Lessons Learned from Teaching a Maritime Industrial Control Systems Cybersecurity Course

Brien Croteau, USNA, Cyber Science

IEEE LCN - MarCaS, 05 Oct 2023

Link to materials:
https://github.com/brienc23/MICS_Course_Materials

My Background

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

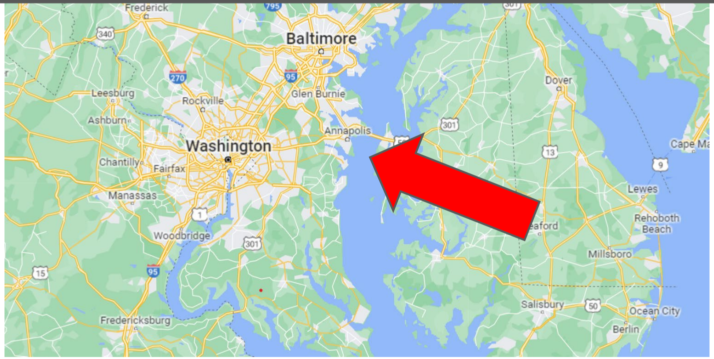
24-year Active Duty Naval Officer, EE Ph.D.
Assistant Professor, USNA Cyber Science Department
Military Deputy for the Dean of Math and Science

USNA 1999 NAVIGAMUS HONORE
RENSSELAER POLYTECHNIC INSTITUTE KNOWLEDGE AND THOROUGHNESS 1824
U.S.N.T.P.S.
UMBC

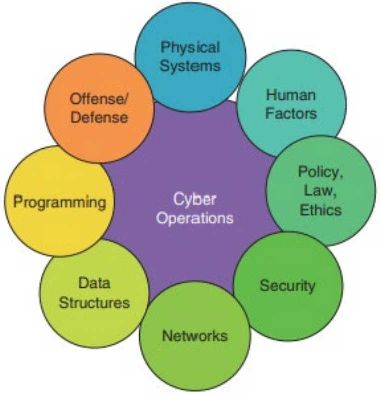
Research in Cyber-Physical Systems (CPS) Security: Detection of malicious sensors using side-channel power analysis, Alternate actuation paths, Actuation limits, Industrial Control Systems (ICS) security, Maritime Hull, Mechanical, & Electrical (HM&E) security

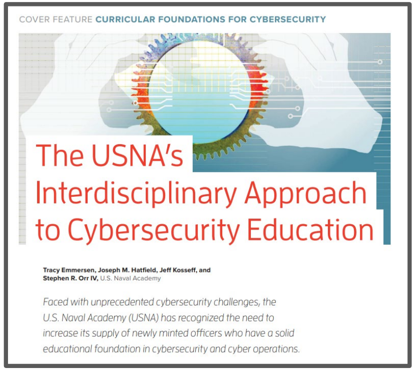
About the U. S. Naval Academy

- 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

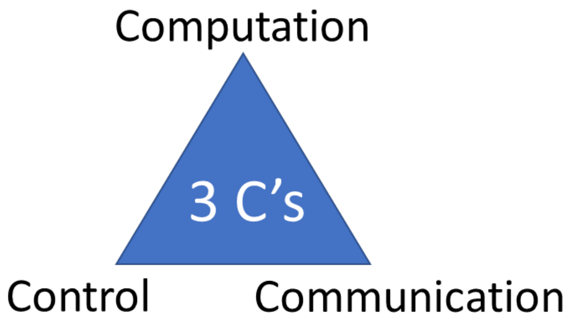
Tracy Emmersen, Joseph M. Hatfield, Jeff Kosseff, and Stephen R. Orr IV, U.S. Naval Academy

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

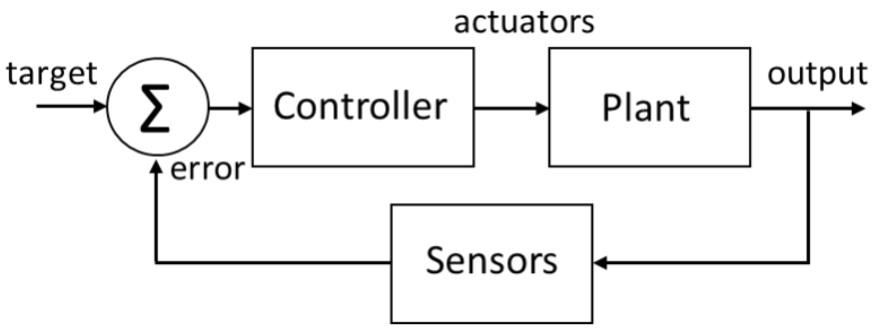
My umbrella term of choice = CPS

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

July 8, 2019
Washington, D.C.

Safety Alert 06-19

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

These were not caused by cyber attacks, but show the devastating potential consequences


USS Fitzgerald 17 Jun 2017, 7 sailors


USS McCain 21 Aug 2017, 10 sailors

Course Motivation

To allow undergraduate students to learn and gain hands-on experience with Programmable Logic Controllers (PLC) and then investigate the unique cybersecurity challenges in CPS.

To provide a relevant application focus, the subdomain of Maritime Industrial Control Systems Cybersecurity was chosen since most of our graduates will go on to serve on ships and submarines.

Course Outline

- Course Introduction
- Maritime Systems
  - Propulsion
  - Electrical
  - Auxiliaries
  - Bridge
- Industrial Control Systems
  - PLCs
  - Ladder Logic
  - Modbus
  - Attacking (and Defending)
- Final Project
  - YP703 Alarms and Monitoring

Week	Lecture	Lab
1	Class Introduction	Intro Video
2	Ship Propulsion Systems	VER Install & Startup
3	Ship Electrical Systems	VER Power Plant
4	Ship Water Systems	VER Aux Systems
5	Ship Nav and Bridge Systems	Bridge Cmd Install
6	Intro to PLCs	Exam 1
7	Intro to Ladder Logic	CCW Instal, LL 1
8	Adv. Ladder Logic	More LL
9	ICS Protocols (part 1)	Modbus RS-232
10	ICS Protocols (part 2)	Modbus RS-485/TCP
11	Attacking ICS (part 1)	Attacking ICS
12	Attacking ICS (part 2)	Exam #2
13	YP703 Systems Overview	YP Field Trip
14	YP Project Intro	HILICS Install
15	YP Project work	YP Status Update
16	YP Project Work	Project Demo

Marine Systems Lectures - Propulsion

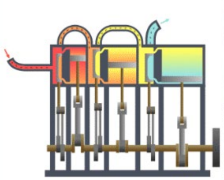
- Propulsion Types
  - Manual
  - Sails
  - Paddlewheel
  - Pump-Jet
  - Propellers
- Power Generation
  - Steam
  - Diesel
  - Gas Turbine
  - LNG
  - Fuel Cell
- Typical Ship Configurations

Paddlewheel / Caterpillar

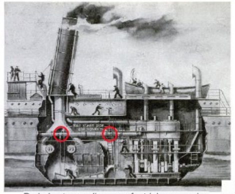
The paddle wheel is a large steel framework wheel. The outer edge of the wheel is fitted with numerous, regularly spaced paddle blades (called floats or buckets). The bottom quarter or so of the wheel travels under water. Cat != MHD

Early Steam Engines

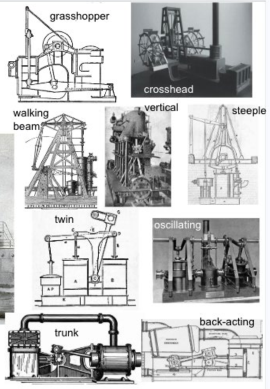
Early marine steam engines came about around 1800 and started with reciprocating pistons and were classified by how the piston(s) moved.



A compound engine is a steam engine that operates cylinders through more than one stage, at different pressure levels. Compound engines were a method of improving efficiency.

