



ETHERNET PACKET INSPECTION

IDS solution

Sd. Sg. Maj. ANDREI Marius-Cristian

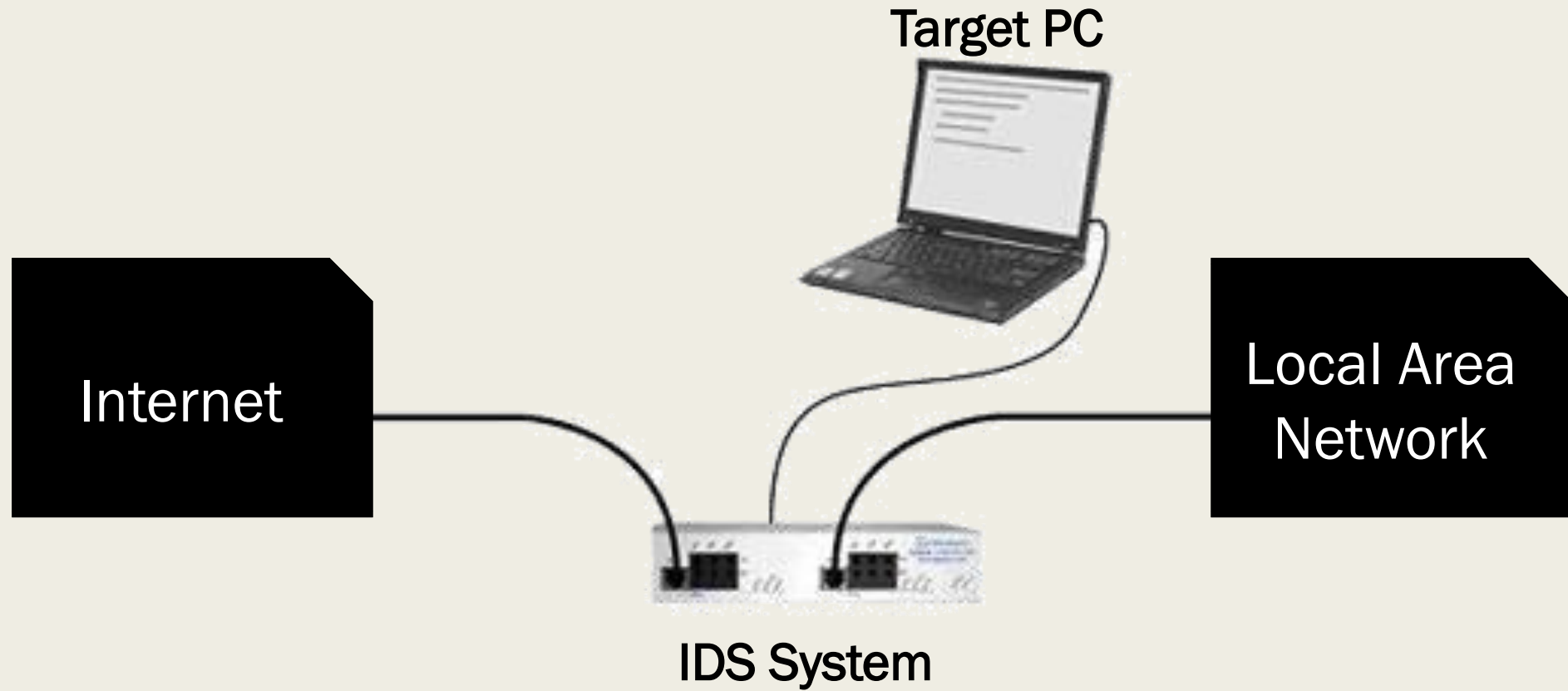


Intrusion Detection Systems

- What is an IDS?
- Most popular IPS/IDS:



