EDRICO - Educational DHBW RISC-V Core

Semester Paper

from the Course of Studies Electrical Engineering

at the Cooperative State University Baden-Württemberg Ravensburg

by

Levi-Pascal Bohnacker, Noah Wölki

June 2021

Time of Project	31 Weeks
Student ID, Course	6818486, 5040009, TEN18
Reviewer	Prof. Dr. Ralf Gessler

Author's declaration

Hereby we solemnly declare:

1. that this Semester Paper , titled *EDRICO - Educational DHBW RISC-V Core* is entirely the product of our own scholarly work, unless otherwise indicated in the text or references, or acknowledged below;
2. we have indicated the thoughts adopted directly or indirectly from other sources at the appropriate places within the document;
3. this Semester Paper has not been submitted either in whole or part, for a degree at this or any other university or institution;
4. we have not published this Semester Paper in the past;
5. the printed version is equivalent to the submitted electronic one.

We are aware that a dishonest declaration will entail legal consequences.

Friedrichshafen, June 2021

Levi-Pascal Bohnacker, Noah Wölki

Contents

Acronyms

AXI	Advanced Extensible Interface
ALU	Arithmetic Logical Unit
CPI	Cycles per Instruction
CSR	Control and Status Register
CU	Control Unit
CPI	Cycles per Instructions
PaR	Place and Route
FPGA	Field Programmable Gate Array
FSM	Finite State Machine
GPR	General Purpose Register
IP	Intellectual Property
ISA	Instruction Set Architecture
ISR	Interrupt Service Routine
PC	Programm Counter
PMP	Physical Memory Protection
PMA	Physical Memory Attributes
RF	Register File
RISC	Reduced Instruction Set Computer
RV32I	RISC-V 32-Bit Integer
SISD	Single Instruction Single Data
VHDL	Very High Speed Integrated Circuit Hardware Description Language
IP	Interlectual Property
RAM	Random Access Memory
ROM	Read Only Memory
RTL	Register Transfer Level
IR	Instruction Register
JALR	Jump and Link Register
EDRICO	Educational DHBW RISC-V Core
EDVAC	Electornic Discrete Variable Automatic Computer
ENIAC	Electronic Numerical Integrator and Computer
MIPS	Microprocessor without Interlocked Pipelined Stages
PCIe	Peripheral Component Interconnect Express
CAN	Controller Area Network
ARM	Advanced RISC Machines
AMBA	Advanced Microcontrol Bus Architecture
AXI4-Lite	Advanced eXtensible Interface 4 Lite
AXI	Advanced eXtensible Interface
MIE	Machine Interrupt Enable
MPP	Machine Previous Privilege
SPP	Supervisor Previous Privilege
PMP	Physical Memory Protection
PMA	Physical Memory Attributes
TOR	Top of Range
NA4	Natural aligned four-byte region
NAPOT	Naturally aligned power-of-two region

List of Figures

List of Tables

Listings

1 Introduction

These days one of the key benchmarks for technology is processing speed and calculation power. To realize mathematical operations and execute programs, different platforms can be utilized. The most commonly used unit is the standard processor consisting of transistors realized on silicium and other materials. Another crucial technology that is gaining more attention is the so-called Field Programmable Gate Array (FPGA). The FPGA consists of logical units that can be wired and configured individually for the required use-case. The advantage of FPGA is that the speed of applications can be drastically increased since the hardware will be very optimized for the specific application. This project aims to develop a Interlectual Property (IP)-core based on the Open Source Instruction Set RISC-V. The goal is to build a reusable unit of logic that can interpret compiled C-Code. The IP core is realized in the Very High Speed Integrated Circuit Hardware Description Language (VHDL) language and will be deployed on a FPGA. IP Cores are used in every computer, phone and electronic device that requires to execute some computational function. The developers of these IP Cores are big companies like Intel, ARM or AMD. These IP Cores and Instruction Sets are strictly licensed and not available for everyone. For the development of an own IP Core the Instruction Set is the main source of information and therefore the RISC-V open-source Instruction Set is used for this project.

1.1 Motivation

RISC-V was first proposed at Berkeley University in 2010. The architecture is therefore relatively new in comparison to others like x86, ARM or SPARC. Even though its young age is already very promising, every year new breakthroughs are achieved in the field of RISC-V based cores. MicroMagic for example announced in 2020 a chip with a total CoreMark score of 13000 and an incredible 110000 Coremark/Watt. This poses a significant development and is approximately 10 times better than any CISC, RISC or MIPS implementation in terms of Performance per Watt. Many other companies like Alibaba, Nvidia and SiFive are currently increasing research on RISC-V based cores. The Motivation behind this project was to gain experience in processor and FPGA design and verification. Furthermore it poses an interesting opportunity for students to work on a new and upcoming processor architecture.

1.2 Project Planning

In order to control the flow of the project, the V-Model approach was taken. The project is therefore divided into Requirements, System Design, Architecture Design, Module Design and Implementation. After Implementation the corresponding verification phases are ready to be executed, starting from the lowest level (Unit Verification) to Integration Verification, System Verification and last but not least Acceptance Verification.

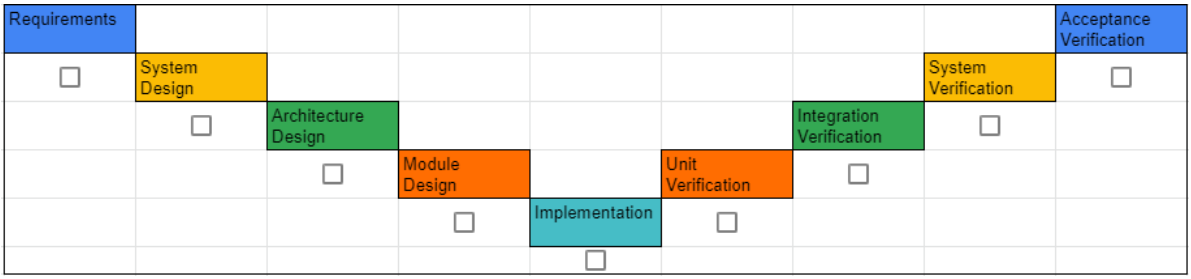

Figure 1.1: V-Model

At the beginning of every project phase, workloads were defined e.g. the definition of the Control Unit Entity. The target of Requirements Engineering was to define everything that is expected from the core and gather information about RISC-V. The data path as well as the entities of the Control Unit, Arithmetic Unit, Register Files, Exception Control, PMP & PMA Checker and AXI4-Lite Interfaces as well as a short summary of their function were defined during System Design. The next step, Architecture Design, aimed to further specify the entities mentioned above and sub-divide them into several entities. Module Design will be executed to define every single architecture, after that implementation and testing may start.

1.3 History

The history of computing is a very complex topic, it goes back to ancient times where mathematicians used simple mechanical devices such as the abacus. An abacus is usually comprised of a frame and multiple rods with pearls mounted on them. Unlike modern computation devices, it does not calculate on its own but is used to provide an overview of the calculations (e.g. the sum and carry)**ORegan:2021**. The following section will give a short overview of the history of computational devices.
The Zuse Z1, often referred to as the first computer, was invented and build by Conrad Zuse in 1938. Despite the fact that it was a mechanical computer, the Zuse Z1 was able to perform several arithmetic operations including floating point arithmetic. Later developments of the Z1 are the Z2 and Z3. The Z3 relied on relays and was therefore not

fully digital. As the first programmable computer the Z3 marks a milestone in the history of computational devices**ORegan:2021**.

Developed by the University of Pennsylvania in cooperation with the Ballistics Research Laboratory of the US Army, Electronic Numerical Integrator and Computer (ENIAC) can be seen as one of the first large scale computers (completed in 1946). It was fully digital, using vacuum tubes. Complex computations such as thirty five 10-digit divisions can be carried out in one second using ENIAC. Reprogramming the machine needed a great deal of effort, since it did not employ the stored-program concept. Its successor the Electornic Discrete Variable Automatic Computer (EDVAC) added this functionality to the design **ORegan:2021**. A major milestone is marked by the invention of the transistor in 1947 (Bardeen and Brattan, point-contact transistor) and the junction-based transistor in 1951 by Shockley **ORegan:2021**. These inventions allowed computers to decrease drastically in size, power and meantime to failure.

With the Intel 4004 the first ever microprocessor was invented in 1971. It was able to run at a speed of 60000 operations per second, providing roughly the same computational power as the ENIAC in 1946**ORegan:2021**. Its successors (the 8008 and 8086) are the base of Intel's current x86 architecture. As one of the first personal computers, the Apple I and its successor the Apple II played a big role in providing more people with access to computational devices. The Apple I was released in 1976, it had to be assembled by the customer**ORegan:2021**. From this point on computing power increased drastically, this is achieved by higher clock frequencies, pipelining, parallel processing etc.. Most computer architectures like the x86 instruction set are **CISC!** (**CISC!**) based. One of the first architectures to take a different approach towards simpler but faster instructions is the Microprocessor without Interlocked Pipelined Stages (MIPS) Instruction Set Architecture (ISA), more information on this architecture can be found in **patterson:2020**.

One of the latest developments of Reduced Instruction Set Computer (RISC) based computers is the developement of the RISC-V ISA in 2010.

2 Basics

2.1 Processing Units

2.2 RISC vs CISC

2.3 RISC-V

RISC-V is an open standard Instruction Set Architecture (ISA) developed by the University of California, Berkely. The ISA is based on reduced instruction set computer (RISC) principles. The ISA supports 32, 64 and 128 bit architectures and includes different extensions like Multiplication, Atomic, Floating Point and more. The ISA is open source and therefore can be used by everyone without licensing issues and high fee requirements. Due to the open source nature of the RISC-V project, many companies like Alibaba and NVIDIA have started to develop hardware based on this ISA. RISC-V opens the opportunity to optimize and configure computer hardware to a level that would not be realizable with licensed ISA like ARM or x86. As a result of this possibility there are many projects and companies working on hardware and software that are beating common CPU in terms of performance and power usage by a lot.

2.4 Benchmarks

2.4.1 Coremark

2.4.2 SPECint

2.5 Memory Management

2.5.1 Memory Hierarchy

One of the major performance factors in computing is how fast can information be accessed. Information in this case is both: data and code. Therefore high-speed infinite sized memory would be the optimum to achieve the best possible performance. Unfortunately multiple difficulties are raised by this requirement. How can an infinite sized memory be achieved, how to guarantee that access time does not increase when increasing the memory size and how to keep costs to minimum are only a few of the many questions that can be asked on this topic.
In general it can be said that infinite sized memory is not possible, therefore the new requirement would be: as big as possible. To achieve low access times, the memory must be placed as close as possible to the processor. The amount of extremely fast memory is therefore restricted to a finite size. Increasing the distance to the processor yields more space, hence a bigger possible memory. Access speed is reduced at the same time.
Therefore the only way to have a big high-speed memory is to emulate it. This is done by taking advantage of two principles: temporal- and spatial locality **patterson:2017**. Temporal locality suggests that data which is accessed will be used again in the near future. This can be caused by loops inside a routine. Spatial locality is very similar. If data from one particular region is accessed, there is a high probability of an access to the same region in the near future. Many data structures, for example arrays, cause spatial locality.
Figure 2.1 shows an example of a possible memory hierarchy:

The closer a memory element is placed to the processing unit, the faster it gets. This is not only caused by the spatial distance but also by the chosen memory type. For example registers are the closest, followed by SRAM which is typically used for L1,L2 and sometimes even L3 caches **patterson:2017**.
If a memory access is performed, the memory management system first checks whether or not the desired data is stored in the upper memory levels. A hit occurs when the data block is found in an upper level of the memory hierarchy. In case of a miss, the search for