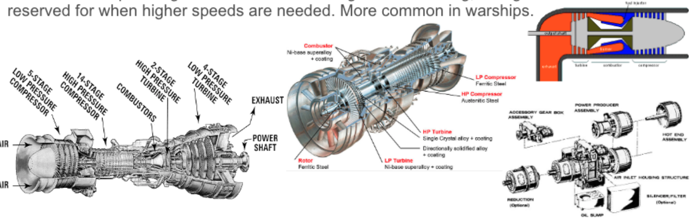


Period cutaway diagram of a triple-expansion steam engine installation, circa 1918. This particular diagram illustrates possible engine cutoff locations, after the Lusitania disaster and others made it clear that this was an important safety feature

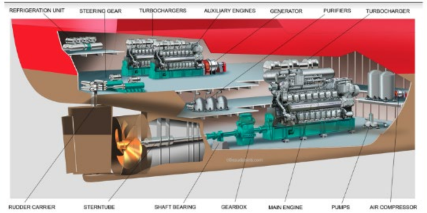


Gas Turbine

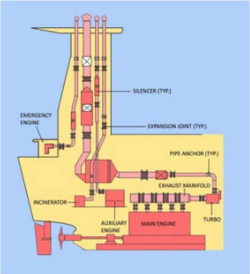
The gas turbine is most familiar to people in it's application to the aerospace industry. Low weight to power ratio, compactness, and a reliable simple design are the major advantages. Because of their poor thermal efficiency at low power (cruising) output, it is common for ships using them to have diesel engines for cruising, with gas turbines reserved for when higher speeds are needed. More common in warships.



Cutaway of a Typical Ship Engine Room



https://www.behance.net/gallery/31936141/EXXONMOBIL-FPSO-Vessel



https://www.marineinsight.com/main-engine/exhaust-gas-system-of-main-engine-on-ship/

Marine Systems Lectures - Electrical

- Components
  - Generators
  - Switchboards
  - Bus Bars
  - Circuit Breakers
  - Transformers
  - Others
    - Switches
    - Fuses
    - Instrument
    - Motors, etc.
- Three-Phase Power
- Electrical Safety
- Inside Switch Boards
- Distribution

Generators

Shipboard power is generated using a prime mover and an alternator working together. International maritime regulations (e.g. SOLAS), require at least two generators for a ship's main electrical power system. AC power is preferred over DC as it gives more power for the same size. Three phases is preferred over single phase as provides more overall power and in the event of failure of one phase, other 2 can still work.

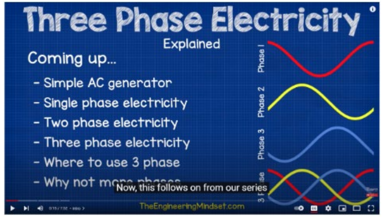


Busbars (or Bus Bars)

In electric power distribution, a busbar is a metallic strip or bar, typically housed inside switchgear, panel boards, and busway enclosures for local high current power distribution.They are generally uninsulated, and have sufficient stiffness to be supported in air by insulated pillars. These features allow sufficient cooling of the conductors, and the ability to tap in at various points without creating a new joint.

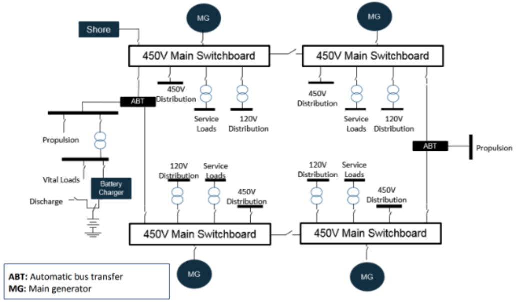


https://www.youtube.com/watch?v=MnH_ifcRJq4



https://www.youtube.com/watch?v=4oRT7PoXSS0

Electrical Distribution - Example 2

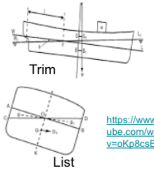


Marine Systems Lectures - Auxiliary (Water Systems)

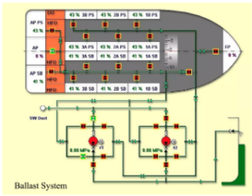
- Ballast
- Cooling
- Fire Mains
- Potable Water
  - Evaporator
  - Reverse Osmosis
- Wastewater
  - Greywater
  - Blackwater

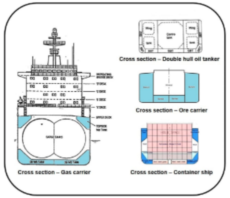
Ballast

Ballast is used in ships to provide moment to resist the lateral forces on the hull. Insufficiently ballasted boats tend to tip or heel excessively in high winds. Too much heel may result in the vessel capsizing. If a sailing vessel needs to voyage without cargo, then ballast of little or no value will be loaded to keep the vessel upright. Some or all of this ballast will then be discarded when cargo is loaded. The advantage of water ballast is that the tanks can be emptied, reducing draft or the weight of the boat (e.g. for transport on ground) and water added back in (in small boats, simply by opening up the valves and letting the water flow in) after the boat is launched or cargo unloaded.



https://www.youtube.com/watch?v=oKp8csBhMgg

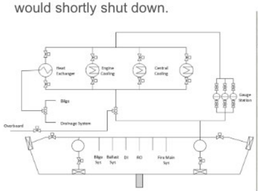


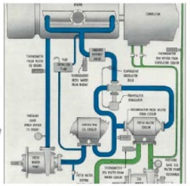


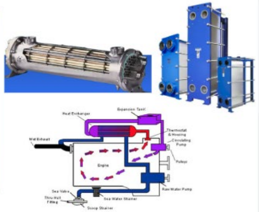
Cooling

https://www.youtube.com/watch?v=ii11V201oFI

The main and auxiliary seawater cooling systems pull water off the vessel through hull valves to provide cooling water to heat exchangers. These valves are located sufficiently below the water line to prevent vapor locking the pumps.Key components to the main and auxiliary seawater systems are the main feed pumps, inductors, strainers, electro-hydraulic through hull valves, expansion tanks, piping, heat exchangers, and any subsystems used to prevent internal pipe biological growth. Without main and auxiliary seawater cooling systems such as propulsion, power generation, and compressed air, a vessel would shortly shut down.



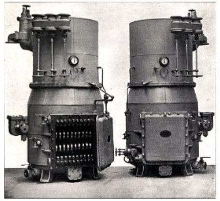


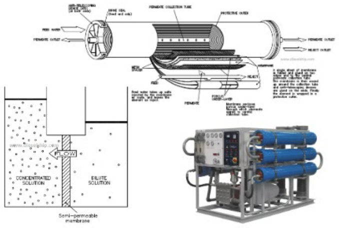


Potable Water

https://www.youtube.com/watch?v=8k56ffiNJ8M

Freshwater may be obtained from shore mains supply or water barge. Alternatively, the majority of ships employ an evaporator system that uses distillation, or a pressurised filtering system which uses reverse osmosis to convert seawater into potable water.



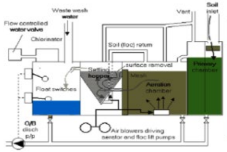


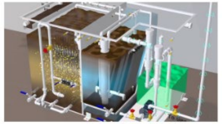
Wastewater

https://www.youtube.com/watch?v=5Z7bTmZVPTI

Greywater refers to wastewater generated from streams without fecal contamination, i.e., all streams except for the wastewater from toilets.

Blackwater in a sanitation context denotes wastewater from toilets which likely contains pathogens that may spread by the fecal-oral route. Blackwater can contain feces, urine, water and toilet paper from flush toilets.

