INFRASTRUCTURE CYBERSECURITY: AN ACADEMIA VIEWPOINT

Irfan Ahmed
Assistant Professor
Department of Computer Science
University of New Orleans

I AM … cs.uno.edu/~irfan

Cyber-Physical
Systems
Laboratory

- Assistant Professor of Computer Science at the UNO
- Director, Cyber-Physical Systems (**CyPhy**) Lab at UNO
- Working on the cybersecurity of ICS since 2010
  - "Forensic Readiness in Control Systems: Tools and Methods"
  - Queensland University of Technology, Brisbane, Australia
  - Had a power generation company as an industrial partner
- Related research interests include
  - Digital Forensics
  - Security via Virtualization
  - Malware Detection and Analysis
  - Cybersecurity Education
- Received more than 2.5 million dollars in research funding

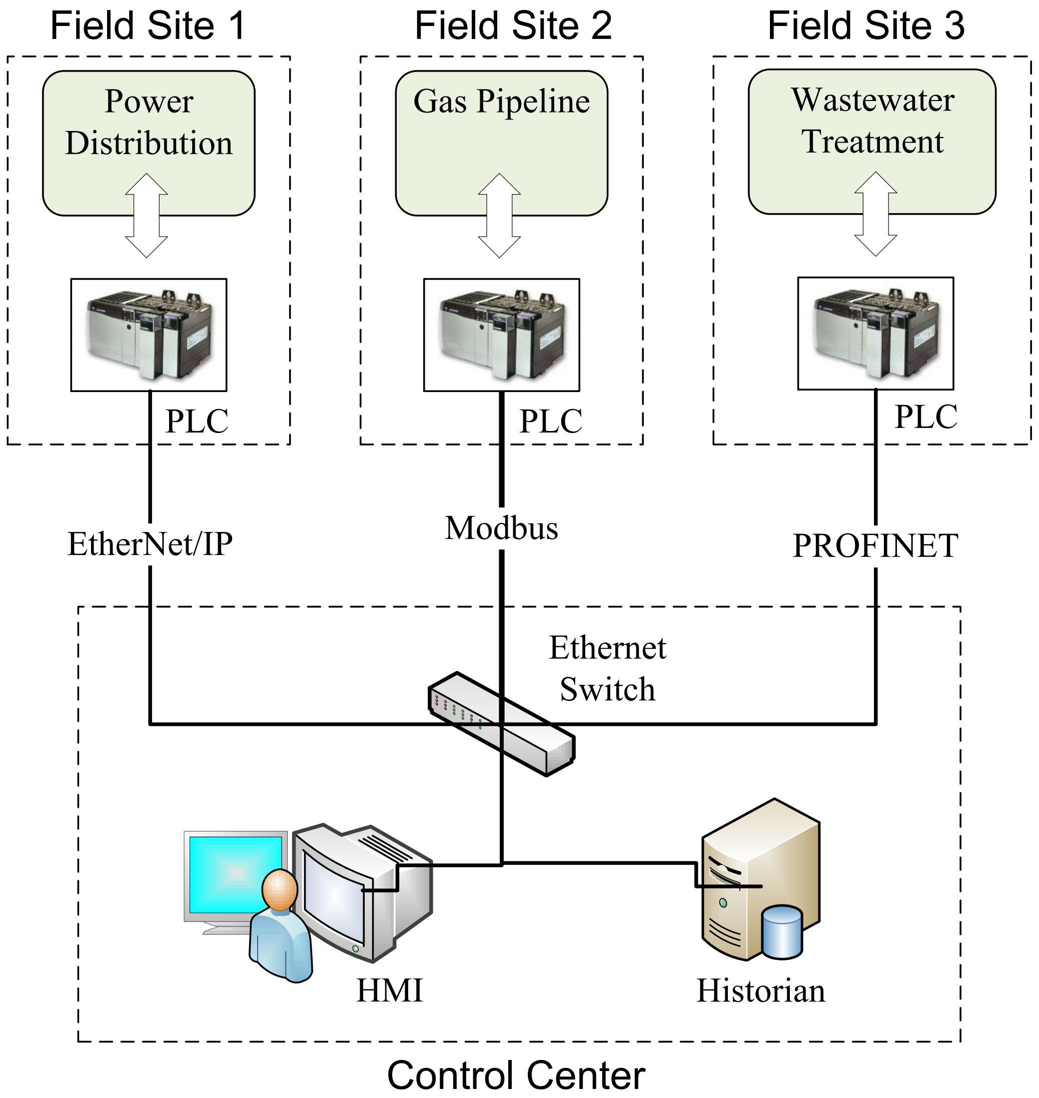
TOP FOUR CHALLENGES FOR ACADEMIA

- Access of an ICS testbed
  - Expensive to build
  - Lack of publicly available testbeds
- Establishing collaborations with Industry
  - Tight-lipped SCADA/ICS owners and operators
- Teaching ICS security to cybersecurity students
  - Interdisciplinary nature of ICS
  - Lack of a textbook and publicly available supporting material
- Small ICS security research community in academia
  - Expand research focus; currently on IDS, Firewall …
  - Encourage security researchers to take interest in ICS

ICS TESTBEDS

- ICS testbed in industry
  - Often used to test vendor patches
- Simulators
  - simSCADA to generate the network traffic of field sites
- Virtualization
  - Virtual machines; each can act as a controller/field device
- Small-scale real-world ICS
  - Use commercial software and hardware
  - Laboratory scale
  - Functional physical processes