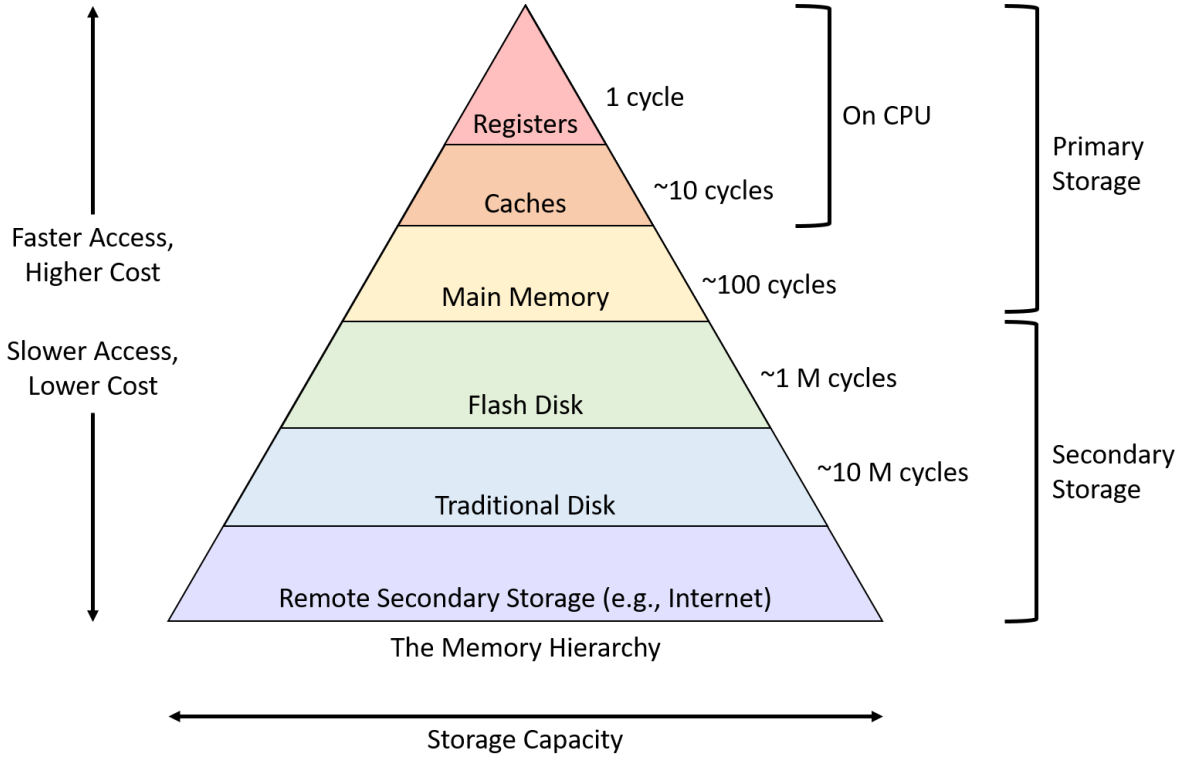

Figure 2.1: Generic Memory Hierarchy **picture:memoryhierarchy**

the required data block is continued in the lower levels. If it is found e.g. in main memory, the data will be provided to the processor and copied into the cache. Therefore satisfying the temporal locality principle. Surrounding data blocks are also copied to the cache in order to prevent another miss in case of spatial locality.
Performance of the memory hierarchy can be measured by the hit and miss rate. These describe the portion of miss and hits of the overall memory accesses. Miss rate can be calculated, if the hit rate is known:

$$missrate = (1 - hitrate)$$

To get a significant measurement of the performance, hit time and miss penalty have to be considered as well. The hit time is defined as the time it takes to get the data block from the cache if a hit occurs. After a miss is detected, that block of data has to be retrieved from main memory, stored in the cache and provided to the processor. The overall time required for these three steps is defined as the miss penalty **patterson:2017**.
Different ways of increasing cache performance are described in **patterson:2017**.

2.5.2 Communication Interfaces

In order to access memory, some sort of communication interface / bus system is required. There are countless options like the widely used Peripheral Component Interconnect Express (PCIe) and Controller Area Network (CAN) bus or application specific systems, e.g. SpaceWire used in satellite systems or Advanced RISC Machiness (ARMs) Advanced Microcontrol Bus Architecture (AMBA).
The following section will provide an overview of the Advanced eXtensible Interface 4 Lite (AXI4-Lite) protocol which is implemented in the Educational DHBW RISC-V Core (EDRICO).
An AXI interface has four independent channels: read address, write address, read data, write data and write response. Figure 2.2 and 2.3 visualizes these three channels:

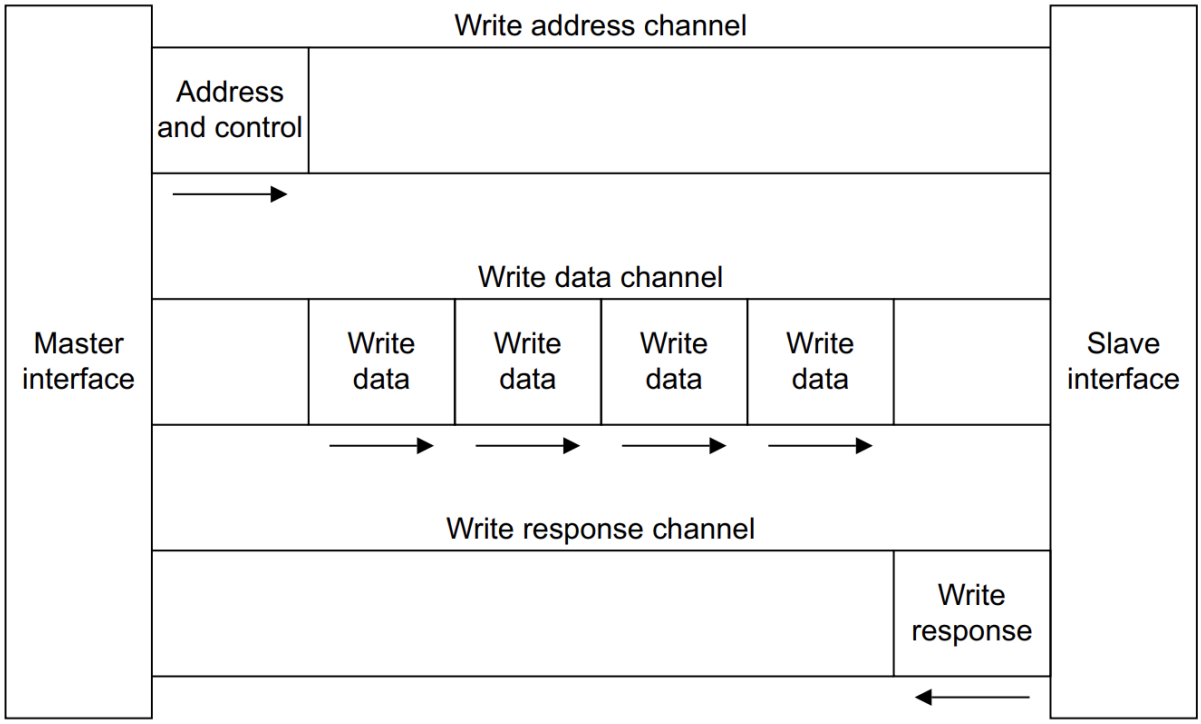

Figure 2.2: AXI4 write channels **AMBA:AXI**

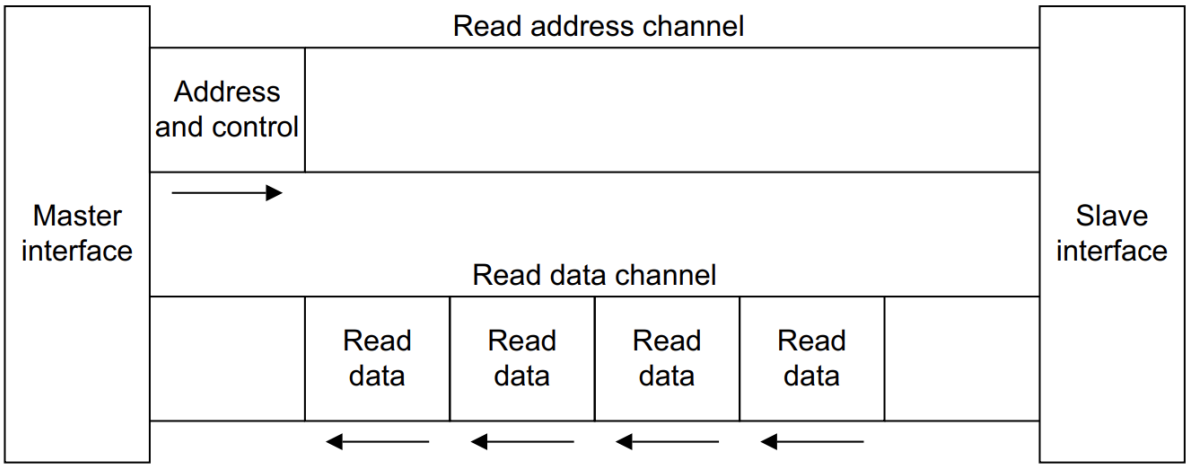

Figure 2.3: AXI4 read channels **AMBA:AXI**

The master interface always initiates the transaction by sending either the write or read address and control. In case of a write, the data is send to the slave using the write data channel. A response is given by the slave, containing information on the transfer. The slaves response on a read does not need a separate channel, since it can be transmitted using the read data channel.
AXI4-Lite does not support burst transfers, hence only one data word can be transmitted in one transfer. To transfer any data over any channel, a generic handshake process must be completed. Figure 2.4 shows how the handshake is performed:

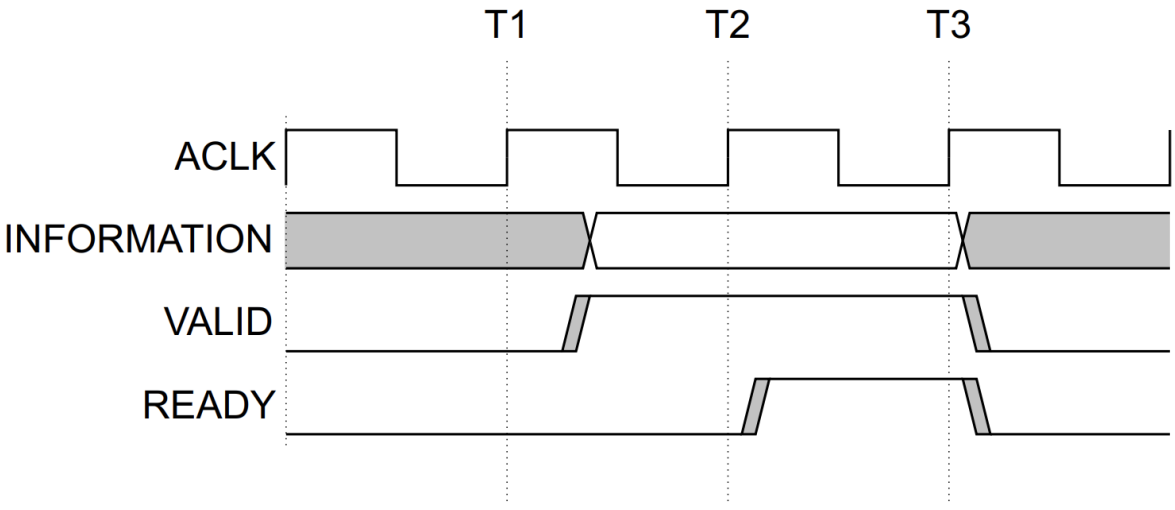

Figure 2.4: AXI handshake **AMBA:AXI**

At transfer begin, the sending interface applies the information (e.g. the read address) on the bus. The Valid signal indicates that the information is valid, it must stay valid until the receiving interface applies the ready signal. Ready indicates that the receiving partner

is ready to receive the information. If both signals (valid and ready) are high on a rising clock edge, the information is read by the receiver and the flow control signals are tied to low **AMBA:AXI**. This handshake mechanism allows the receiving AXI interface to extend the length of the transfer when needed. Since each of the five AXI4 channels are independent five handshake mechanisms are implemented.
A response of a slave contains the *RRESP* or *BRESP* signals, respectively. They can be set to OKAY, EXOKAY, SLVERR, and DECERR. In case of an okay or exclusive okay, no error has occurred. SLVERR indicates that an error has occurred on the slave side, even though the slave successfully registered the access. If no slave is available on the interrogated address, a DECERR is returned.

Based on the response of the slave, a masters behavior must adapt. If (EX)OKAY is returned it may proceed normal operation. If an error is detected error handling methods such as exceptions must be triggered.
The AMBA protocols are widely used in embedded systems. Many IPs deployed in FPGAs can be interfaced using the AXI4 or AXI4-Lite bus. Therefore it is mandatory to be familiar with this particular bus architecture when working with embedded systems.

2.6 FPGA

To verify a digital circuit software simulations as well as implementing the design on a prototype are common practice. For prototyping and even implementing a finished product, FPGA are widely used. FPGAs are special fine granularity Programmable Logic Devices. The digital logic can be described using hardware description languages such as Verilog or VHDL. These designs are then synthesized, placed and routed in order to generate a hardware configuration file, also called bitstream. The bitstream can then be loaded onto the FPGA via a programming interface e.g. JTAG. Many different vendors produce FPGAs, the most famous ones are Xilinx, Altera/Intel and Microchip. Some smaller vendors like NanoXplore produce FPGAs targeting rare use cases like space applications. Despite the many differences in design of an FPGA, the basic architecture always remains the same. An array of logic cells and building blocks of different features 9 like BRAM and DSP slices are connected to each other through configurable routing channels. Figure 2.5 shows the basic architecture of a Xilinx FPGA:

The CLBs in this architecture are comprised of LUTs and Flip-Flops, in order to implement boolean functions and allow the design of synchronous circuits. FPGAs produced by Xilinx are mostly SRAM based, other approaches are flash or anti-fuse based architectures.

