Maritime Cybersecurity

Patching the Holes in Control System Cybersecurity

WRITTEN BY

Joe Weiss, PE, CISM, CRISC

Scott Lynn

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

Abstract

Current US Coast Guard cybersecurity regulations are intended to provide a framework which, if followed, will reduce the vulnerability of the maritime industry to malicious cyberattacks and unintentional cyber incidents. However, those regulations do not provide the depth required to fully protect Operational Technology (OT) control systems. Likewise, current cybersecurity education omits much of the curriculum needed to prepare practitioners for existing real-world threats and demonstrated actual cyber incidents.

This paper is intended to:

1. Summarize lessons learned from land-based and maritime organizations about threats to OT
2. Identify current OT vulnerabilities in the maritime industry.
3. Make specific recommendations which, if addressed via training, practice and regulation, can reduce maritime vulnerability to cyber incidents and cyber threats.

Traditional Information Technology (IT) hardware, software and networking practices are necessary. However, as illustrated by control system cyber incidents affecting military and commercial ships and ports, there are holes needing filling. This paper will discuss some of those holes and suggest practical and regulatory changes to improve maritime cybersecurity.

We submit these recommendations in the hope that the information in this paper might be used by governments, ports and shipping companies, and others to preemptively ameliorate OT cyber threats in our rapidly changing world.

INTRODUCTION

Maritime cybersecurity regulations cover IT and OT networks and data. But they miss where the rubber meets the road – control system cybersecurity.

Coast Guard Maritime cybersecurity requirements are given in the Code of Federal Regulations (33 CFR Part 101 Subpart F - Part 101: Maritime Security: General, Cybersecurity).[1] The regulation provides definitions and requirements for maritime cybersecurity, focused on network security to address data threats from manipulation and exfiltration. However, issues unique to maritime industrial control systems can be improved in three sections: Cybersecurity Definitions, Cybersecurity Officer Qualifications and Device Security.

This is not an attempt to “bash” either regulations or staff. Rather it is our effort to apply lessons learned from land-based cyber incidents to the maritime world. Note that these issues are also common to onshore power plants, substations, water treatment plants, and manufacturing.

In the following sections we will look at maritime control system cyber incidents which illustrate holes in the CFR and training which need to be patched. Adversarial nation-states are aware of these control system cybersecurity gaps and their continuing vulnerability. The United States therefore needs to expeditiously patch the holes in maritime cybersecurity and related regulations.

Note that this paper only addresses ships and ports. It does not address other vulnerable maritime facilities with control systems such as canals, locks, etc.

[1] https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101 , Subpart F—Cybersecurity.

NAUTICAL OT

Maritime (port) control systems

OT is technology that monitors and controls physical processes. OT is Separate from IT in that the latter deals purely in data while OT typically deals in physics (physical and electrical processes). Ports typically contain multiple types of OT: loading and unloading equipment, pipelines, railroads, fuel storage, fueling facilities, warehouses, electric substations, water treatment facilities, etc. The technologies in these facilities use control systems containing process sensors, actuators, Programmable Logic Controllers (PLCs), Human-Machine Interfaces (HMIs), pumps, motors, turbines, relays, transformers, etc.

Maritime (ship) control systems

Ships have been described as “powerplants and electric distribution substations with rudders”. Maritime control systems include cargo handling, HMIs, propulsion/steering, process sensors, and actuators. A large ship can contain 30,000-50,000 process sensors.

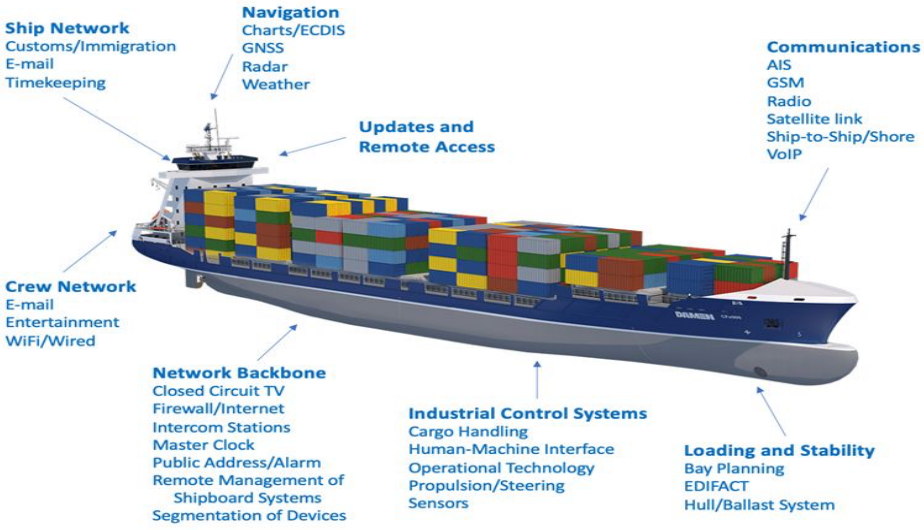


Figure 1 Cybersecurity issues affecting ships

The control systems used on ships are often the same as those used in port and other onshore facilities, and control system communication protocols are also common to ships and port facilities. For example, the same type of Siemens controllers compromised in the Stuxnet attack are also used in ships and shore facilities.

At sea are other applications of OT. The Safety of Life at Sea (SOLAS) convention requires most cargo vessels to employ Global Maritime Distress and Safety Systems (GMDSS). Figure 2; The diagram below shows how many of those devices depend on the Global Navigation Satellite System (GNSS).[2]

There are many well documented examples of various systems on vessels malfunctioning during or after GNSS interference. This includes systems which are not primarily for navigation. These issues impact end-user equipment with cybersecurity vulnerabilities as well as navigation vulnerabilities. Their assessment and management must be considered within cybersecurity frameworks. The masters of these vessels are dealing with more than the loss of access to a navigation source. They also suffer the consequences of invalid data being used by a variety of digital systems which take input from GPS data"[3]

---

[2] Navigation Center, United States Coast Guard, U.S. Department of Homeland Security, GMDSS Compliance Requirements, https://www.navcen.uscg.gov/gmdss-compliance-requirements

[3] "Impacts of GNSS Interference on Maritime Safety", A special report by the RIN Maritime GNSS Interference Working Group Digital Report, Page.9, January 2026

