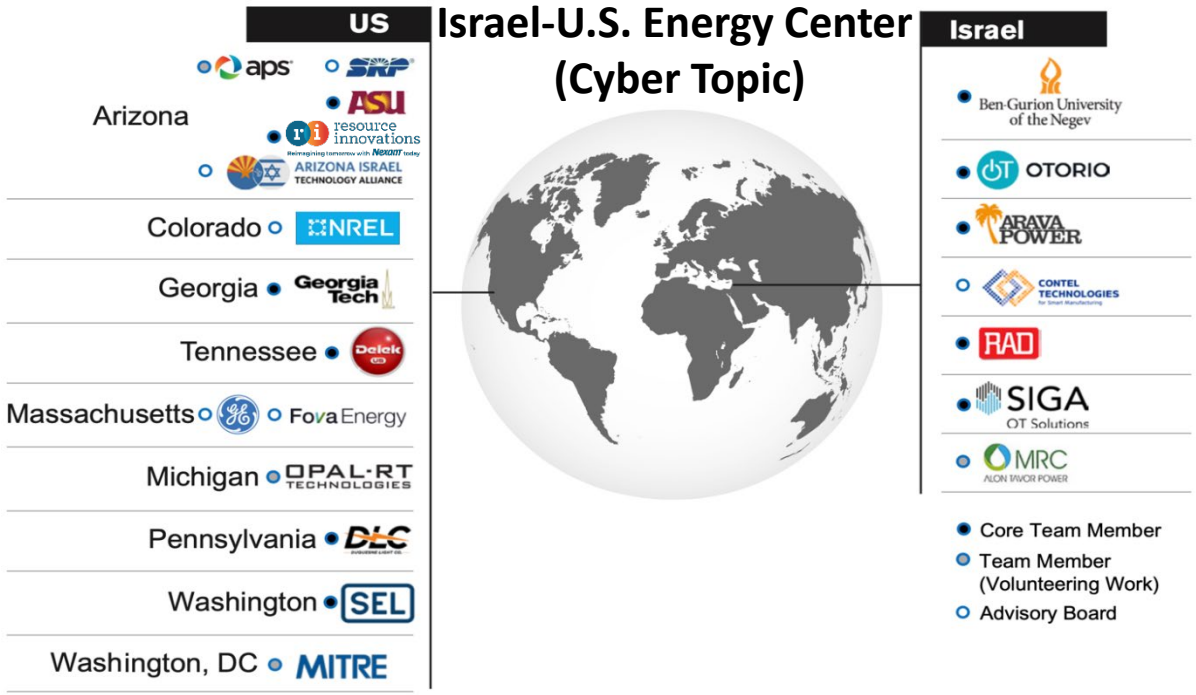
Task 13: Firmware Verification

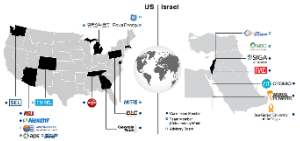


Dr. Yossi Oren

Michael Amar

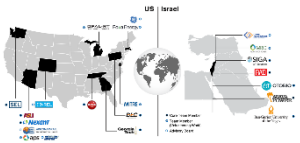
Lojenaa Navanesan

Introduction & Goal



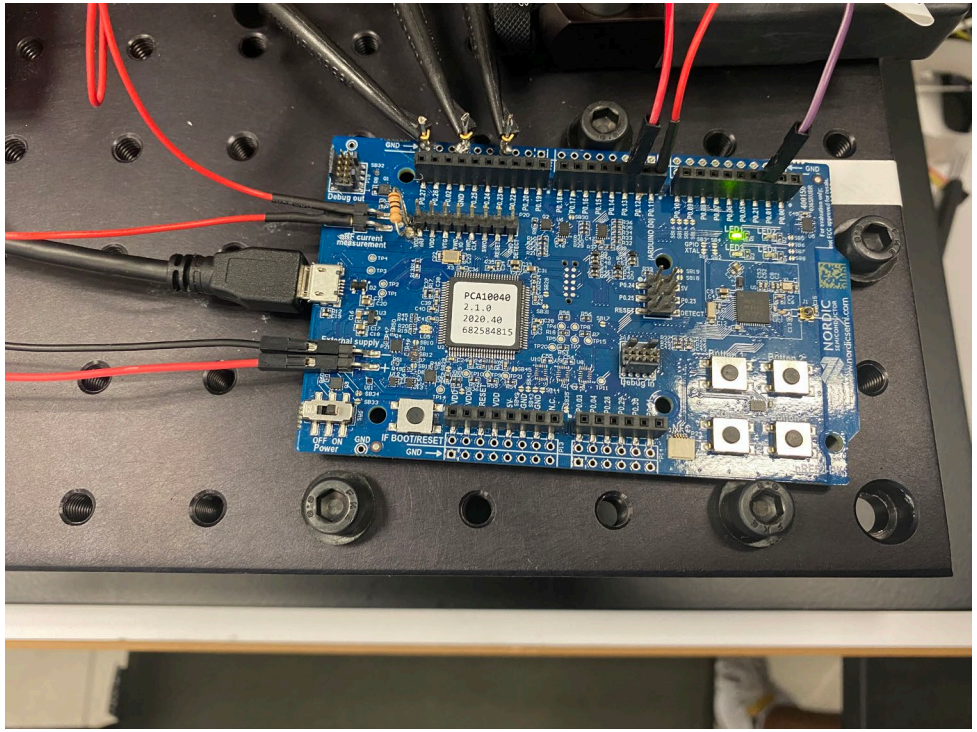
- Verify the firmware installed on PLC devices
- Passively monitor code execution
- Minimal reduction to real time guarantees

Experimental environment