Overview



Unauthorized Traffic Detection System as a Solution

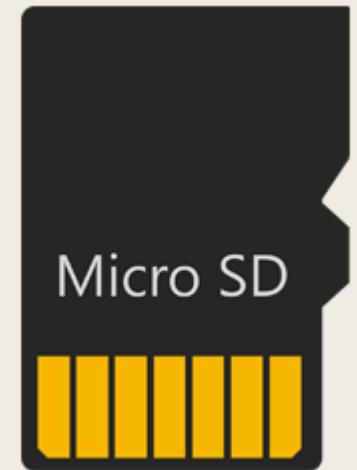
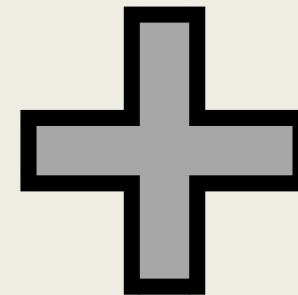
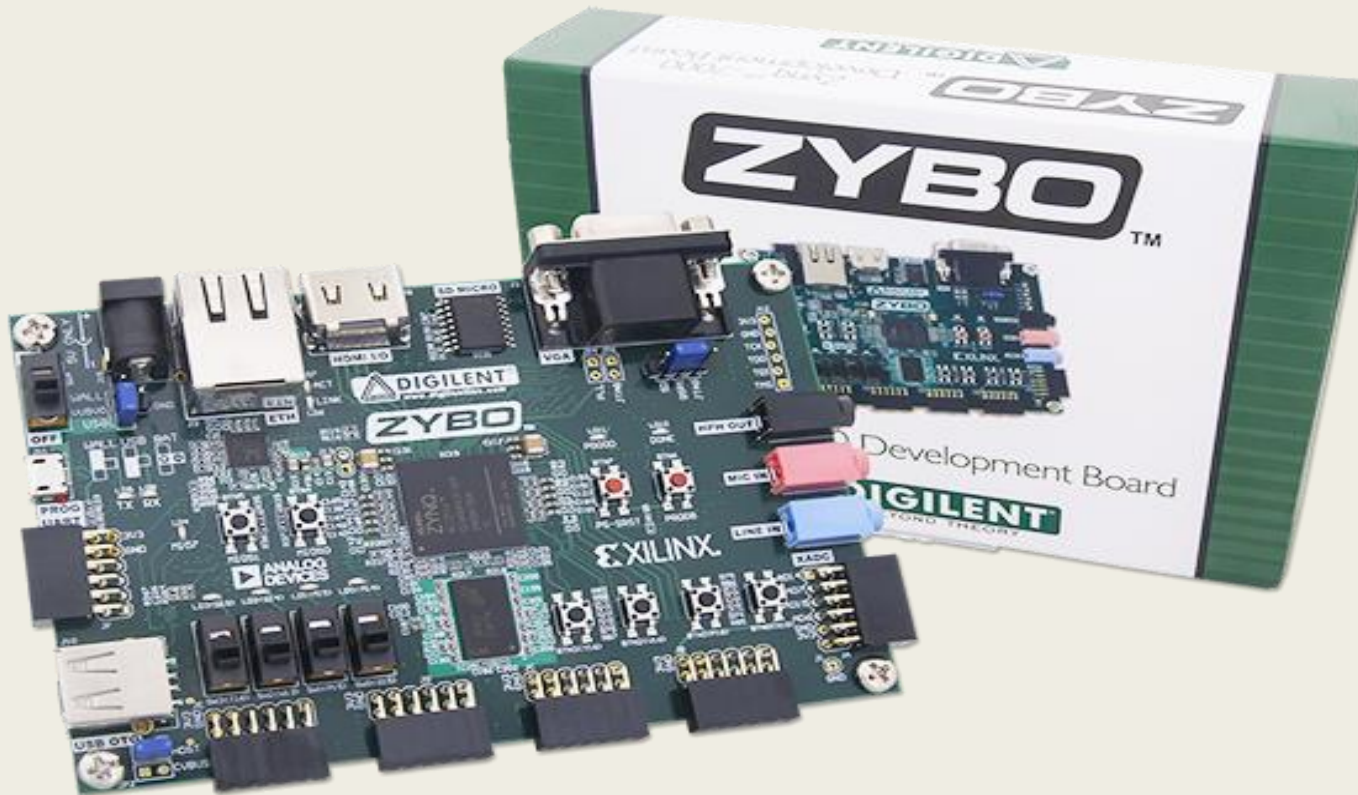
EPI
Solution:

+ Fast

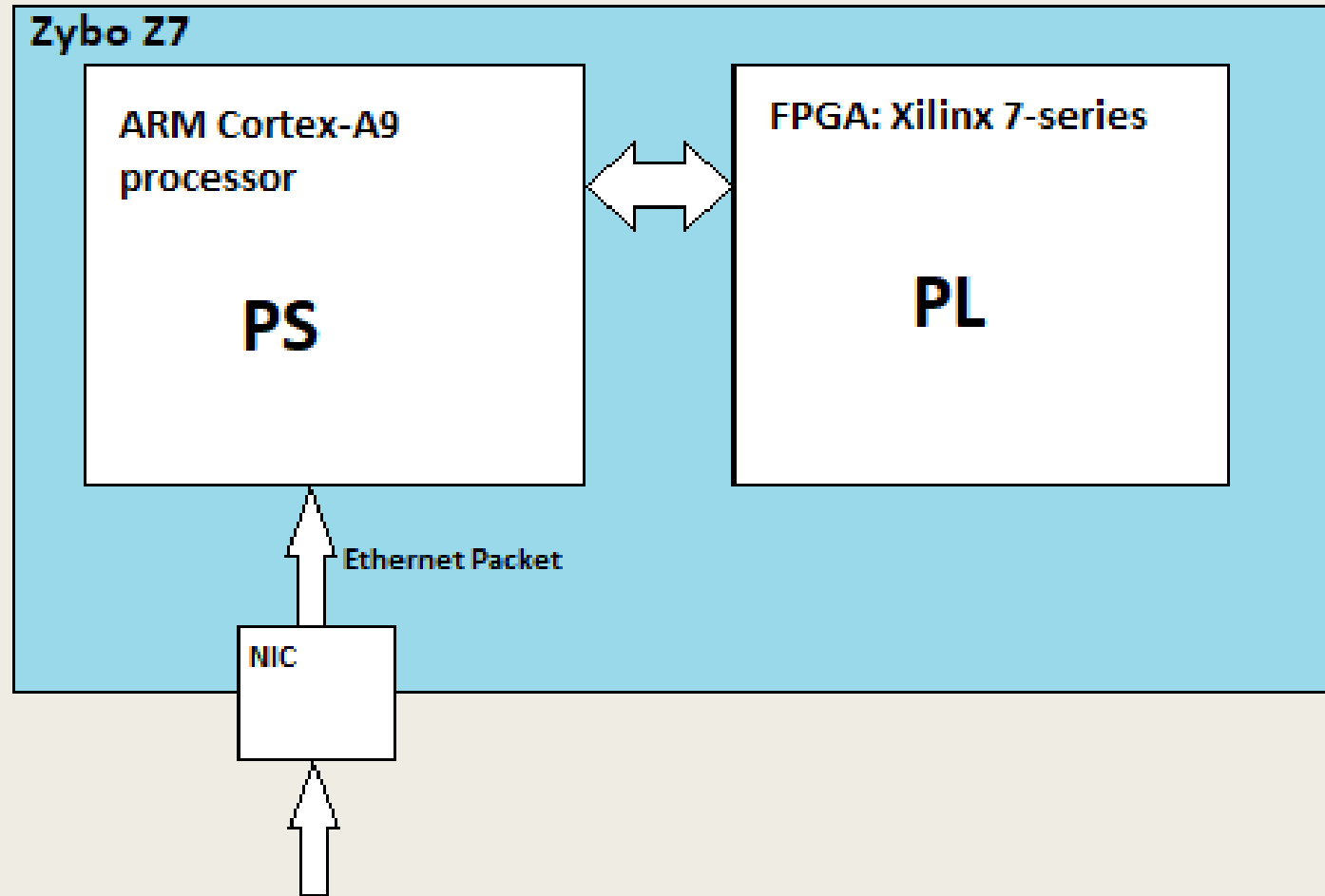
+ Easy to use

- Requires hardware

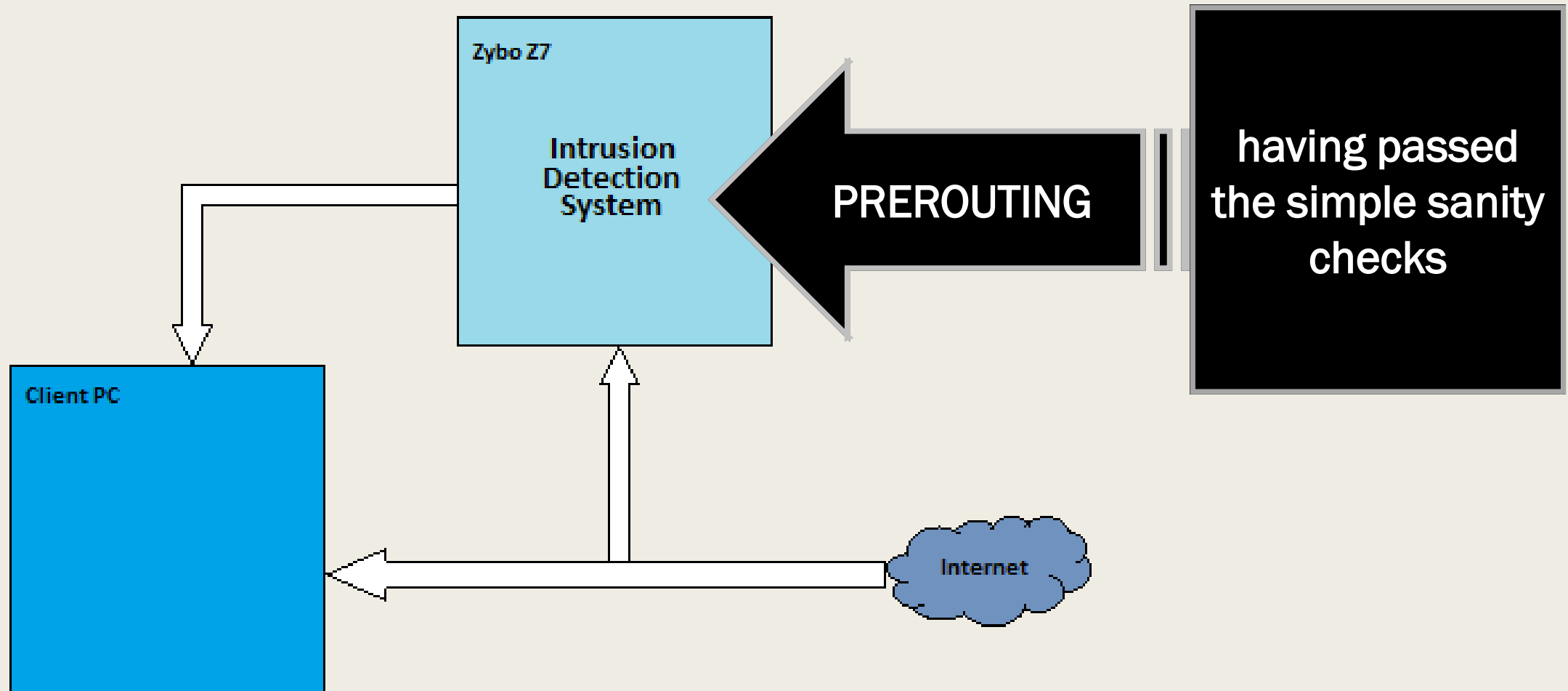
Hardware



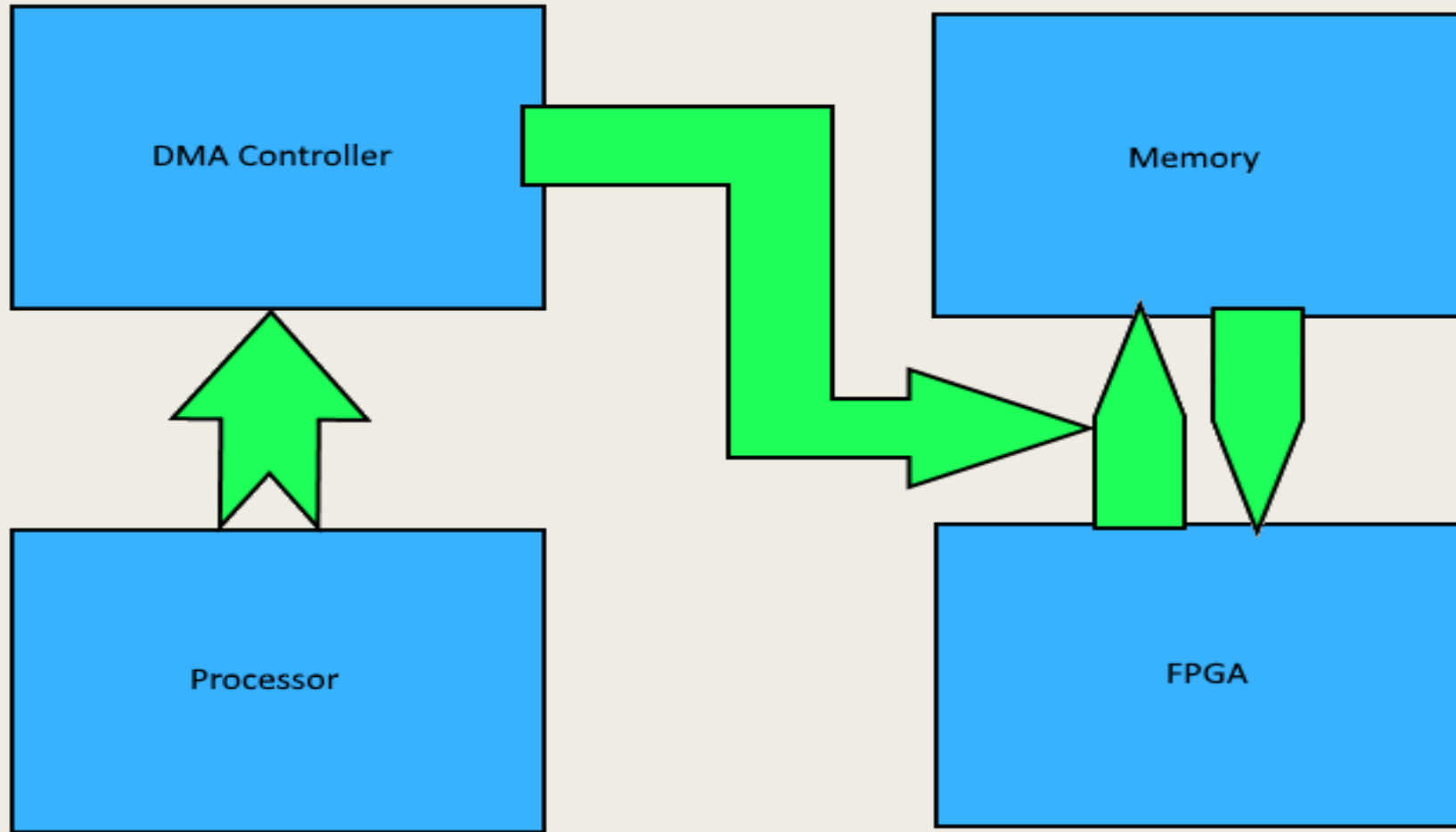
Hardware Design



Hardware Design



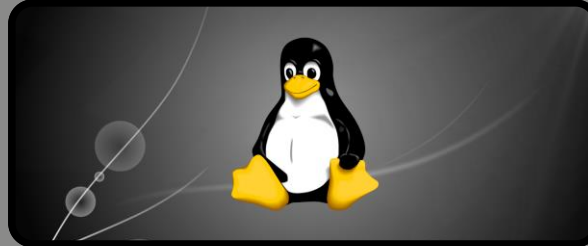
DMA Transfer



Tools



**Xilinx Vivado
Design Suite**



**Linux Kernel
Xilinx**

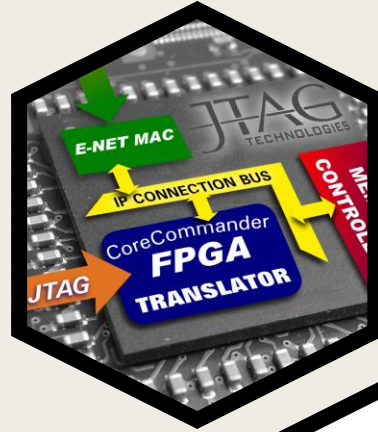
```
/RAM: 1 GiB
ERROR: usb dr_mode not found

it /home/fla/peta_proj/burn_latra/build/tmp/work/plnx_aarch64-xilinx-li
ERROR: usb dr_mode not found

it /home/fla/peta_proj/burn_latra/build/tmp/work/plnx_aarch64-xilinx-li
EL Level: EL2
Chip ID: xczu7ev
MMC: sdhci@ff160000: 0 (eMMC)
reading uboot.env
in: serial
out: serial
err: serial
```