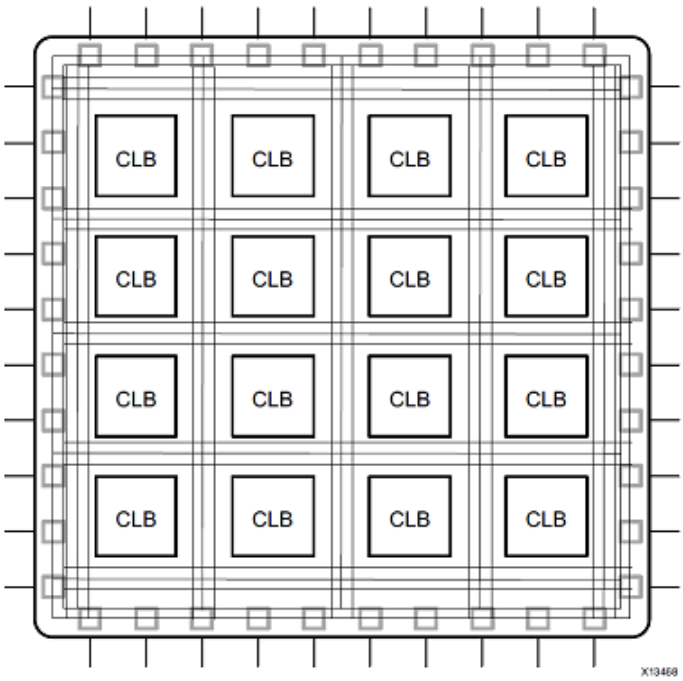

Figure 2.5: Xilinx FPGA **xilinx:2017**

2.7 Hardware Description Languages

3 EDRICO

The Proposed Processor design named Educational DHBW RISC-V Core (EDRICO) implements a basic RV32I instruction set architecture. Besides the mandatory "Zicsr" extension no other instruction set extensions are implemented. To keep the implementation simple and straight-forward only one privilege mode (Machine-mode) is implemented. This mode allows full access to the processor and peripherals. Future Versions could be extended to implement Supervisor-Mode and User-Mode.
The core is a simple Single Instruction Single Data (SISD) processor without any pipeline or cache. The basic instruction cycle of fetch, decode, execute, store is performed for every instruction one at a time.
Figure 3.1 shows the full overview of the processor design:

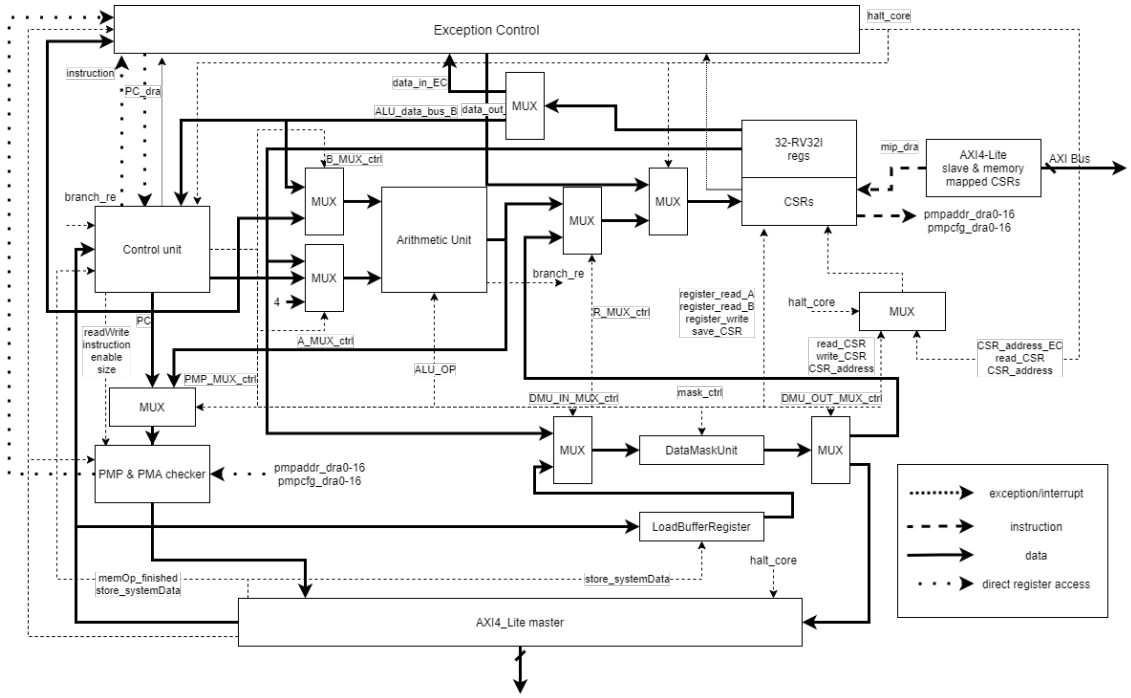

Figure 3.1: EDRICO Overview

Its main components are the Exception Control, Control Unit, Arithmetic Unit, Register Files, PMP & PMA checker and the AXI4 Interfaces. How these components interact with each other, in order to execute Instructions, is specified in the Data Path. The following sections will describe each one of the sections in more detail.

3.1 Data Path

The Data Path specifies how the data is passed through the Processor Core at run time. It therefore determines what registers are read and written at which clock cycle, what control signals need to be applied and how many cycles the instruction execution takes.
To run an instruction, it must be fetched, decoded and executed. Execution varies for different instructions.
To perform for example a load, the target address must be calculated and verified for possible access constraints. After successfully accessing the memory space, the obtained data is modified to satisfy the instruction specific formatting. A load half-word unsigned operation for instance must return a 32-Bit value by zero extending the loaded two bytes of data.
In case of a simple register-register addition, execution is found to be a lot simpler. Addition is performed inside the Arithmetic Logic Unit on two register values. The result is stored to the target register on the next falling clock edge.
With the end of the execute phase, the Programm Counter is updated. This ensures that the 32-Bit register always contains the address of the current instruction to be fetched, decoded and executed.
Figure 3.2 shows the different actions that are performed on each clock cycles during run time:

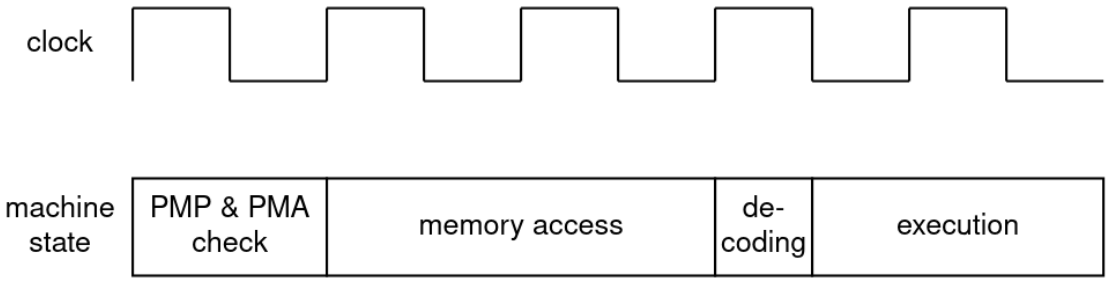

Figure 3.2: Generic Data Path

Prior to memory access, the address must be checked for possible violations of the physical memory protection (PMP) and physical memory attribute (PMA) rules. Therefore the PC is passed to the PMP and PMA checker unit (see: 3.1).
PMP and PMA checks are finished one clock cycle later, if an exception is generated, the trap is taken. Otherwise the data as well as the control signals are passed to the AXI4-Lite master. The AXI4-Lite transfer will take multiple clock cycles. Its length can be increased by external factors, such as the memory to be accessed or the amount of data currently passing through the AXI-interconnect. To simplify the depiction in 3.2 it is assumed to take only two clock cycles.

After successfully accessing the memory, decoding is performed in half a clock cycle. Decoding returns all the control signals of EDRICO set to the correct levels in order to perform the desired operation. Hence, no control signals do change during execution. This is desired since it will allow an easier pipelined implementation of a RISC-V core based on EDRICO.
Execution is displayed to take one and a half clock cycles. The registers are written at the falling clock cycle, one cycle after decoding started. Therefore execution is finished after only one clock cycle and not one and a half. Since the next instruction fetch is issued at a rising clock edge the machine must remain in execution state for an additional half clock cycle.
The fact that some registers are falling-edge and others rising-edge sensitive may seem a little bit disturbing at first glance. It is done to allow easier implementation and achieving of timing-closure during place and rout. If, for example, a critical path is found to be at the decode process, the duty cycle of the clock can be modified in order to achieve a higher possible clock frequency.

3.2 Control Unit

The Control Unit (CU) is the heart of the processor and controls the other parts of the processor depending on the input instruction. The CU is responsible for fetching instructions from the instruction memory, decode the bitstream and set the respective control signals for the other processor components. Due to the complexity of the CU, there are several sub-modules which together form the overall CU.

3.2.1 Architecture and Design

A general overview of the CU architecture is displayed in Figure 3.3.

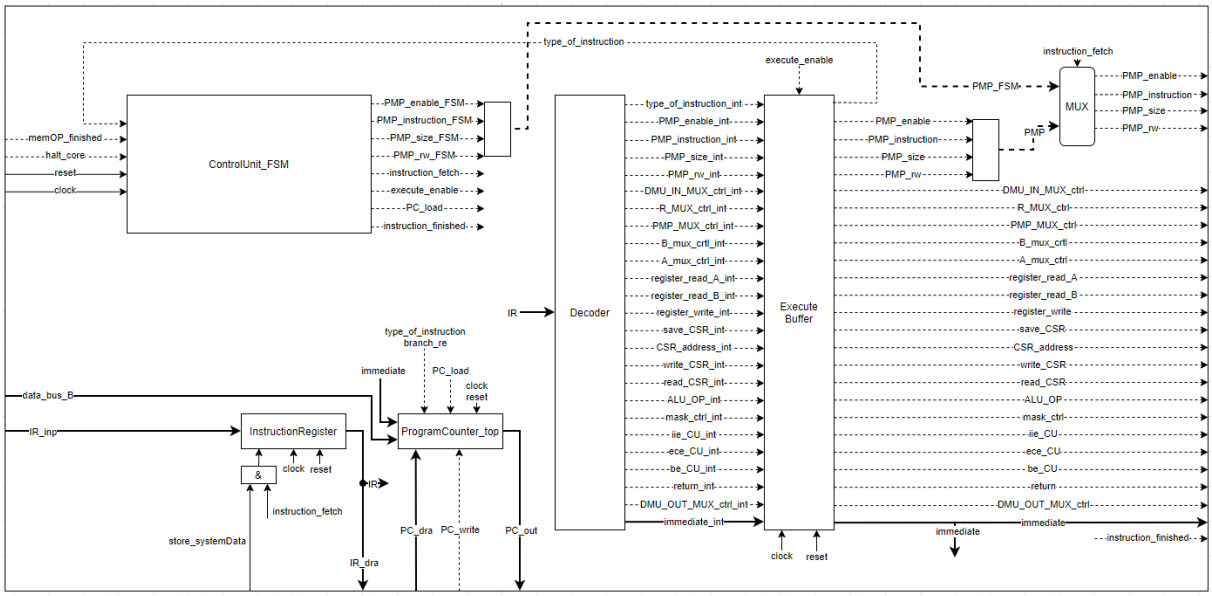

Figure 3.3: Control Unit Architecture

To describe the functionality of the CU in more detail, every sub-module will be described closely.

Since the Control Unit is responsible for the whole processor, it is important to have a persistent and stable procedure for every instruction that shall be executed. The Control Unit Finite State Machine (FSM) is responsible for the correct clock timings which is important due to memory operations and the execution time of the other processor parts. The states and conditions of the FSM are displayed in Figure 3.4.

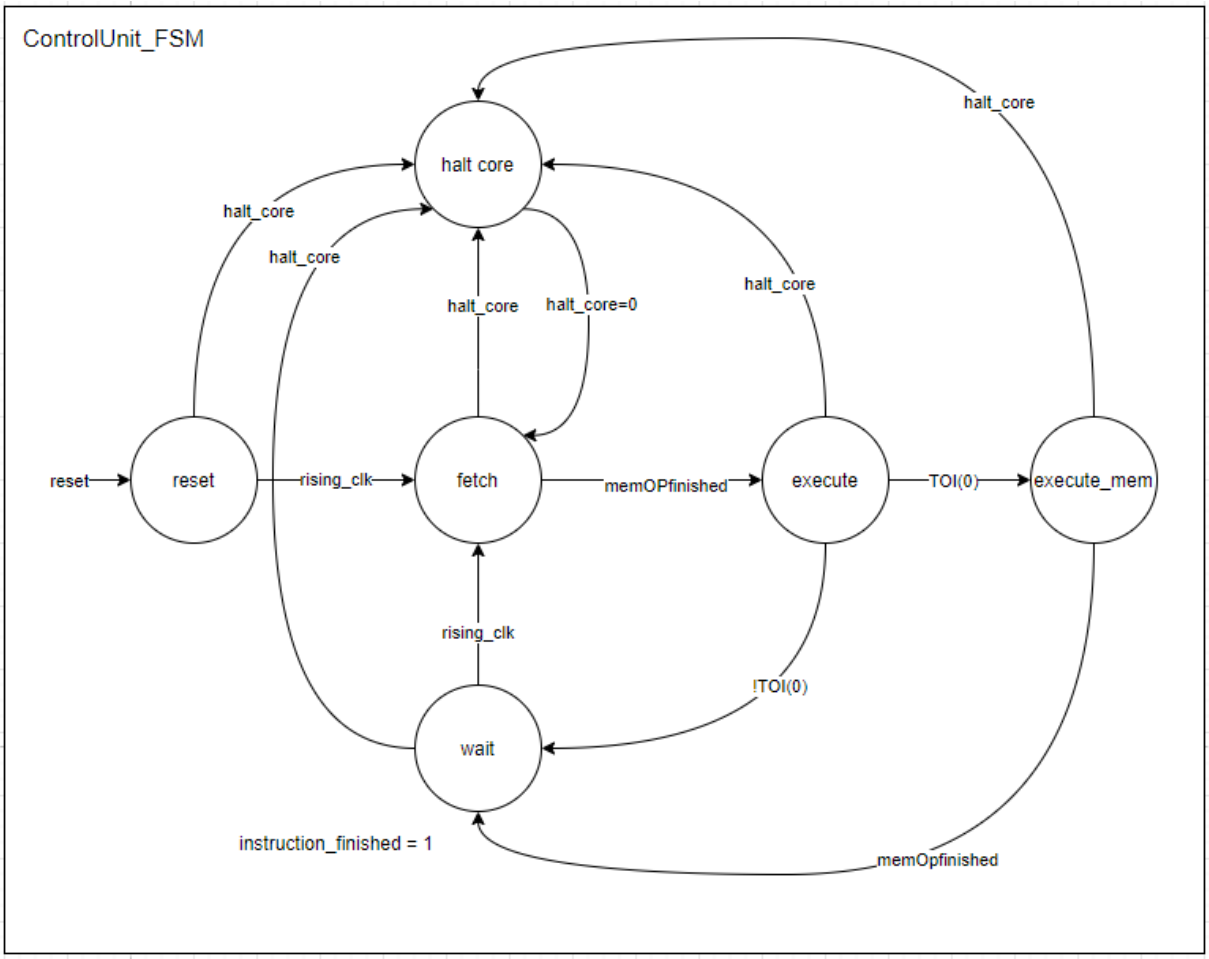

Figure 3.4: Control Unit FSM overview

Table 3.1 shows a more detailed overview of the clock cycles and the corresponding actions and states:

ClockCycle	Edge	Action	Signal
1	rising	pass the PC and enable PMP & PMA checker with respective information	
	falling	N/A	
4	rising	data is ready in instruction register - switch to execute state	*memOPfinished* & *store_systemData* is high
5	rising	execution is started - if memory operation wait for another *memOPfinished* flag, otherwise wait	*execute_enable*
x	rising	during memory operation: data loaded to buffer \store transfer finished → wait state	*memOPfinished* & *store_systemData* is high
	falling	if load: store data form buffer to specified location	
6 / x+1	rising	go to *fetch_state*	

Table 3.1: Timing of FSM

During an execution cycle, the FSM controls the rest of the CU consisting of memory, decoding unit, PC control and the different multiplexers. To understand what the purpose of the different signals are, the other components of the Control Unit are described in the following sections.

