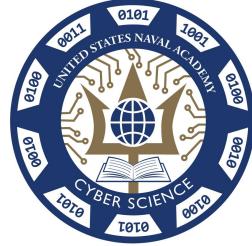




UNITED STATES
NAVAL ACADEMY

Annapolis



Lessons Learned when building a Maritime Systems Security Laboratory Testbench

Brien Croteau, USNA, Cyber Science

DefCon 31- ICS Village, 12 Aug 2023

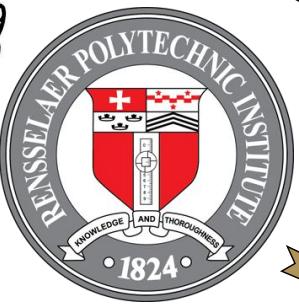


Link to these slides:
https://github.com/brienc23/Defcon31_workshop_materials

My Background

24-year Active Duty Naval Officer, EE Ph.D.
Assistant Professor, USNA Cyber Science Department
Military Deputy for the Dean of Math and Science

Disclaimer: All my own opinions, not those of the US Gov, US Navy, or USNA



EA-6B Naval Flight Officer



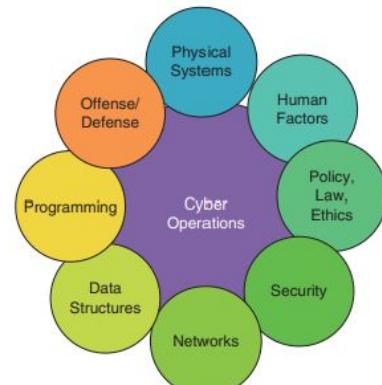
Research in Cyber-Physical Systems (CPS) Security: Detection of malicious sensors using side-channel power analysis, Alternate actuation paths, Actuation limits, Industrial Control Systems (ICS) security, Maritime Hull, Mechanical, & Electrical (HM&E) security

About the U. S. Naval Academy

- Located in Annapolis, MD
- One of Five Federal Military Academies
 - feeding the U. S. Navy and Marine Corps
- Approx. 4500 students and 600 Faculty
 - 300 civilian, 300 military
- 26 Majors
 - 65% graduates must be STEM majors



Cyber Operations:
Interdisciplinary
Major



COVER FEATURE CURRICULAR FOUNDATIONS FOR CYBERSECURITY

The USNA's
Interdisciplinary Approach
to Cybersecurity Education

Tracy Emmerseil, Joseph M. Hatfield, Jeff Kosseff, and
Stephen R. Orr, U.S. Naval Academy

Faced with unprecedented cybersecurity challenges, the
U.S. Naval Academy (USNA) has recognized the need to
increase its supply of newly minted officers who have a solid
educational foundation in cybersecurity and cyber operations.

<https://ieeexplore.ieee.org/abstract/document/8677342>



What do I mean by CPS?

Cyber-Physical Systems

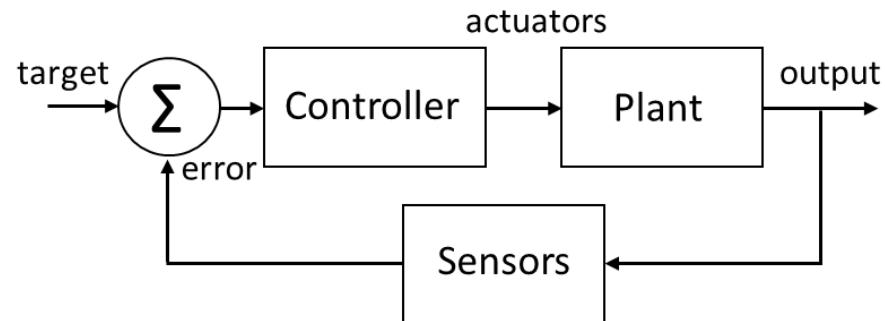
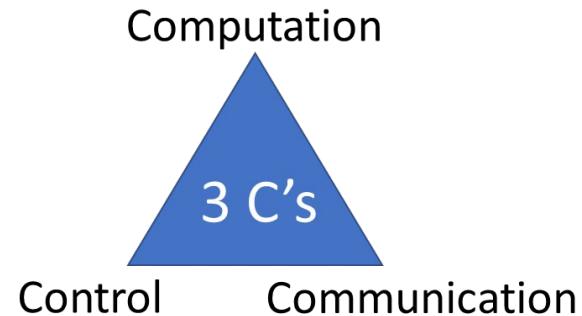
Other Monikers:

OT = Operational Technology

ICS = Industrial Control Systems

Industry 4.0, IIoT

SCADA



Why should you care about this?

