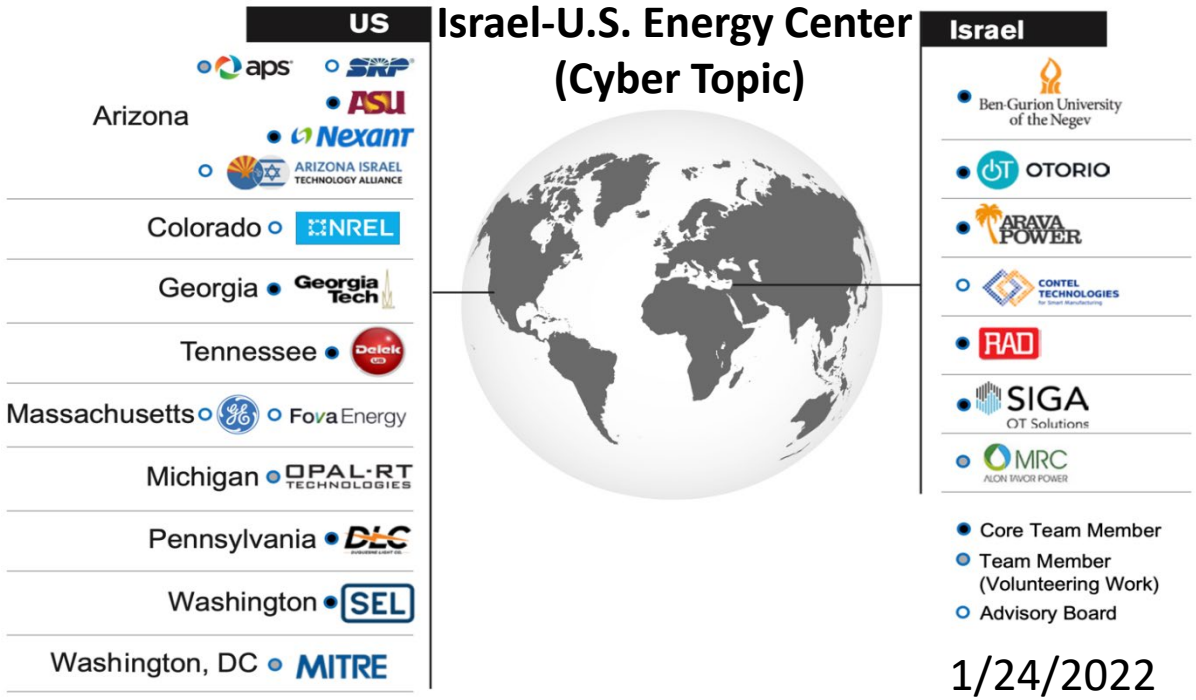
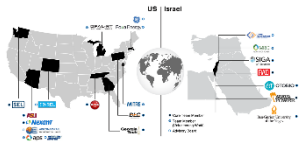
BIRD ICRDE: Task 13 – Firmware Verification



- Michael Amar
- Dr. Yossi Oren

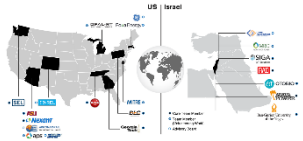
1/24/2022

Introduction & Goal



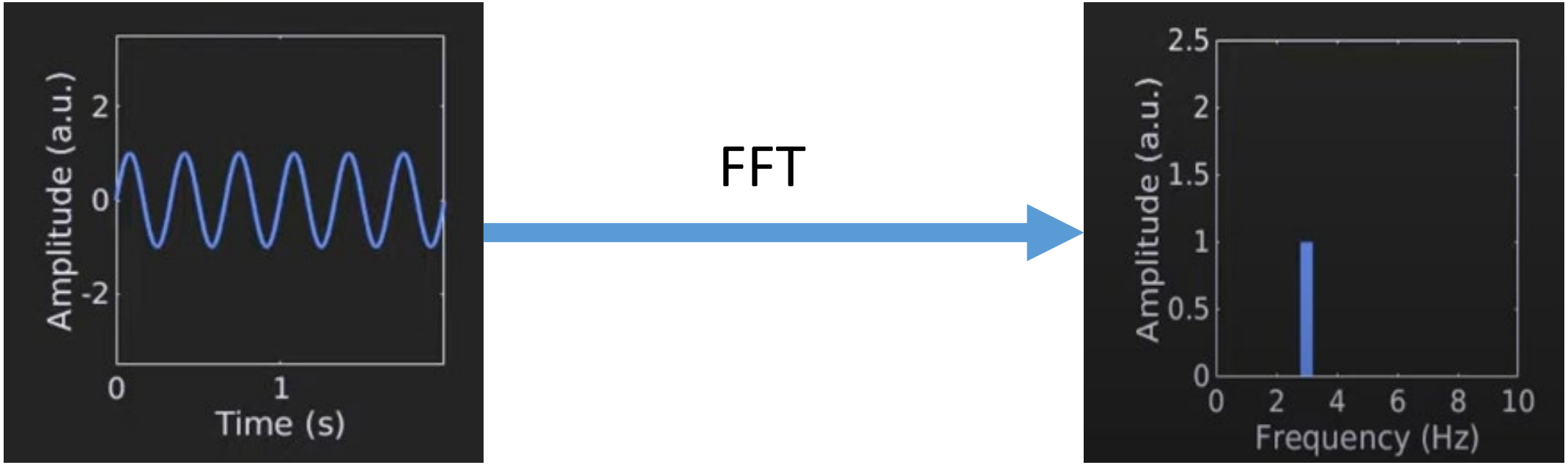
- Verify The Firmware on PLC Devices
- Passively Monitor code execution
- Minimal reduction to real time guarantees