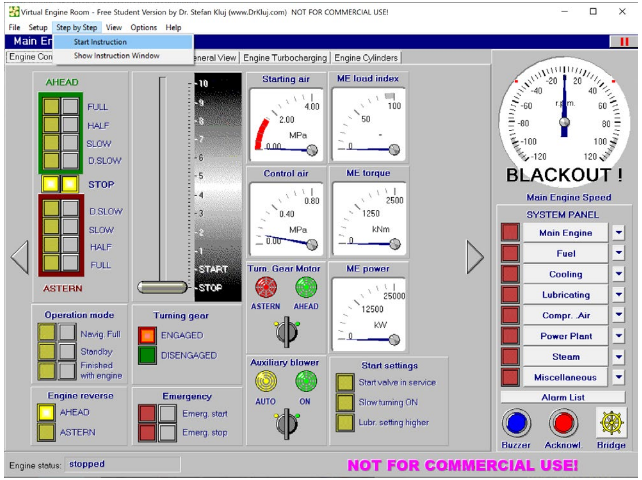


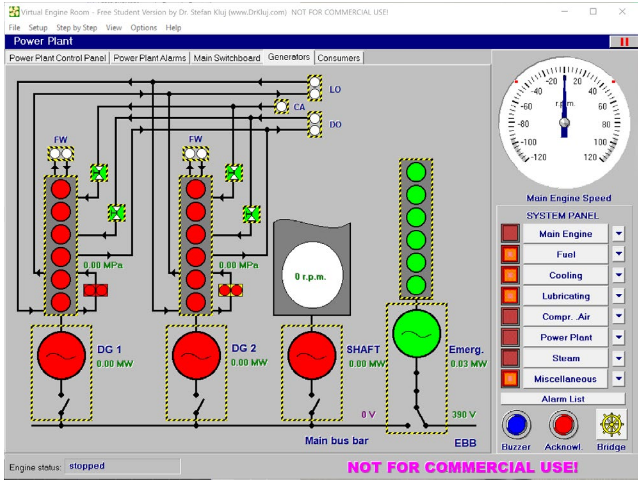


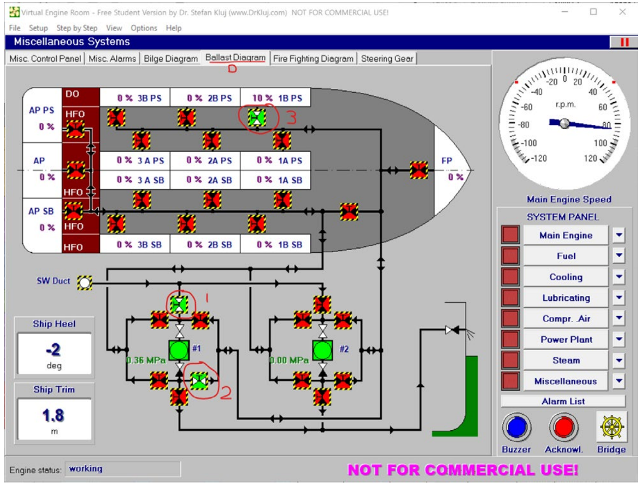
Virtual Engine Room Labs (#1-3)

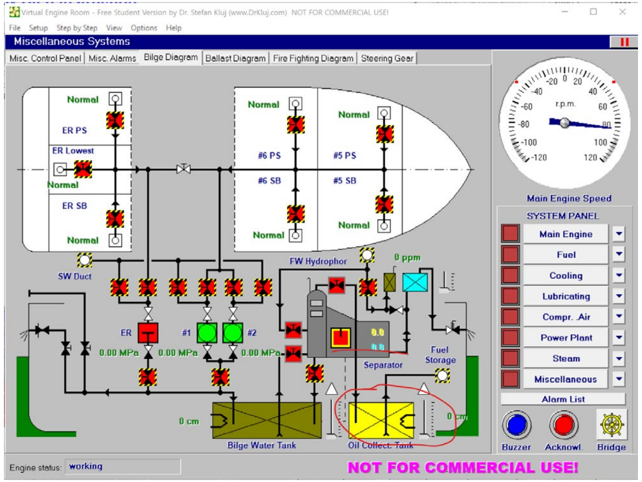
https://drkluj.com/simulators/free-student-version/

- SW Install
- Engine Startup
  - Checklists
  - Bunkering
  - Main Engine
- Electrical
  - Start/Stop
  - Failover
  - Synchronization
- Auxiliaries
  - Ballast
  - Fire Fighting
  - Bilge
  - Cooling









Marine Systems Lectures - Bridge Systems

- Definitions
- Manning
- Components
    - ECDIS
    - AIS
    - Radar
    - Communications
    - Other Systems
- Automation

Manning

https://www.youtube.com/watch?v=xumcG8FvH7k

There is a stark difference between the number of personnel required on civilian and military bridge watch crews. Changes have reduced USN footprint in recent years.

Seven Rotation (dog evening) (a)	Watchstander Standard 1 in 3 Watch System Day 1	Day 2	Day 3	Day Workers
0000-0400	A	B	C	
0400-0800	B	C	A	0.5
0800-1200	C	A	B	3
1200-1600	A	B	C	3
1600-1800	B	C	A	1
1800-2000	C	A	B	1.5
2000-2400	A	B	C	
Work	15.5	10	12	9
Free Time (b)	8.5	14	12	15
Uninterupted Period	2.5	6.5	4	8

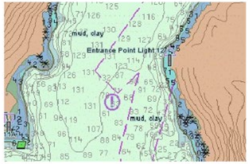
Table 11. MSC vs. U.S. Navy bridge watchstanders

	MSC method	AS-39 (USN old method)	FFG (USN new method)	DDG-51[a] (USN new method)	CG-52[b] (USN new method)
Bridge Watch	Mate	OOD JOOD QMOW BMOW	OOD JOOD Bridge Spec.	OOD JOOD Bridge Spec.	OOD JOOD Bridge Spec.
	Helmsman	Helmsman EOT(JV Talker)	Control Console	Control Console	Control Console
	Utilityman	Messenger JL Talker	JL Talker		
		Lookout Stbd Lookout Port			
	Lookout Fwd	Lookout Aft	Lookout Aft	Lookout Aft	Lookout Aft
Signal Bridge		Supervisor Recorder			

a. Type I, Type II, and Type IIA.
b. Smart Ship and Non-Smart Ship.

ECDIS

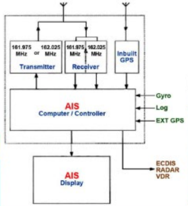
An Electronic Chart Display and Information System (ECDIS) is a geographic information system used for nautical navigation that complies with International Maritime Organization (IMO) regulations V/19 & V/27 of SOLAS convention as amended, by displaying selected information from a System Electronic Navigational Chart (SENC).

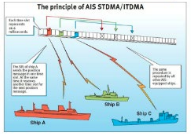


AIS

https://youtu.be/mRtBr-2Oqz0?t=30

The Automatic Identification System (AIS) is an automatic tracking system that uses transceivers on ships and is used by vessel traffic services (VTS). Information provided by AIS equipment, such as unique identification, position, course, and speed, is intended to assist a vessel's watchstanding officers and allow maritime authorities to track and monitor vessel movements.



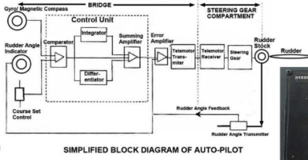


Automatic Steering

https://www.youtube.com/watch?v=3T-wFfPm37U

Innovation for hands-free steering for sailing vessels initially came from model ship competitions and was used during solo Transatlantic journeys in the 1930s.

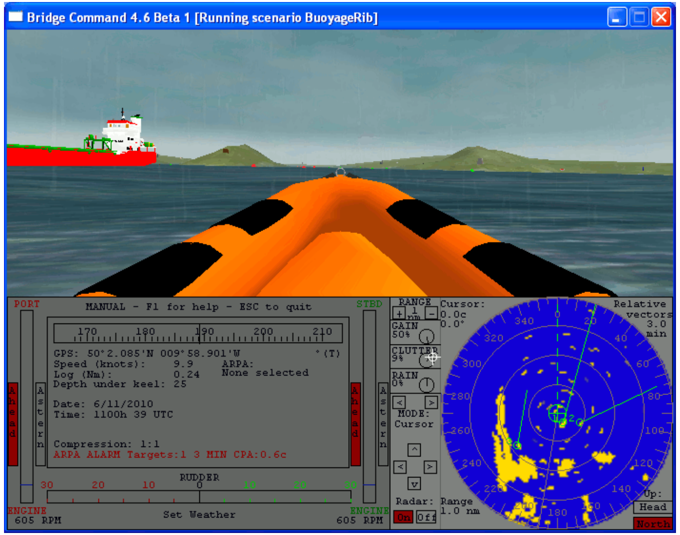
Modern autopilot systems use electronic gyro inputs and have several modes of operation and follow a course entered in the integrated ECDIS system.