After loading an instruction from the memory to the instruction register, the decoding process can begin. The responsible part for this process is the decoding unit which is described below.(Also visible in figure 3.3)
In this project the RISC-V RS32I instruction set is used which consists of 32-bit instruction words. The instruction words have a pre-defined structure and are divided into six instruction formats. The instruction formats are shown in Figure 3.5.

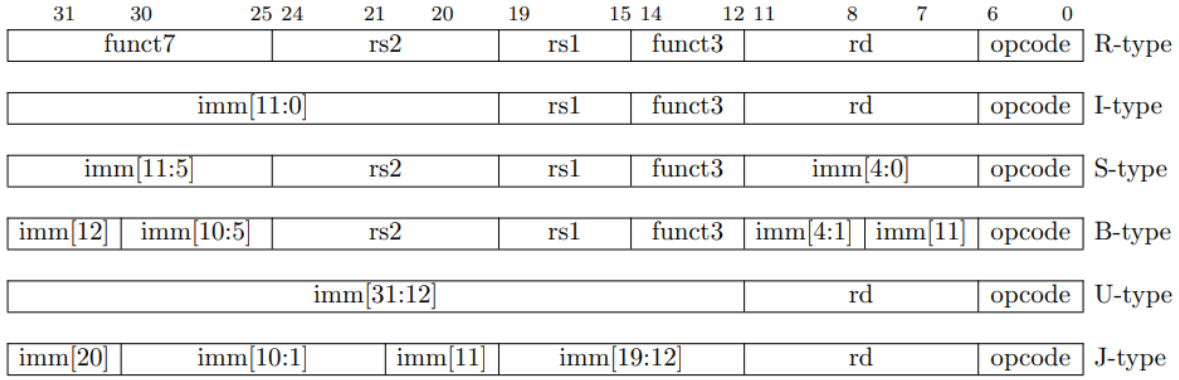

Figure 3.5: RISC-V Instruction formats **riscv**

The different instruction formats are useful for the decoding process since e.g. all LOAD instructions have the same structure and therefore, the effort to decode the 32-bit word can be reduced. Since the control signals are unique for every instruction and depending on the content of the 32-bit word, the decoder has to identify the encoded instruction, extract the information and respectively set the control signals, calculate immediates and control the multiplexers. A more detailed description of the decoding process can be found in section 3.2.2.
After the instruction is decoded, all output control signals are stable and ready to be fed through. Before leaving the CU, the *Execute Buffer* (figure 3.3) buffers the control signals. Once the FSM sets the *execute_enable* flag, the control signals are fed through. This buffer prevents the processor to confuse timing and clock cycles, or use signals which are not yet set correctly.
During an instruction execution, the program counter has to be incremented for the processor to know what instruction will follow. *But* since there are several instructions that modify the program counter, a so called *PC control* is designed. The PC control receives information from the decoder which consists of a 4 bit signal. The different instructions and the respective action as well as the respective control signal are shown in following table 3.2.1:

Instruction	Action	Control Signal
Default	No action required	**0000**
Branch	Depending on the result of branch operation, PC will be incremented respectively	**0010**
JAL	Target address obtained by adding current PC and immediate, rejump address stored in register	**0100**
JALR	Target address obtained by adding input register to immediate	**1000**

Table 3.2: Program Counter control: Instructions and resulting actions

For instructions which do not influence the program counter, the standard operation performs the **PC + 4** operation.

The instruction register displayed in figure 3.3 manages the instruction string coming from the memory. All of these parts together form the Control Unit and are responsible for the correct execution of the instructions. The implementation of the sub-units in VHDL are described in the following section 3.2.2.

3.2.2 Implementation

The implementation of the Control Unit is split up into multiple sub-implementations. As shown in figure 3.3 those sub-modules are the *FSM, decoder, execute_buffer, PC control and instruction register*. Since the implementation of the FSM is very similar to other FSM implementations in this project, the detailed description of a FSM in VHDL is found in the next chapters.
In this section the implementation of the decoder will be described more closely. As already described in section 3.2.1 the instructions can be separated in different instruction formats. To distinguish the different instructions, so-called *instruction clusters* are created. These clusters sum up instructions which are encoded in the same instruction format or in general are similar. The following table shows the different clusters and the corresponding instructions:

Cluster	**Instructions**
LOAD	Load - Byte \Halfword \Word
STORE	Store - Byte \Halfword \Word
BRANCH	Different Branch Instructions (e.b. Branch if equal)
JALR	only JALR, since it has a unique instruction structure
JAL	only JAL, since it has a unique instruction structure
OP	All arithmetic instructions like ADD, SUB, shift and comparisons
OP-IMM	All arithmetic instructions performed with immediate
AUIPC	only AUIPC, since it has a unique instruction structure
LUI	only LUI, since it has a unique instruction structure

Table 3.3: Decoding instruction clusters

To determine the cluster for each instruction, a decoding procedure is implemented in VHDL based on structure visualized in figure 3.6:

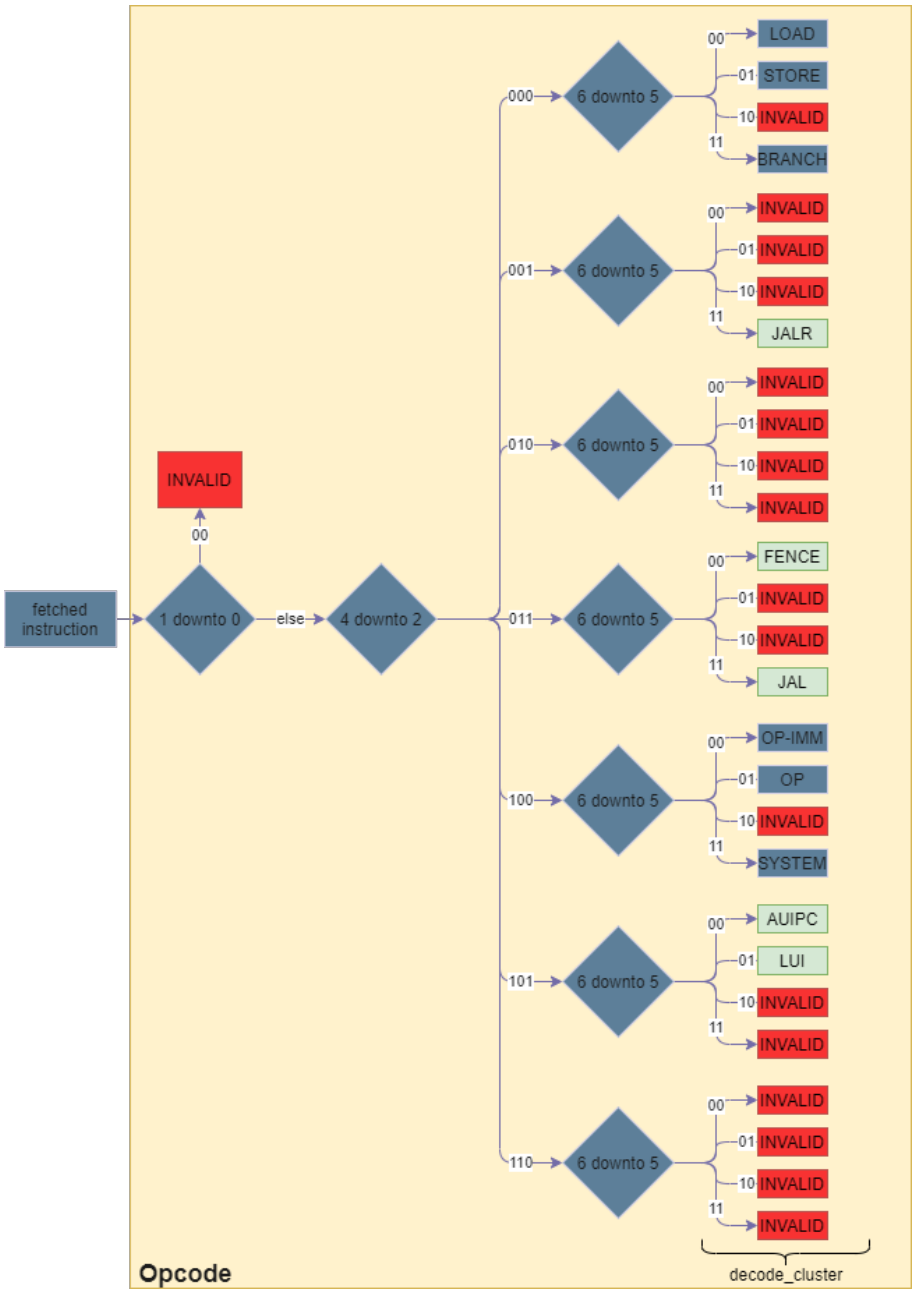

Figure 3.6: Decoding Structure to determine instruction cluster

After determining the cluster, the VHDL code assigns all the outputs visible in figure 3.3 with the respective information. For a better understanding of the information extraction, figure 3.7 shows how the 32-bit instruction word is split up (in this case for the *OP* and *OP-IMM* instructions.)

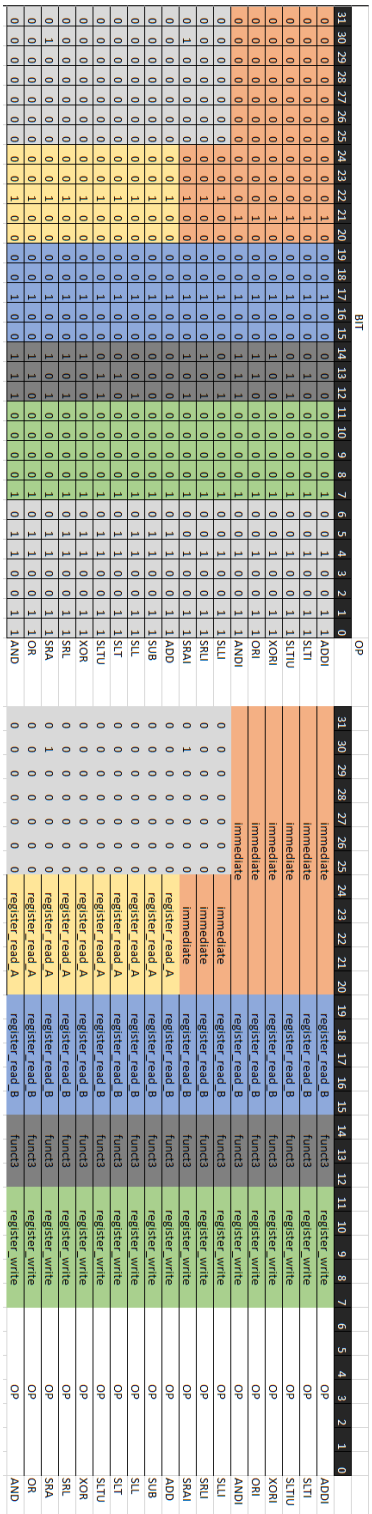

Figure 3.7: Information extraction from 32-bit instruction word

3.3 Arithmetic Logical Unit

The Arithmetic Logical Unit (ALU) is the part of the processor that performs the arithmetic and logical operations. Figure 3.8 gives an overview of what type of operations are performed.