= threatpost Cloud Security / Malware / Vulnerabilities / InfoSec Insider

Researcher: Not Hard for a Hacker to Capsize a Ship at Sea

Mashable TECH ▾ SCIENCE ▾ SOCIAL GOOD ▾

Remotely hacking ships shouldn't be this easy, and yet ...

UNITED STATES COAST GUARD
U.S. Department of Homeland Security

MARINE SAFETY ALERT
Inspections and Compliance Directorate

Safety Alert 06-19

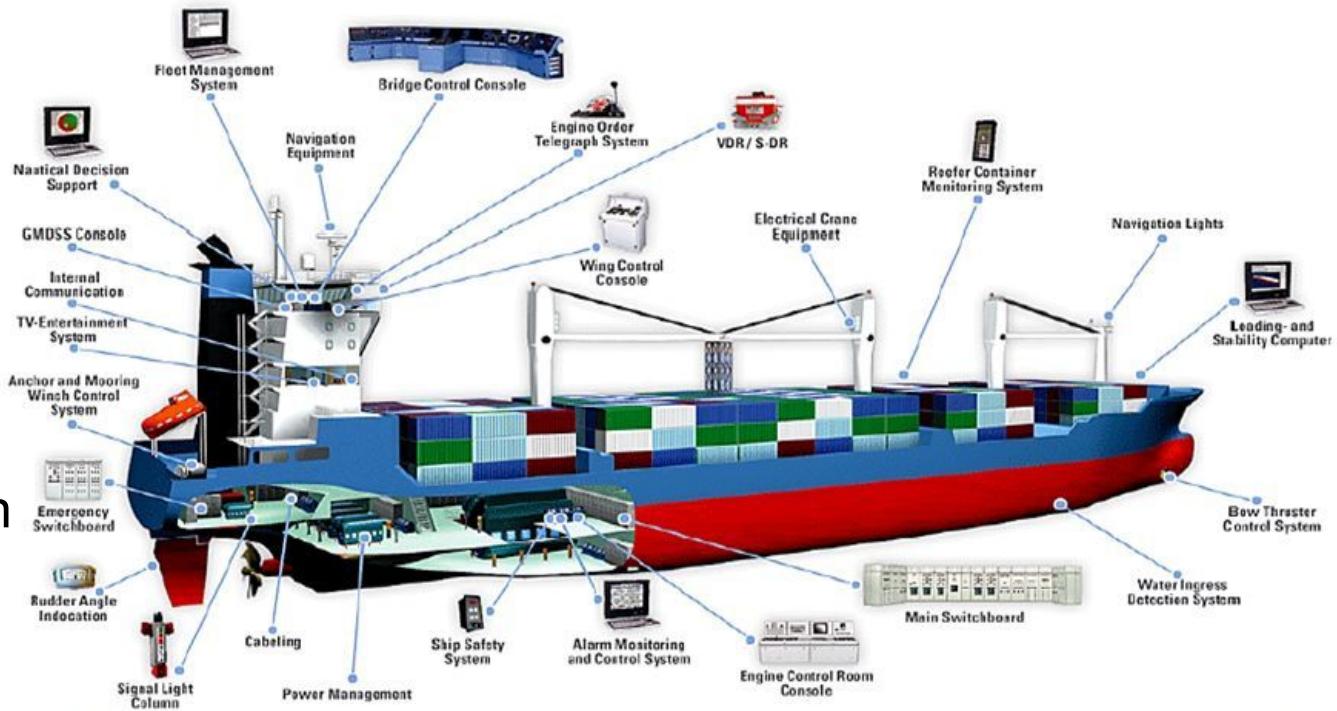
July 8, 2019
Washington, D.C.

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels



Maritime Systems Overview

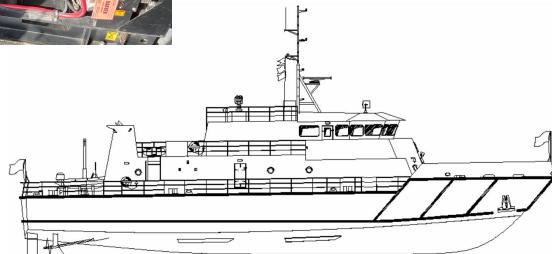
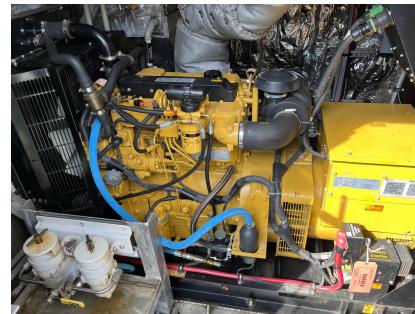
- Propulsion
- Electrical
- Auxiliary
 - Fresh Water
 - Sea Water
- Bridge
 - Navigation
 - Communication
 - Sensors



