Project Title: **DETECT ANOMALIES IN CPS WITH GENERATIVE ADVERSARIAL NETWORKS**

Proposed by: Runhao Wang (runhaow@uci.edu)

The emergence of Internet of Things (IoT) has led to more and more systems and devices being sensorized and coming online, communicating and operating autonomously. Securing cyber-physical systems (CPS) against malicious attacks is of paramount importance because these attacks may cause irreparable damages to physical systems. Current detection techniques that employ simple comparison between the present states and predicted normal ranges for anomaly detection are inadequate to address the highly dynamic behaviors of the systems.

The project developed a machine learning method based on Generative Adversarial Networks (GANs) to detect anomalies in CPSs.

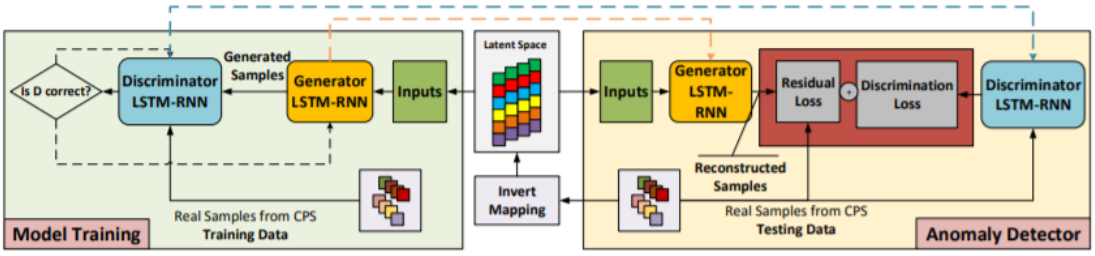
Learning Objectives:

1. Study and analysis:
    a. Embedded system with sensor networks
    b. Time-series data and LSTM
    c. Generative adversarial networks for trianing and modeling
2. Optimization:
    a. Comparing different structure or NN
3. Implementation:
    a. Build up the embedded sensor network systems
    b. Implementing the GAN
    c. Modeling and tuning

Technology and Tools:

- Python
- PyTorch
- SystemC

Project Illustration:



[Image source: Dan Li, et al 2019]