IoTlab.space

Industrial Automation security Lab

Ver 1.0 – 23 Apr 23

IoTlab.space

Automation

IDMZ

IT

Safety critical

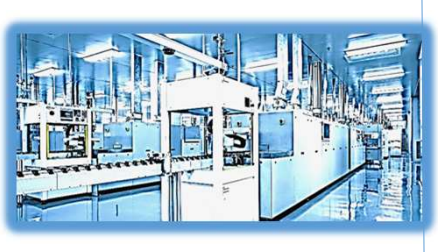
Areas

Operation & Control

Internal

Internet

Enterprise



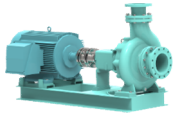
ERP

MES

SCADA

RTU

PLC



Business operations

CISCO ISE

Analyzer

Cybervison Stealthwatch

Device level

IE switch

IE switch

Simulated attacks

Automation Hacking Lab

Demo scenarios

- A factory is in normal operation, with legacy PLC and Actuators, pumps are working, actuators and & lights are on.
- Not all equipment in the factory is the latest model, there are traditional products.

- Modbus Man-In-The-Middle | SANS ICS Concepts - YouTube

Components

- Honeypot, traffic simulation: Conpot
- Vulnerability scan: Snort, nmap
- Scan & protect: Cisco Cybervision, Cisco Steathwatch
- Hacking: Ettercap