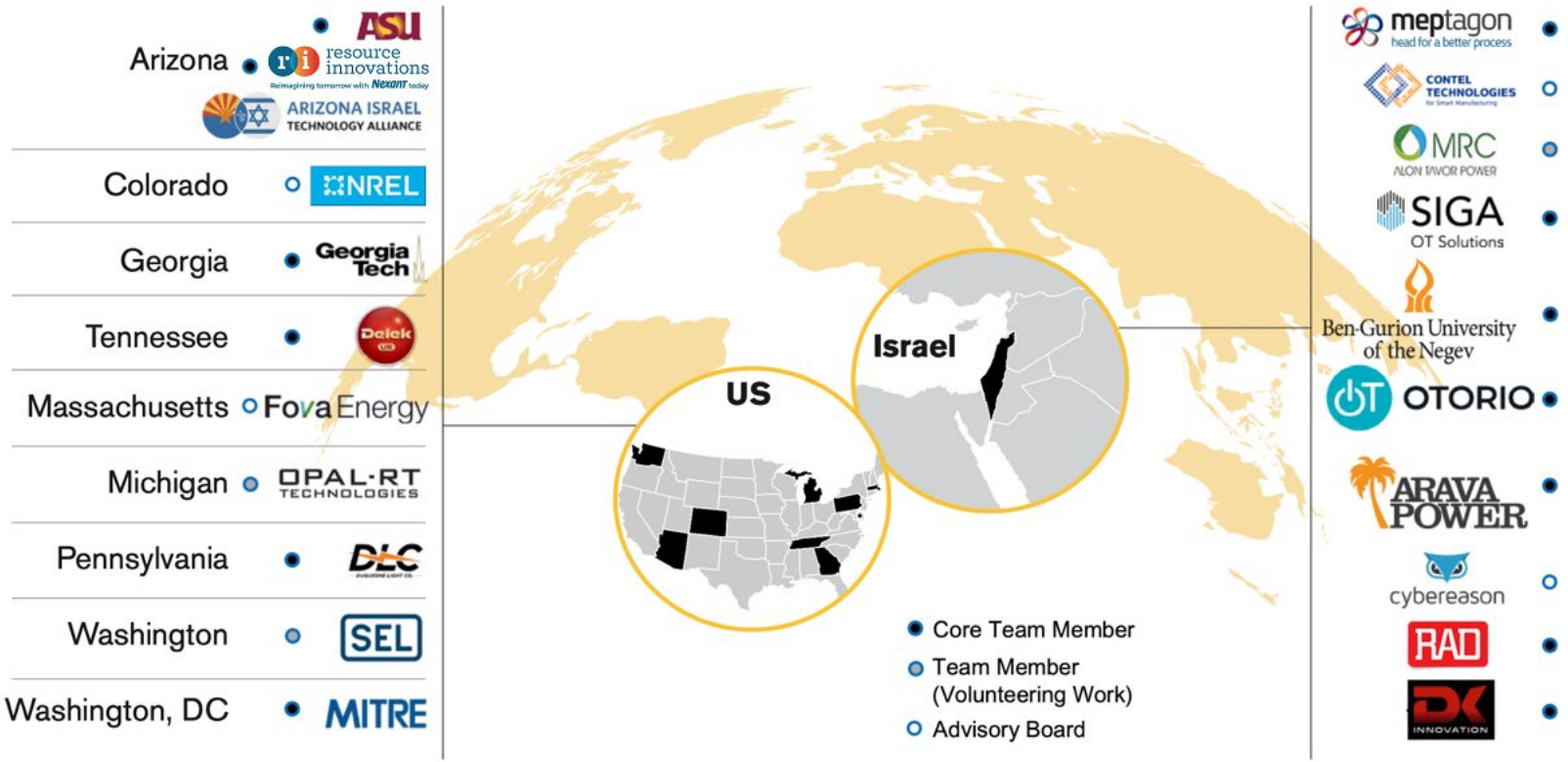
Task 13 – Firmware verification

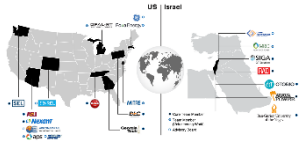


Dr Yossi Oren

Michael Amar

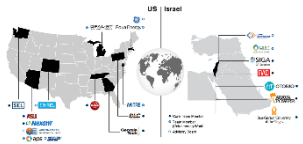
Lojenaa Navanesan

Objectives:



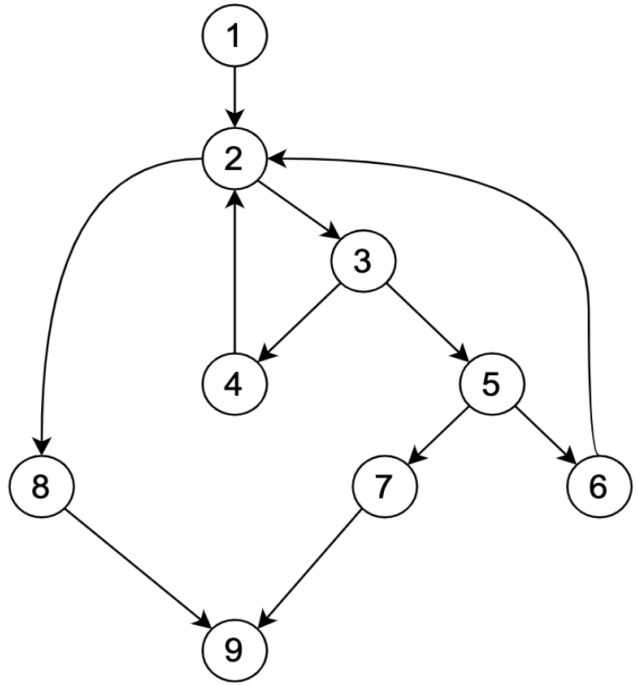
- Passively monitor Code execution on PLC devices
- No interference to real time guarunatees
- Minimal OS interference

Methodology:



1. Analyze the source code statically (assumed accessible)
2. Generate representative test cases to achieve maximal code coverage
3. Run the test cases with deactivated outputs
4. Collect EMI signals from the PLC (power consumption, EM radiation)
5. Train an anomaly detector model based on the signals.

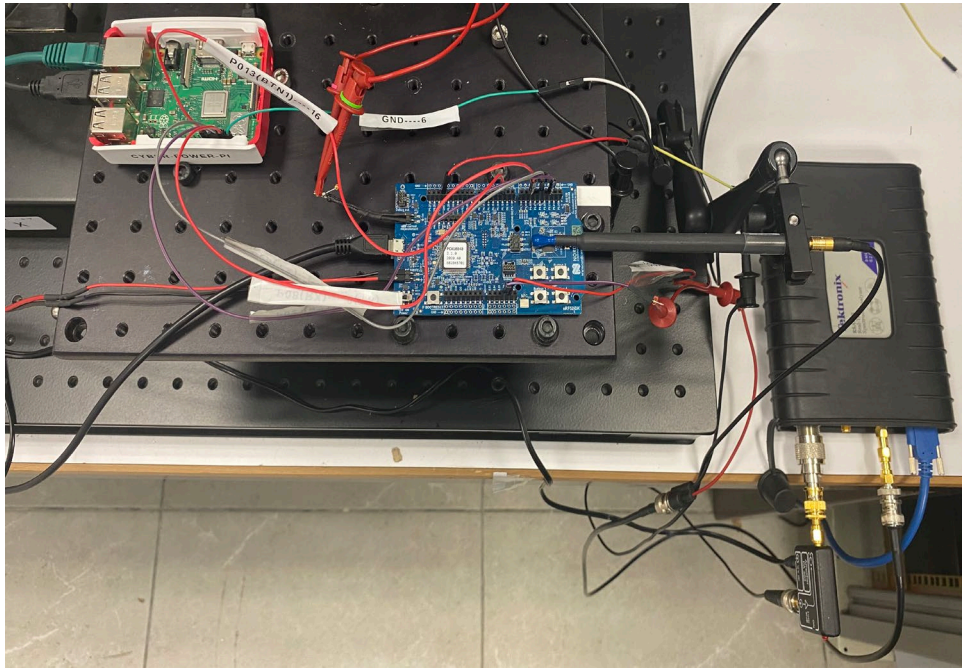
Control Flow Graph



Methodology:

Our model:

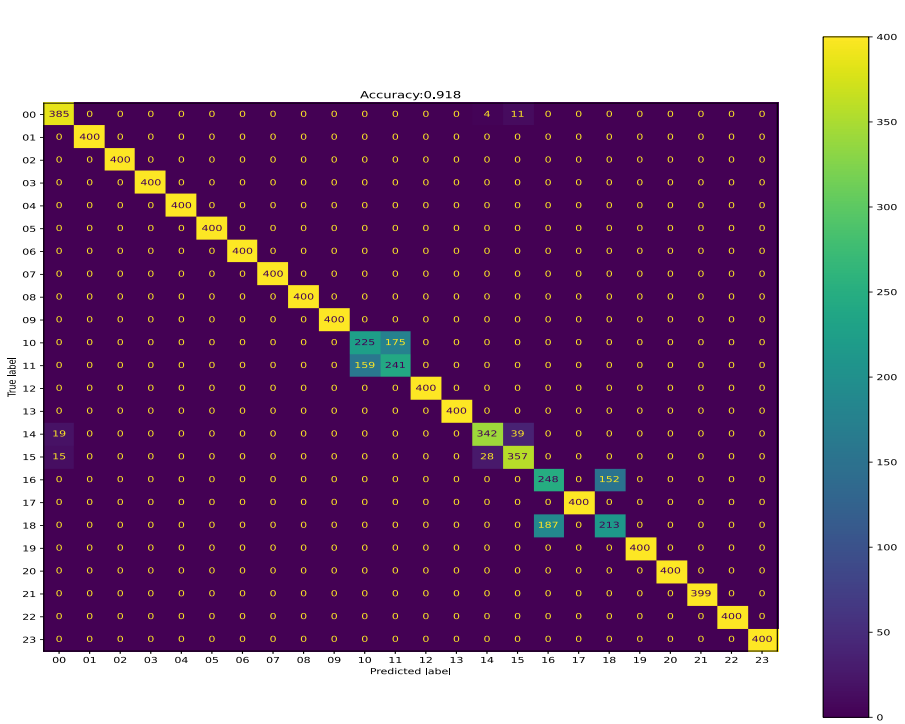
- Transformer based Classifier
- A class is an execution path
- Anomaly – low confidence in all classes



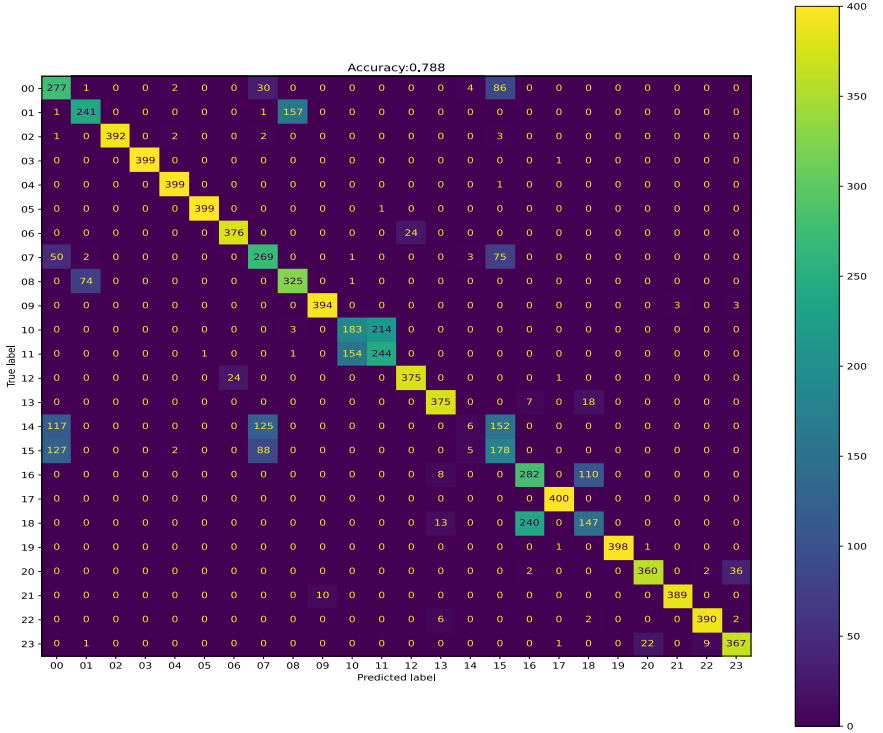
Experimental setup

Our model as a classifier:

- 24 classes (24 feasible execution paths)