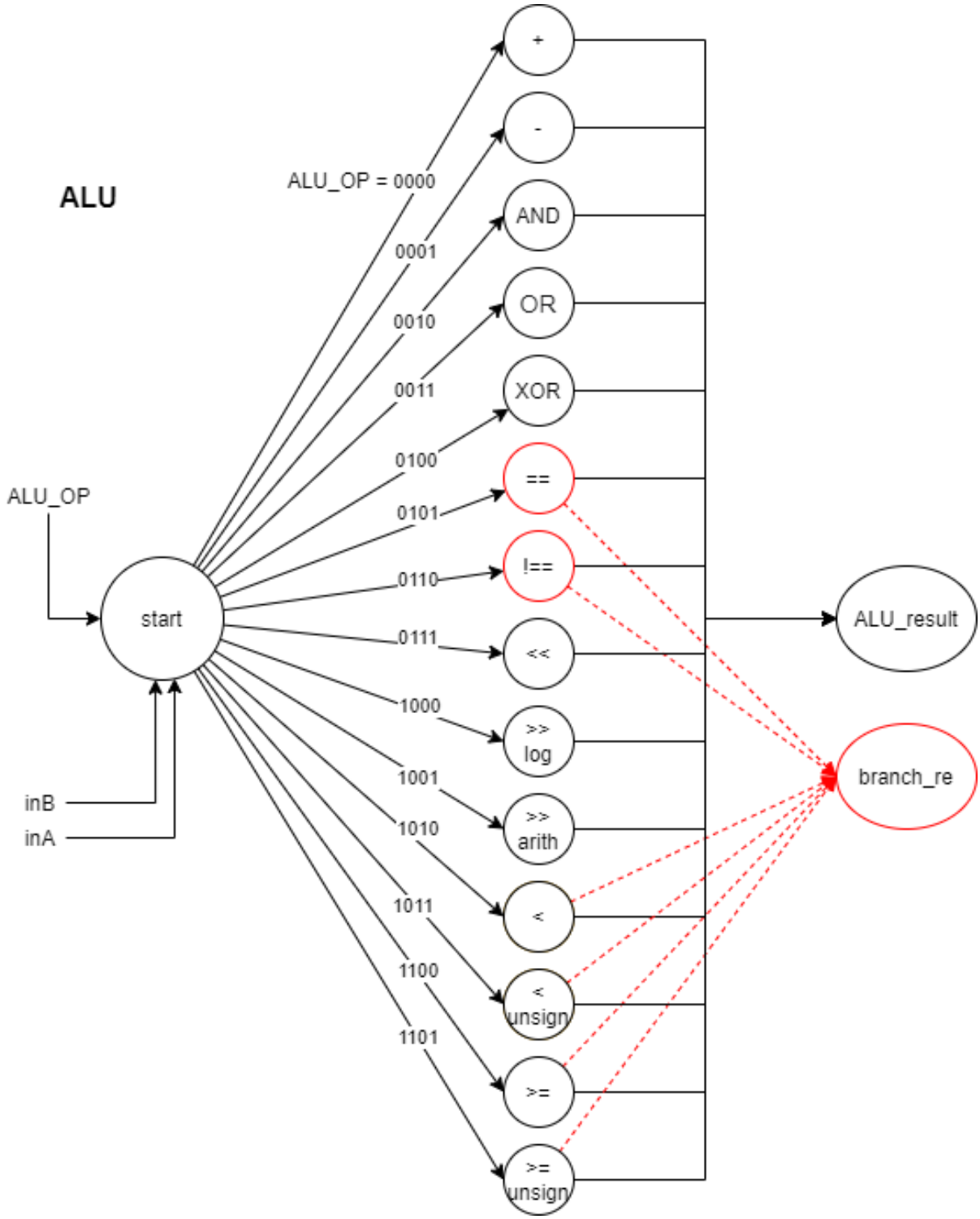

Figure 3.8: ALU operations

3.3.1 Architecture and Design

To implement the ALU, it is required to have the data inputs as well as clock input and a control signal consisting of 4 bits to specify the required operation to be performed. Since there are instructions that require a branch response to know whether the next instructions shall be skipped or not, the ALU needs an additional output called *branch_re* other than the result output of the arithmetic/logical operation. The architecture of the ALU is shown in figure 3.9:

Figure 3.9: ALU operations

Not only the instructions e.g. *ADD, SUB, XOR...* require an arithmetic operation but also *LOAD, STORE..* require an ALU action. While *ADD, SUB, XOR...* require an operation between the two input values (either register-register or register-immediate) to get a mathematical or logical result, the *LOAD, STORE...* instructions require the ALU to build the target addresses for the memory access.

3.3.2 Implementation

The implementation of the ALU is based on figure 3.8 and performs a switch-case on all the different input values of *ALU_OP*. The 4-bit input variable specifies the operation based on following declarations:

ALU_OP	Operation
0000	ADD
0001	SUB
0010	AND
0011	OR
0100	XOR
0101	EQUAL
0110	NEQUAL
0111	shift_left
1000	shift_right
1001	shift_right (arithmetic)
1010	$<$
1011	$<$ (unsigned)
1100	$\geq$
1101	$\geq$ (unsigned)

Table 3.4: Input code and respective operation

To visualize the implementation, a part of the VHDL code is displayed in the following. The case statement is based on the input *alu_op*. The ALU then performs the corresponding operation with the two inputs *in_a and in_b*.

```
1  begin
2    process(in_a, in_b, alu_op)
3    begin
4    --default output is 0
5    branch_re <= '0';
6    alu_result <= "00000000000000000000000000000000";
7      case alu_op is
8        when "0000" =>--"ADD"
9          alu_result <= in_b + in_a;
10       when "0001" =>--"SUB"
11         alu_result <= in_b -in_a;
12       when "0010" =>--"AND"
13         alu_result <= in_b AND in_a;
14       when "0011" =>--"OR"
15         alu_result <= in_b OR in_a;
16       when "0100" =>--"XOR"
17         alu_result <= in_b XOR in_a;
18       when "0101" =>--"EQUAL"
19         if(in_b = in_a) then
20         branch_re <= '1';
21         else
22         branch_re <= '0';
23         end if;
24   ...
```

Listing 3.1: ALU VHDL code

In case the operation determined by *alu_op* might be originating of a branch instruction, the *branch_re* flag has to be set respectively (line 19). Since the branch instructions only include some of the arithmetic and logical operations of the ALU, the default value for the *branch_re* is set as *0*.

3.4 Register File (RF)

A register is a small memory element with high read and write speeds. It is therefore often used inside digital circuits to store data locally. In the case of a processor core, the total data stored in all registers specifies the machine state.
If the contents of each register are saved to some arbitrary memory the current state of the core can later be restored by loading this data to the corresponding registers.
The RISC-V unprivileged specification specifies 32 32-Bit general purpose register for the RV32I base instruction set **riscv:unprivileged**. To configure the core as well as storing status and general information about it multiple Control and Status Register (CSR) are introduced by the RISC-V privileged specification **riscv:privileged**.
EDRICO implements both, all 32 32-Bit integer general-purpose registers as well as a selection of required CSRs.

3.4.1 Architecture and Design

A requirement for the Register Files is to allow access on one input data bus and two output data bus, each with a size of 32-Bit respectively. Multiple control signals can be accessed to control the data flow through the module. Registers are read asynchronously, hence a read operation is not dependent on any clock. Writes to a register are performed on a falling clock edge.
Some of the CSRs need to provide their contents to other modules without using one of the two designated output buses. This decreases unnecessary overhead on e.g. load and store operations.
Figure 3.10 depicts the architecture of the Register File module.

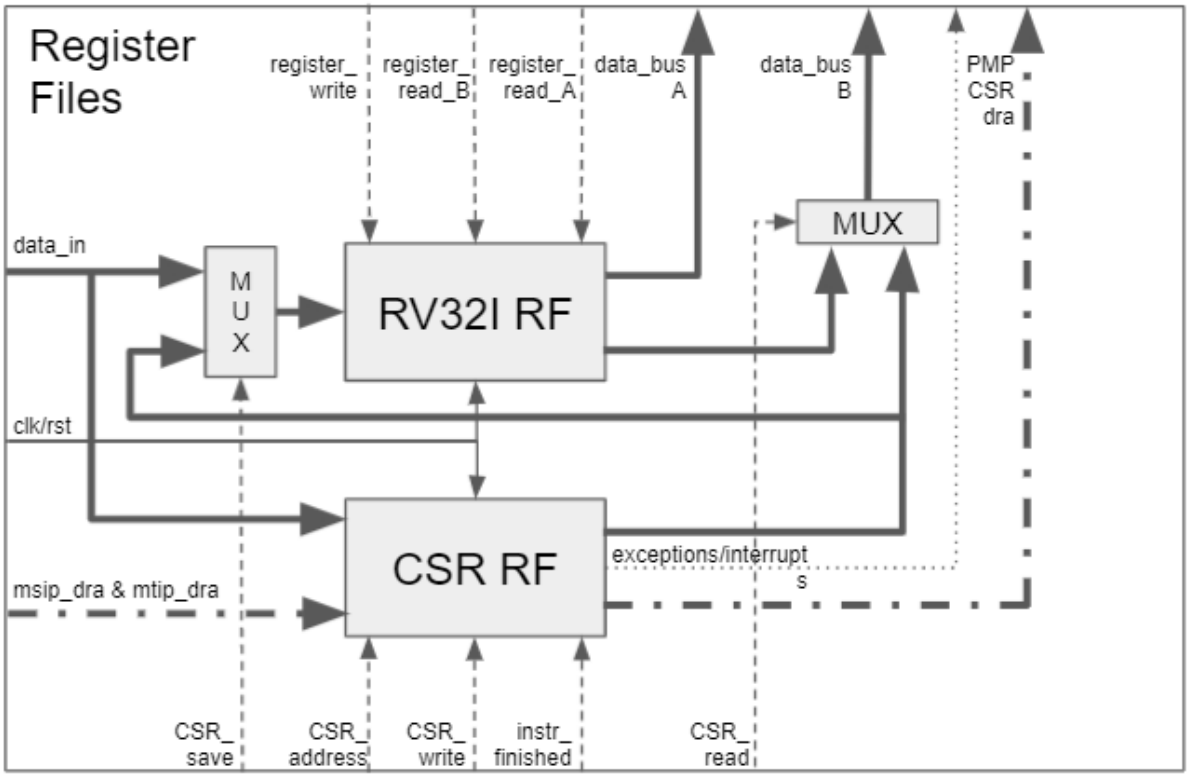

Figure 3.10: Register Files architecture

In order to write data to a register, the value needs to be put on the *data_in* bus and the corresponding control signals need to be configured. Data can be read either via the *data_busA* or *data_busB*, the CSR registers can only be accessed on *data_busB* via a MUX controlled by the *CSR_read* signal. If the bit is set, the CSR specified by *CSR_address* will be visible on *data_busB* at the next rising clock edge.
In order to store data to a CSR register, it has to be put on the *data_in* bus. If the *CSR_write* bit is set, the data is saved to the register specified by *CSR_address* on the next falling clock edge.
Execution of special CSR instructions, like the Atomic Read/Write CSRRW **riscv:unprivileged**, requires writing to both a general-purpose RV32I register and a CSR. Since the control signals are not allowed to change during execution, it is mandatory to allow the CSR RF to write directly to the RISC-V 32-Bit Integer (RV32I) RF without utilizing the *data_in* bus. In order to do so, the *CSR_save* signal is added to design. If it is applied, the CSR Register File output is connected to the data input bus of the general purpose registers.
Some of the CSR allow direct memory accesses. These are implemented in a separate module, including the *mtime*, *mtimecmp* and *msip* registers as well as a dedicated AXI4-Lite slave interface. To set the software and timer interrupt pending bits (which are caused by the memory mapped CSR), the *msip_dra* and *mtip_dra* inputs are implemented.

The CSR Register File is accessed by a 12 Bit addresses, RV32I registers are accessed using a four byte address signal for each data bus, respectively.

General Purpose Registers

The general purpose registers are used to store the data on which operations are performed on. Since RISC-V is a load-store architecture no data from the memory can be modified directly without loading it to a General Purpose Register (GPR) first (except when using atomic operations) **riscv:unprivileged**.
Figure 3.11 shows the design of RV32I Register File:

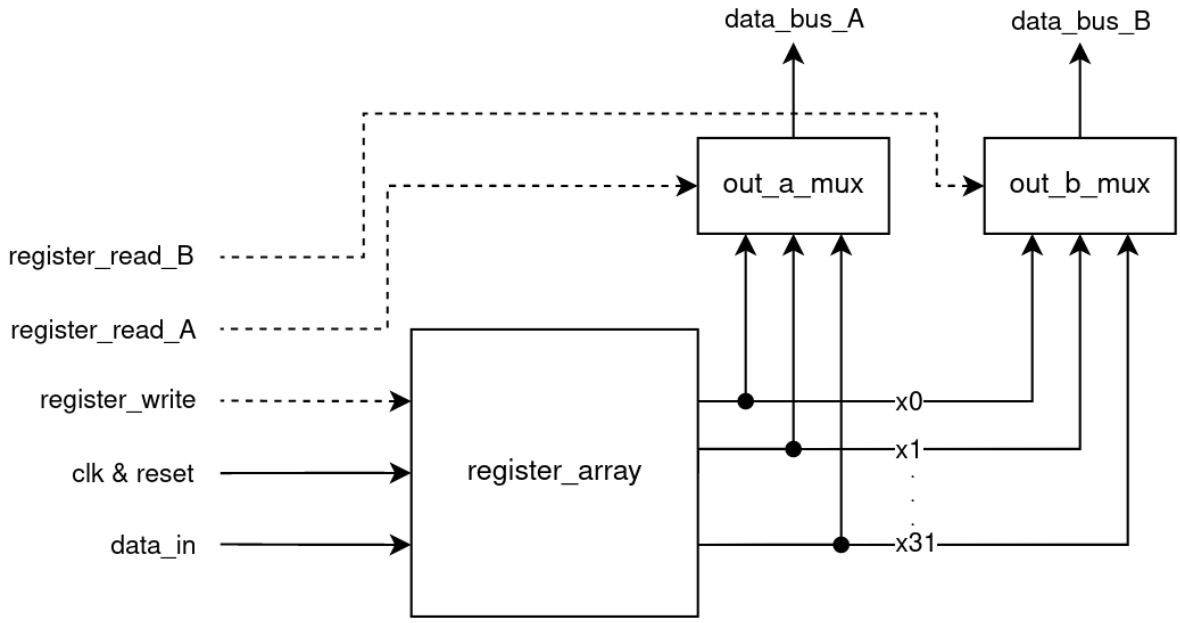

Figure 3.11: General Purpose Registers

Every register may be modified via *data_in* and read via *data_busA* and *data_busB*. The only limitation is *x0*, per definition *x0* must be hardwired to zero. Writing to the register is allowed but has no effect, reading will return *0x00000000*. According to the RV32I programmers model some of the other registers should be used for dedicated purposes, like the stack pointer. There are no hardware checks implemented in order to enforce those rules.
Writes are executed on a falling edge if the corresponding *register_write* signal is high. Reads are performed on a rising edge if the corresponding *register_read_A/B* is high. There are no hardware checks implemented to prevent multiple registers from writing to the same data bus at the same time. This must be prevented by the controlling element e.g. the control unit.
All registers are cleared to *0x00000000* on reset.