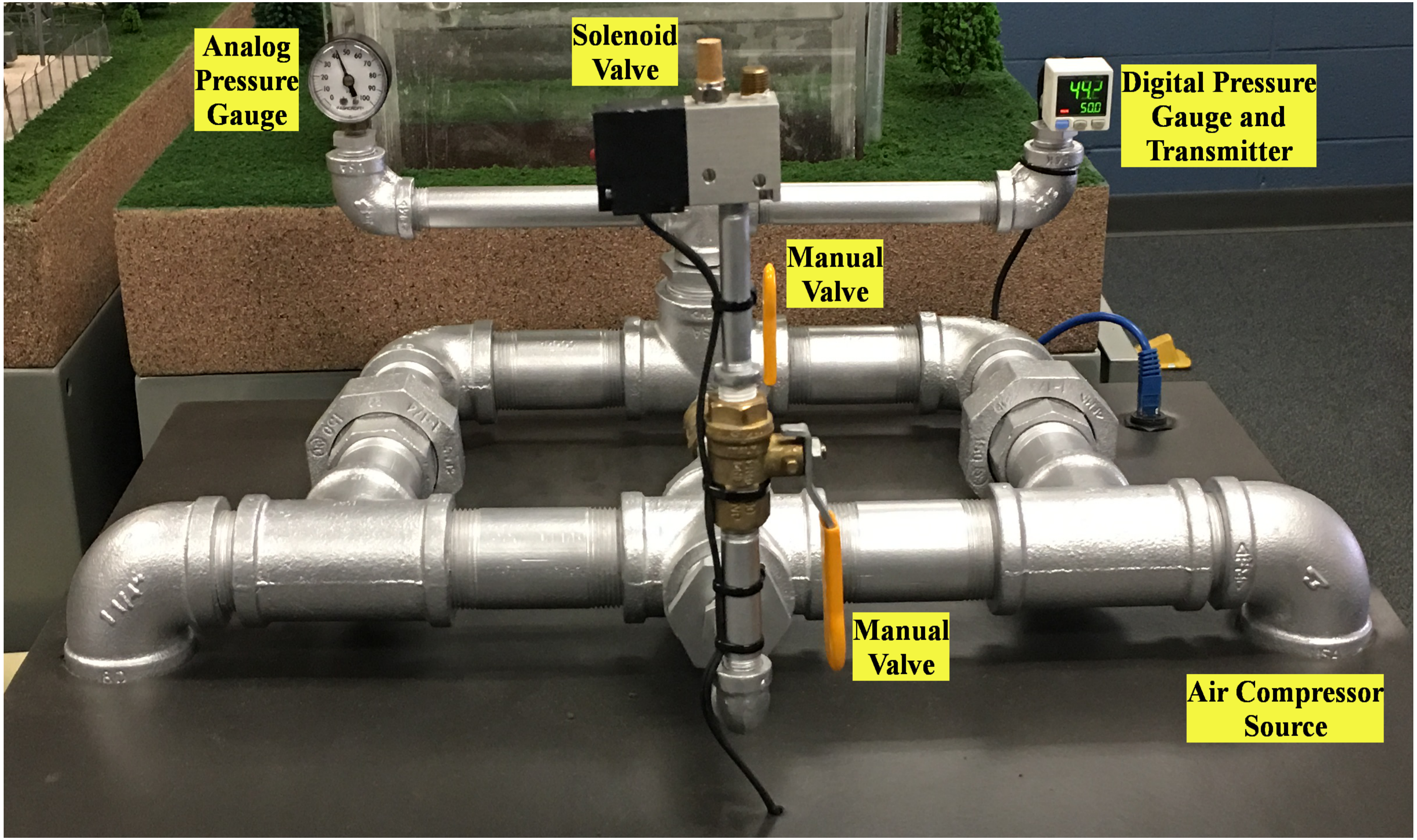
ICS TESTBED AT UNO



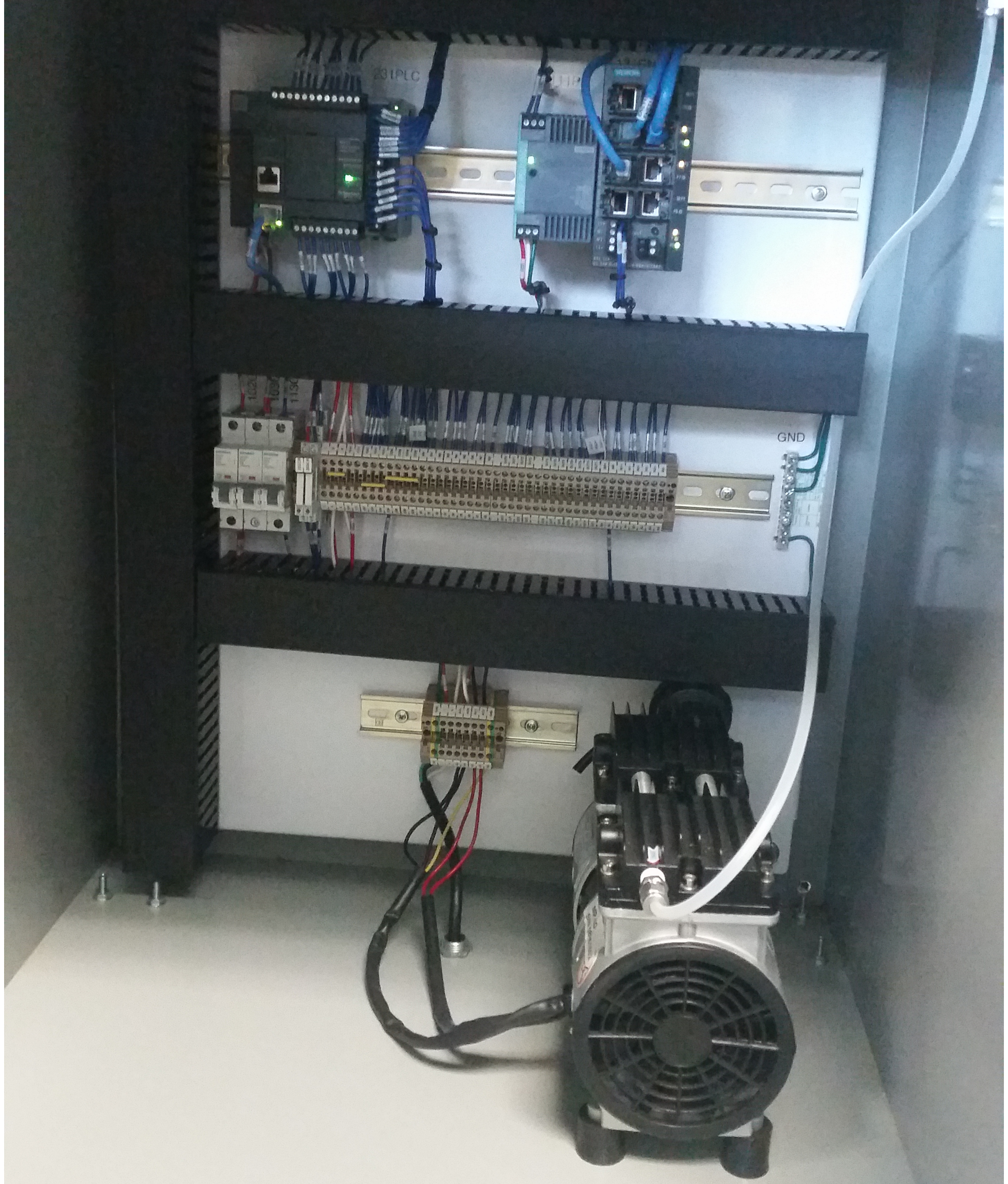
ICS TESTBED AT UNO - FUNDING

- DoD’s Defense University Research Instrumentation Program (DURIP)
- $96,000 from Army Research Office (ARO)
- $50,000 from UNO Foundation

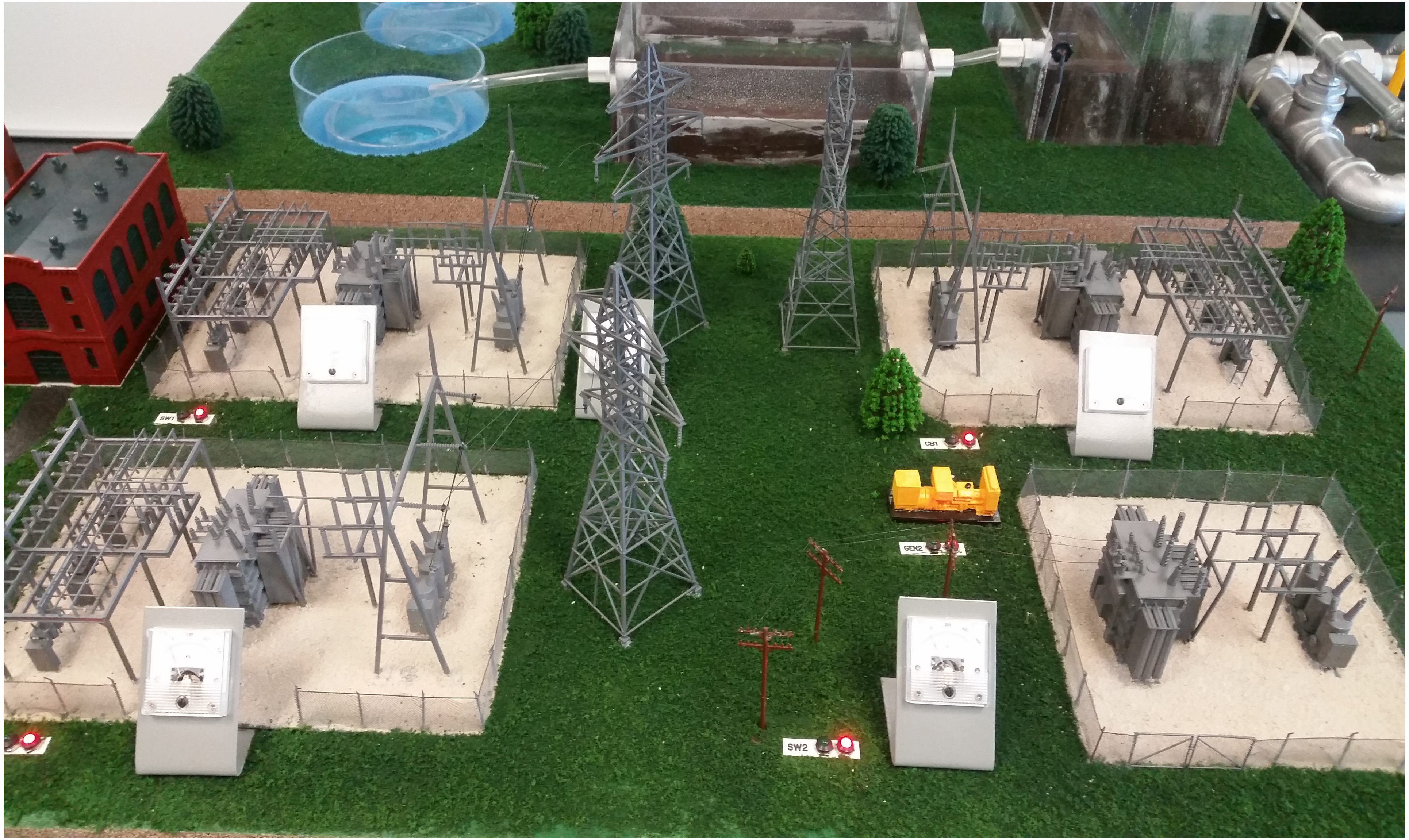
GAS PIPELINE – TOP VIEW



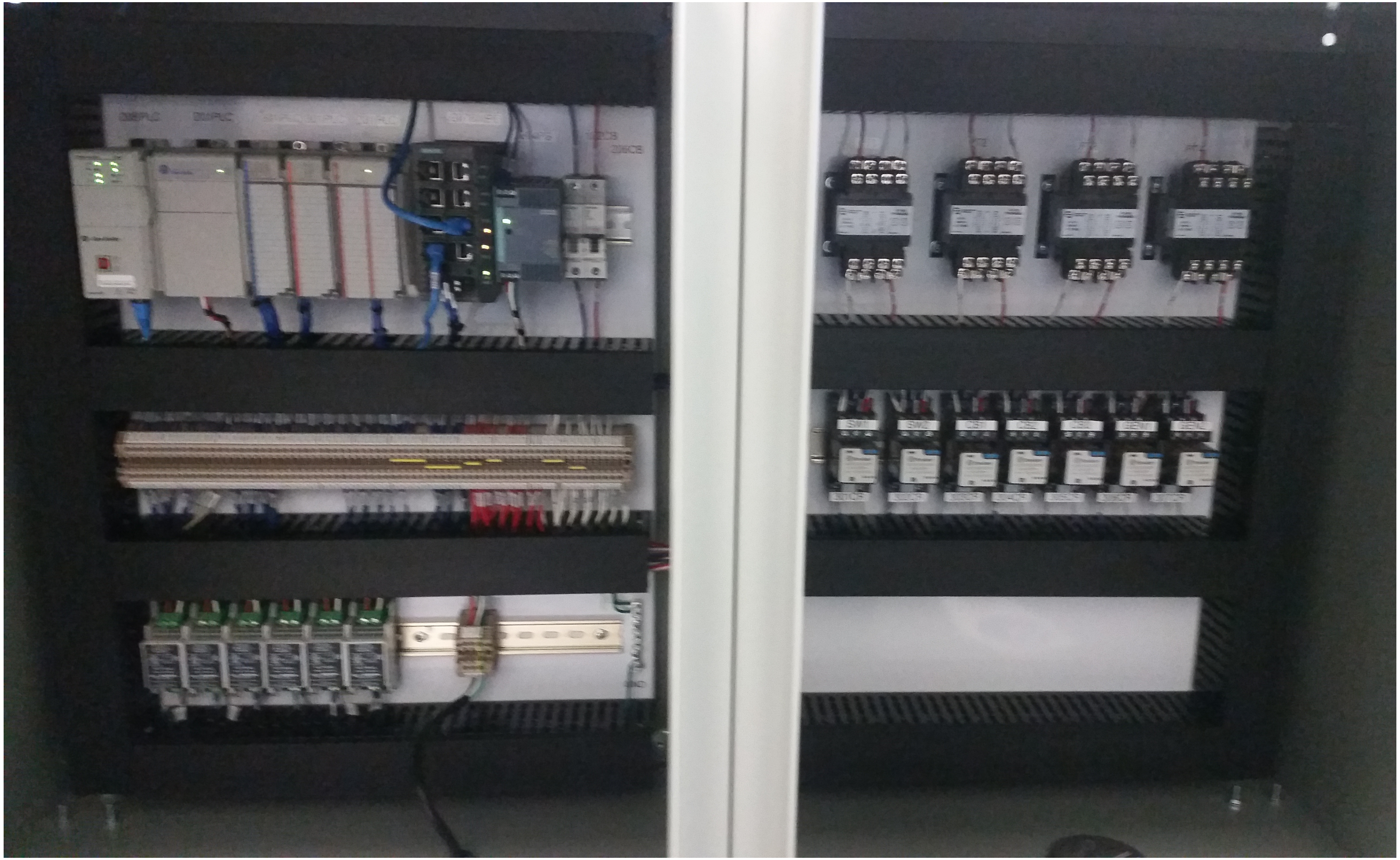
GAS PIPELINE — CABINET VIEW



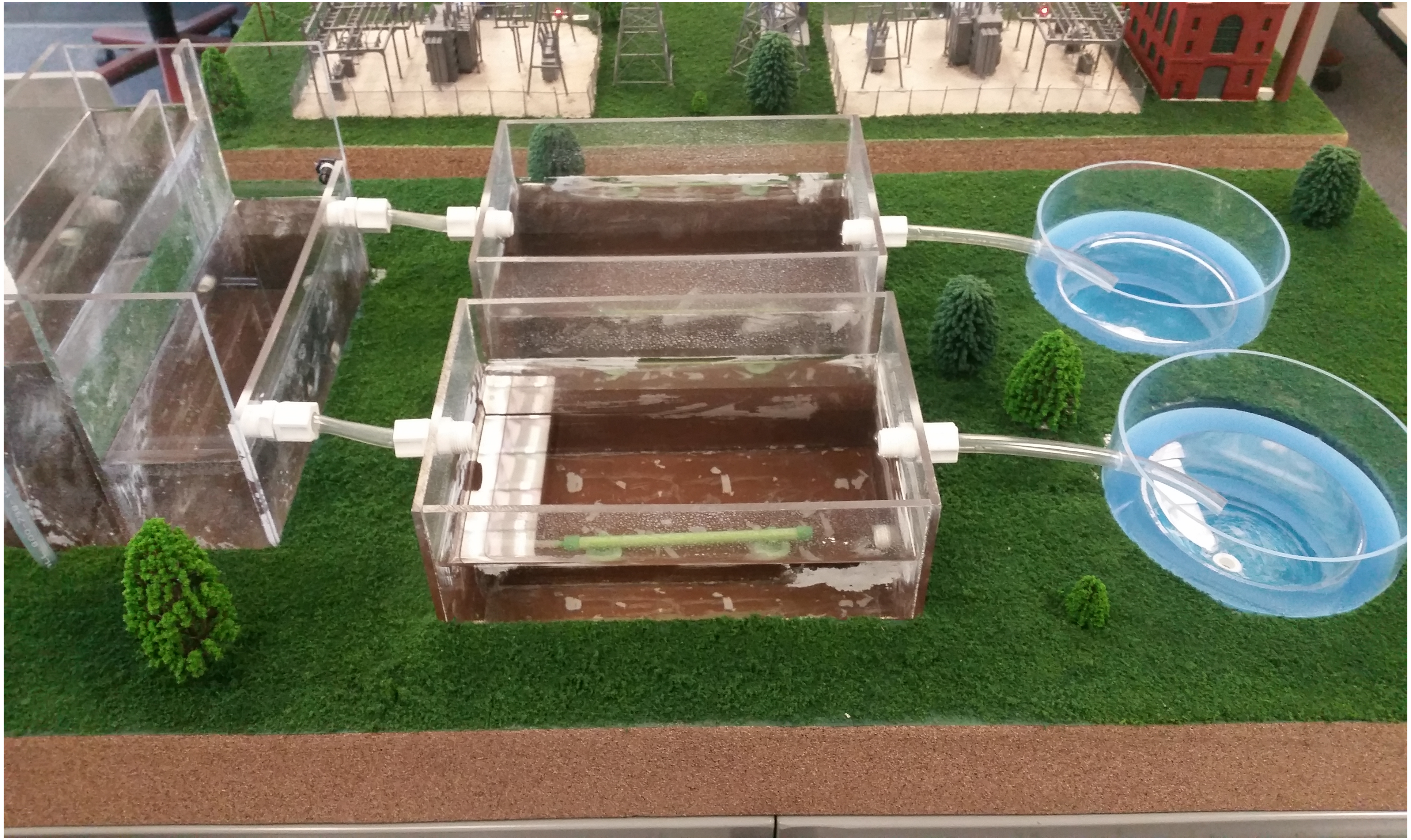
POWER DISTRIBUTION – TOP VIEW



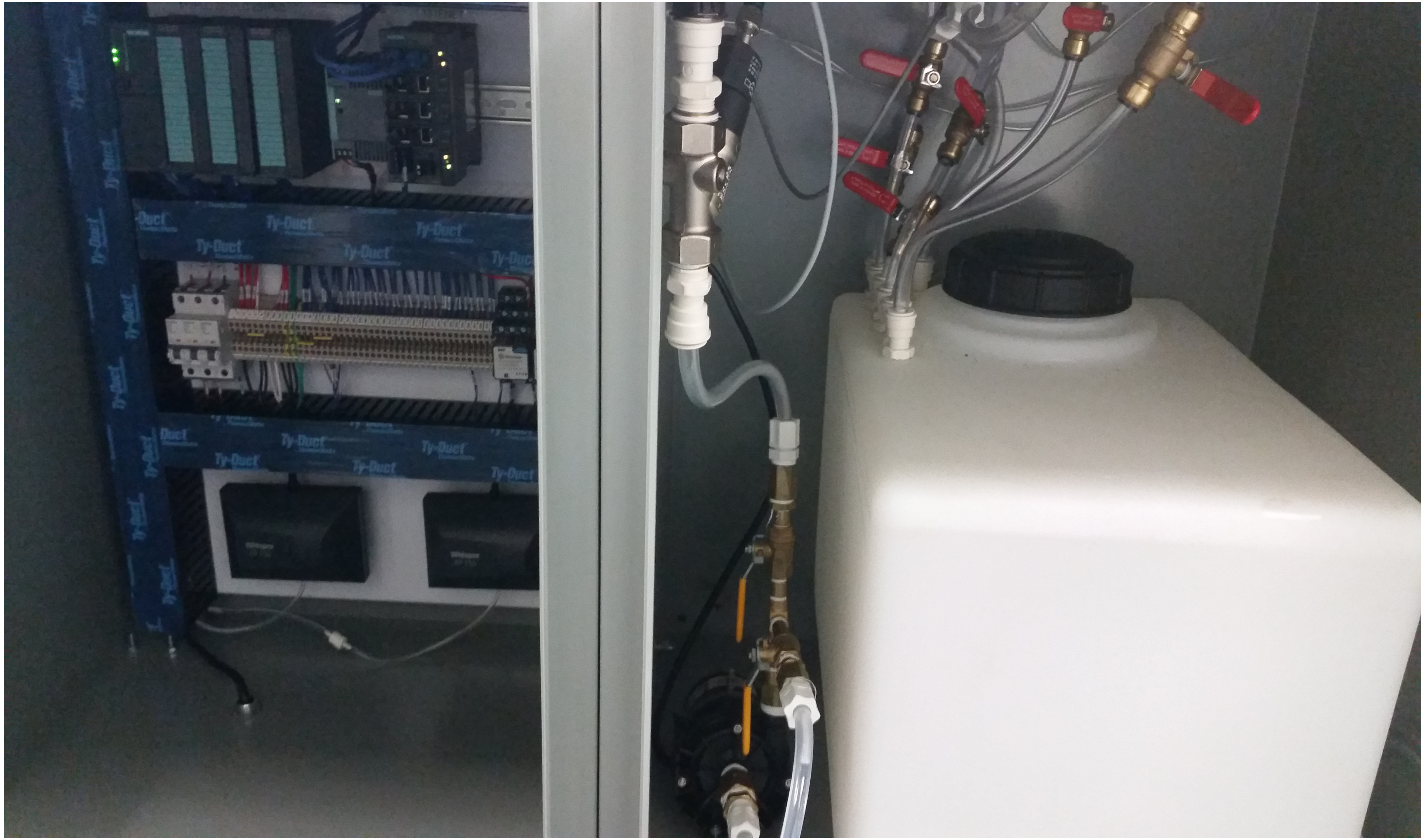
POWER DISTRIBUTION – CABINET VIEW



WASTEWATER FILTERING – TOP VIEW



WASTEWATER FILTERING – CABINET VIEW



COLLABORATION WITH INDUSTRY

