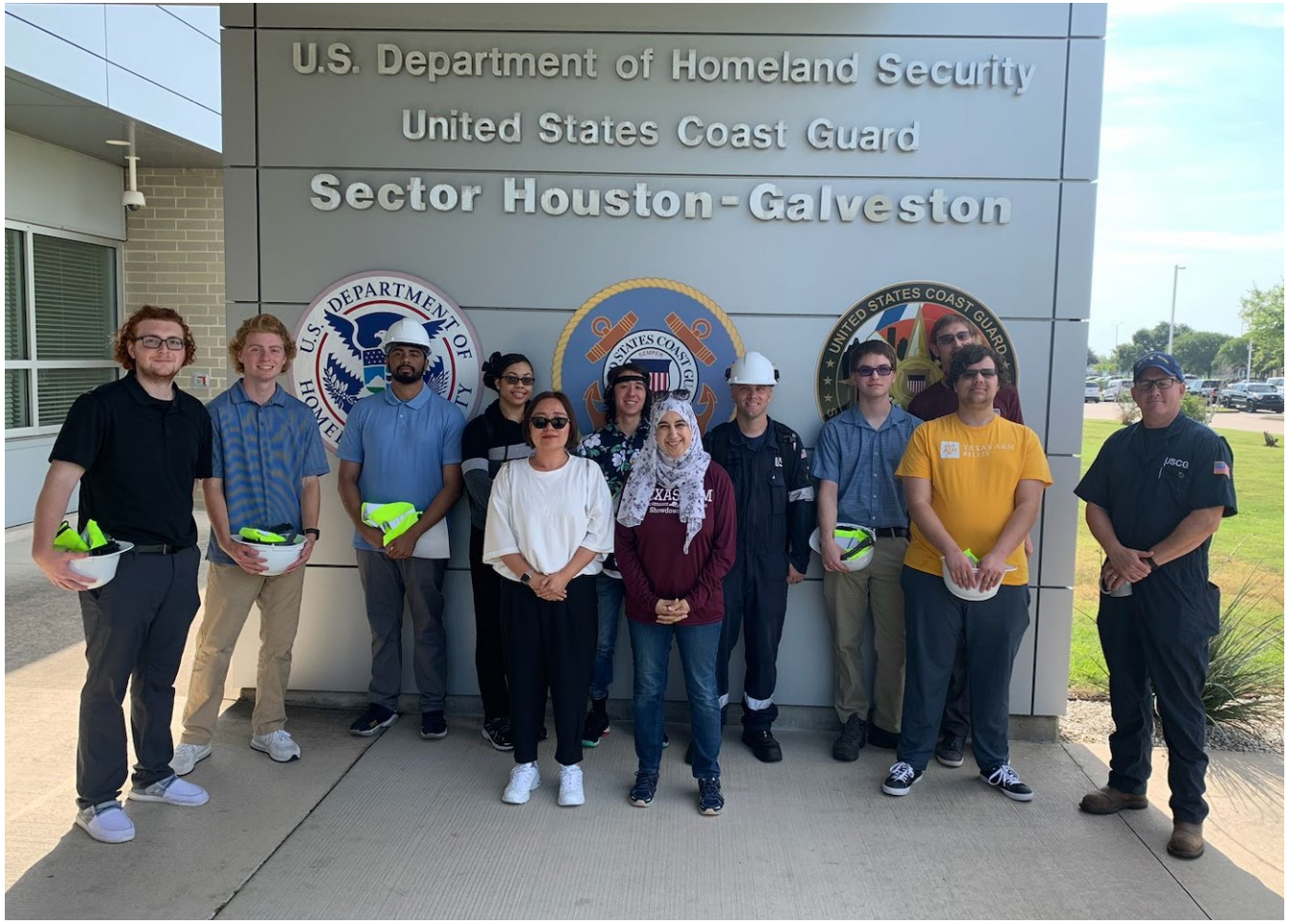
CROSS-BORDER THREAT SCREENING AND SUPPLY CHAIN DEFENSE

DEPARTMENT OF HOMELAND SECURITY
SCIENCE AND TECHNOLOGY CENTER OF EXCELLENCE

SUMMER RESEARCH INSTITUTE

JULY 24, 2023

CBTS Summer Research Institute
Final Student Fellow Presentations



CROSS-BORDER THREAT SCREENING
Center of Excellence

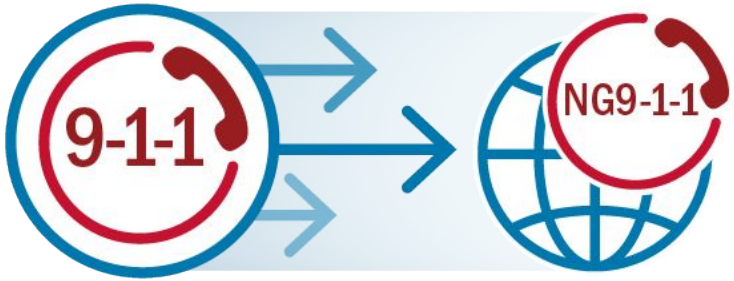
Presentations:

- Next Generation 911 Cybersecurity Threat Modeling and Risk Analysis

- Towards Zero-Trust: A Systems Engineering Approach for Vital Ship Systems' Cybersecurity Risk Assessments

CBTS CyberSecurity Summer Research Institute

Next Generation 911 Cybersecurity Threat Modeling & Risk Assessment



TAMU Commerce Faculty Mentors

CROSS-BORDER THREAT SCREENING
Center of Excellence

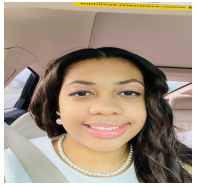
Dr. Eman Hammad

- Assistant Professor, Computer Science & Information Systems
- Office: ACB2-208
- Email: Eman.Hammad@tamuc.edu
- Location: RELLIS Campus, Bryan, TX

Dr. Yuehua Wang

- Associate Professor, Computer Science & Information Systems
- Office: Jour 230
- Email: Yuehua.Wang@tamuc.edu
- Location: Jour 101/102, Commerce, TX

William Hatcher
3rd year, Computer Information Systems
TAMUC-RELLIS
whatcher@leomail.tamuc.edu



Reine Watkins
2nd year, Computer Information Systems
TAMUC-Commerce
rwatkins7@leomail.tamuc.edu

Tag Kalat
3rd year, Cybersecurity
TAMUC-RELLIS
tkalat@leomail.tamuc.edu

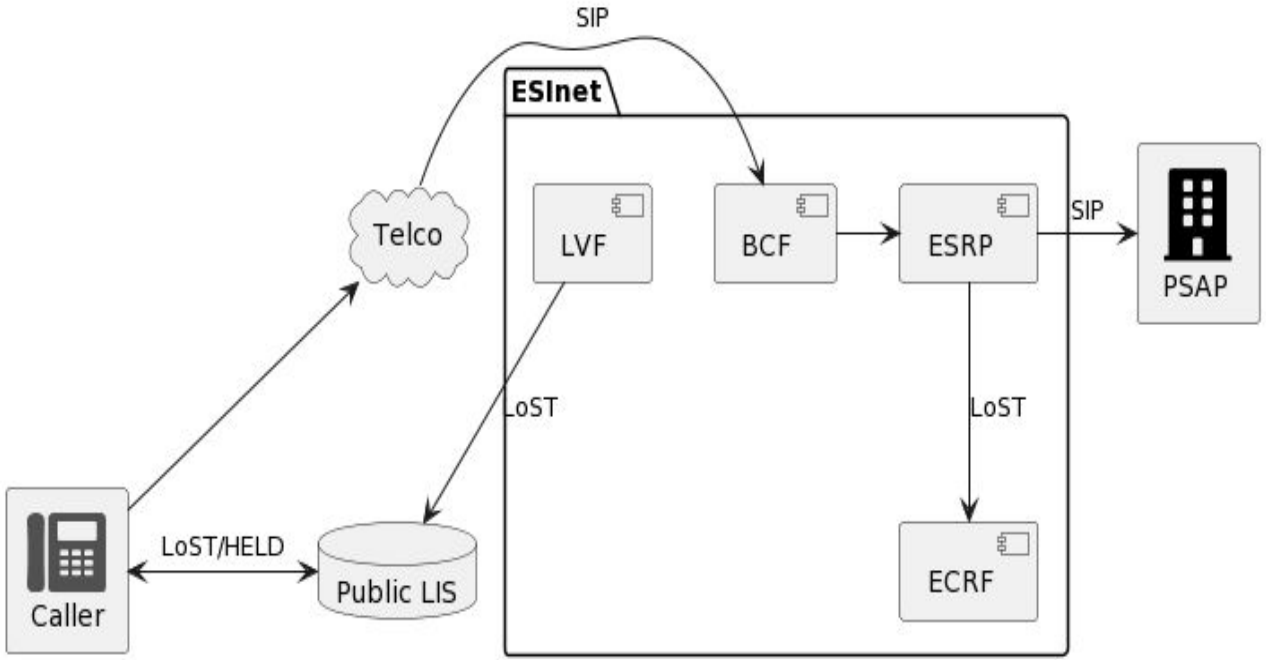
Colten Van Voorhis
3rd year, Computer Science
TAMUC-Commerce
cvanvoorhis@leomail.tamuc.edu

Overview of NG911

What is Next Generation 911 (NG911)?

- Allows for call, text, and video communication with emergency services
- Facilitates data sharing between Public Safety Answering Points (PSAPs)
- Improves acquisition of call location information
- Enables more efficient transfer of calls between geographical regions
- Improves upon existing 911 architecture to implement security safeguard and redundancy components

NENA I3 Architecture



PSAP: Public Safety Answering Point that serves as a call center.

ESInet: private network for emergency services

LVF: Location Verification Function

BCF: Border Control Function

ESRP: Emergency Service Routing Proxy

LoST: Location to Service Translation

HELD: HTTP Enabled Location Delivery.

LIS: Location Information Server

ECRF: Emergency Call Routing Function

SIP: Session Initiation Protocol - Used for calls

Improved Location Services

- **LoST** (Location to Service Translation) - transmit location information, used to map location information to one or more Uniform Resource Identifiers

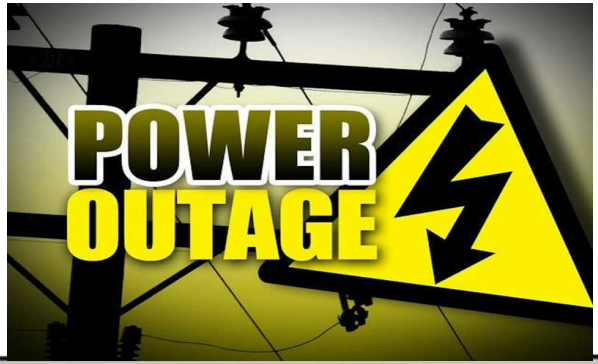
- **HELD** (HTTP-Enabled Location-Delivery) - used to acquire location information from a Location Information Server (LIS) within an access network.

Cybersecurity and Public Safety Examples

- In Dec 2018, there were significant phone and broadband service interruptions as a result of the outage, including 911 calls.
  - Lasted almost 37 hours.
  - Up to 22 million customers in 39 states were impacted, with about 17 million of those lacking dependable access to 911 in 29 states. At least 886 911 calls could not be answered
- In 2020, the law enforcement agencies in Arizona, Colorado, North Carolina, North and South Dakota, Minnesota and Utah were affected for **two hours** due to outages.

The 911 service was disrupted.

Source: https://www.apu.apus.edu/area-of-study/security-and-global-studies/resources/most-law-enforcement-agencies-are-not-prepared-for-long-term-power-outages/



Source: https://twitter.com/LongviewISD/status/1317093439641706496

Cybersecurity Threat Modeling and Risk Assessment

- **Threat Model** - A structured representation of all relevant information that could directly impact the security of a system including vulnerabilities or lack of safeguards.

- **Risk Assessment** - The process of identifying potential hazards to a system and analyzing what would happen in the event of an incident.

Emerging Technologies

- Artificial Intelligence (AI) - used to facilitate the creation of false packets on a larger scale than what's currently possible enabling an increase in DoS attacks
- 5G/6G - improves network speeds allowing for supply chain threats presented by Man-in-the-Middle attacks

Research Question

How can automated risk assessment suite/tool be developed and tested to identify and describe cyber risks associated with NG911 system architecture?

