Bootprocess E310-G000

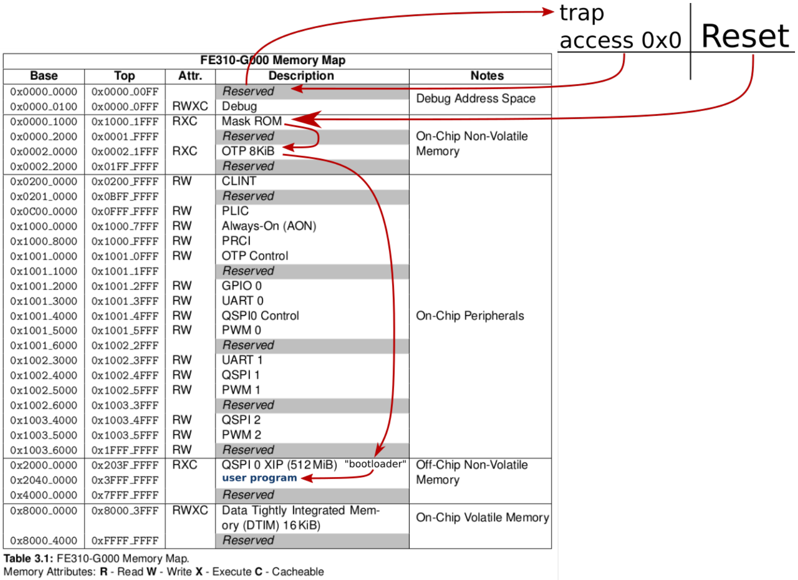
SiFive - HiFive1 Board

Pascal Pieper

Pascal.Pieper@dfki.de

Deutsches Forschungsinstitut
für Künstliche Intelligenz

Cyber-Physical Systems


trap
access 0x0
Reset
"bootloader"
user program

FE310-G000 Memory Map

Base	Top	Attr.	Description	Notes
0x0000_0000	0x0000_00FF		*Reserved*	Debug Address Space
0x0000_0100	0x0000_0FFF	RWXC	Debug	
0x0000_1000	0x1000_1FFF	RXC	Mask ROM	On-Chip Non-Volatile Memory
0x0000_2000	0x0001_FFFF		*Reserved*	
0x0002_0000	0x0002_1FFF	RXC	OTP 8KiB	
0x0002_2000	0x01FF_FFFF		*Reserved*	
0x0200_0000	0x0200_FFFF	RW	CLINT	On-Chip Peripherals
0x0201_0000	0x0BFF_FFFF		*Reserved*	
0x0C00_0000	0x0FFF_FFFF	RW	PLIC	
0x1000_0000	0x1000_7FFF	RW	Always-On (AON)	
0x1000_8000	0x1000_FFFF	RW	PRCI	
0x1001_0000	0x1001_0FFF	RW	OTP Control	
0x1001_1000	0x1001_1FFF		*Reserved*	
0x1001_2000	0x1001_2FFF	RW	GPIO 0	
0x1001_3000	0x1001_3FFF	RW	UART 0	
0x1001_4000	0x1001_4FFF	RW	QSPI0 Control	
0x1001_5000	0x1001_5FFF	RW	PWM 0	
0x1001_6000	0x1002_2FFF		*Reserved*	
0x1002_3000	0x1002_3FFF	RW	UART 1	
0x1002_4000	0x1002_4FFF	RW	QSPI 1	
0x1002_5000	0x1002_5FFF	RW	PWM 1	
0x1002_6000	0x1003_3FFF		*Reserved*	
0x1003_4000	0x1003_4FFF	RW	QSPI 2	
0x1003_5000	0x1003_5FFF	RW	PWM 2	
0x1003_6000	0x1FFF_FFFF	RW	*Reserved*	
0x2000_0000	0x203F_FFFF	RXC	QSPI 0 XIP (512 MiB)	Off-Chip Non-Volatile Memory
0x2040_0000	0x3FFF_FFFF			
0x4000_0000	0x7FFF_FFFF		*Reserved*	
0x8000_0000	0x8000_3FFF	RWXC	Data Tightly Integrated Memory (DTIM) 16 KiB	On-Chip Volatile Memory
0x8000_4000	0xFFFF_FFFF		*Reserved*	

Table 3.1: FE310-G000 Memory Map.
Memory Attributes: **R** - Read **W** - Write **X** - Execute **C** - Cacheable

Figure: Modified, from FE310-G000 Manual

Details

Reset Path

- Initial program counter at `0x1000` (MROM)
- Mask ROM contains single instruction: Jump to `0x2_0000` (OTP)
- One Time Programmable Memory jumps to `0x2000_0000` (QSPI)
- "bootloader" on Flash initializes CPU and jumps to `0x2040_0000` (QSPI)
- User defined program starts

Details

Invalid Access (e.g. nullpointer dereference)

- If trap vector is still default (`0x0`), a null instruction (`0x0000_0000`) is fetched
- Trap vector is called again, looping endlessly
- ... until reset or *debugger* interrupt
- Debug interrupt handler is wired to debug ROM (`0x0400`) which calls debug RAM (`0x0800`)
- Debug RAM may load programs from an *openocd*-session via debug peripheral to "userspace" (`0x2040_0000`)
- Debug RAM finally jumps to user program

Special Memory Regions

OTP (One Time Programmable Memory)

Contains:

- Trim settings for Internal Oscillator (HFROSC)
- Configuration string for chip information
- (Jump to flash bootloader)

Special Memory Regions

Bootloader

Scenario

- User Program modifies system clock and "breaks" the execution
- Debugger peripheral is also dependent on clock

→ Device can’t be programmed
(too little time between reset and execution of "malicious" user program)

Solution

- "bootloader" gets executed first and checks for wakeup reason
- If (manually) reset twice inside booloader, it stops execution (spinlock)

→ user can upload new (hopefully better) program via debugger