- Device under test – connected to oscilloscope

- Options for code execution monitoring:
  - Power side channel
  - Electromagnetic side channel

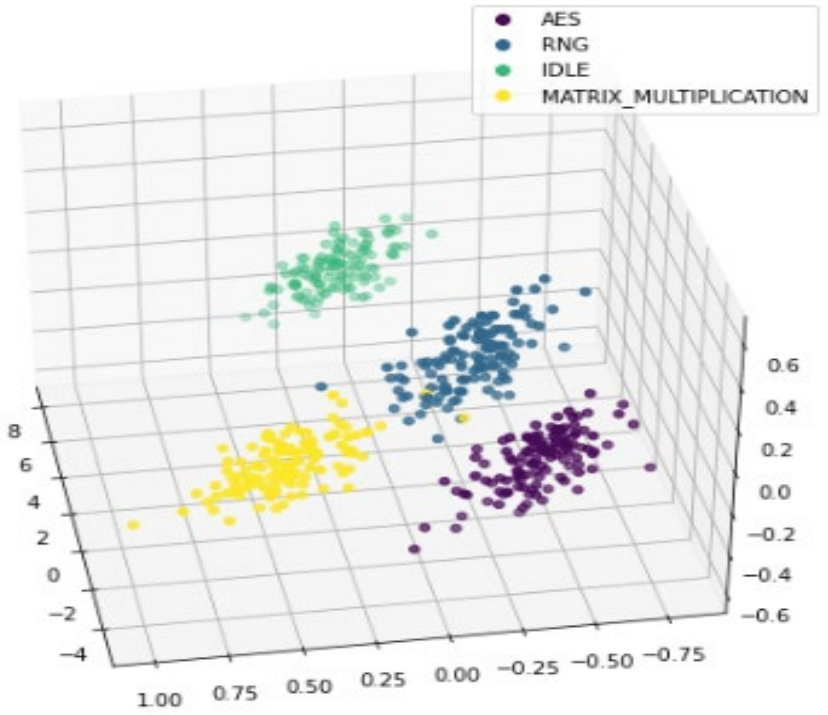


Power side channel

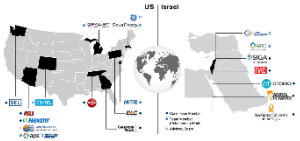
- Program classification experiment:
  - AES encryption
  - Random number generator
  - Matrix multiplication
  - Idle

- Over 95% accuracy for several classifiers (Logistic regression, LSTM)

