
3 – 7 SmartFusion 2 pins connected to HDMI connector. 22
3 – 8 Motherboard ZIF connector pinout 23
3 – 9 Motherboard ZIF connector pinout 27
3 – 10 Daughter board SmartFusion 2 pinout 27
3 – 11 Daughter board SmartFusion 2 - SATA connector power supply . . . 27
3 – 12 DBS6 common pins used 29
3 – 13 Daughter board Spartan 6 - SATA connector power supply 29
3 – 14 Daughter board Spartan 6 pinout 29
5 – 1 AIS-31 tests during under-voltage of FPGA core (P - passed, F - failed) 47
5 – 2 AIS-31 tests during under-voltage of PLL power (P - passed, F - failed) 48

List of Symbols and Abbreviations

ASIC **A**pplication-**S**pecific **I**ntegrated **C**ircuit

BFM **B**us **F**unctional **M**odel

BGA **B**all **G**rid **A**rray - a type of surface-mount packaging

CCC **C**lock **C**ondtitional **C**ircuitry

DB **D**aughter **B**oard

DDR **D**ouble **D**ata **R**ate

DFF **D** **F**lip **F**lop

DMA **D**irect **M**emory **A**ccess

DSP **D**igital **S**ignal **P**rocessing

EMI **E**lectro**m**agnetic **I**nterference

eNVM **E**mbedded **N**on**v**olatile **M**emory

FIFO **F**irst **I**n **F**irst **O**ut - typically register

FPGA **F**ield **P**rogrammable **G**ate **A**rray

HDMI **H**igh-**D**efinition **M**ultimedia **I**nterface

HECTOR **H**ardware **E**nabled **C**rypt**o** and **R**andomness

HMB **H**ECTOR **M**other**b**oard

IDE **I**ntegrated **D**evelopment **E**nvironment

IO **I**nput **O**utput pin

JTAG **J**oint **T**est **A**ction **G**roup

LPDDR **L**ow **P**ower **D**ouble **D**ata **R**ate

LUT **L**ook **U**p **T**able

MMCX **M**icro **M**iniature **C**oa**x**ial

MSS **M**icrocontroller **S**ubsystem

OTG **O**n-**T**he-**G**o

PC **P**ersonal **C**omputer

PCB **P**rinted **C**ircuit **B**oards

PLL **P**hase **L**locked **L**oop

PRNG **P**seudo **R**andom **N**umber **G**enerator

PUF **P**hysically **U**nclonable **F**unction

RAM **R**andom **A**ccess **M**emory

RNG **R**andom **N**umber **G**enerator

SATA **S**erial **ATA**

SD **S**ecure **D**igital

SF2 **S**mart**F**usion2

SMA **S**ub**M**iniature version **A**

SoC **S**ystem **o**n **C**hip

SRAM **S**tatic **R**andom **A**ccess **M**emmory

TRNG **T**rue **R**andom **N**umber **G**enerator

UART **U**niversal **A**synchronous **R**eceiver **T**ransmitter

USB **U**niversal **S**erial **B**us

VCP **V**irtual **C**OM **P**ort

ZIF **Z**ero **I**nsertion **F**orce

Introduction

Nowadays, we live in an information society where almost everyone works with information in a digital form. Electronic mail is used more often than traditional mail, documents are stored in a digital form more than in a paper form and information is often very expensive. Therefore, cryptography has become increasingly used to ensure data security.

In the framework of the information security of the European union, a project called HECTOR was recently accepted for funding. The main motivation of this project is to bridge basic algorithmic approaches with hardware-level security implementations. It requires to evaluate many hardware dependent cryptographic primitives, therefore there is a need to have a flexible platform for testing and evaluation of primitives implemented on various Field Programmable Gate Array (FPGA) and Application-Specific Integrated Circuit (ASIC) devices.

This thesis describes such an evaluation platform, which was designed according to the HECTOR project requirements. The thesis describes complete hardware and software design of the platform. All the hardware was designed in cooperation with Micronic a.s., Trebejov, Slovakia. The software part of the evaluation platform was developed as a part of my research stay in the Hubert Curien Laboratory, Saint-Etienne, France.

The first chapter introduces cryptography and describes cryptographic terms used in the thesis. It also describes the aims of HECTOR project in the context of the cryptography needs.

The next chapter describes requirements on the hardware and software of the evaluation boards within the HECTOR project requirements and main objectives of this master thesis.

The third chapter describes the hardware design of the mother board and two daughter boards. It also points to various issues during the design and explains their solutions.

The fourth chapter describes software requirements and the ways of using the evaluation platform. It also describes the software template designed for the true random number generator (TRNG) evaluation.

The last chapter demonstrates implementation of the TRNG using the proposal evaluation platform.

1 Cryptography and randomness

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [1]. It uses cryptographic primitives to build cryptographic protocols. Examples of cryptographic primitives are:

- block ciphers using symmetric or asymmetric key,
- stream ciphers,
- random number generators (RNGs),
- physical unclonable functions (PUFs),
- one way functions,
- hash functions,
- signatures and identifications primitives,

1.1 Random number generators

Random numbers are very important for cryptographic and information security applications. Random numbers in cryptographic algorithms are used for example in [2]:

- RSA algorithm keys generation,
- DSA based digital signatures,
- session keys generation in symmetric encryption/decryption schemes,
- identifiers used for authentication in key distribution algorithms.

Random number generators (RNGs) generate sequences of random numbers. These sequences have to fulfil two fundamental requirements: randomness and unpredictability. RNGs can be classified in two categories:

- deterministic RNGs,
- non-deterministic RNGs.

Deterministic RNGs use a mathematical function and internal generator state to generate sequence of random numbers.

The number of generator states is finite and periodically repeated with very big period. Therefore, the generated sequence is not random but pseudo-random and thus the generator which produces this sequence is called pseudo-random number generator (PRNG). Advantages of these generators are their high speed and good statistical properties of the output sequences. Disadvantage is their predictability.

Non-deterministic generators are called true random number generators (TRNG). They use various physical phenomena like quantum mechanics, radioactive decay or thermal and semiconductor noise to generate random numbers [3]. TRNGs are slower than PRNGs but the output is unpredictable.

1.2 Physically unclonable functions

Physical Unclonable Functions (PUFs) are defined as functions based on physical characteristics which are unique for each chip, difficult to predict, easy to evaluate and reliable [4]. It can not be replicated, even if the full design is known [5]. It can be described as a hardware version of a hash function. When it is implemented in a challenge - response method, it may be referred to as a physical one-way hash function. The usage of PUF reduces attackers' ability to intrude a secured system.

1.3 Hardware dependence of TRNGs and PUFs

Both TRNGs and PUFs depend significantly on the underlying hardware. TRNGs use dynamic random process like electric noises to generate random numbers. PUFs use random phenomena appearing during manufacturing process of logic devices. Both TRNGs and PUFs are impacted by surrounding hardware, which must be designed very carefully. This is one of the main constrains of my thesis.

1.4 HECTOR project

HECTOR (**H**ardware **E**nabled **C**rypt**o** and **R**andomness) is a European cooperative research project. The main motivation of this project is to close the gap between basic algorithmic approaches and hardware-level security implementations [8]. It requires integrating secure cryptographic primitives like RNGs and PUFs together. The goal is to study, design and implement RNGs and PUFs with demonstrable entropy guarantees and quality metrics. This includes on-the-fly entropy testing and physical attacks evaluations, which will enable more secure systems and easier certification.

HECTOR is a 3-year project, where 9 partners with cryptography and hardware experience cooperate. One of cooperating partners is Micronic, company oriented in development and production of data security products. One of the objectives of Micronic within the project is to design the HECTOR evaluation platform and demonstrator. The task of Micronic includes design and manufacturing of hardware and software tools designed for evaluation of HECTOR results. I worked in Micronic on the hardware design of the HECTOR evaluation board and on the design of the software template dedicated for the evaluation board.

2 HECTOR evaluation platform

The main requirement for the evaluation platform was to design hardware, which would be optimized for a comfortable evaluation of cryptographic primitives [7]. It should consist of a single motherboard and exchangeable daughter boards (modules) constituting a modular system.

The daughter modules should be designed to allow evaluation of primitives across different FPGA families, and ASICs. They should be as cheap and as simple as possible. It should be possible to connect the daughter board and motherboard via a cable to enable Faraday Cage testing but also by direct inserting the daughter board to the motherboard. It should be possible to connect the motherboard and the daughter board modules using a 32-wire interface testing of ASICs. The motherboard should have also USB interface to enable computer connection.

2.1 Evaluation platform specifications

The motherboard should be based on an existing Micronic product, universal cryptographic disk (UCD). The UCD will be also used as a HECTOR demonstrators later. That will be useful for easy migration from the HECTOR evaluation platform to demonstrators. Therefore, the motherboard should be based on the same Microsemi SmartFusion 2 FPGA SoC as the UCD. The USB connection should provide a Mass storage class interface and a virtual COM port (VCP), which should be supported in common operating systems like Windows or Linux. The mother board should have two SD card slots connected to the FPGA and one SD card slot connected to USB. It should provide external 64 - 128 MB DDR RAM to cache data. The power management of the boards should be based on linear, low noise regulators, to achieve better conditions for the side-channel analysis. The mother board should provide additional voltage regulators, which should reserved for daughter

board power management, to reduce their price.

Daughter modules should be connected using the Serial ATA (SATA) connector, to ensure easy, exchangeable and low noise connection (see Fig. 2 - 1). Daughter modules connected to the SATA connector on board should be provided by an optional aluminium lid to ensure board shielding. A HDMI cable could also be used to connect the daughter module with the motherboard at greater distances, where an adaptor from the HDMI to SATA format must be used. The adapter should contain the power management. The ASIC daughter modules should be connected using a DIP 40 socket to achieve their flexible interfacing. Both 2.5 V and 3.3 V I/O standards should be supported.

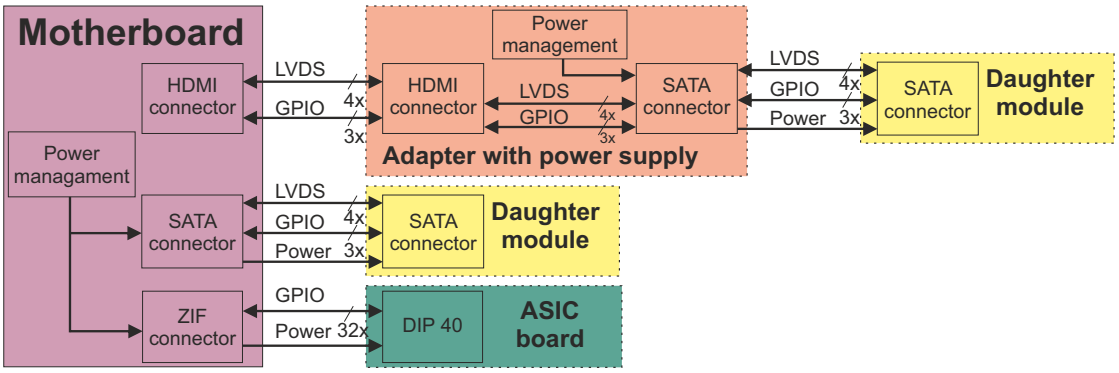

Figure 2 - 1 Block diagram of required daughter board connections

2.2 Required cryptographic primitives

The hector evaluation platform is aimed to evaluate following primitives:

- True Random Number Generator (TRNG),
- Physically Unclonable Function (PUF),
- Cipher for Authenticated Encryption (AE).

Appropriate software solution should be implemented in hardware to achieve their easy evaluation. Micronic is responsible for creating the template, which would enable their easier implementation in software.

2.3 Objectives of the diploma thesis

Development of the evaluation platform consists of numerous tasks, which can be grouped in three following objectives:

- Design of a modular hardware platform associated with the HECTOR project and addition of the appropriate documentation,
- Design of the appropriate software for the hardware platform on both host PC and embedded processor (ARM) side. This software must be suitable for evaluation of cryptographic primitives (mainly TRNGs).
- Evaluation of the TRNG design.

Process of the design is shown in Fig. 2 - 2. The individual steps of the design are detailed in the following sections.

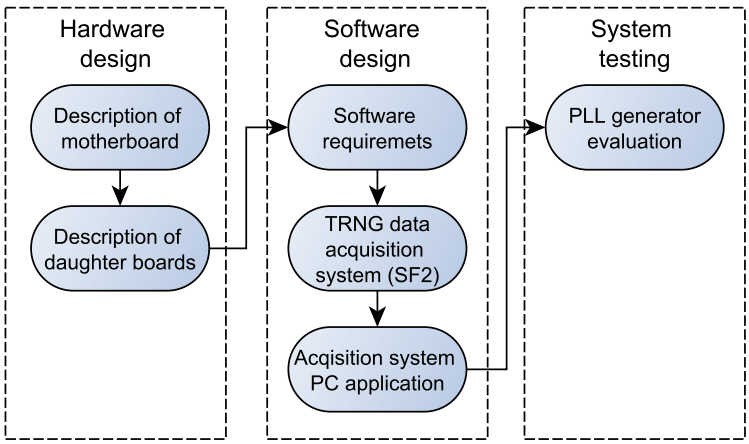

Figure 2 - 2 Flow chart of description in following sections

3 Hardware design

Hardware of the evaluation platform was designed according to the HECTOR project requirements (see section 2). The platform consists of a single motherboard (HMB) and exchangeable daughter board (DB) modules (Fig. 3 - 1).

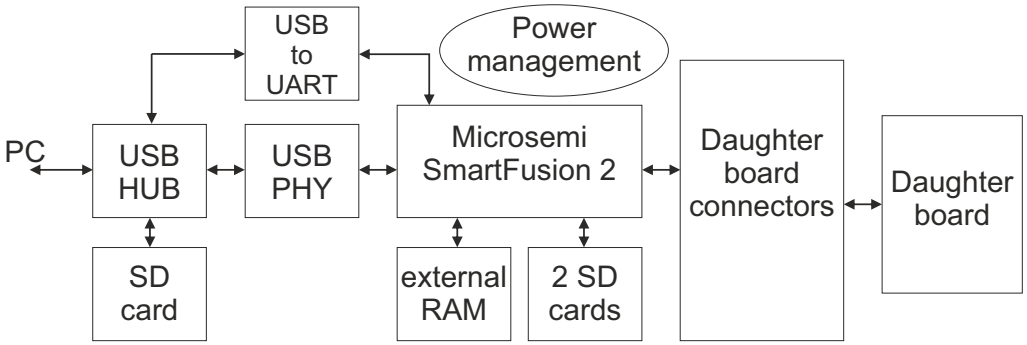

Figure 3 - 1 Hardware design block diagram

I designed a HMB (architecture and layout), which is based on Microsemi SmartFusion 2, with external 64 MB DDR RAM, 2xSD cards connected to the FPGA, as well as an SD card connected to USB hub. The HMB features the data and power supply interface for daughter boards and the communication interface between PC and HMB using USB interface. Special attention is required for power management distributed between DB and HMB, which must be low noise to easy side channel measurements. The HMB contains 3 connector types dedicated to daughter modules. Parts of block diagram shown below are detailed in the next subsections.

In addition to HMB, I designed two daughter boards based on Microsemi SmartFusion 2 and Xilinx Spartan 6 FPGAs. They are described in the last two chapters (see section 3.8 and section 3.9).

I used the Altium Designer [9] software to draw the schematic diagram and the board layout (Fig. 3 - 12). Schematics and printed circuit board (PCB) drawings are attached in appendix B. My design is mainly based on commercial examples,

datasheets and guidelines of electrical parts, but I used also the parts existing in the Micronic designs too.

3.1 SmartFusion 2

SmartFusion 2 (SF2) is a system on chip (SoC) FPGA, which integrates a flash-based FPGA fabric and a 166 MHz ARM Cortex-M3 processor .

The SmartFusion 2 M2S025 device features:

- 27696 logic elements (4 LUT + DFF),
- 34 math blocks, 6 PLLs, MSS (Microcontroller Sub-System) 166MHz,
- MSS 256 kB eNVM and 64 kB eSRAM,
- 267 total user I/O.

3.1.1 Device programming

The SmartFusion 2 can be programmed through the JTAG interface (XK2) by FlashPro programmer [10]. JP1 pin header supports JTAG controller selection, when jumper is:

- **installed** - it's the recommended setup for programming the fabric and for debugging of the microcontroller through the SoftConsole tool,
- **not installed** - it's the recommended setup for debugging of the microcontroller using tools like IAR or KEIL.

3.1.2 System reset

It is necessary to hold reset of the SF2, while sufficient power conditions are not reached. The user usually needs this option too to reset the internal firmware (see Fig. 3 - 2).

Therefore, the input reset pad (DEVRST_N) allows asserting a full reset to the chip at any time. The DEVRST_N signal (active low) is asserted in the following cases:

- when the SW6 button is pressed,
- when the power supply level 3.3 V falls below the threshold level (supervised by U9 - MIC803-29D3VM3TR [11]).

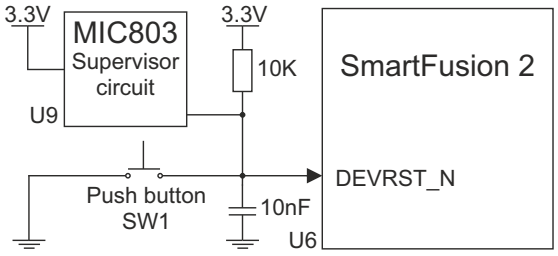

Figure 3 - 2 System Reset Interface

3.1.3 Clocking of the device

The SF2 device can be clocked by various means [12]. It contains 1 MHz and 50 MHz internal RC oscillators. The 12 MHz crystal with an accuracy of ±20 ppm is also connected to the SF2 to provide an additional system reference clock. An on-chip SF2 PLL can be configured to generate a wide range of high precision clock frequencies. Please note, that NE0 and SW1 PLL power source is not connected through an RC filter (due to lack of space). The filter is used to achieve a reasonable level of the long term jitter.

3.1.4 SF2 banks voltage

One of the FPGA circuit advantages is the availability of numerous IOs (input output pins). IO pins are usually associated to banks and every bank can be powered by various voltage values. Banks of SF2 use voltages shown in Tab. 3 – 1. PLLs are powered by 2.5 V. It is necessary to configure these values in the Libero project, otherwise some unexpected issues may occur during the long term using.

Table 3 – 1 Used SmartFusion 2 IO bank supplies

Bank number	0.	1.	2.	3.	4.	5.	6.	7.
Voltage [V]	1.8	2.5	3.3	3.3	2.5 / 3.3	-	2.5	3.3

3.2 Motherboard power supply

The board is powered by 5 V through a 2.5 mm power jack [13]. It is designed to consume the maximum current of 5 A. One of problems came from various amounts of currents consumed by FPGA depending on its configuration. Therefore, the board power consumption is a little bit overrated. If the FPGA is not configured, current consumption is around 250 mA. The power consumption is increased also by voltage regulators (Fig. 3 - 3), because the whole board use only linear regulators, which have very low efficiency. Linear regulators were used due their low noise compared to switch regulators, which have high power efficiency, but they are very noisy. Therefore linear regulators are suitable for side channel measurements. Regulators used on the board:

- LT1963 [14] to regulate 5 V to 3.3 V 2.5 V 1.8 V,
- LT3083 [15] to regulate 2.5 V to 1.2 V and 0.9 - 1.5 V,
- TPS7A7300 [16] to regulate 5 V to 0.9 - 3.5 V,
- TPS51200 [17] to regulate 1.8 V to 0.9 V (termination voltage).

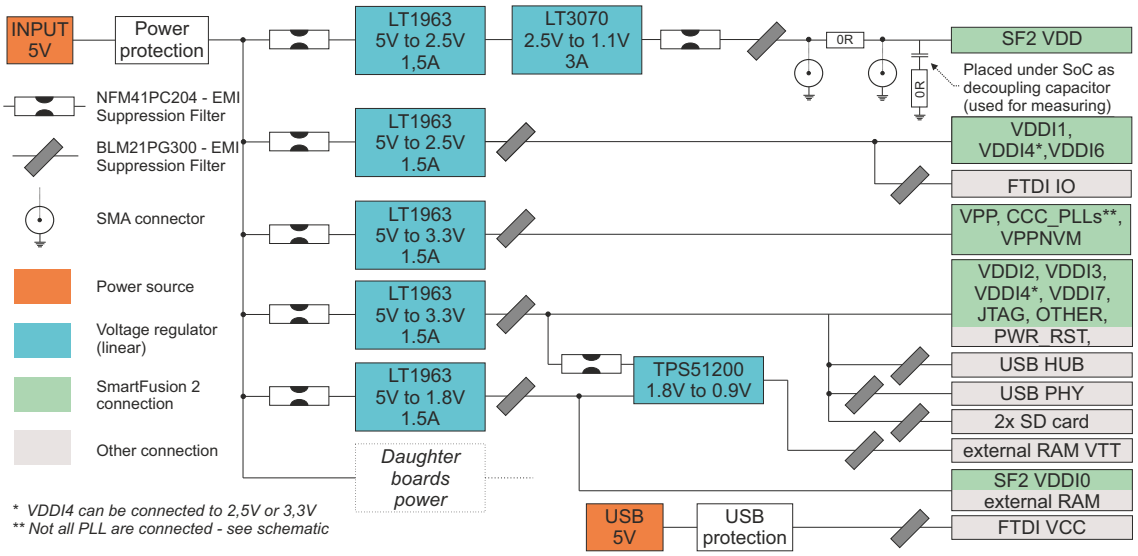

Figure 3 - 3 Motherboard power line block diagram

3.2.1 Filtering

Many digital circuits like PLL are very sensitive to noise in their power supply. Therefore it is necessary to properly filter the power supply. The power is filtered by two EMI filter types [18], which are mutually complementary. The first filter BLM21PG300 is a miniaturized ferrite bead useful for smaller noise radiation. Its impedance at 100 MHz is typ. 30 Ω. The second filter NFM41PC204 is a capacitor type filter, with great noise suppression effect, useful to reduce higher noise frequencies. Its capacitance is 0.2 μF. The NFM41PC204 is used before every input power line of the voltage regulator and the BLM21PG300 is used after the regulator output (except for the core regulators). The BLM21PG300 can be easily unsoldered to measure current of the power line.

Every connector shield is connected through a parallel combination of the 100 nF capacitor and the BLM21PG300 to ground. It is used to eliminate transferring of power through the shield.

3.2.2 Power protection

The motherboard is intended for laboratory using, where it could be powered accidentally by a wrong power supply. Therefore, protection controller [19] and a dual mosfet transistor [20] protect the board against undervoltage and overvoltage conditions ($\pm$ 30 V)(Fig. 3 - 4). A single blow fuse is used to the overcurrent protection to 7 A [21]. The fuse uses special technology, which does not damage the fuse permanently if an interrupt occurs.

We observed an issue, when the board was powered by a source with current less than approx. 1 A. The issue results in the activation of power protection followed by power supply disabling. The problem can be solved by using the power supply with sufficient current source.

If some protection controller problem occurs, it is possible to discard it using a schottky rectifier diode (D2) [22]. In this case, it is recommended to pick out dual mosfet transistor from the board.

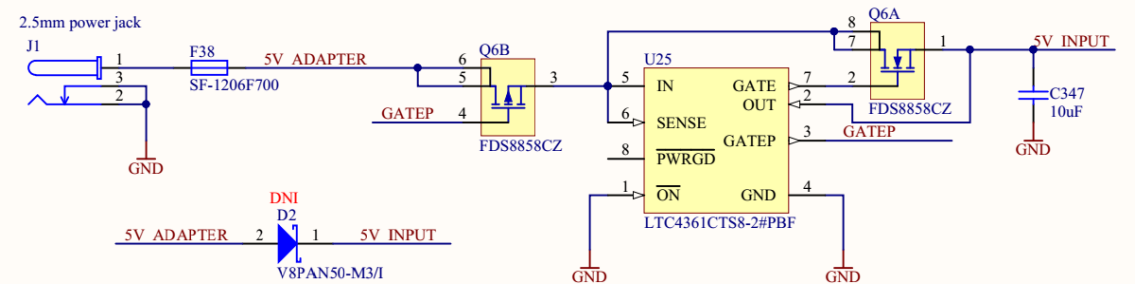

Figure 3 - 4 Motherboard power protection

3.2.3 Side channel measurements

Two SMA connectors (P1, P2) on the daughter board are designed to measure the power line of the SF2 core (Fig. 3 - 5). A resistors is placed between the SMA connectors (Fig. 3 - 6). Its value can be chosen as needed. A decoupling capacitor in

series with resistor is connected between the others decoupling capacitors of the SF2 to improve measurement results, by degrading parameters of the capacitor. They have a bigger form factor for easier replacement.

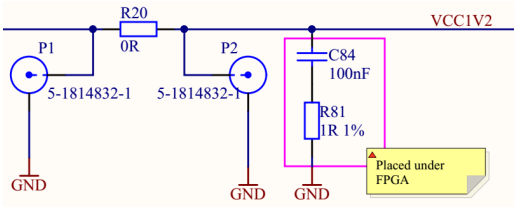

Figure 3 - 5 Schematic of SmartFusion 2 SoC CORE side channel measurement connection

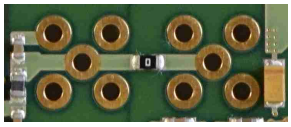

Figure 3 - 6 Replaceable resistor between SMA connectors

The SMA connector (P3) is designed for triggering purposes, needed in measurements. Alternatively, the board can be mounted by two 2.54 mm pin headers instead of SMA connector (one in the corner and one in the centre of the SMA connectors pad).

3.2.4 Daughter boards power management

Daughter boards are powered by the voltage regulators reserved to them on the motherboard. Three of them are user-configurable by micro switches. The configurable regulators were used to ensure compatibility across various daughter boards, which usually require various power supplies (e.g. the power voltage of the FPGA core may be different). The whole power supply is properly filtered to avoid any interference or noise (see Fig. 3 - 7).

Every power supply rail is lead out on pin headers (X2, X5, X6). It is designed to interrupt, measure or change the power supply of the DB. These pins can be alternatively used to test behaviour of the DB, depending on the power supply. It is necessary to properly jumper these pin headers, for using regulators on the HMB with the DB (see Fig. 3 - 8 and Fig. 3 - 9).

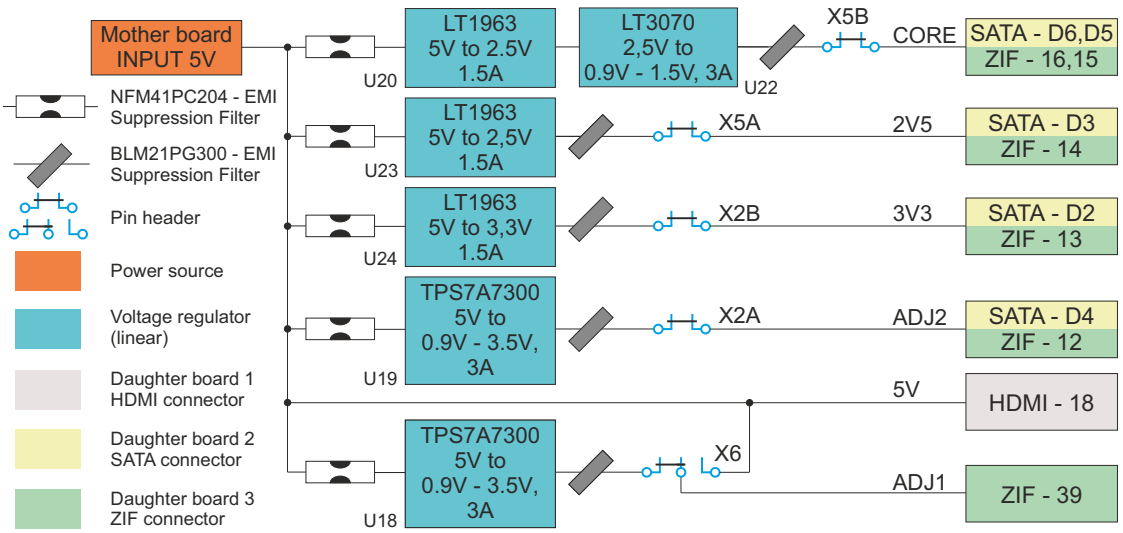

Figure 3 - 7 Daughter boards power supply block diagram

Regulator U22 is dedicated to common FPGA core voltages ranging from 0.9 V to 1.5 V. Regulator U20 is used to reduce power dissipation of U22, by reducing its input voltage. It is configured by switch SW1 and its configuration is shown in Tab. 3 – 2. Regulator U19 is configured by SW2 and regulator U18 by switch SW3. These regulators are the same and they can be configured to achieve voltages from 0.9 V to 1.5 V. Their common configurations are shown in Tab. 3 – 3. Detailed configurations can be find in datasheet [16]. Before board insertion, it is necessarily to verify the voltages on connector pins according to daughter boards requirements, because the board could be damaged permanently.