**U-Boot
Xilinx**

Code



FPGA

- 16 strings patterns
- 2048 bytes packets
- Returns Yes/No

Controls the FPGA –
Captures Eth Packets –
Uses DMA transfer –

Driver



App

- User Friendly
- Tests the Data Flow



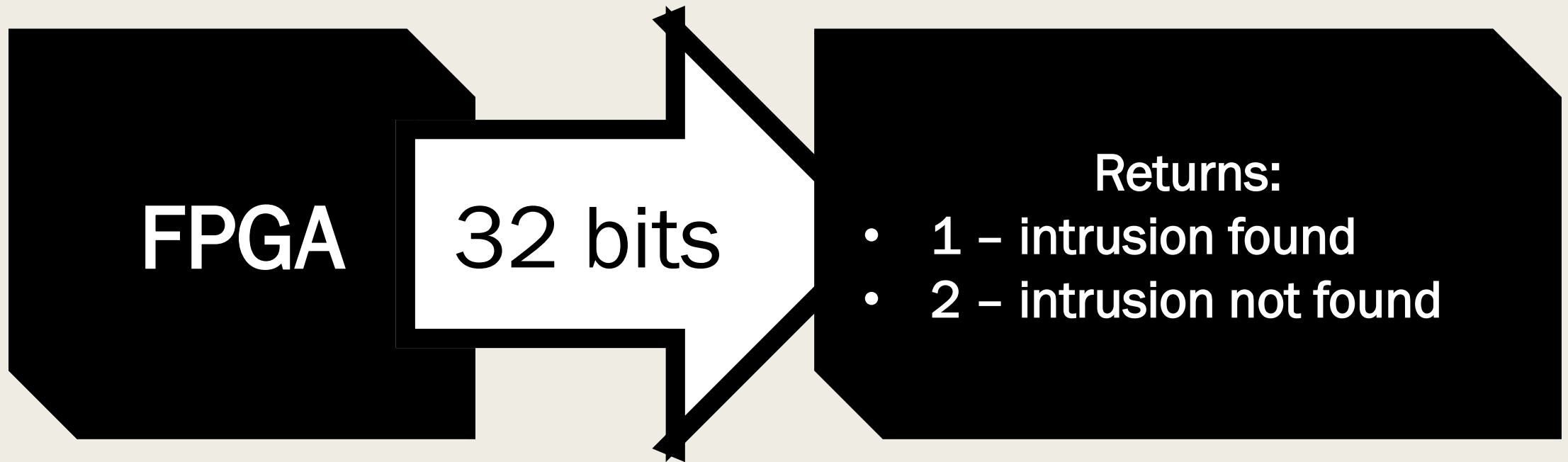
Test

Sample
Data

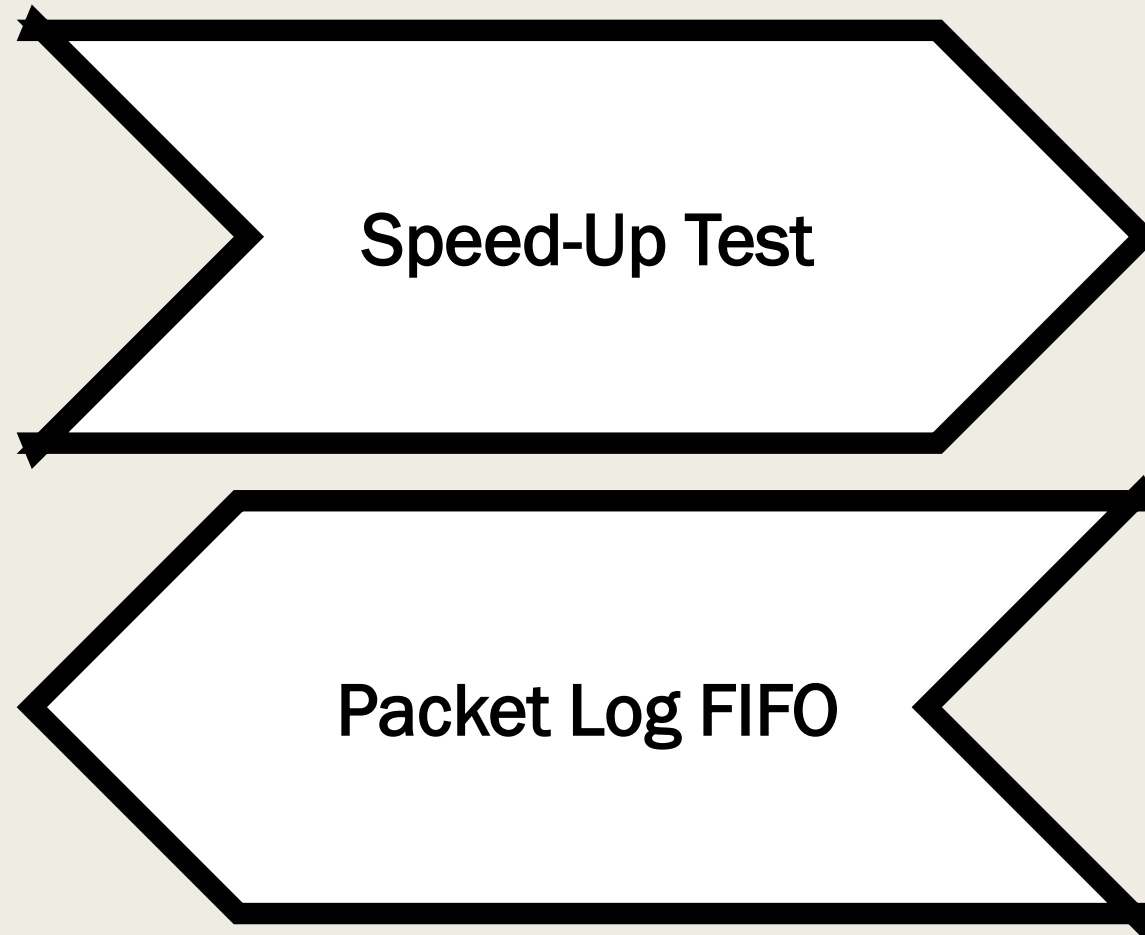


Automatic
check