Control and Status Register (CSR)

CSRs are Control and Status Registers that are introduced to the design by the RISC-V privileged specification. Some of the values stored inside the CSRs need to be provided to the Exception Unit and the PMP & PMA checker to decrease complexity, some of that accesses can be performed through direct memory access. Some of the CSRs are memory mapped. Memory mapped means they need to be accessible via the system bus by any AXI4-Lite master. In order to implement this, an AXI4-Lite salve module implementing all memory mapped CSRs is added to the design.
Further Information about this module can be found in the chapter 3.8. The CSRs that provide direct access are:

- *msip* and *mtip* bits in the *mpi* register (write)
- *pmpcfg* (read)
- *pmpaddress* (read)

Some registers are specified as WARL registers, meaning anything can be written to them, but the value returned on read must be a legal value. Table 3.4.1 displays every non memory mapped CSR, the corresponding address, type, access possibility, width and a short description:

register	address	type	access	width	description
misa	0x301	WARL	R	32-bit	describes supported ISAs
mvendorid	0xF11	N/A	R	32-bit	describes vendor id
marchid	0xF12	N/A	R	32-bit	describes architecture ID
mimpid	0xF13	N/A	R	32-bit	describes implementation ID
mhartid	0xF14	N/A	R	32-bit	describes hart id
mstatus	0x300	N/A	R/W	32-bit	reflects & controls a hart's current operating state
mtvec	0x305	N/A	R/W	32-bit	holds trap vector configuration
mie	0x304	N/A	R/W	32-bit	reflects interrupt enable state
mip	0x344	N/A	R	32-bit	holds interrupt pending bits
mcycle	0xB00	N/A	R/W	64-bit	holds count of clock cycles
minstret	0xB02	N/A	R/W	64-bit	holds count of executed instructions
mhpcounter(3-31)	0xB03-0xB1F	N/A	R/W	32-bit	holds count of events (lower 32 bit)
mhpcounterh(3-31)	0xB83-0xB9F	N/A		32-bit	holds counter of events (upper 32 bit)
mhpevent(3-31)	0x323-0x33F	N/A	R/W	32-bit	specifies events on which to increment corresponding mhpmcounter
mcountinhibit	0x320	WARL	R/W	32-bit	controls which hardware performance monitoring counters increment (if set, no increment)
mscratch	0x340	N/A	R/W	32-bit	Dedicated for use by machine-mode
mepc	0x341	WARL	R/W	32-bit	holds jump-back address during interrupt
mcause	0x343	N/A	R/W	32-bit	specifies cause of exception/interrupt
mtval		N/A	R/W	32-bit	holds information about trap
pmpcfg0-3	0x3A0-0x3A3	N/A	R/W	32-bit	Physical memory protection configuration
pmpaddr0-15	0x3B0-0x3BF	N/A	R/W	32-bit	Physical memory protection address register

Table 3.5: List of implemented CSRs

The architecture of the CSR Register File is shown in 3.12.

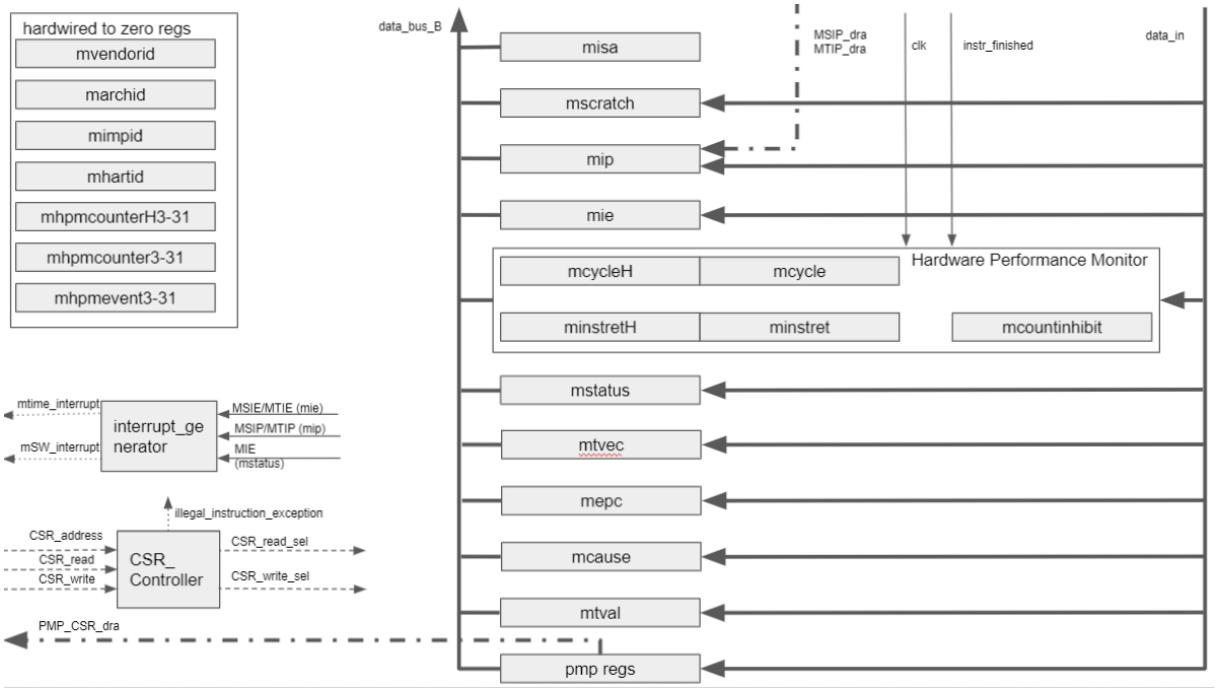

Figure 3.12: CSR Register File Architecture

The CSR Register File is comprised of the different CSR Registers, *CSR_Controller* and *interrupt_generator*.

Some of the implemented CSR registers are hardwired to zero, reads to those addresses return *0x00000000* and writes have no effect if the register is defined as read only the write will result in an *illegal_instruction_exception*. Other CSR registers may be defined as read-only.

The *CSR_Controller* checks if a CSR access is allowed and produces access signals for each register from the given address. If an address is not writable but yet a write is requested, the *CSR_Controller* raises an *illegal_instruction_exception*.

The *interrupt_generator* checks if an interrupt is pending, enabled and if interrupts are globally enabled. In that case the corresponding interrupt is raised. The interrupts remain pending, as long as the corresponding direct register access signals it. To prevent the machine from being stuck in the interrupt, the programmer of the Interrupt Service Routine (ISR) must clear the pending interrupts, e.g. the timer interrupt by writing to the memory mapped CSRs.

Some registers have special functionalities. The Hardware Performance Monitor for example counts the number of clock cycles as well as the number of executed instructions. Calculation of the Cycles per Instructions (CPI) can be performed as shown in (3.1):

$$CPI = \frac{mcycleH >> 32 + mcylce}{minstretH >> 32 + minstret} \tag{3.1}$$

During Benchmarks these registers can be used to calculate the performance of the core. For physical memory protection, several attributes such as read and write can be specified inside the Physical Memory Protection (PMP) CSR, a more detailed description of these specific registers can be found in: **riscv:privileged**.
There are 16 *pmpaddr* and four *pmpcfg* registers. In order to verify that a memory access does not violate any PMP rules, the PMP and PMA checker needs access to these registers. Performing this accesses over the *data_out_B* bus would result in 16+4 data transfers, so 20 register accesses in total. This would impose a significant overhead of at least 20 clock cycles on every memory access. To reduce the effect of checking the PMP rules a direct register access is implemented.

3.4.2 Implementation

Implementing the RV32I RF is done by defining an array of 32 *std_logic_vector* of 32-Bit each. The zeroth element in the array corresponds to the x0 register, therefore it can not be written and is hardwired to zero.
On a write, the 5-Bit *register_write* signal is used to index the corresponding array element. This is only possible since writes to the x0 register do not effect the state of the machine. Hence, no writes are performed if the write signal is set to *0b00000*.
Since some CSR have additional features they need to be implemented individually, therefore the matrix approach used for the RV32I register files can not be taken. There are multiple registers that are hardwired to zero, they are implemented as one and the read write multiplexers access the same register if an access to one of these registers occurs.
To safe resources all CSR implement just the bits that are needed, the others are hardwired to zero. The following listing illustrates this concept, using the *mstatus* register as an example, figure 3.13 shows the mstatus register according to **riscv:privileged**:

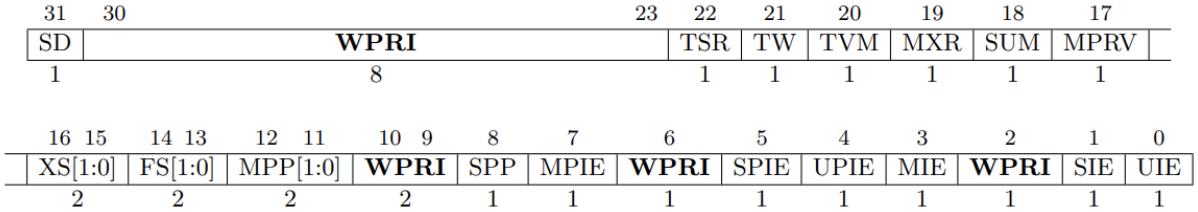

Figure 3.13: 32-Bit machine mode register (*mstatus*) **riscv:privileged**

```
1  ------------------------------------------------------------
2  --mstatus register
3  ------------------------------------------------------------
4  mstatus_proc: process(reset, clk)
5  begin
6  if(reset = '1') then
7  mstatus_reg <= (others => '0');
8  elsif(clk'event and clk = '0' and write(0) = '1') then
9  mstatus_reg <= data_in(7) & data_in(3);
10 end if;
11 end process;
12
13 mstatus <= x"000018" & mstatus_reg(1) & "000" &
       mstatus_reg(0) & "000";
```

Listing 3.2: mstatus implementation

For the chosen implementation only two bits in the status register are relevant, **(!** ((**!**)MPIE) and Machine Interrupt Enable (MIE). Every Other bit can be hardwired to a specific value. Since neither supervisor nor user mode are implemented are the corresponding (prior) interrupt enable bits tied to zero. The *(*xPP) fields hold the previous privilege mode in which the machine was prior to a trap. Only machine mode is implemented, hence Machine Previous Privilege (MPP) can be hardwired to "11" and Supervisor Previous Privilege (SPP) to "00". According to **riscv:privileged** all other bits may be hardwired to zero if only machine mode is implemented.

3.5 PMP and PMA Checker

Physical memory protection and attribute checking must be done in order to ensure that only allowed and defined memory regions are accessed, providing minimum of security and preventing the core from accessing not defined regions, which may result in the core getting stuck.