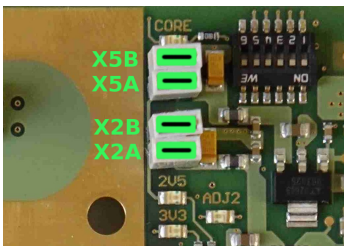

Figure 3 - 8 XK5 and XK2 jumper position

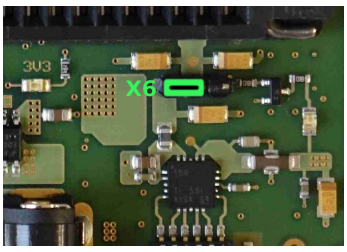

Figure 3 - 9 XK6 jumper position - set to ADJ1

Table 3 – 2 U22 regulator options configured by the SW1 switch

Switch options						
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**Voltage**
OFF	OFF	OFF	OFF	ON	N/A	0.9 V
OFF	OFF	OFF	ON	ON	N/A	1.0 V
OFF	OFF	ON	ON	ON	N/A	1.1 V
OFF	ON	ON	ON	ON	N/A	1.2 V
ON	ON	ON	ON	ON	N/A	1.5 V

Table 3 – 3 U18 (U19) regulators option configured by the SW3 (SW2) switch

Switch options						
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**Voltage**
OFF	OFF	ON	ON	OFF	OFF	1.1 V
OFF	OFF	ON	ON	ON	OFF	1.2 V
OFF	ON	OFF	ON	OFF	OFF	1.5 V
OFF	ON	ON	OFF	ON	OFF	1.8 V
ON	OFF	ON	OFF	OFF	OFF	2.5 V
ON	ON	ON	OFF	OFF	OFF	3.3 V

The SATA connector (XK8) can support full power for daughter board, therefore it is not necessary to connect some other power supplies. Before the first insertion of the daughter board, it is necessary to check the voltages, e.g. to measure them by a multimeter on the connector (see Fig. 3 - 10).

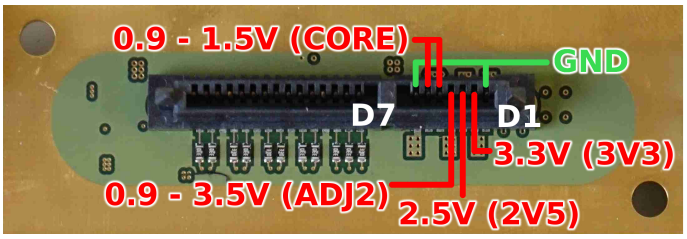

Figure 3 - 10 SATA connector dedicated to the daughter board connection

The HDMI connector (XK6) has only the 5V output, which is restricted only for signalling, not for the power line (HDMI cables are constructed to transfer aprox.

50mA per wire). Therefore, every daughter board connected through the HDMI connector must have its own power source. For this purpose, an adapter from the HDMI connector to SATA connector was designed. It allows to power daughter board with its own power sources.

Various boards can be connected to the ZIF connector (XK9). ZIF connector voltages are shown in Tab. 3 – 4.

Table 3 – 4 ZIF connector power supply pins

Voltage	**0.9 - 1.5**	**2.5**	**3.3**	**0.9 - 3.5**	**0.9 - 3.5 or 5**	**GND**
Pin	15, 16	14	13	12	39	11, 40

3.3 SD cards

Two required micro SD card slots are connected to the SF2 FPGA device. Both SD cards have their own power enable signal which is connected to the adjustable current-limited power switch TPS2552 [23]. The switch current is limited to approx. 200mA to protect board against corrupted SD card. The card detect signal is not used. The SD card pins for both cards are shown in Tab. 3 – 5.

The Altium designer tool called *Interactive length tuning* was used to meet required lengths of wires. It is necessary to draw very similar lengths of wires, because data bus inputs must receive data at the same time. It was used for all n-bit buses (e.g. USB, RAM).

Table 3 – 5 SmartFusion 2 - SD cards pinout

	DAT0	DAT1	DAT2	DAT3	CMD	CLK	PWR EN
SD1	G1	H1	C1	D1	E2	E1	D3
SD2	A2	B1	D5	C4	B3	B2	D4

3.4 External RAM

The RAM memory is usually one of the most difficult part to include in the system design. It contains many signals, which must meet sufficient signal integrity results to ensure high-speed of the memory. Therefore, the RAM device was selected according to one used in the commercial Microsemi evaluation boards, to minimize risk of possible failures. The design of a commercial board was used as an example, which helped me to connect and route the RAM correctly. A big challenge was also to route it on 6 layers (instead 8) and to achieve good signal integrity results.

The HECTOR motherboard supports external synchronous 512 Mb (64 MB) RAM memory (U21). MT46H32M16LFBF-6 [24] is a low-power DDR SDRAM. It is running at 166 MHz, for a total theoretical bandwidth over 5.3 Gbps. It is provided as flexible volatile memory for user applications. The whole LPDDR interface is implemented in bank 0. Specifications of the external RAM are as follows:

- MT46H32M16LF – 8 Meg x 16 x 4 banks,
- Type: LPDDR SDRAM,
- Density: 512 Mb,
- Frequency: 166 MHz,
- Theoretical bandwidth: 5.3 Gbps.

3.5 USB connection

USB connection between the SmartFusion 2 and the PC is ensured by two data channels (Fig. 3 - 11). The first one, the virtual COM port is designed to provide instruction exchange between SF2 and PC by a simple UART protocol. The FTDI device FT232RL [25] is designed for this purpose. It is a simple, UART to USB' converter, which is supported by many operating systems, due to their wide driver support (see section 3.5.1).

The second channel, is designed to provide reliable data transfer by the USB mass storage class interface natively supported by operation systems. It is ensured by the USB physical layer circuit (USB3300 [26]), which creates an intermediate interface between the SF2 and the USB differential wires. The physical layer circuit was chosen due to its frequent use on many commercial boards.

Both USB ports are connected to the USB HUB (USB2640 [27]). It ensures reliable data transfers to the PC by using just one USB cable and a micro USB connector. The selected USB HUB has on integrated Micro SD card reader with a mass storage class interface, suitable for the future use of the motherboard.

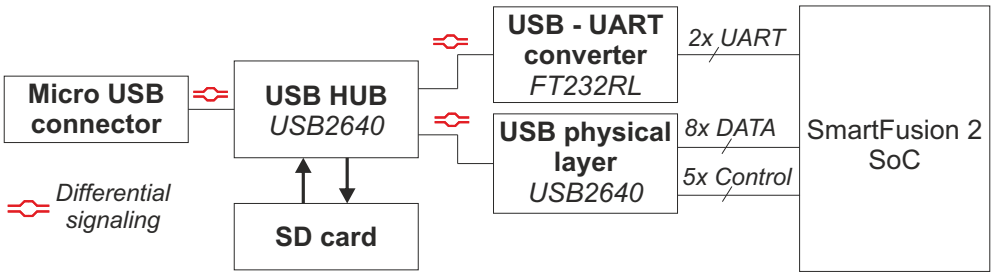

Figure 3 - 11 USB devices block diagram

3.5.1 FTDI RS232RL drivers

It is recommended to use drivers provided by the FTDI company, to provide proper function of the FTDI converter. FTDI provides two types of drivers: D2XX direct driver and a virtual COM port (VCP) driver. The D2XX drivers [28] allow direct access to the USB device across the DLL. The application SW then can access the USB device through a series of the DLL function calls. The virtual COM port (VCP) drivers [29] cause the USB device to appear as an additional COM port available to the PC. The application SW can access the USB device in the same way as it would access a standard COM port. It is recommended for being used with the HECTOR motherboard. Installation guides are available on the FTDI website [30].

3.6 Daughter boards connection

The motherboard provides three connectors for connecting an additional board:

- High-Definition Multimedia Interface (HDMI) connector,
- Serial - ATA (SATA) connector,
- Zero insertion force (ZIF) connector.

According to HECTOR requirements, the daughter modules use a SATA connector, which consists of 4 LVDS wires, 3 single ended wires and a power supply wire. The SATA connector in this case is used mainly for its good signal integrity and mechanical features. However, the way the SATA connector is used is totally different from its standard use. The daughter boards can be connected through SATA connector, either directly by inserting the SATA socket, or via the HDMI-to-SATA interface (including the power management) and the HDMI cable. The ZIF connector is dedicated to ASIC boards (see section 3.6.3).

The signals of the HDMI and SATA connectors can be driven by 2.5 V or 3.3 V, according to jumper position on the pin header X3. The impedance of conductors used for these two connectors are 50 Ω (100 Ω differentially). Every data wire is ended by a resistor, to ensure a current limitation.

3.6.1 SATA connector

The SATA connector provides entire data and power connection to daughter modules. No additional cables and power supply is needed. Data pins connected to SATA connector are shown in Tab. 3 – 6.

Its main advantage is that it allows the required direct shielding of the daughter board by aluminium lid, which protects the board against the EMI (electromagnetic interference). An additional place is reserved around the SATA connector for this

lid. Many compromises were necessary to make suitable dimensions for the lid and for the DB inside the lid.

The lid has the led out SMA connector, which is a part of the adapter with a MMCX (Micro Miniature Coaxial) connector on the other side of the cable. The adapter is connected to the daughter board and it is used to measure the power supply of the daughter board. It is also used to lead out the trigger signal. The MMCX connectors were used due to their dimensions and durability (around 500 mating cycles) [31]. Instead of the MMCX connector, standard 2.54 pin header can be mounted.

Table 3 – 6 SmartFusion 2 pins connected to SATA connector.

Signal	**DATA 0**		**DATA 1**		**DATA 2**		**DATA 3**		**IO 0**	**IO 1**	**IO 2**
	N	**P**	**N**	**P**	**N**	**P**	**N**	**P**			
SF2 pin	AA15	AB15	AB14	AB13	AB11	AA11	AB10	AA10	Y9	W10	W9
SATA pin	P14	P15	P12	P11	P8	P9	P6	P5	P3	P2	P1

3.6.2 HDMI connector

HDMI connector is used to communicate with the daughter board for longer distances using the common HDMI cable. This connection type is suitable for measurements in isolated places, like temperature controller or shielded room. Full data connection is supported, but the power must be provided by an external power source. Data pins dedicated to SATA connector are shown in Tab. 3 – 7.

Table 3 – 7 SmartFusion 2 pins connected to HDMI connector.

Signal	**DATA 0**		**DATA 1**		**DATA 2**		**DATA 3**		**IO 0**	**IO 1**	**IO 2**
	N	**P**	**N**	**P**	**N**	**P**	**N**	**P**			
SF2 pin	Y19	Y18	AB19	AB18	AA18	AB17	W17	Y17	Y20	U18	V17
HDMI pin	3	1	4	6	9	7	10	12	13	15	16

3.6.3 ZIF connector

To connect the daughter boards, a DIP 40 connector with zero insertion force (ZIF) was used. Its advantage is easy and a effortless board insertion. The ZIF connector has 40 pins, 8 of them are dedicated to power supply (see section 3.2.4) and remaining 32 are single ended data wires. The data wires are connected to various banks, therefore, 24 pins are driven by 2.5 V, remaining 8 pins are driven by 3.3 V. ZIF pins and their SF2 connections are shown in Tab. 3 – 8. Following boards can be connected to ZIF socket:

- ASIC circuits boards,
- EVARISTE boards (using adapter) [32],
- expansion boards (e.g. with switches and LEDs).

Table 3 – 8 Motherboard ZIF connector pinout

GPIO	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
ZIF pin	1	2	3	4	5	6	7	8	9	10	17
SF2 pin	R3	R1	R2	T4	T3	L3	M3	L4	L5	P4	L21
Bank voltage	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	2.5V

GPIO	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
ZIF pin	18	19	20	21	22	23	24	25	26	27	28
SF2 pin	M22	M21	L20	G16	G17	F19	F20	G2	F5	F6	E5
Bank voltage	2.5V	2.5V	2.5V	3.3V	3.3V	3.3V	3.3V	2.5V	2.5V	2.5V	2.5V

GPIO	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**
ZIF pin	29	30	31	32	33	34	35	36	37	38
SF2 pin	K4	K2	K1	L2	M2	M1	N3	N1	P2	P1
Bank voltage	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V

3.7 Manufacturing of the printed circuit printed boards

The whole manufacturing of the motherboard was managed by Micronic. A printed circuit board (PCB) was manufactured by the SQP International company [33]. The board was mounted and soldered by Micronic. My task was to make documents for the manufacturing such as assembly drawing and list of the used material. I was also responsible for finding and eliminating errors in the first mounted boards. The last version of motherboard is version 1.2 (the version 1.1 is the same, no electrical differences are between them - see 3.7.1). The final product is shown in Fig. 3 - 12. The board is designed using 6 PCB layers.

Two designed daughter modules (described in next sections) were manufactured in same way.

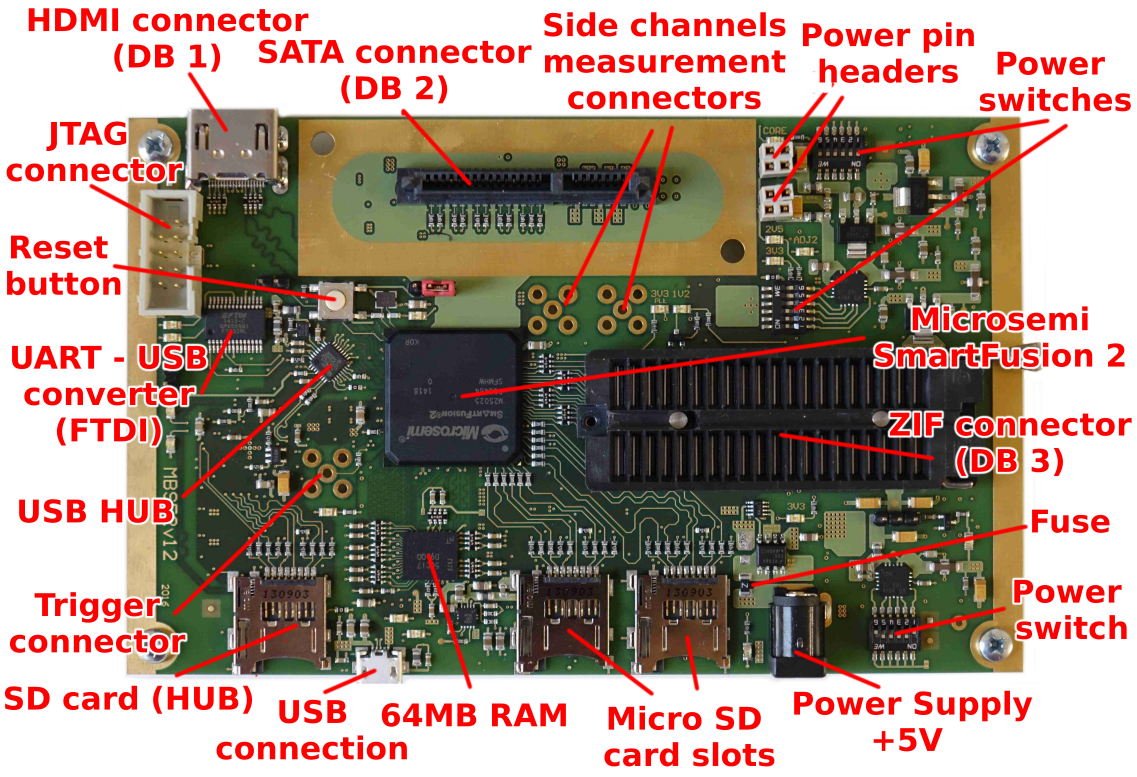

Figure 3 - 12 Motherboard description

3.7.1 Motherboard releases notes

Three versions of the motherboard were made. Release notes are the following:

- **v1.0:**
  - first prototype,
- **v1.1:**
  - changed order of the HDMI connector wires,
  - changed pins of the SmartFusion 2 device used for daughter boards,
  - enlarged place restricted for the SATA connector shield,
  - 5 V power supply connected to the ZIF connector,
  - added power supply protection,
  - deleted possibility of power board by USB,
  - enlarged JTAG connector,
  - aligned lengths of USB physical layer interface,
  - deleted possibility to choose the bank voltage for the ZIF connector,
  - changed voltage of bank number 1 from 3.3 V to 2.5 V,
  - FTDI chip UART signals driven by 2.5 V instead of 3.3 V,
- **v1.2:**
  - electrically same as v1.1, the difference only in the SF2 BGA footprint, v1.1 has the Solder Mask Defined (SMD) BGA pads and v1.2 has the Non-Solder Mask Defined (NSMD) BGA pads [34].

3.8 Daughter board featuring SmartFusion 2 device

The daughter board featuring the SmartFusion 2 (DBSF2) device is based on the same circuit as the motherboard: SmartFusion 2 M2S025 (see section 3.1). The board is connected to the motherboard by the SATA connector. It contains only a limited number of elements ensuring the proper function of the SF2 device.

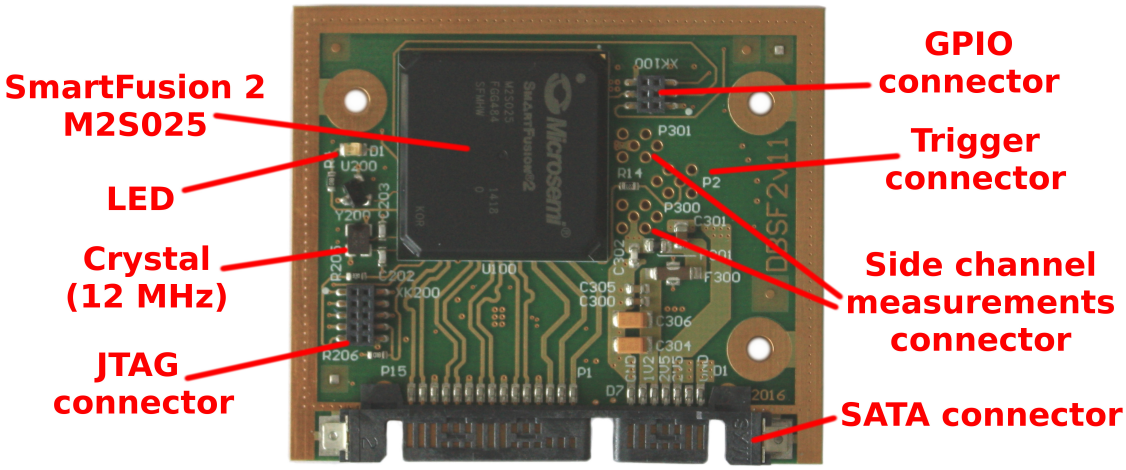

Figure 3 - 13 Description of the daughter board featuring the SmartFusion 2 device

It is the second version of the board and compared with the first version, its dimensions were visibly reduced. Smaller connectors were used, to meet internal dimensions of the lid. Therefore, a small JTAG programming adapter, which changes connector pitch from 1.27 mm to 2.54 mm must be used. The connector is used with the FlashPro programmer. Before the programming interface is used, the VPUMP option from programmer settings must be selected, because the JTAG interface is powered by 2.5 V [37].

The daughter board is designed using a 4 layer PCB. The FPGA banks are powered entirely by 2.5 V and only necessary banks are powered. The PLLs are powered by 2.5 V, but only necessary PLLs are connected according to the recommendations (NW0, NW1, SW0). Remaining PLLs are powered but the recommended filter is not integrated. All PLLs use a linear regulator reserved for them. It ensure a low

noise power to the card. Similarly to the motherboard, the supervisor circuit is used to monitor voltage and to generate reset if it is needed.

The board contains an additional connector (XK100) enabling the JTAG mode selection and three GPIOs, for the future use. The board has one LED and a trigger connector (it can be connected to the lid). The SF2 connections of these pins are shown in Tab. 3 – 9.

Table 3 – 9 Motherboard ZIF connector pinout

Signal	**Trigger**	**LED**	**XGPIO1**	**XGPIO2**	**XGPIO3**
SF2	B22	V19	AB13	AB11	AB10

The SATA connector is connected according to the motherboard SATA socket. The SF2 GPIOs used for the SATA connector are shown in Tab. 3 – 10 and required power supplies are shown in Tab. 3 – 11.

Table 3 – 10 Daughter board SmartFusion 2 pinout

Signal	**DATA 0**		**DATA 1**		**DATA 2**		**DATA 3**		**IO 0**	**IO 1**	**IO 2**
	N	**P**	**N**	**P**	**N**	**P**	**N**	**P**			
SF2 pin	V21	V22	R22	P22	M22	M21	K20	K21	H22	G22	E22
SATA pin	P14	P15	P12	P11	P8	P9	P6	P5	P3	P2	P1

Table 3 – 11 Daughter board SmartFusion 2 - SATA connector power supply

SATA pin	**D7**	**D6**	**D5**	**D4**	**D3**	**D2**	**D1**
Voltage	GND	1.2V	1.2V	2.5V	2.5V	N/A	GND

3.9 Daughter board featuring the Spartan 6 device

The daughter board featuring the Spartan 6 (DBS6) device uses the most cost-optimized FPGA family of the Xilinx company, Spartan 6 XC6SLX16 [35]. The board uses a SATA connector and it is designed with a minimum number of components to ensure its function (Fig. 3 - 14). The board can be clocked by the 125 MHz LVDS oscillator. The selected FPGA device has the following features:

- 14579 logic cells,
- 18224 configurable logic block flip-flops,
- 576 Kb of memory,
- 32 DSP slices,
- 232 IO.

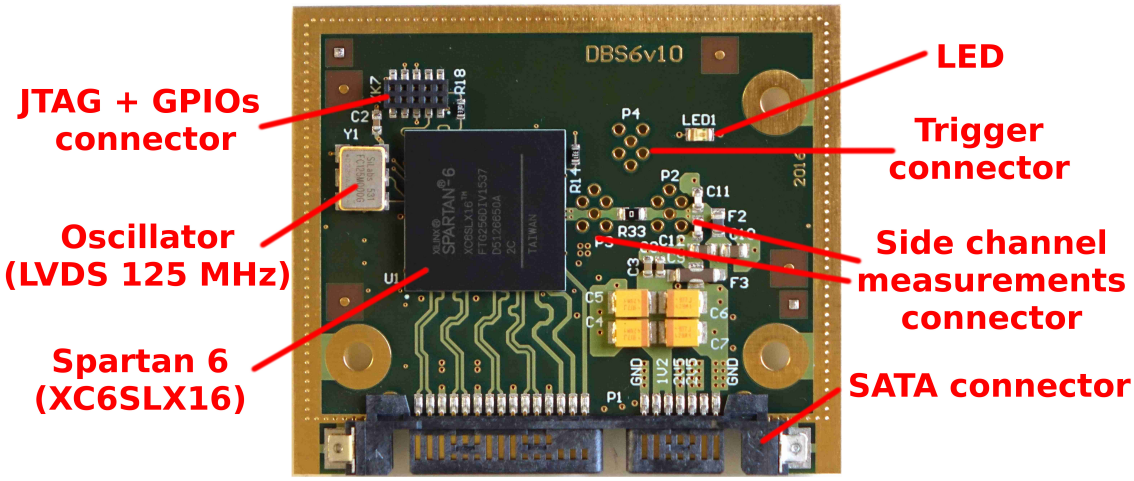

Figure 3 - 14 Daughter board Spartan 6 description

The board contains the MMCX connector for side channel measurements and for the trigger, which can be connected to the lid. The DBS6 does not contain a flash memory and it can be programmed only trough the JTAG connector (XK7), including also 4 GPIO connectors. These connections and other FPGA connections are shown in table 3 – 12. One of the options how to program the device is to use a low cost programmer Digilent HS2 [36]. However, an adapter adapting the 1.27 mm

pitch to 2.54 mm must be used. The schematic diagram of the adapter is shown in Fig. 3 - 15.

Table 3 – 12 DBS6 common pins used

Signal	Trig	LED	XGPIO1	XGPIO2	XGPIO3	XGPIO4	CLK P	CLK N
S6	R15	T15	G16	D16	A12	A11	B10	A10

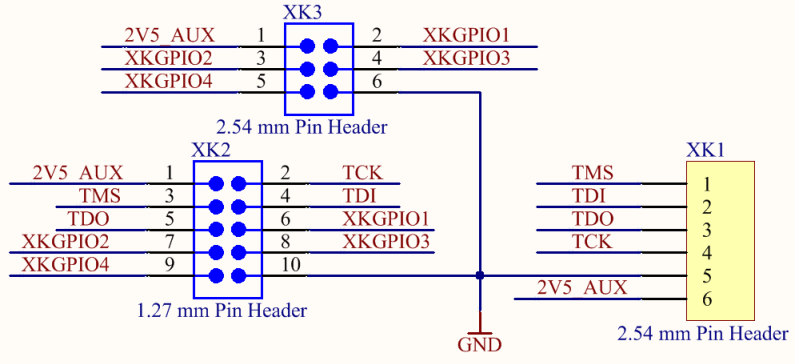

Figure 3 - 15 Daughter board Spartan 6 programming reduction

The FPGA core is powered by 1.2 V, the auxiliary power input is powered by single 2.5 V regulator and the IO banks by another 2.5 V regulator. The voltage configurations for the motherboard SATA connector are shown in Tab. 3 – 13. The pins used for data signals are shown in Tab. 3 – 14.

Table 3 – 13 Daughter board Spartan 6 - SATA connector power supply

SATA pin	D7	D6	D5	D4	D3	D2	D1
Voltage	GND	1.2V	1.2V	2.5V	2.5V	N/A	GND

Table 3 – 14 Daughter board Spartan 6 pinout

Signal	DATA 0		DATA 1		DATA 2		DATA 3		IO 0	IO 1	IO 2
	N	P	N	P	N	P	N	P			
S6 pin	C2	C3	F1	F2	K1	K2	M1	M2	P1	R1	T3
SATA pin	P14	P15	P12	P11	P8	P9	P6	P5	P3	P2	P1

4 Design of the software tools and functions

The software design of the evaluation platform consists of several different tools and functions. It can be divided into two groups, the motherboard software and the user PC application.

The motherboard software realizes a user communication interface and control components of the motherboard. The PC application creates user interface for communication with the motherboard. In the framework of my master thesis, I designed a complete TRNG acquisition system, which can be used as a template for the HECTOR evaluation platform.

4.1 Motherboard software requirements

The main advantage of using the SF2 SoC platform is that the user can merge a complicated fabric system with a simple microcontroller subsystem (MSS). The time-critical parts of the system can be processed by the fabric and the communication protocol can be implemented in the MSS.

According to HECTOR requirements the software should serve for testing primitives implemented on the daughter board. Essentially three cryptographic primitives were required: TRNG, PUF and data encryption algorithm. To meet these requirements, every primitive needs its own software approach.

The TRNG evaluation needs a fast acquisition system featuring big storage capacity. Usually, generated data need to be stored in an external RAM and send it to the host PC through USB. The TRNG implemented in the DB is expected to use just one data signal and one strobe signal.

The PUF functions have higher requirements on communication than the data stor-

age. Essentially they need to receive requests and answer to them. Therefore, the PUF realized in the DB needs an SPI based protocol for communications with the motherboard.

The encryption system has the highest implementation requirements. It needs to receive user data streams, to encrypt (decrypt) them and then send back. Moreover, the system may use the TRNG or PUF functions. The key entry protocol needs to be implemented to. For this purpose the coprocessor implemented in fabric should be used.

Fig. 4 - 1 shows the block diagram of a possible SF2 software implementation for the HECTOR project purposes. The MSS communicates with user using the USB interface. The MSS also operate the FPGA part of the SF2 device using the AHB bus. The daughter board can be accessed through the control block and also by the coprocessor. The DB interface must meet requirements of the component instance or of the primitive used inside.