Such a suite/tool should be

- Compliant: generalized to adhere to NENA i3 standard
- Adaptive: work with different technologies
- Specific: capable of considering the NG911 threat model and emerging threat landscape

Project Approach

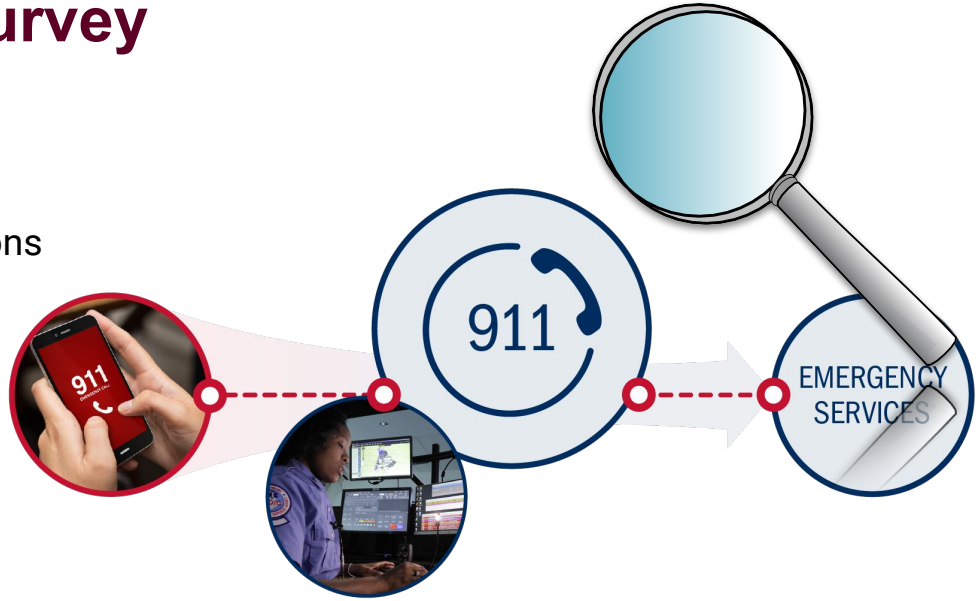
Research	Threat Model	Testbed	ECASTT	Automation
- Research NENA i3 standards -Applicable RFCs & Documents -Determine current NG911 deployment status and landscape	- Determine Technical objectives of NG911 -Develop Threat Model	-Determine testbed requirements -Build testbed	-Define test cases -Realize requirements -Implement tests	-Future Work: Automate

NG911 Security Literature Survey

- Searching and examining the extant literature
- Assessing the results of primary studies
- Outlining our observations
- Defining and formulating the research questions
- Working on our research questions
- Discussing the future work

Specially,

- Current NG911 systems and issues
- Threat modeling and risk assessment
- Research NENA i3 standards
- Applicable RFCs & Documents
- Determine current NG911 deployment status and landscape



Source: https://www.jacquesvaphotography.com/next-generation-911

NG911 Threat Modeling

NG911 Threat Modeling

Cybersecurity Objectives of NG911 system could include:

- Ensuring the availability of call centers, and call routing
- Ensuring the availability of Location Information Servers
- Ensuring repudiation of Location Information Servers
- Maintain privacy of user information
- Detect/respond integrity breaches as they arise

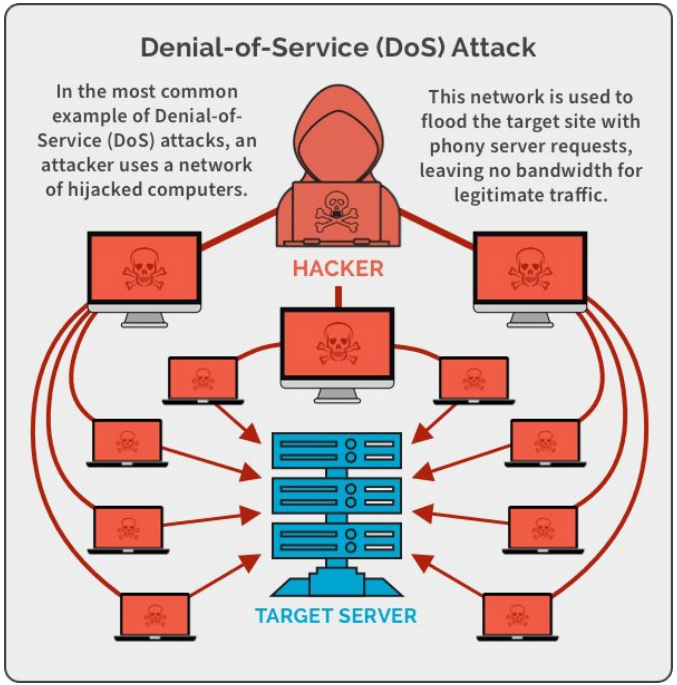
Threat Model

Threats	Impacts	Components
DoS	• Prevented or limited user access to 911 • Lack of correct location information • Hindered or prevented call routing to relevant PSAPs	ESInet BCF ESRP ECRF PRF
Malware	• Limited availability of PSAP response capabilities due to unavailable resources • Jeopardization of encrypted personal data	BCF ESRP ECRF PRF
Man-in-the-Middle (MITM)	• Interception of personal data, information, and calls • Location information can be modified whilst on route to PSAP	BCF ECRF ESRP PSAP ESInet
Spoofing	• Inaccurate location information • Compromised user location information	LIS Server PSAP/L-PSAP

Denial of Service (DoS) Example

In the context of the NG911 system, a DoS attack involves flooding the emergency communication infrastructure with an overwhelming number of malicious requests.

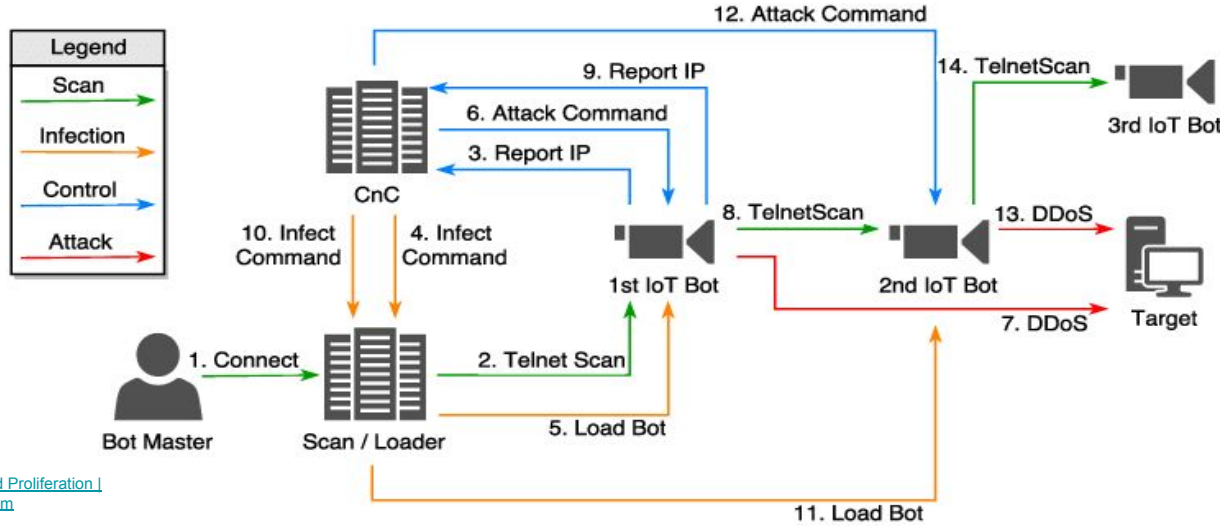
This could cause the system to become overloaded, unable to handle genuine emergency calls, and potentially disrupt emergency response services.



Source: denial-of-service-attack-example.png (600×610) (spanning.com)

Malware (Botnet) Example

A malware infection could turn the NG911 system into a part of a botnet. Botnets are networks of compromised computers controlled by a central attacker.



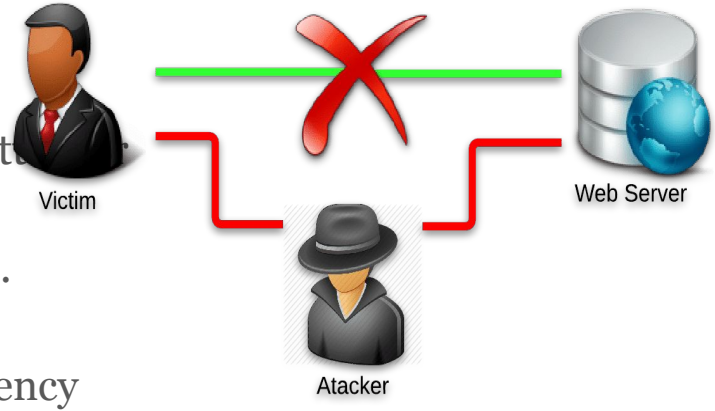
Source: Botnet Infection and Proliferation | Download Scientific Diagram (researchgate.net)

In this scenario, the NG911 system's resources might be exploited to participate in other cyberattacks or generate massive amounts of fake traffic, leading to a denial-of-service situation that hampers services.

MITM Example: Call Interception

In a man-in-the-middle attack on the NG911 system, the att... could position themselves between a caller calling the emergency number and the NG911 system's infrastructure.

The caller believes they are speaking directly to the emergency services, but the attacker is actually listening to the conversation in real-time. The attacker might even impersonate the emergency services operator, potentially providing misleading or dangerous information to the caller.

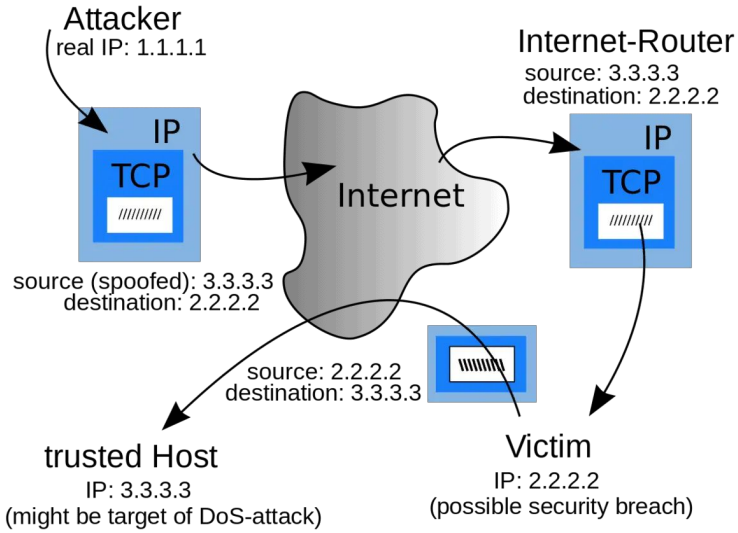


Source: Ask These 9 Security Questions to Better Protect Your Software (mentormate.com)

Spoofing Example: Location Spoofing

Location spoofing involves the manipulation of GPS or location data transmitted from the caller's device to the NG911 system.

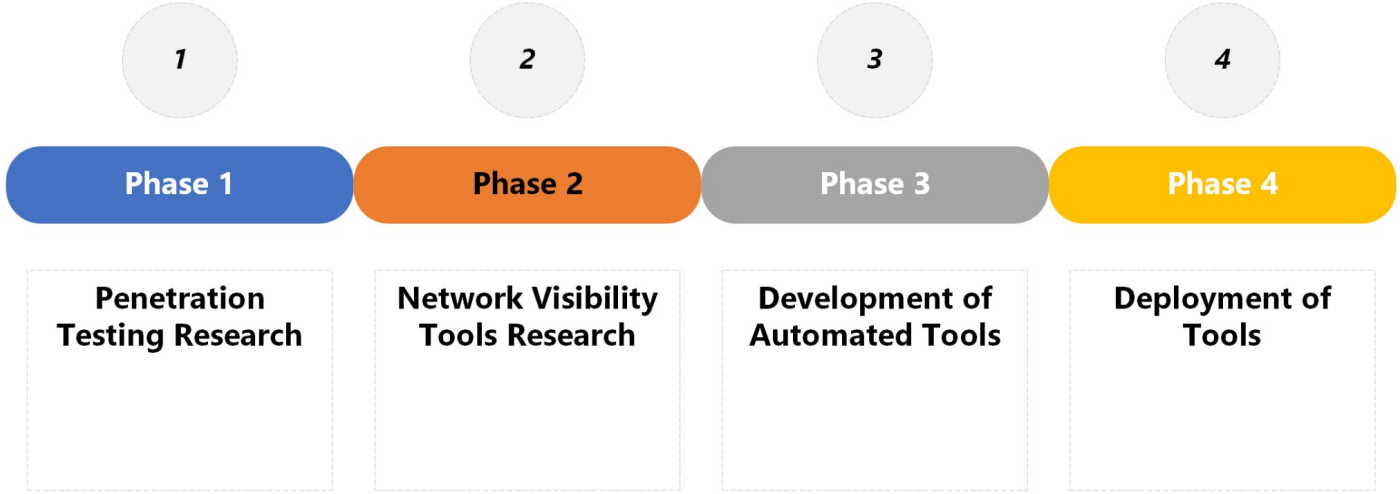
By doing so, the attacker could make it seem as though the emergency call is coming from a different location, leading to misdirected emergency services or delayed response times.