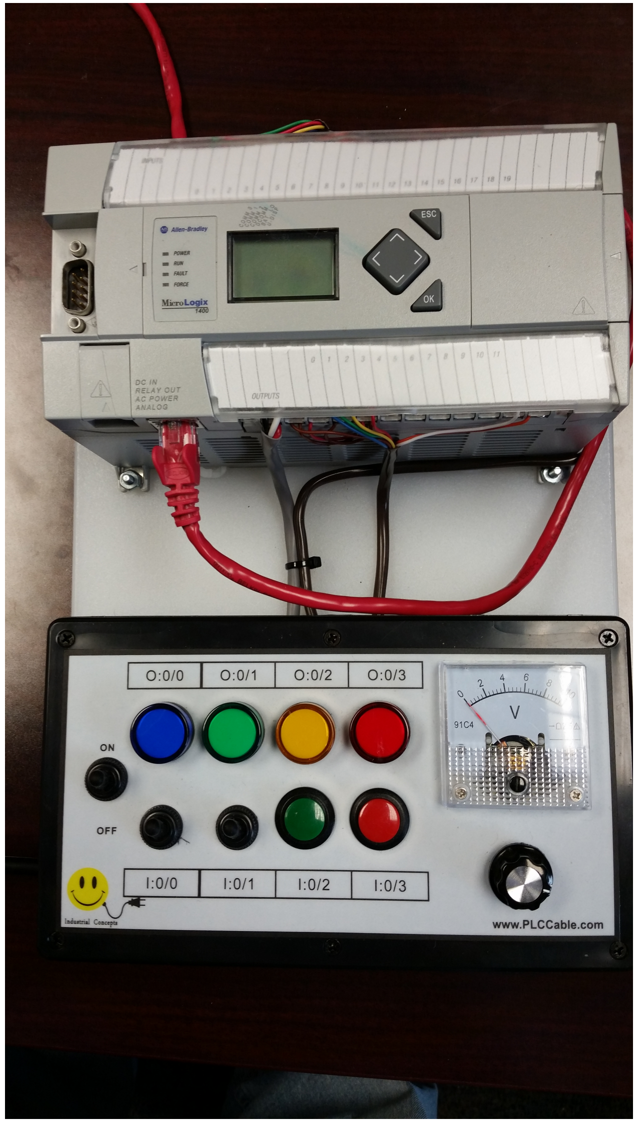
- Industry can provide
  - close access to a real-world ICS/SCADA system,
  - technical assistance, and
  - financial support
- Industry collaboration is challenging
  - critical nature of ICS and physical processes
  - information leakage may cause damage
- Government can play a mediator role
- Community-of-interest meetings
  - gather ICS/SCADA owners and operators, vendors, and academia

TEACHING ICS SECURITY TO CS STUDENTS

- Challenges
  - ICS is *interdisciplinary* in nature
  - Raising interest of CS students
  - Lack of a textbook on ICS security
  - Lack of prerequisites for an ICS course
- ICS Security Course at UNO
  - Content covers from Basic introductory level to Advance
  - Hands-on approach, taught in a lab

COURSE ON ICS SECURITY FOR CS AT UNO

- Course Topics
  - Introduction to industrial control systems
  - PLC programming
  - ICS network protocols
  - ICS vulnerabilities and cyber attacks
  - ICS security solutions
- Hands-on Exercises
  - *PLC:* Allen-Bradley's Micrologix 1400 B
  - Program PLC to control Traffic Lights
  - Implement man-in the middle attack



ICS SECURITY RESEARCH COMMUNITY

- Small ICS security research community in academia
- Encourage cybersecurity researchers to take interest in ICS security
- Current research efforts are mostly limited to
  - IDS
  - Firewall, etc.
- Expand ICS research focus to other areas such as
  - Digital forensics
  - Virtualization
  - Human factors such as security practices of control operators/engineers and mitigation of human errors
  - ICS Security Education

Contact me @

Irfan Ahmed
irfan@cs.uno.edu
504 – 982 – 5578