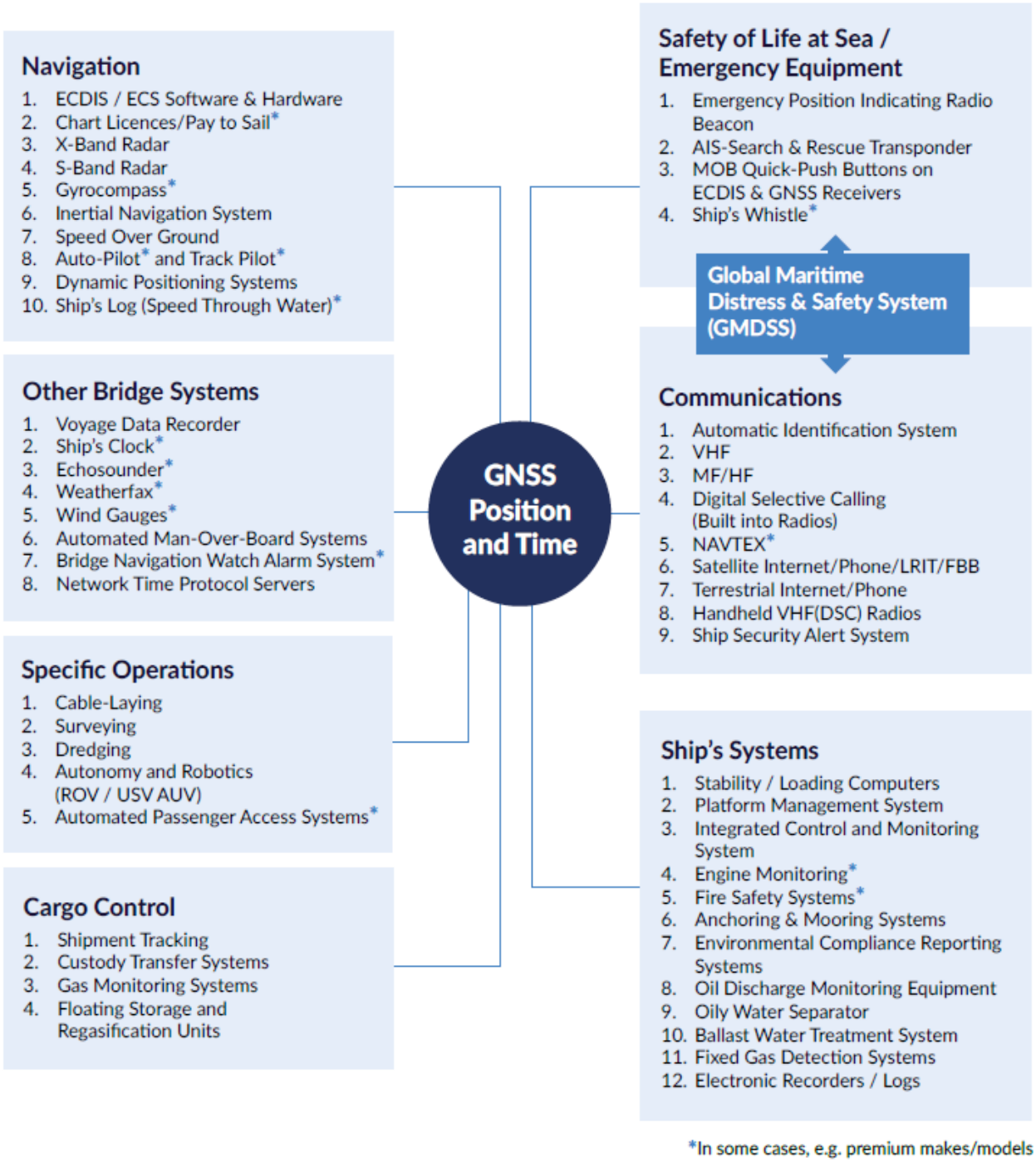


Figure 2; Devices depending on the Global Navigation Satellite System (GNSS)

MARITIME CYBER VULNERABILITIES

Computers are increasingly under attack, whether in cold wars, hot wars, or for criminal purposes.

Cyber incidents have been defined as “events that could jeopardize the confidentiality, integrity, or availability of digital information or information systems.”[4] They typically take the form of electronic communication between systems, or between systems and people (as when users interact with displays), that can affect the traditional IT triad of Confidentiality, Integrity, or Availability.

According to Anderson[5], security engineering is about building systems that remain dependable in the face of **malice, error, or mischance.**” Therefore, cyber incidents include both malicious and unintentional incidents. Moreover, the 2010 Stuxnet attack against the Iranian centrifuge facility at Natanz demonstrated that a sophisticated cyberattack can be made to look like equipment malfunctions. This means they cannot be expeditiously identified as a cyberattack.

There are various types of cybersecurity issues to which the maritime world is vulnerable, onshore or offshore. This section discusses some examples. Again, note that these same control system issues affect other critical infrastructure sectors.

Aurora

Aurora is an attack on electric systems caused by opening and closing breakers connecting motors and generators out of phase with the local grid (Figure 3). The lack of synchronization creates damaging mechanical and electrical forces on alternating current (AC) equipment and electric transformers. While Aurora can be

---

[4] A Unified Message for Reporting to the Federal Government, Department of Homeland Security, accessed 3/3/2025, https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf#:~:text=A%20cyber%20incident%20is%20an%20event%20that,to%20report%20all%20cyber%20incidents%20that%20may

[5] Anderson, Ross, 2008, Security Engineering: A Guide to Building Dependable Distributed Systems

triggered by maliciously reclosing breakers out-of-phase, it can also be unintentional. This means a physics-based cyber event cannot be detected by traditional cyber defense. This makes Aurora an ongoing gap in protection of shipboard and land-based power grids.

In 2007, Idaho National Laboratory tested the Aurora threat using a 2.5MW diesel generator. The test destroyed the generator, with a video of the test available online.[6]

Figure 3 Aurora demonstration at the Idaho National

There have been several domestic and international Aurora events that have damaged critical equipment, including on ships. As ships often use shore power when in port, the ships are directly connected to the electric utility's distribution grid.