Source: What is an IP Spoofing Attack? - NETWORK ENCYCLOPEDIA

Development and Implementation

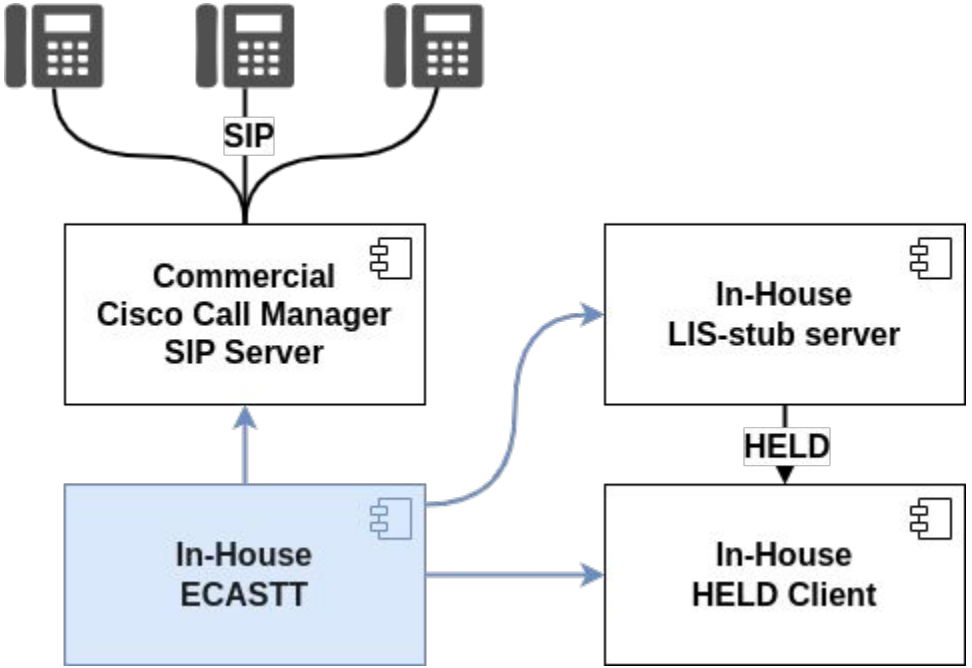
Project Phases



ECASTT Testbed

Emergency Communication Automated Security Testing Tool

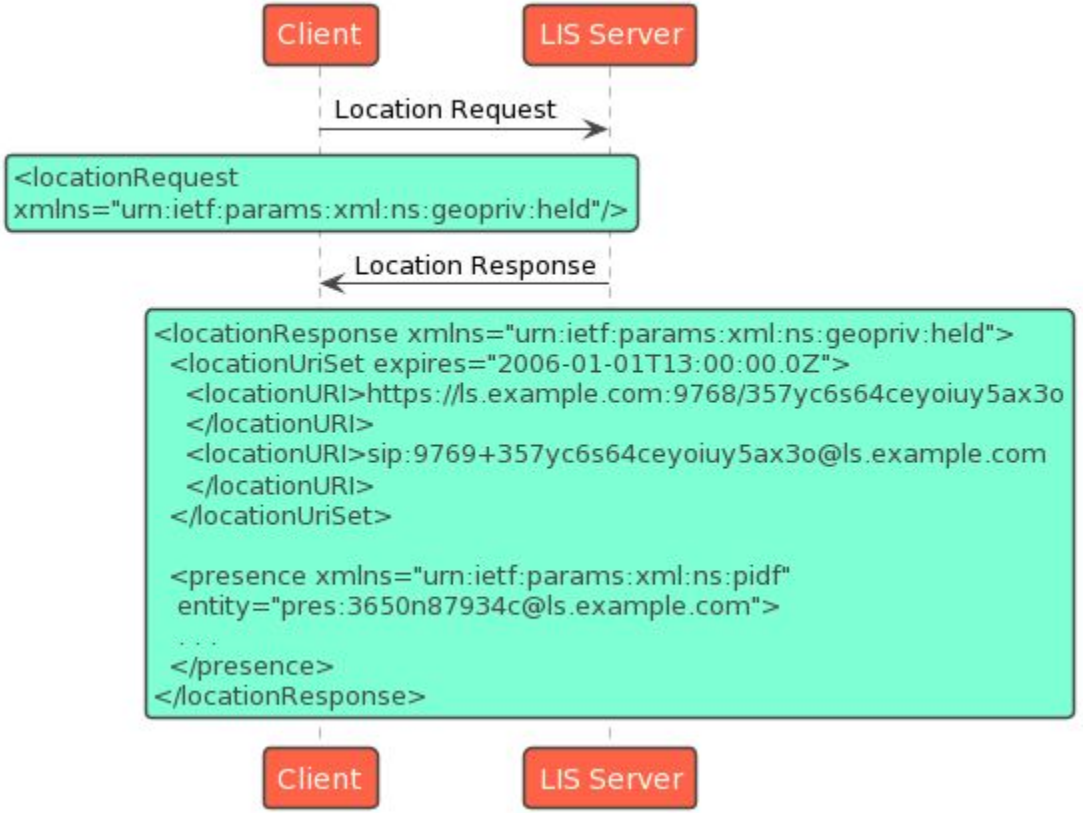
Testbed Architecture



In-House Components

LIS Server - Used to give requesting devices either a location (address or coordinates) or tell the device where to find its location over the next few hours. Adheres to RFC 5985

HELD Client - Program that asks the LIS server for its device's location. Uses the HELD protocol. Adheres to RFC 5985



Commercial Component: Cisco Call Manager (SIP Server)

- Enterprise SIP Server used in all sectors
- Trusted by DoD and deployed in many American military bases
- Supports all major SIP standards including voice calls, video, and various types of messaging

ECASTT Development

ECASTT Framework Development Approach

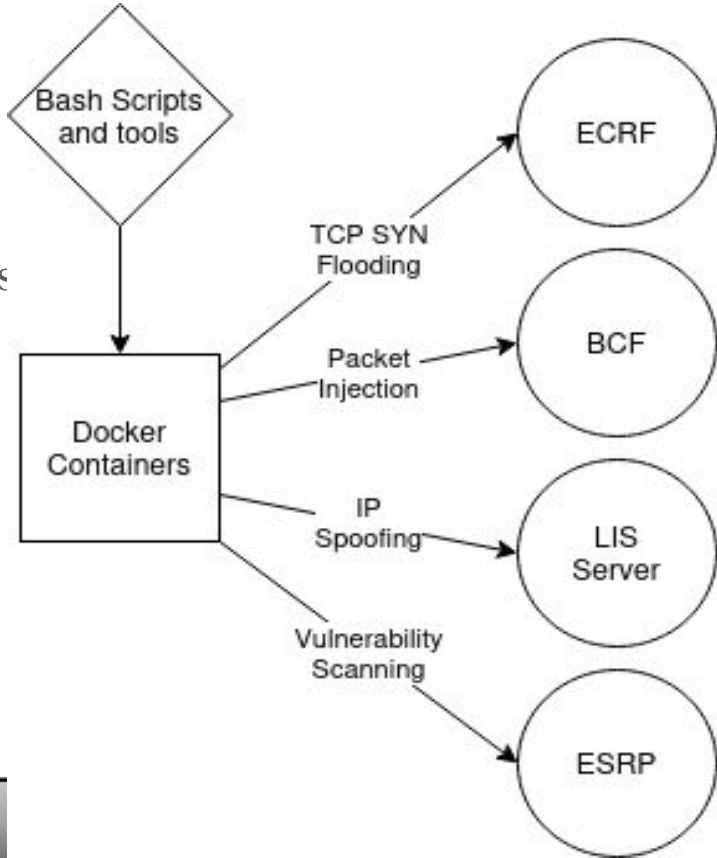
- Tests should be applicable to a variety of NG911 implementations
- Tests should be conducted using industry standard tools
- Test results should provide actionable information
- Tests should be focused on threats relevant to the NG911

What are these tests?

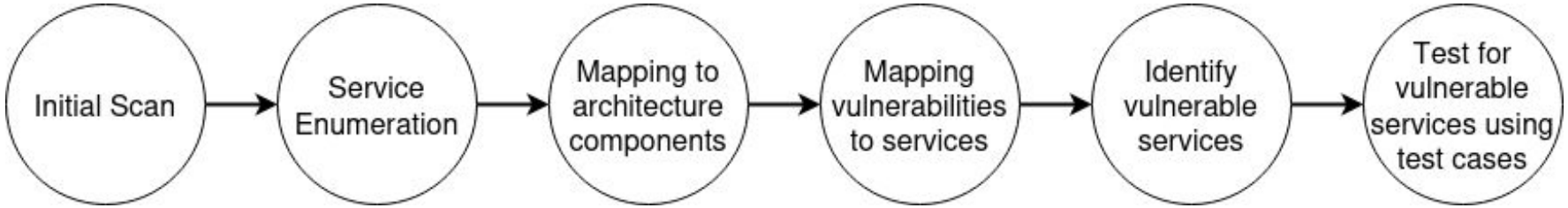
DoS	Targets are flooded with ICMP, TCP SYN, and SIP traffic
Malware	Targets are scanned for service versions that have publicly available vulnerabilities
MITM	ESInet traffic is analyzed for use of secure protocols (ie. HTTPS, SSH, etc.)
Spoofing	Important Esinet services and user requests are spoofed

ECASTT Objectives

- Realistic attack scenarios
- Real offensive tools
- All components are tested against relevant test scenarios
- Only relevant tests are conducted
- All tests should be produce actionable results
- Tests are scoped to the relevant components of the i3 standard



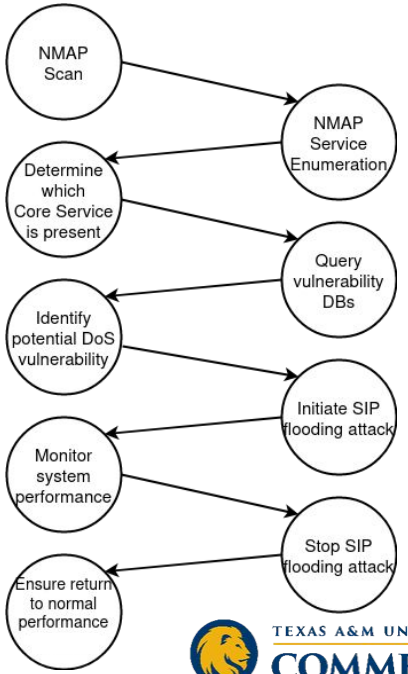
Testing Workflow



Testing Scenarios for Automation

Threats	DoS
Impacts	• Prevented or limited user access to 911 • Lack of correct location information • Hindered or prevented call routing to relevant PSAPs
Components	ESInet BCF ESRP ECRF PRF

Given: The ng911 system is operational and connected to the internet.
When: The ng911 system experiences SIP (Session Initiation Protocol) flooding.
Then:
1. The ng911 system detects an unusually high volume of incoming SIP requests.
2. The ng911 system activates its traffic monitoring and analysis mechanisms.
4. The system identifies the source IP addresses from where the flood of SIP requests is originating.
5. The ng911 system initiates measures to mitigate the impact of the SIP flooding(ie.rate limiting, filtering techniques)
6. The system dynamically adjusts its network resources to handle the increased traffic and prevent service degradation.
7. The system provides real-time statistics and status updates on the SIP flooding.
8. The ng911 system resumes normal operations once the SIP flooding has been effectively mitigated, ensuring that emergency calls can be processed without interruptions.



Next Steps & Expected Results

- Actionable results will be scoped to relevant technologies with specific issues listed (ie. CVEs, performance metrics)
- Results will be able to point to which components are vulnerable
- Results will include information on both passed and failed tests

Benefits of ECASTT

- Provide actionable information that can easily be used to understand the security posture of the system
- Only reports vulnerabilities that are relevant to NG911
- Independent of vendor specifications or implementations
- Easily provide up to date vulnerability information

Towards Automation

- Automatic scripting of testbed containers
- Pursuing the implementation of machine learning algorithm to orchestrate testing

Future Work

- Full implementation of Automation
- Implement BCF into testbed
- LoST protocol implementation
- Data Analysis and Visualization

NG911 Security Lessons Learned

- NG911 networks have wildly different objectives than normal networks
- Implementing RFC standards can be challenging
- Much work remains to be done in the field of automating risk assessments
- More work is needed to determine the security effects of emerging threats

Thank you

Special thanks to

Department of Homeland Security (DHS) - Cross-Border Threat Screening (CBTS) Center of Excellence,
RELLIS Academic Alliance
TAMU Internet 2 Technology Evaluation Center (ITEC)

CBTS CyberSecurity Summer Research Institute

Towards Zero-Trust: A Systems Engineering Approach For Vital Ship Systems' Cybersecurity Risk Assessments

TAMU Commerce Faculty Mentors

CROSS-BORDER THREAT SCREENING
Center of Excellence

Dr. Eman Hammad

- Assistant Professor, Computer Science & Information Systems
- Office: ACB2-208
- Email: Eman.Hammad@tamuc.edu
- Location: RELLIS Campus, Bryan, TX

Dr. Yuehua Wang

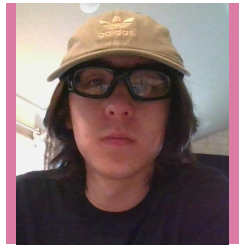
- Associate Professor, Computer Science & Information Systems
- Office: Jour 230
- Email: Yuehua.Wang@tamuc.edu
- Location: Jour 101/102, Commerce, TX

Texas A&M AgriLife Research

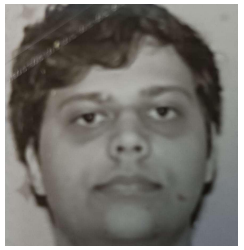
RELLIS
THE TEXAS A&M UNIVERSITY SYSTEM

Texas A&M University Commerce

Colin Barber
3rd year, Computer Science
TAMUC-RELLIS
cbarber5@leomail.tamuc.edu



Zachary Phelps
3rd year, Computer Science
TAMUC-Commerce
zphelps@leomail.tamuc.edu



Zenon Nowakowski
3rd year, Computer Science
TAMUC-RELLIS
znowakowski@leomail.tamuc.edu

Cayden Cather
3rd year, Computer Science
TAMUC-Commerce
ccather@leomail.tamuc.edu

Outline:

- Motivation: Introduction & Background
- Research Questions
- Project Plan
- Systems
- Testbed
- Future Work

Background & Motivation

Research Questions

Main Q: What are the cybersecurity risks of incorporating autonomous technologies into maritime systems and ships/vessels?