USNA Yard Patrol vessels (YP703)

- Builder: C&G Boat Works Inc. (YP703-2010 to YP708-2014)
- Propulsion: 2x715 bhp (2x448kw) Cat C-18 diesel engines at 2,100 RPM
- Electrical: 2x CAT Diesel Generators 480V, 99 KW, 3-phase AC
- Length: Overall: 119 feet (36.3 meters)
- Beam: 27.9 feet (8.51 meters)
- Displacement: 227.6 Metric Tonnes (223.9 long tons)
- Draft: 7.5 feet (2.27 meters)
- Speed: 12.6 knots (23.3 kilometers per hour)

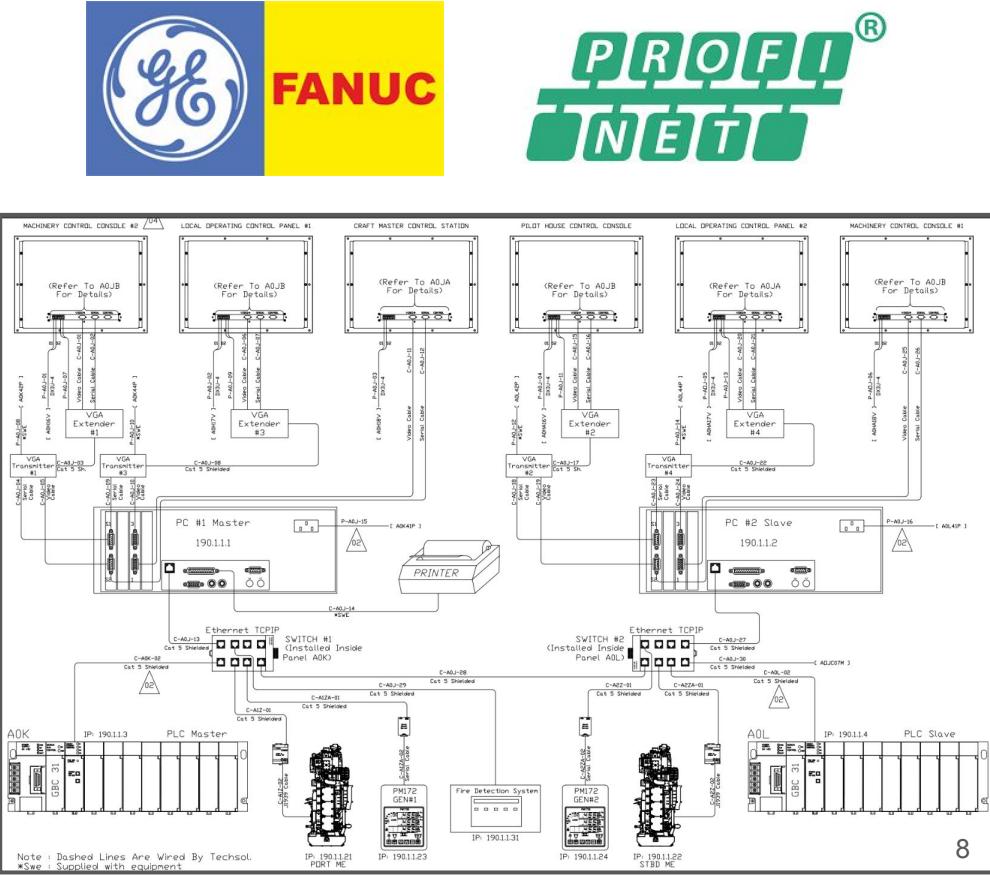
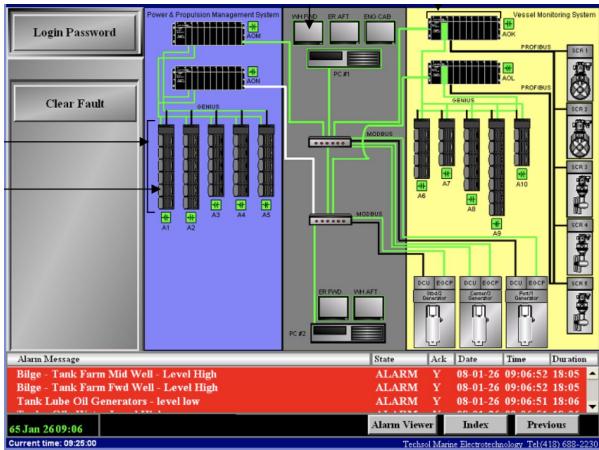
Used for local ship-handling
training operations and summer
cruises on the eastern seaboard