[6] Muckrock, 2016, Aurora Test Footage, https://www.youtube.com/watch?v=LM8kLaJ2NDU

This makes them vulnerable to Aurora incidents onshore. At sea, numerous ship-board systems use protective relays to protect AC-based systems. Naval Facilities Command (NavFac) recognized the Aurora threat to shore facilities and military bases. This resulted in the Navy Mission Assurance Division developing an Aurora hardware mitigation program.

Note that the North American Electric Reliability Corporation (NERC)'s Critical Infrastructure Protection (CIP) cybersecurity standards[7] only address electric transmission. Electric distribution serving ports is explicitly excluded from the NERC CIPs. This means there are no legislated mandatory cybersecurity requirements to address cybersecurity threats affecting shore facilities.

Shipboard Aurora incident example

A navy vessel leaving San Diego to Hawaii suffered an Aurora incident. As the ship was leaving the port, the #1 generator tripped off-line, which automatically started the back-up emergency diesel generator. As there was no feedback in the control room that the emergency generator had started, a sailor closed the breaker to get the emergency generator online without having synched it first. The breaker was closed out-of-phase, causing a large AC induction motor spike that, in turn, "fried" all of the solenoids on the ventilation fans. As a result, there was no control of the fans until the ship reached Hawaii.

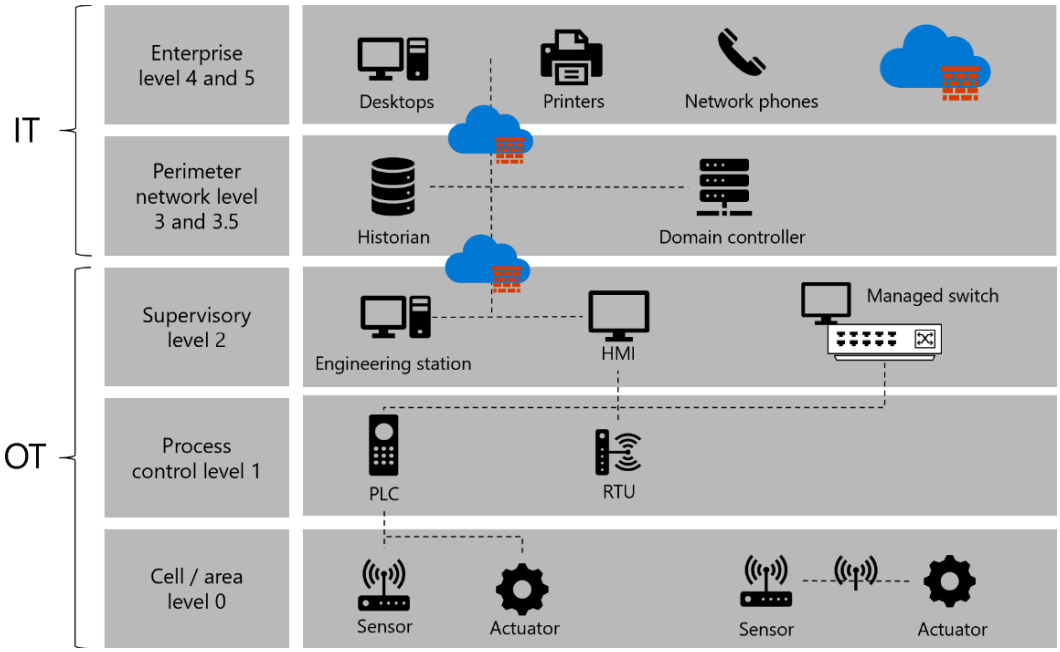
Level 0 Device Vulnerabilities

In the early 1990s, a group at the Purdue Laboratory for Applied Industrial Control developed a framework for describing different levels of automation. Known as the Purdue Reference Model, it describes network automation architecture in levels. [8]

---

[7] NERC, Critical Infrastructure Protection, https://www.nerc.com/standards/reliability-standards/cip

[8] Microsoft, Defender For IOT And Your Network Architecture, https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/best-practices/understand-network-architecture, accessed 4/3/2026.



It is important to know this about Purdue Model organization:

- Level 0 devices measure and directly control physical processes. These devices include process sensors, motors, actuators, and safety systems. If they are "smart" devices with embedded firmware, they may be a “Level 0 / 1” combination.
- For safety and control purposes, Level 0 /1 devices are assumed to be trustworthy, authenticated, and respond within specific time constraints.
- IT security is typically focused at the network or enterprise level, between Levels 2 and 5. Firewalls and security are customary here but not at Level 0 / 1.
- This means that malware or hacks in Level 0 / 1 devices can send signals to control devices or data displays without being detected.

Because most Level 0 devices lack authentication, integrity checks, or cyber forensic capabilities, both unintentional issues (sensor drift, miscalibration) and malicious actions (signal spoofing, counterfeit hardware) can lead to dangerous physical outcomes. In addition, even modern Level 1 devices with embedded security features are often deployed with those features disabled. But because Level 2 or higher devices trust them, the system cannot reliably distinguish genuine process data from manipulated or spoofed inputs.

An example of how process sensor networks operate can be found in 4-20 milliamp (mA) loops (Figure 4)[9]. PLCs and other controls interpret that 4-20mA signals as a range of pressures, temperatures, speeds, or other physical conditions, and respond to maintain preset conditions.