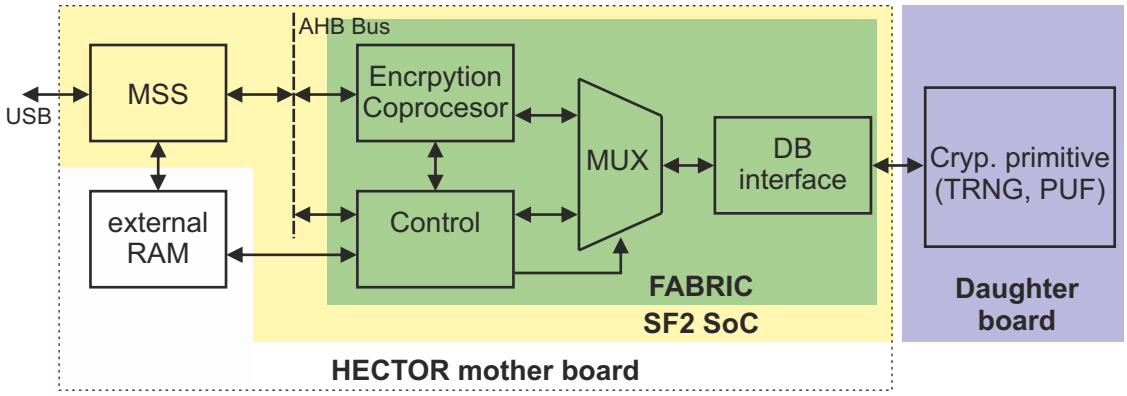

Figure 4 - 1 Motherboard software design block diagram

4.2 PC application requirements

The main task of the PC application is to provide the user interface for the motherboard. It is based on the USB interface, which uses VCP to transfer commands and the USB mass storage to transfer data (see section 3.5). It is necessary to create the communication protocol on this interface to ensure reliable command exchange and to execute commands in the motherboard.

Big advantage of using this communication interface is its support, because the USB mass storage interface is natively supported by common operation systems (OS) and VCP drivers (see section 3.5.1) provided by the FTDI company. Therefore the PC application can be written in any programming language, depending only on the user choice. Researchers often need to automate operations on the board. Hence, it is very useful to have application, which is able to read user scripts.

4.3 Data acquisition from a TRNG

My main software development objective was to make a system aimed at the TRNG data acquisition. The task of the system was to store data generated by the TRNG in the daughter board to the external RAM in the HMB and to read them using the USB mass storage interface.

The block diagram of the software architecture is shown in Fig. 4 - 2. The MSS receives user instructions (section 4.3.1) and execute them by the internal state machine. The communication with the PC is performed using two channels: the commands are transferred by the UART interface and data are transferred by the USB mass storage class interface. Both channels use one USB interface (see section 3.5). The MSS also monitors and controls the FPGA fabric system using the AHB bus and common GPIO signals. The GPIO signals are used for generating asynchronous resets and for optional user purpose. The AHB bus is used to write or

read from the FPGA fabric registers.

Data generated by the TRNG are transferred to the S/P converter, where they are collected to 32-bit words. Then the 32-bit words are transferred across the Control block to the RAM WR (RAM write) interface. The Control block writes data to external RAM. It acts as a Master AHB device and writes data to the slave AHB device - an external RAM.

The RAM bridge is a HW part of the SoC, which allows to access external RAM from the FPGA fabric or MSS. The whole acquisition is controlled by the Control block. It is responsible for caching the TRNG data and for data transfers to the RAM WR block. At the end of the acquisition, the MSS sends acquired data to the user via USB bus.

At the beginning, I had already implemented the USB mass storage on RAM disk and preconfigured project for the FPGA design. I implemented and designed whole MSS state machine, UART packet recognition system and the FPGA data acquisition system with the AHB master implementation.

The parts of the diagram shown below will be described in next subsections.

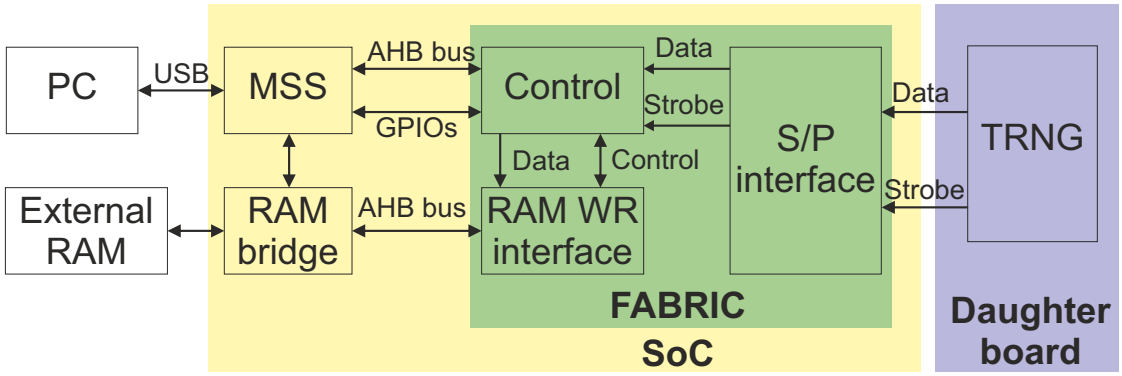

Figure 4 - 2 Design of TRNG acquisition system

4.3.1 UART packets

Commands are transferred from the host computer to the system by the UART interface. The UART packets are received by MSS in an interrupt mode and the functional diagram of the MSS is shown on Fig. 4 - 3.

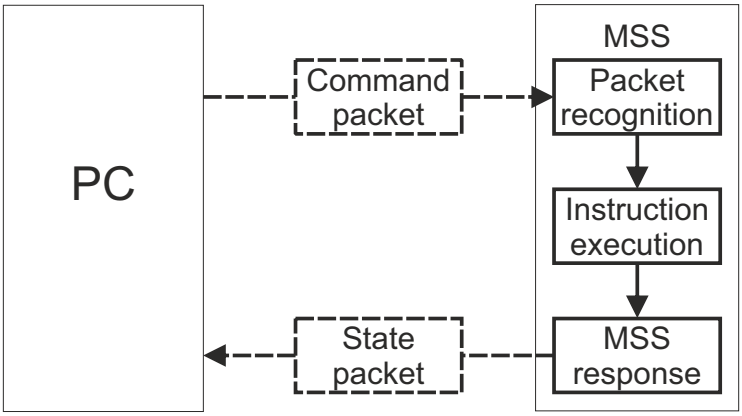

Figure 4 - 3 Functional diagram of MSS packet manipulation

The UART is configured as follows:

- 115200 baud rate,
- 8 data bits, 1 stop bit,
- no parity, no data flow.

Commands between the PC and MSS are transferred in packets. The format of packets originates from the Evariste platform [32], but it is completely redesigned. Four types of packets are used:

- command packet,
- read data packet,
- write data packet (not implemented yet),
- status packet.

Packets feature always a big endian format [43], so the UART transfers can be easily read. Start of packets are recognized by their header (8-bit word 0x13). The packet header is followed by the prefix. It is an 8-bit word, which is different for every packet type. The command prefix is 0xC0, read data (RD) prefix is 0xFD, and the status packet prefix is 0x57. The write data (WD) prefix is 0x3D. The sequence of heads and prefixes is followed by 16 bits of zero padding data blocks.

The command packet is used for transfer of the MSS instructions (see Fig. 4 - 4). A 32-bit is reserved to transfer a command to the fabric or an optional data to the controller. The next two bytes are not used as input for MSS, but they can be optionally used. The packets contain also a byte, which is reserved for the GPIO commands. The MSS instruction is situated at the end of the command packet. The MSS instruction list is located in *mss_instr.h* file of the MSS firmware, and it is explained in section 4.3.2.

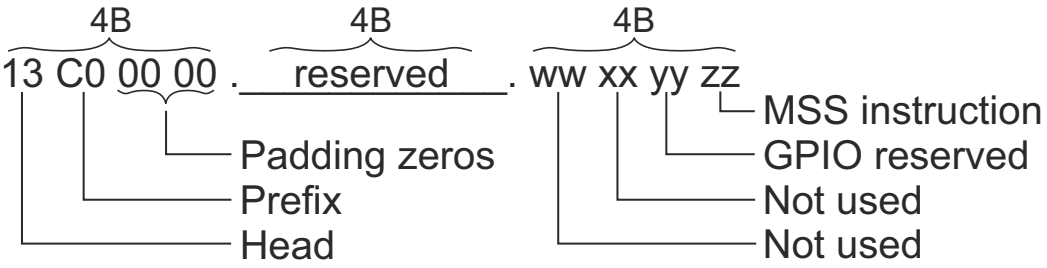

Figure 4 - 4 Format of the command packet

Every recognized command packet is responded by a status packet (see Fig. 4 - 5). The status packet contains 32-bit reserved word, which can be used for reading the fabric register or for an optional user transfer. The next is the operation progress byte, which shows the state of the current MSS operation (number from 0 to 100). It is followed by the operation state. The GPIO state is the state of input or output (depends on configuration of the pin) of the MSS pins (pin number 8-15). At the end of the status packet, the command execution response is positioned.

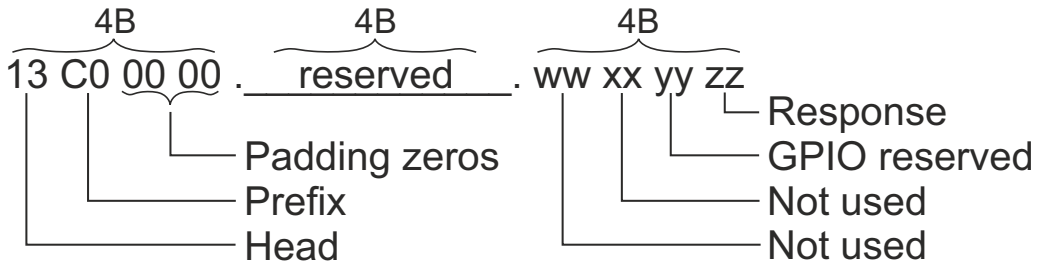

Figure 4 - 5 Format of the status packet

The read data (RD) packet is a special type of the command packet. It is restricted to data transfers especially for the TRNG data acquisition (see Fig. 4 - 6). The file name is formed by 12 characters and it is limited by the used file system function. The space character is situated at the end of the file name. It is followed by the required stream size (32-bit word). The size of stream must be multiple of 4 bytes, else it will be rounded up, to the nearest multiple. The size of the required file is limited by the half size of the RAM memory (less than 32 MB). The MSS sends its response after every RD packet received.

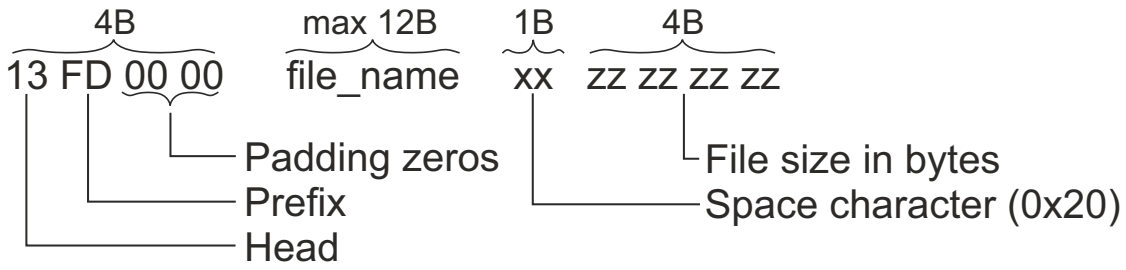

Figure 4 - 6 Format of read data packet

4.3.2 MSS instructions

This subsection describes commands (MSS instructions) implemented in motherboard's MSS. They are concatenated to the end of the command packet. The fol-

lowing list contains instructions designed for the TRNG template. New instructions can be very easily added to the MSS code and their implementation depends only on the user needs.

The **‚make fabric'** command (in the MSS defined as MB_FAB_CMD with the code word 0x01) takes a 32-bit word from the packet and writes it to the fabric command register. The implementation of this command depends only on the fabric. When number 3 is written then the fabric sets the HDMI connector to be active. Similarly, when number 4 is written, then the SATA connector becomes active.

The **‚Make fabric reset'** command (MAKE_FAB_RST, 0x04) asserts the reset signal of the acquisition module (Contol unit and RAM WR interface) during 1 ms. The **‚Make generator reset'** command (MAKE_GEN_RST, 0x05) is similar to the previous command. It asserts the reset signal of the generator and of the S/P converter during 1 ms.

The **‚Mount disk'** command (MB_MOUNT_DISK, 0x06) connects the RAM memory with fat32 file system to the PC using USB connection.

The **‚Get operation state'** command (MB_GET_OP_STATE, 0x07) just returns state of the operation. It is very useful, when an information about the acquisition progress is needed.

The **‚Make file system'** command (MB_MAKE_FSYS, 0x08) generates the file system on the RAM disk and removes the whole data from the disk.

The **‚GPIO configuration'** command (MB_GPIO_CGF, 0x09) configures GPIO pins (number 8. - 15.) according to the reserved 8-bit word in command packet (one means output, zero means input).

The **‚GPIO set'** command (MB_GPIO_CGF, 0x0A) configures output value of the GPIO pins (number 8. - 15.) according to the reserved 8-bit word in the command

packet (,one means high assertion and zero low assertion).

The **‚Operation reset'** command (MB_OP_RST, 0x0B) resets the whole acquisition system implemented in the MSS and FPGA fabric.

4.3.3 RAM and USB mass storage

The USB mass storage class disk drive is based on the Microsemi example [48]. The disk is located in the external RAM. The memory space is divided to two halves, where first half is used for the file system and the second half is a cache reserved for the TRNG data acquisition.

The implemented file system is based on the library called FatFs [49]. It is a generic FAT/exFAT file system module aimed at small embedded systems implementations. The FatFs module is written in compliance with ANSI C (C89) and it is completely separated from the disk I/O layer. The embedded file system library is distributed as an open source software.

The data acquisition implemented in FPGA writes data directly to the external RAM. During the data acquisition, the external RAM is not accessible. At the end of the data acquisition, data are copied to the existing file system in the second half of the RAM memory.

4.3.4 MSS - FPGA interface

The MSS features the following options to communicate with FPGA:

- 8 optional GPIOs,
- generator and fabric reset,
- AHB lite bus.

Eight GPIOs can be optionaly used in fabric design as output or input off the MSS. Types and value of GPIOs are controlled by GPIO commands. Two resets (generator and fabric reset) are used to reset internal logic of FPGA. The fabric reset is used to reset FPGA control logic. These reset signals have special commands, which asset them during 1 ms (resets are active in zero). The AHB bus is used to write and read 32-bit fabric register words (see section 4.3.7).

4.3.5 External RAM write interface

A direct access to the external memory is necessary to implement fast data acquisition systems. It was one of the first tasks, while I was designing the acquisition system. My implementation is based on the Microsemi AHB example of the AHB Fabric Master device [40]. However, in contrast with this example, my application writes data to external RAM directly, using a DMA controller that I had to design.

The DMA block implemented in FPGA is very simple and it is not optimized (e.g. the starting address is always identical and the access to the memory is reserved to the acquisition system). The process is controlled only by the address bus, the data bus and a start signal. The writing procedure starts by asserting the start signal to high. When data and address buses were loaded, block replies by asserting the state signal to low during one clock period.(see Fig. 4 - 7).

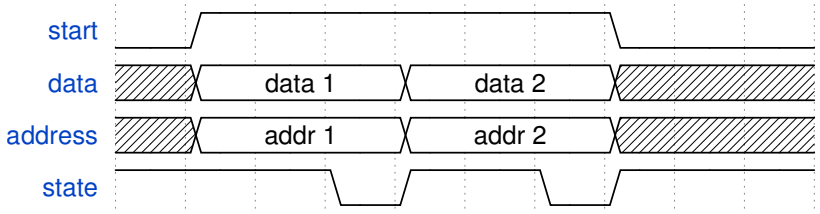

Figure 4 - 7 External RAM write interface (AHB Fabric Master)

4.3.6 Serial to parallel converter

Synchronization of two independent clock domains is one of important problems in digital systems. Any asynchronous part of the system can cause a lot of issues. In our case we have two independent clock domains. The first one is TRNG domain and second is the acquisition system. The output of the generator usually consists of data and strobe signal. Data are typically valid on the rising edge of the strobe signal. The standard approach is to sample generator output signal using the strobe signal rising or falling edge.

New approach of this design is, that data are collected to 32-bit words in the TRNG clock domain and the 32-bit words are sent to the second clock domain. Consequently, the sampling of a slower 32-bit word is easier than the sampling of only one generator bit. This task is performed by the serial to parallel (S/P) converter. The S/P converter is very simple. It inserts TRNG output bits to the FIFO register and once 32-bits inserted, it inverts the strobe out signal. The acquisition system (in the second domain) just samples a new value of the strobe signal (Fig. 4 - 8), which is 32 times slower than the generator speed.

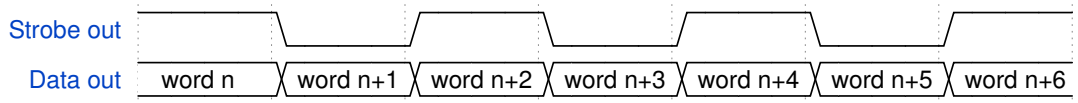

Figure 4 - 8 S/P converter data output (32-bit words)

Advantage of this solution is in the simplicity of the S/P converter and independence of the solution on the clock frequency of the first domain (Fig. 4 - 9), because the speed of the generator is limited only by the speed of the acquisition data processing. Maximum obtained throughput is around 400 Mbps.

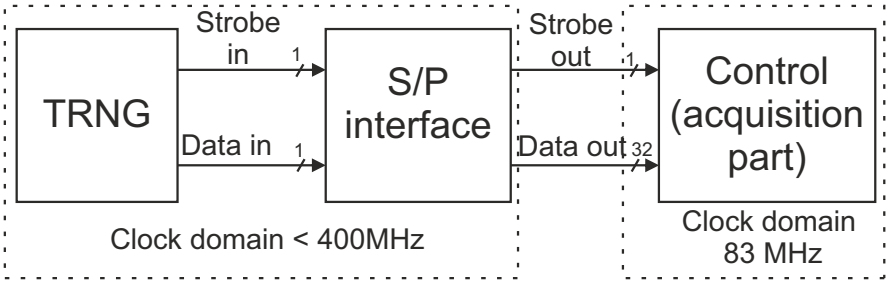

Figure 4 - 9 Serial to parallel converter

4.3.7 Control block implementation

Main tasks of the control block are as follows:

- AHB bus communication with MSS,
- execute simple commands,
- manage data acquistion process,
- transfer data from S/P converter to external RAM.

An AHB lite bus is used to transfer data between MSS and FPGA fabric part. The control block is based on the AHB lite protocol specification [42]. It is written very simple and it enables MSS to write or read to/from fabric registers without any special routines in MSS.

The command execution system is also implemented in the control block. It is a simple state machine, which executes received commands. The command is transferred by a simple MSS writing to the 32-bit command register. Commands can be used to various purposes, e.g. process control or choice of the daughter board slot.

The data acquisition process takes care of reliable, fast data transfer from S/P converter to external RAM. The acquisition process can be described as a controlled DMA transfer. It is defined by the start address and end address registers and it

starts using the start acquisition command.

The control block obtains data from the S/P converter and it puts them to the buffer. It samples the strobe signal and if two sampled values in a row are equal (to the active level of the strobe signal), than data are inserted to buffer. The buffer has 512 bits to store 16 words from converter. The supervisor block checks possible overflow of the buffer and stops the acquisition process if overflow occurs.

4.3.8 Testing

The whole software functionality was tested by a simple counter implemented in the daughter board. The application increments 32-bit word stored in a shift register. The MSB is shifted first and the S/P converter shift bits to the right side. Next, data are written to the external memory by the AHB Master Fabric block (RAM WR interface), but the memory uses the little endian format. Therefore data are rearranged as depicted in Fig. 4 - 10.

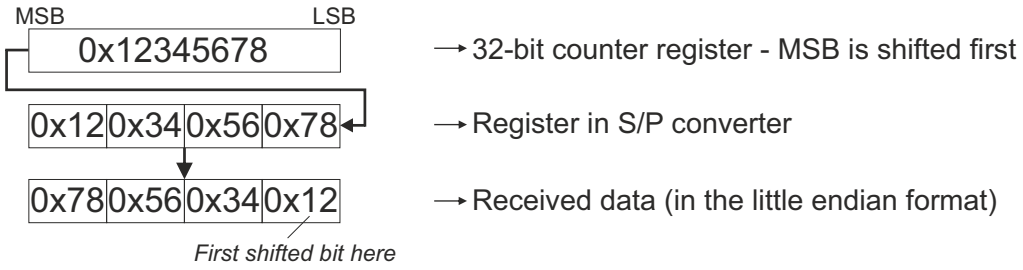

Figure 4 - 10 Shifting of a 32-bit word

4.3.9 Host PC software for TRNG data acquisition

As I mentioned earlier, the application running on the host PC should be system independent. Its main objective is to process user instructions and to provide reliable communication between host PC and the HECTOR mother board.

I wrote the application in the C programming language. The application uses D2XX FTDI drivers for communication with the USB UART converter (see section 3.5.1). I used it only for the debugging purposes during evaluation platform development, because it was too simple and system dependent.

Therefore the first application designed for the HECTOR platform is written in the Tcl programming language [53]. The application was written in Hubert Curien Laboratory. It is system independent because it needs only a Tcl interpreter to execute commands. Usually, every installation of the Microsemi Libero or Altera Quartus IDE (integrated development environment) contains the Tcl interpreter.

The whole application is written in one script file, which consists of functions targeted to the motherboard or for other additional processing. The script file is included by entering ‚source SCRIPT_NAME' to the Tcl interpreter in the script file directory.

The next step consist in opening the COM port of the motherboard by entering ‚set dev [openDevice COMx]', where letter ‚x' is number of COM port. It sets variable ‚dev' with COM port number.

Once the communication port is open, commands defined in the script file can be entered. E.g. the acquisition is started by entering ‚acquireData $dev FILE_NAME FILE_SIZE', where ‚FILE_NAME' is the name of the file to which data will be copied and ‚FILE_SIZE' is the size of the required file.

4.4 Software tools for development of hardware and software embedded system

The SF2 SoC software design is divided to two parts. First is design in FPGA part (sometimes called fabric) written in VHDL and second dedicated as MSS part

written in C programming language. The hardware part of the SoC was designed in VHDL, synthesized using the Synopsis compiller and simulated in Model Sim. The Software part of the SoC was written in C.

The Libero SoC v11.7.0.119 tool was used to develop FPGA design for the SF2 device[45]. It is dedicated to Microsemi SoC devices and it combines Microsemi tools with EDA tools like Synplify Pro and ModelSim. The Libero software provides complete design flow guidance and support for novice or experienced users.

The SoftConsole v4.0.0.13 was used to develop and debug the firmware for the SF2 MSS [46]. It is a free software development environment delivered by Microsemi to produce C and C++ executables for Microsemi FPGAs using ARM processors. The Libero SoC design software can export firmware targeted to embedded processor into the into the SoftConsole tool. If the SoftConsole v3.4 is used, processor cannot be debugged using the FlashPro 5 programmer. It is supported only in the SoftConsole v4.0.

SoftConsole projects generated by Libero in version v11.7 and lower are for use with SoftConsole v3.4 SP1 and they are not compatible with SoftConsole v4.0. Firmware exported by Libero into the ‚firmware' folder of a Libero project is compatible with SoftConsole v4.0 and should be copied into a SoftConsole v4.0 project [47].

I used embedded Microsemi ModelSim for simulations of the FPGA design. One disadvantage of using the SoC lies in very limited simulation possibilities. It is possible to fully simulate the FPGA design, but the behaviour of the embedded MSS firmware can not be simulated. BFM (Bus Functional Model) scripts are one of way how to simulate the MSS, but scripts are independent from the embedded firmware used by the MSS. Another problem is that the documentation of the BFM script is very poor [44]. Pre-simulated packages also exists, which can be used to partially simulate MSS buses.

5 Evaluation of PLL-Based TRNG

I demonstrated the use of the HECTOR evaluation platform by implementing a PLL-based TRNG (PLL-TRNG) in the SmartFusion 2 daughter module. The generator was first proposed in [51] and again discussed within the HECTOR project [38]. I didn't make a design of the PLL-TRNG, I just used an existing design of the PLL-TRNG developed by the Hubert Curien laboratory. I tested reliability of generator in various voltage conditions and evaluate it using AIS-31 tests [55].

5.1 Design and principle

The source of randomness in the PLL-TRNG is the tracking jitter introduced by the PLL. The jitter is defined as phase fluctuations in a clock or data signal, caused by the noise or other disturbances [52].

The basic principle of PLL-TRNG is shown in Fig. 5 - 1. The PLL 2 output clock signal CLK_{jit} is sampled in a D flip-flop (DFF) using the reference clock signal CLK_{ref} generated by PLL 1. Simultaneously XOR operation is made on sequence of the samples. Following DFF sample one output bit after a defined samples was counted. If sampled sequence contains at least one random sample caused by jitter signal, it will take effect to randomness of output bit.

Sampling period must be enough to capture the jitter. The entropy role at TRNG output depends on PLL output frequencies, i.e. on selection of multiple an division factors of PLLs and on input clock signal CLK_{in}.

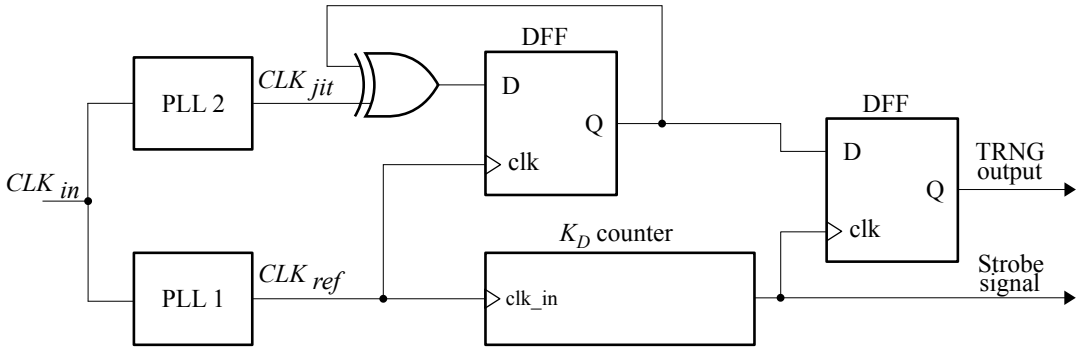

Figure 5 - 1 Principle of Phase-locked loop-based TRNG [38]

5.2 Testing and results

Under-voltage of the circuit is very often a method of attacks of device intruders. I tested the generator applying the same method on the evaluation hardware platform without any additional power sources.

I connected SmartFusion 2 daughter module to the motherboard using a HDMI cable and a SATA adapter (Fig. 5 - 2). The daughter module was powered by the cable from the pin header of the motherboard regulators (this configuration can also be used in a Faraday cage). I used the motherboard configurable regulators to change the power voltage value. First, I tried to change the voltage of the SF2 core (VDD voltage). Its recommended operating conditions are from 1.14 V to 1.26 V. I stored a 10 MB binary data stream from the TRNG.

Subsequently, I tested the quality of the generator output according to the AIS-31 standard. AIS-31 is a German standard specifying necessary properties of secure TRNGs and the way they must be evaluated. The AIS20/31 test suite consists of 9 tests T0 - T8, where T0 - T5 are the statistical tests aimed at testing the statistical quality of internal random numbers [54]. Tests T6 - T8 are aimed at testing raw random numbers. T6 is a uniform distribution test and T7 is a comparative test for multinomial distributions. Last entropy test, T8 corresponds to Coron's entropy

estimation.

In our case tests T0 - T8 passed for 1.2 V - 1 V but during 0.9 V the tests failed (received file contains only zeros). Tab. 5 – 1 shows the values of entropy estimation. Lower the TRNG entropy is caused by a lower power voltage, but these difference is not very considerable. However, more unreliable is output when the core is supplied by a 0.9 V. The generator returned only zeros.

Table 5 – 1 AIS-31 tests during under-voltage of FPGA core (P - passed, F - failed)

Core voltage	**T0 - T8**	**Coron's entropy estimation for 1 bit**
1.2 V	P	0.999951
1.1 V	P	0.999850
1.0 V	P	0.999606
0.9 V	F	N/A

Next, I tested the generator for the influence of the under-voltage of the PLL. Recommended operating conditions range from 2.375 V to 2.625 V for a 2.5 V nominal voltage and from 3.15 V to 3.45 V for a 3.3 V voltage. I stored again a 10 MB TRNG binary data stream in a file. Tab. 5 – 2 shows that the PLL power has not any significant influence on the generator. Generator stops working under 1.9 V, when its strobe signal became inactive (because of the low voltage).

