Secure SmartHome

SoC Architectures and Modelling

2016

Michael Astl, Christian Halbfurter, Gregor Hauseder,
Markus Knoll, Hannes Plank, Christian Reisinger,
Roman Silberschneider, Christoph Wiesmeier

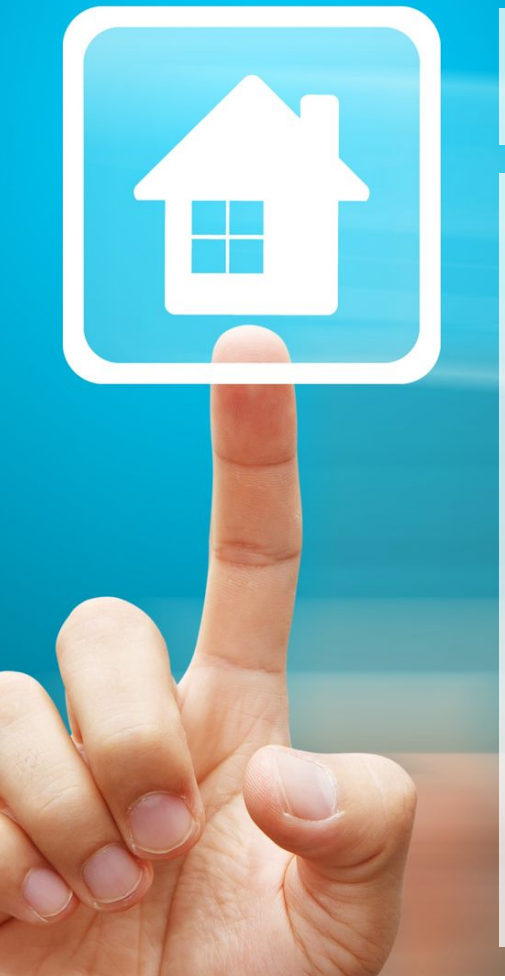
TU Graz

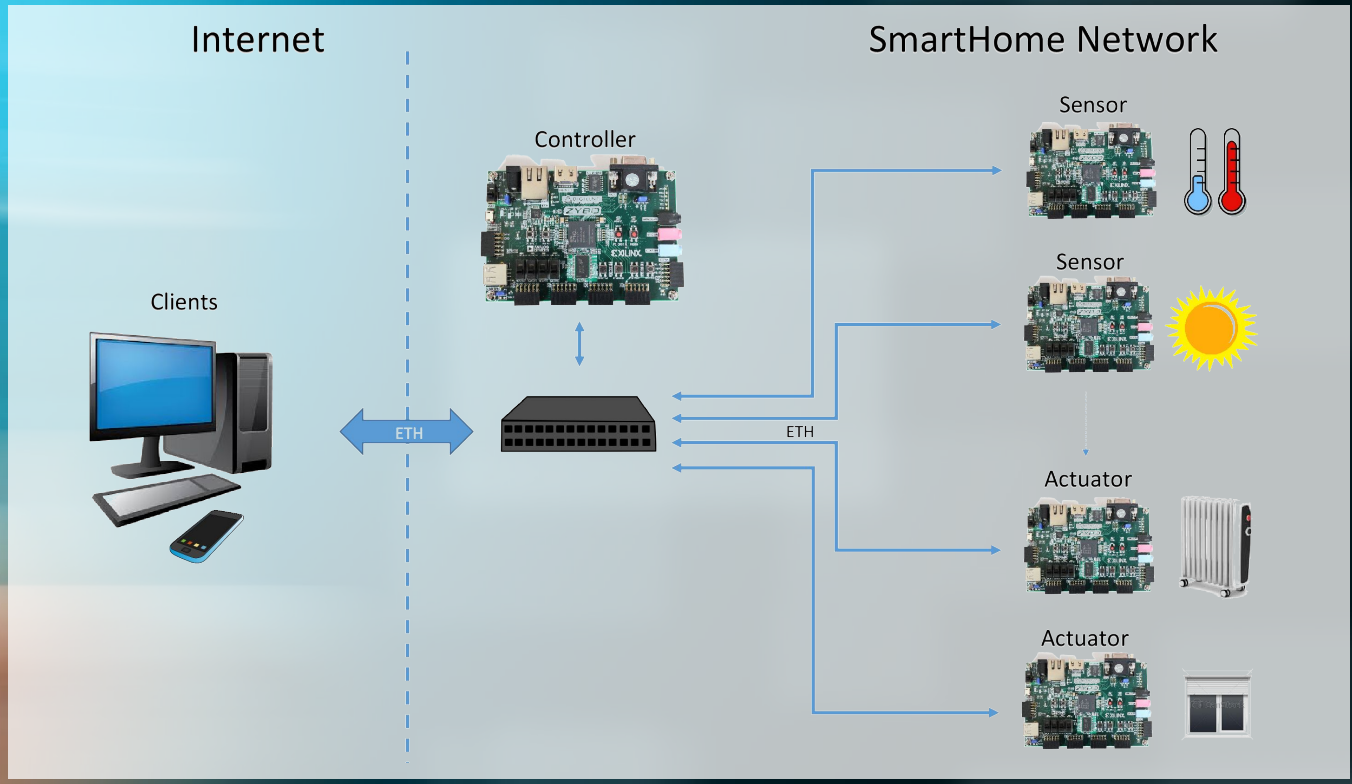
Motivation

Most home automation systems are insecure!

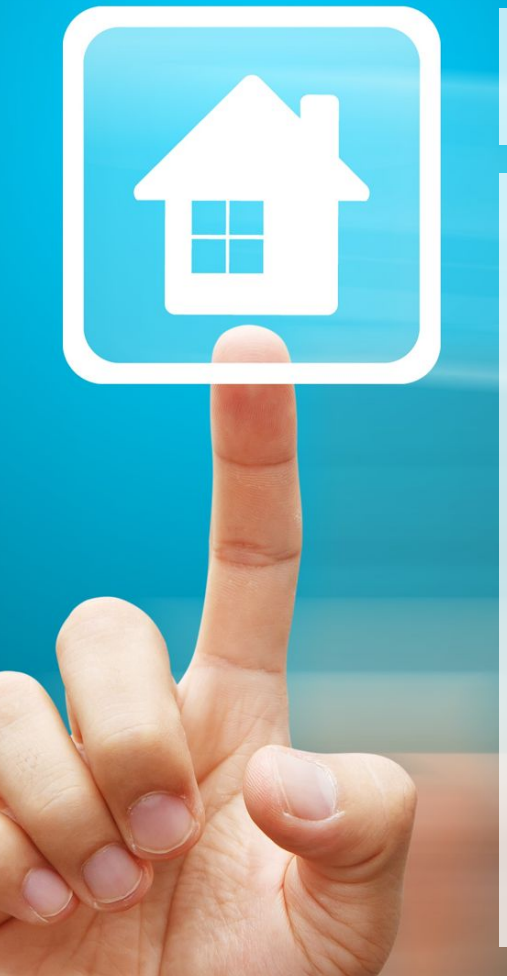
- Connected to the internet
- Sensors and actors connected via local network
- Easy to access the network
- No data encryption
- Manipulate sensor data
- Get control of the house
  - Burglary attacks
  - Military attacks