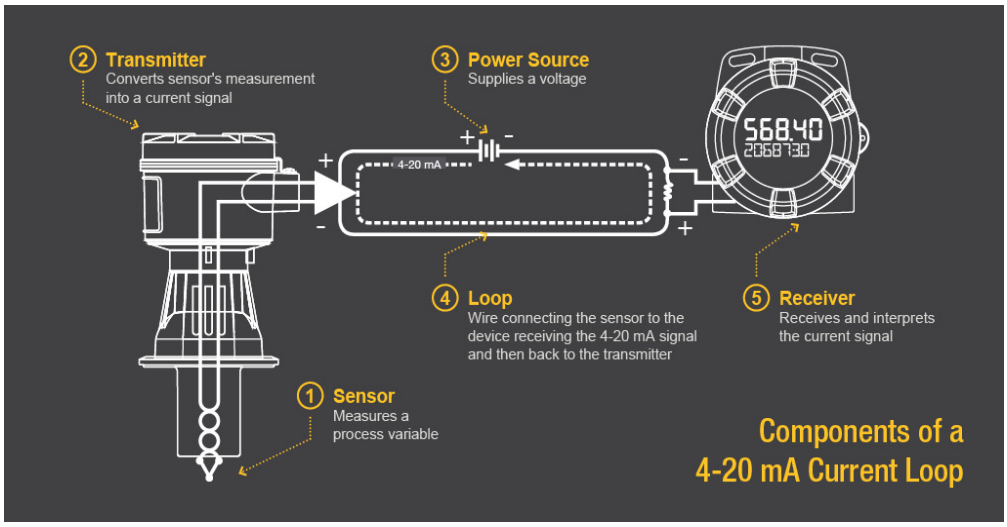


Figure 4

If an attacker can inject or attenuate current on the 4-20mA loop, they can change the sensor displays or system responses. For example, if the HMI reports 6mA when the actual measure is at 16mA, a potentially unsafe condition would appear “normal” on the operator's HMI.

Level 0 outputs or setpoints can be changed unintentionally or maliciously so the sensors read properly but do not actuate an alarm or trip signal. Systems using 4-20 mA systems have no way to validate that the electrical signal matches physical reality without starting at the physics level of the sensor[10]

[9] https://www.predig.com/indicatorpage/back-basics-fundamentals-4-20-ma-current-loops
[10] Joseph Weiss, Michael Hood, Nadine Miller, James Bret Michael, IEEE Computer, “Using Machine Learning to Work Around the Operational and Cybersecurity Limitations of Legacy Process Sensors”, Novembetr 2022.

When this kind of event occurs, a sensor might indicate 100° F when the actual process is at an unsafe 300° F, a depth sounder might read 50ms when the depth is actually 20m, or a speed signal might be higher or lower than displays indicate.

Adversarial nation-states are aware of the Level 0 gap and the reticence by cyber defenders to address it.

Incidents involving control systems and components are more plentiful and impactful than most observers expect, with more than 17 million control system cyber incidents (mostly unintentional) directly resulting in more than 30,000 deaths and tens of billions of dollars in damage.[11] (As of April 2026, the number is over 20 million). Stuxnet and Aurora attacked control system devices. The engineering-based cyberattacks did not involve the Internet, Windows, or OT networks to carry out the attacks. Consequently, these incidents were not identifiable by network cyber forensics and would not fall under the Chief Information Security Officer's (CISO) domain. Consequently, most of these incidents would not be addressed by existing government and industry cyber security guidance. Note that it has been speculated that, in a conflict, China may do the same to more than the 600 large Chinese-made transformers in the US electric grid[12] and in Chinese-made Battery Energy Storage Systems[13].

Until the OT network-focused regulators and practitioners are willing to address engineering-based incidents and attacks, critical infrastructure cannot be secured. It is also evident that monitoring the process sensor signals at the physics layer would have identified most of the incidents regardless of cause. This is a governance failure masquerading as a vocabulary issue. “If you define ‘cyber incident’ through

---

[11] https://www.controlglobal.com/blogs/unfettered/blog/21438102/more-than-17-million-control-system-cyber-incidents-are-hidden-in-plain-sight

[12] Presidential Executive Order 13920, May 1, 2020, Securing the United States Bulk-Power System, https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system

[13] Weiss, Joe, “How Vulnerable to Cyber Attacks are Battery Energy Storage Systems” T&D World, April 2025.

an IT breach lens, you will miss (or dismiss) the incidents that actually move risk and degrade continuity lifelines by disrupting physical processes. Control-system cyber incidents include electronic/automation failures across sensor signals, control logic, firmware and field device communications. Many are non-malicious yet still produce loss of view, loss of control, equipment damage, and safety/environmental consequences.[14]

Diagnosing Level 0 Incidents

Diagnosing Level 0 incidents is often challenging because the causes are difficult to diagnose. It can be difficult to tell if an incident was accidental or malicious. Therefore, there are two tasks to address when resolving incidents. The first is what device(s) failed and how they failed. This task is performed by maintenance or engineering. The second is whether the device or devices are connected to a network where it could be remotely accessed. This task is performed by the network security staff to determine if there were any suspicious data transmissions.

Examples of Level 0 incidents:

Note that the following are not all failures of Level 0 components but include incidents resulting from improper use of data from Level 0 devices. They illustrate what can happen if Level 0 devices are compromised.

Stuxnet: Perhaps the most famous Level 0 incident was the attacks on Iran's nuclear centrifuges. The Stuxnet Worm damaged Iranian centrifuges by rapidly changing causing motor speeds (Level 0 devices) to rapidly change. At the same time, the worm prevented the SCADA system from displaying those speed changes. The attack appeared to be caused by equipment malfunctioning rather than what it really was: a cyber-attack affecting control devices[15].

---

[14] https://www.controlglobal.com/blogs/unfettered/blog/55360902/ot-cybersecurity-is-a-governance-failure-masquerading-as-a-vocabulary-issue, March 2, 2026

[15] Langner, Ralph, 2013, The Langner Group, To Kill a Centrifuge, https://archive.org/stream/to-kill-a-centrifuge/to-kill-a-centrifuge_djvu.txt

US Navy: A ship experienced engineering control system "core failures" causing the ship to lose remote control of the engineering plant multiple times. The core failures were caused by incorrect parameters associated with the Chilled Water Pump's Suction Temperature signal. Suspiciously, the signal's "low out of range" reset limit was set higher than its low alarm limit. Each time the system came online, the equipment was simultaneously in a "low out of range" and "low alarm" state. The engineering control system was unable to manage this conflict and crashed. At sea this resulted in loss of steering and throttle control on the bridge. Control was regained and maintained locally, but the ship was forced to return to port. As there was no control system cyber forensics it was not possible to determine if the incidents were unintentional or malicious.

Maersk Eindhoven: February 17, 2021, Maersk said a loss of propulsion led to hundreds of containers falling overboard from the Maersk Eindhoven in severe weather off the coast of Japan.[16]. The company reported that a loss of propulsion was the result of low engine oil pressure which triggered a safety feature causing the ship's main engine to shut down, as opposed to some other malfunction or maintenance issue. "The loss of maneuverability resulted in severe rolling with 260 containers overboard and 65 containers damaged on deck. "Propulsion power was quickly restored to the vessel, and the initial analysis indicates engine oil pressure triggered a safety feature, causing the engines to shut down. No malfunction or maintenance issues were identified.