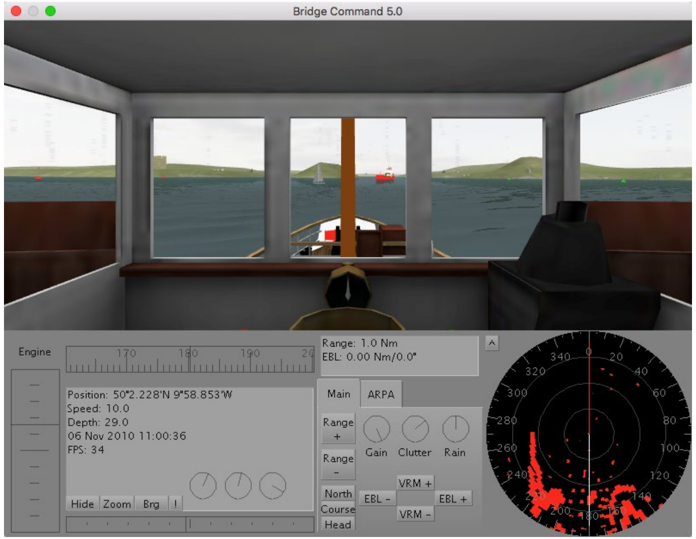


Bridge Command Lab (#4)

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

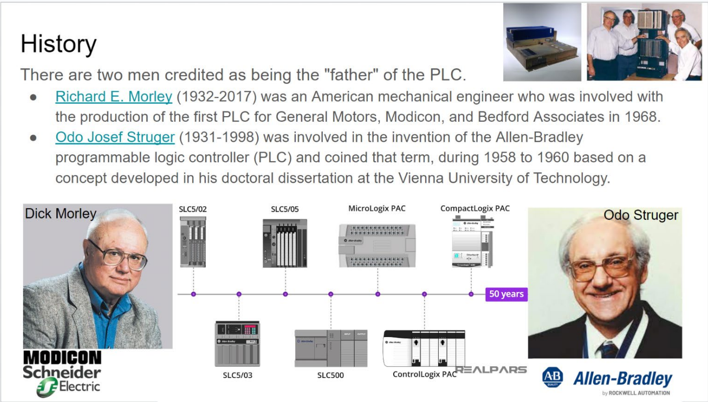
- SW Install
- Bouyage
  - RHIB
  - Basic Controls
- Leaving Harbor
  - Lifeboat
  - Radar
  - Man Overboard

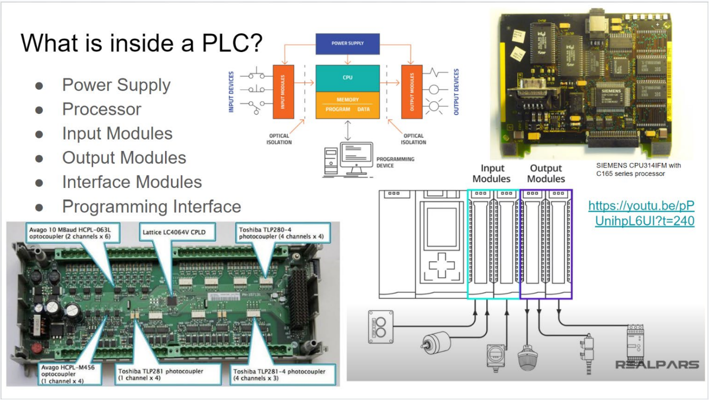


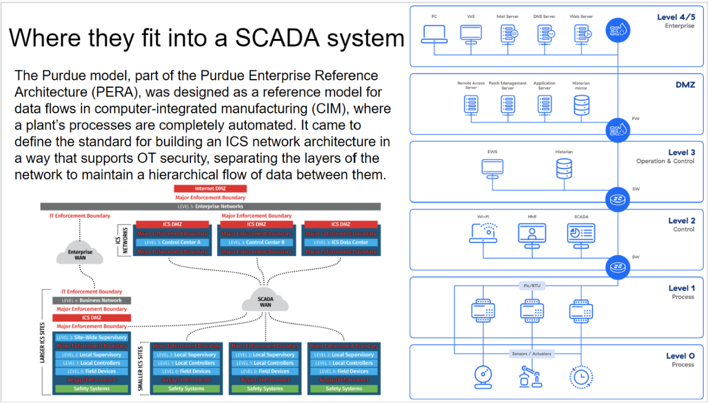


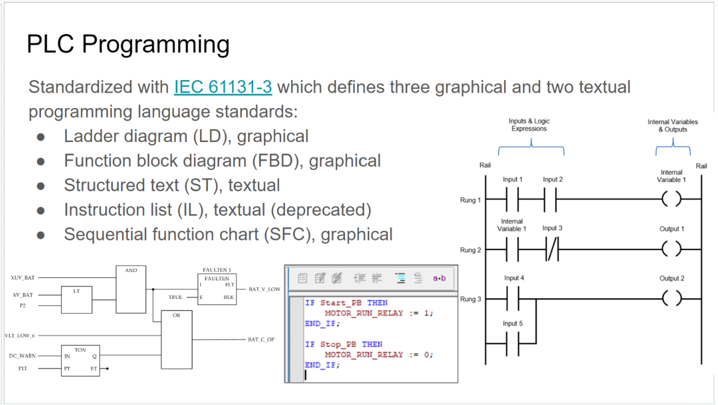
PLC Lectures - Introduction to PLCs

- Overview
- History
- Components
- Applications
- SCADA
- Organization
- Programming







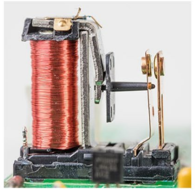


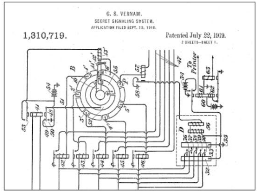
PLC Lectures - Ladder Logic

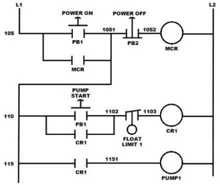
- History
- Conventions
  - L to R, top to bot.
- Symbols
  - Contacts
  - Coils
- Function Blocks
  - Modbus Message
  - Timer
  - Num. Conversion
  - User Defined
- Examples

Where does LL come from?

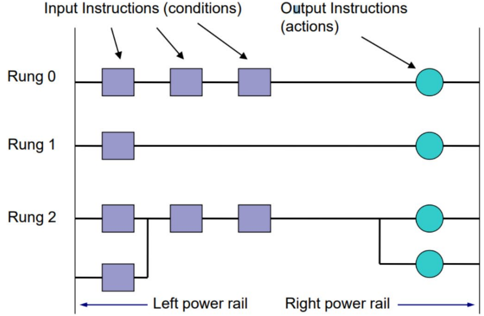
Ladder logic was originally a written method to document the design and construction of relay racks as used in manufacturing and process control.[1] Each device in the relay rack would be represented by a symbol on the ladder diagram with connections between those devices shown. In addition, other items external to the relay rack such as pumps, heaters, and so forth would also be shown on the ladder diagram.