Since the operation of the generator degrades outside the recommended operational conditions (the power voltage), it is necessary to include same kinds of detectors, but these detectors can be easily made inactive by the intruder. Therefore, one of best protection is to implement embedded online tests inside the generator. The AIS-31 test T8 indicate in some cases entropy higher than 1 per bit (it is nonsense). These results have only information character. The accuracy of the results is also deformed by a small number of measurements and instability of temperature.

Table 5 – 2 AIS-31 tests during under-voltage of PLL power (P - passed, F - failed)

Core voltage	T0 - T8	Coron's entropy estimation for 1 bit
3.3 V	P	0,999942
3.15 V	P	0,999977
3.0 V	P	0,999997
2.75 V	P	1,000264
2.5 V	P	1,000011
2.3 V	P	1,000154
2.1 V	P	0,999937
2.0 V	P	1,000088
1.95 V	P	0,999494

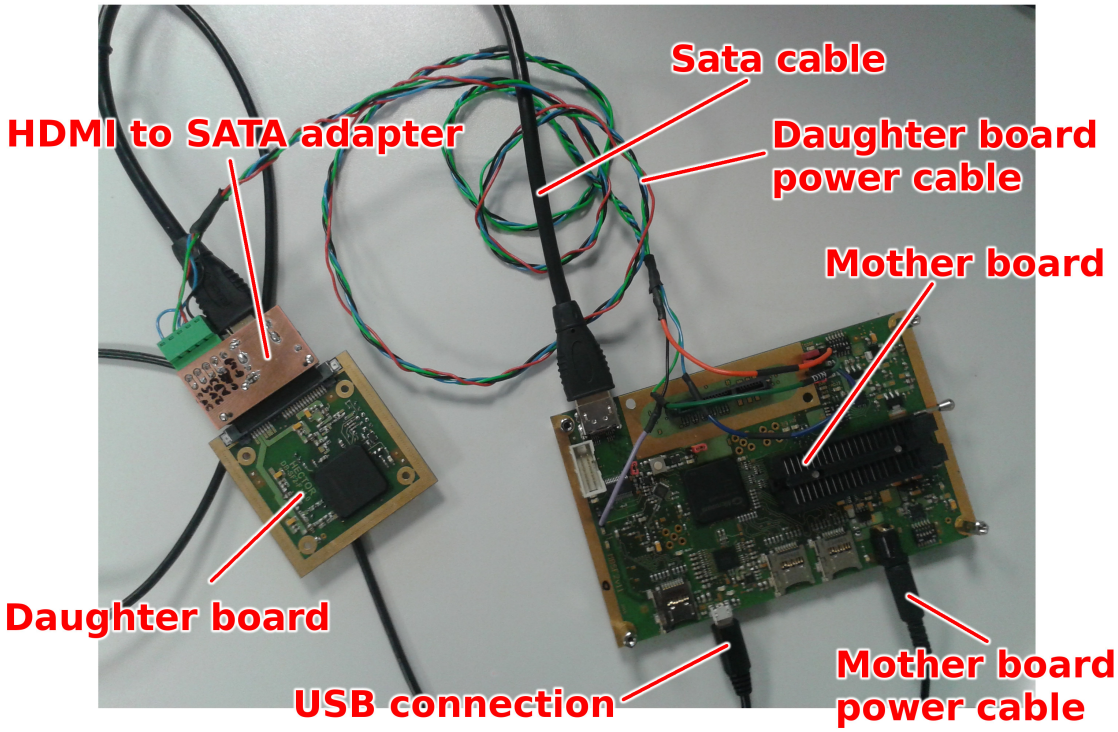

Figure 5 - 2 Connection of the evaluation platform during testing

6 Conclusion

This thesis described the design of the hardware platform and software tools aimed at testing and implementation of cryptographic primitives. The whole HW platform was designed according to requirements specified by the HECTOR project industrial partners: STMicroelectronics France and Italy, Thales Communications & Security France, Technikon Austria, Brightsight Netherlands and Micronic Slovakia. The designed motherboard is fully optimized for evaluation of cryptographic primitives. The SATA and HDMI connectors available of the daughter module were successfully tested. The designed daughter modules represents a basis for the development of the next modules. They can be modified in the future to achieve requirements defined by researchers and industrial partners.

A new motherboard will be probably desgined in the future. It will be based on a more powerful FPGA-Altera Cyclone V SoC, which will feature a gigabit ethernet, 1GB of RAM and a USB OTG (USB On-The-Go) interface.

The SW design intended for TRNG acquisition represents a template for the development of the evaluation platform for other primitives like PUFs and AE. The SW platform will be improved in the future to support evaluation of these primitives.

Implemented PLL-TRNG demonstrated practical usefulness of the evaluation platform and brought interesting results of the generator behaviour during its testing. Its implementation was realized with a big assistance of colleagues from the Hubert Curien Laboratory due to the lack of time.

The designed platform is unique due to its possibilities of evaluation of hardware-dependent cryptographic primitives. It represents an ideal solution for the side channel attack evaluations and for evaluation of cryptographic primitives across different ASIC and FPGA families. No similar commercial platform exists, therefore these tools are very valuable for the hardware-dependent cryptography research.

References

[1] *Handbook of Applied Cryptography*, Menezes, Oorschot, Vanstone, ISBN 0-8493-8523-7

[2] *Kryptografia v komunikačnej bezpečnosti*, Levický D., 2014, ISBN 978-80-8086-235-0

[3] Drutarovský, M. - Fischer, V. - Šimka, M. - Celle, F.: *A simple pll-based true random number generator for embedded digital systems*, Computing and informatics, Vol. 23, 2004 , pp. 501-515

[4] *Physical Unclonable Functions guide*, NXP, available online: http://www.nxp.com/documents/other/75017366.pdf

[5] *Design and evaluation of a delay-based FPGA physically unclonable function*, Aaron Mills, Iowa State University, available online: http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3416&context=etd

[6] *Quantum random number generators and their use in cryptography*, STIPČEVIĆ, M., Zagreb, Croatia, available online: http://arxiv.org/ftp/arxiv/papers/1103/1103.4381.pdf

[7] *HECTOR document D1.1*, Evaluation Platform and Industry-driven Requirements Specification

[8] *HECTOR project*, project description on web page, available online: https://hector-project.eu/

[9] *Altium designer website*, available online: http://www.altium.com/

[10] *FlashPro programmer website*, Microsemi, available online: http://www.microsemi.com/products/fpga-soc/design-resources/programming/flashpro#hardware

[11] *MIC803 voltage supervisor datasheet*, Micrel, available online: http://www.micrel.com/_PDF/mic803.pdf

[12] *Clocking resources user guide*, Microsemi, available online: http://www.microsemi.com/document-portal/doc_download/132012-ug0449-smartfusion2-and-igloo2-clocking-resources-user-guide

[13] *2,5mm power jack datasheet*, Wurth Electronik, available online: http://katalog.we-online.de/em/datasheet/6941xx301002.pdf

[14] *LT1963, voltage regulator datasheet*, Linear technology, available online: http://cds.linear.com/docs/en/datasheet/1963fc.pdf

[15] *LT3083, voltage regulator datasheet*, Linear technology, available online: http://cds.linear.com/docs/en/datasheet/3083fa.pdf

[16] *TPS7A7300, voltage regulator datasheet*, Texas Instruments, available online: http://www.ti.com/lit/ds/symlink/tps7a7300.pdf

[17] *TPS51200, voltage regulator datasheet*, Texas Instruments, available online: http://www.ti.com/lit/ds/symlink/tps51200.pdf

[18] *EMI Suppression Filters datasheet*, Murata, available online: http://www.murata.com/ /media/webrenewal/support/library/catalog/products/emc/emifil/c31e.ashx?la=en-us

[19] *LTC4361-2 circuit datasheet*, Linear technology, available online: http://cds.linear.com/docs/en/datasheet/436112fb.pdf

[20] *Dual N and P-Channel Power MOSFET datasheet*, Fairchild, available online: http://katalog.we-online.de/em/datasheet/6941xx301002.pdf

[21] *SF-1206F Fuse Series datasheet*, Bourns, available online: http://www.bourns.com/docs/Product-Datasheets/sf1206f.pdf

[22] *Schottky rectifier diode datasheet*, Vishay General Semiconductor, available online: http://www.vishay.com/docs/87911/v8pan50.pdf

[23] *TPS2552, adjustable current limited power switch datasheet*, Texas Instruments, available online: http://www.ti.com/lit/ds/symlink/tps2553.pdf

[24] *MT46H32M16LFBF-5 DDR SDRAM datasheet*, Micron, available online: https://www.micron.com/~/media/documents/products/data-sheet/dram/mobile-dram/low-power-dram/lpddr/60-series/t67m_512mb_mobile_lpddr_sdram.pdf

[25] *FT232RL, USB to UART converter datasheet*, FTDI, available online: http://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT232R.pdf

[26] *USB3300, USB physical layer datasheet*, Microchip, available online: http://ww1.microchip.com/downloads/en/DeviceDoc/00001783B.pdf

[27] *USB2640, HUB / card reader datasheet*, Microchip, available online: http://ww1.microchip.com/downloads/en/DeviceDoc/2640_2641.pdf

[28] *D2XX drivers website*, FTDI, available online: http://www.ftdichip.com/Drivers/D2XX.htm

[29] *VCP drivers website*, FTDI, available online: http://www.ftdichip.com/Drivers/VCP.htm

[30] *FTDI driver installation guides website*, FTDI, available online: http://www.ftdichip.com/Support/Documents/InstallGuides.htm

[31] *RF connectors quick reference guide*, Te connectivity, available online: http://www.te.com/commerce/DocumentDelivery/DDEController?Action=srchrtrv&DocNm=1-1773725-8_RF_COAX_QRG&DocType=DS&DocLang=English&s_cid=1046

[32] *Evariste wiki page*, Laboratoire Hubert Curien, available online: http://labh-curien.univ-st-etienne.fr/wiki-evariste/index.php/Main_Page

[33] *SQP international s.r.o. website*, available online: http://www.plosnyspoj.sk/

[34] *Difference between NSMD and SMD pads*, Topline website, available online: http://www.topline.tv/SMD_vrs_NSMD.html

[35] *Spartan 6 datasheet*, Xilinx, available online: http://www.xilinx.com/support/documentation/data_sheets/ds160.pdf

[36] *HS2 programmer datasheet*, Digilent, available online: https://reference.digilentinc.com/_media/jtag_hs2:jtag-hs2_rm.pdf

[37] *Programming user guide*, Microsemi, available online: http://www.microsemi.com/document-portal/doc_view/132014-ug0451-igloo2-and-smartfusion2-programming-user-guide

[38] *HECTOR document D2.1*, Report on Selected TRNG and PUF Principles

[39] *FPGA-based True Random Number Generation using using Circuit Metastability with Adaptive Feedback Control*, Mehrdad Majzoobi, Farinaz Koushanfar, Srinivas Devadas, Rice University, Houston, Circuit Metastability with Adaptive Feedback Control https://www.iacr.org/archive/ches2011/69170017/69170017.pdf

[40] *AHB design guide*, Microsemi, available online:
http://www.microsemi.com/document-portal/doc_view/134389-ac388-smartfusion2-dynamic-configuration-of-ahb-bus-matrix-app-note

[41] *FIC design guide*, Microsemi, available online:
http://www.actel.com/documents/SmartFusion2_FIC_Tutorial_UG.pdf

[42] *AHB bus specification*, ARM, available online:
http://www.eecs.umich.edu/courses/eecs373/readings/ARM_IHI0033A_AMBA_AHB-Lite_SPEC.pdf

[43] *Little and big endian explanation*, available online:
https://www.cs.umd.edu/class/sum2003/cmsc311/Notes/Data/endian.html

[44] *BFM simulation for AMBA*, Microsemi, available online:
http://www.actel.com/ipdocs/CoreAMBA_BFM_UG.pdf

[45] *Libero web site*, Microsemi, available online:
http://www.microsemi.com/products/fpga-soc/design-resources/design-software/libero-soc

[46] *Softconsole web site*, Microsemi, available online:
http://www.microsemi.com/products/fpga-soc/design-resources/design-software/softconsole

[47] *Softconsole v4.0 release notes document*, Microsemi, available online:
http://www.microsemi.com/document-portal/doc_download/135569-softconsole-v4-0-release-notes

[48] *USB OTG demo guide*, Microsemi, available online:
http://www.microsemi.com/document-portal/doc_download/132615-dg0476-smartfusion2-usb-otg-capabilities-libero-soc-v11-7-demo-guide

[49] *Generic FAT file system module website*, The Electronic Lives Manufacturing - presented by ChaN, available online: http://elm-chan.org/fsw/ff/00index_e.html

[50] *Evaluation board kit - board files*, Microsemi, available online: http://www.microsemi.com/document-portal/doc_download/134422-smartfusion2-security-evaluation-kit-board-files

[51] *True random number generator embedded in reconfigurable hardware*, V. Fischer, M. Drutarovsky, In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), volume 2523 of LNCS, pages 415–430.

[52] *Estimation of the clock signal jitter using the time-interval measurement system*, Zielinski, Kowalski, Chaberski,Grzelak, available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.9114&rep=rep1&type=pdf

[53] *Informations about Tcl programming language*, Tcl developer exchange available online: https://www.tcl.tk/about/language.html

[54] *AIS-31 test application*, Bundesamt fur Sicherheit in der Informationstechnik, available online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_testsuit_zip.zip?___blob=publicationFile

[55] *Cryptographic Hardware and Embedded Systems*, Oswald, Rohatgi, Springer 2008

[56] *Security requirements for cryptographic modules*, U.S. department of commerce / National Institute of Standards and Technology, available online: http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf

Appendices

Appendix A CD medium consists of:

- thesis in electronic form and its Latex project,
- schematics, final artwork prints, composite drawings of designed boards,
- designed SW for mother board, daughter board and PC application.

Appendix B Schematics, final artwork prints and composite drawings of designed boards.

Appendix A

Content of CD medium:

- Hardware
  - **MBSF2** - schematic diagram, composite drawing and final artwork of mother board Smart Fusion 2,
  - **DBSF2** - schematic diagram, composite drawing and final artwork of daughter board Smart Fusion 2,
  - **DBSF2** - schematic diagram, composite drawing and final artwork of daughter board Spartan 6,
- Software
  - **app** - PC application written in Tcl programming language,
  - **app_obs** - PC application written in C programming language (obsolete),
  - **cnt_db** - Daughter board counter (DBSF2) used for debugging,
  - **Eval_pfm** - Complete project for Libero v11.7 of TRNG acquisition system for Mother board (MSS part inside SoftConsole4 directory),
- Tests
  - **CORE** - data stream files of PLL-TRNG during core under-voltage conditions,
  - **PLL** - data stream files of PLL-TRNG during PLL under-voltage conditions,
- Thesis
  - **PDF** - Master thesis in electronic form,
  - **Latex** - Master thesis Latex project folder.

Appendix B

Appendix B consists of following images:

- Mother board schematic 6 - 1 - 6 - 10,
- Mother board final artwork 6 - 11 - 6 - 16,
- Mother board composite drawing 6 - 17 and 6 - 18,
- Daughter board SF2 schematic 6 - 19 - 6 - 22,
- Daughter board SF2 final artwork 6 - 23 - 6 - 26,
- Daughter board SF2 composite drawing 6 - 27 and 6 - 28,
- Daughter board S6 schematic 6 - 29 - 6 - 31,
- Daughter board S6 final artwork 6 - 32 - 6 - 35,
- Daughter board S6 composite drawing 6 - 36 and 6 - 37.