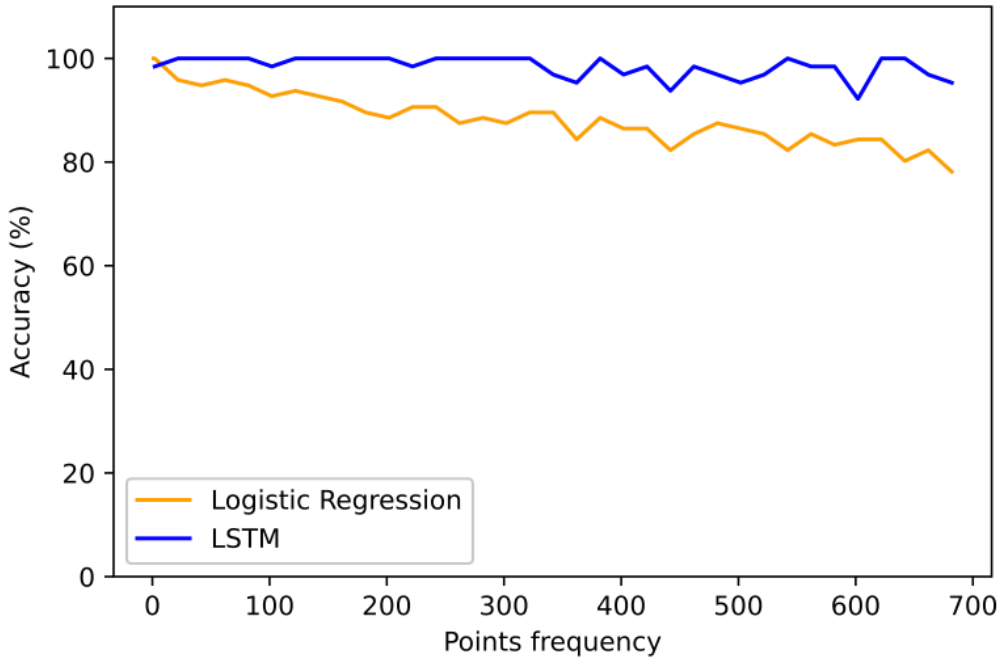
After applying PCA:



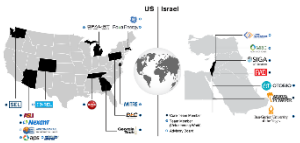
Decimation



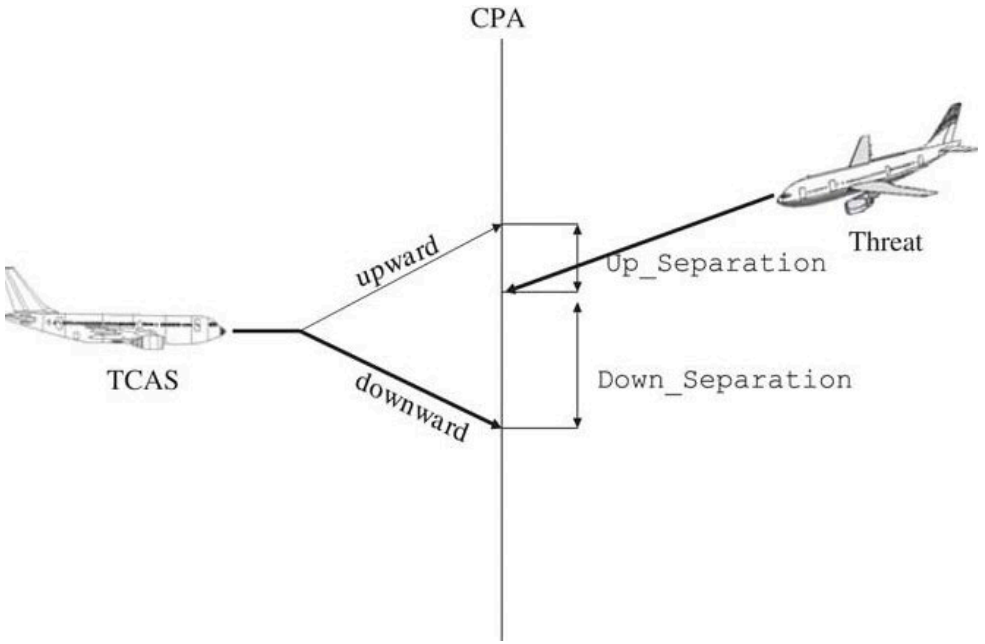
- High sampling rate
  - High volume data
  - Slower models



TCAS - Traffic Alert and Collision Avoidance System



- TCAS program flow:
  - Read inputs
  - Compute risk
  - Issue an alert (or not)
  - Repeat