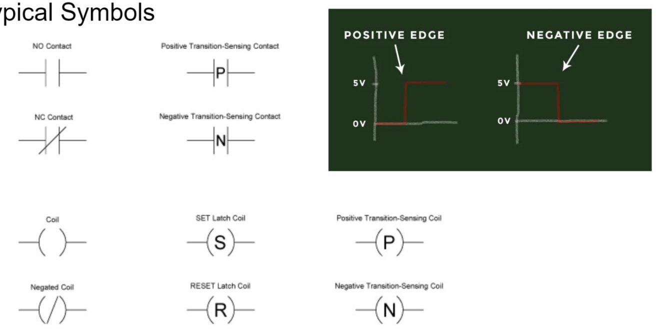




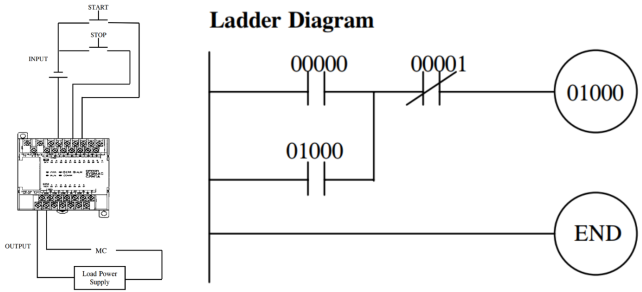
Anatomy of a Ladder Program



Typical Symbols



Latch / Self Holding Circuit

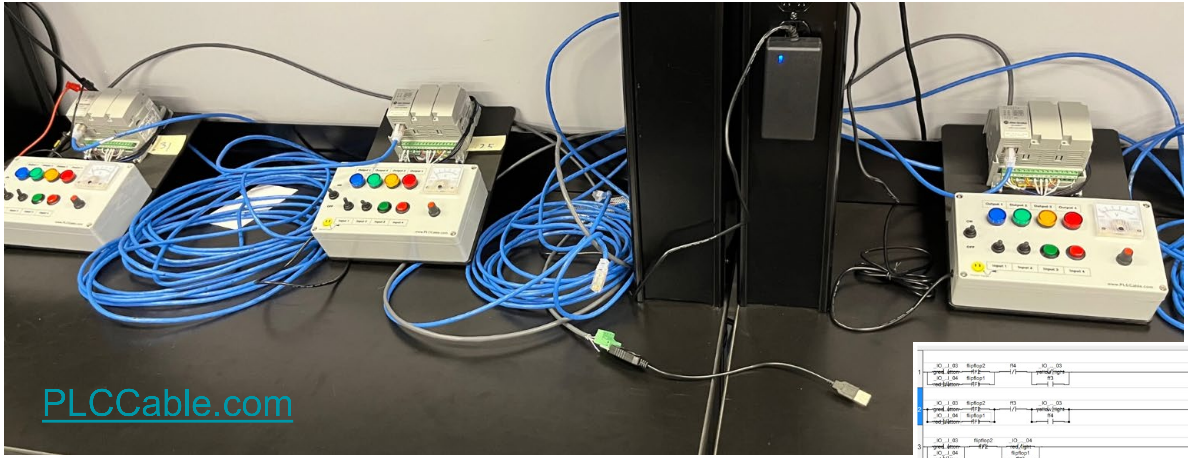


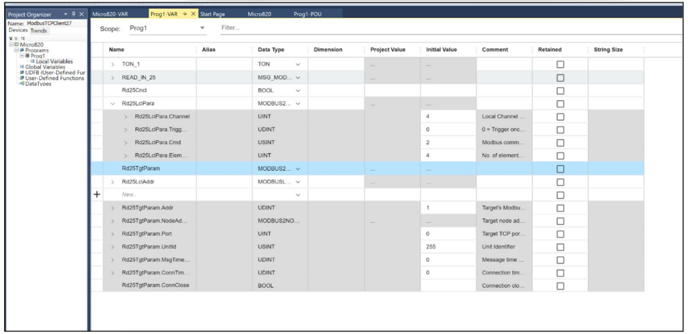
PLC Labs (#7-11)

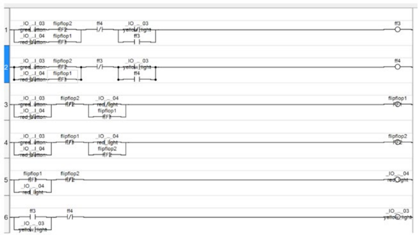
Rockwell Automation

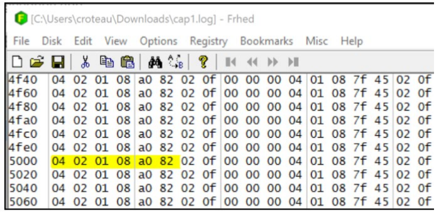
Connected Components Workbench™ Software

- Allen-Bradley (AB) micro820 PLC based
- Individual Ladder Logic Programming
- Modbus Communication (RS-232, RS-485, and TCP)









PLC Lectures - PLC Communication

- Modbus History
- Intro
- Object Types
- Protocols
- Message Format
  - Function Codes
  - Data Format
  - CRC
- Physical Medium
- Others
  - CIP
  - EtherNet/IP
  - DNP3
  - HART
  - BACNet
  - OPC
  - Profinet

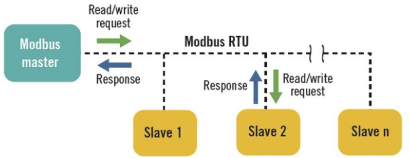
Philosophy of Modbus

Every message in Modbus deals with reading or writing one of only these four object types:

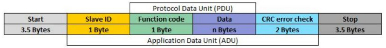
- Coils
- Discrete Inputs
- Input Registers
- Holding Registers

Single "Controller" that makes requests to "Peripheral" device responses.

Object type	Access	Size	Address Space
Coil	Read-write	1 bit	00001 – 09999
Discrete input	Read-only	1 bit	10001 – 19999
Input register	Read-only	16 bits	30001 – 39999
Holding register	Read-write	16 bits	40001 – 49999

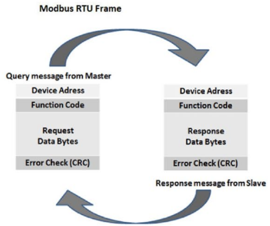


Mb RTU Message Format



1. There are 3.5 Bytes of of quiet before or after a message is sent
2. An ID of the slave device is next (1 byte)
3. Then a Function Code (1 byte)
4. Then a variable amount of Data
5. Lastly, a CRC error check (2 bytes)

PDU = FC + Data
ADU = Entire message



Function Codes

Each message sent from the Master will use one and only one of these codes to either read or manipulate a particular value in the Slave's memory tables.

If the slave needs to send back an error code, they will change the first (MSB) of the FC to "1" during the reply.

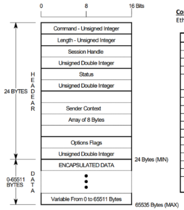
Function Code	Action	Table Name
01 (01 hex)	Read	Discrete Output Coils
05 (05 hex)	Write single	Discrete Output Coil
15 (0F hex)	Write multiple	Discrete Output Coils
02 (02 hex)	Read	Discrete Input Contacts
04 (04 hex)	Read	Analog Input Registers
03 (03 hex)	Read	Analog Output Holding Registers
06 (06 hex)	Write single	Analog Output Holding Register
16 (10 hex)	Write multiple	Analog Output Holding Registers

https://www.youtube.com/watch?v=JBGaInI-TG4

EtherNet/IP (IP = Industrial Protocol)

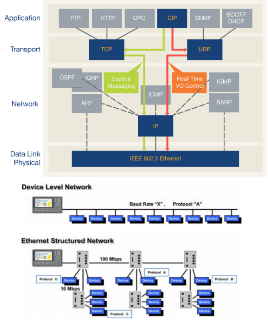
An industrial network protocol that adapts the Common Industrial Protocol (CIP) to standard Ethernet.