Supporting Q: Can we create a reasonably representative testbed to enable cybersecurity studies, assessments and testing?

Project Plan

- Phase 0: Preliminary research into existing testbeds
- Phase 1: Building the testbed
- Phase 2: Integrating security tools into network
- Phase 3: Security evaluation of testbed
- Phase 4: Finalization, writeup

Industrial Systems OT/ICS/SCADA

Operational Technology (OT):

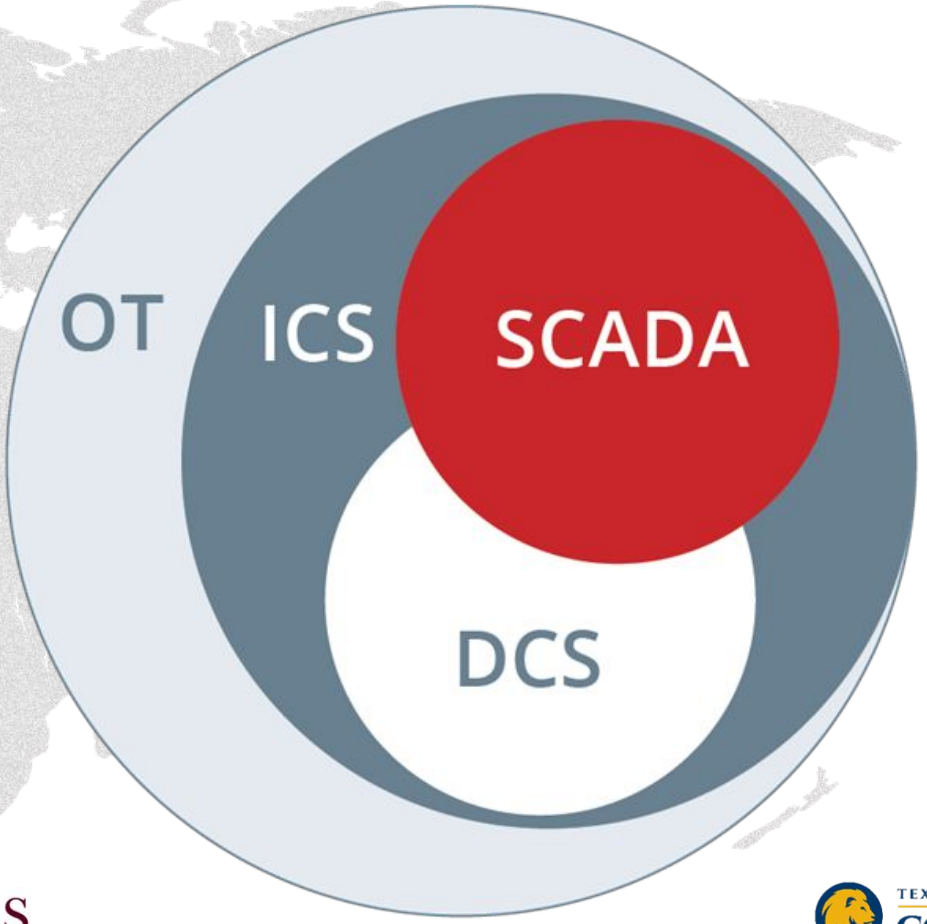
- the utilization of software and hardware in industry. Ex: Historian. Includes ICS, DCS, IIoT, SCADA

Industrial Control Systems (ICS):

- systems used to control critical industrial infrastructure, such as water treatment plants, with technologies like HMIs, PLCs.

Supervisory Control and Data Acquisition (SCADA):

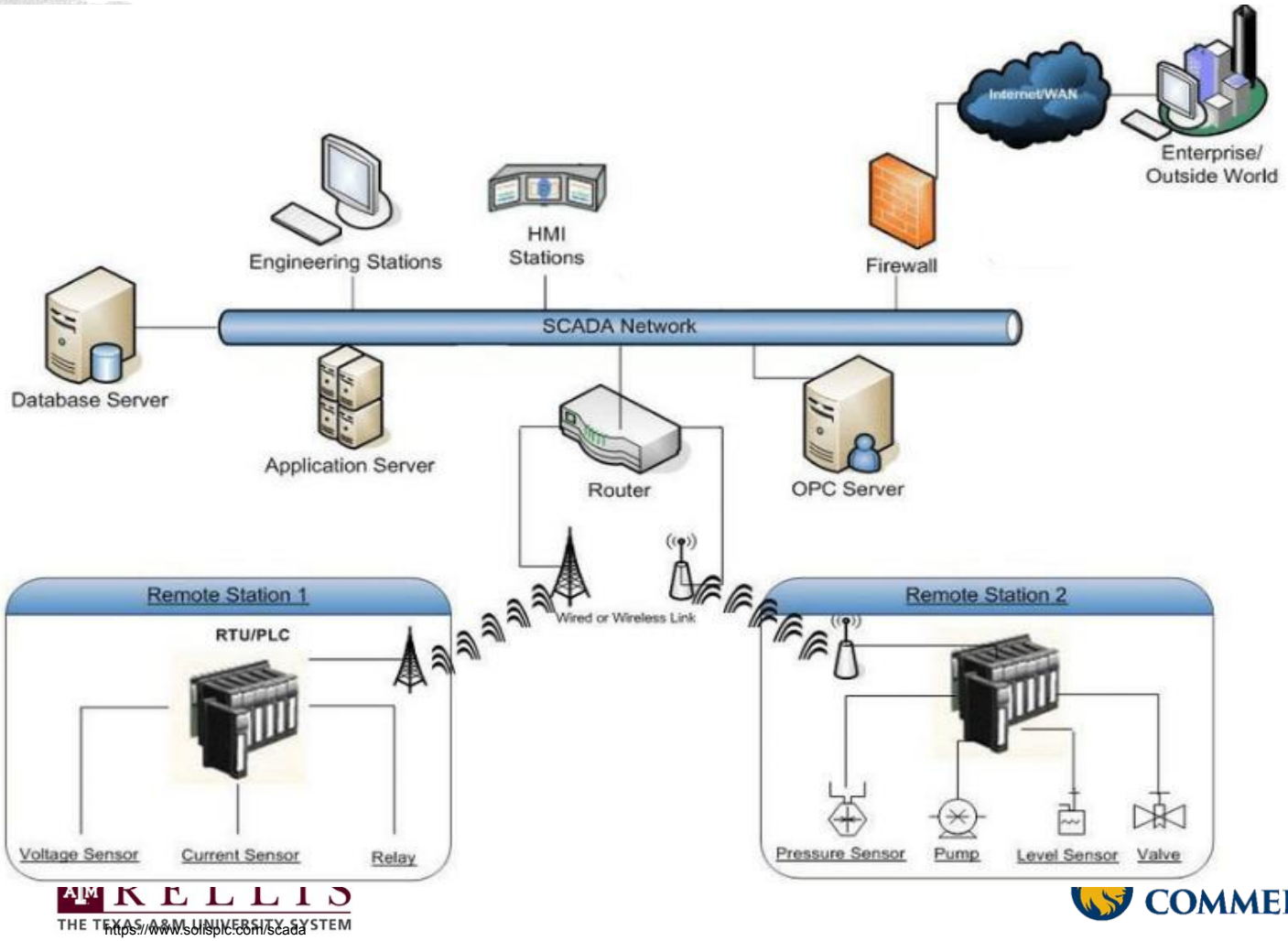
- a control system used to remotely monitor and control devices that are used for data acquisition and industrial control



https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

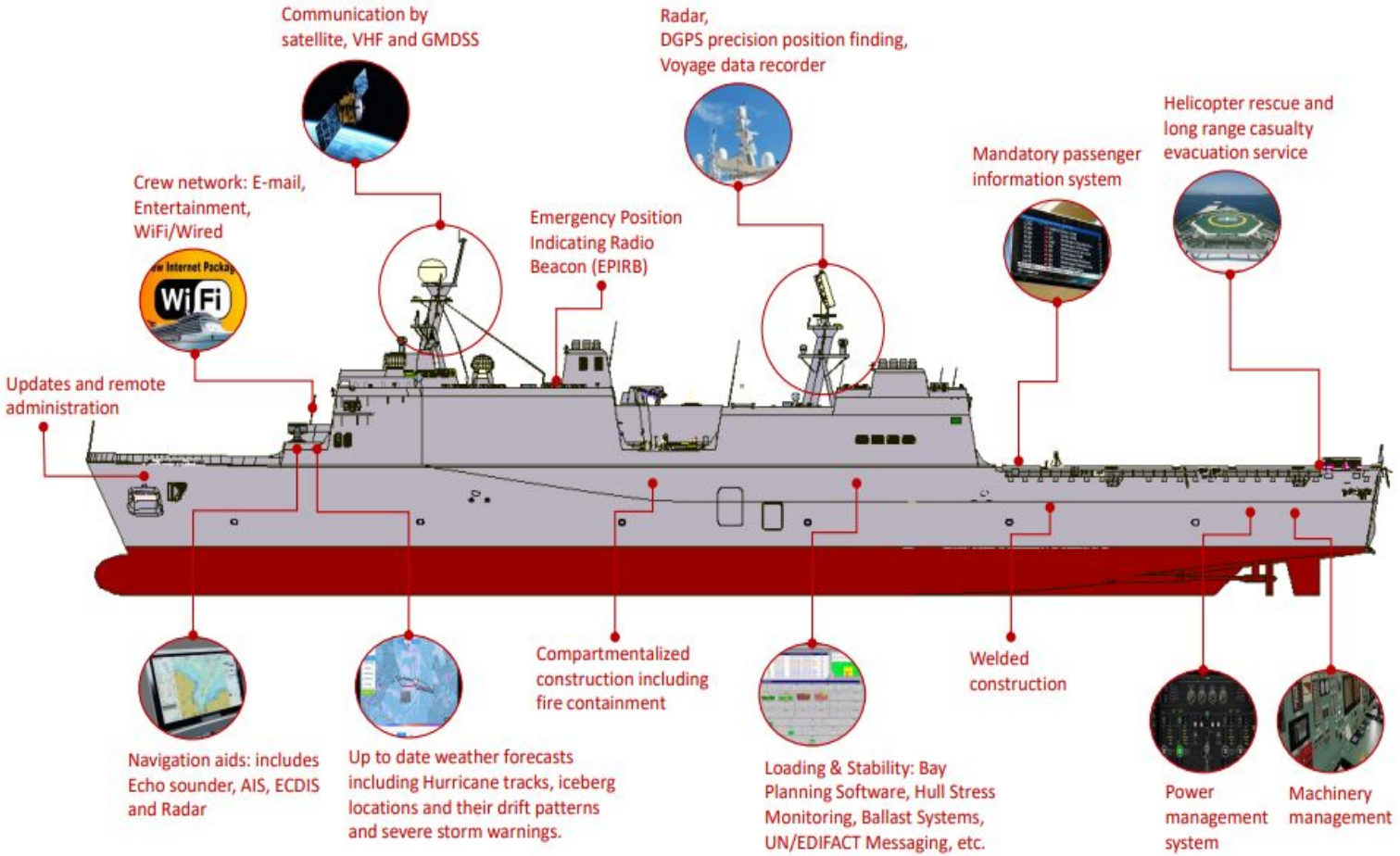
SCADA Architecture

- Internet
- Firewall
- Scada Network
- HMI Stations
- Engineering Stations
- Database Server (Historian), Application Server, OPC Server
- Router, Switches, VLan
- RTU, MTU
- PLC
- Accrators: Pumps, Lights, Values
- Sensors: Transmitters, Switches, push buttons