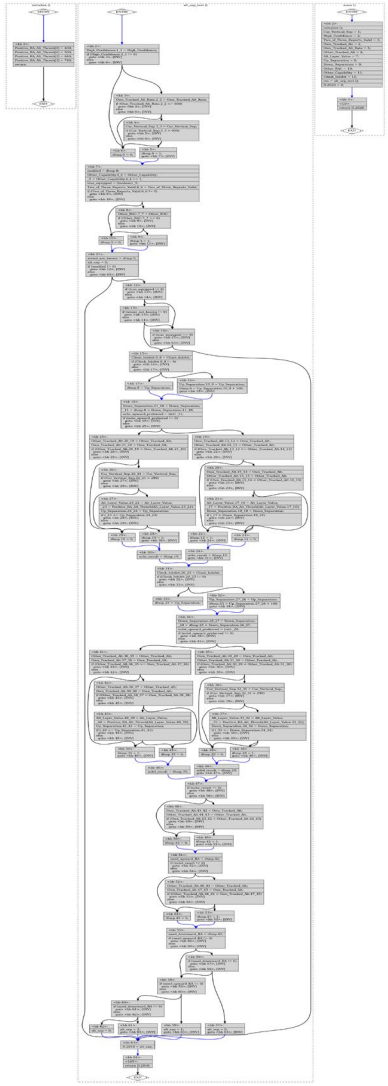


- PLC scan cycle:
  - Scan inputs
  - Execute program
  - Update outputs
  - Repeat

TCAS – tests generation

- Test for every feasible execution path (full coverage)
- Tests generated using PathCrawler
- 43 feasible execution paths

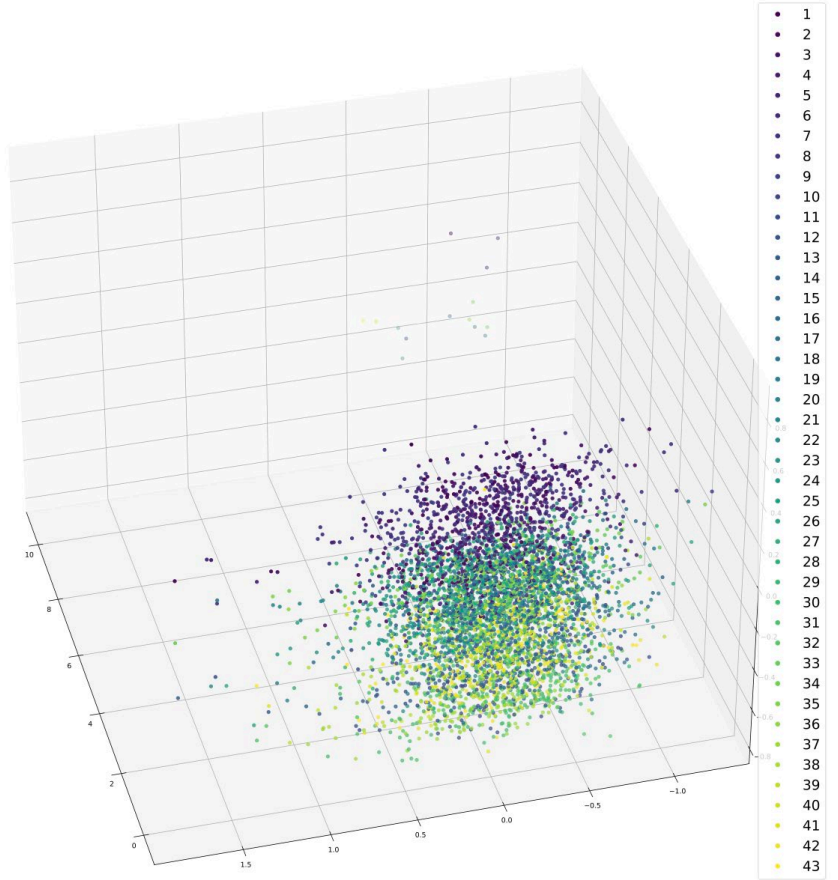
TCAS control flow graph



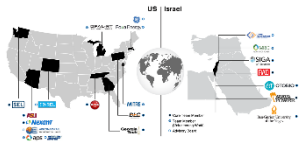
TCAS - tests generation

- 43 feasible execution paths

- Options for anomaly detection models:
  - Classification with 43 classes
  - One class training model



Next steps



- Implement anomaly detection model

- Apply method based on EM side channel