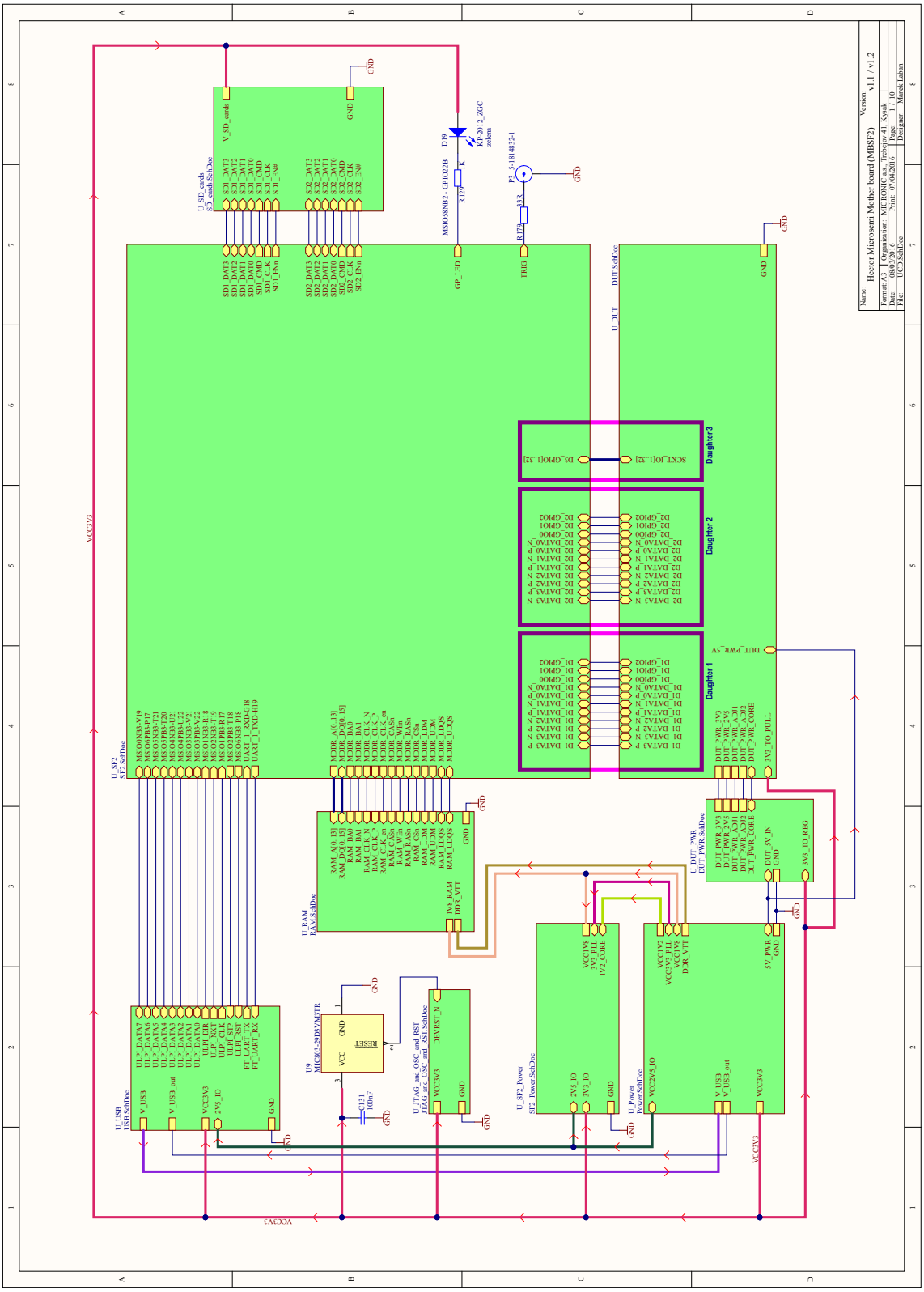

Figure 6 - 1 Schematic of mother board page 1/10

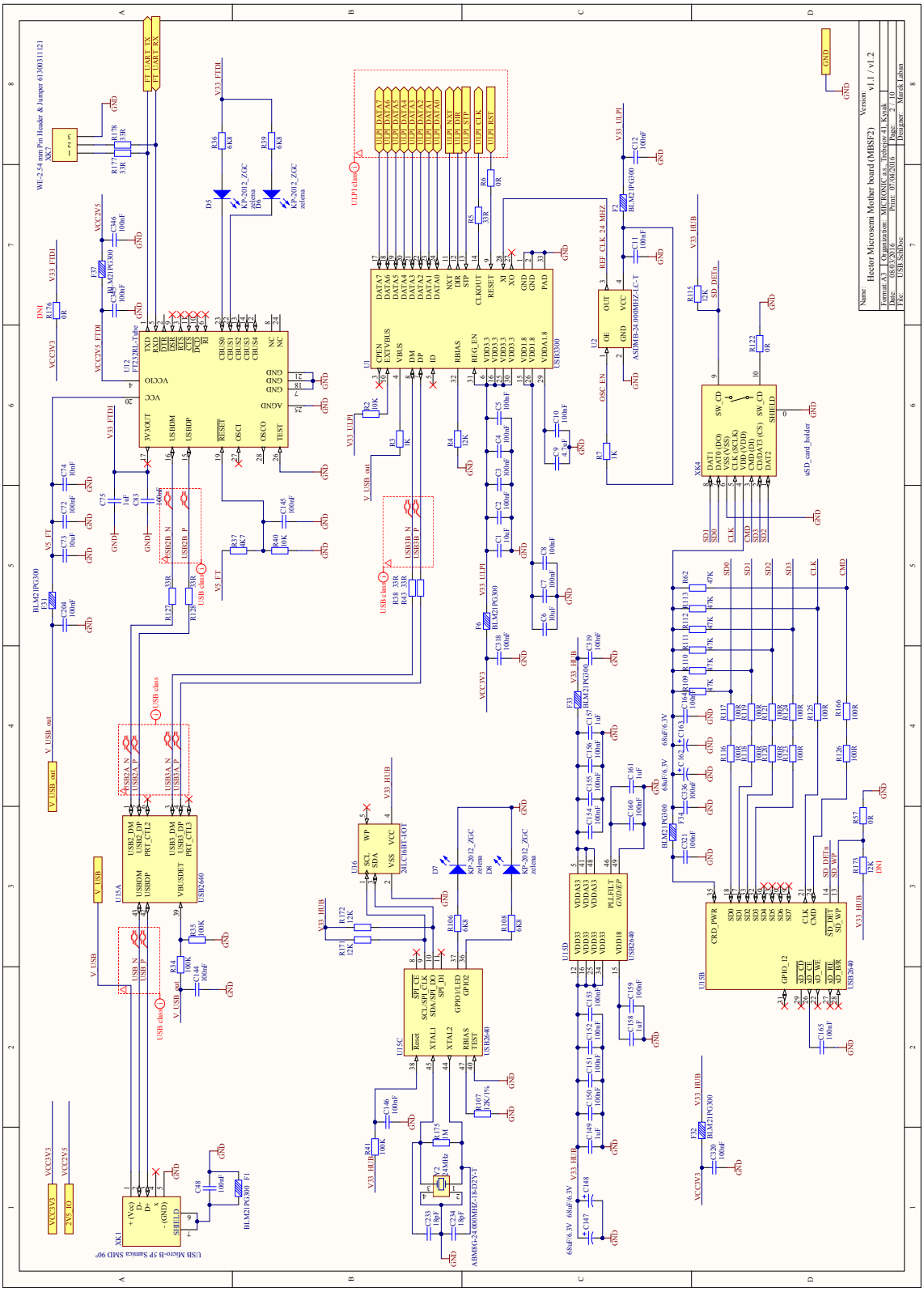

Figure 6 - 2 Schematic of mother board page 2/10

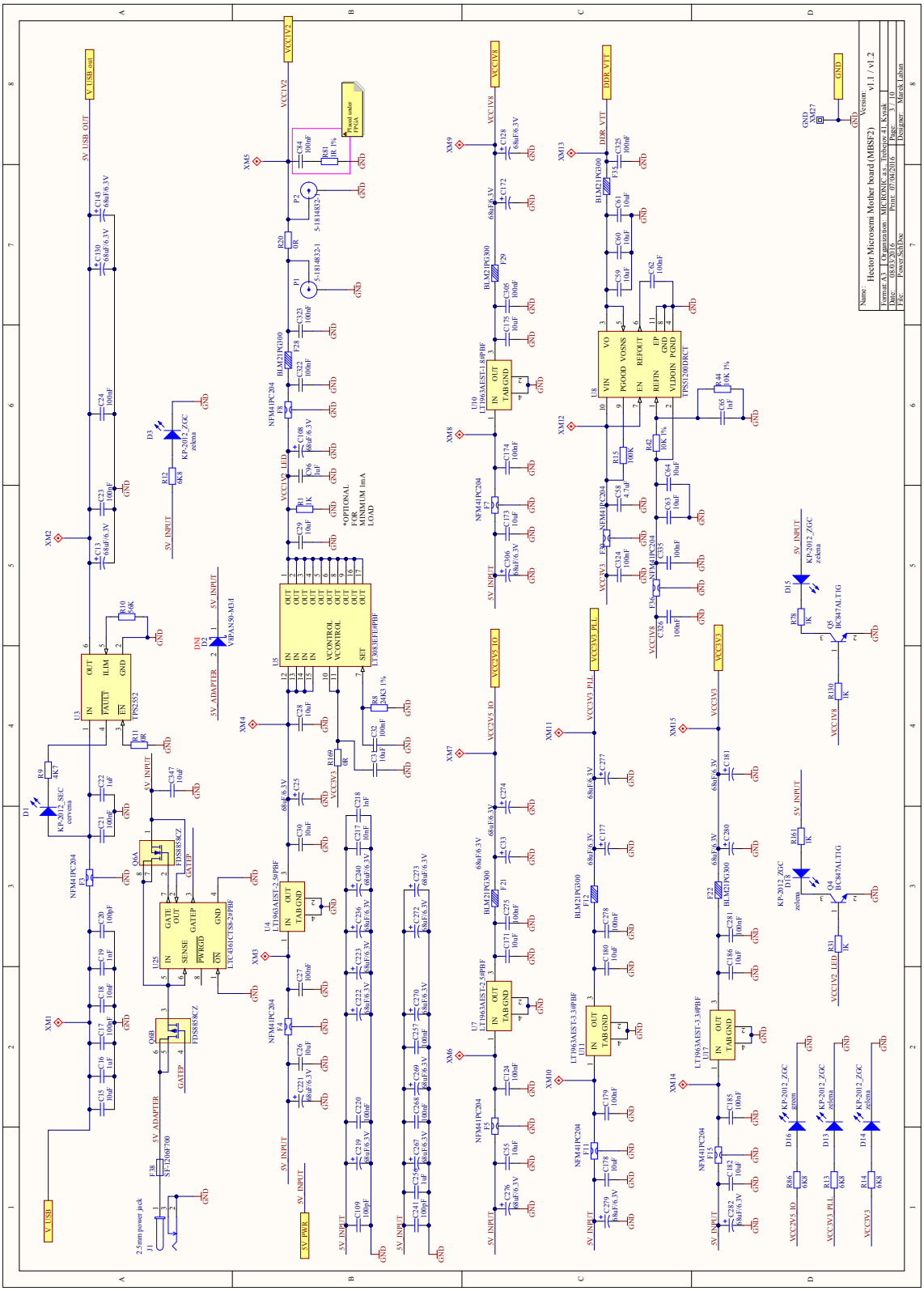

Figure 6 - 3 Schematic of mother board page 3/10

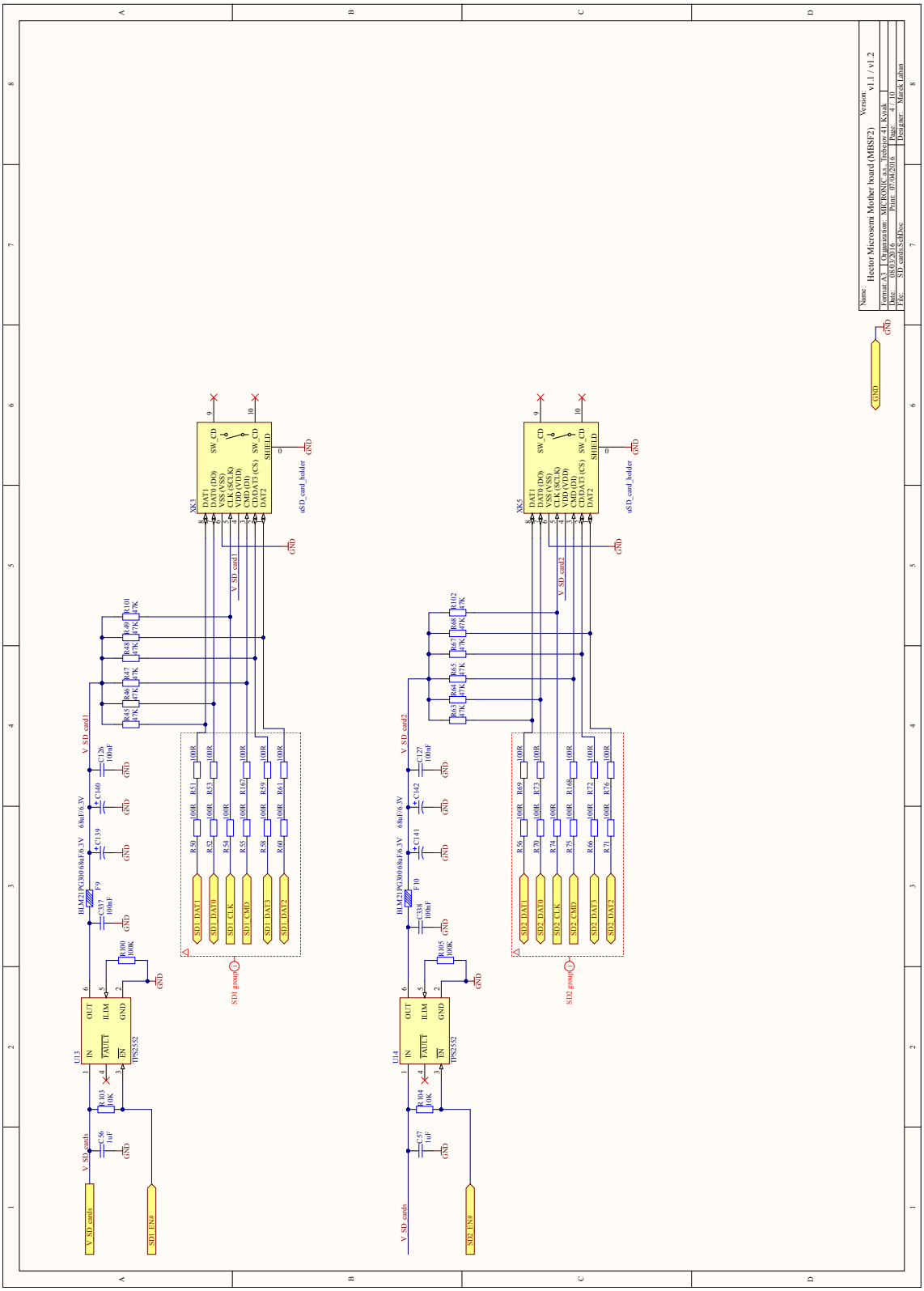

Figure 6 - 4 Schematic of mother board page 4/10

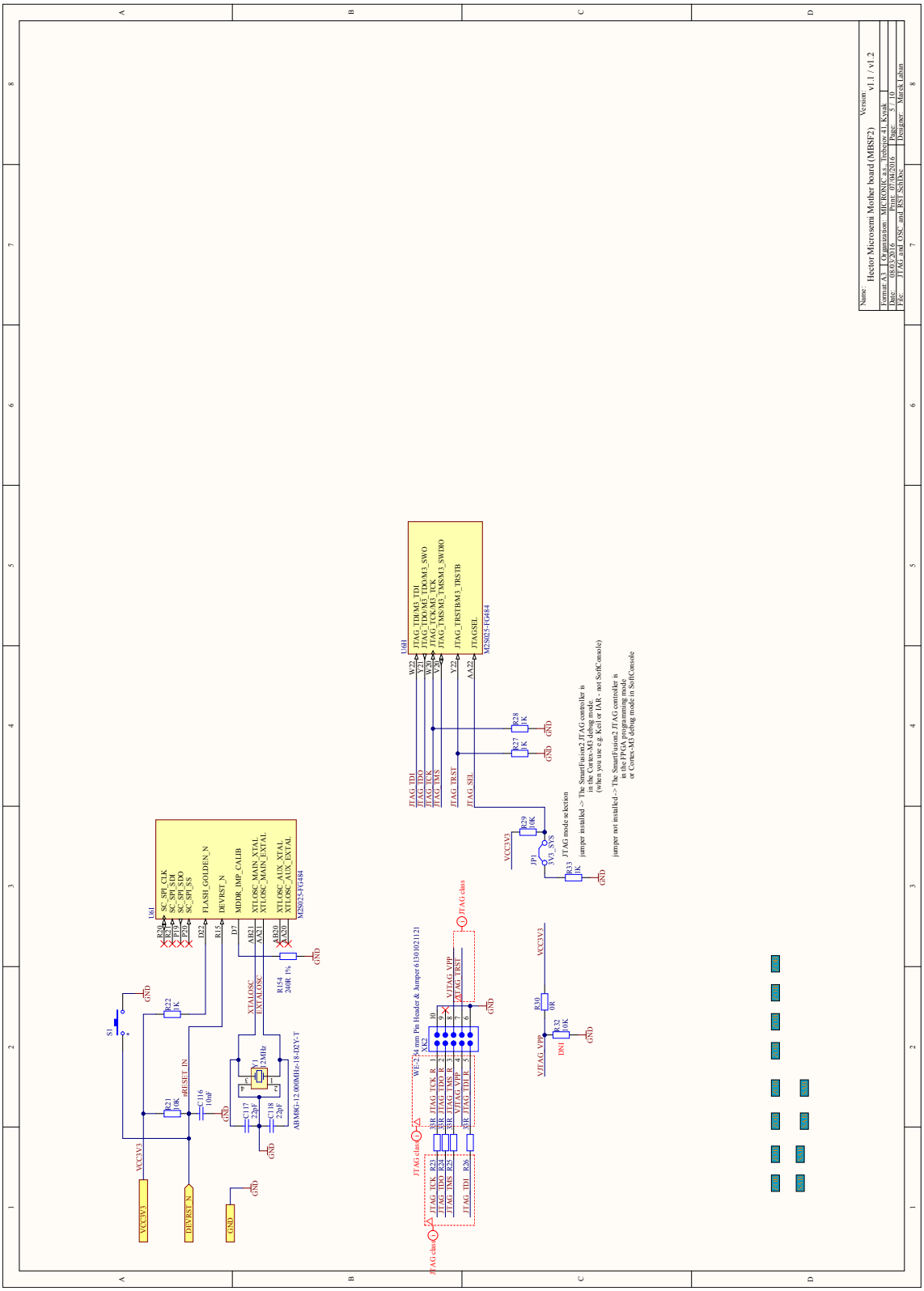

Figure 6 - 5 Schematic of mother board page 5/10

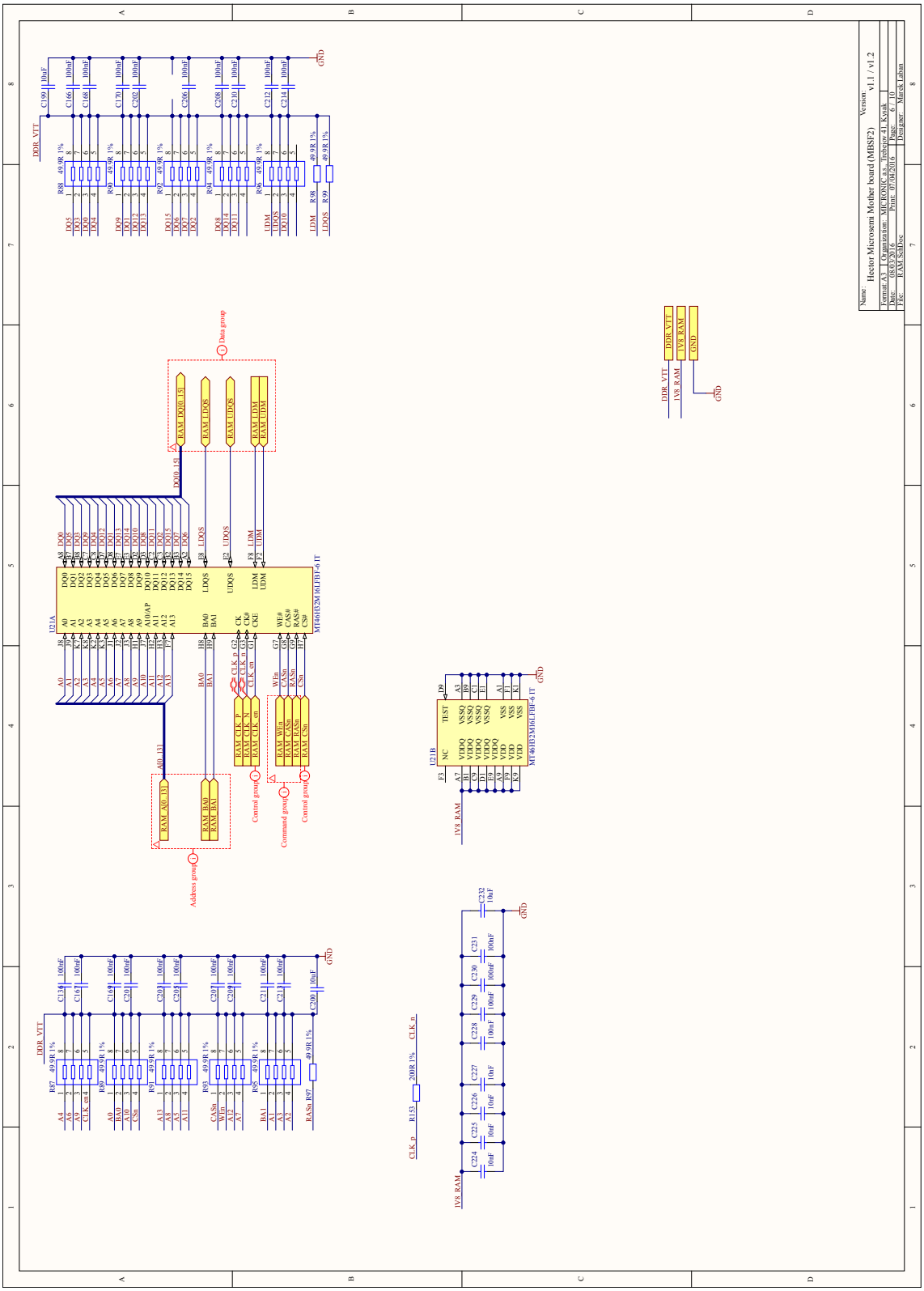

Figure 6 - 6 Schematic of mother board page 6/10

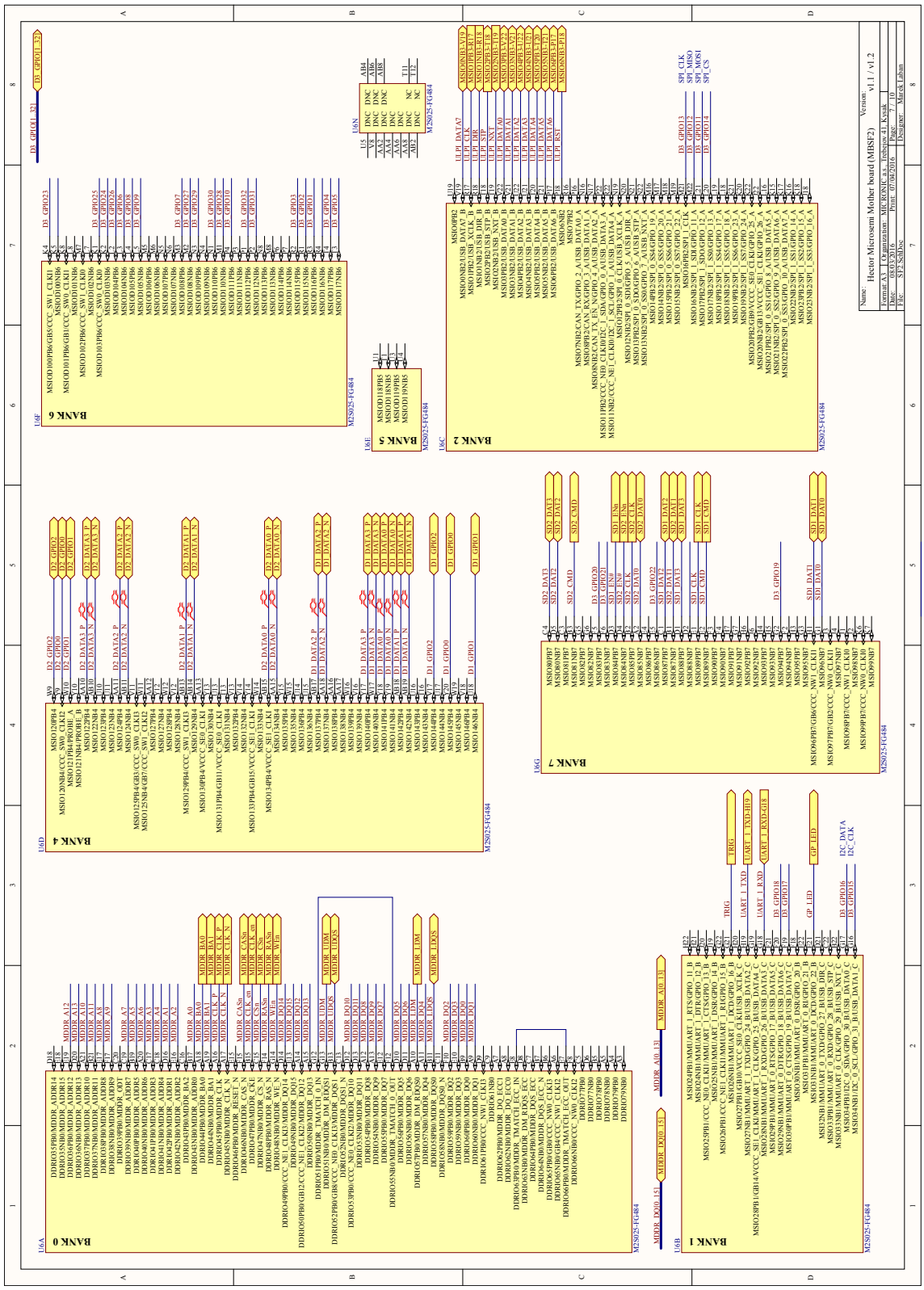

Figure 6 - 7 Schematic of mother board page 7/10

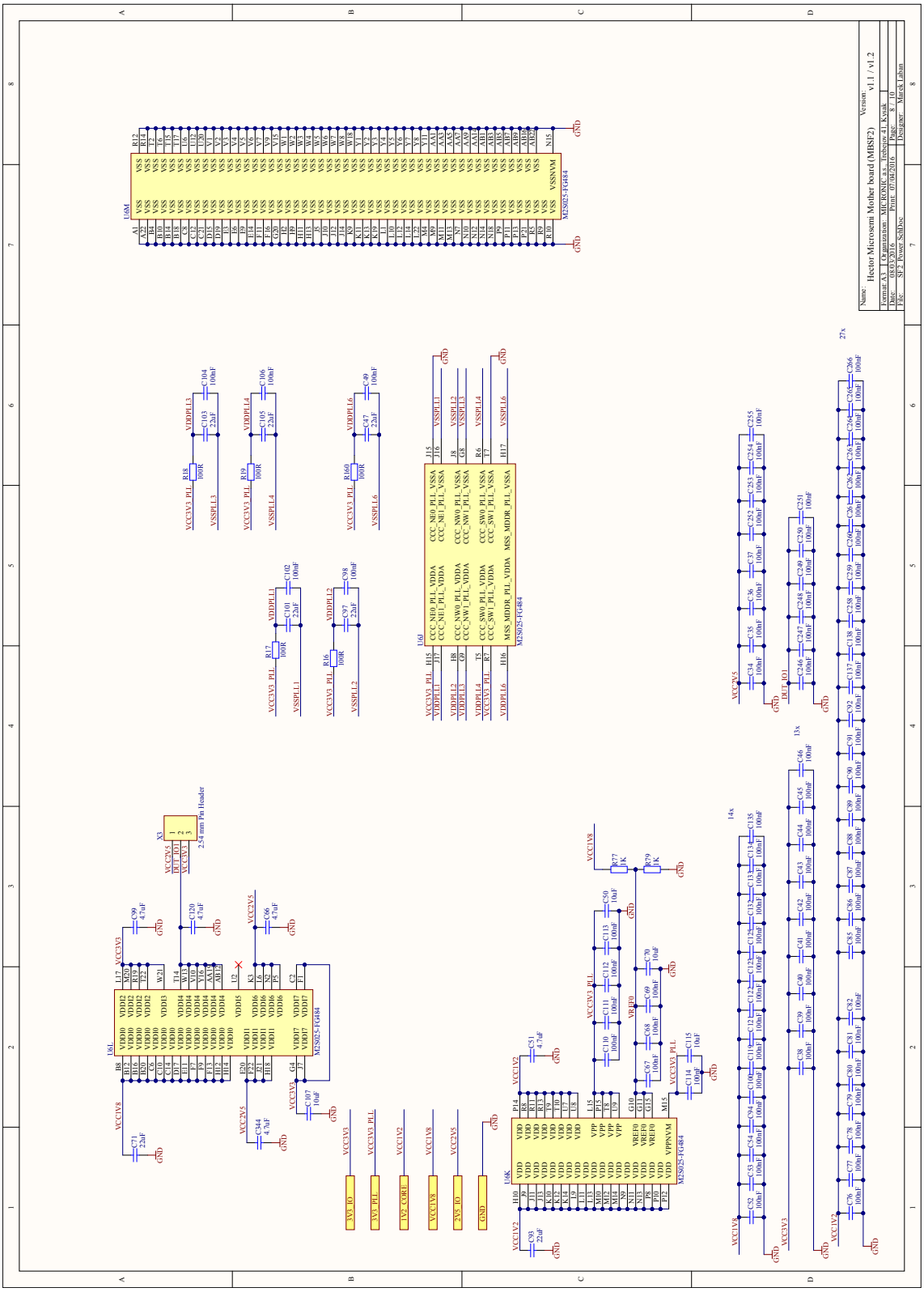

Figure 6 - 8 Schematic of mother board page 8/10

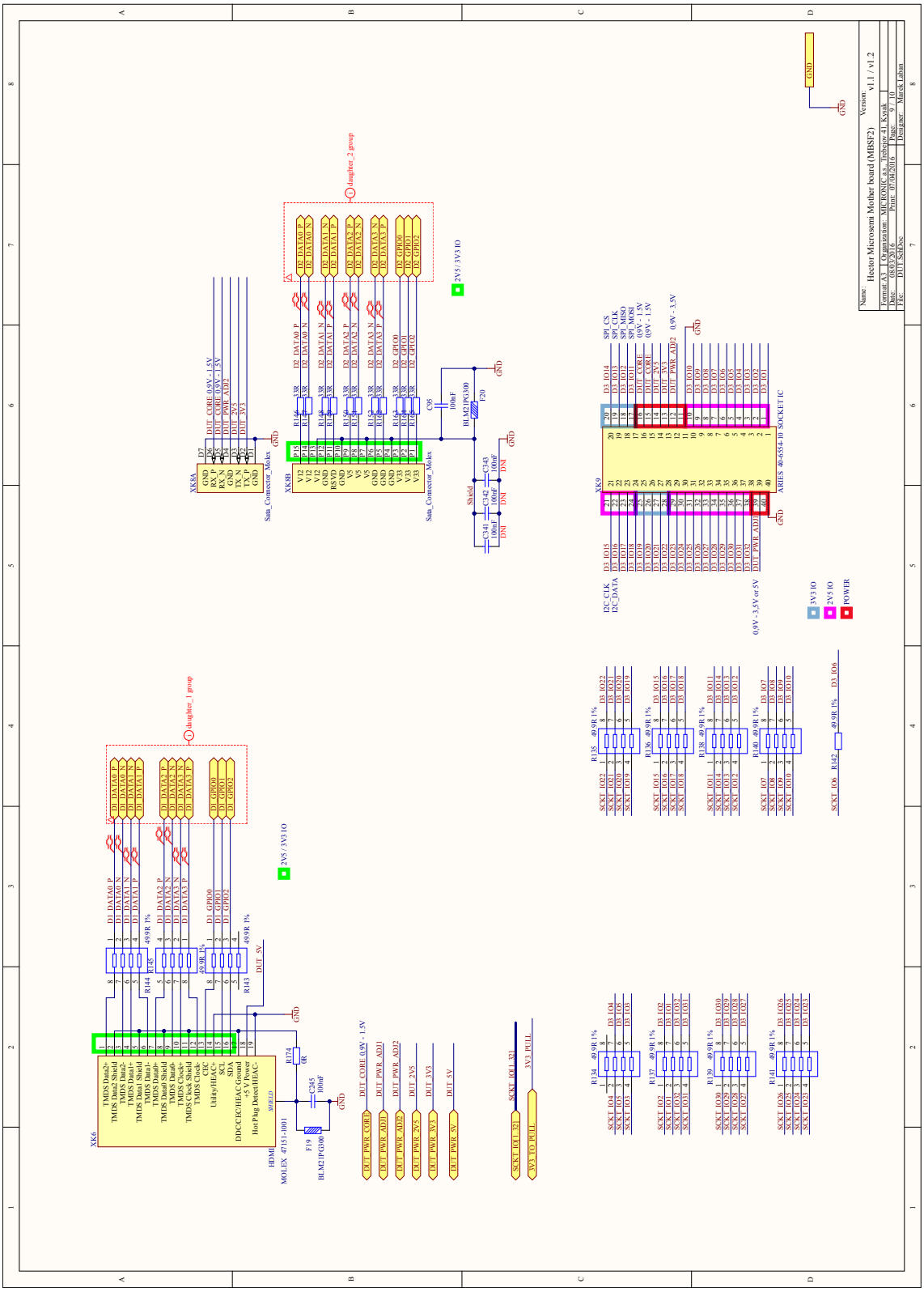

Figure 6 - 9 Schematic of mother board page 9/10

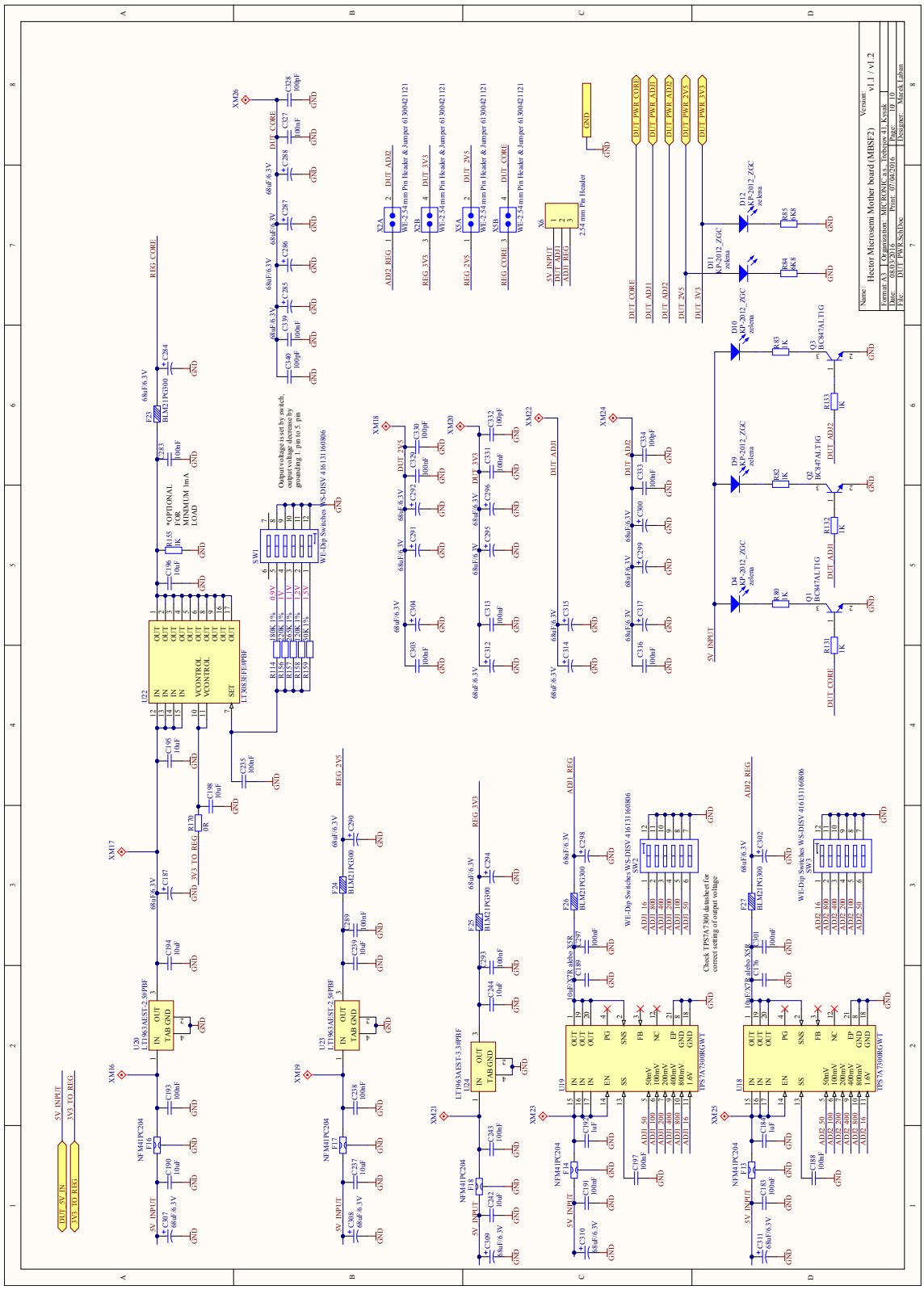

Figure 6 - 10 Schematic of mother board page 10/10