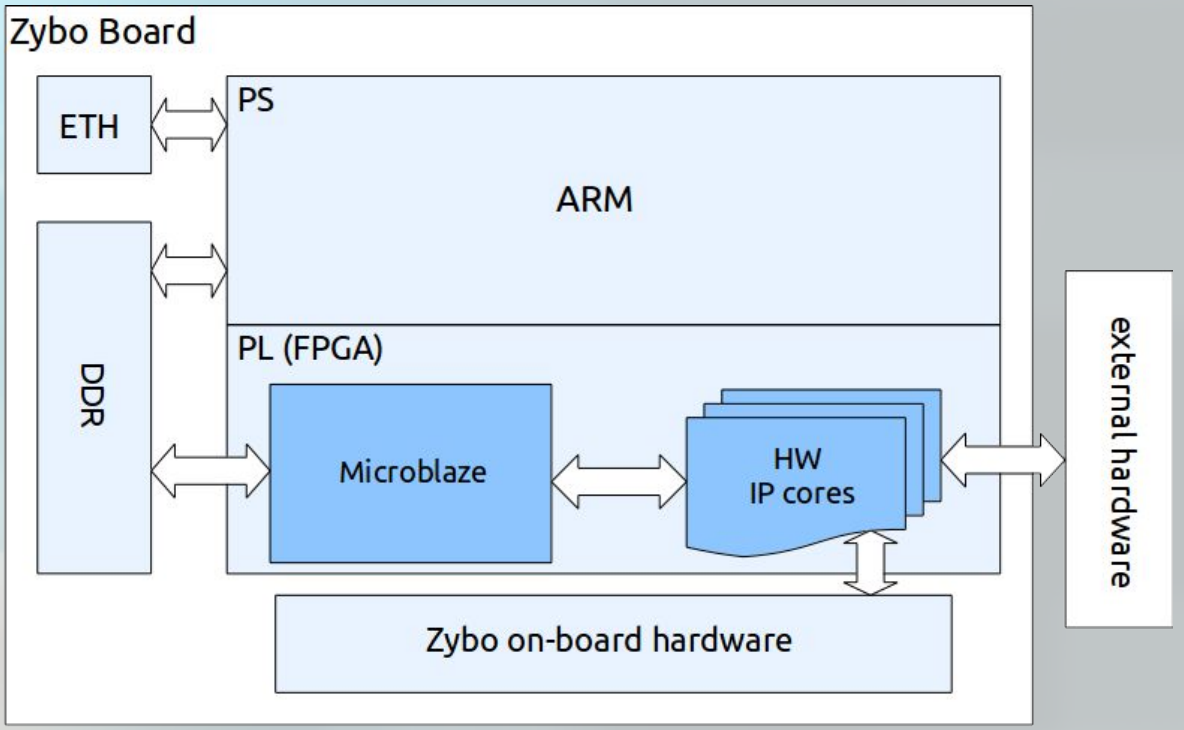
Design Overview



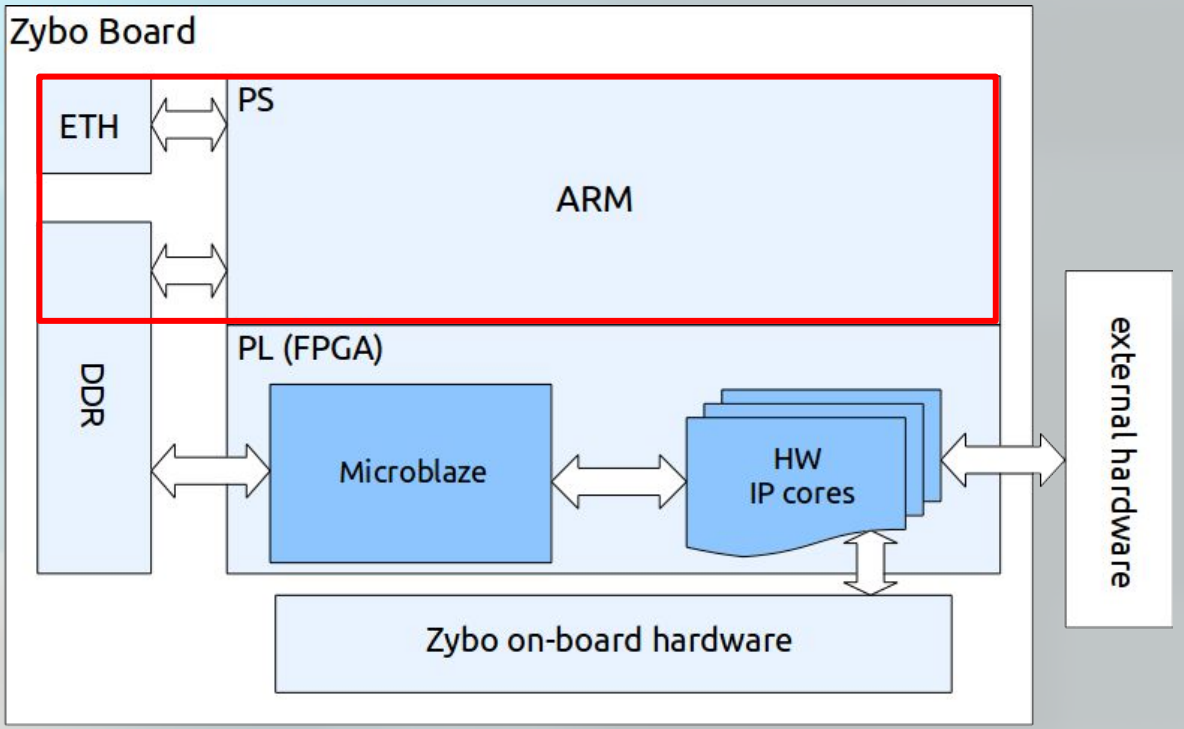


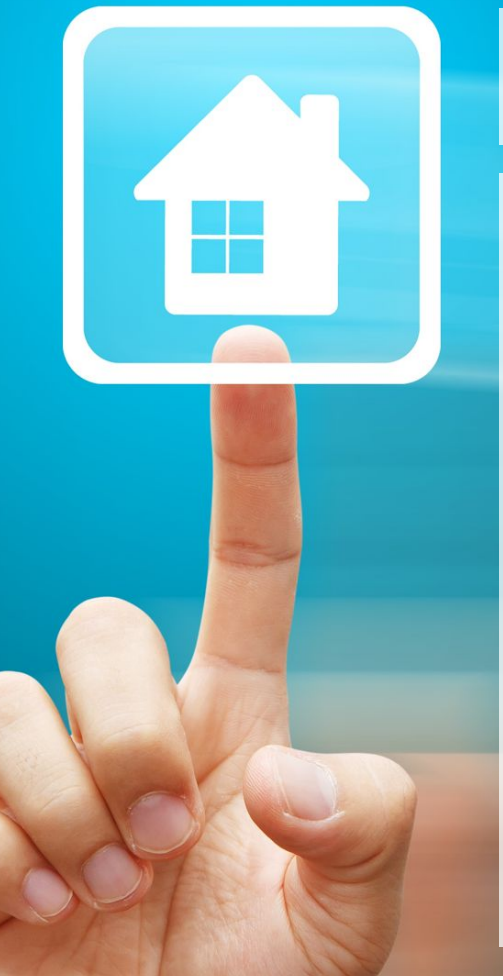
Board Overview





SW/Linux

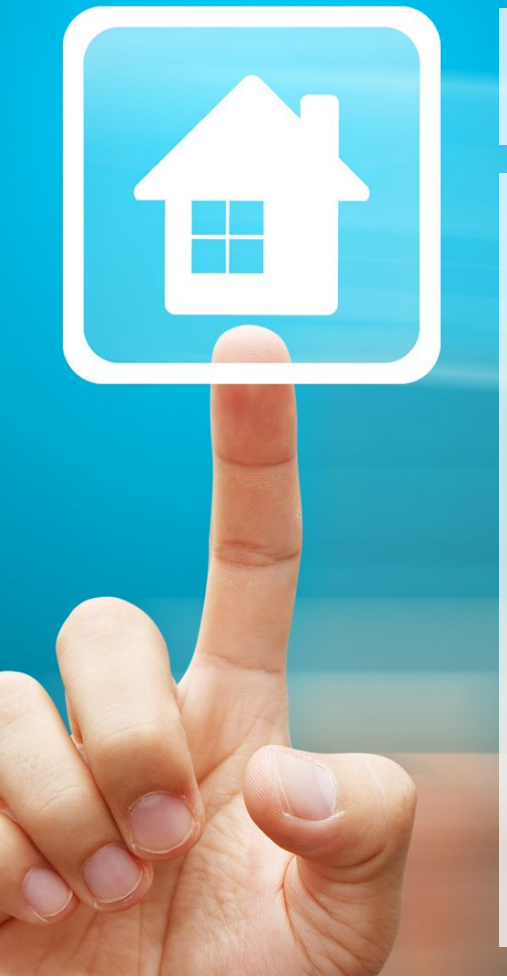

Zybo Board
ETH
PS
ARM
PL (FPGA)
DDR
Microblaze
HW
IP cores
external hardware
Zybo on-board hardware