MAX II Alarms and Monitoring System on the YP703 class

GE Fanuc based custom install

- 2x PC to drive 6x touchscreen Human Machine Interface (HMIs)
- 2x Programmable Logic Controllers (PLCs)
- Dual redundant IP/serial communications
- Interfaces with:
 - Engines
 - Generators
 - Tanks
 - Fire Detection

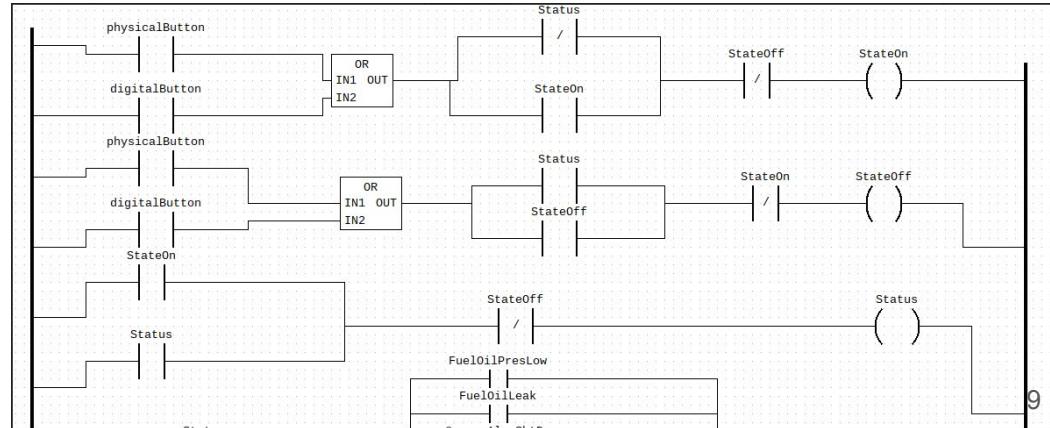
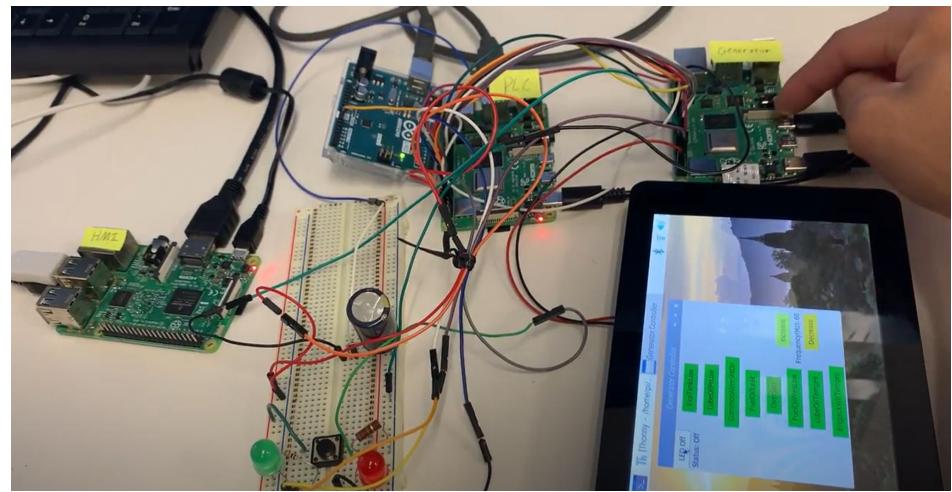
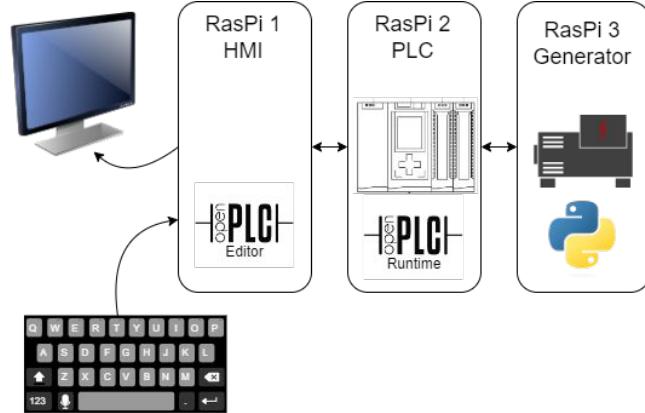


5 min [demo video](#)

v1.0 Proof of Concept

3x Ras Pi: HMI, PLC, "Generator"

- OpenPLC v1.0
- 8 discrete faults
- 1 "analog" frequency
- toggle on/off status



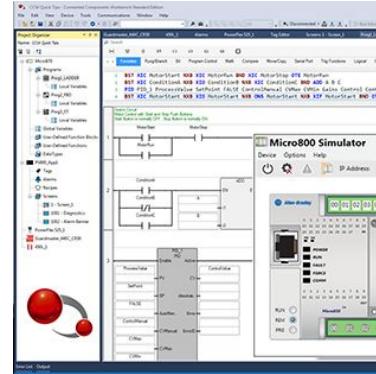
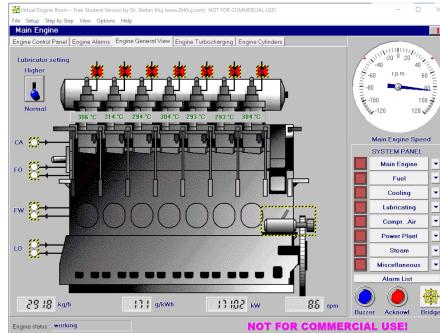
MICS Course Offering

Spring 2023, SY486K Maritime Industrial Control Systems Cybersecurity

Three-credit technical elective

Lectures, Labs, Student Presentations, and YP Project

Topics included: Maritime Systems, PLC, Ladder Logic, Modbus, CIP, Attacking ICS



https://github.com/brienc23/MICS_Course_Materials

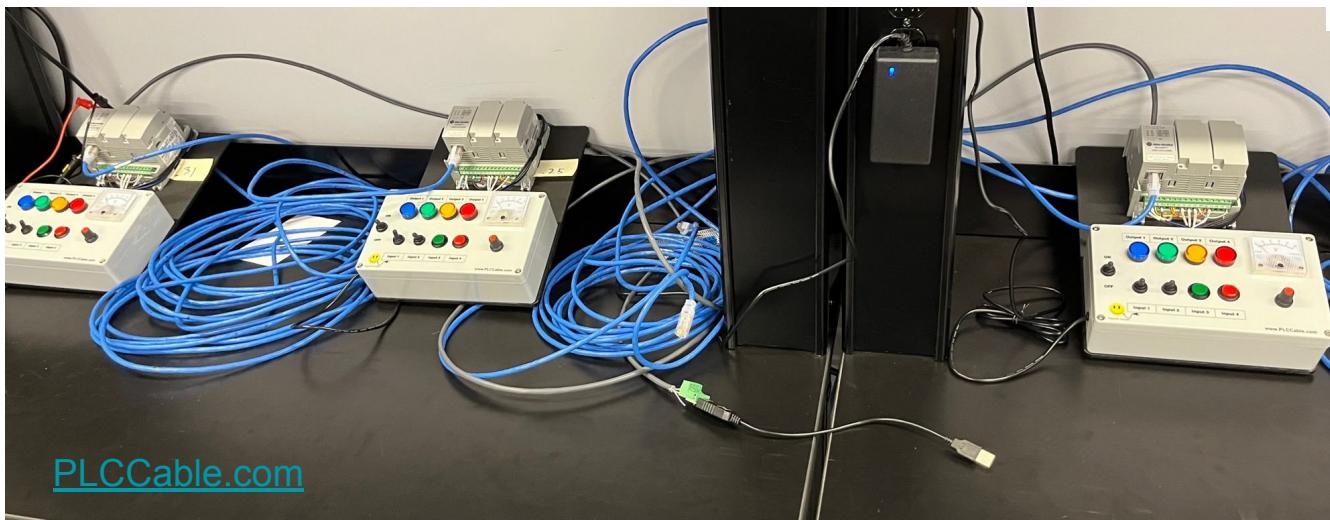


v2.0 Classroom Trainers

Allen-Bradley (AB) micro820 PLC based

Individual Ladder Logic Programming

Modbus Communication (RS-232, RS-485, and TCP)



**Rockwell
Automation**

**Connected
Components
Workbench™
Software**



v2.5 Hardware-in-the-Loop ICS (HILICS)

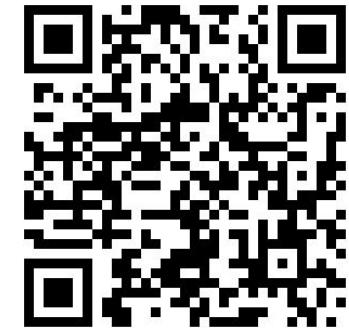
On loan from Air Force Institute of Technology (AFIT)

AB microLogix 1100+RasPi

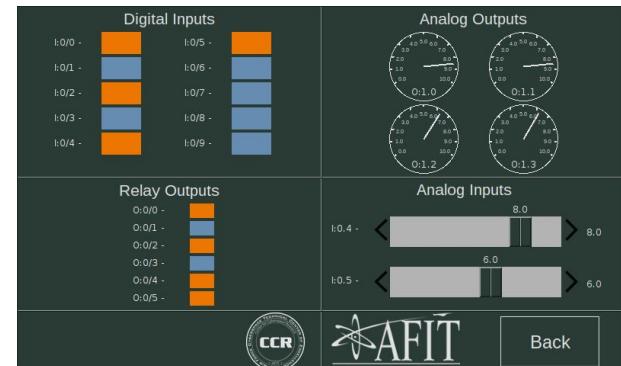
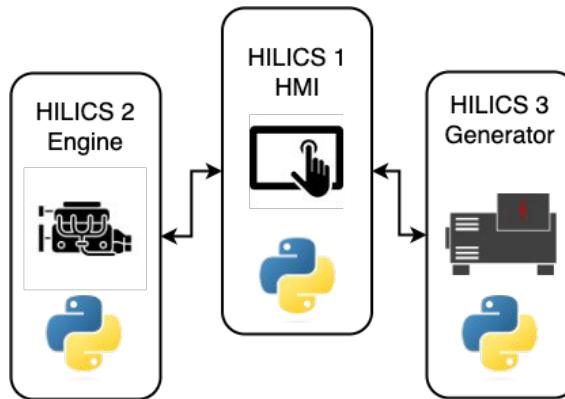
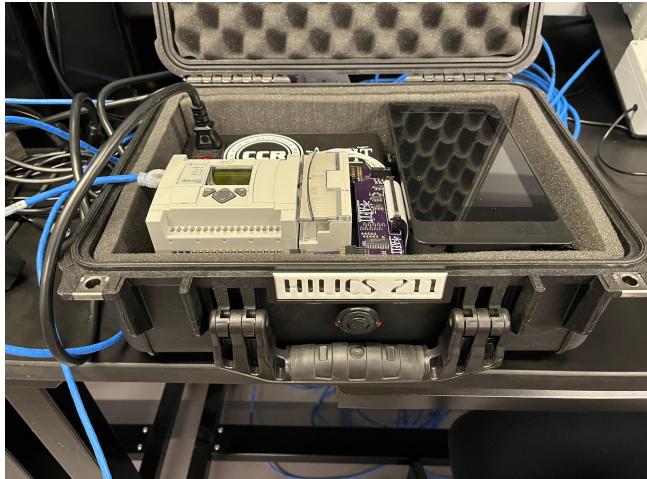
Students made a 3-node network replicating a portion of the YP703 system:

- 1x HMI
- 1x Diesel Engine
- 1x Generator

Captured their work in an Interface Control Document



[https://github.com/
sdunlap-afit/hilics](https://github.com/sdunlap-afit/hilics)



[Future] v3.0 Modular PLC Laboratory

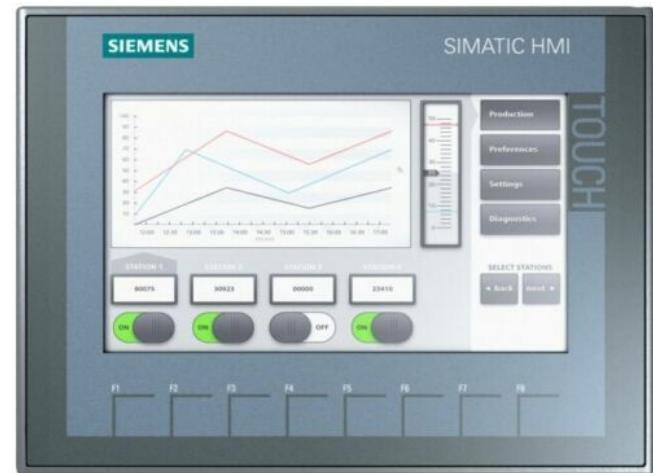
Siemens S7-1215C PLCs + ktp700 Basic HMI

Envision a reconfigurable PLC centric lab that can emulate different applications

- Naval Vessel
- Factory Floor
- Water Treatment
- Building Automation



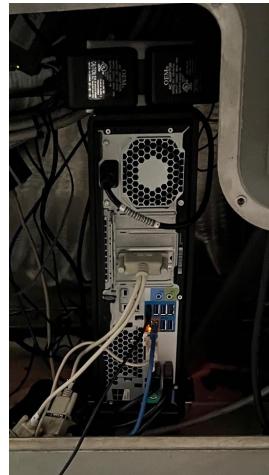
UlrichAAB CC3.0, https://commons.wikimedia.org/wiki/File:Simatic_S7-1200.JPG



[Future] v4.0 Actual YP Hardware in the Loop

GE Fanuc PLC hardware from YPs + PC

Computer endpoints and networks allow a wider range of students to interact



[Future] v5.0 Bridge and Simulated Motion Integration

<https://www.bridgecommand.co.uk/>



Research platform to work on defense on advanced cyber attacks on ships

<https://github.com/osrf/vrx>



GAZEBO ROS

Conclusion

Shared the journey that I have begun on iterating towards a more comprehensive and realistic training and research environment.