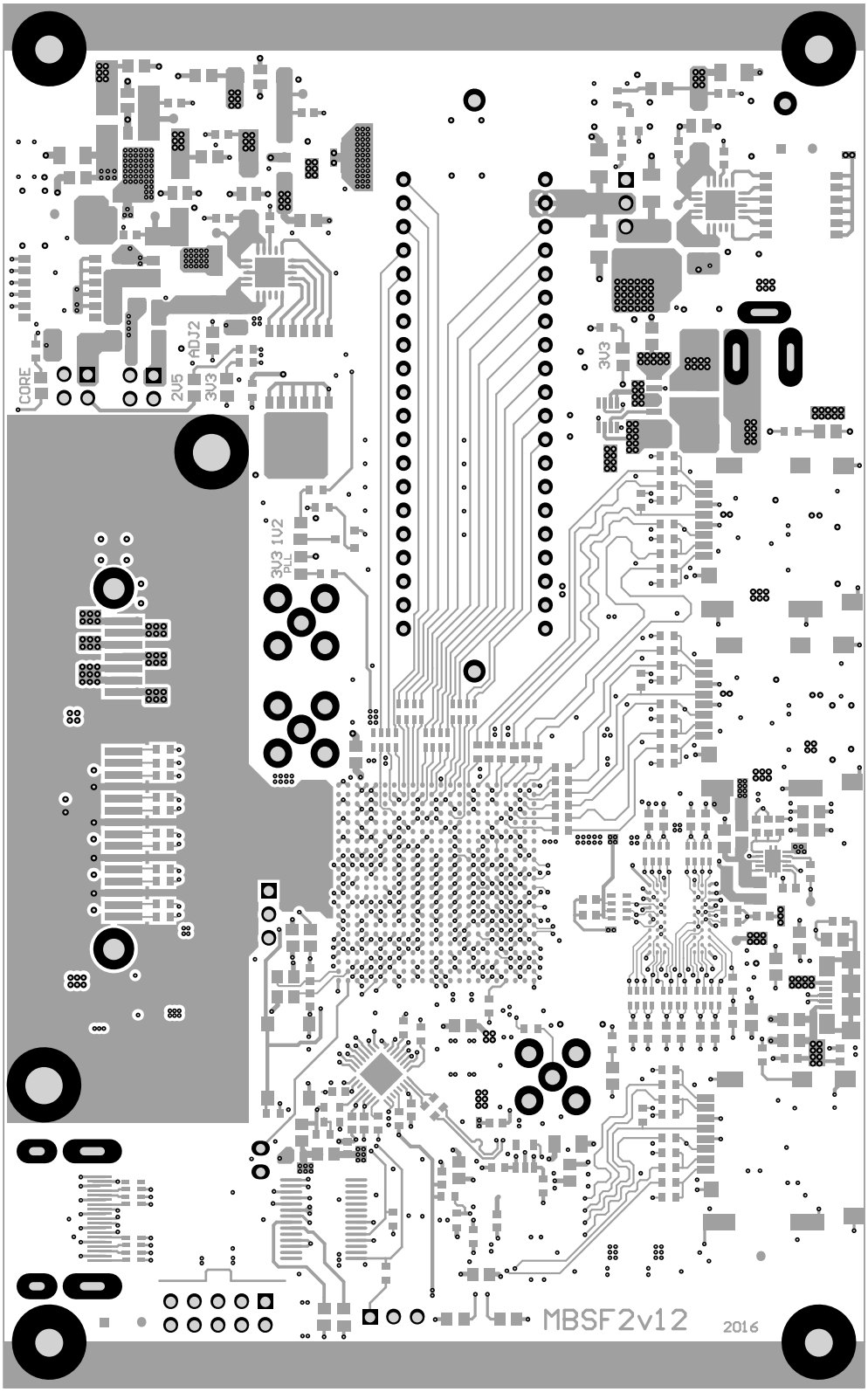

Figure 6 - 11 Mother board final artwork prints - 1. Top layer

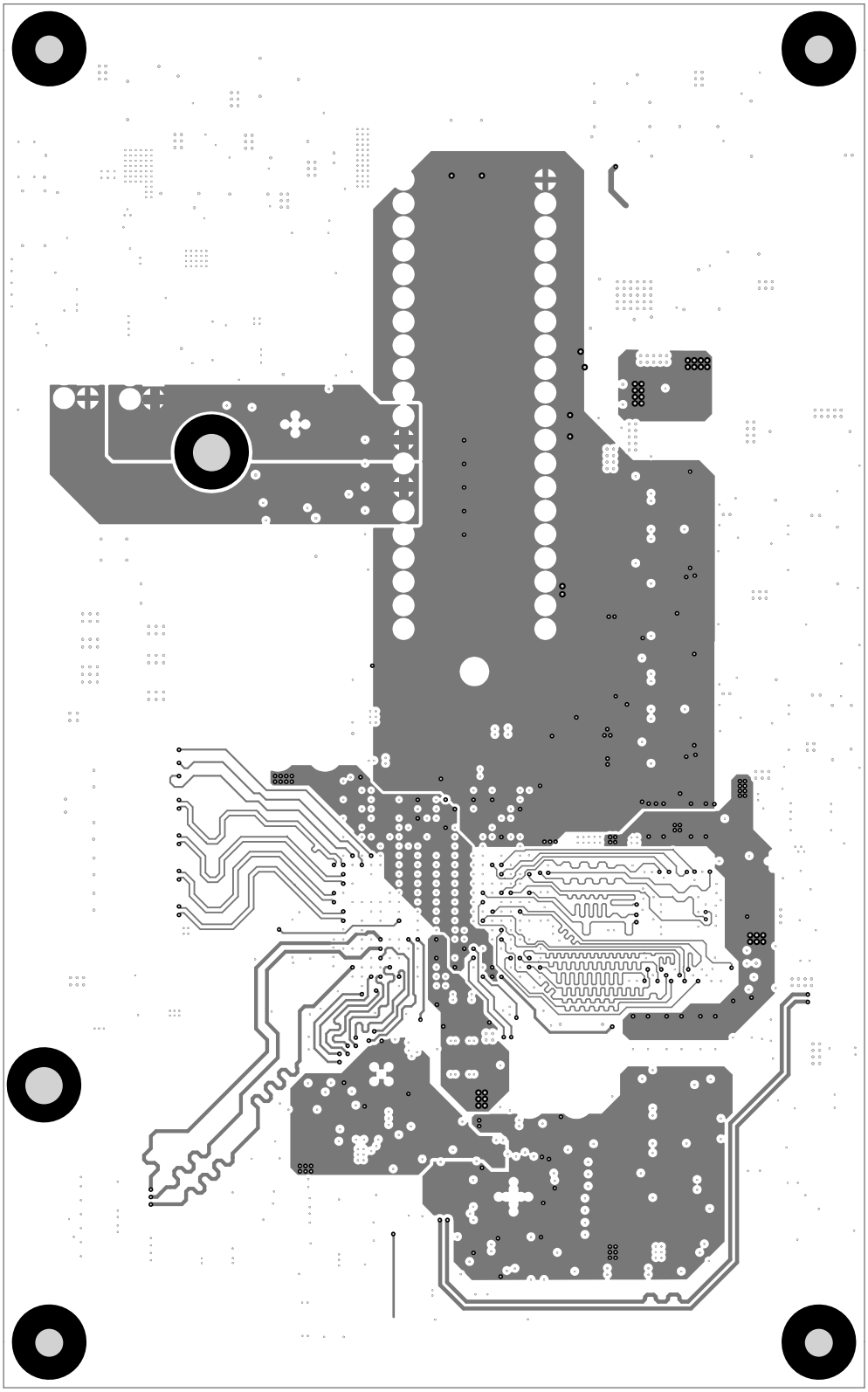

Figure 6 - 12 Mother board final artwork prints - 2. Signal layer

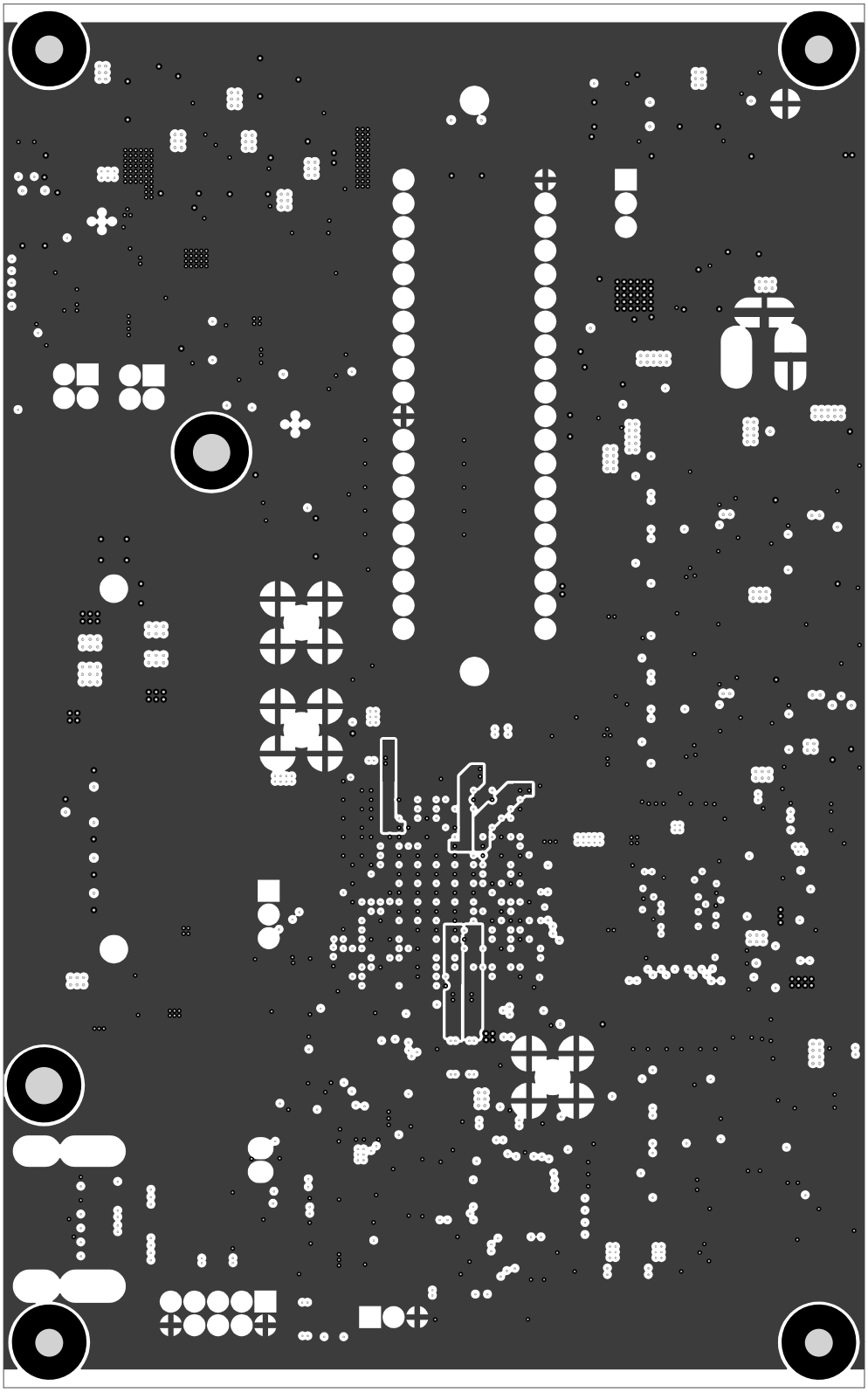

Figure 6 - 13 Mother board final artwork prints - 3. GND layer

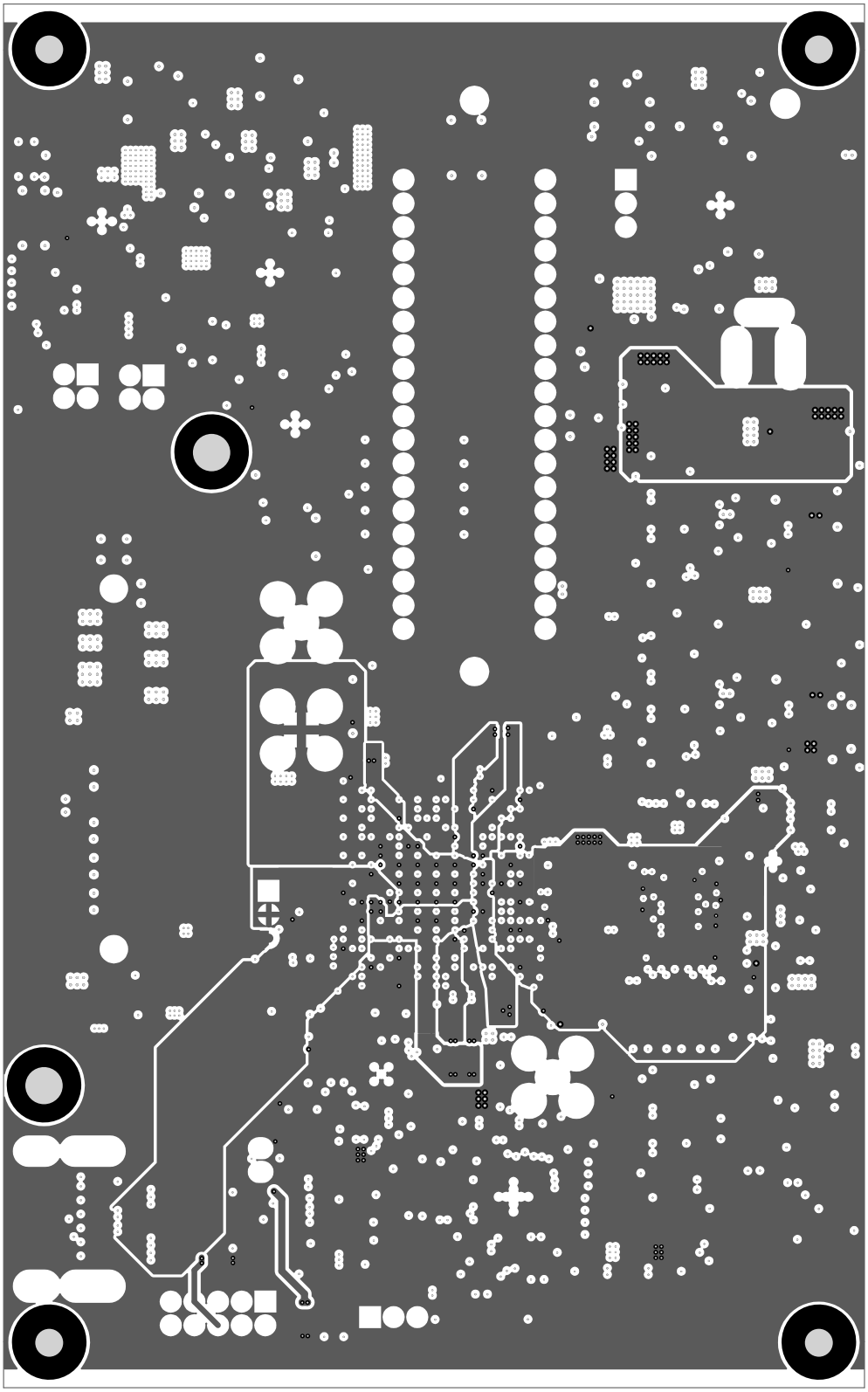

Figure 6 - 14 Mother board final artwork prints - 4. VCC layer

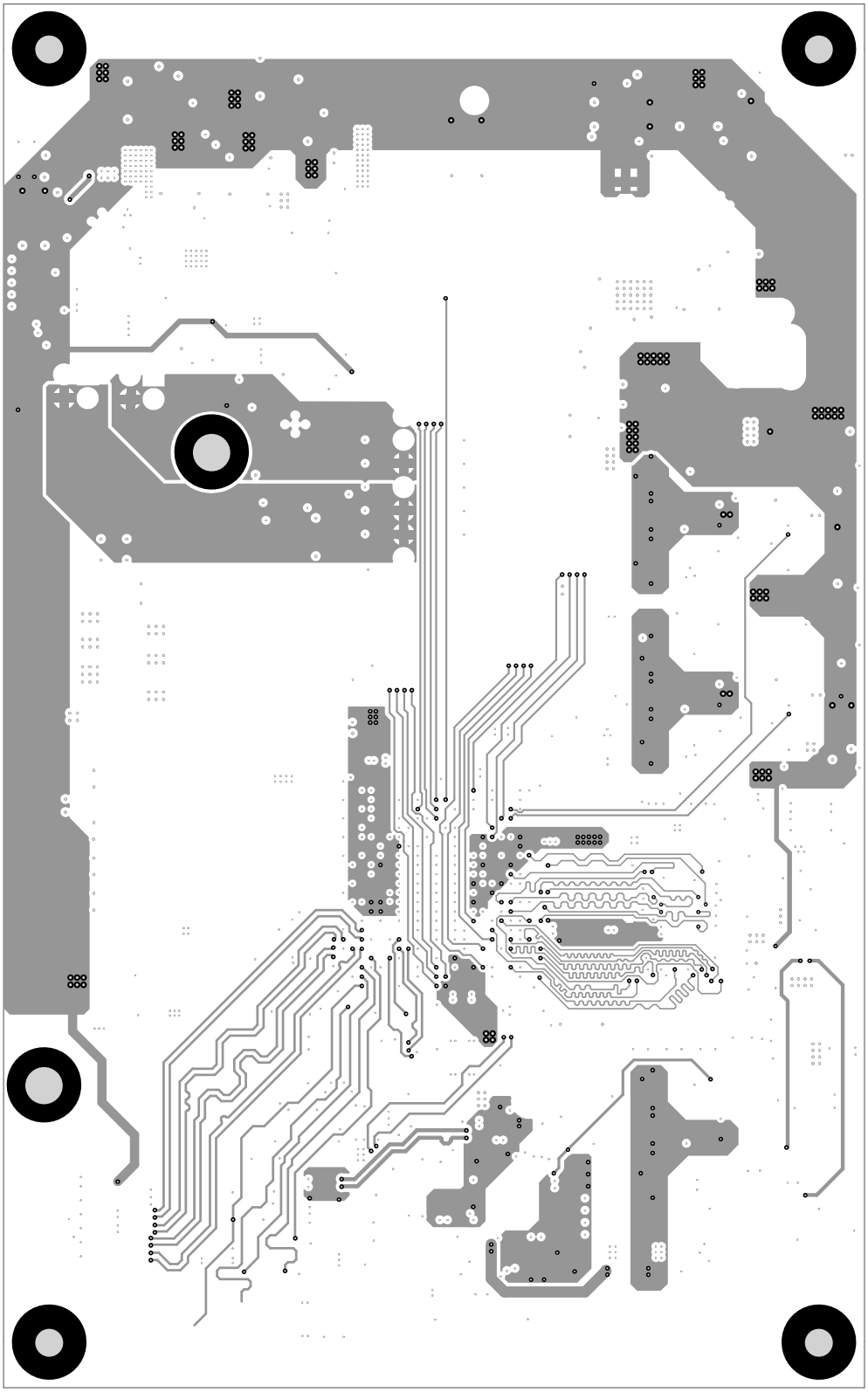

Figure 6 - 15 Mother board final artwork prints - 5. Signal layer

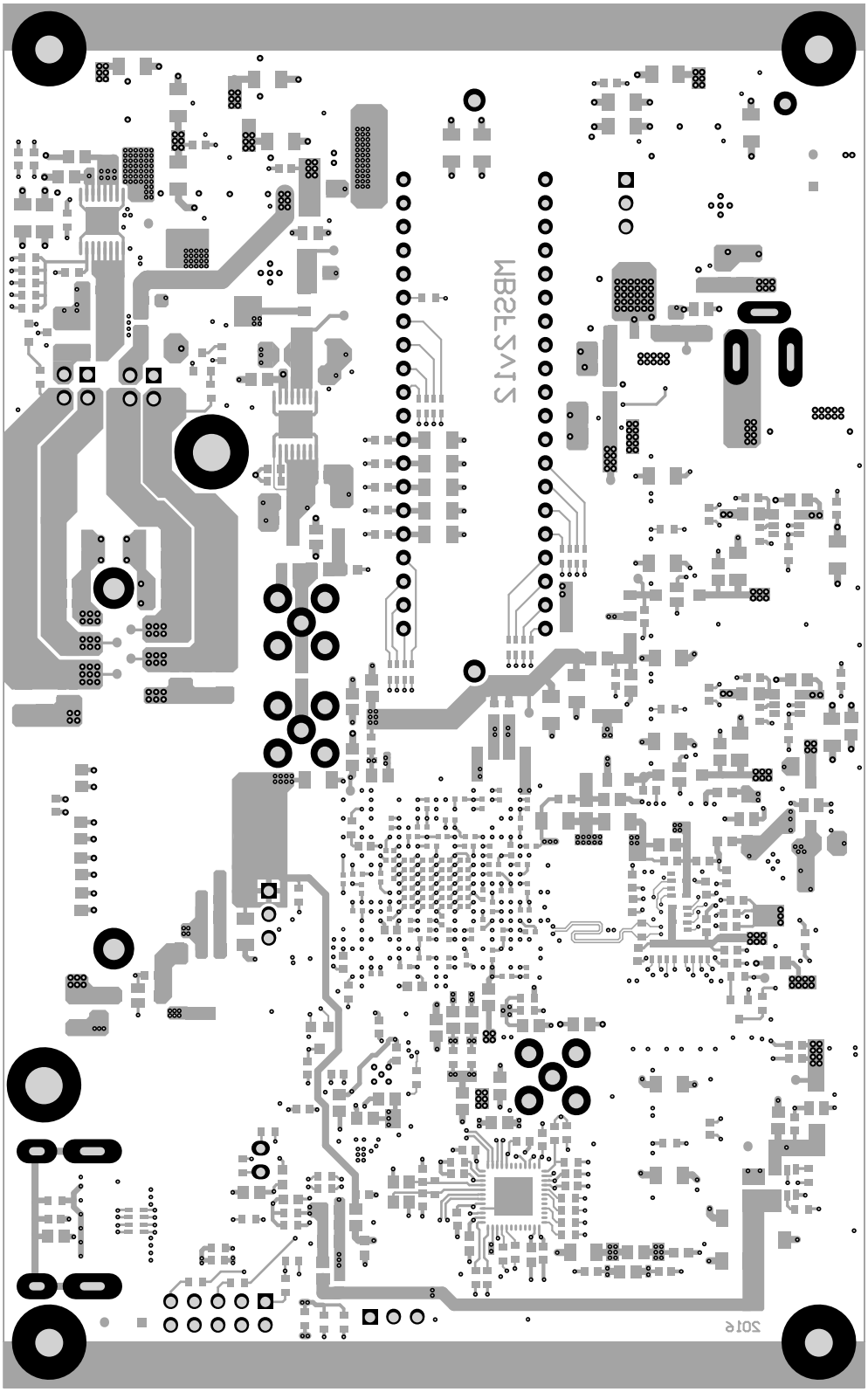

Figure 6 - 16 Mother board final artwork prints - 5. Signal layer

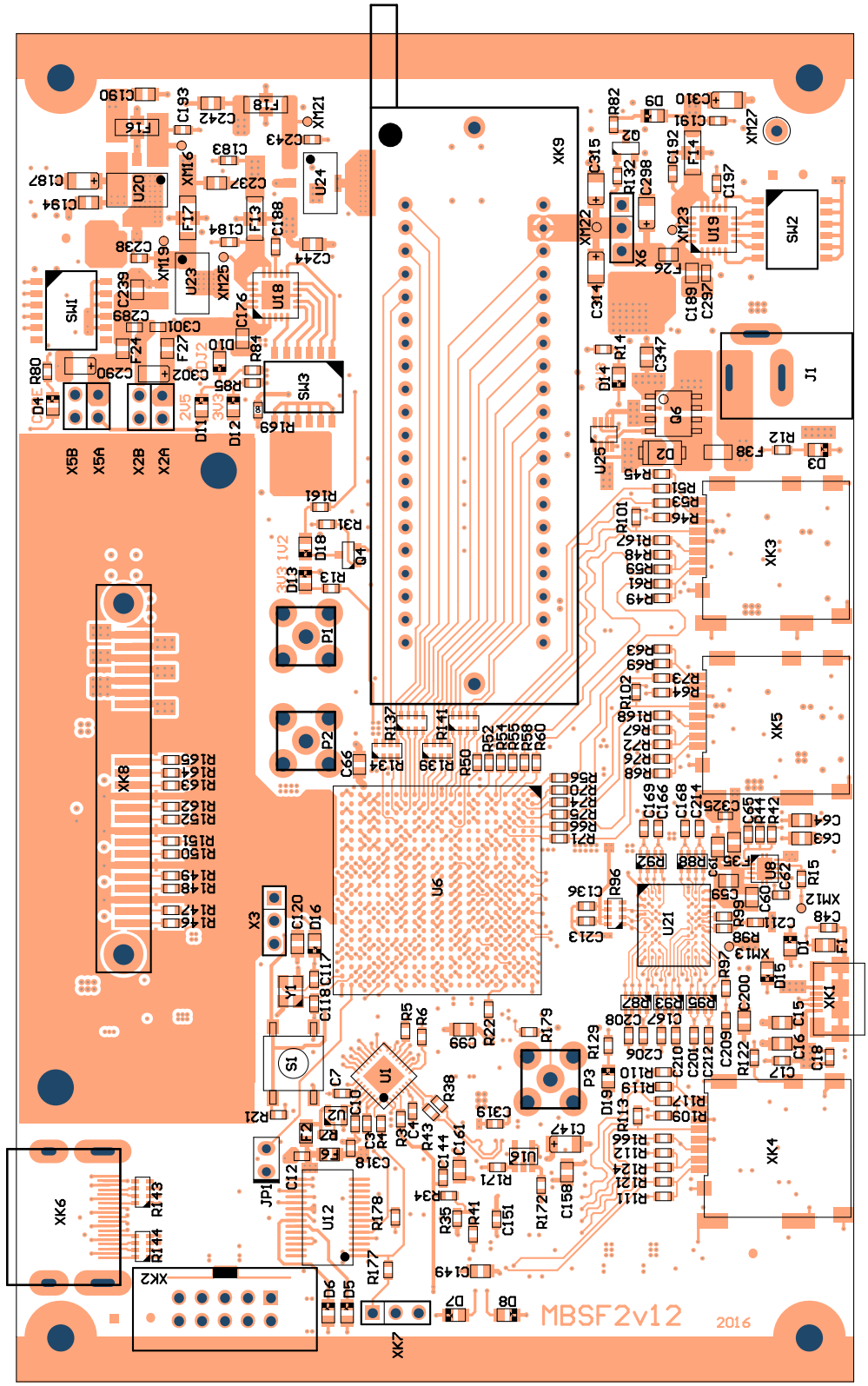

Figure 6 - 17 Mother board composite drawing - Top layer

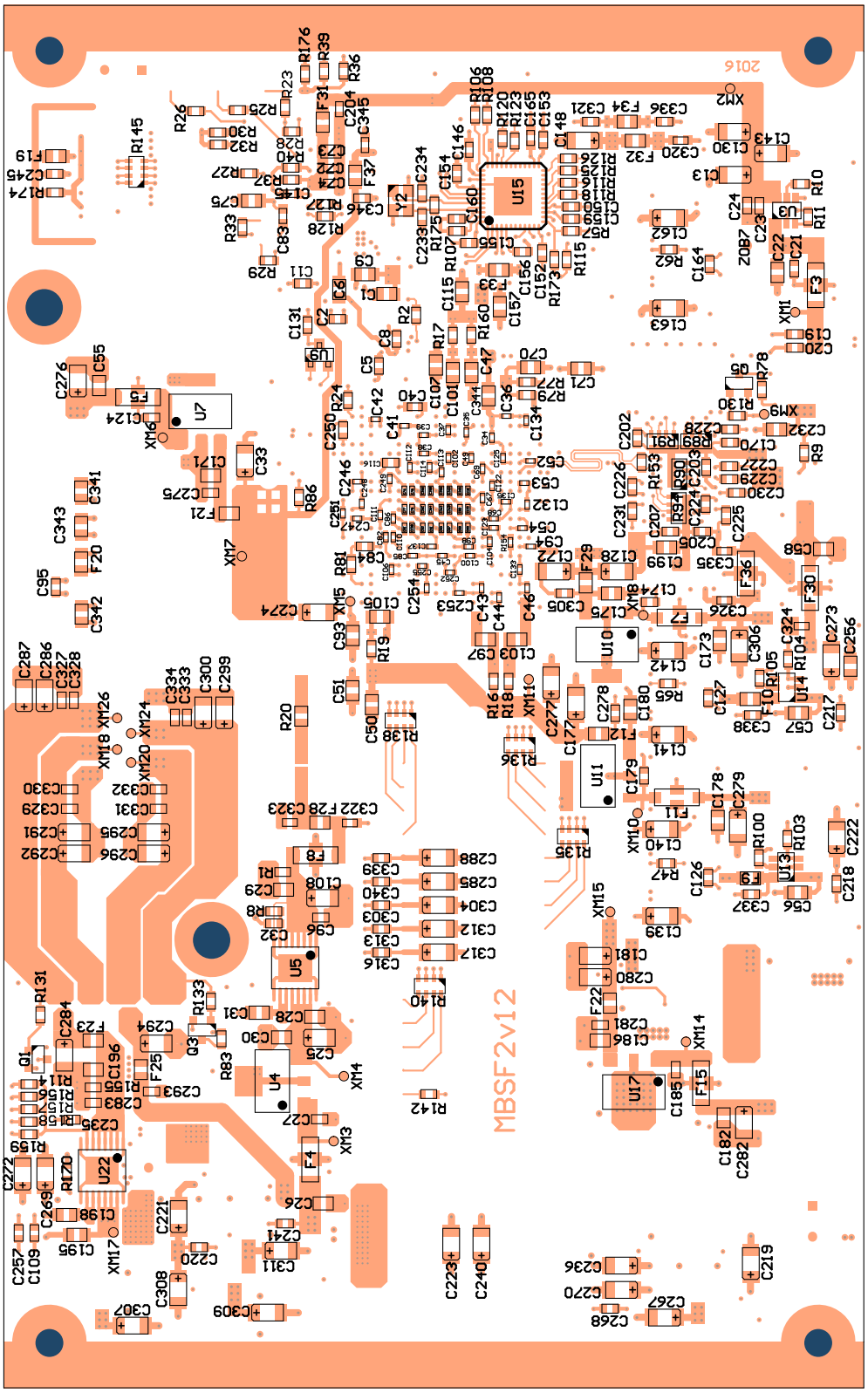

Figure 6 - 18 Mother board composite drawing - Bottom layer

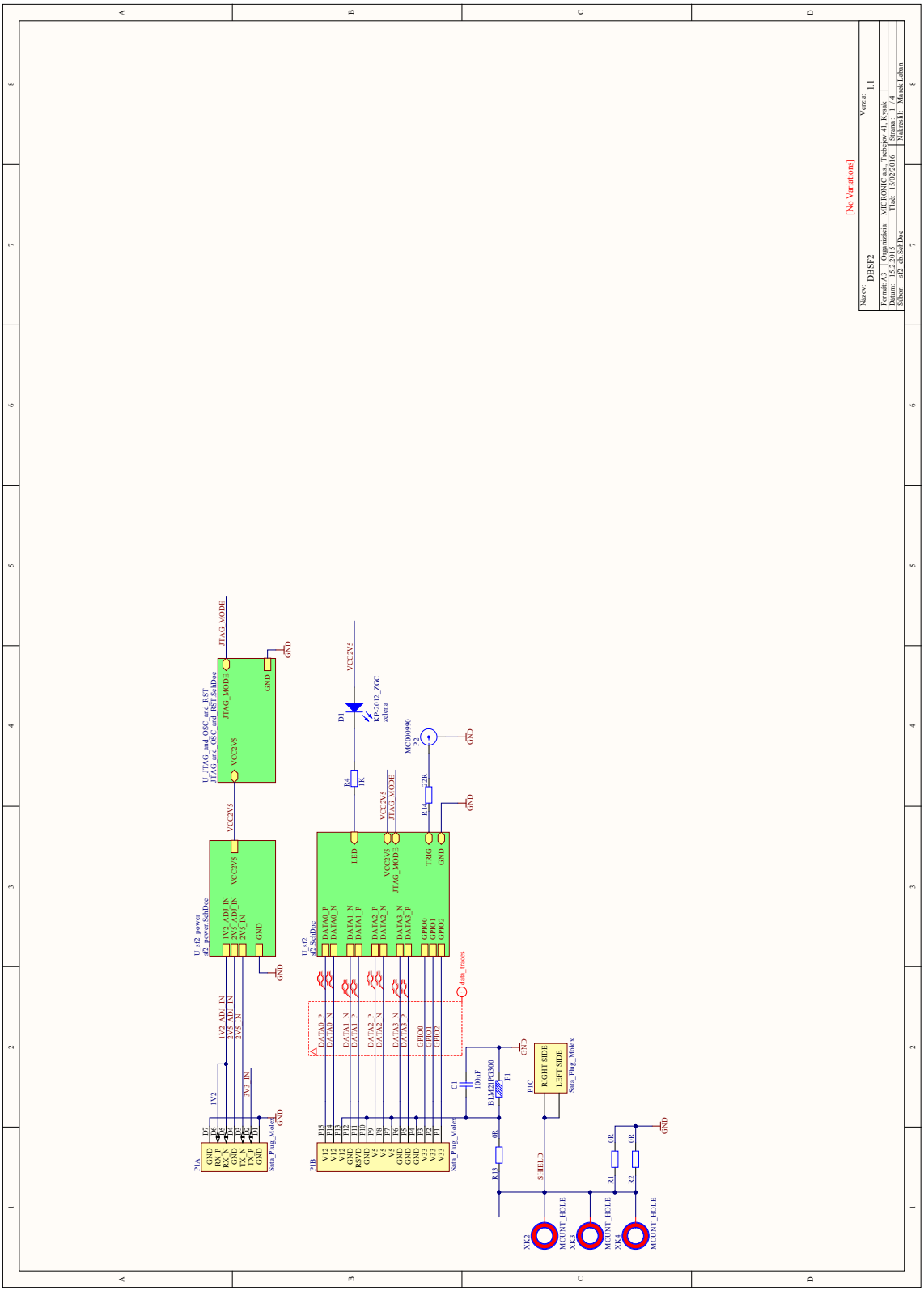

Figure 6 - 19 Schematic of daughter board SF2 page 1/4

