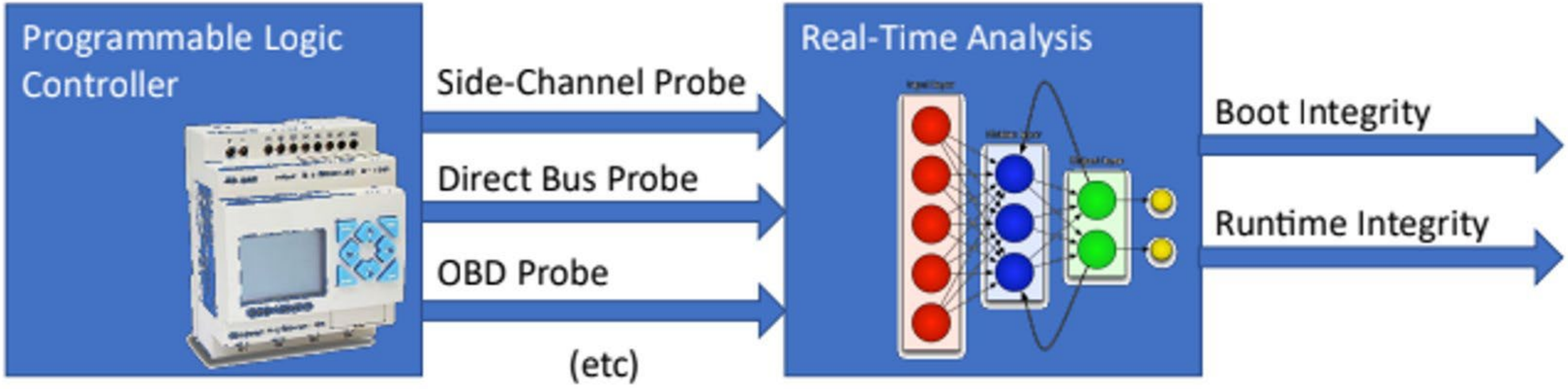
Task 13 : Firmware Verification

Principal Investigator: Dr. Yossi Oren, BGU

Lead Researcher: Mr. Michael Amar, BGU

Task Overview



Programmable Logic Controller

Side-Channel Probe

Direct Bus Probe

OBD Probe

(etc)