https://www.solispic.com/scada

Example Maritime Technologies



https://www.mdpi.com/2673-8732/2/1/9

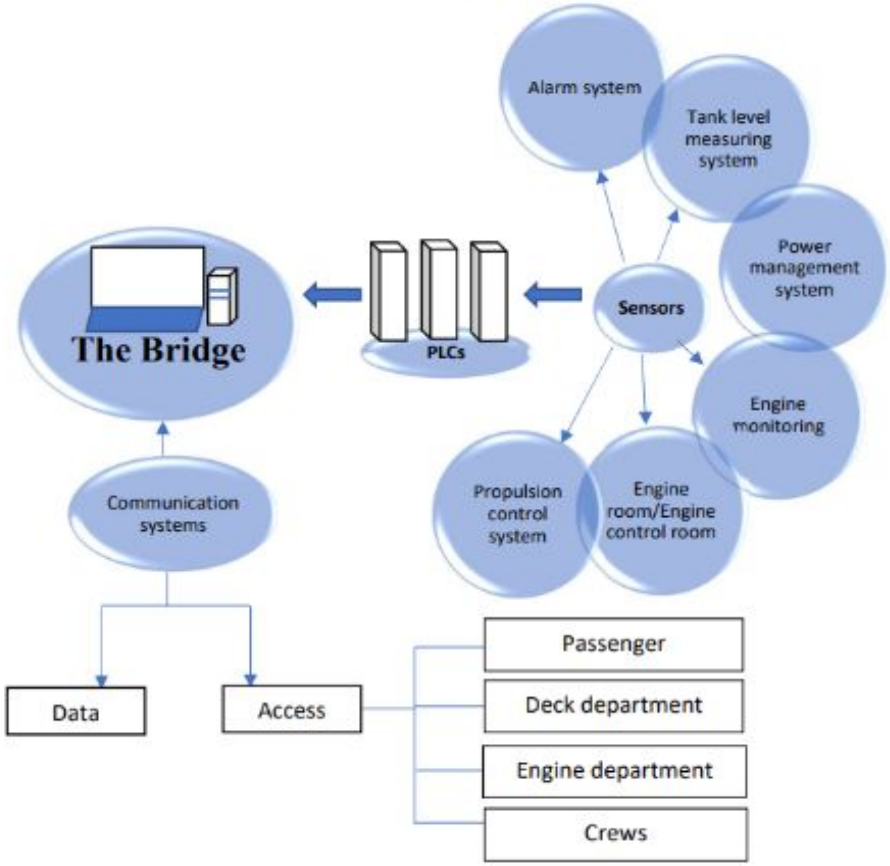
Example Maritime Communication and Information Technologies

- **AIS:** Automatic Identification System, Automated tracking system
- **GMDSS:** Global Maritime Distress and Safety System, communicates with authorities through terrestrial or satellite
- **DSC:** Digital Selective Calling, allows for individual signals to be sent for the location of the ship giving the signal
- **GNSS:** Global Navigation Satellite System, shows location, speed, and destination time of ships
- **GPS:** Global Positioning System, Satellite based radio navigation system that is run by the United States of America
- **RADAR:** Radio Detection and Ranging, Detects objects by sending radio waves and receiving waves that are reflected back
- **ECDIS:** Electronic Chart Display and Information System, Navigation

OT/ICS in Maritime

Several vessel vital systems rely on OT with control dashboards in the ship Bridge (control deck). Examples include:

- ICS PLC is an controller for actuators and sensors
- Alarm system
- Tank level measuring systems
- Power management systems
- Engine monitoring
- Engine control
- Propulsion control system



Source:https://www.mdpi.com/2078-2489/13/1/22

Cybersecurity and Maritime Incidents

Maritime Attacks

- 2019 **U.S. Coast Guard** issued a cyber attack alert after malware hit a ship heading towards the new york port.
- 2017 **Maersk** cyber-attack - ransomware exploited a vulnerability in Microsoft systems. Microsoft released a patch but Maersk did not update their systems. Maersk lost over $300 million due to shipping delays.
- **DNV's** ShipManager software ransomware attack in January 2023, putting the data of around 1,000 vessels at risk.

OT/ICS Attacks

- **Stuxnet** - malicious computer worm that attacked SCADA systems, causing significant damage to the Iranian nuclear program. The worm targeted PLCs to cause centrifuges to tear themselves apart.
- 2015 **Ukraine power grid** attack - hackers took control of SCADA systems to turn off the electric supply.
- 2017 to 2019 known significant cyber attacks increased from 50 to 120 to over 300 attacks

Maritime Related Cybersecurity Regulations and Standards

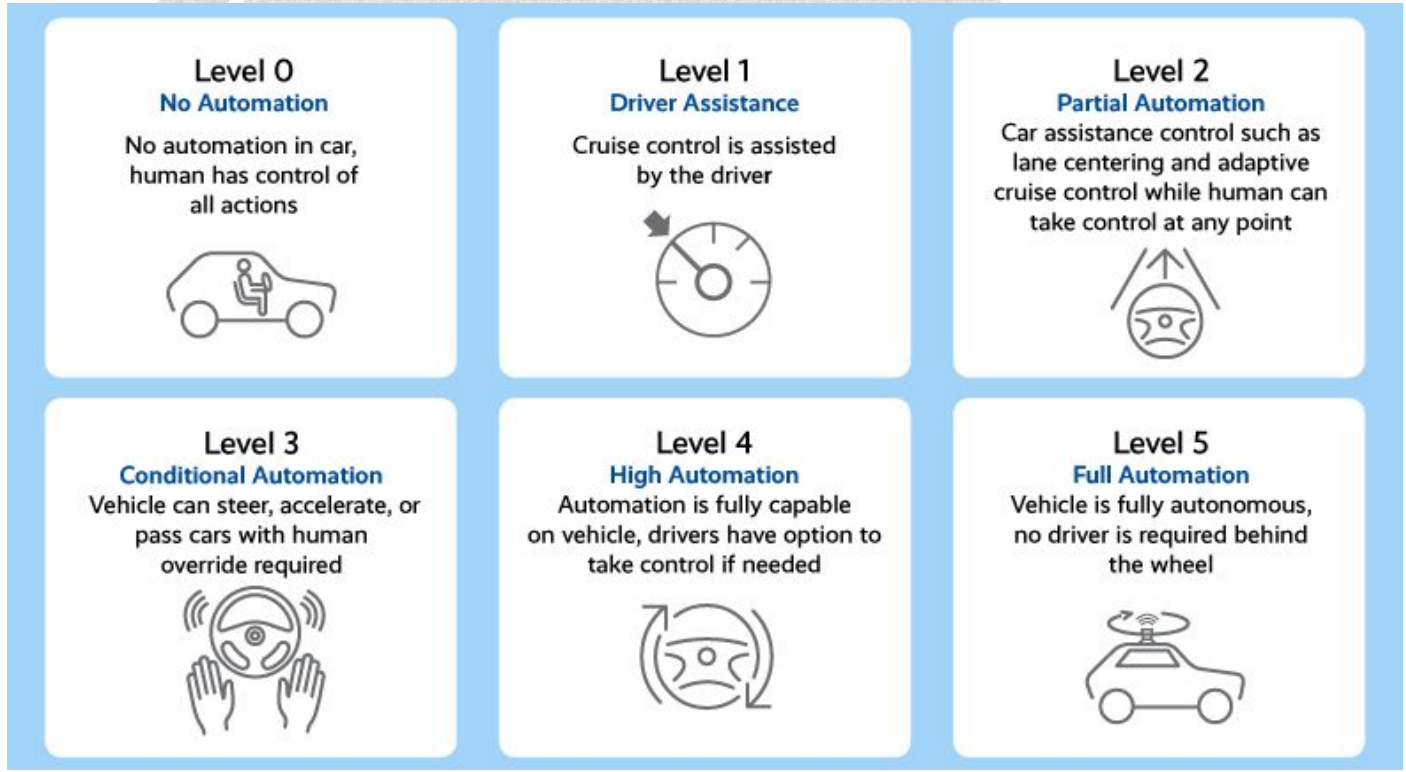
- **Marcsec levels:** defines levels of alertness and physical security.
- **CRF (Cybersecurity Regulatory Framework) standards:** CRF are Federal Codes of Regulations. The components of the ship need past inspections and predefined metrics.
- **International Maritime Organization** regulations: agency of the UN that sets global standards for safety and security for international shipping.
- **General Cybersecurity Standards and Regulations:** general cybersecurity standards also apply to the industry including NIST Cybersecurity Framework (CSF) and IEC OT/ICS Security Standards.

Cybersecurity Threat Modeling and Risk Assessment

Attack name	Target	Impact	Mitigation
Supply Chain Compromise	Exploitable/exploited vendors	unauthorized access	Audit, supply chain management, vulnerability scanning, update software
Data spoofing	Sensors	manipulation/denial of view	Audit, vulnerability scanning, update software, data authentication, network segmentation, process/device authentication
Compromised Workstation	Workstations	Unauthorized access, unauthorized control	Audit, network network segmentation, vulnerability scanning, update software

Levels of Automation and Threat Modeling

- The levels of automation, ranging from no automation to full automation.
- As the reliance on automation increases, there is a higher risk of cyber attacks.



Emerging Technologies & Emerging Threats

AI (Artificial Intelligence)

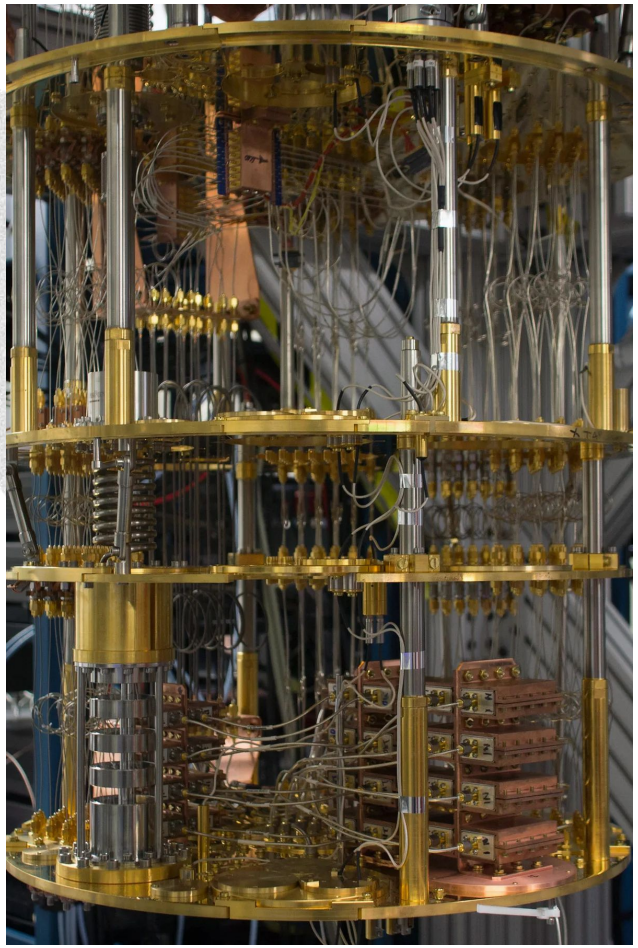
- ➔ Operational: using AI to defend against threat
- ➔ Threat: using advanced AI to create and execute attacks

Quantum Computing

- ➔ Operational: support advanced encryption, and more efficient communication and computing
- ➔ Threat: can break non quantum-safe encryption, can be used to amplify brute-force attack capabilities.