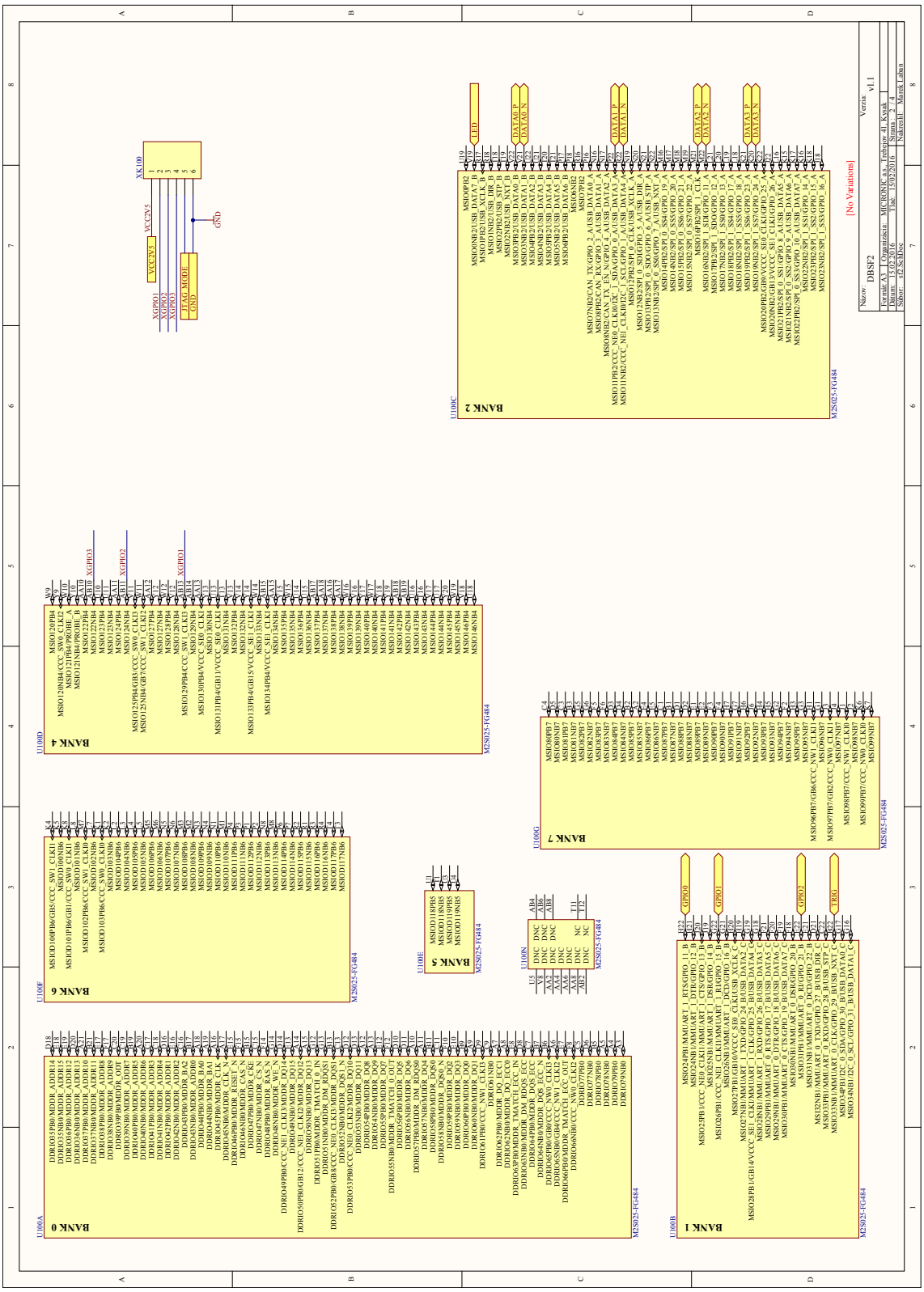

Figure 6 - 20 Schematic of daughter board SF2 page 2/4

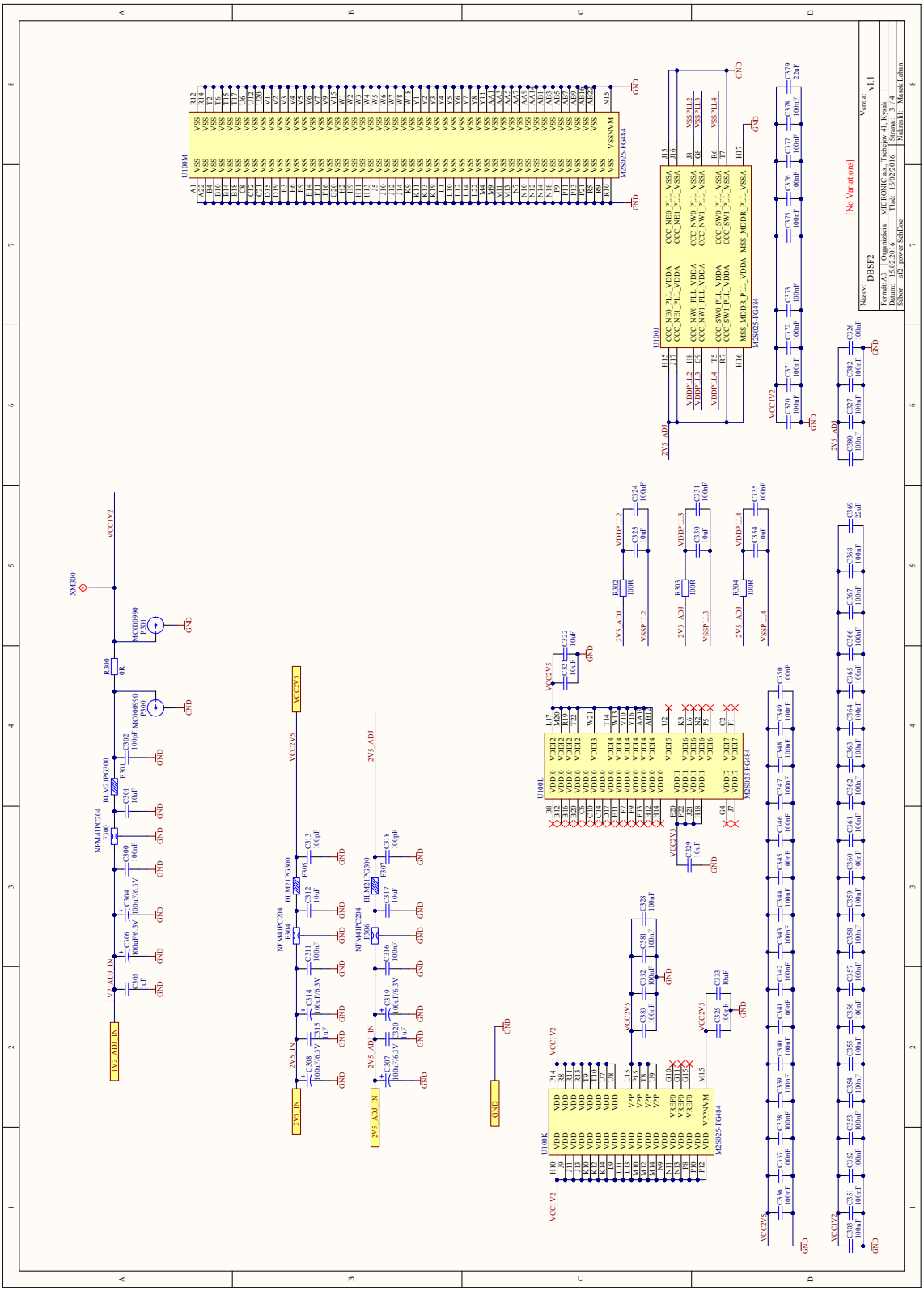

Figure 6 - 21 Schematic of daughter board SF2 page 3/4

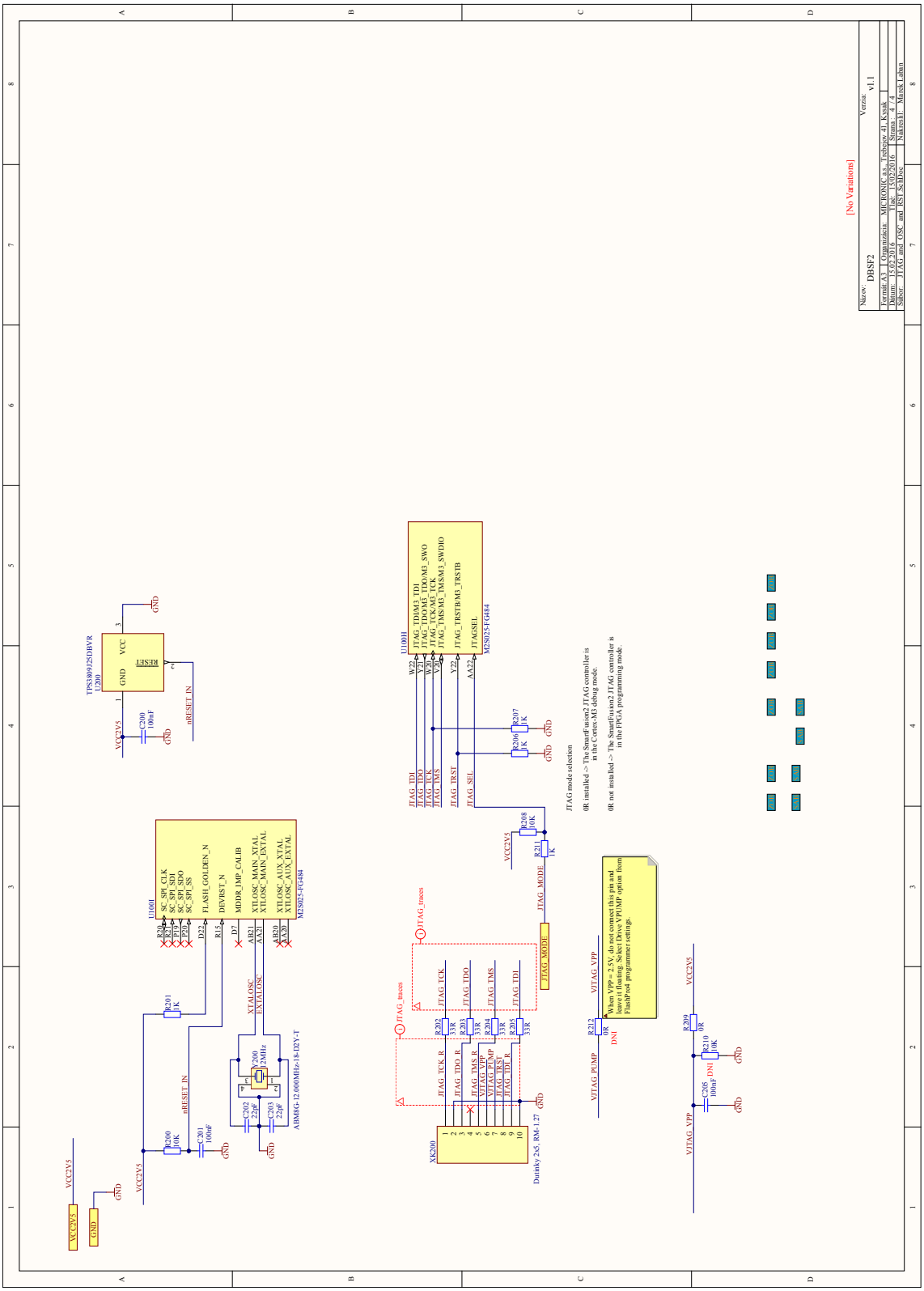

Figure 6 - 22 Schematic of daughter board SF2 page 4/4

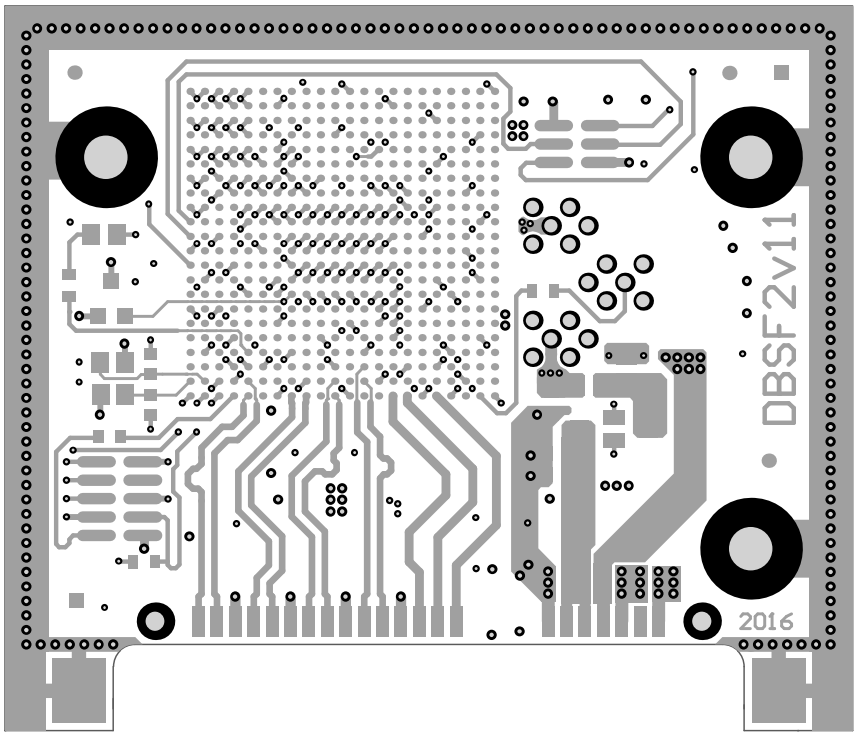

Figure 6 - 23 Daughter board SF2 final artwork prints - 1. Top layer

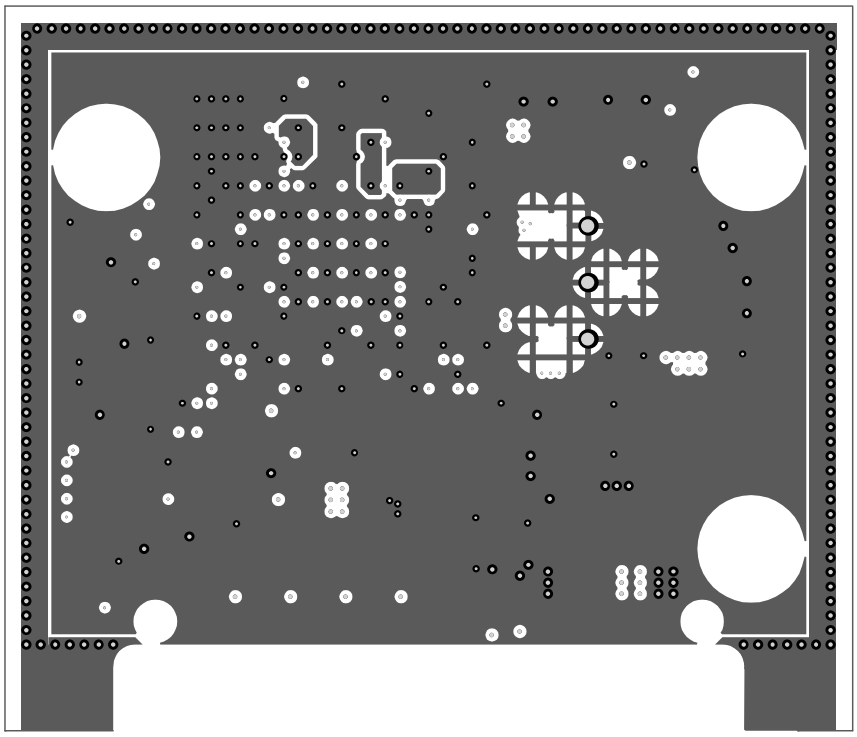

Figure 6 - 24 Daughter board SF2 final artwork prints - 2. GND layer

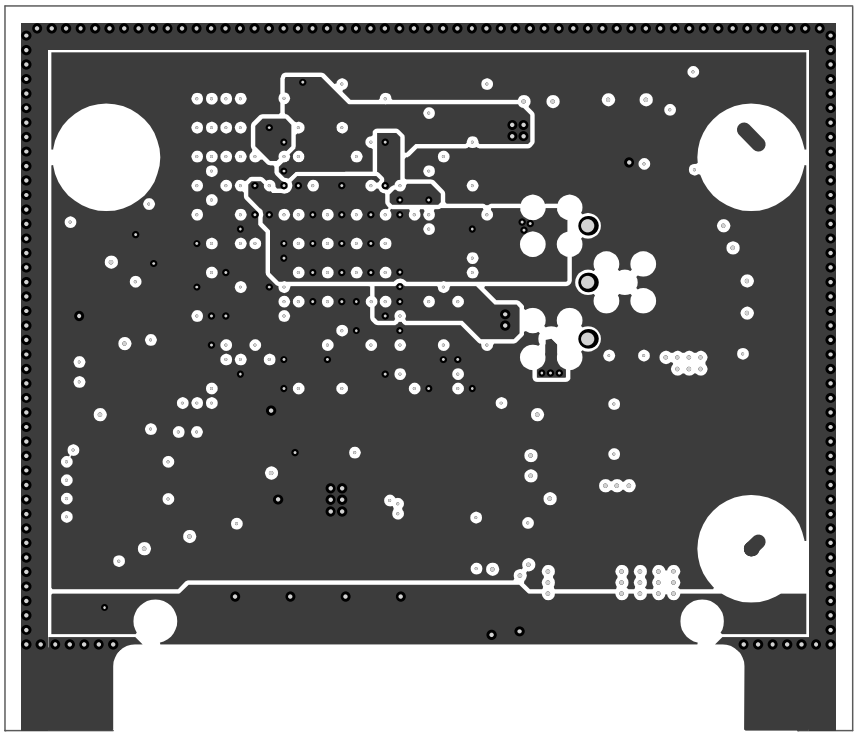

Figure 6 - 25 Daughter board SF2 artwork prints - 3. VCC layer

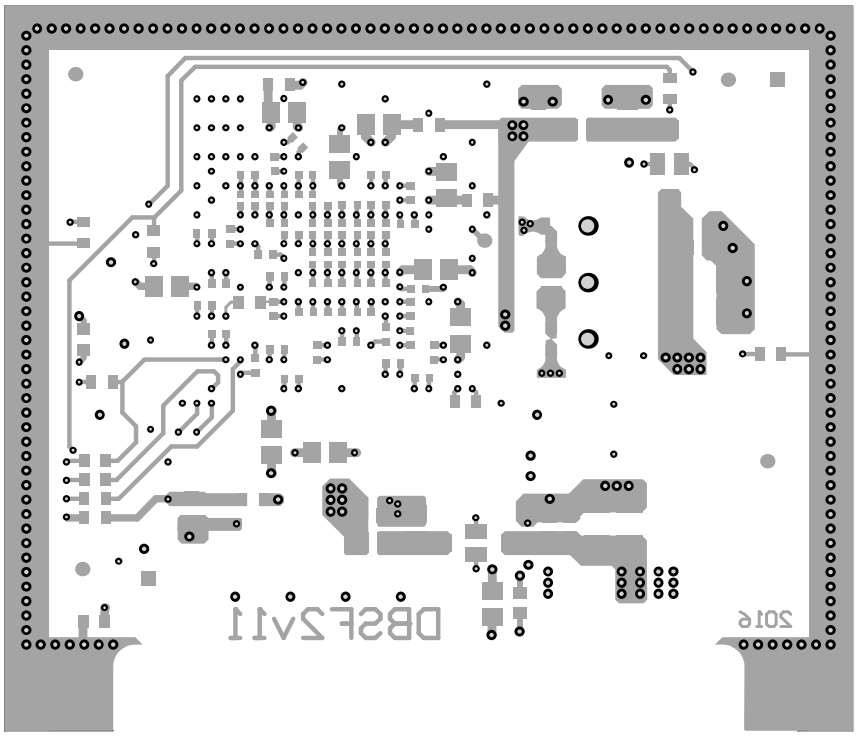

Figure 6 - 26 Daughter board SF2 artwork prints - 4. Bottom layer

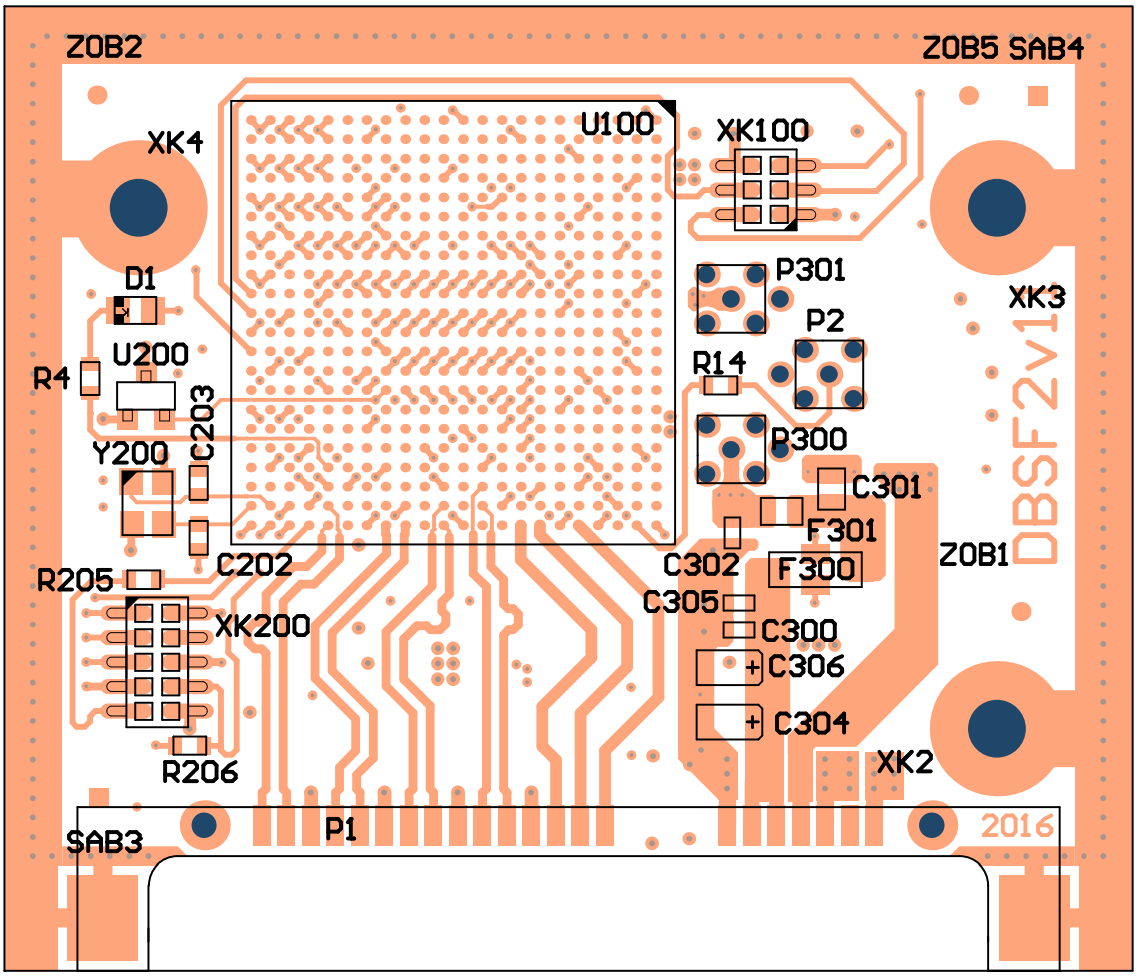

Figure 6 - 27 Daughter board SF2 composite drawing - Top layer

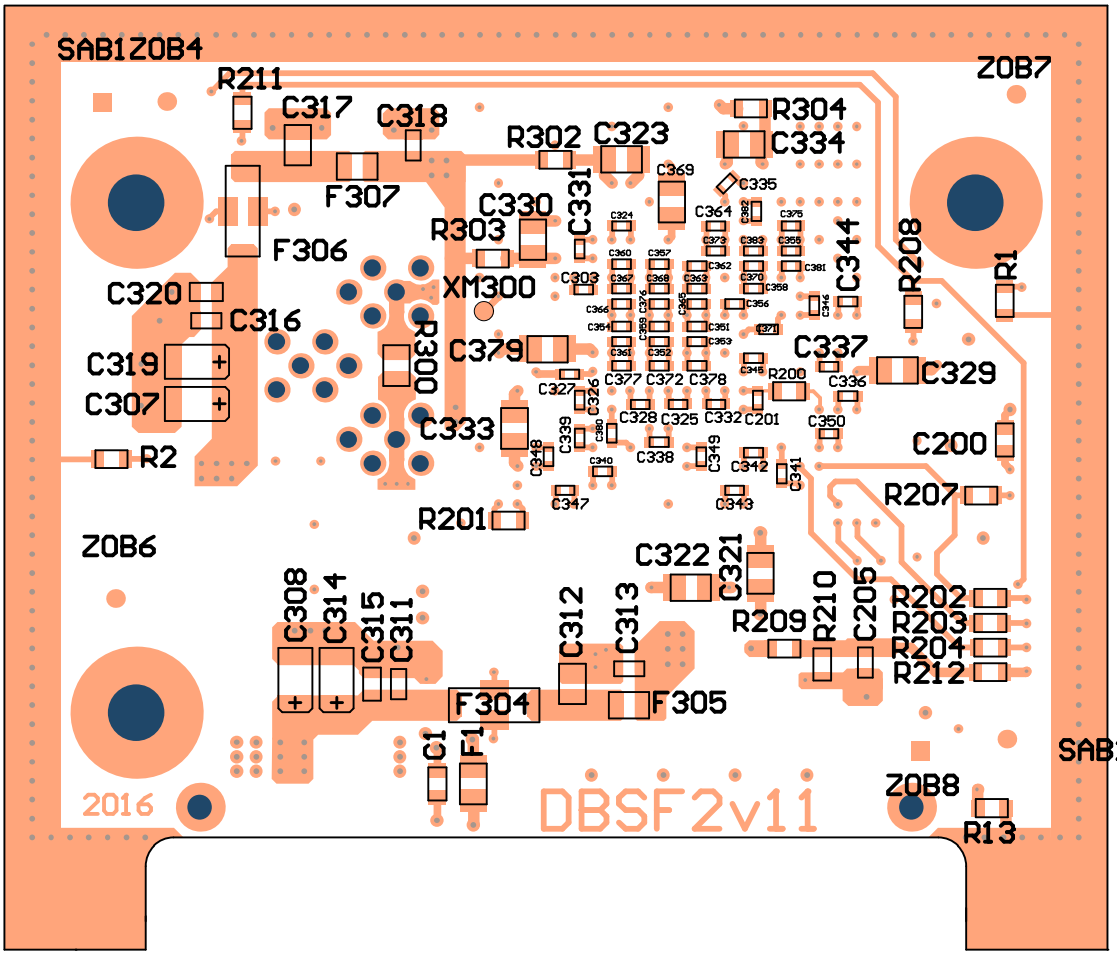

Figure 6 - 28 Daughter board SF2 composite drawing - Bottom layer