3.5.1 Architecture and Design

An overview of the PMP & Physical Memory Attributes (PMA) Checker is illustrated by 3.14:

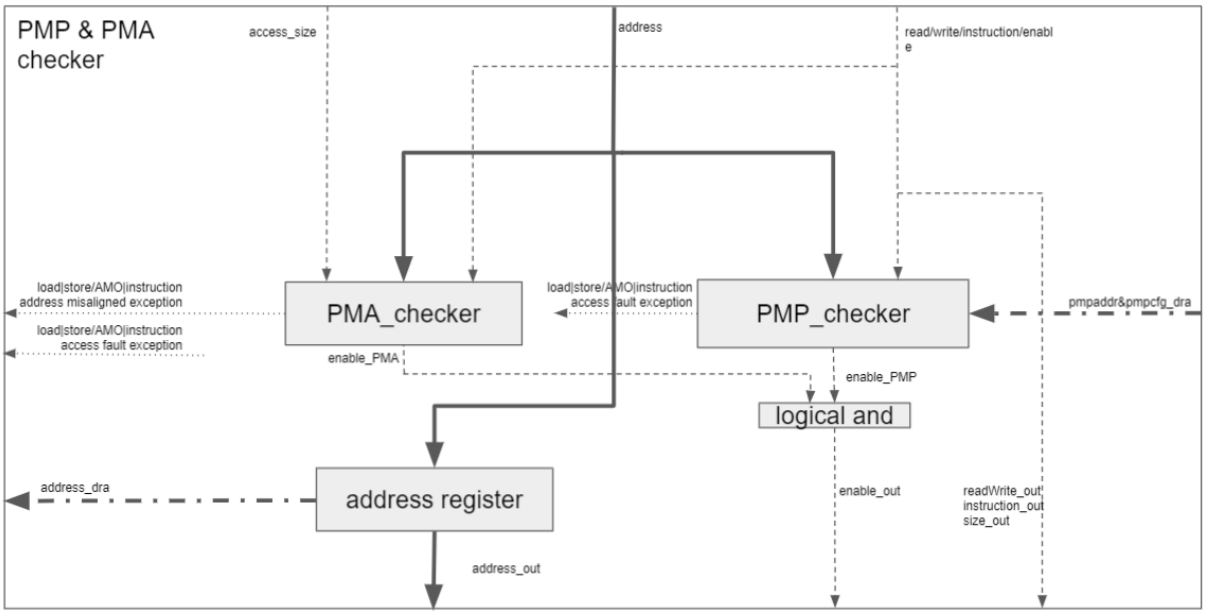

Figure 3.14: PMP & PMA Checker Architecture

The *PMP_checker* is used to define memory regions and enforce several rules onto those, for example if instructions may be fetched from a region or if writes are allowed. In order to apply the rules the corresponding region must be locked by setting the L-bit inside the corresponding *pmpcfg* CSR. Once locked, regions may only be unlocked by a system reset. After a restart every region is unlocked and reset, e.g. a boot loader could enforce several rules for memory accesses in M-Mode before control hand-over to the main software running on the core. If a PMP entry is not locked, every memory access that matches this address space succeeds.
In order to specify, if reads, writes or instruction fetches are possible to a certain address, it needs to be specified inside the *pmpaddr* and corresponding *pmpcfg* CSRs. If an address is not specified every access is allowed, as long as the hart operates in machine mode. The PMP unit has direct access to those and enforces the rules. Figure 3.15 and 3.16 show these two registers.

7	6 5	4 3	2	1	0
L (**WARL**)	0 (**WARL**)	A (**WARL**)	X (**WARL**)	W (**WARL**)	R (**WARL**)
1	2	2	1	1	1

Figure 3.15: 8 Bit from 32-Bit *pmpcfg* register **riscv:privileged**

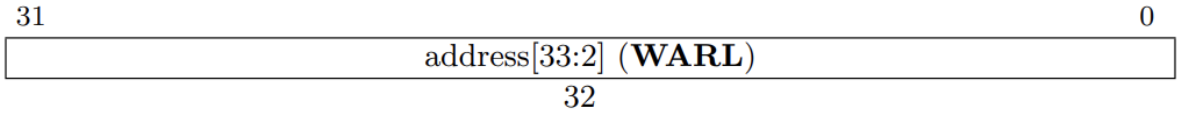

Figure 3.16: *pmpaddr* register **riscv:privileged**

One *pmpcfg* register is comprised of four 8-bit configuration fields, one of which is shown in 3.16. The X, W and R bit specify whether or not the region defined by this entry is fit for instruction accesses, reads or writes. The size and range of the region is specified by the mode chosen by setting the A field in the configuration register. It can be configured to disable the region, specify it as Top of Range (TOR), Natural aligned four-byte region (NA4) or Naturally aligned power-of-two region (NAPOT).

Right now there is a single PMA check implemented, its job is to check if the memory access is aligned. A word is 32-bit, halfword 16-bit and byte 8-bit. The smallest addressable data unit is one byte long. Therefore a word access is aligned, if the memory address modulo 4 is 0 (two LSBs are zero), for a halfword access the memory address modulo 2 must be zero (LSB is zero) and byte accesses are allowed on every address.
For both units (PMP and PMA) information about the access like the access size and type must be provided, this is done by the control unit. PMP and PMA checks are applied on the data present as soon as the enable signal is applied. Both checks are simple logical functions and must be performed under a clock cycle. The address register is updated with the corresponding address after every PMP, independent of its result. This must be done since the Exception Control needs access to the faulty address at the rising clock edge if an exception is risen.
The logical and is used, in order to ensure that both the *PMA_checker* and *PMP_checker* rules are enforced.

3.5.2 Implementation

3.6 Exception Control

The Exception Control Unit is used to guard exception entries and exits one of its tasks is e.g. to modify the PC accordingly and save information about the exception. In addition, two interrupt entries are guarded by the unit. A list of all supported exceptions and interrupts is listed below:
Exceptions can be caused by the following modules:

- Control Unit

- CSR register file
- PMP & PMA checker

The Control Unit may cause the following exceptions:

- illegal instruction exception
- breakpoint exception
- environment-call-from-M-mode exception

The PMP & PMA checker may cause the following exceptions:

- load access fault exception
- store/AMO access fault exception
- instruction access fault exception
- load address misaligned exception
- store/AMO address misaligned exception
- instruction address misaligned exception

The CSR register file may cause the following exceptions/interrupts:

- timer interrupt
- software interrupt
- illegal instruction exception

3.6.1 Architecture and Design

Figure 3.17 shows the architecture of the Exception Control:

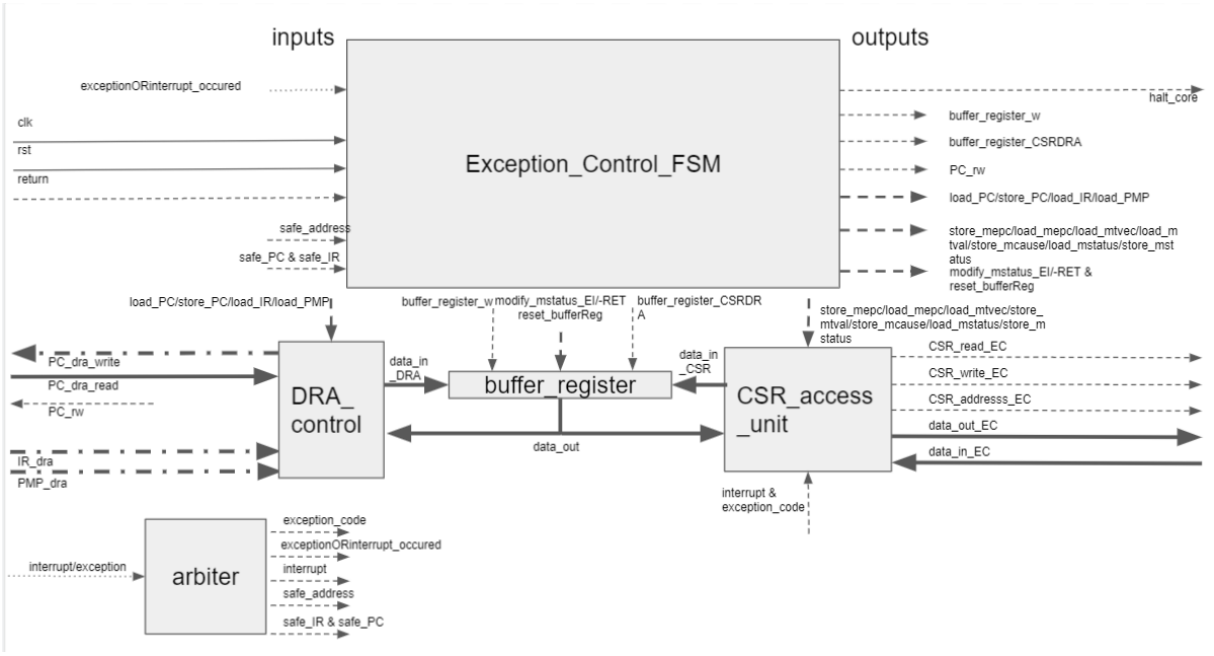

Figure 3.17: Exception Control Architecture

The Exception Control module is comprised of a FSM, an arbiter to decide if an interrupt or exception is taking place and which one shall be handled if multiple are raised at a time. To modify registers a *DRA_control* as well as a *CSR_access_unit* and a buffer register are added to the design.

The arbiter receives the different exception and interrupt signals, it's purpose is to decide which interrupt will be executed and generate the according exception code as well as the signal for the FSM to start the routine.

The *DRA_control* module is used to load the Instruction Register, PMP address register and Program Counter. A load to the PC may also be performed, in order to do so the *PC_rw* signals must be asserted one clock cycle earlier by the FSM.

The *buffer_register* is implemented to allow data shares between the *DRA_control* and *CSR_access_unit*. It implements another functionality that allows to set either the MIE register to 1 (exit) or the MPIE register to 0 (entry) and switch the two bits (MIE and MPIE) on the *data_out* line. This feature is used during the phase of modifying the *mstatus* register and allows the modify to happen in at least two clock cycles.

The *CSR_access_unit* is used to perform register accesses to the CSR register file. During Exception entry or return the data bus B must be connected to the *data_in_EC* bus and the *data_in* bus to the *data_out_EC* bus. This is done by implementing a multiplexer at the corresponding buses controlled by the *halt_core* signal.

If an Exception or Interrupt is raised, the Exception Control unit must write the current *PC+4* to the *mpec* register, modify the *mcause* register to reflect the cause of the exception/interrupt and update the *mtval* CSR to provide additional information on the taken

trap. If multiple exceptions occur at once, only the highest priority exception is taken. If an Exception is raised, while the processor is handling another exception, *mpec*, *mcause* & *mtval* are overwritten. The saving of the return address and other information stored in those registers is left to the trap handler, in order to avoid a large hardware register stack. If an exception entry is performed the *exceptionORinterrupt_occured* signal on the FSM is high, if the return signal is high it indicates that an exit shall be performed, however if both signals are high (should not happen in normal operation) the entry will be performed.

3.6.2 Implementation

3.7 AXI4-Lite Master

To connect the processor to peripherals the AXI4-Lite protocol is used. Due to its popularity many IPs such as BRAM can be connected to each other using an Interconnect. EDRICO contains a Master and a Slave interface. Both of which are explained in more detail in the following sections:

3.7.1 Architecture and Design

The AXI4-Lite Master is implemented in order to allow memory accesses e.g. to a BRAM or UART IP. The following figure depicts the architecture of the master:

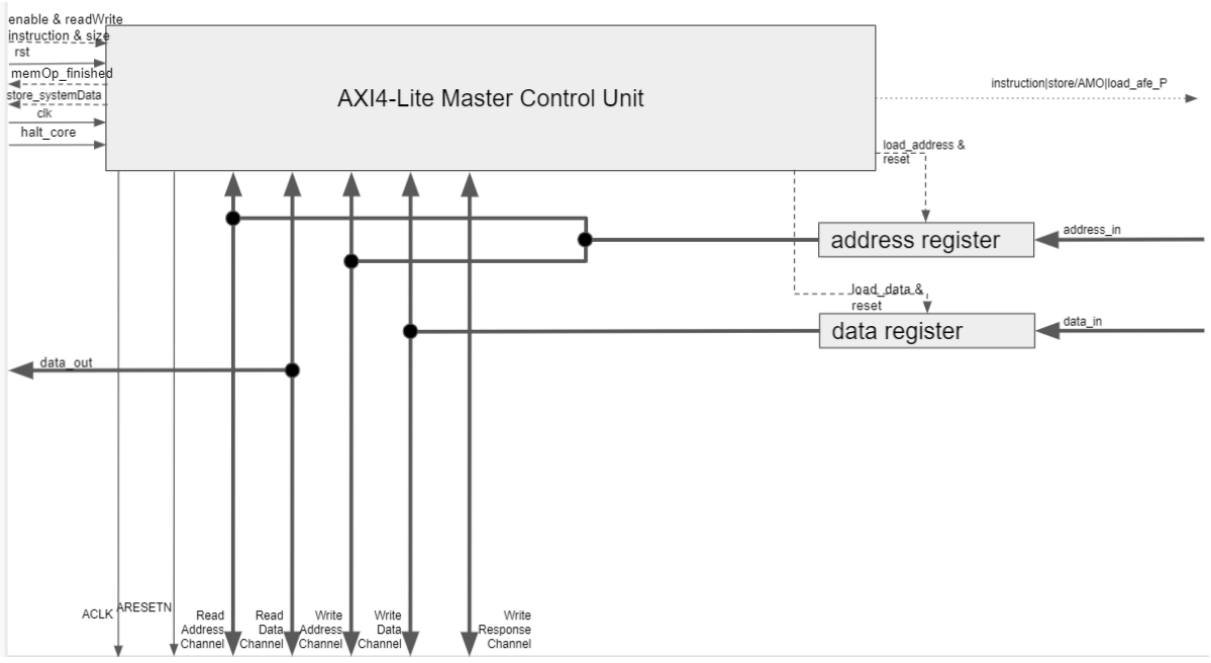

Figure 3.18: AXI4-Lite Master Architecture

It includes two registers, the data register and the address register, these are loaded on the rising edge of the system clock if the corresponding load signal is applied. Both register outputs are constantly applied to the corresponding AXI signals *(AWADDR, ARADDR and WDATA)*.
The AXI4-Lite Master Control Unit is in charge of controlling the AXI Transfer. It controls the ready and valid signals as well as the register reads and writes. It is clocked with *clk*. The *rst* signal will reset it. The Master also provides the clock and reset for every slave connected to the AXI interconnect. To start a transfer, the enable signal must be high on a rising edge of the clock, in that case the address and data register are loaded on the next falling edge of system clock.
If data is ready to be read from the system bus, it is routed to an output of the Master and the *store_systemSystemData* is set to high, in order to ensure a correct read, this process shall not be clocked. The surrounding system must then process these signals to store the data in the correct register.
At the end of a data transfer, the *memOp_finished* signal is set to high and remains high until a new transfer is initiated.
If an error occurred during an access, the *instruction_afe_P*, *storeAMO_afe_P* or *load_afe_P* exceptions are raised. And remain high until the *halt_core* signal is applied to the AXI4-Lite Master Control Unit.