EMI/RFI interference

EMI is a disruption in an electrical circuit due to electromagnetic induction or external electromagnetic radiation. It occurs when the electromagnetic fields from one device interfere with another device. RFI is a type of EMI that occurs when unwanted radio

[16] https://gcaptain.com/maersk-eindhoven-cargo-loss-engine-oil-pressure-triggered-loss-of-propulsion/

frequency signals disrupt the normal operation of electronic or communication systems. RFI disrupts wireless devices like phones and Wi-Fi by causing unwanted signals that lower performance and cause connection problems. Unsecured Wi-Fi is a cyber threat to Ethernet-based communication systems, especially in high-speed or industrial environments where it can degrade signal quality, reduce data throughput, or even cause complete communication failure. Devices such as motors and Variable Frequency Drives (VFDs) are susceptible to EMI/RFI issues. This equipment is common on ships and shore facilities.

Examples of EMI/RFI incidents

Supervisory Control and Data Acquisition (SCADA) incidents: In November 1999, the. Navy was conducting exercises during which two commercial Spectrum users experienced severe EMI to their SCADA wireless networks. As a result, the water and electric utilities were unable to remotely actuate critical valve openings and closings. This necessitated sending technicians to remote locations to manually open and close water and gas valves.[17]

Pipeline incident: In the late 1980s, RF energy from a naval radar impacted the SCADA system at a plant located approximately one mile from the Den Helder naval port. The RF energy caused a large 36-inch gas flow-control valve to open and close at the same frequency as the radar scanner. The resulting changes in pressure created shock waves that traveled down the pipeline. This caused a pipeline failure and large gas explosion in the (roughly) 36-inch diameter pipeline.

---

[17] Muhlheim, M; Belles, R; Killough, S; Anderson, L et.al., Oak Ridge National Laboratory, Criteria for Determining the Safety of Wireless Technologies at Nuclear Power Plants, Technical Letter Report TLR-RES-DE-2023-006, U.S. Nuclear Regulatory Commission https://info.ornl.gov/sites/publications/Files/Pub181088.pdf#:~:text=928.5%20MHZ%20%5BG.9%5D.%20The%20San%20Diego%20County,Electric%20(SDGE)%20companies%20were%20unable%20to%20remotely

Two maritime and port cases additionally demonstrate the impacts of EMI/RFI interference[18]. In Europe, a 30-meter-high crane dropped its load into a harbor when RFI generated by dockworkers using their walkie-talkies inadvertently opened the crane jaws. In the US, several ferries crashed into their piers because their propeller pitch remote control was interfered with by a local radio transmitter.

GPS impacts

GPS provides geolocation and time information to a GPS receiver anywhere on or near the Earth where signal quality permits.[4] It does not require the user to transmit any data, and operates independently of any telephone or Internet reception, though these technologies can enhance the usefulness of the GPS positioning information.[5] GPS provides critical positioning capabilities to military, civil, and commercial users around the world. Although the United States government created, controls, and maintains the GPS system, it is freely accessible to anyone with a GPS receiver.[6]

GPS and other Global Satellite Navigation Systems (GNSS) work through trilateration. Satellites broadcast precisely timed signals from 12,000 miles above the earth, receivers measure the time delays and then calculate geographic position. The signals are weak, about the same power as a car's dome light. GNSS is effectively “sensor input” (Level 0) to navigation and control systems.

In addition to navigation, power grids rely on GPS. Phasor Measurement Units (PMUs) monitor grid stability across vast distances. These devices must time-stamp measurements with microsecond precision to detect phase angle differences. If an

---

[18] Mardiguian, M. (2025). What Is EMI/EMC? An Introduction to Interference Control. In: Electromagnetic Compatibility. Springer, Cham. https://doi.org/10.1007/978-3-032-02688-0_1

attacker can manipulate the timing reference, they can make destabilizing events invisible.

Civil GPS signals have no cryptographic authentication. This was intentional - the system was designed for global accessibility. Anyone with a receiver can use it. No keys, no verification. The architecture assumes GPS signals are valid and come from satellites.

Many critical systems use GPS as their timing source because it is convenient and free. But GPS signals are extraordinarily weak. Malicious or unintentional transmissions can overpower the authentic signals and have in many cases.

GPS can be jammed by jammers transmitting a low-power signal that creates signal noise and fools a GPS receiver into thinking the satellites are not available.[19] This creates RF noise that drowns out satellite signals. This can be unintentional, as strong power sources near receivers can jam GPS signals. [20] Receivers lose lock and navigation fails, users know immediately something is wrong.

Spoofing is different - an attacker broadcasts fake GPS signals stronger than the real ones but formatted to look legitimate. The receiver sees what appears to be valid satellite data, performs its calculations, gets a position. The mathematics check out. The signal structure is correct. The receiver is doing exactly what it was designed to do by trusting mathematically valid inputs.[21] The mathematical calculations would be correct, but the results would be misleading. [22]

---

[19] Hambling, David, March 4, 2011, GPS chaos: How A $30 Box Can Jam Your Life, New Scientist, https://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life/

[20] Lomas, Chris, January 9, 2025, Flightradar24.com, GPS jamming: the benign, the bad, and the scary, https://www.flightradar24.com/blog/inside-flightradar24/types-of-gps-jamming/

[21] Cornell, Norris, January 15, 2026, LinkedIn.com, When 1,100 Flights Trust Signals They Can't Verify, https://www.linkedin.com/pulse/when-1100-flights-trust-signals-cant-verify-norris-cornell-gddwe/

[22] “Investigating Physical Consequences of Cyber-Attacks Using a Cyber-Physical Model of a Compressor Station”. In a presentation by the Sandia National Laboratory, the assumption was made the sensors were not compromised, MORS presentation, January 29, 2026,

In another case, the system receives a spoofed signal. The structure looks correct. The satellite IDs are valid. But the timing is shifted. Digital validation passes, and the attack succeeds because the system trusts the "verified" input.