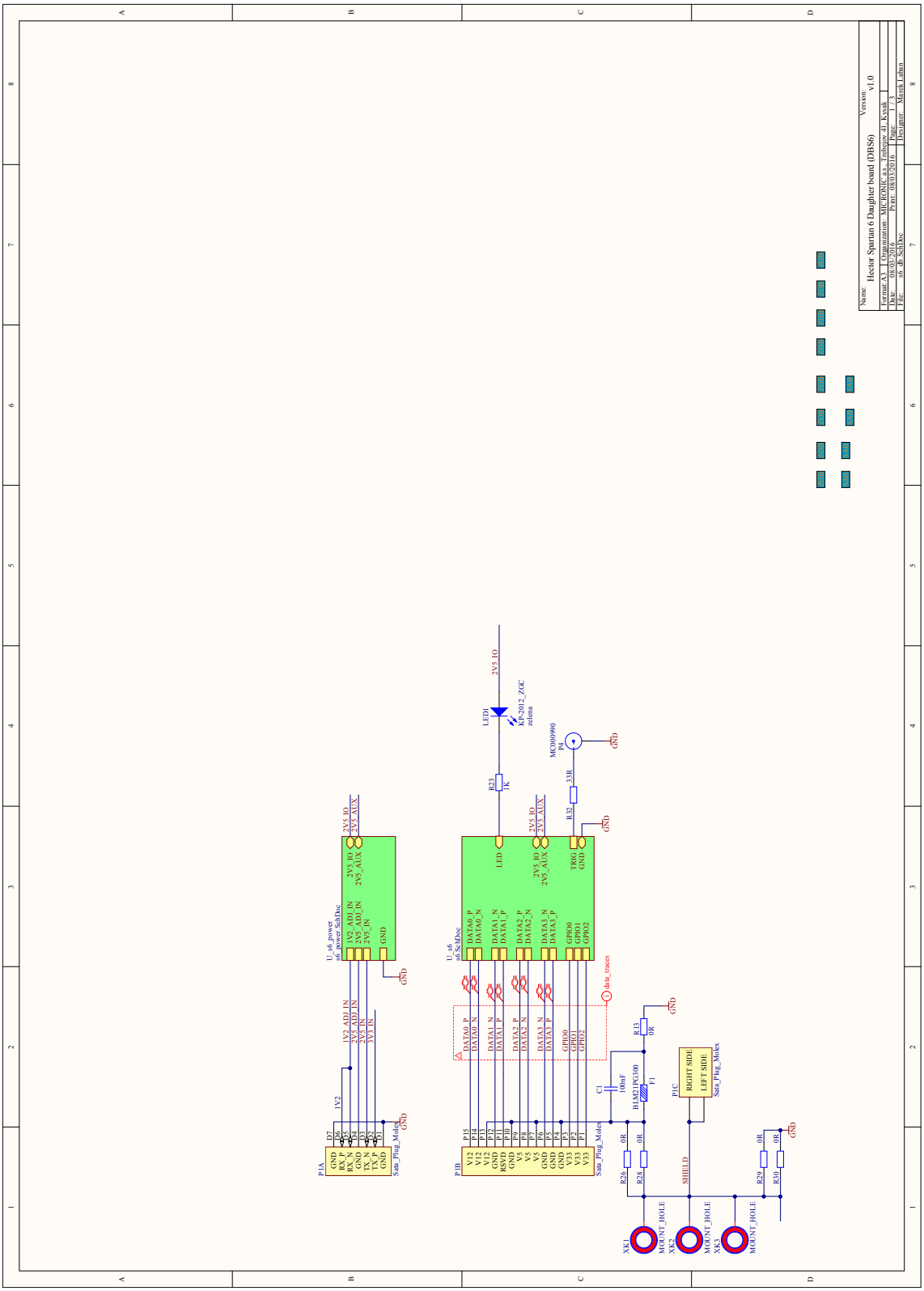

Figure 6 - 29 Schematic of daughter board S6 page 1/3

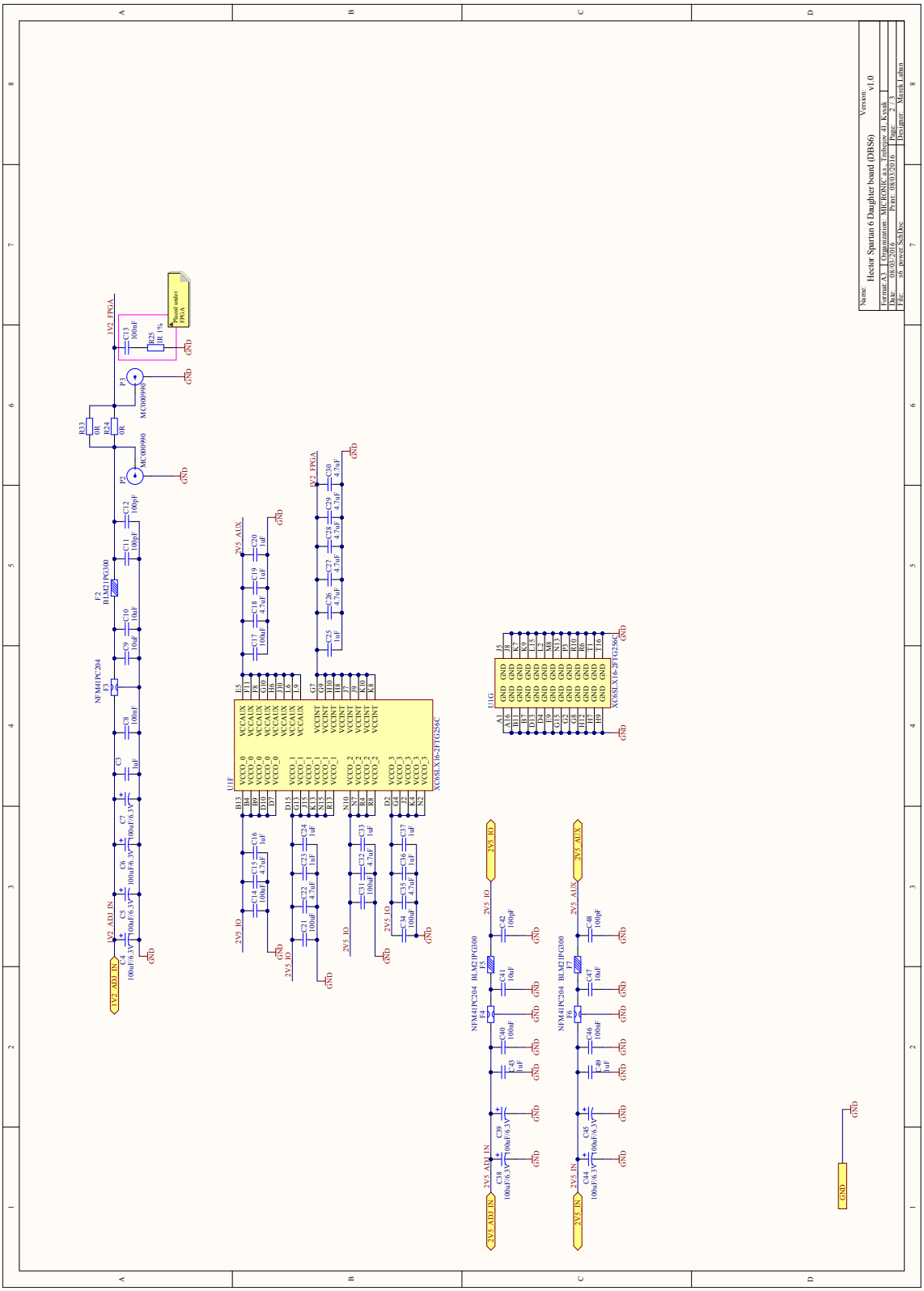

Figure 6 - 30 Schematic of daughter board S6 page 2/3

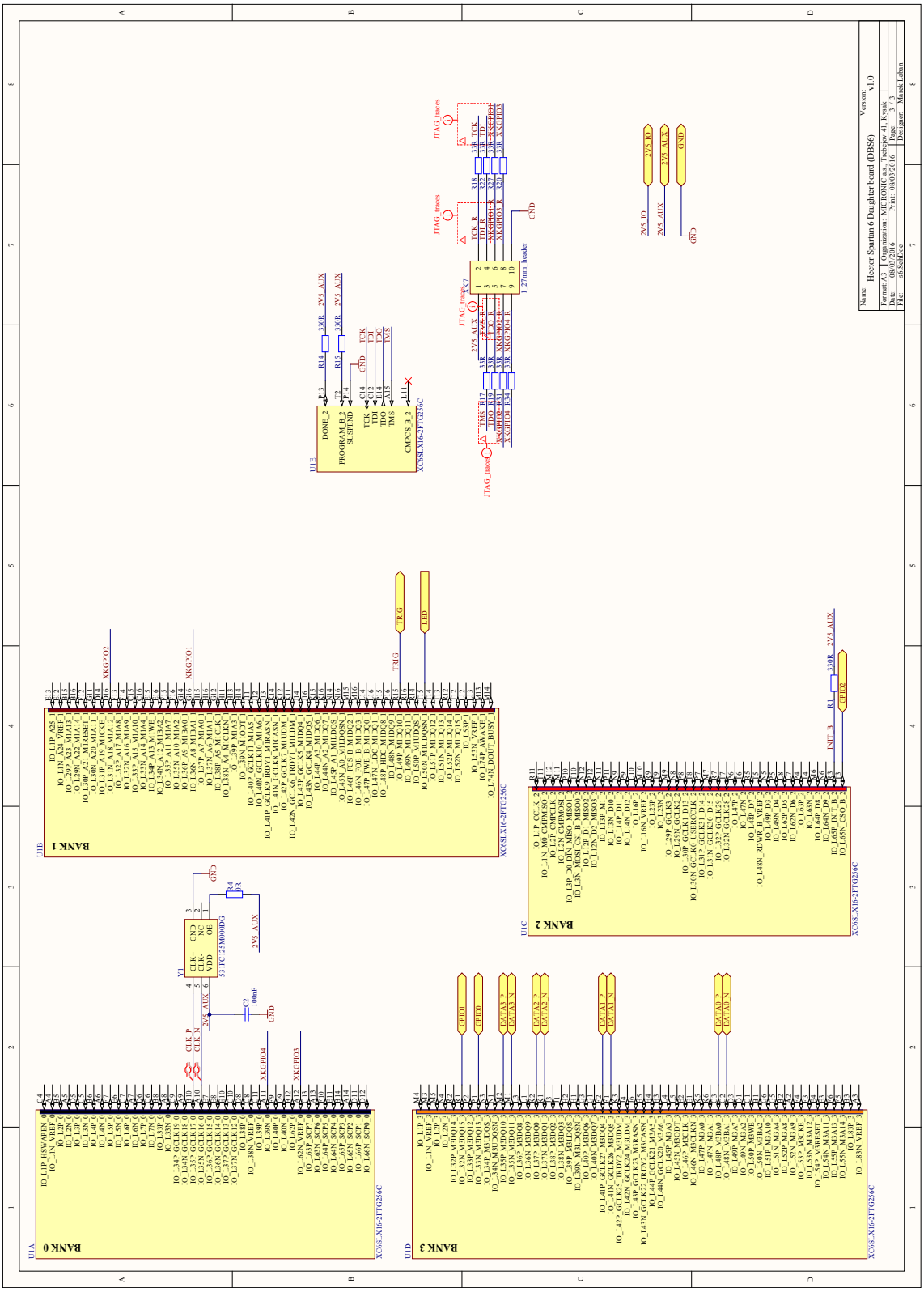

Figure 6 - 31 Schematic of daughter board S6 page 3/3

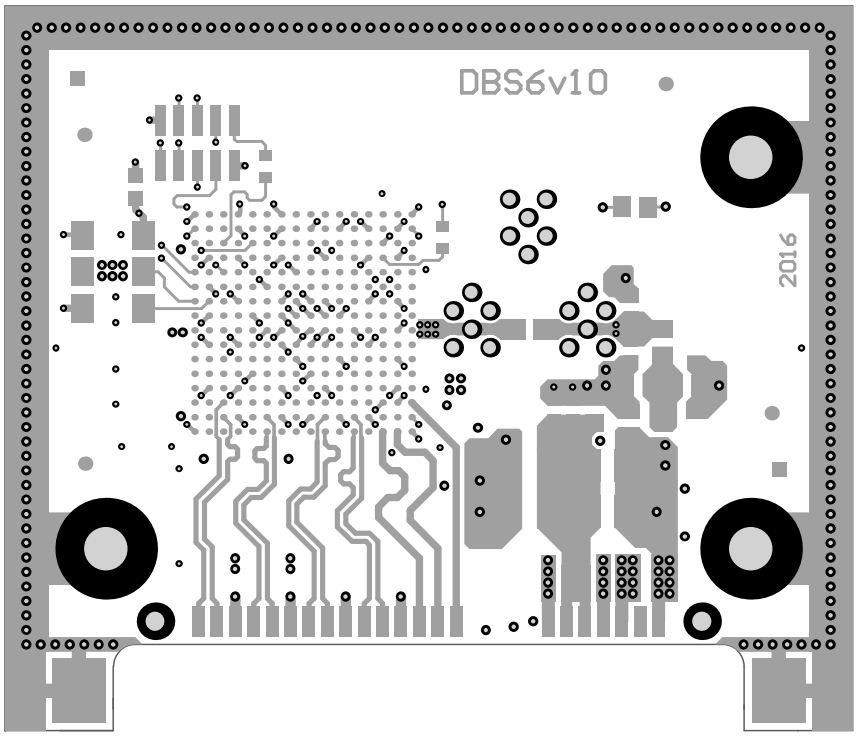

Figure 6 - 32 Daughter board S6 final artwork prints - 1. Top layer

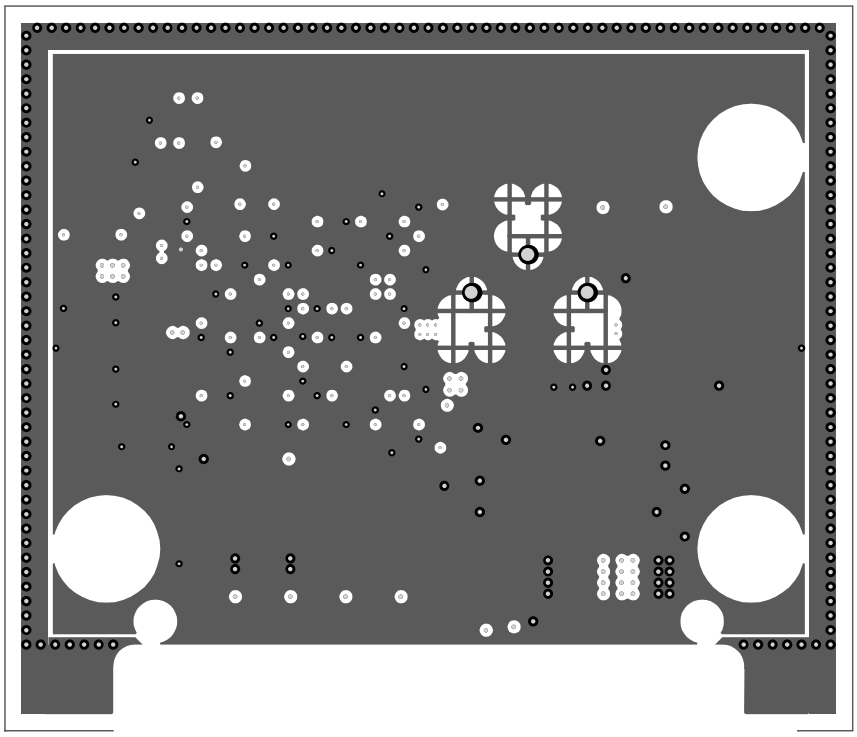

Figure 6 - 33 Daughter board S6 final artwork prints - 2. GND layer

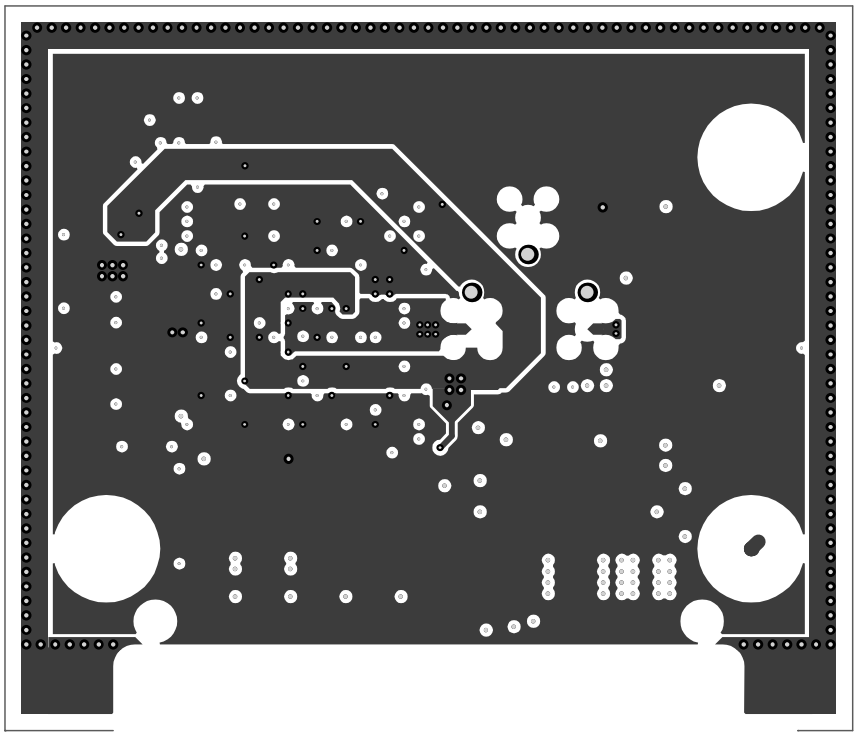

Figure 6 - 34 Daughter board S6 artwork prints - 3. VCC layer

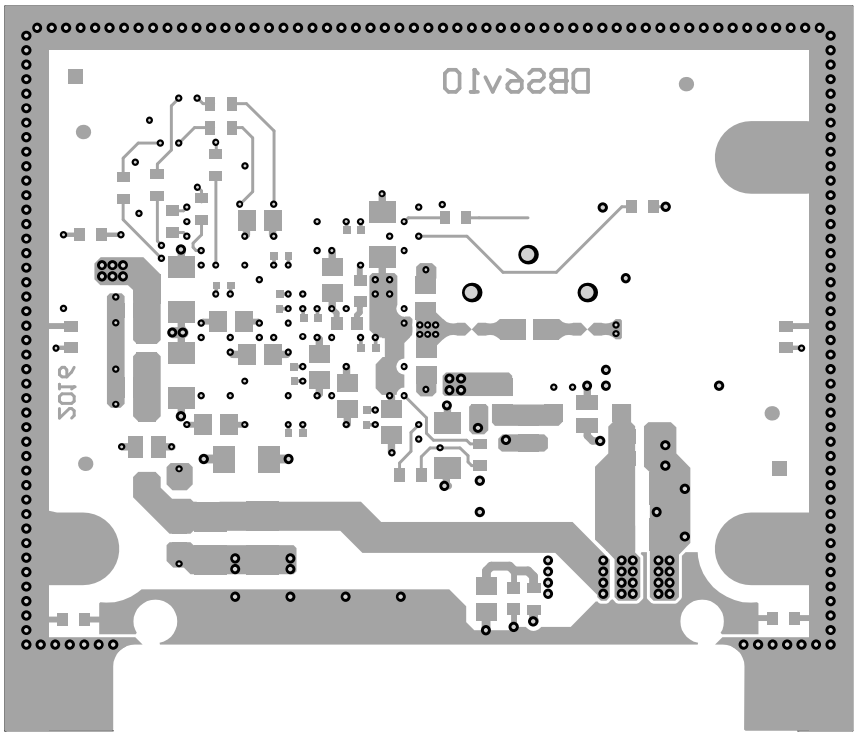

Figure 6 - 35 Daughter board S6 artwork prints - 4. Bottom layer

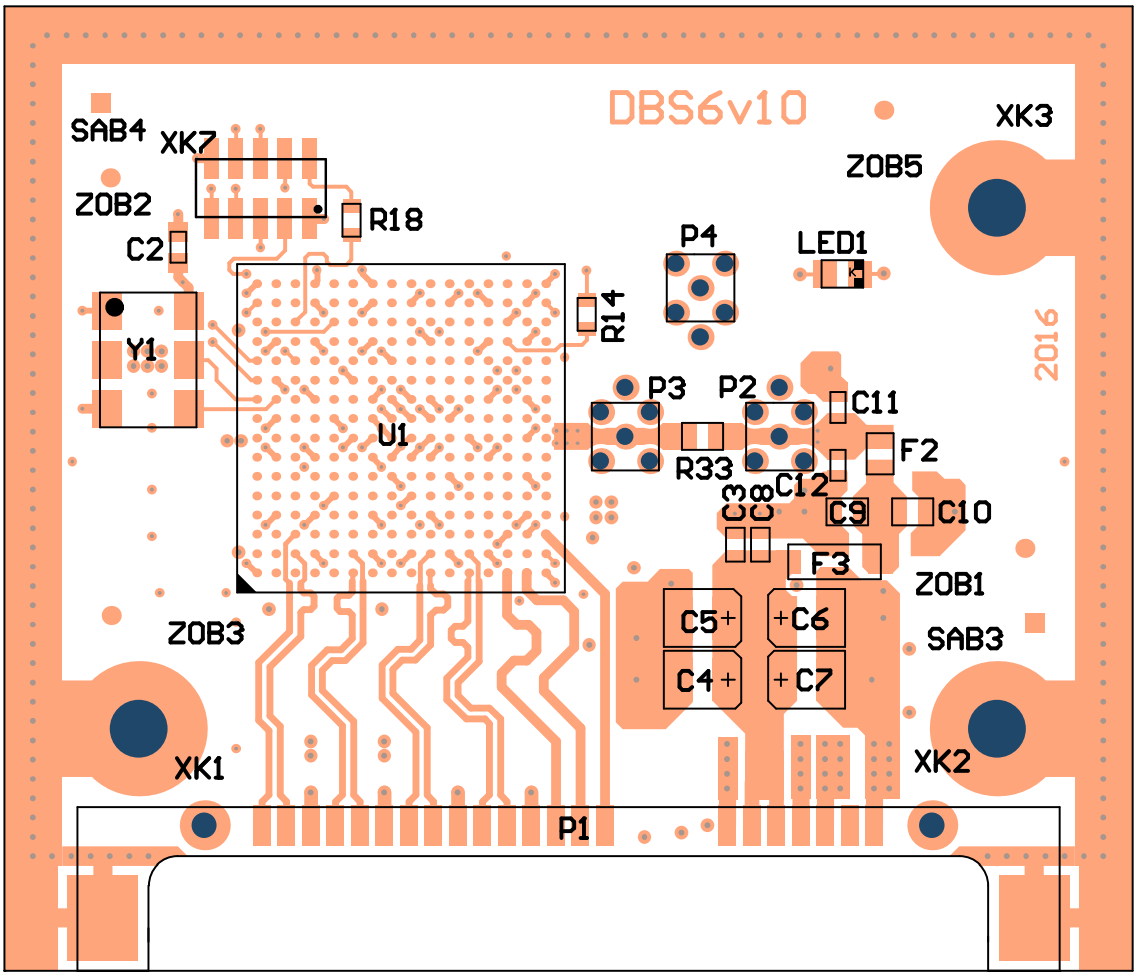

Figure 6 - 36 Daughter board S6 composite drawing - Top layer

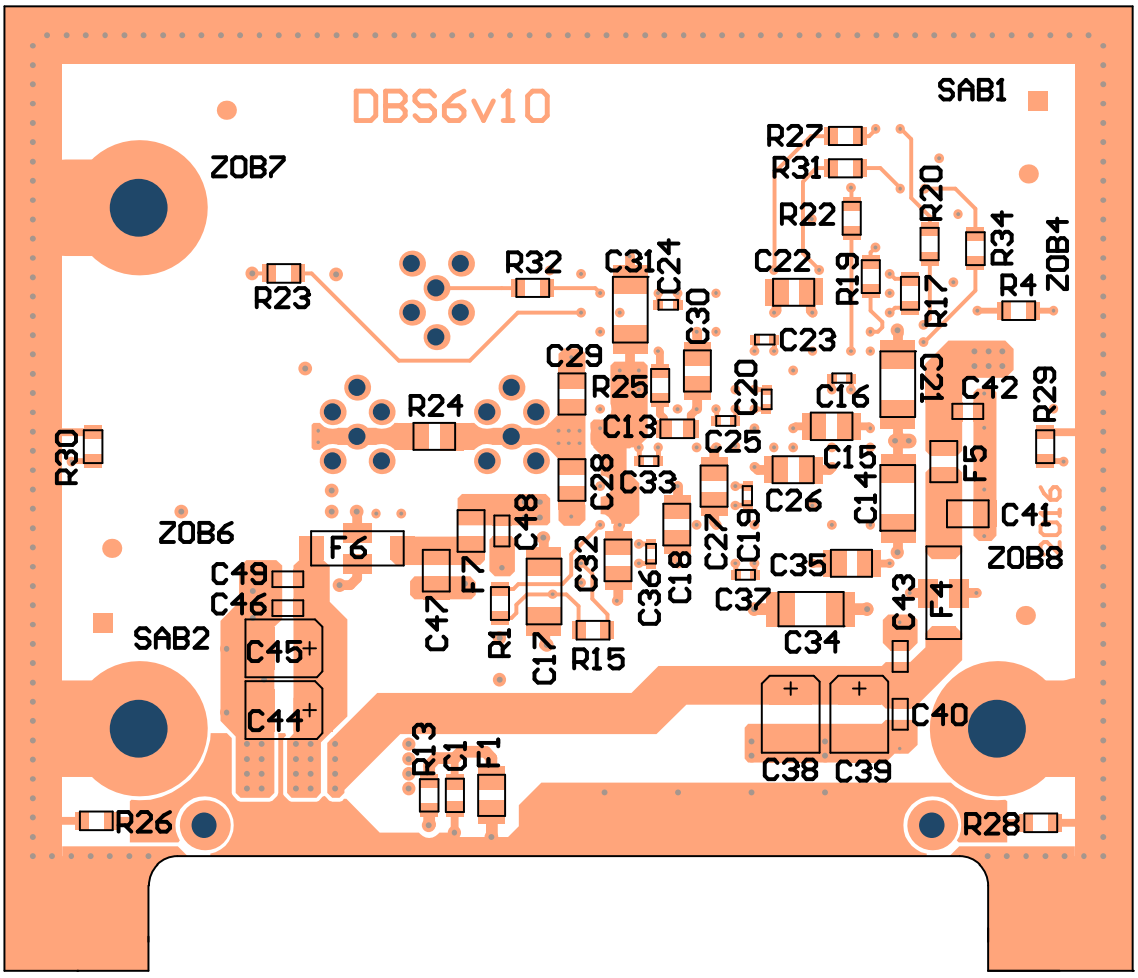

Figure 6 - 37 Daughter board S6 composite drawing - Bottom layer