3.7.2 Implementation

3.8 AXI4-Lite Slave

Some of the RISC-V CSRs must be memory mapped, meaning the must be accessible by other devices via the memory space. The addresses can be specified by setting a generic in the VHDL code. A basic address is predefined for each CSR, corresponding to the CLINT module by sifive since this is the closest thing to industry standard.

register	address	access	width	description
msip	0x0200_0000	R/W	32-bit	hold software interrupt pending bit
mtimecmp	0x0200_4000	R/W	32-bit	hold time compare value (lower 32 bit)
mtimecmph	0x0200_0004	R/W	32-bit	hold time compare value (upper 32 bit)
mtime	0x0200_BFF8	R/W	32-bit	hold time (lower 32 bit)
mtimeh	0x0200_BFFB	R/W	32-bit	hold time (upper 32 bit)

Table 3.6: Memory Mapped CSRs

3.8.1 Architecture and Design

The AXI4-Lite slave is in charge of accepting data transfers and reading/writing the CSRs. Figure 3.19 shows the architecture, including the memory mapped CSRs:

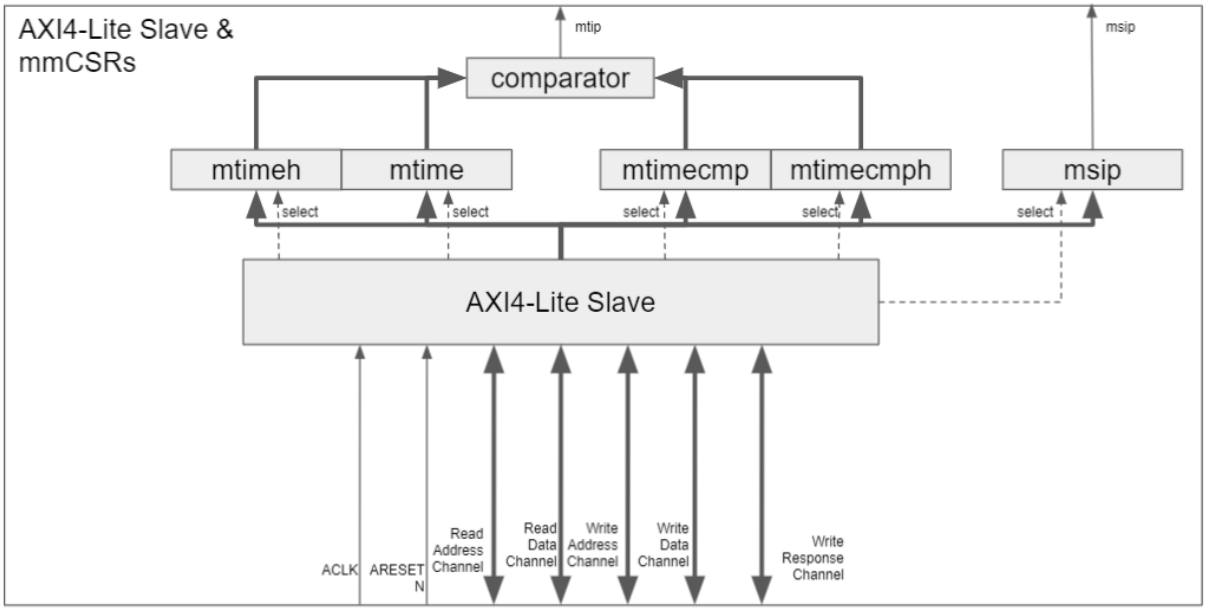

Figure 3.19: AXI4-Lite Slave Architecture

As an AXI4-Lite slave an IP core may be used. In fact the Vivado AXI Interface generator may be used to generate the AXI4-Lite Slave as well as the registers, this IP could then be modified with the comparator and the *msip* and *mtip* output The AXI Slave allows reads and writes to the 32 bit registers *mtimeh*, *mtime*, *mtimecmp* and *mtimecmph* and the one byte *msip* register.
The comparator is used to trigger a timer interrupt. It compares *mtime* and *mtimecmp*.

If the value of *mtime* is equal or greater than the one in *mtimecmp*, the *mtip* signal is asserted.
The interrupt remains posted, until it is cleared by writing to the *mtimecmp* register. The *msip* register is a one byte register, the remaining 31 bits are hardwired to zero. Its reset value is zero. If it is set to one, the *msip* bit in *mip* is set and therefore, a software interrupts may be risen.
Table 3.8.1 shows the reset values for each CSR:

register	**value**
msip	'0'
mtimeh	0x00000000
mtime	0x00000000
mtimecmph	0xFFFFFFFF
mtimecmp	0xFFFFFFFF

Table 3.7: Memory Mapped CSRs reset values

3.8.2 Implementation

4 Test and Verification

4.1 Unit and Integration Verification

4.2 System Verification

After successful unit and integration verification, the entire system must be verified. This is done in Simulation to ensure that the system works before performing synthesis and Place and Route (PaR) to map the core in a FPGA.
There are basically two ways to do this. Designated tools exist to test a custom RISC-V core for its functionality. These often require a specific debug interface such as the RISC-V External Debug Support: **riscv:debug**. An example for such a verification IP is the Imperas RISC-V Reference Model. Due to the not implemented debug interface as well pressure of time to verify the functionality, another approach for system verification was chosen.
The basic idea is to write a simple test code and define the expected machine state after execution of said code. The code can be written in assembly and assembled using the RISC-V gcc compiler, or any other feasible compiler such as clang. A list of available compilers and software tools can be found at **RV:software**. This test code is then executed in simulation.
In order to execute the code a test bench is implemented, containing a the EDRICO IP, an instruction Read Only Memory (ROM), data Random Access Memory (RAM) and a tester Register Transfer Level (RTL) module. The tester is added to the design in order to provide the proper reset and clock signals. As an additional feature it can be configured to check the machine status after execution and display status messages.
Debug outputs are added to the EDRICO IP for every register inside the RF block as well as the Instruction Register (IR) and Programm Counter (PC). The test bench also contains an AXI inteconnect, this allows to connect multiple s to a single AXI-master. The interconnect is, as well as the RAM and ROM, an IP block provided by Xilinx. The test bench can be found in the appendix.
Figure 4.1 shows the memory map of the test bench.

Figure 4.1: memory map of the system verification test bench

The instruction ROM is defined to start at address 0x00000000 it has a size of 8KB. This is sufficient, since the test cases contain a fairly small amount of code to be executed. The same applies to the 8KB data memory at the base address of 0xA0000000.
In between data and instruction memory, a 32KB address space is reserved for the memory mapped CSR.

The test code is written in assembly, it is designed to test every RV32I instruction that is implemented. Therefore in this first test, no Zicsr instructions are tested. Hence only the GPR and PC contents need to be verified after execution. The IR does not need verification, since any error in it will cause the machine to work in an undefined state, which would modify contents of the other registers to be unequal to the expected outcome. Table 4.2 compares expected and actual register values:

Register	Expected	Actual	Register	Expected	Actual
PC	0x000000C0	0x00000000	x16	0x0A000000	0x0A000000
x1	0xA0000000	0xA0000000	x17	0x00010000	0x00010000
x2	0xC0BAD000	0xC0BAD000	x18	0x00000000	0x00000000
x3	0x12345000	0x12345000	x19	0x00000001	0x00000001
x4	0x00001000	0x00001000	x20	0xC0BAC000	0xC0BAC000
x5	0x000000AB	0x000000AB	x21	0xC0BAD000	0xC0BAD000
x6	0x12345014	0x12345014	x22	0x00000000	0x00000000
x7	0x0000C0BA	0x0000D000	x23	0x12344000	0x12344000
x8	0x000000C0	0x00000000	x24	0xD2EF2000	0xD2EF2000
x9	0x12345000	0x13450000	x25	0xF4000000	0xF4000000
x10	0xFFFFC0BA	0xFFFFD000	x26	0x28000000	0x28000000
x11	0xFFFFFFC0	0x00000000	x27	0x00010000	0x00010000
x12	0x00000000	0x00000000	x28	0x00000000	0x00000000
x13	0x123451EA	0x123451EA	x29	0x00000001	0x00000001
x14	0x00000004	0x00000004	x30	0xA0000100	0xA0000100
x15	0xFA000000	0xFA000000	x31	0x000000B8	0x000000B8

Table 4.1: System Verification results and expected values

The test code is made up of 48 instructions, therefore the PC is expected to be:

$$PC = 48 * 4 = 192 = 0xC0$$

after execution. When taking a look at table 4.2 one sees a difference between the expected and actual result for the PC. This problem is caused by the last instruction that is executed. It is a jump back to the start of the address, hence 0x00000000. After investigating the assembly code, the cause for this behavior is found. The last instruction is a Jump and Link Register (JALR) instruction.

```
1  JAL x31, 8 #jump 8 byte
2  NOP
3  JALR x0, x0, 0 #jump to start
```

Listing 4.1: Snippet 1 from the executed test code

Therefor the PC is set to 0x00000000. Using the simulators waveform viewer, it can be verified that the PC prior to this instruction was set to 0x000000BC. This confirms the correct behavior of the program counter register during execution.
Comparing the remaining results in the table shows another error at registers x7,x8, x10 and x11. The instructions responsible for these registers are shown below:

```
1  SW x2, 0(x1)
2  SW x3, 4(x1)
3  SW x4, 8(x1)
4  ADDI x5, x0, 0xAB
5  SB x5, 13(x1)
6  SH x2, 14(x1)
7
8  LB x11, 3(x1) #expect 0xFFFFFFC0
9  LH x10, 2(x1) #expect 0xFFFFC0BA
10 LW x9, 4(x1) #expect 0x12345000
11 LBU x8, 3(x1) #expect 0x000000C0
12 LHU x7, 2(x1) #expect 0x0000C0BA
```

Listing 4.2: Snippet 2 from the executed test code

This code snippet shows how the memory at base address x1 is modified by multiple store word, half-word and byte instructions. In the second part of the code x11 to x7 are modified by load instructions. It is interesting to note, that only x9 contains the expected results, and that the instruction modifying x9 is a load word instruction. To see if the error is caused by the load instructions or if the store instructions are wrong, the memory is checked. Figure 4.2 shows the memory in the simulation wave form view:

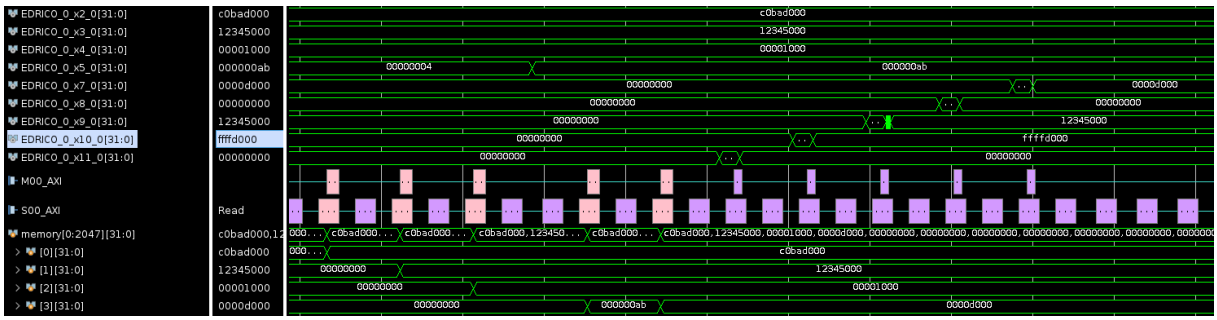

Figure 4.2: wave from view of the memory, AXI4-Lite transfer, x2-x5 and x7-x11 during System Verification

The write transfers are displayed in the light pink-orang-ish colour whereas reads are marked in purple. As verified by comparing the memory contents with the registers x2-x4, all three store word operations are executed correctly. The store byte operation to the 0xA000000D should load 0x0000AB00 into the third memory array, followed by a store half-word to 0xA000000E which should modify the memory contents to be 0xD000AB000. However, the fourth memory element is set to 0x000000AB instead of 0x0000AB00. This is then again overwritten to be 0x0000D000. When taking a closer look at the AXI transfer everything seems fine, the right write addresses are specified and the write strobe signal (which indicates what bytes of the transfer are valid) is correct.
This leads to the conclusion that the mismatch in expected and actual data is not caused by the core itself. Much rather the used memory is not properly byte but word addressable. Future tests must verify this.

One important measured value to compare processor performances is the CPI, hence the amount of clock cycles are needed to execute an instruction. As described earlier, the CPI is calculated using the values of the *mcycle* and *minstret* registers:

$$CPI = \frac{mcycleH >> 32 + mcycle}{minstretH >> 32 + minstret} = \frac{0x207}{0x2b} = 12.07$$

Hence in average every instruction takes 12.07 clock cycles to execute. Of course this value is highly dependent on the ratio of load/store instructions to other operations. An instruction accessing memory takes 18 cycles, whereas normal operations take 10 clock cycles. Therefore improving memory access time will decrease the CPI. Of course this assumption is very vague since, according to Amdahl's law, the improvement will not be linear **patterson:2017**.

5 Future Work

6 Conclusion

Appendix