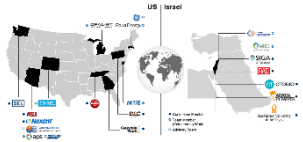


EM based classifier – 91% accuracy



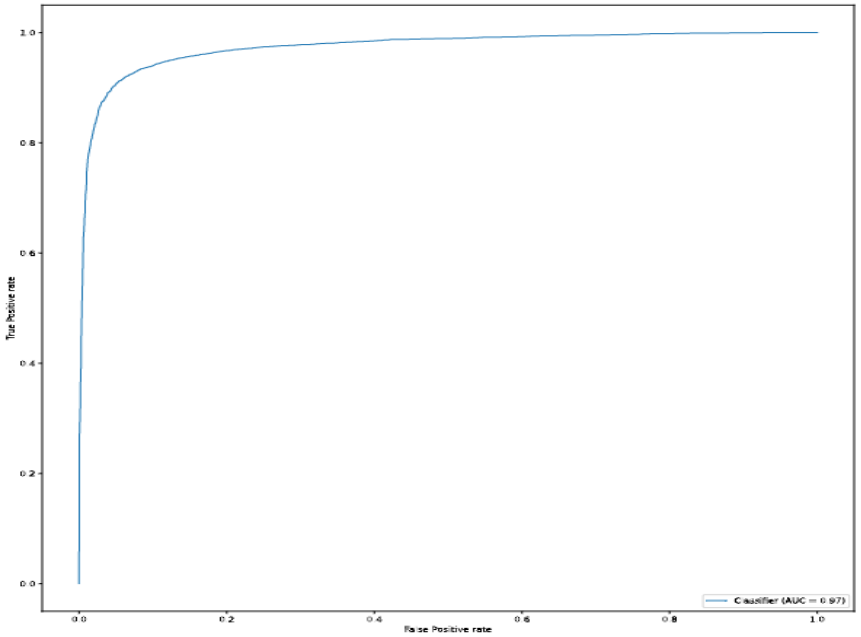
Power based classifier – 78% accuracy

Our model as anomaly detector:

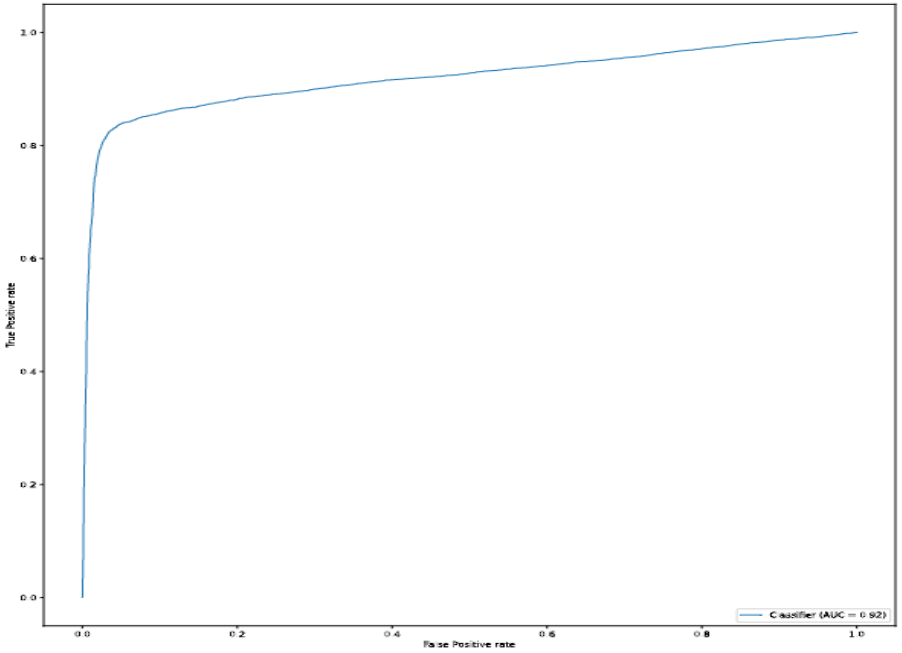


Simulated attacks:

- Code injection attacks
- Data extraction attacks



EM (AUC - 97%)



POWER (AUC - 92%)

Future work:

- More realistic EMI measurements
- Differnet programs
- OS based environment

Commercialization:

- SEL - PLC manufacturer