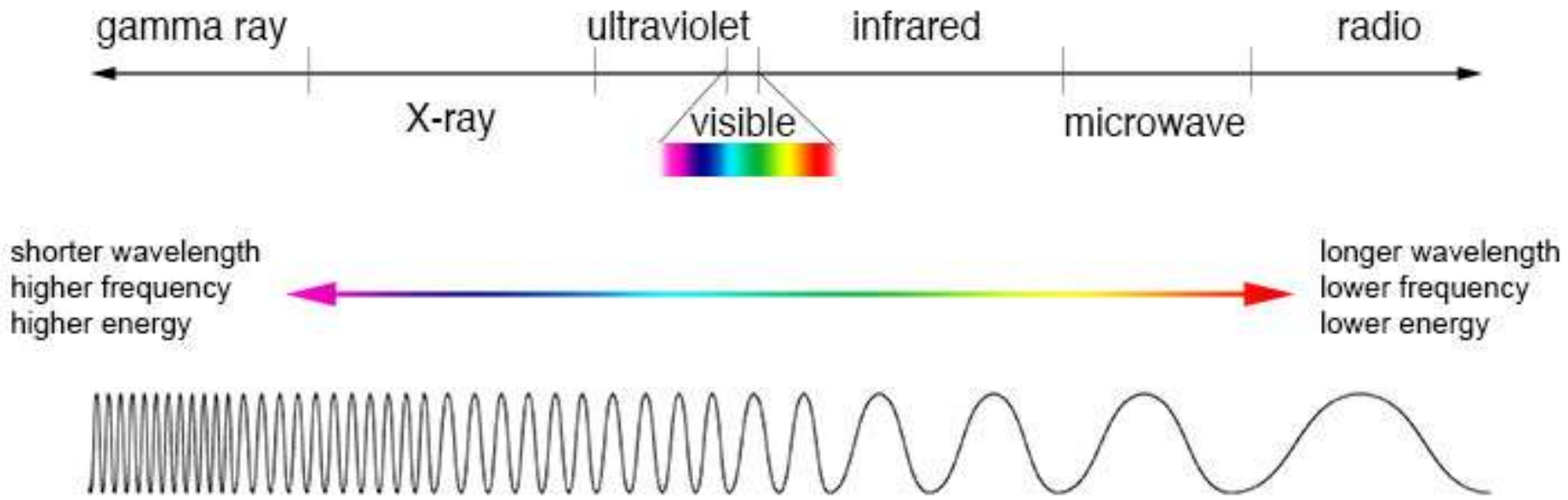
Addressing the Challenges of Creating Infra-Red Vision Systems for the IIoT and IoT

ADAM@ADIUVOENGINEERING.COM

Why IR?

- Thermal Imager completely passive able to detected temperature of objects
- All objects above 0K exhibit thermal emissions and absorption
- No scene illumination required
- Wide range of applications from Military & Security
- Industry 4.0 and IIoT
  - thermographic applications
  - Detect early failures – In solar panels using a Drone mounted IR Imager

Different Sensor technology



Types of Sensor

- Cooled IR sensor
  - Requires cooling engine – Size, Complexity, MTBF & Clost
  - Takes time to reach operational temperature
  - HgCdTe or InSb semi conductors required
  - Higher Resolution – High Definition Resolution possible
- Uncooled Sensor
  - Microbolometer based solutions – works on change of resistance
  - More compact solution
  - Limited resolution when compared to Cooled
  - Ideal for IIOT

Challenges

- High performance processing solution, to implement image processing algorithms, communication and application security
- Security, the ability to implement secure configuration, access authentication, secure communication and anti-tamper features to prevent unauthorised access.
- Flexible interfacing capabilities, able to interface with the IR modules, local displays along with wired and wireless communication using both industry standard and proprietary interfaces.
- Power efficiency, not only a solution capable of reducing power consumption depending upon the operating mode but also one which offers the most power efficient implementation.

How do we protect it?

- Secure Boot – The ability to decrypt an encrypted boot image. Secure boot should also provide cryptographic authentication of the image.
- Authentication – Only authorised users should be able to connect with the IoT /IIoT system. Strong passwords and authentication protocols should be used.
- Secure Communication – Communication to and from the IoT/IIoT device should be encrypted.
- Secure Data – Data stored within the system should be secure, encryption standards such as AES, Simon or Speck can be used to secure data.
- Anti-Tamper – Able to determine unauthorised access attempts to the system. This may include monitoring the presence of enclosure lids, device voltages and temperatures.

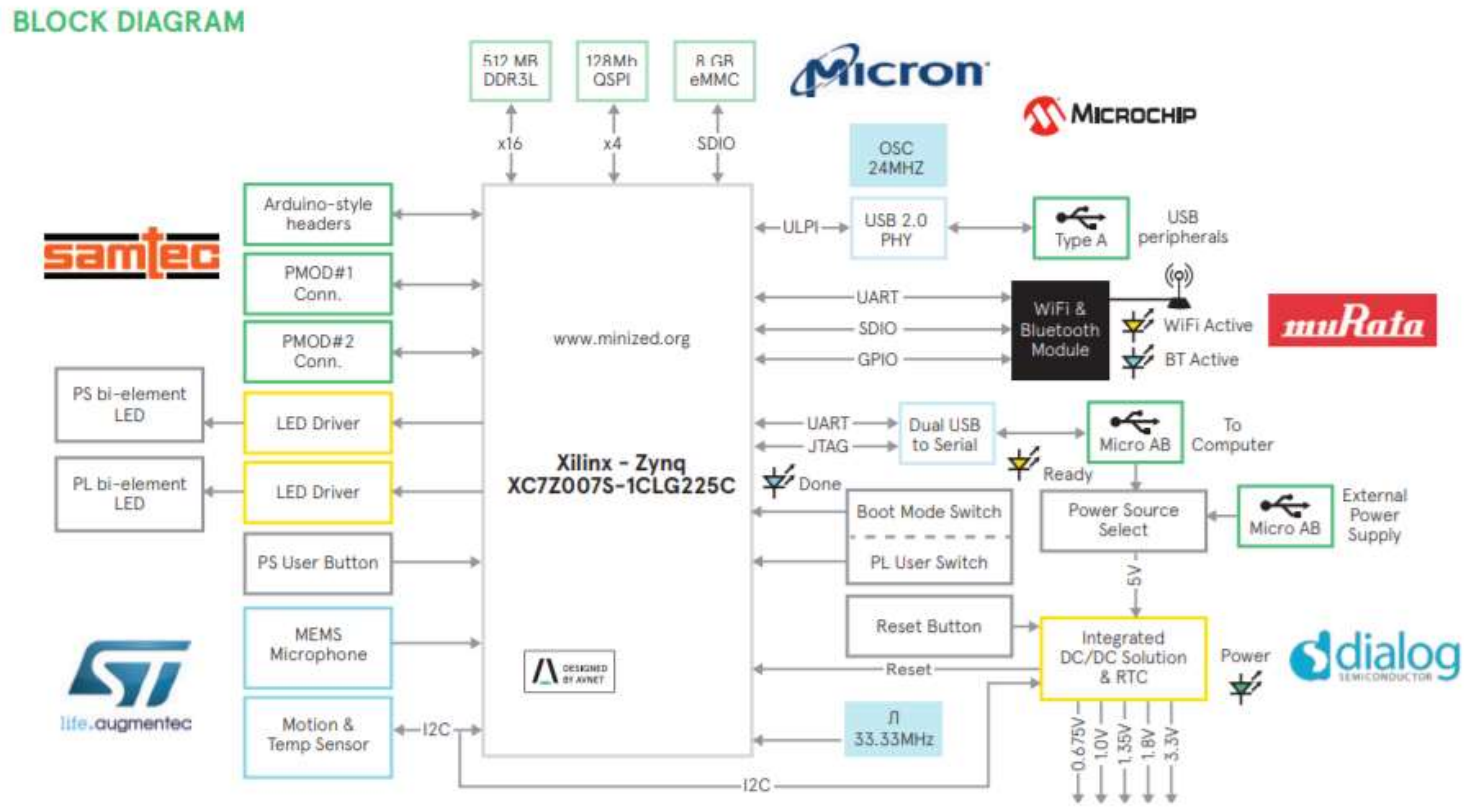
Prototype – Reduce time to market

- Creation of Minimum Viable product – demonstrator
- Imaging Device
  - FLIR Lepton 2 or 3 (80x60 or 160x120)
- MiniZed
  - Single core Zynq – Combines ARM 9 Processor and Programmable Logic
  - Build In WIFI and Blue Tooth (LE)
  - PMOD & Arduino shield connections – for interfacing
  - Mems sensors –Accelerometers, Temperature & Microphone

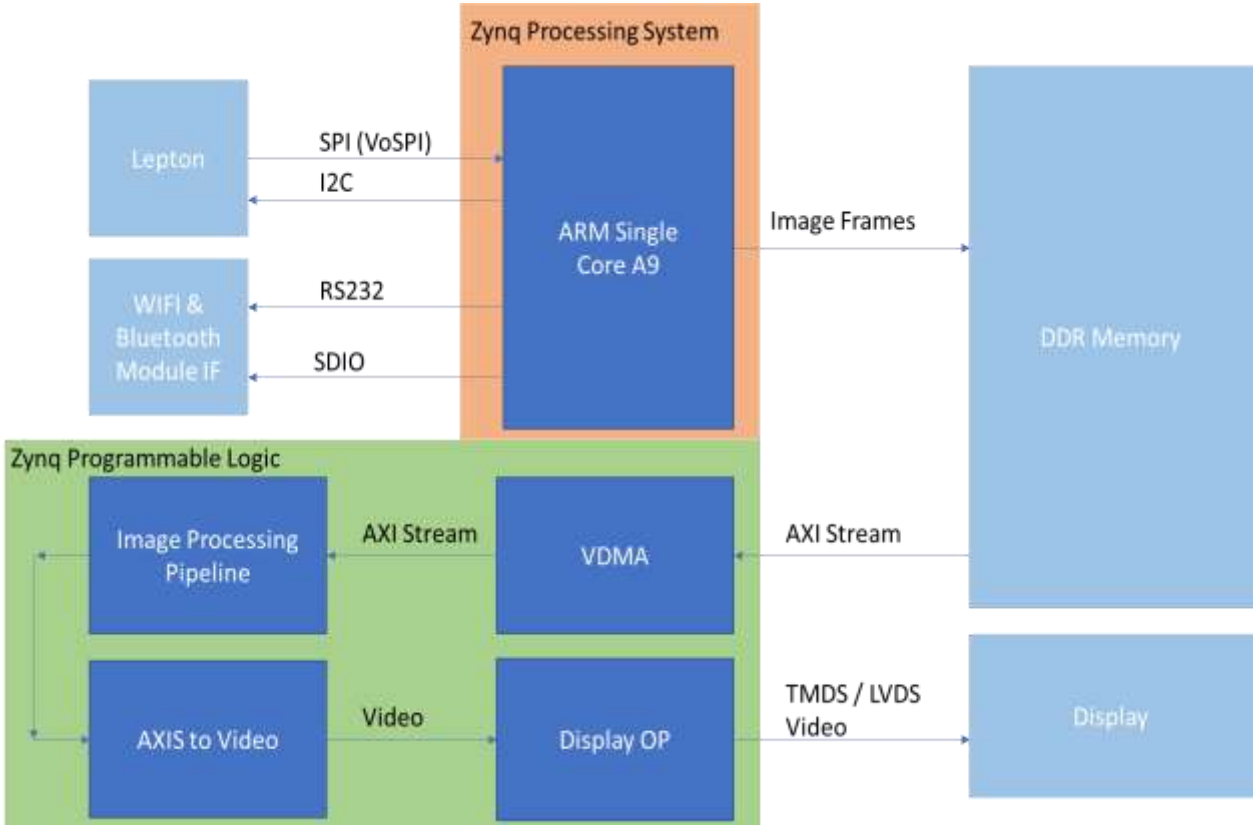
FLIR LEPTON

- Mounted on breakout board
  - Single 3 or 5 volt power input
  - I2C – for configuration
  - Video Over SPI
- Video output over SPI
  - Packets of 164 bytes each contain 1 line of video plus header
  - Need to synchronise based on the header
  - For export compliance frame rate is 9 Hz

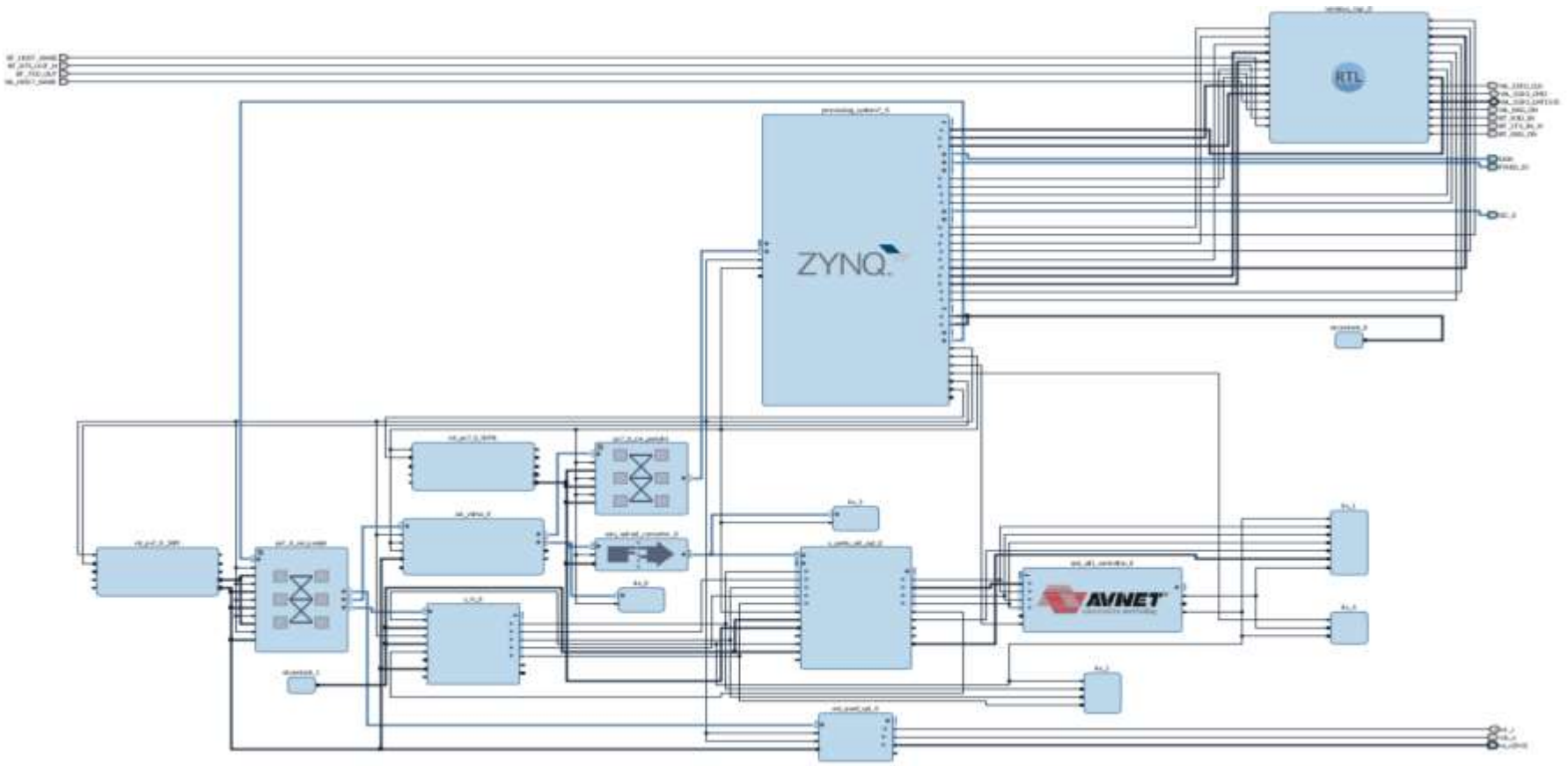
MiniZed Block Diagram



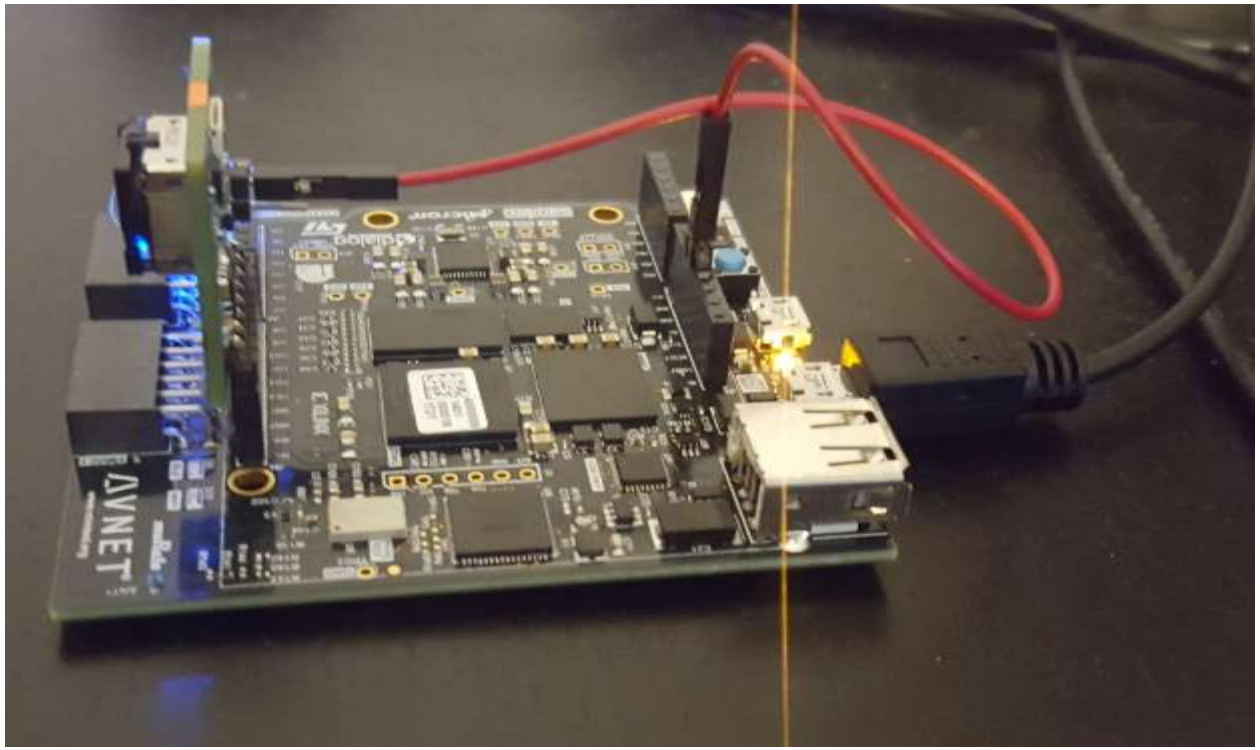
Architecture of Solution



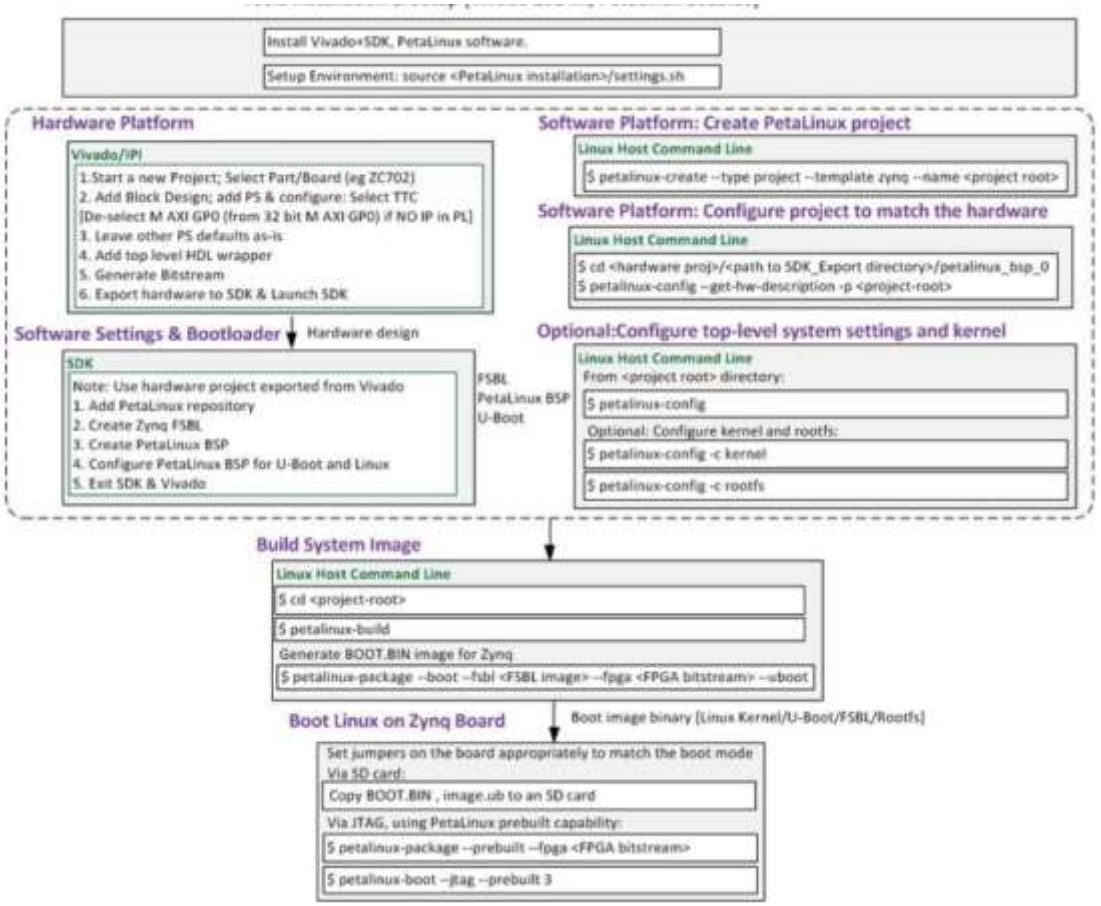
Vivado Design



What it looks like



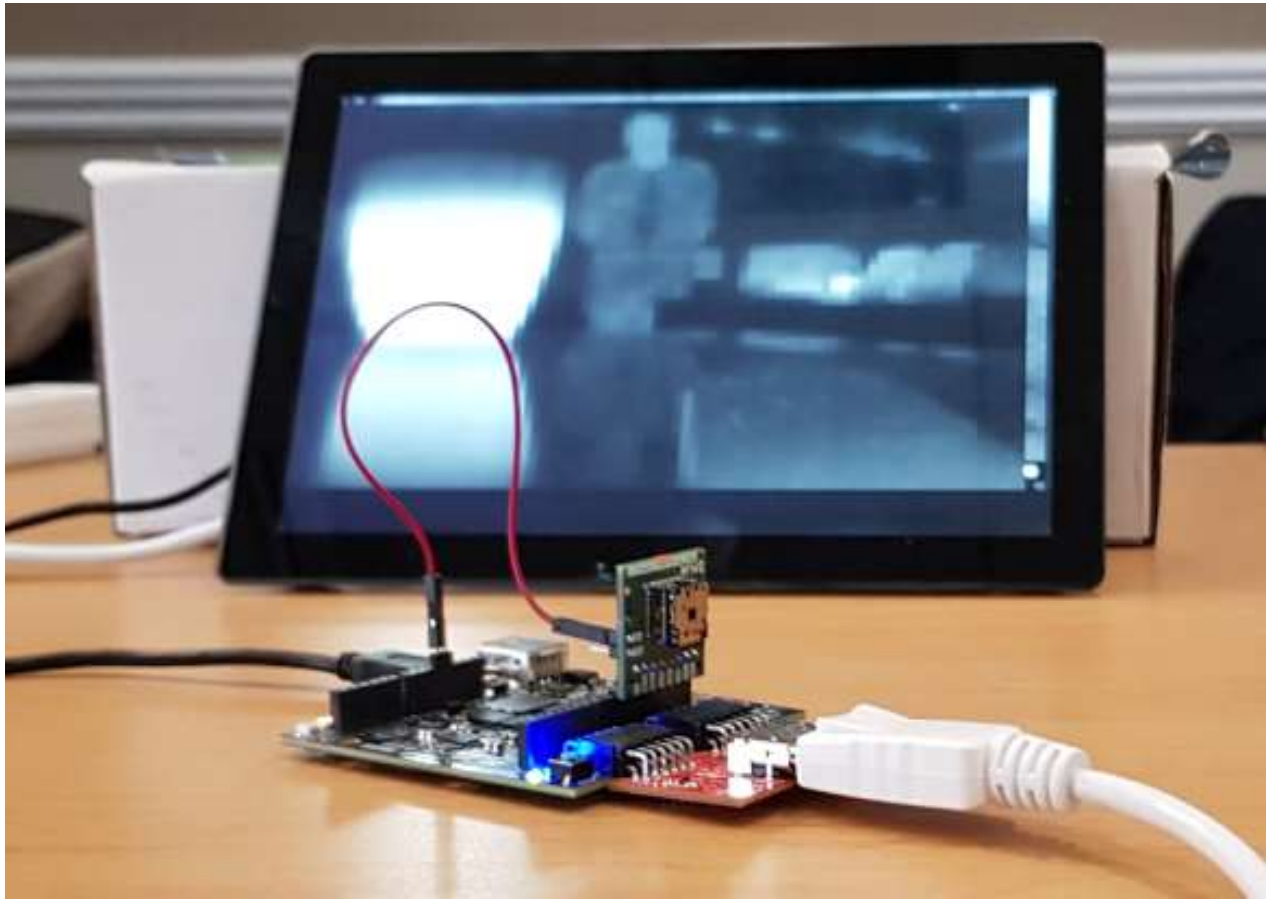
PetaLinux – Creating the high level SW



What do we need to do

- Configure the FLIR Lepton to perform Automatic Gain Control
- Synchronisation with the VoSPI data to detect the start of a valid frame
- Applies a Digital Zoom to scale up the image to utilise efficiently the 800 pixels by 480-line display. This can be achieved by outputting each pixel either 8 or 4 times depending upon the sensor selection.
- Transfer the frame to the DDR Memory as the FLIR Lepton only outputs 8 bits data when ACG is enabled this is mapped to the green channel of the RGB display.
- Application that's up to you?

Imaging with a local display



Questions ?

- Grab the code from
- https://github.com/ATaylorCEngFIET/MiniZed-FLIR-Lepton-2