GPS resilience matters both at sea and in port, as maritime GPS is used for:

1. Vessel approach and docking
2. Channel and harbor transits
3. Tug coordination
4. Crane automation and container tracking
5. Automatic Identification System (AIS) as AIS uses GPS, VHF radio and sophisticated digital processing to automatically communicate between vessels without any operator interaction.
6. Dredging and surveying
7. Offshore platform positioning

Ports are especially exposed because:

1. GPS signals are weak
2. Jamming devices are cheap
3. Spoofing can misdirect vessels
4. Dense port infrastructure can leave ships little time to respond to misdirection.

As with Level 0 incidents, GPS jamming may not be malicious, but the impacts are the same.

Examples of GPS impacts (malicious and unintentional)

MSC Antonia: The *MSC Antonia*, a Liberian-flagged container vessel measuring 304 meters in length, was traveling from Marsa Bashayer, Sudan to Jeddah, Saudi Arabia. GPS jamming caused the ship to run aground near the Eliza Shoals close to Jeddah Port on May 10, 2025.[23] Following a review of the available data, Captain Steve Bomgardner, Vice President of Shipping and

[23] Schuler, Mike, 2025, gCaptain.com, https://gcaptain.com/pole-star-confirms-gps-interference-caused-msc-antonia-grounding/

Offshore at Pole Star Global, concluded that the vessel's AIS was subject to GPS jamming, where threat actors introduced fake signals that gave the crew inaccurate positioning information. "In reviewing the data, we also concluded that the vessel's AIS was subject to GPS jamming," said Bomgardner. "This happens when a threat actor introduces fake signals which the GPS unit picks up as genuine, therefore giving the vessel's crew an inaccurate picture of where they are."

The incident occurred amid an alarming increase in GPS interference in the region. On May 9th, the day before the grounding, the UK Maritime Trade Operations (UKMTO) said it had received a number of corroborating reports from vessels experiencing GPS interference affecting navigation systems in the Red Sea, with disruptions lasting several hours. According to Windward's Q1 report, vessels are now experiencing position "jumps" averaging 6,300 km, a significant increase from 600 km in Q4 2024.[24] The Red Sea area, particularly near Sudan, has become a major hotspot, with more than 180 vessels affected in Q1 2025 alone. While Bomgardner noted that this particular jamming incident was "unsophisticated" compared to other recent attacks, he stressed that "any form of electronic warfare, no matter how sophisticated, presents a danger to the very seafarers that our economies rely upon." "I've seen firsthand how the surge in jamming, spoofing, and other AIS tampering has made our oceans more dangerous," said Bomgardner.

United States Navy: According to an article in the New Scientist, a GPS outage happened when the Navy accidentally jammed GPS signals in downtown San Diego in 2007.

2026 Iran War: During the attack on Iran in the early days of March, 2026, over 1,100 ships were affected by GPS hacking. According to Wired Magazine, "Ships

---

[24] Marinelink.com, April 9, 2025, Windward Tracks Change to GPS Jamming Hotspots, https://www.marinelink.com/news/windward-tracks-change-gps-jamming-524514

have been made to appear as if they were inland on maps, including at a nuclear power plant".[25]

Training

With the implementation of the Maritime Transportation Security Act (MTSA), many new regulations will take effect. They will significantly improve maritime cybersecurity. However, there appear to be some gaps in "§101.625(e) Cybersecurity Officer Qualifications" with respect to OT security. This section discusses them and the opportunity for personnel to fill those gaps.

Maritime Operational Technology is typically maintained by Maintenance and Engineering. With a focus on mechanical operation, these two disciplines are typically oriented toward reliability than security. Conversely, IT personnel are focused on networks and security rather than the physics of OT.

There is a growing field of maritime cybersecurity, but practitioners need to understand both IT and maritime OT functions. While some cybersecurity training does include OT there is typically a gap between IT and OT protocols and systems. Addressing this gap requires specific training on OT cybersecurity and an understanding of how OT systems work.

Again, Stuxnet was an example of how hard it might be to identify a cyberattack on OT having cyber origins instead of equipment malfunctions.[26] Understanding how both IT and OT systems communicate, and how OT operates, gives security personnel a better chance at identifying cyber-attacks. This is a challenge that might be overcome by IT training with OT understanding.

---

[25] Burgess, Matt, March 3, 2026, Wired.Me, Attacks on GPS Spike Amid US and Israeli War on Iran, https://www.wired.me/story/attacks-on-gps-spike-amid-us-and-israeli-war-on-iran.
[26] Langner, Ralph, 2013, The Langner Group, To Kill a Centrifuge, https://archive.org/stream/to-kill-a-centrifuge/to-kill-a-centrifuge_djvu.txt

Level 0 Control System Cyber Security Training

Government and industry are not teaching, distinguishing, or addressing Level 0 cybersecurity. Much of today's OT cybersecurity training assumes a security posture at Level 0 that simply does not exist.

Focusing on cyber mechanisms that only apply at higher Purdue levels leaves a critical blind spot in the protection of the physical process itself. Level 0 cybersecurity training is needed, or the foundation of physical operations will remain vulnerable.

The US needs commercial and government organizations to address the unique cybersecurity issues at Level 0. This means root cause analyses need to extend beyond component failures and programming areas to investigate possible malicious causes.

Serial Network Cybersecurity Training

Cybersecurity training is typically built around Ethernet communication. It usually does not cover serial communication and compensating controls for serial communication protocols. However, serial networks still make up about 60–80% of shipboard operational systems. Because many standards were designed around serial buses, the percentage is higher (often 70% to 90%) in navigation and sensor networks. These networks are primarily Modbus and CAN bus[27], which have very limited cybersecurity capabilities.

To be effective, IT personnel managing security must specifically be trained in OT serial communication.

---

[27]Gary Kessler, "The CAN Bus in the Maritime Environment – Technical Overview and Cybersecurity Vulnerabilities", TransNav, Volume 15, Number 3, P.531-540, September 2021.

RECOMMENDED MARITIME CYBERSECURITY MEASURES

As has been discussed, both shipboard operation and SOLAS systems rely on both computer technology and automated OT. To ensure their safety, the United States Government CFRs contains rules regarding Maritime Cybersecurity. This section discusses those regulations, areas which are vulnerable to OT cyberattack, and makes recommendations on how these vulnerabilities might be addressed.