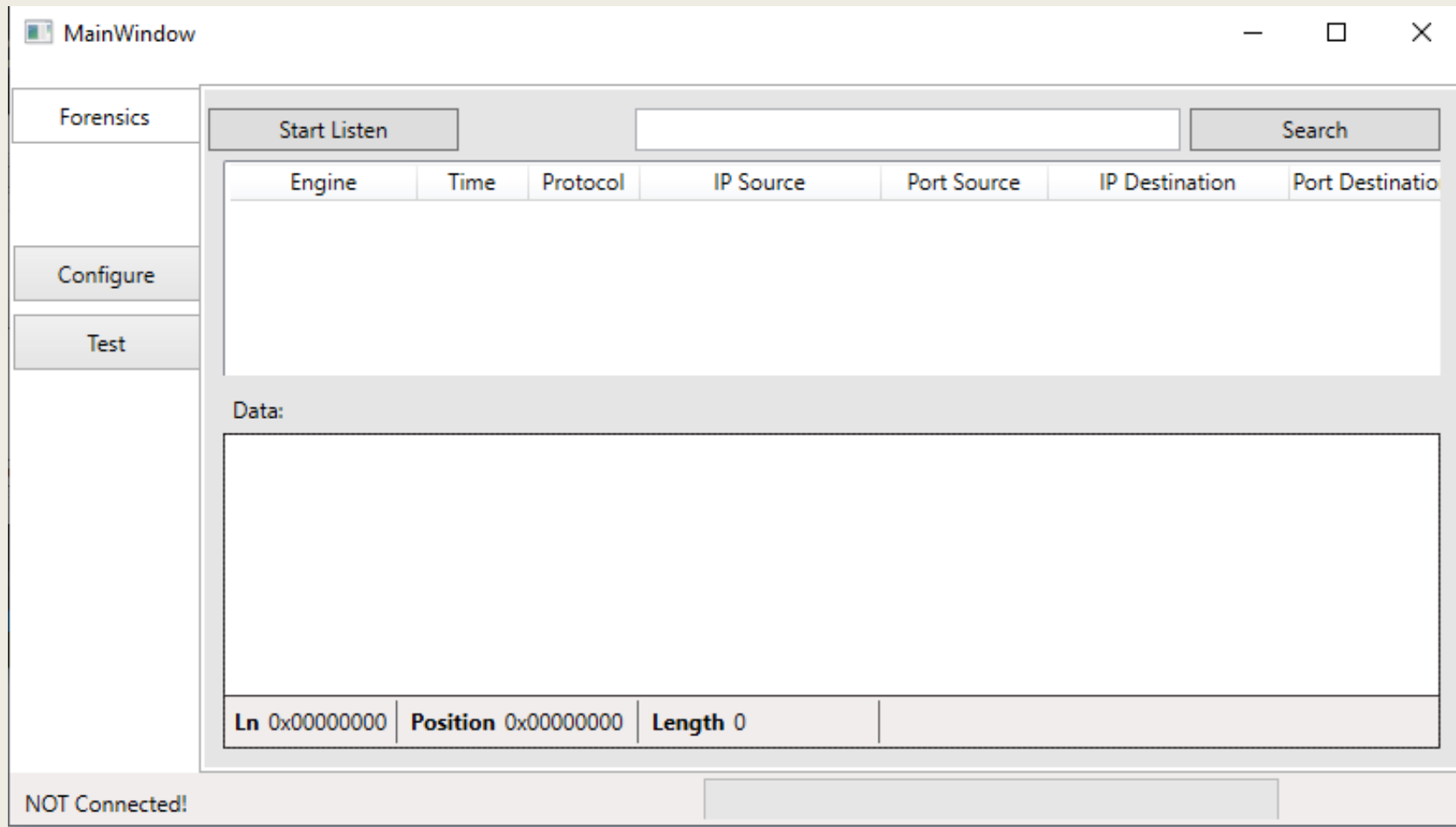
Implementation: FPGA



Implementation: Driver



Implementation: interface




Implementation: Application

- Interface functions to control the FPGA via Driver
- 3 types of tests
- UART communication with Host Computer
- **Main purpose:**
 - *Reads the logs from driver and sends them to the Host Computer*