5G/6G Networks

- ➔ Operational: fast, scalable, flexible and efficient networks with high degrees of autonomy (Self-X).
- ➔ Threat: faster speeds needs faster security



https://www.flagshippioneering.com/stories/quantum-computing-is-real-its-most-important-application-will-be-simulating-the-subatomic-world

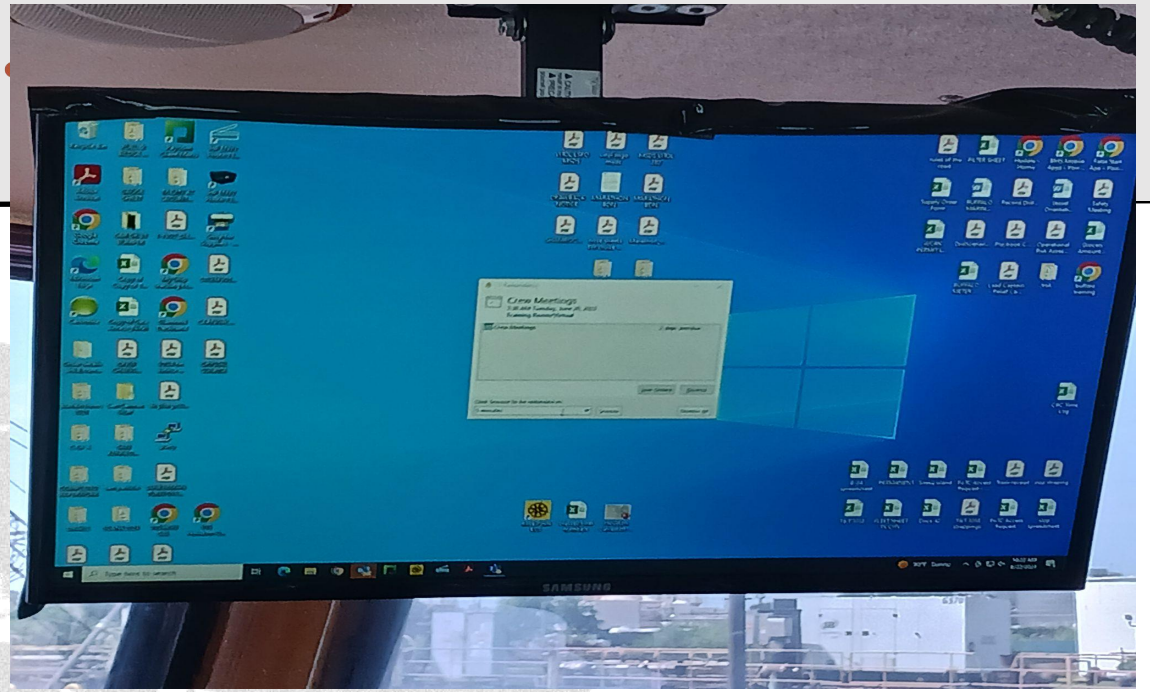
USCG Houston-Galveston Port Field Trip

Tony Tug vessel Tour (old)

- **Tug vessel:** is an maritime ship that pulls or pushes another vessel or cargo.
- Automation used in an Old Tug vessel are low
- **Drying docks:** vessels are regularly pulled for maintenance

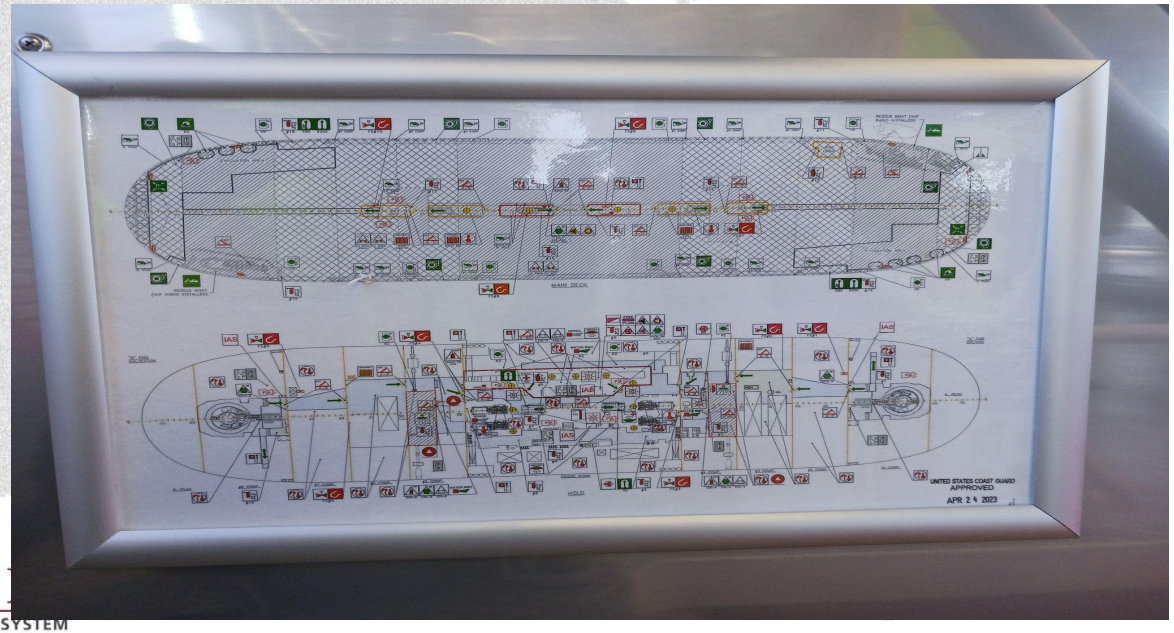
Tony Tug vessel Tour (old)

- **Geolocation:** use of Window OS Workstation and GPS
- **Identification Systems:** AIS Automatic Identification System uses VHF frequencies to communicate
- **Logging**: timetables, charting with the help on online services.
- **Hardware:** Operational technology (OT) on board are mostly hardwired and use a simple alert dashboard. Communication is strictly radio.
- **Technical staff:** minimal operational staff on board. Technical systems' maintenance is done based on need and mostly when at port.



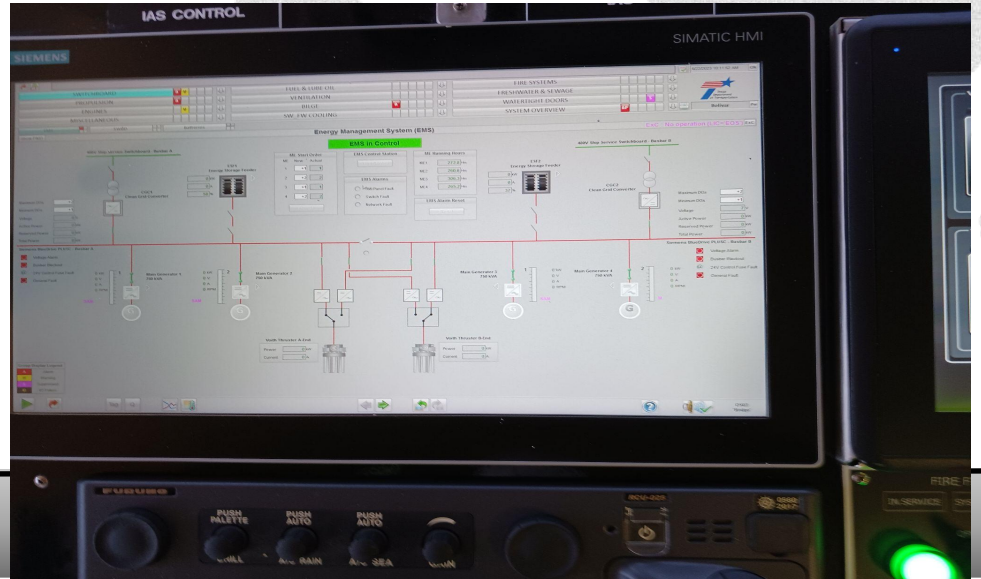
Ferry Vessel Tour (new)

- New vessel going through final testing and validation
- Ship could travel in two directions
- Higher levels of automation
    - PLC, HMIs, SCADA
    - Energy management
    - Redundant vital systems (e.g. bridges, generation, etc.)
    - Failover mechanisms
    - Ship systems connected via ethernet and fiber
- More recognisable (OT/ICS) vendors: Siemens, Honeywell, etc.
- AIS communication



Ferry Vessel Tour

- **Communications:** FM radio communication, MLCS
- **Navigation:** Rosepoint software is used for navigation and is updated manually using a USB.
- **OT Automation**: Fully automated valve system, AMS for Container Management



Field Trip Lessons Learned

- The biggest concern and target is commercial assets and logistics.
- USCG has limited ability to enforce standards, some companies approach the USCG for guidance.
  - Working theory from USCG is a major threat will need to present itself in order for policy to change.
- Security compliance is still lacking.
  - A lack of mass adoption of standards.
  - Older generations are reluctant to adapt to the ever-changing threat landscape.

Common OT/ICS Security Challenges:

- Legacy Software and Hardware
- Lack of Documentation
- Lack of Encryption
- No Backups and Outdated Components
- Lack of Network Segmentation
- Insider Threats
- Threat of Malware
- Command Injection and Parameters
- Identification and Authentication Failures
- Logging and Monitoring Failures

https://www.naval-group.com/en/5-things-know-about-naval-groups-cyber-management-system-cyms

Cybersecurity Risk Assessment

Risk = Criticality (Likelihood × Vulnerability Scores [CVSS]) × Impact

Likelihood: Percent that some event will happen

Vulnerability: The resource that is at risk

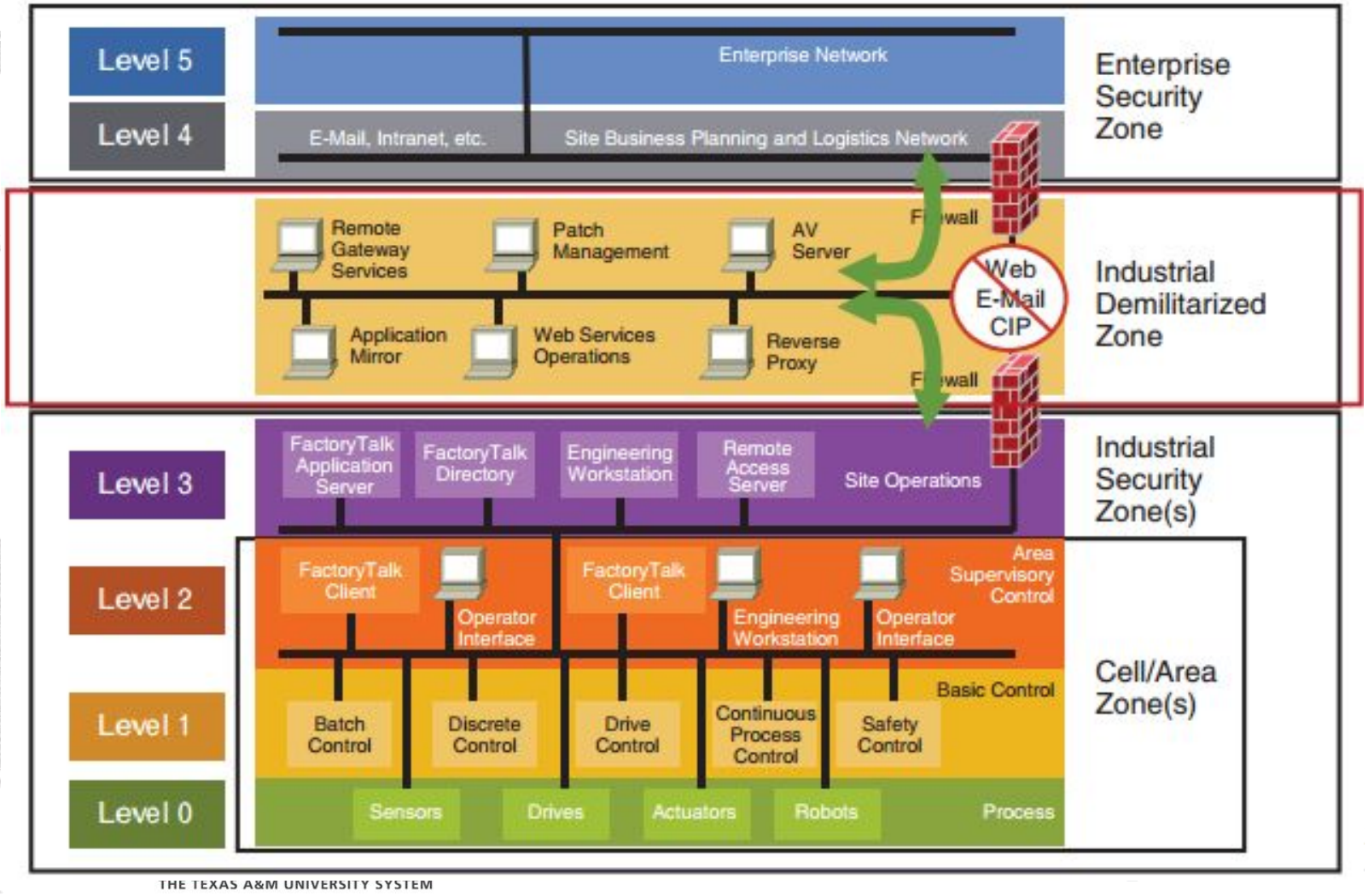
Impact: Assets that will be affected

LIKELIHOOD	insignificant	minor	moderate	major	critical
almost certain	Moderate	Major	Critical	Critical	Critical
likely	Moderate	Major	Major	Critical	Critical
possible	Moderate	Moderate	Major	Major	Critical
unlikely	Minor	Moderate	Moderate	Major	Critical
rare	Minor	Minor	Moderate	Moderate	Major

CONSEQUENCE

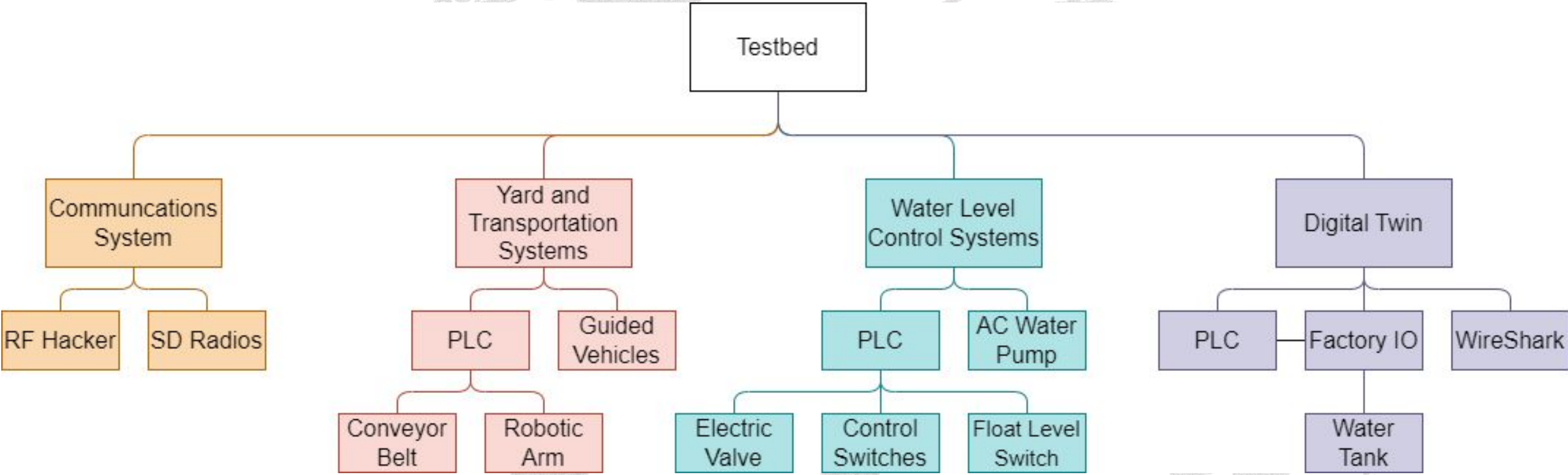
Purdue Model

The Purdue Model is a reference architecture for OT/ICS networks. It provides abstraction that helps define security zones and network segments, so that resources are isolated in a way to ensure minimal exposure to potential attacks.