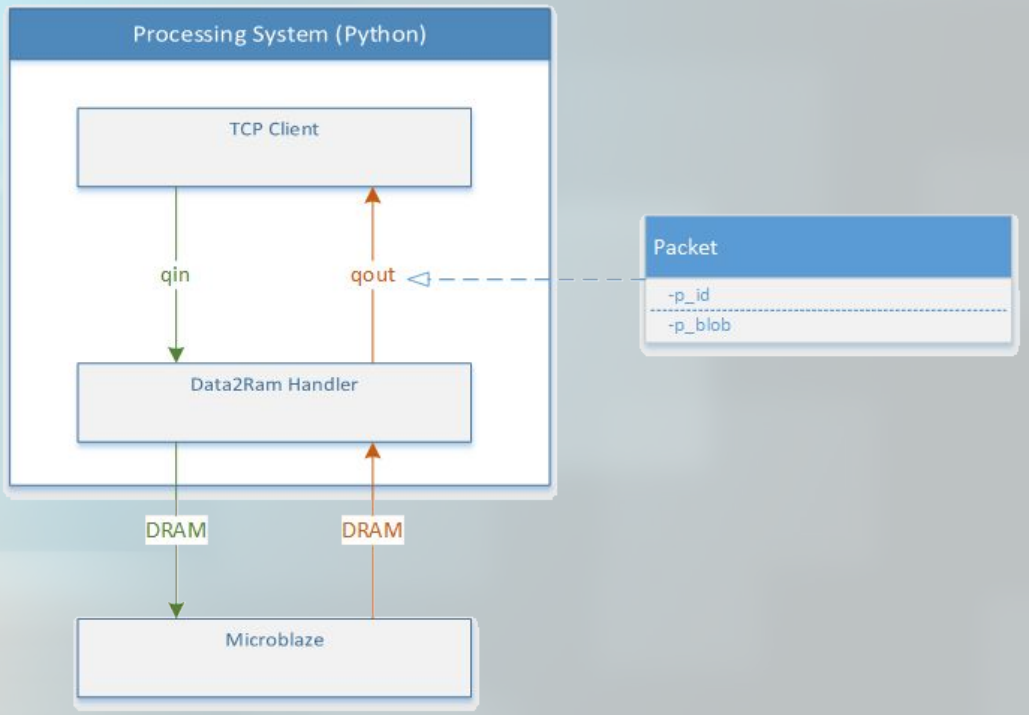


SW/Linux

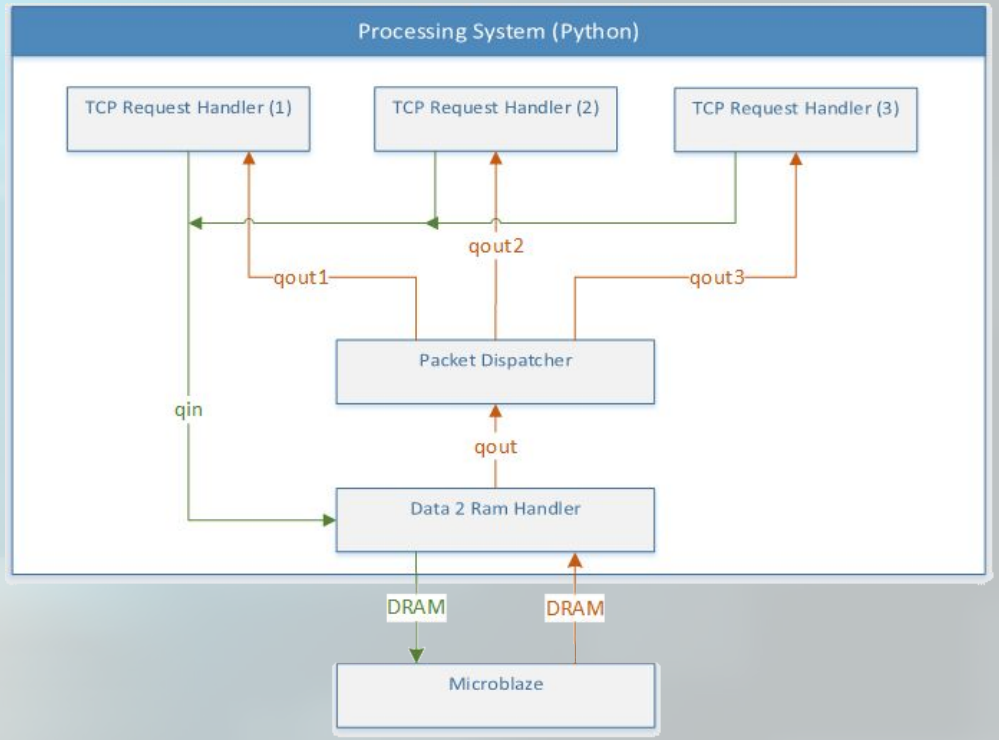
- Buildroot
  - Kernel (version Xilinx-4.4)
  - Rootfs
  - U-Boot
- Python 3.5
  - Node
    - Sensor
    - Actuator
  - Controller
- Data2Ram driver