I look forward to hearing your questions and suggestions you might have about ideas moving forward.

Link to these slides:

https://github.com/brienc23/Defcon31_workshop_materials

Brien Croteau, USNA, croteau@usna.edu

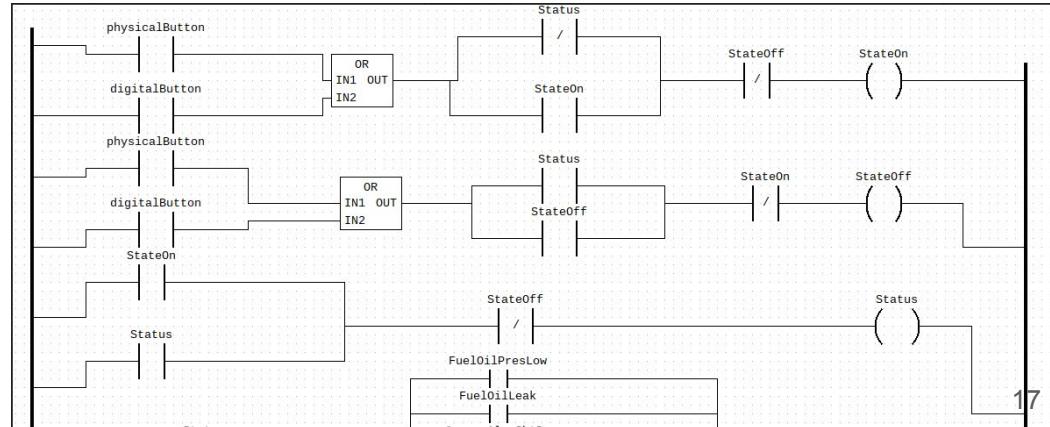
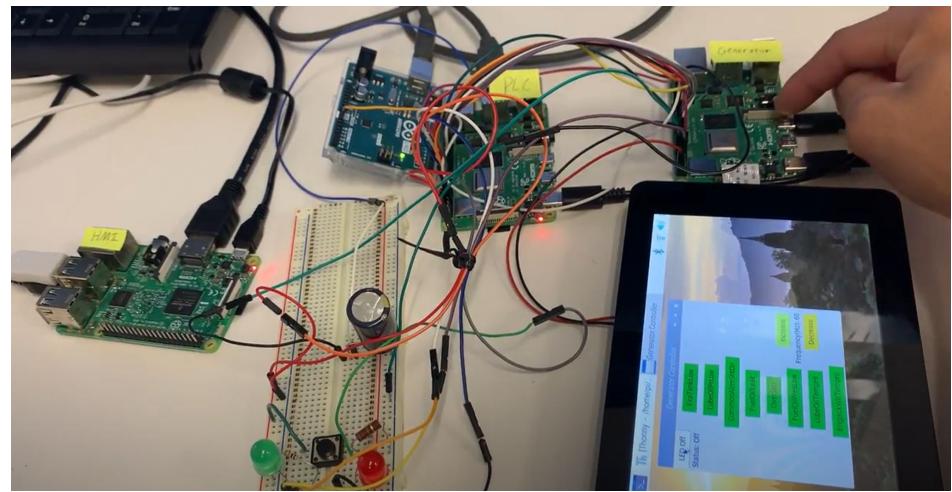
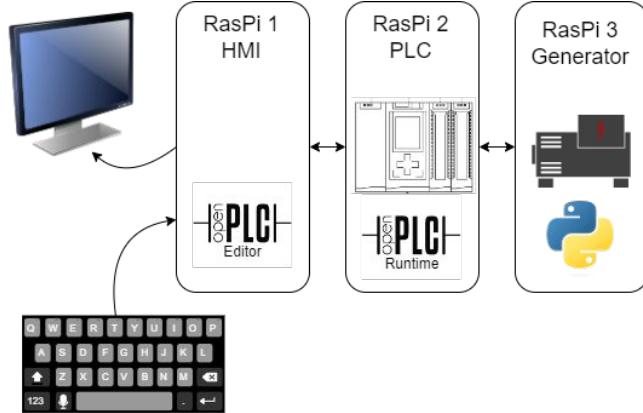