Testbed Development

Maritime Security Testbed (Process/Setup)

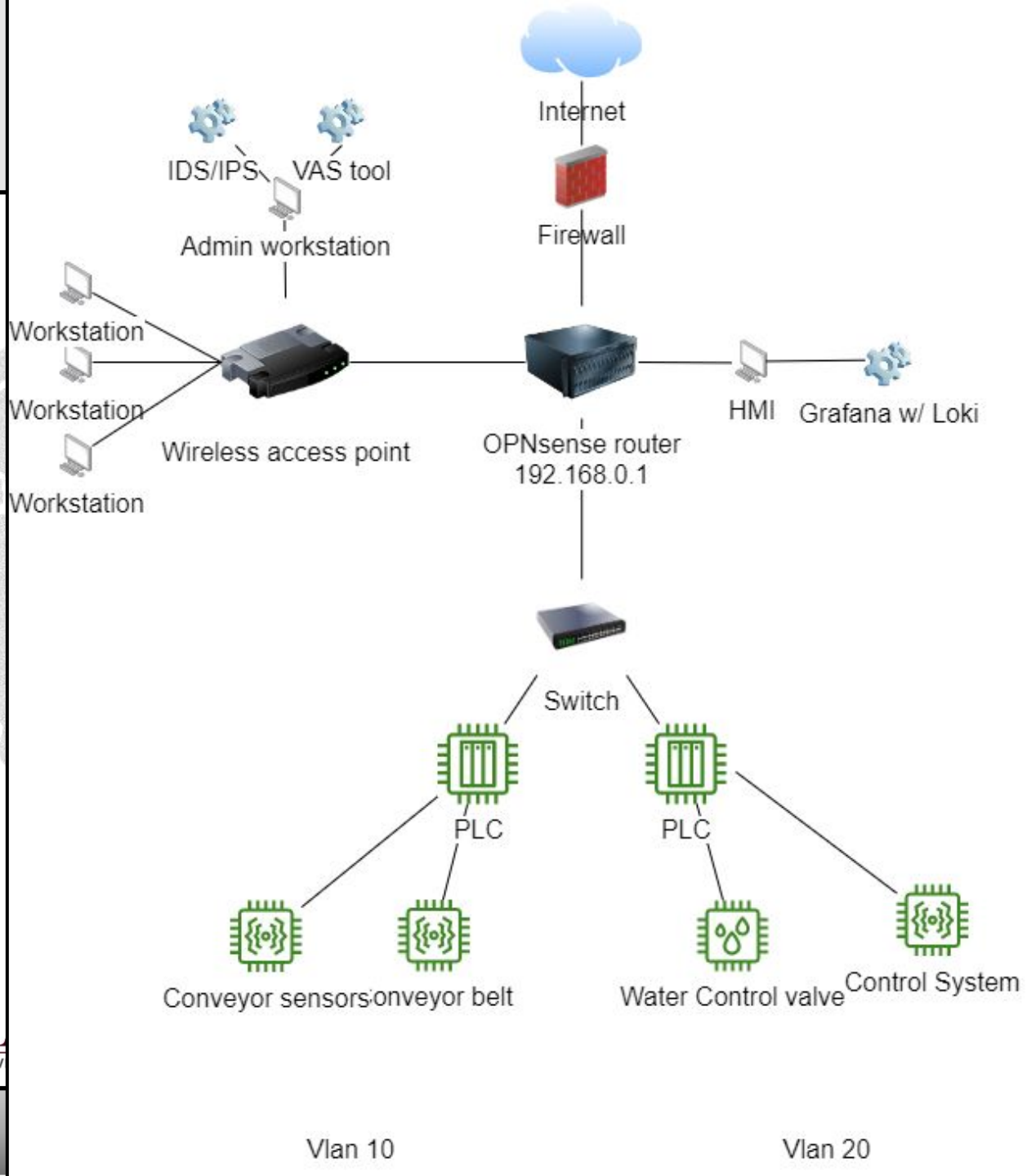


THE TEXAS A&M UNIVERSITY SYSTEM

Maritime Security Testbed

(network diagram)

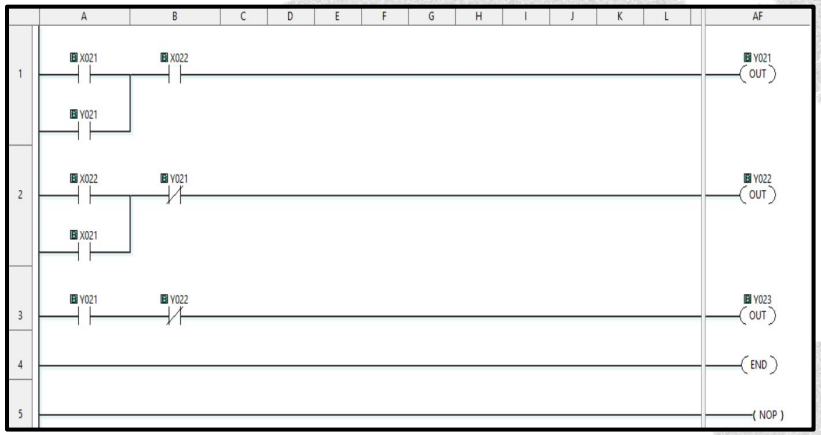
- Firewall/ Routing : OPNsense allows for routing and firewalls configurations
- IDS/IPS: Snort that can send alerts
- Network Logging: prometheus: prometheus is a network monitoring software.
- Network visualization: Grafana Loki is an open source GUI for dashboards of charts and graphs