Communication

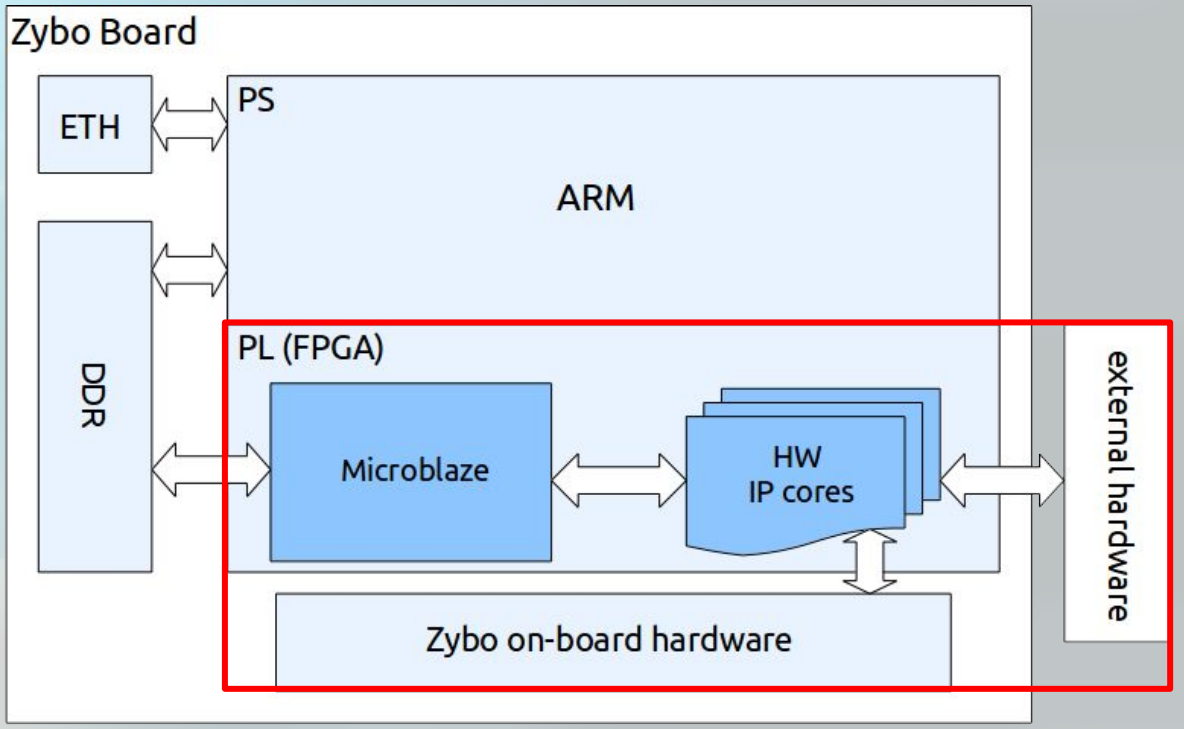




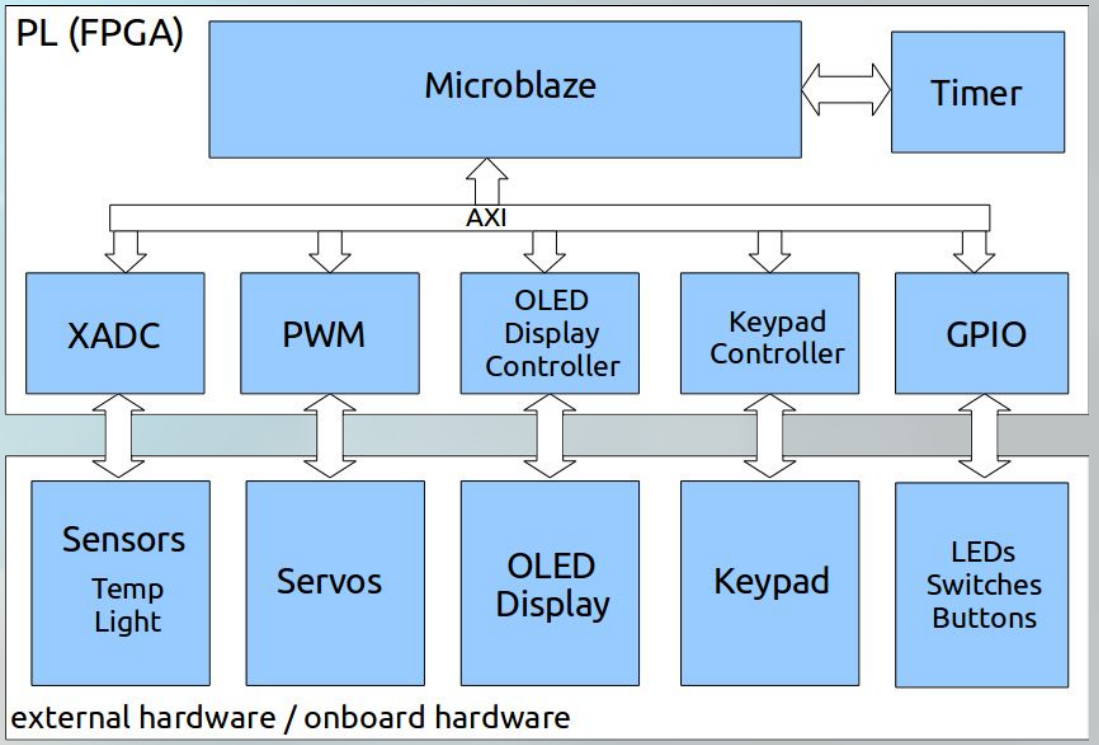
Communication



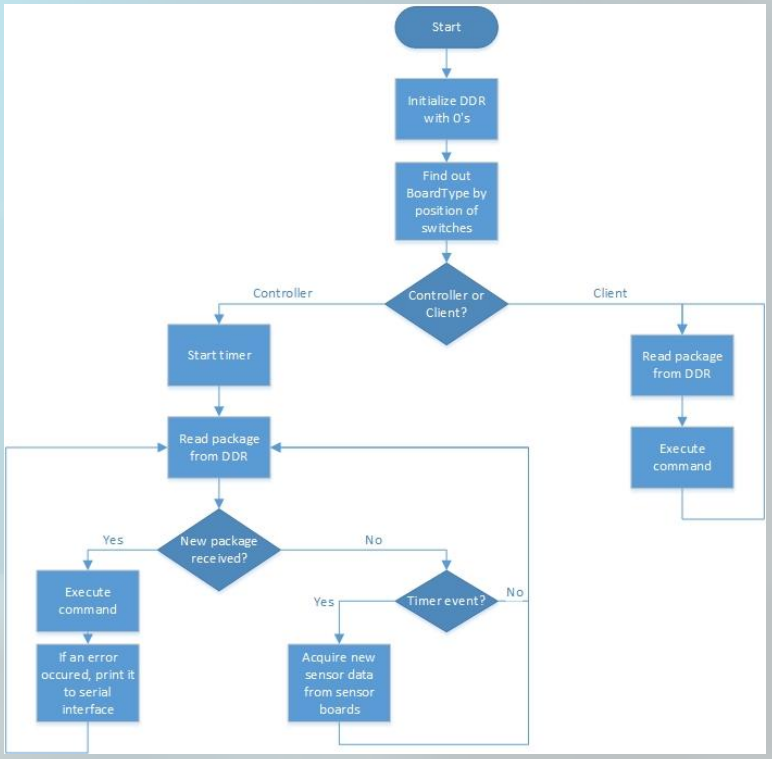
HW/Block Design



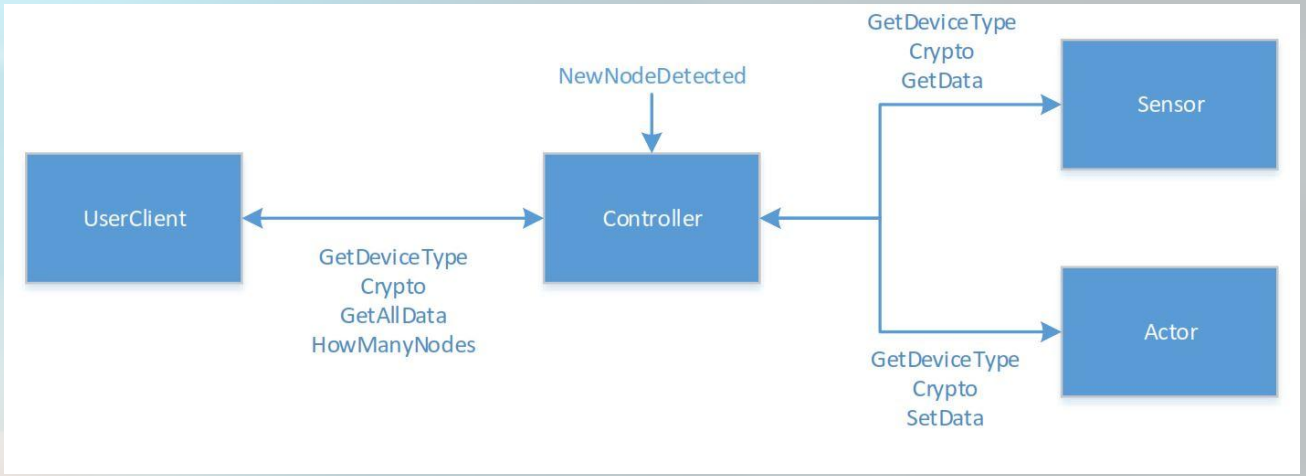
HW/PL and Hardware



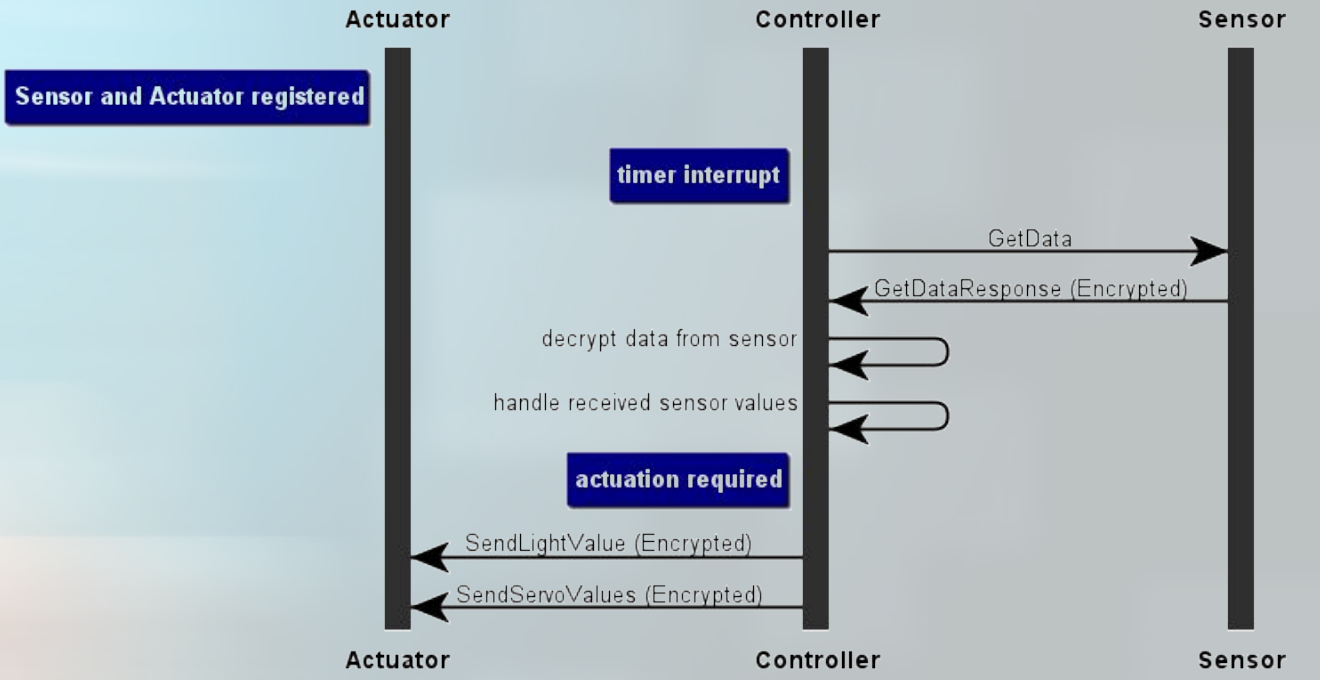
SW/MicroBlaze - Software Flow

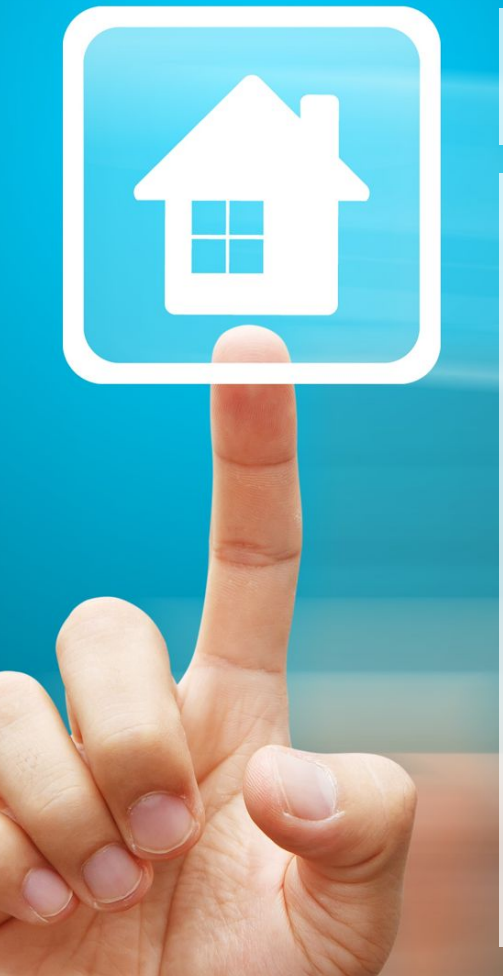


SW/MicroBlaze - Commands



SW/MicroBlaze - Timer Event

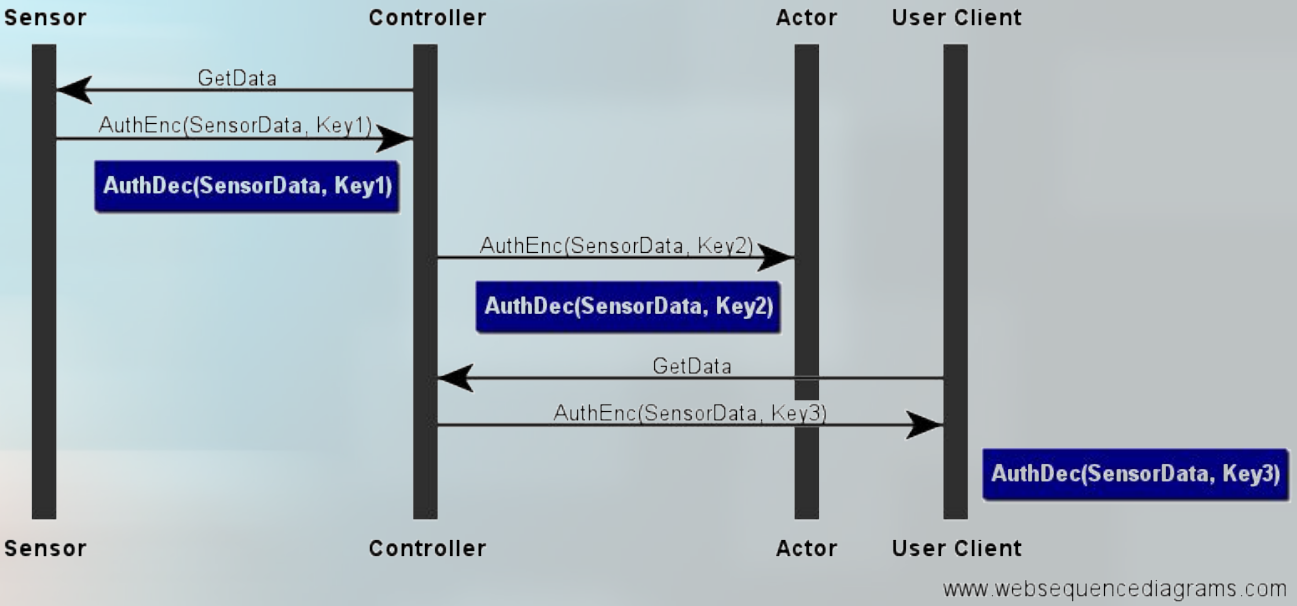


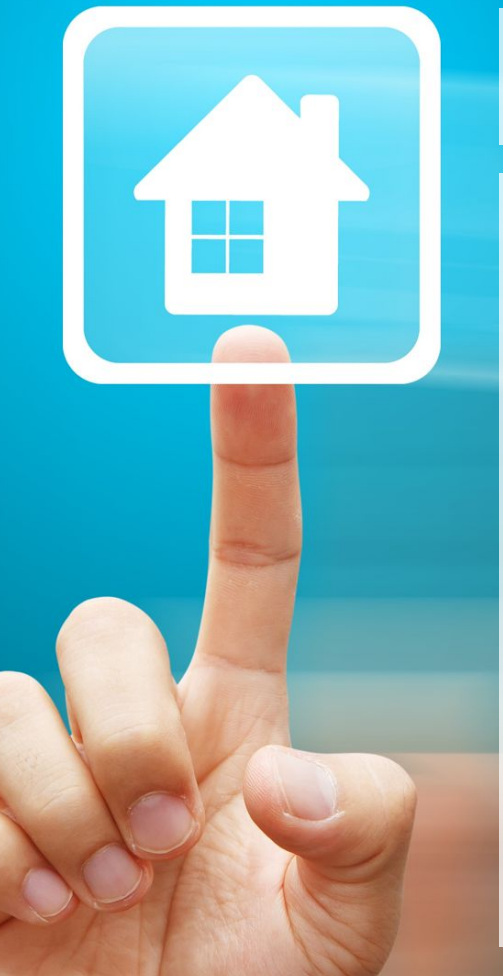


SW/Encrypted Communication

- Private-key cryptography
- Authenticated encryption
- Used algorithm: Ascon-128 v1.2
- Different key per client
- Whole communication via controller

SW/Encrypted Communication

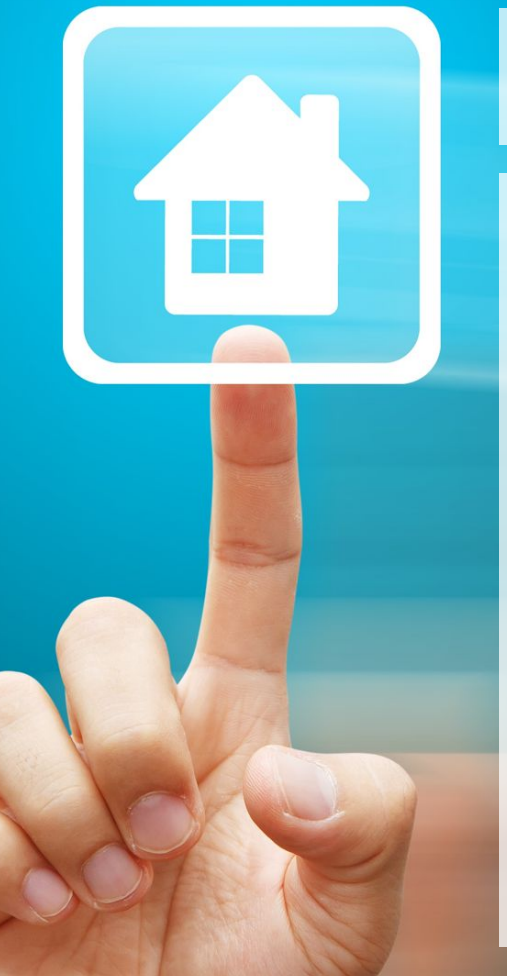


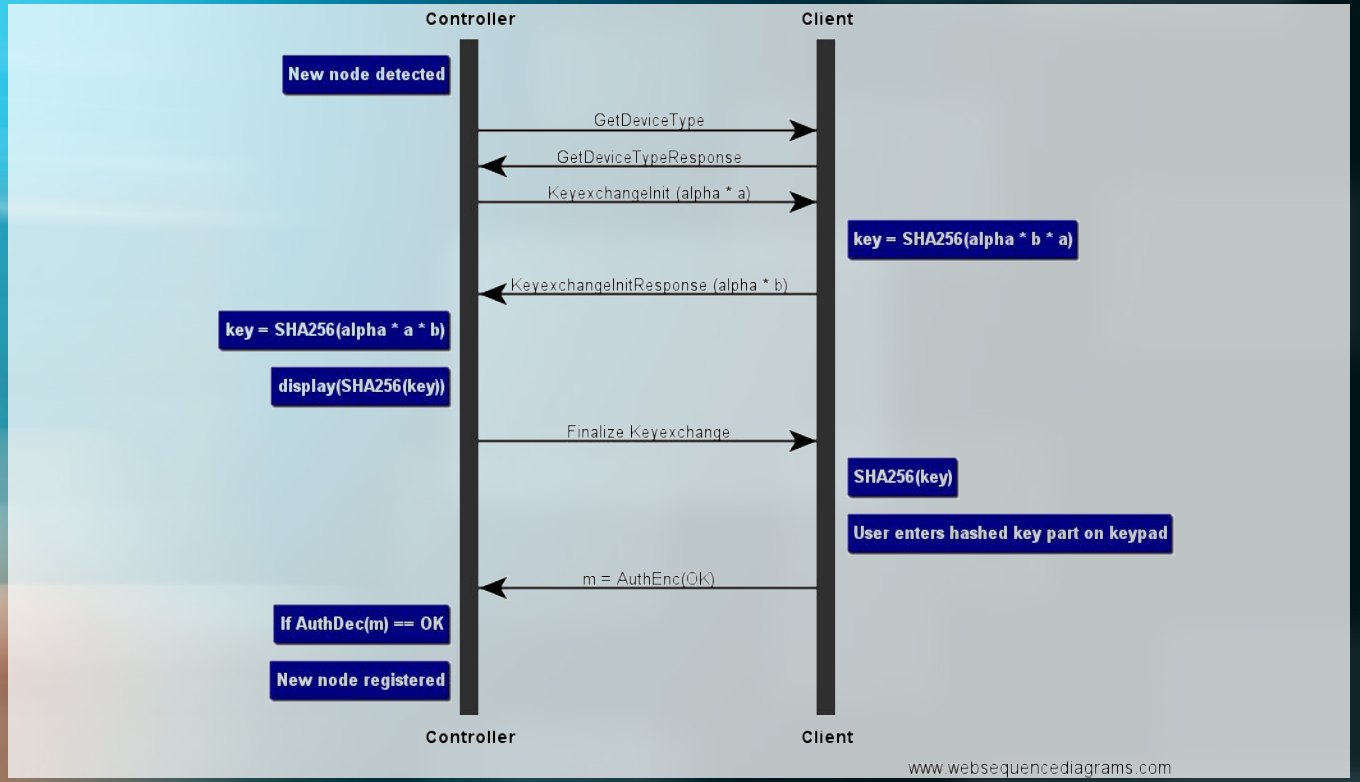


SW/Key Exchange

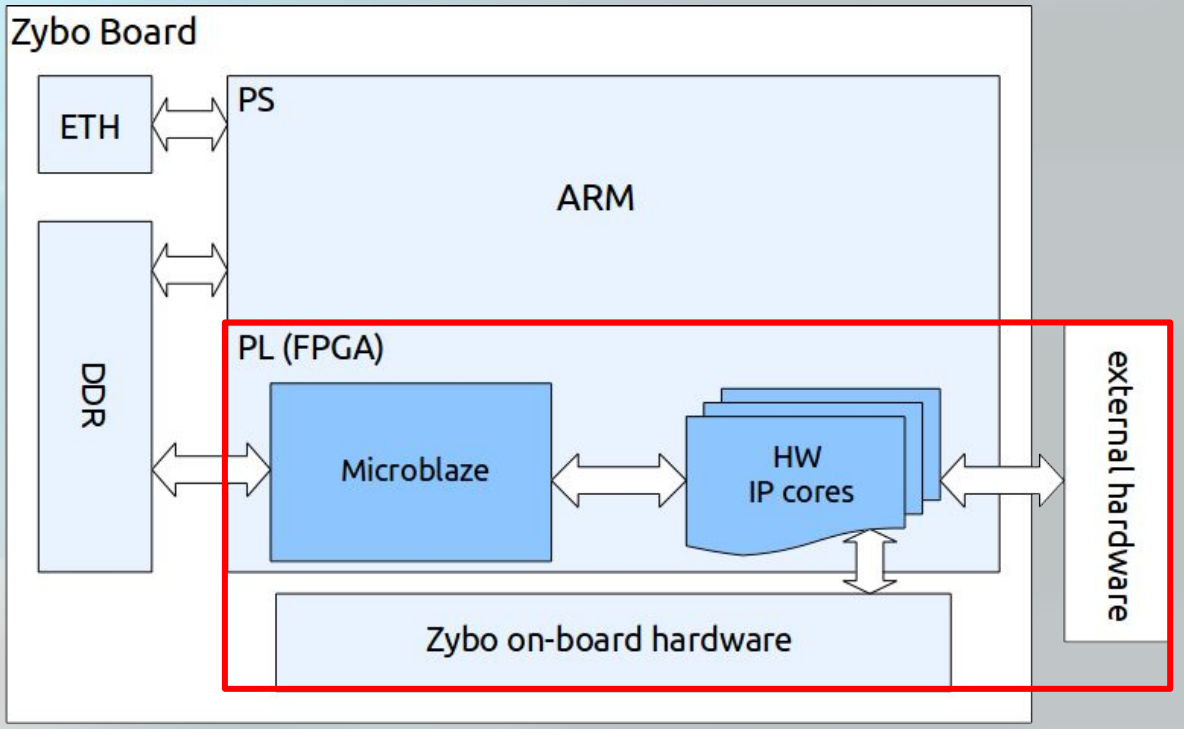
- Public-key cryptography
- Elliptic curve Diffie-Hellman (ECDH)
- SHA256
- Used curve: SECP256R1
- Used library: FLECC
- Man in the middle attack?!
  - User action: display + keyboard

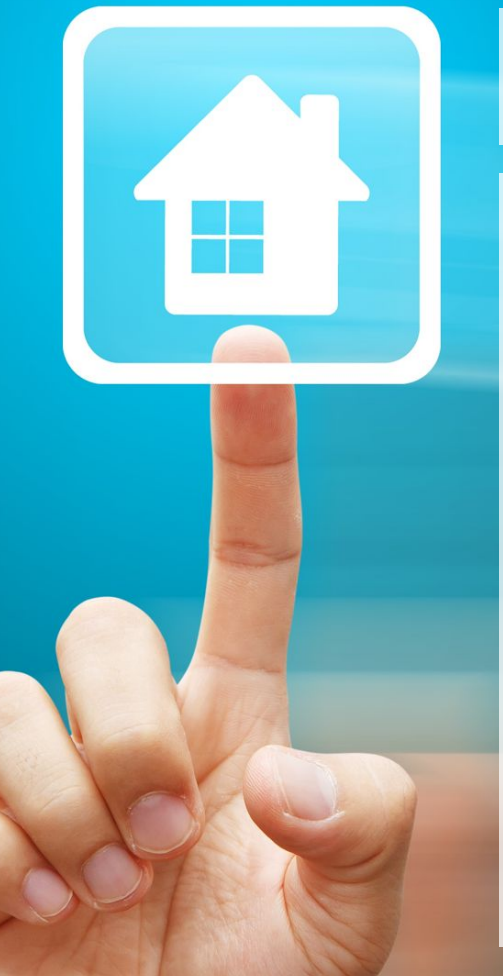
SW/Key Exchange





HW/Extern

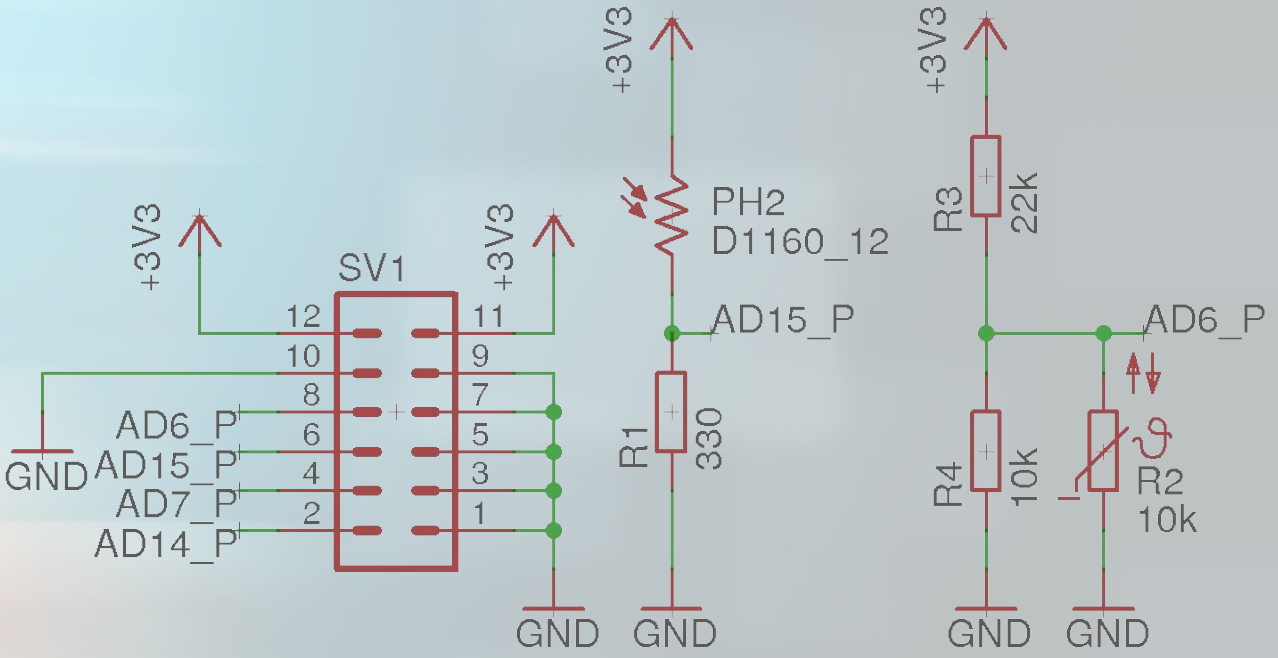

Zybo Board
ETH
PS
ARM
DDR
PL (FPGA)
Microblaze
HW
IP cores
external hardware
Zybo on-board hardware



HW/Light and Temp Sensors

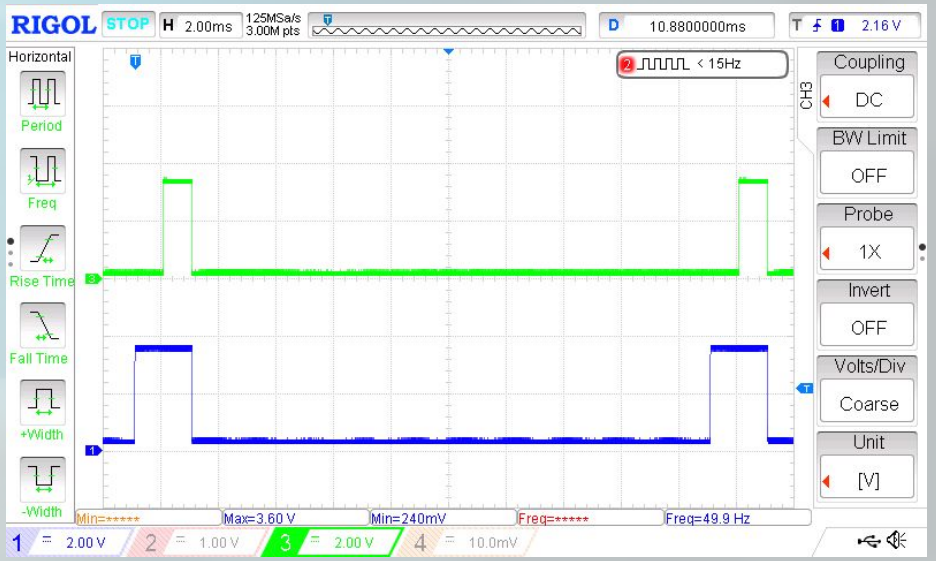
- XADC (embedded part of the FPGA)
- NTC temperature sensor
  - Calibrated with look-up-table
- Photoresistor as light sensor

HW/Light and Temp Sensors

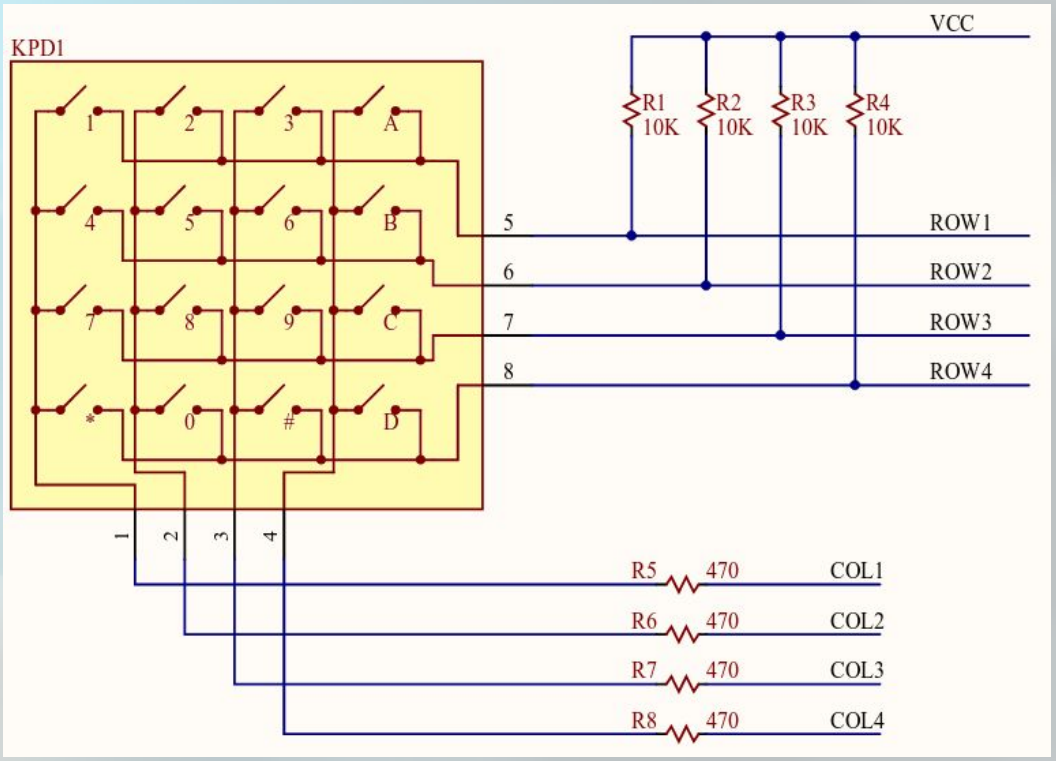


HW/Servos

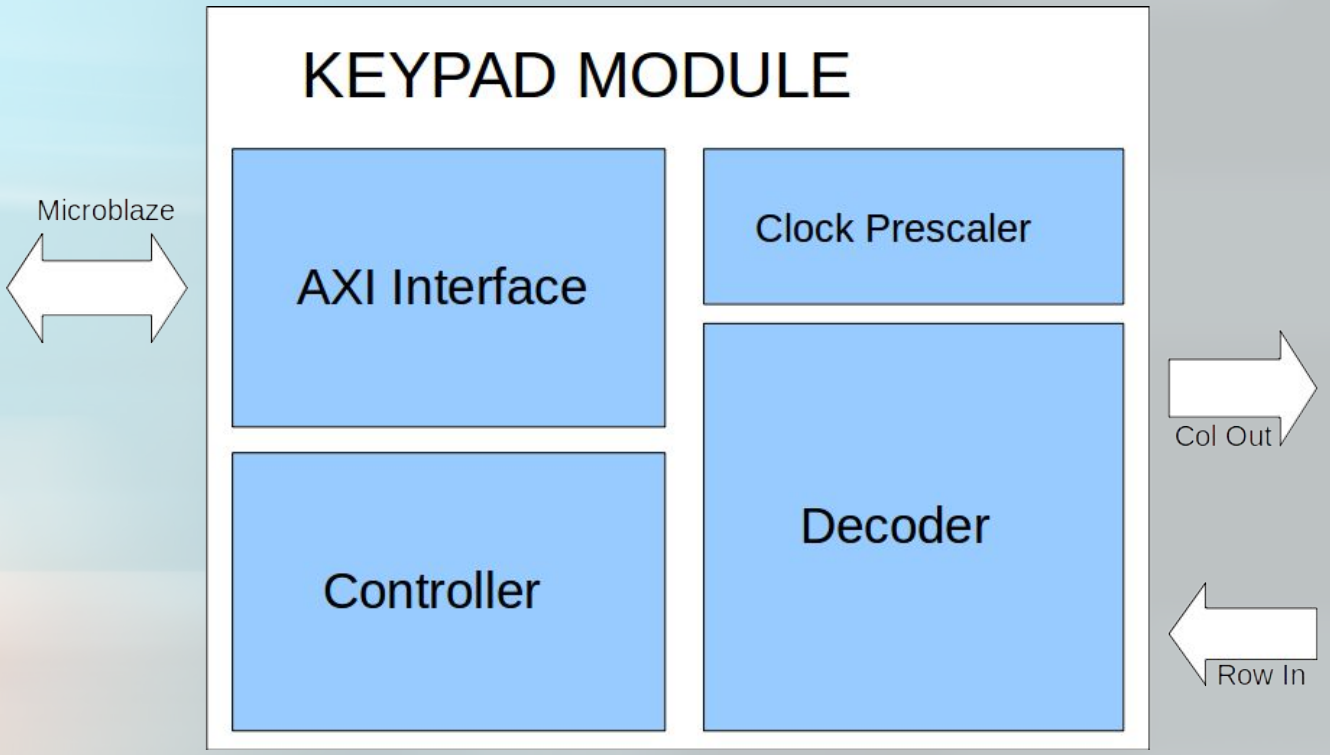
- Controlled using PWM typical 50Hz
- Pulse width 1-2ms