ENCAPSULATION PACKET



Command (2 Bytes) – This is the encapsulation command code (refer to the EtherNet/IP Specification for detailed information on commands):

CODE (HEX)	DESCRIPTION
0000H	NOP (No operation) – Sent only via TCP.
0001..0003H	*Reserved for legacy*
0004H	List_Services - May be sent via TCP or UDP
0005H	*Reserved for legacy*
0006..0062H	*Reserved for future expansion – compliant products may not use command codes in this range.*
0063H	List_Identity – May be sent via TCP or UDP.
0064H	List_Interfaces (optional) - May be sent via TCP or UDP.
0065H	Register_Session – Sent only via TCP.
0066H	UnRegister_Session – Sent only via TCP.
0067..006EH	*Reserved for legacy*
006FH	SendRRData – Sent only via TCP.
0070H	SendUnitData – Sent only via TCP.
0071H	*Reserved for legacy*
0072H	Indicate_Status (optional) – Sent only via TCP.
0073H	Cancel (optional) – Sent only via TCP.
0074..00C7H	*Reserved for legacy*
00C8..FFFFH	*Reserved for future expansion – compliant products may not use command codes in this range.*



PLC Lectures - Attacking and Defending PLC Networks

Industrial Control System Cyber Attacks

Thomas H. Morris[1], Wei Gao
Mississippi State University
Mississippi State, MS, USA
[1]*morris@ece.msstate.edu*

This paper presents a set of attacks against SCADA control systems. The attacks are grouped into 4 classes; reconnaissance, response and measurement injection, command injection and denial of service. The 4 classes are defined and each attack is described in detail. The response and measurement injection and command injection classes are subdivided into sub-classes based on attack complexity. Each attack described in this paper has been exercised against industrial control systems in a laboratory setting.

Industrial Control System. Threat Model. Taxonomy.

1. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are computer-based industrial control

functional SCADA control systems which model a gas pipeline and a water storage tank using commercial control system hardware and software.

https://www.scienceopen.com/hosted-document?doi=10.14236/ewic/ICSCSR2013.3

Table 1: *List of Attacks against MODBUS Industrial Control Systems*

Attack Index	Name	Classification
1	*Address Scan*	*Reconnaissance*
2	*Function Code Scan*	*Reconnaissance*
3	*Device Identification*	*Reconnaissance*
4	*Naïve Read Payload Injection*	*NMRI*
5	*Invalid Read Payload Size*	*NMRI*
6	*Naïve False Error Response*	*NMRI*
7	*Sporadic Sensor Measurement Injection Attack*	*NMRI*
8	*Slope Sensor Measurement Injection*	*CMRI*
9	*High Slope Measurement Injection*	*CMRI*
10	*High Frequency Measurement Injection*	*CMRI*
11	*Altered System Control Scheme*	*MSCI*
12	*Altered Actuator State*	*MSCI*
13	*Altered Control Set Point*	*MPCI*
14	*Force Listen Only Mode*	*MFCI*
15	*Restart Communication*	*MFCI*
16	*Invalid Cyclic Redundancy Code (CRC)*	*DOS*
17	*MODBUS Slave Traffic Jamming*	*DOS*

Exams

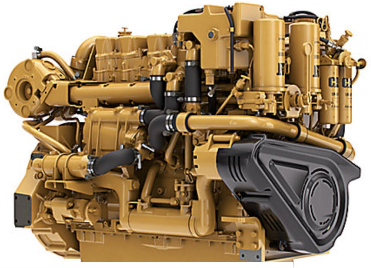
Three exams, primarily short answer having the students recall material introduced in lectures.   Example Questions:

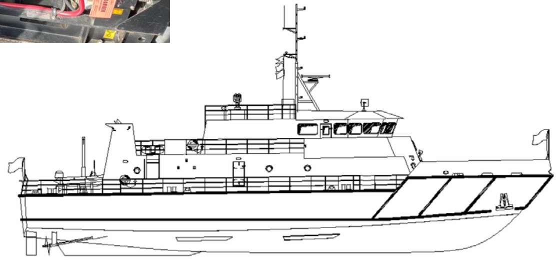
1. What are some reasons why a ballast system is required on a ship?
2. What is an ECDIS and what is it used for on a ship?
3. Describe how the HART protocol can encode both digital and analog data on the same legacy wire.
4. Decode the following Modbus message and describe in plain english what it means: 0x13 0x06 0x00 0x04 0x00 0x06 0x4B 0x7B
5. Think about two different attacks that a knowledgeable cyber attacker could launch on a typical ship. Describe the method of ingress, systems affected, and consequences to the vessel.

Final Project

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)



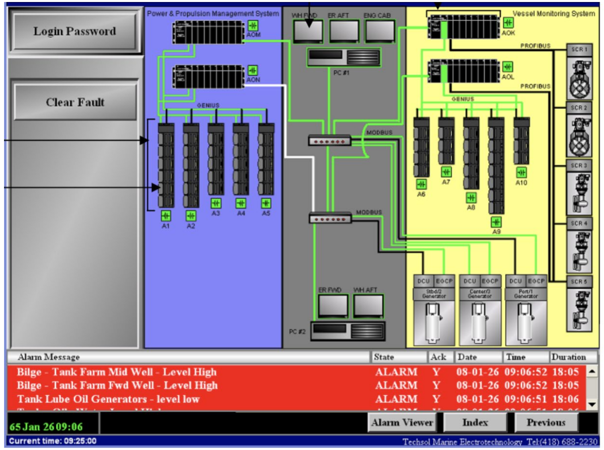


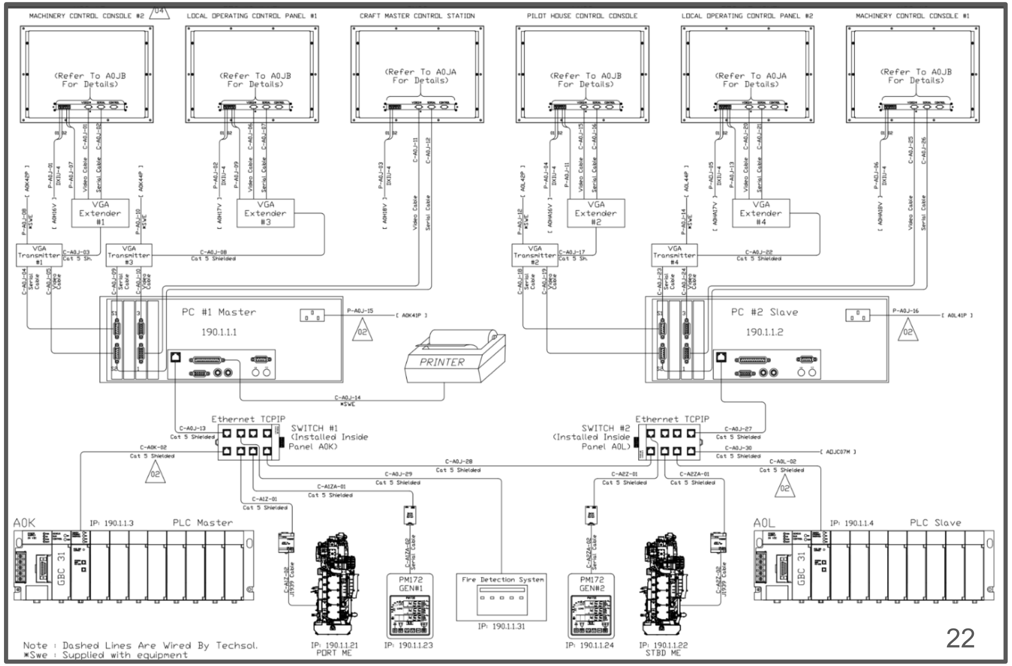
Used for local ship-handling training operations and summer cruises on the eastern seaboard

MAX II Alarms and Monitoring System on the YP703 class

GE Fanuc based custom install

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





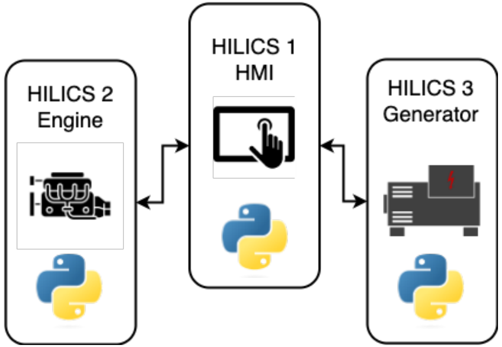
Project Results

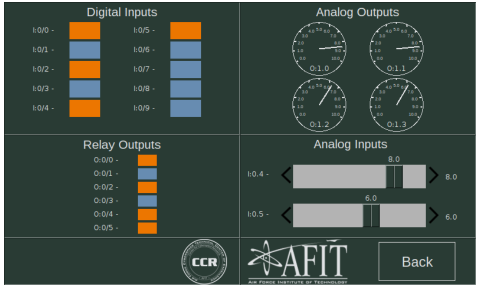
https://github.com/sdunlap-afit/hilics

Students successfully connected three PLC kits together to replicate a portion of the YP alarms system.