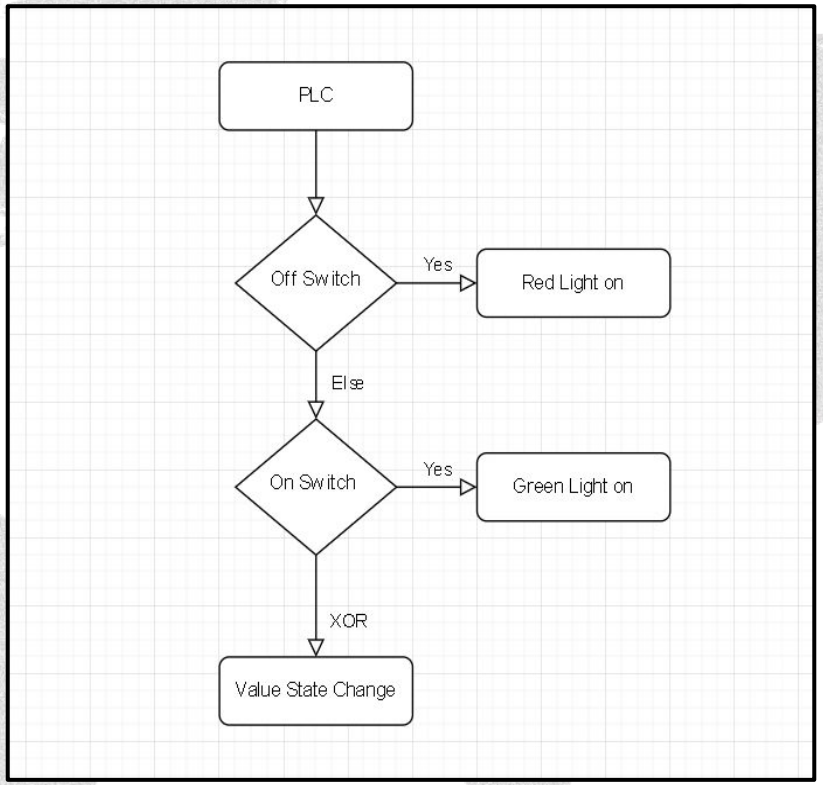
TEXAS A&M AGRILIFE RESEARCH

THE TEXAS A&M UNIV

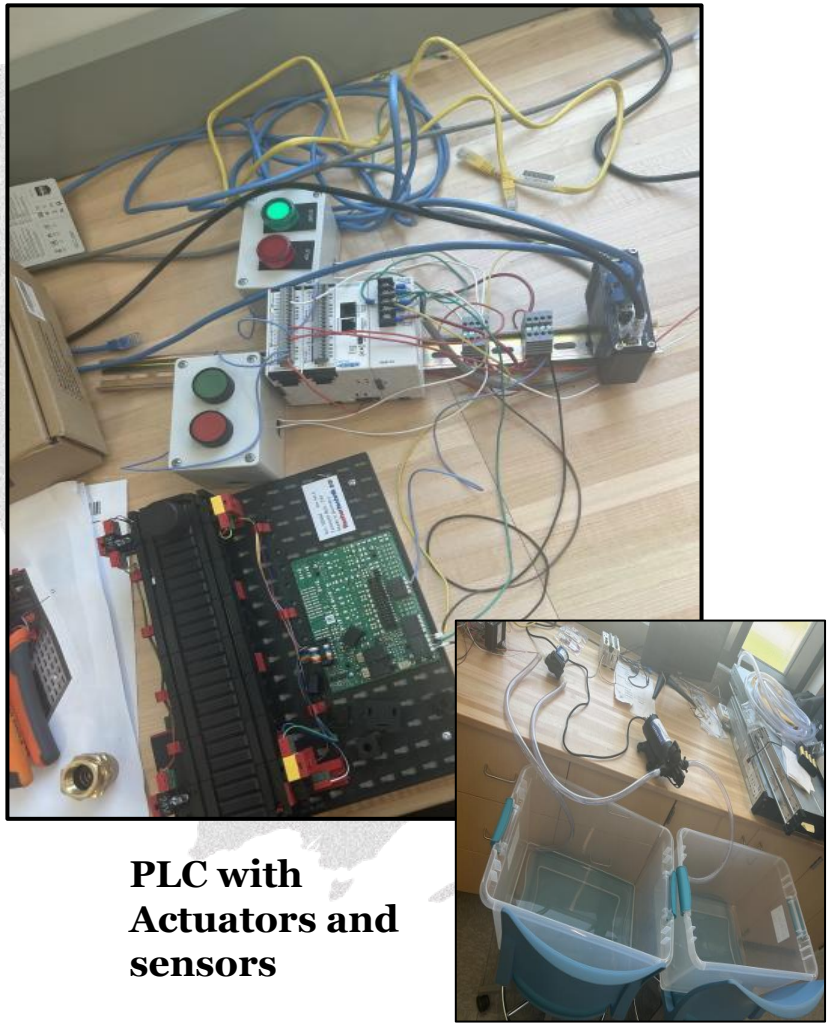
Testbed: Water Level Control



Ladder Logic for the value control



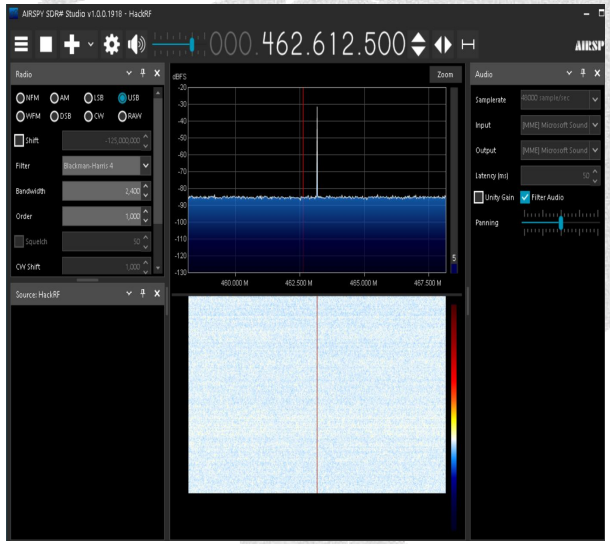
PLC workflow Visualization



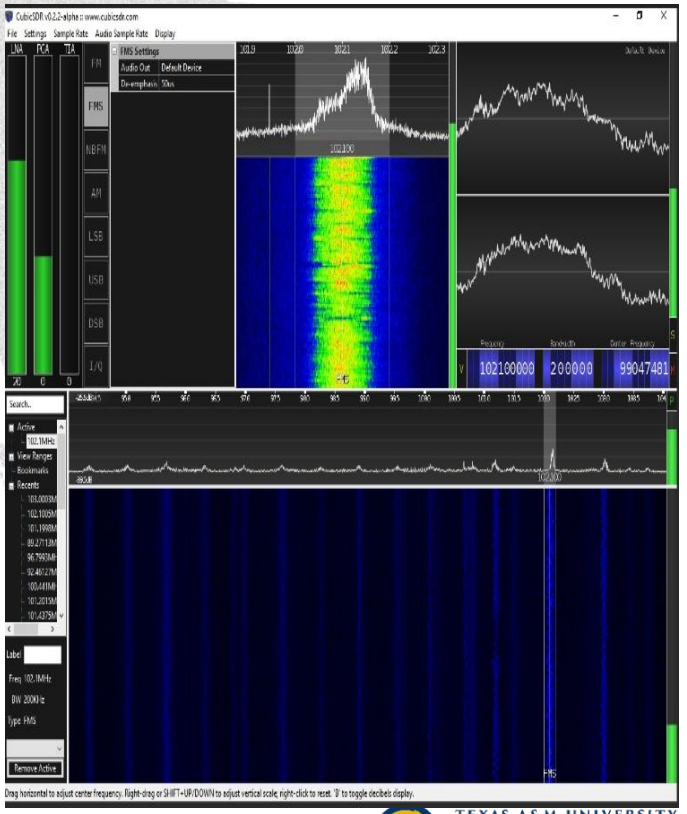
PLC with Actuators and sensors

Radio Communication & Hacker RF

Software defined radios w/ Hacker RF

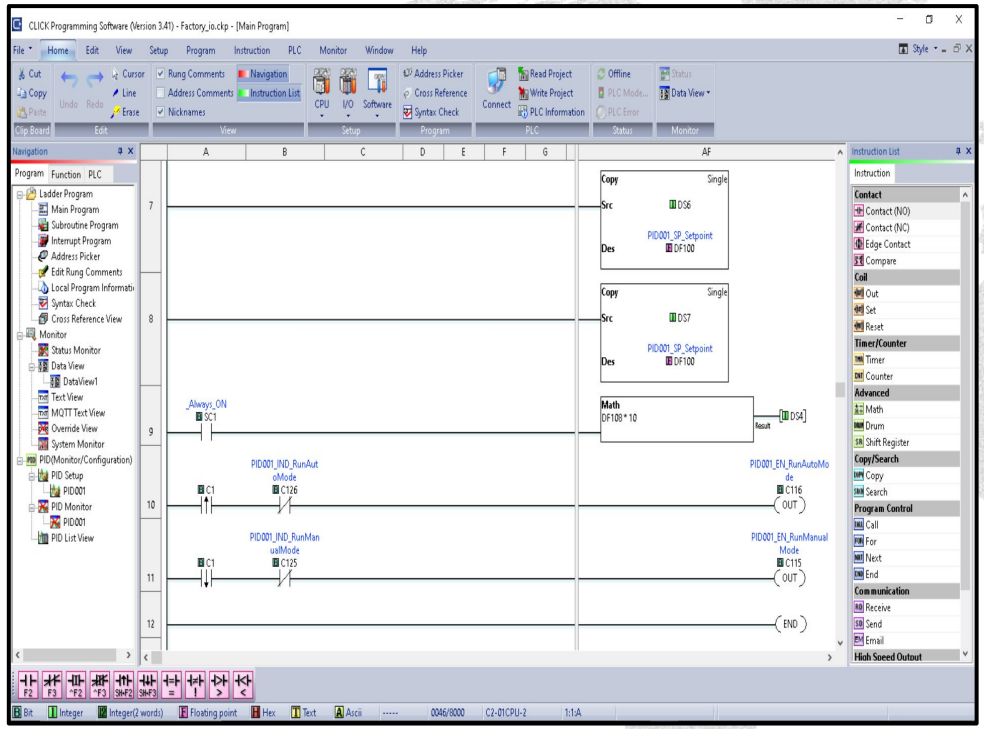


SDR airspy

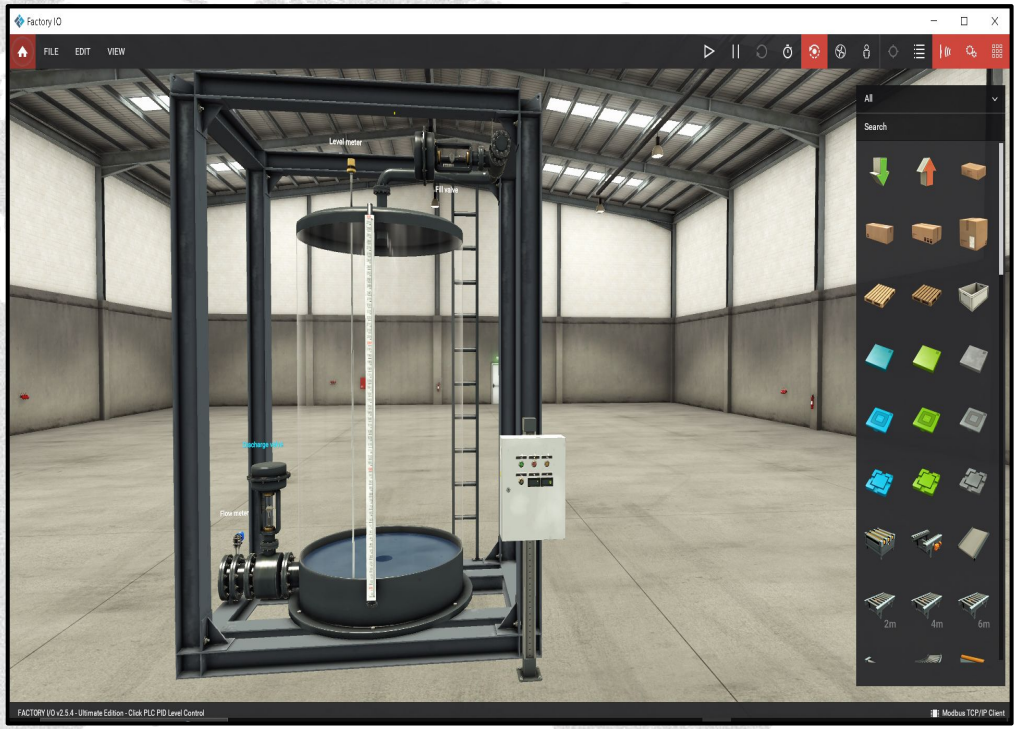


SDR Cubic

Testbed: Factory I/O, Digital Twin



Ladder logic for the water control system that factory io is using and communication with the plc



Water level control system in factory Io

Wireshark Network Packet Capture between Factory I/O and physical PLC (Modbus traffic)

Factory_IO_Cap_7_18_2023.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.218	192.168.0.5	Modbus/TCP	68	Query: Trans: 64561; Unit: 1, Func: 15: Write Multiple Coils
2	0.001851	192.168.0.5	192.168.0.218	Modbus/TCP	66	Response: Trans: 64561; Unit: 1, Func: 15: Write Multiple Coils
3	0.001938	192.168.0.218	192.168.0.5	Modbus/TCP	73	Query: Trans: 64562; Unit: 1, Func: 16: Write Multiple Registers
4	0.003461	192.168.0.5	192.168.0.218	Modbus/TCP	66	Response: Trans: 64562; Unit: 1, Func: 16: Write Multiple Registers
5	0.003571	192.168.0.218	192.168.0.5	Modbus/TCP	66	Query: Trans: 64563; Unit: 1, Func: 2: Read Discrete Inputs
6	0.004899	192.168.0.5	192.168.0.218	Modbus/TCP	64	Response: Trans: 64563; Unit: 1, Func: 2: Read Discrete Inputs
7	0.004988	192.168.0.218	192.168.0.5	Modbus/TCP	66	Query: Trans: 64564; Unit: 1, Func: 4: Read Input Registers
8	0.006411	192.168.0.5	192.168.0.218	Modbus/TCP	71	Response: Trans: 64564; Unit: 1, Func: 4: Read Input Registers
9	0.032040	192.168.0.218	192.168.0.5	Modbus/TCP	68	Query: Trans: 64565; Unit: 1, Func: 15: Write Multiple Coils
10	0.033845	192.168.0.5	192.168.0.218	Modbus/TCP	66	Response: Trans: 64565; Unit: 1, Func: 15: Write Multiple Coils
11	0.033947	192.168.0.218	192.168.0.5	Modbus/TCP	73	Query: Trans: 64566; Unit: 1, Func: 16: Write Multiple Registers
12	0.035840	192.168.0.5	192.168.0.218	Modbus/TCP	66	Response: Trans: 64566; Unit: 1, Func: 16: Write Multiple Registers
13	0.035924	192.168.0.218	192.168.0.5	Modbus/TCP	66	Query: Trans: 64567; Unit: 1, Func: 2: Read Discrete Inputs
14	0.037376	192.168.0.5	192.168.0.218	Modbus/TCP	64	Response: Trans: 64567; Unit: 1, Func: 2: Read Discrete Inputs
15	0.037555	192.168.0.218	192.168.0.5	Modbus/TCP	66	Query: Trans: 64568; Unit: 1, Func: 4: Read Input Registers
16	0.039799	192.168.0.5	192.168.0.218	Modbus/TCP	71	Response: Trans: 64568; Unit: 1, Func: 4: Read Input Registers
17	0.065217	192.168.0.218	192.168.0.5	Modbus/TCP	68	Query: Trans: 64569; Unit: 1, Func: 15: Write Multiple Coils
18	0.067363	192.168.0.5	192.168.0.218	Modbus/TCP	66	Response: Trans: 64569; Unit: 1, Func: 15: Write Multiple Coils
19	0.067483	192.168.0.218	192.168.0.5	Modbus/TCP	73	Query: Trans: 64570; Unit: 1, Func: 16: Write Multiple Registers
20	0.068902	192.168.0.5	192.168.0.218	Modbus/TCP	66	Response: Trans: 64570; Unit: 1, Func: 16: Write Multiple Registers
21	0.069063	192.168.0.218	192.168.0.5	Modbus/TCP	66	Query: Trans: 64571; Unit: 1, Func: 2: Read Discrete Inputs
22	0.070462	192.168.0.5	192.168.0.218	Modbus/TCP	64	Response: Trans: 64571; Unit: 1, Func: 2: Read Discrete Inputs

```
> Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{B2B5B2AE-4937-4CE3-A32D-DADAABB0C7EA}, id 0
> Ethernet II, Src: IntelCor_40:c9:78 (44:03:2c:40:c9:78), Dst: KoyoElec_1a:53:09 (00:d0:7c:1a:53:09)
> Internet Protocol Version 4, Src: 192.168.0.218, Dst: 192.168.0.5
> Transmission Control Protocol, Src Port: 1048, Dst Port: 502, Seq: 72, Ack: 64, Len: 19
> Modbus/TCP
v Modbus
    .001 0000 = Function Code: Write Multiple Registers (16)
    Reference Number: 0
    Word Count: 3
    Byte Count: 6
  > Register 0 (UINT16): 0
  > Register 1 (UINT16): 0
  > Register 2 (UINT16): 0
```

v Modbus
.001 0000 = Function Code: Write Multiple Registers (16)
Reference Number: 0
Word Count: 3
Byte Count: 6
> Register 0 (UINT16): 0
> Register 1 (UINT16): 0
> Register 2 (UINT16): 0

Future Work

Towards Zero Trust in Maritime systems communication and OT/ICS

- Zero-Trust Principles: Verify implicitly, Always assume breach, Use least Privilege

- **Monitoring:** Emphasize the need for creative solutions for network visibility and security monitoring specially for devices that don't support logging
- Employ machine learning **(ML)** for active anomaly detection and root-cause analysis
  - Rely on partial logging with proper enrichment
  - Testbed: implement Purdue L3/L4 functions including a variety of OT/ICS protocols
- **Identity:**
  - Testbed: integrate light-weight IAM (identity and Access Management) for OT/ICS

Thank you

Special thanks to

**Department of Homeland Security (DHS) - Cross-Border Threat Screening (CBTS) Center of Excellence,
United States Coast Guard (USCG),
RELLIS Academic Alliance**