Note that some of the recommendations specifically mention OT. The sheer volume of OT on board ships raises the importance of adding OT to existing cyber definitions or creating new definitions. These will be shown ***underlined, in bold Italics***:

§101.615 Definitions

Cyber-incident

Cyber-incident means an occurrence that actually jeopardizes the integrity, confidentiality, or availability of information or an information system ***or operational technology***, or actually jeopardizes an information system ***or operational technology*** via ***malice, error or mischance***.[28]

Cybersecurity Officer

Cybersecurity Officer - or CySO, means the person designated as responsible for the development, implementation, and maintenance of the cybersecurity portions of the Vessel Security Plan (VSP), Facility Security Plan (FSP), or Outer Continental Shelf (OCS) FSP, and for liaison with the Captain of the Port (COTP) and Company, Vessel, and Facility Security, ***Engineering and Maintenance Officers***. The owner or operator may designate an alternate CySO(s) to assist with the duties and responsibilities of the CySO, including during periods when the CySO is on leave,

[28] Malice, error or mischance" from **Security Engineering: A Guide to Building Dependable Distributed Systems:** Ross Anderson, Ph.D., *"security engineering is about building systems to remain dependable in the face of* ***malice, error, or mischance."*** This would include malicious and unintentional cyber incidents

unavailable, or unable to perform their duties. Hereafter, “CySO” will refer to both the CySO and the alternate CySO(s), as applicable.

Adding “Engineering and Maintenance” gives the CySO the authority to interact with those directly involved with Operational Technology and to ensure that even Level 0 Operational Technology threats are assessed and understood.

Cybersecurity Plan

Cybersecurity Plan means a plan developed as a part of the VSP, FSP, or OCS FSP to ensure application and implementation of cybersecurity ***and Operational Technology*** measures designed to protect the owners' or operators' systems and equipment, as required by this part. A Cybersecurity Plan is either included in a VSP, FSP, or OCS FSP; as an annex to a VSP, FSP, or OCS FSP; provided in a separate submission from the VSP, FSP, or OCS FSP; or addressed through an Alternative Security Program.

OT includes controllers, communication devices, motors, actuators, hydraulics, etc. These devices contain communication devices and ports such as USB plugs (currently banned on US Navy bases). This definition ensures that the large scope included in “OT” is included in protecting ship and shore facility assets. By reference, adding OT to the definition of a Cybersecurity Plan adds protecting OT to:

§ 101.620(4) Owner or operator duties.
§ 101.625(d)(1) Cybersecurity Officer responsibilities.
§ 101.630(a) General Cybersecurity Plan.
§ 101.630(c)(14) Format: Cybersecurity Assessment.
§101.650(e)(1) Cybersecurity measures
§101.665 Noncompliance, waivers, and equivalents.

Cybersecurity vulnerability

Cybersecurity vulnerability means any attribute of hardware, software, ***operational technology***, process, or procedure that could enable or facilitate the defeat of security controls.

Firmware

Firmware means computer programs (which are stored in and executed by computer hardware ***and operational technology***) and associated data (which is also stored in the hardware) that may be dynamically written or modified during execution.

This modification ensures that firmware in networked OT is included in the definition. As this extends to process sensors, it is a significant change.

Hardware

Hardware means, collectively, the equipment that makes up physical parts of a computer ***or networked operational technology***, including its electronic circuitry, together with keyboards, readers, scanners, and printers.

The definition for hardware should be expanded to include networked control systems and their components as these include networked process sensors, actuators, PLCs, pumps, motors, protective relays, transformers, turbines, etc.

Network

Network means information system(s) implemented with a collection of interconnected components. A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to allow data sharing. A network consists of two or more computers ***and / or operational technology*** that are linked in order to share resources, exchange files, or allow electronic communications.

This revision ensures that OT and networkable OT devices are specifically included in the definition of a network

Operational Technology (OT)

OT means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a change through the monitoring or

control of devices, processes, and events***, Operational Technology specifically includes Level 0 devices as defined under the Purdue Enterprise Reference Architecture – (PERA) model.***

This ensures that level 0 devices, which are increasingly networkable and contain their own firmware, are accounted for in the definition of OT.

Operational Technology Assessment

To highlight the importance of protecting OT and the magnitude of the job, we recommend adding the term "***Operational Technology Assessment***, meaning the appraisal of the risks facing the OT system, whether in port or at sea.

Similar to Cybersecurity Assessment, the purpose of this modification is to specifically identify risks associated with ship and port OT.

" with the definition meaning the appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations, or society, and includes identification of relevant vulnerabilities and threats and determining the extent to which adverse circumstances or events could result in operational disruption and other harmful consequences.

Cybersecurity Officer, or CySO, means the person designated as responsible for the development, implementation, and maintenance of the cybersecurity and Operational Technology Security portions of the Vessel Security Plan (VSP), Facility Security Plan (FSP), or Outer Continental Shelf (OCS) FSP, and for liaison with the Captain of the Port (COTP) and Company, Vessel, and Facility Security Officers.

§101.625 Cybersecurity Officer

The following sections are focused on adding protection to specific known vulnerabilities.

§101.625(d) Responsibilities

Following are recommendations with respect to CySO functions. While we make specific recommendations, our intent is only to highlight certain areas for reference. This is not an attempt to change specific regulations but rather introduce functional equivalents to address control system issues.

Subpart F does not address the organizations other than network security which need to be involved in developing control system cybersecurity policies and training. Two extremely important ones are Engineering and Procurement. Critical operational functions not under the purview of network security such as propulsion, navigation, ballasting, etc. can be affected by control system cyber threats. Moreover, Subpart F focuses on the cyber impacts on ships, not the ship's cyber impacts on shore facilities.

Modify "§101.625(d) Responsibilities" as follows:

NEW The CISO will work with the local electric utilities to ensure that port distribution substations serving the ports have addressed Aurora[29]

This will ensure ports are not subject to Aurora attacks in either transmission or distribution systems.

NEW Following equipment-related incidents or failures, work with engineering to determine if a cyberattack could have caused the incident and work to remediate any vulnerabilities found.