Proposed Method

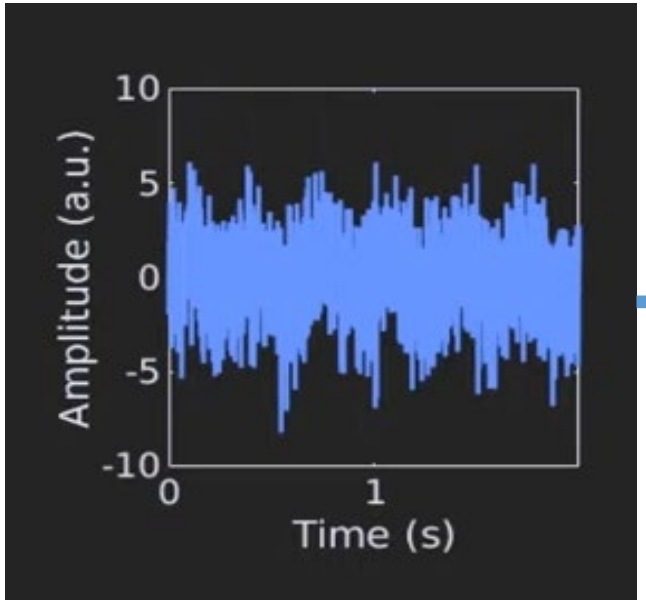


- Capture runtime power traces
- Remove noise from the traces
- Train LSTM model to detect normal execution

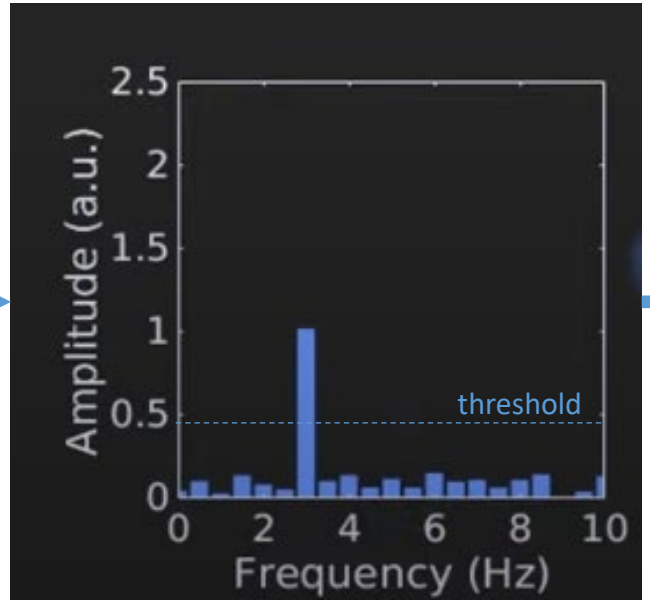
Cleaning the Data : FFT



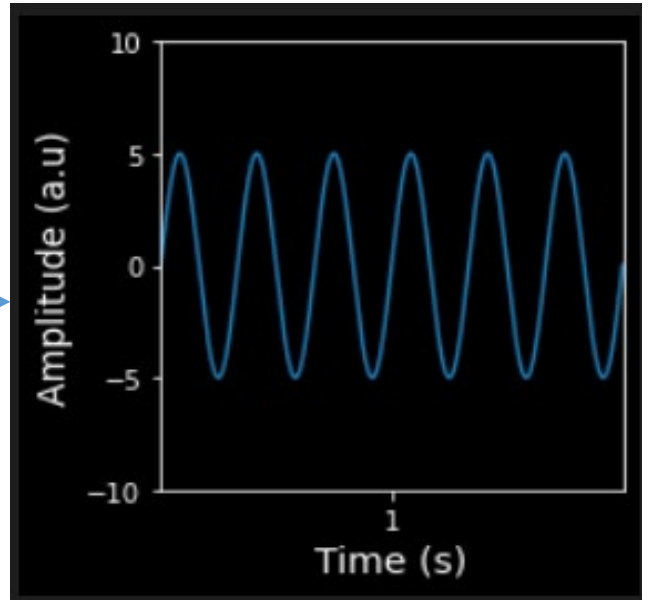
Cleaning the Data : FFT Cont’



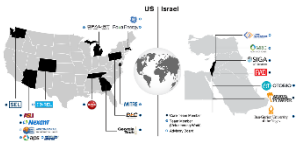
FFT



Inverse FFT

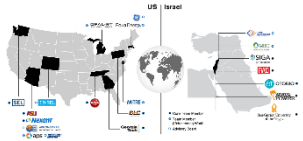


LSTM



- Good with sequential data
- Give context to the model
- Combine previous states for current decisions

Commercialization



- Consulting with SEL engineers

- We presented several options for monitoring:
  - Monitoring via power traces
  - Monitoring via Electromagnetic Emanations
  - Monitoring via System Buses (Address Bus, Data Bus)

Questions