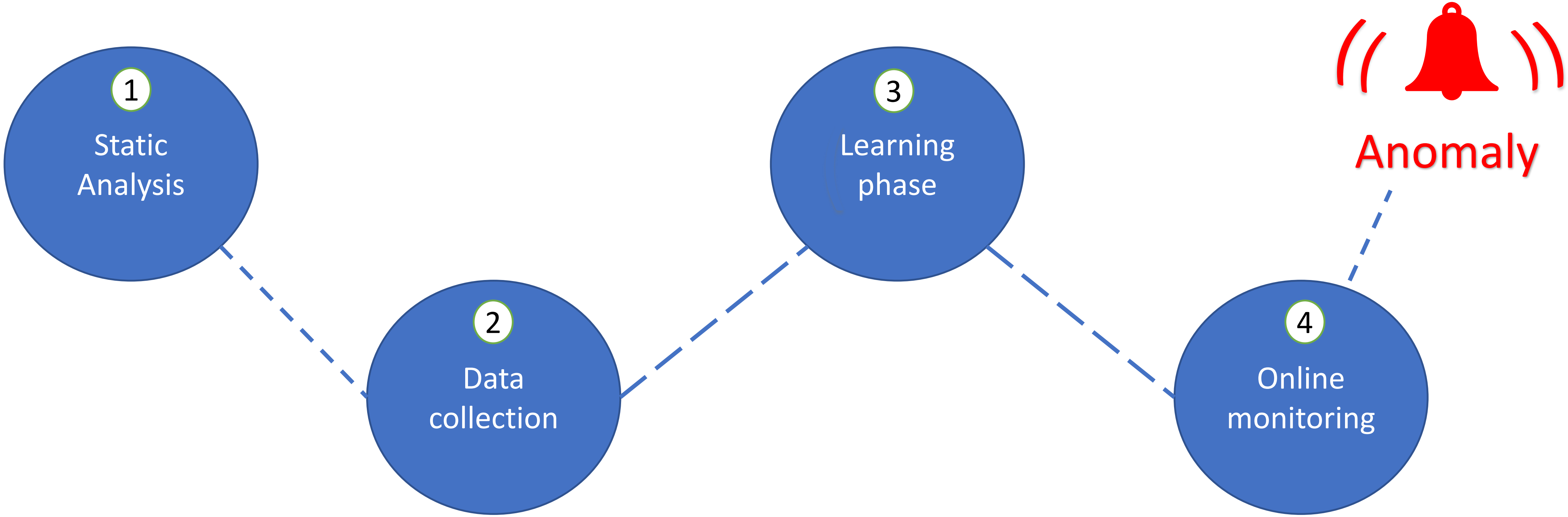
Real-Time Analysis

Boot Integrity

Runtime Integrity

- Involved Consortium Members: BGU, Resource Innovations, ASU, DLC, Arava
- Additional Participation: MITRE, APS, Alon Tavor, SEL
- Start Date: 05/2022

Proposed method

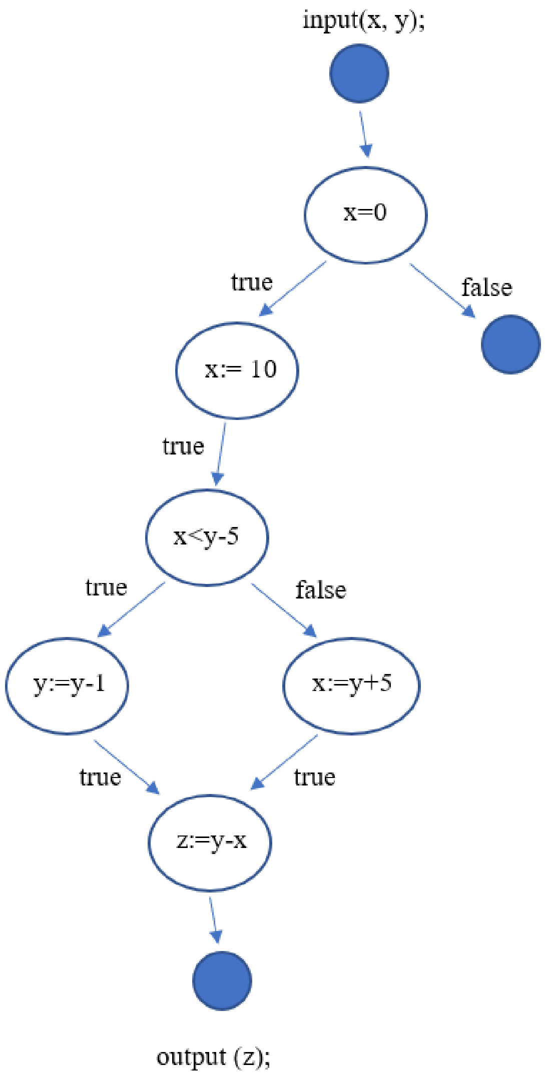


Static Analysis

- Building Control Flow Graph

- Detecting feasible paths

- Generating representative test cases



Data Collection

- Running the representative test cases

- Collect useful side-channel data
  - Running time
  - Memory usage
  - Power consumption
  - Bus activity
  - Etc..

Learning Phase

- Extract useful features
- Train model based on both legitimate and malicious executions
- Querying the model will result probability of legitimate execution

Online Monitoring

- Continually supervise the PLC execution

- Constantly check if the code is benign/malicious

- Alert about anomalies

Integration and Commercialization

- Side-channel monitoring will be demonstrated on SEL PLC

- ASU will provide malware prototypes and act as "red team”

- SEL, Nexant, RI, DLC will consider commercialization plan for developed technology