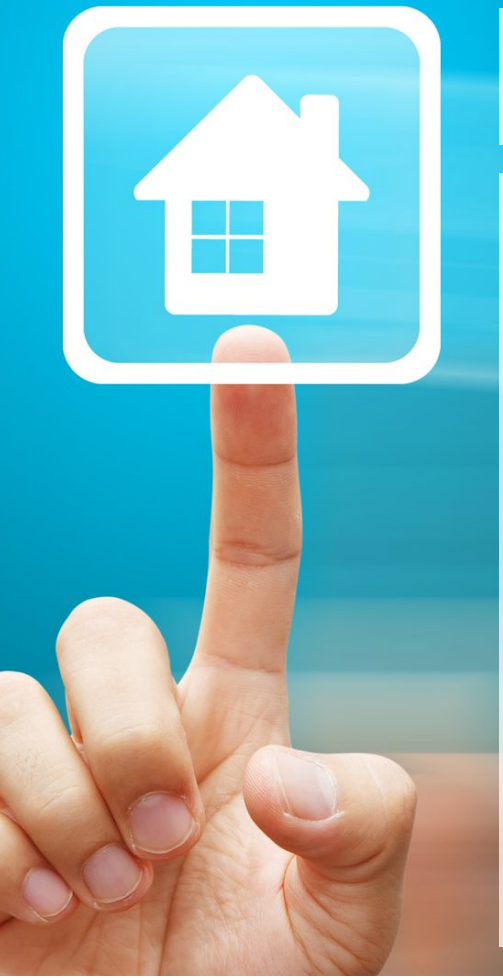


HW/Keypad - Schematic



HW/Keypad - IP

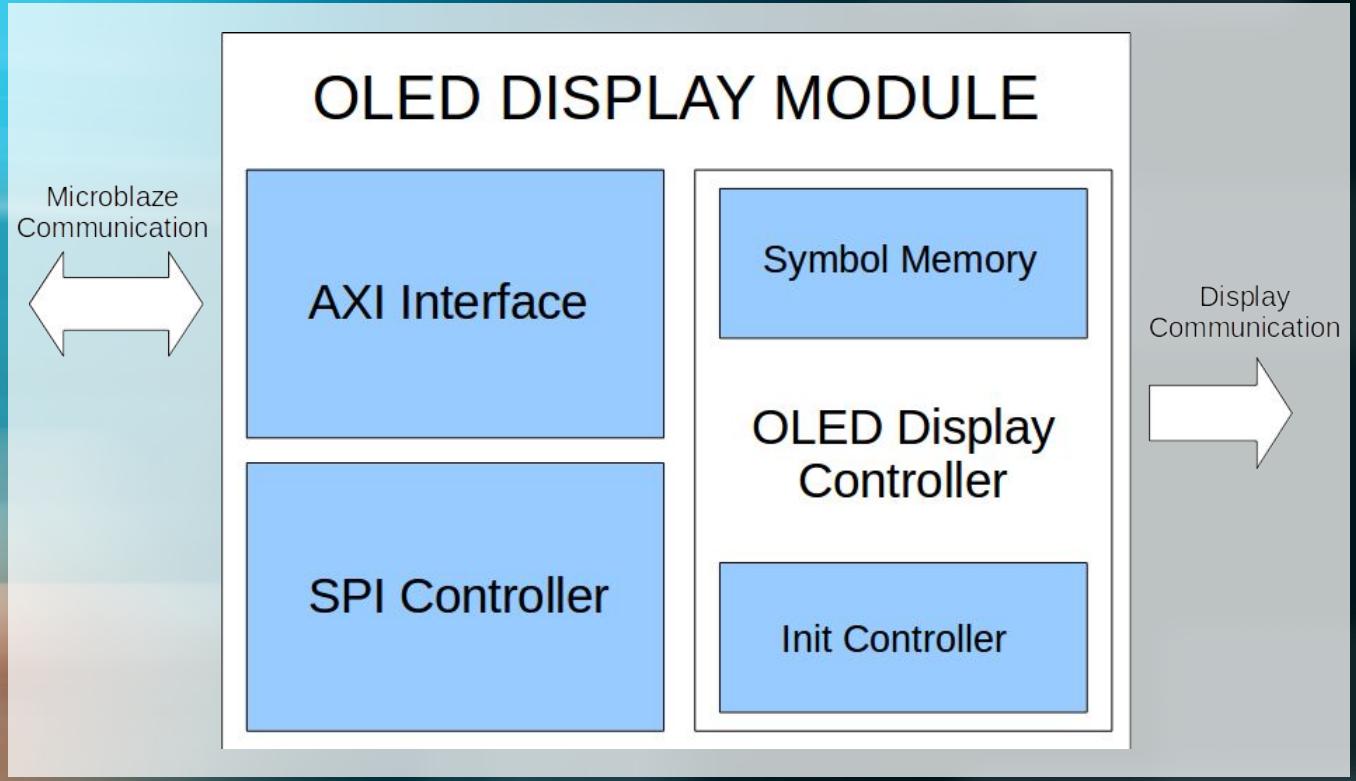

KEYPAD MODULE
Microblaze
AXI Interface
Clock Prescaler
Controller
Decoder
Col Out
Row In

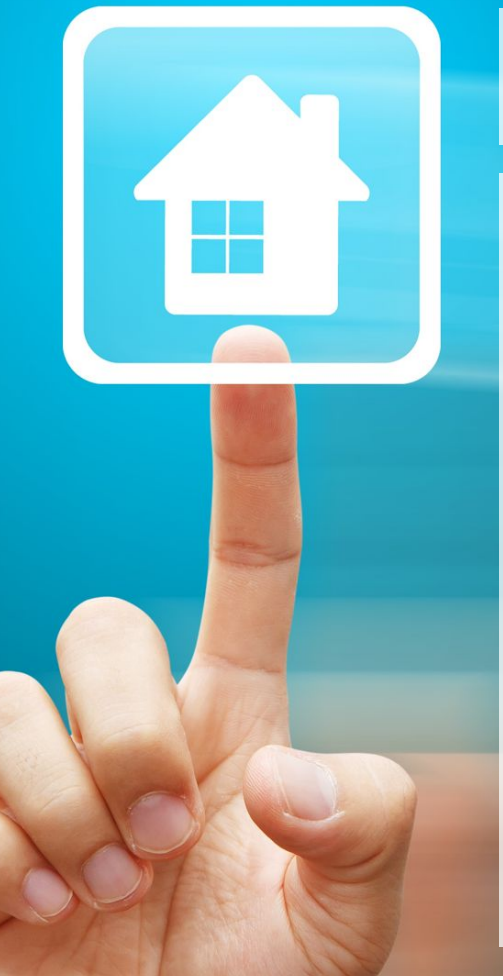


HW/OLED Display

- Usage: Key exchange (client registration)
- Technical facts:
  - 128x32 pixel graphic OLED display
  - Communication via SPI
- Implementation on Zynq:
  - Hardware module (PL)
    - Microblaze communication: AXI
    - Display communication: SPI send controller
    - Control logic (sending symbols, sending commands)

HW/OLED Display

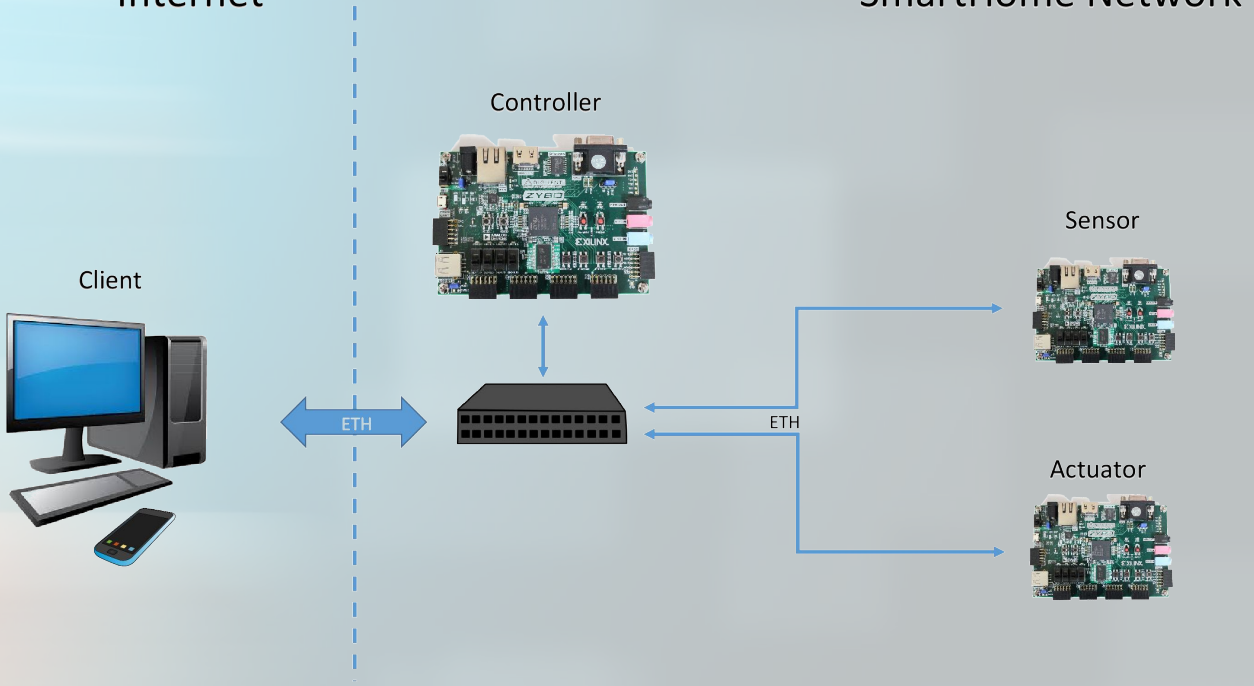




SW/Client

- Python 3.5
  - GUI - tkinter
  - Threading
  - Sockets
- Security
  - Ascon
  - ECDH

Live Demo


Internet
SmartHome Network
Controller
Client
Sensor
Actuator
ETH
ETH

End