Modified the HILICS IO_Test program to share discrete and analog values and trigger alarms.

Produced a 9-page Interface Control Document (ICD) that recorded the message format and context for the information displayed and the displays.





2. Interface Description

2.1 System Overview

This system is meant to simulate a Yard Patrol Craft alarm apparatus and messaging system between a Control Panel, Engine, and a Generator. The system is made up of three separate PLCs and, via ladder logic, is coded on the RSLogix program. The simulated Generator and Engine are very similar in functionality; each have two analog inputs and three discrete inputs

Conclusion

An overview of the new Maritime ICS Course taught at USNA.

I look forward to hearing your **questions** and and suggestions you might have about ideas for future offerings.

Brien Croteau, USNA, croteau@usna.edu

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

Backup Slides

UNITED STATES NAVAL ACADEMY
Annapolis

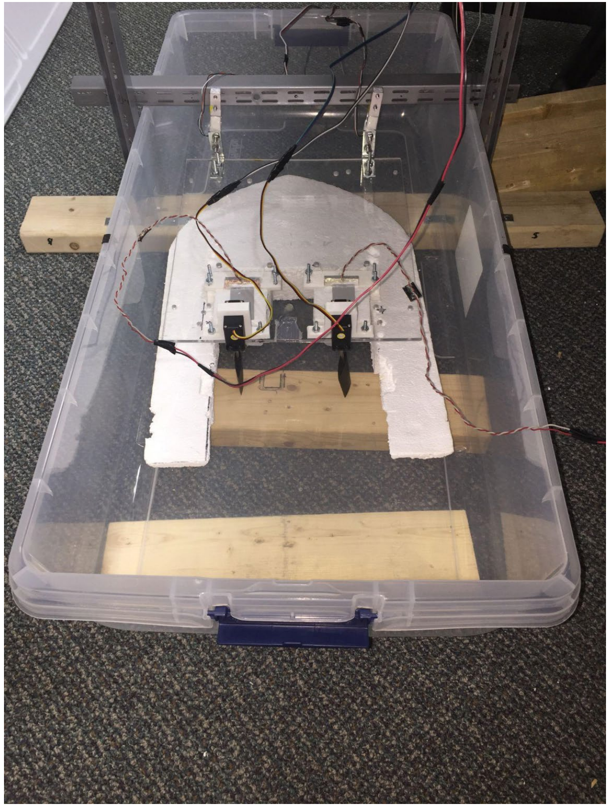
Lessons Learned when building a Maritime Systems Security Laboratory Testbench

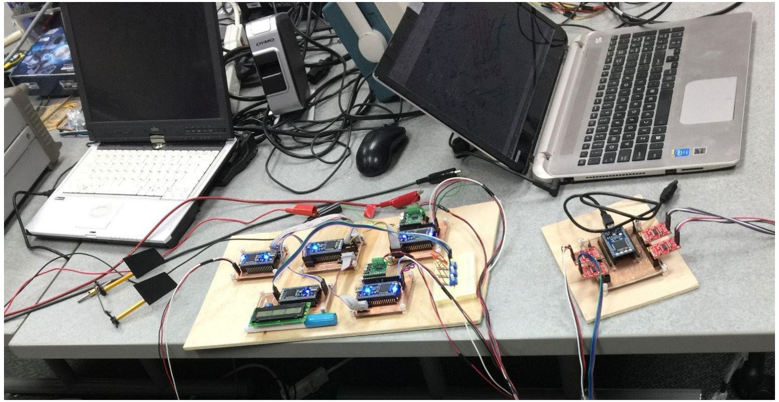
Brien Croteau, USNA, Cyber Science

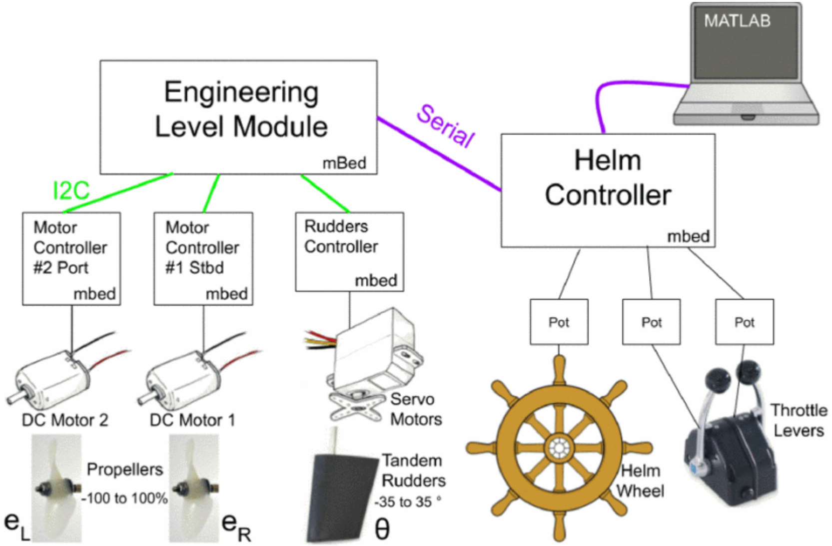
DefCon 31- ICS Village, 12 Aug 2023

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

v0.1 UMBC Ship System Testbed





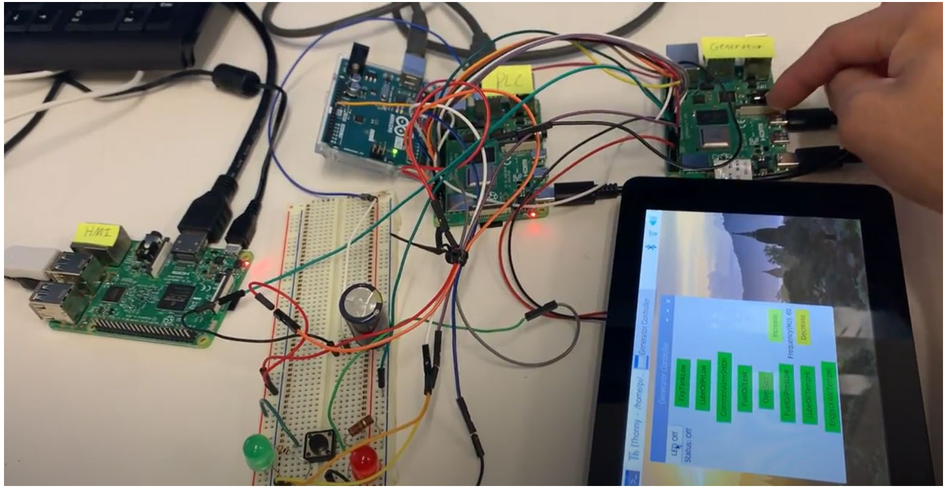


2019 R Week Paper

[Alternative Actuation Paths for Ship Applications in the Presence of Cyber-Attacks]