Quality Assurance

- Unit Tests
- Integration Tests
- System Test

- 
- FPGA = Test Bench
 - Driver = File Functions Calls
 - App = Self Test

- Driver – VIO Core IP
- App – Driver – App Loopback

- Stress Test
- Speed Test
- User Experience Test

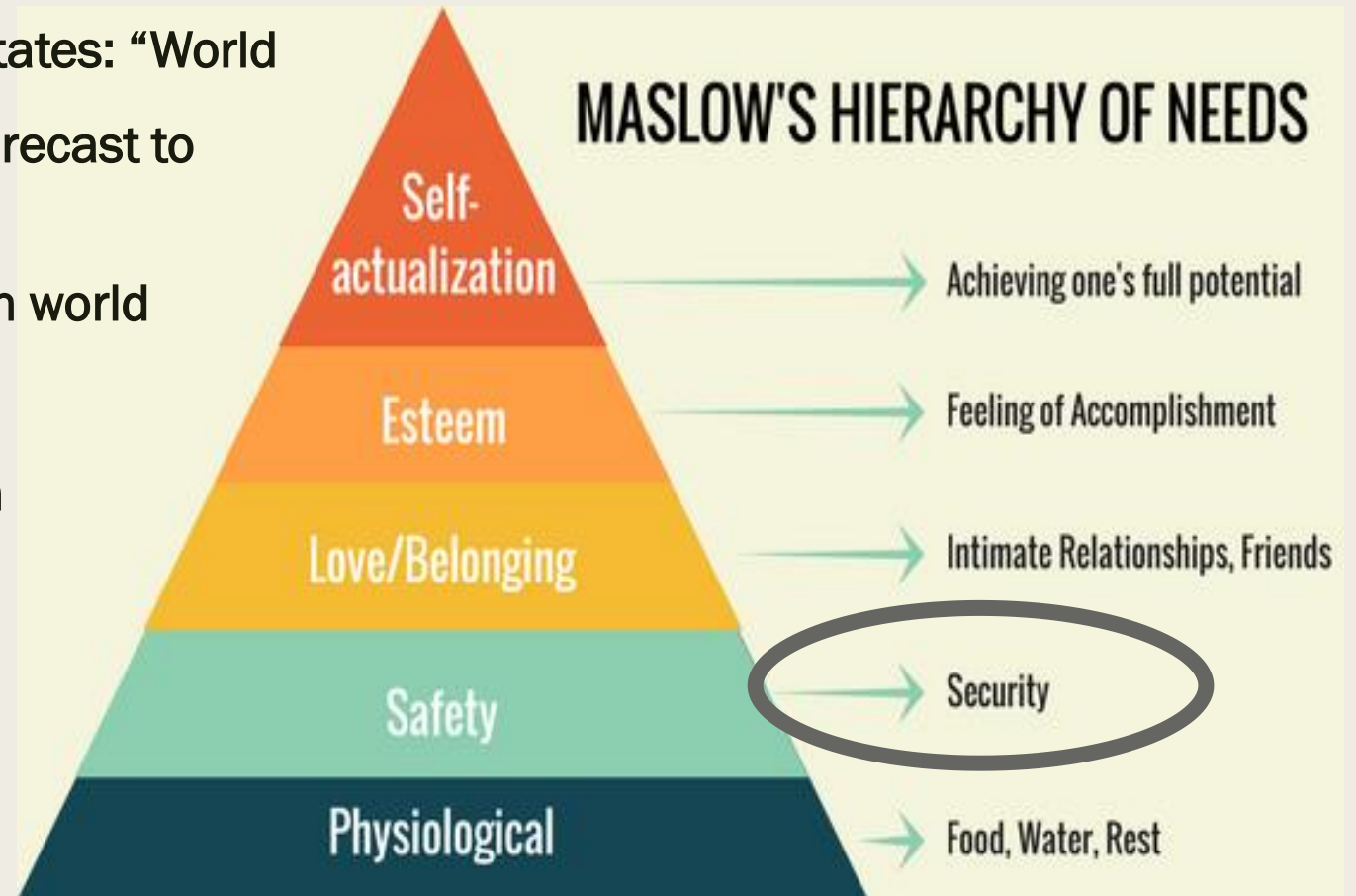
Speed-Up

Speed-Up:
 $3 \rightarrow 6$



Marketing

- In 2016, a [Freedonia](#) research states: “World demand for security equipment is forecast to increase 6.8 percent”
- Size of the industry: \$90.2 billion world security equipment in 2016
- Size of the industry: \$126 billion world security equipment in 2018
- The higher the threat, the higher the *need for security*



Questions?





DEMO