5 min [demo video](#)

v1.0 Proof of Concept

3x Ras Pi: HMI, PLC, "Generator"

- OpenPLC v1.0
- 8 discrete faults
- 1 "analog" frequency
- toggle on/off status



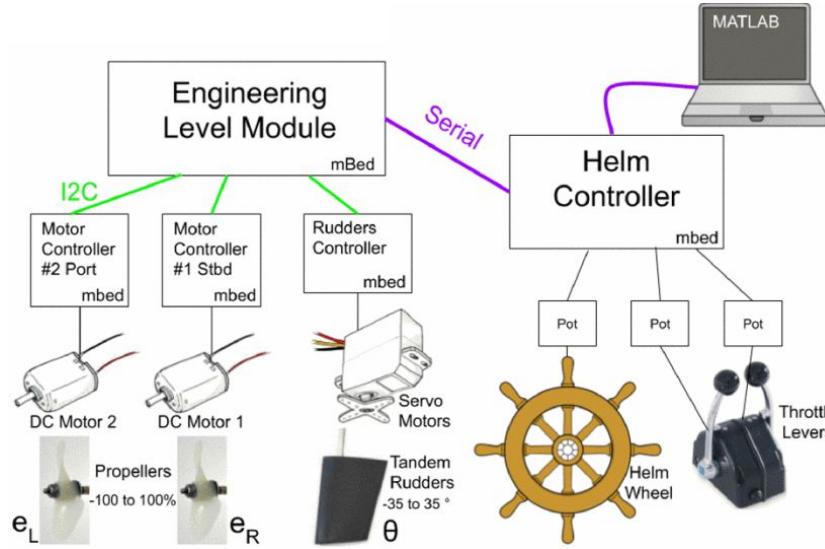
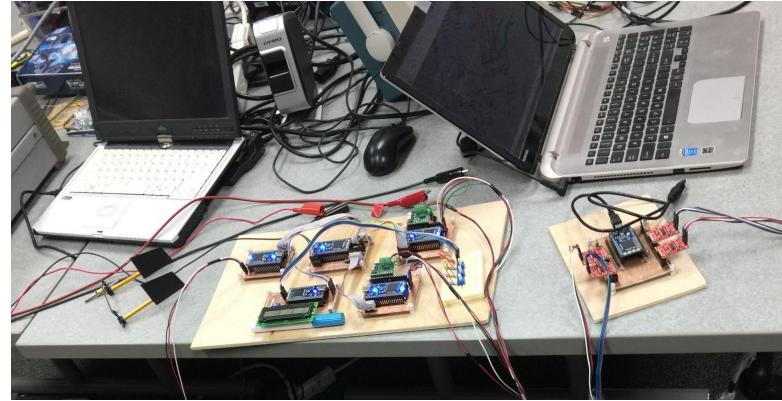
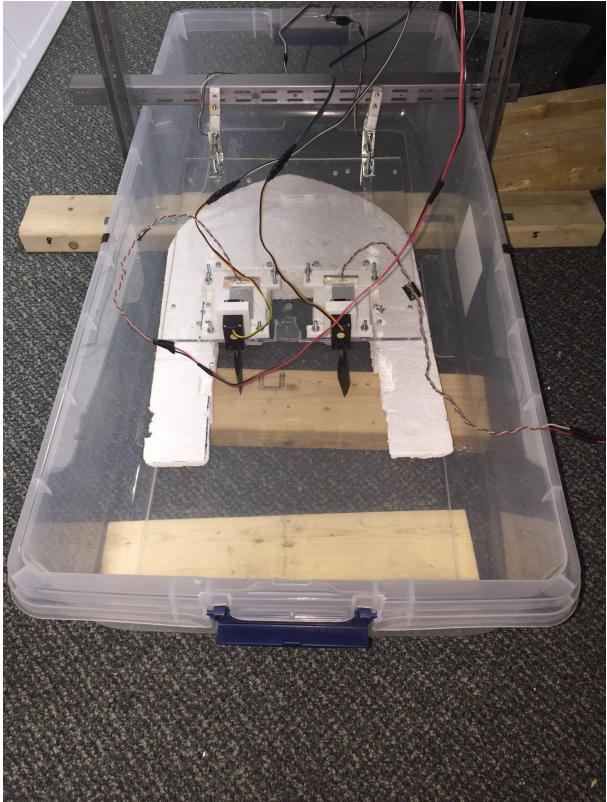
Other Maritime Testbenches



<https://www.fathom5.co/systems>



v0.1 UMBC Ship System Testbed



2019 R Week Paper
[Alternative Actuation Paths for Ship Applications in the Presence of Cyber-Attacks](#)