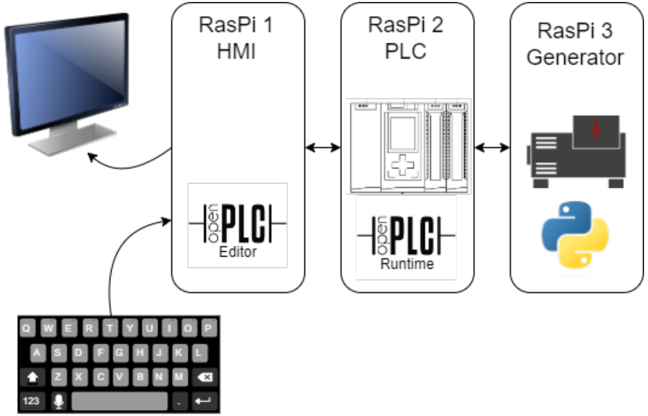
5 min demo video

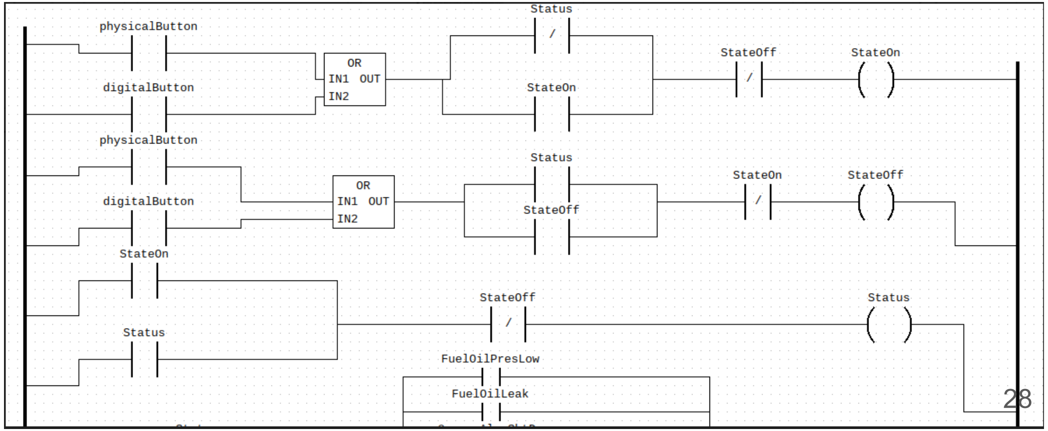
v1.0 Proof of Concept



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

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



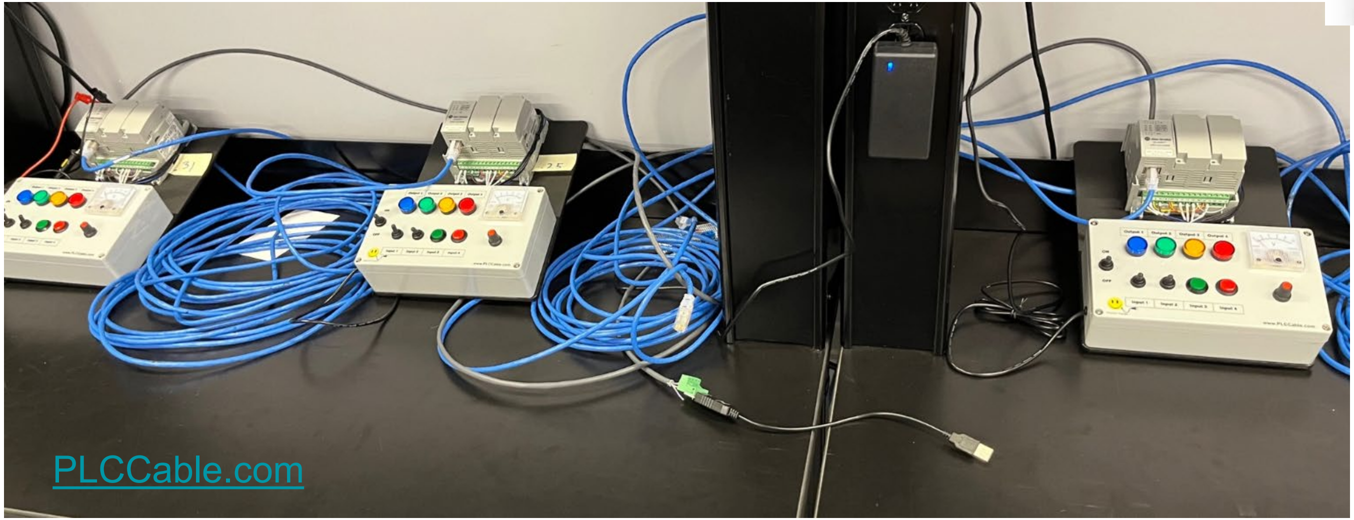


v2.0 Classroom Trainers

Allen-Bradley (AB) micro820 PLC based

Individual Ladder Logic Programming

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



PLCCable.com

Rockwell Automation

Connected Components Workbench™ Software

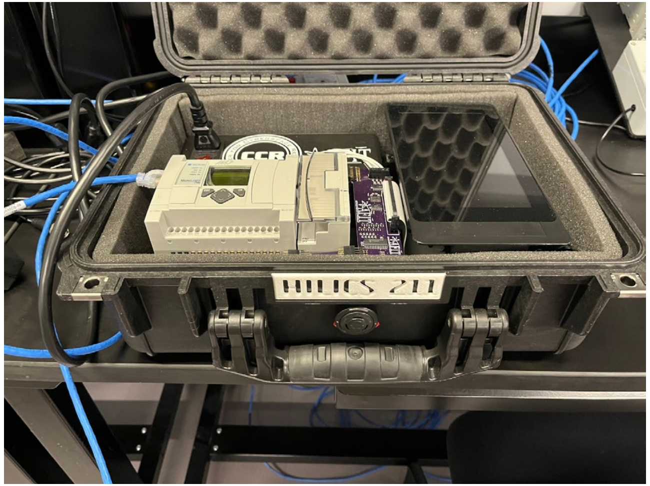
v2.5 Hardware-in-the-Loop ICS (HILICS)

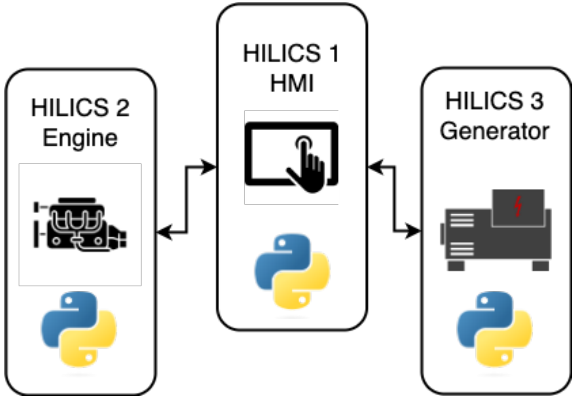
On loan from Air Force Institute of Technology (AFIT)
AB microLogix 1100+RasPi
Students made a 3-node network replicating a portion of the YP703 system:

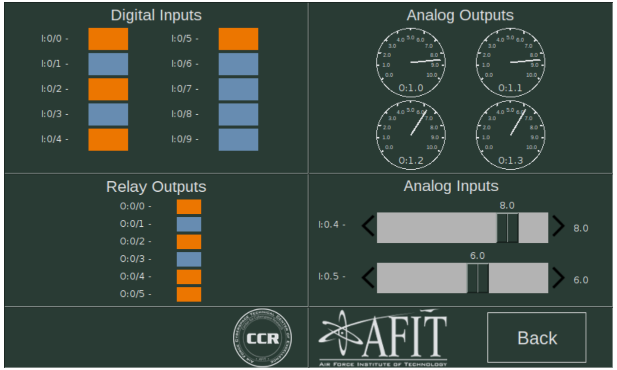
- 1x HMI
- 1x Diesel Engine
- 1x Generator

Captured their work in an Interface Control Document

https://github.com/sdunlap-afit/hilics







Other Maritime Testbenches


https://www.kongsberg.com/

https://www.fathom5.co/systems