---

[29] J. Weiss, J. B. Michael and M. T. Swearingen, "Physics-Based Cyberattacks Against Electric Power Grids and Alternating Current Equipment," in *Computer*, vol. 58, no. 10, pp. 157-161, Oct. 2025,

NEW Expand the responsibilities of Cybersecurity Officers under "§101.625 Cybersecurity Officer" to include working cooperatively with engineering and maintenance to investigate for underlying cyber causes to OT failures.

These should help identify if Cyber Incidents are caused by "bad actors".[30]

§101.625(e) Qualifications

This section[31] provides qualifications for the ship's Cybersecurity Officer (CySO). The current regulation is primarily focused on addressing data manipulation and exfiltration threats via Ethernet networks. It does not address cybersecurity issues unique to control system OT.

Specific cybersecurity gaps include lack of cybersecurity, authentication, and cyber forensics in process sensors and actuators (Purdue Reference Model Level 0 devices)[32], the Aurora vulnerability, Electromagnetic Interference (EMI)/Radio Frequency (RFI) interference, Global Positioning System (GPS) issues, and lack of adequate control system cybersecurity training.

Therefore, current regulations leave open known vulnerabilities of OT networks and control systems. Therefore, we recommend the measure in the following section, shown ***underlined, in bold Italics***:.

"The CySO must have general knowledge, through training, education, or equivalent job experience, in the following:

(1) General vessel, facility, or OCS facility operations and conditions ***including control systems*;**

---

[30] Weiss, 2025, Who's in Charge of OT Security?, Sam Houston State University, Institute for Homeland Security, https://ihsonline.org/Portals/0/Tech%20Papers/2024_Papers/Weiss_Whos_in_Charge_of_OT_Security.pdf?ver=dDp8PytV0TTz8UqIu687gg%3D%3D

[31]:90 FR 6447, Jan. 17, 2025, Code of Federal Regulations, Part 101—Maritime Security: General, Subpart F—Cybersecurity, https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101

[32] Purdue Reference Model

(4) The vessel, facility, or OCS facility's Cybersecurity Plan, ***including for control systems***;

(8) Instruction techniques for cybersecurity training and education, including ***control system-specific issues;***

(10) Current cybersecurity threat patterns and KEVs (Known Exploited Vulnerabilities);

(12) Conducting and assessing cybersecurity drills and ***exercises which include control systems.***

§101.650 Device security

§ 101.650(b) Device security measures.

NEW: We recommend specifying non-Ethernet-connected devices (process sensors, actuators, motors, etc., unless the system employing them is isolated (firewalled) from connection to other networked systems.

Adding this requirement will reduce the exposure of OT devices to malware infiltration.

§ 101.650(i) Physical Security

NEW We recommend that any calibration equipment not to be allowed to connect to the internet.

Many calibrators connect to the internet, rendering the Level 0 devices they calibrate to miscalibration and / or other malware. While this may make documenting calibration information easier, it also opens a path for malware to attack the calibrator and the device being calibrated.

Other

Physics level monitoring and calibration.

Monitoring at the physics level is needed to ensure critical process sensors or control devices have not been corrupted.[33]

Education

This section does not address current regulations, but rather background needs for preparing maritime personnel. Hence the naval academy, maritime academies, engineering and maritime trade schools would serve the industry well by adding the following to their curriculum.

- Training course in control system cybersecurity, specifically including Level 0 devices.
- In forensic evaluation of control system incidents as being cyber-related.

[33] J. Weiss, M. Hood, N. Miller, C. Potorieko and J. B. Michael, "Using Machine Learning to Work Around the Operational and Cybersecurity Limitations of Legacy Process Sensors," in Computer, vol. 55, no. 11, pp. 106-111, Nov. 2022, doi: 10.1109/MC.2022.3200076, https://ieeexplore.ieee.org/document/9928204.

CONCLUSION

This paper combined land-based control system cybersecurity lessons learned and maritime world realities, with a goal of offering policy recommendations based on current security state-of-the-art practices. The threats originated on shore and are rapidly spreading to the seaborne world. We hope that applying the knowledge gained on shore will also help ships and port facilities enhance their cybersecurity.

As threats evolve, we will continue to update recommendations. In the meantime, we trust that passing these lessons along will help America's Maritime Industry protect itself against threats as widespread as our world's oceans.

AUTHOR BIOGRAPHIES

Joe Weiss
Joe Weiss is an expert on control system cyber security. He has published over 100 papers on instrumentation, controls, and diagnostics including chapters on cyber security for Electric Power Substations Engineering, Securing Water and Wastewater Systems, and Data Center Handbook. He coauthored Cyber Security Policy Guidebook and authored Protecting Industrial Control Systems from Electronic Threats. Mr. Weiss has made numerous presentations to various government and industry organizations. In February 2016, Mr. Weiss gave the keynote to the National Academy of Science, Engineering, and Medicine on control system cyber security. He has conducted SCADA, substation, nuclear and fossil plant control system, water system, and other sector vulnerability and risk assessments and conducted short courses on control system security. He has amassed a database of more than 18 million control system incidents. He is an ISA Life Fellow, Emeritus Managing Director of ISA99, a Ponemon Institute Fellow, and an IEEE Life Senior Member. He was featured in Richard Clarke's book- Warning – Finding Cassandras to Stop Catastrophes. He has patents on instrumentation, control systems, and OT networks, is a registered professional engineer and has CISM and CRISC certifications. He is a member of Control's Process Automation Hall of Fame.

Scott Lynn
Scott Lynn is a Project Manager at Sam Houston State University's Institute for Homeland Security. Scott earned BAs in Environmental Studies and Economics at the University of California, Santa Barbara and a Master's degree at Arizona State University (solar energy). He is based in Ventura, California.

Scott spent most of his career in project engineering, sales engineering and management roles. His focus was capital equipment projects, primarily to improve efficiency by automating manufacturing, packaging and logistics. This gave him experience in virtually all manufacturing sectors, as well as with electric and water utilities. It also gave him a broad view of various company's automation security postures. He has enjoyed the intersection of engineering and dealing with customers and the opportunity to "translate" technical concepts to the "normal English" used by customers.

Scott currently manages research contracts for the Institute.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

Weiss, J. (2026). Maritime Cybersecurity: Patching the Holes in Control System Cybersecurity. (Report No. 2026 - 1040). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/BPWY5

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY