INSTITUTE FOR HOMELAND SECURITY


# The Need for Interdisciplinary Programs for Control System Cybersecurity

Joseph Weiss

# The Need for Interdisciplinary Programs for Control System Cybersecurity

Joseph Weiss, PE, CISM, CRISC
Applied Control Solutions, LLC

## Acknowledgements

The author gratefully acknowledges the following at Sam Houston State University for their support and review for preparing this paper.

Recayi (Reg) Pecen, Ph.D., Quanta Endowed Professor, Department of Engineering Technology at Sam Houston State University

Shannon Lane, Ph.D., Program Manager, Research, Institute for Homeland Security

Scott Lynn, Project Manager, Research, Institute for Homeland Security

Robert Crane, Program Executive for Energy Security, Institute for Homeland Security

The author also gratefully acknowledges contributions from colleagues from many organizations, too many to name.

## Abstract

Operational Technology (OT)/Control Systems support the critical infrastructures of electric power in traditional and renewable energy systems, water, oil/gas, chemicals, manufacturing, pipelines, rail, maritime, building controls, food, agriculture, and defense. There is a convergence of highly integrated automation sharing constructs with Information Technology (IT). As opposed to business IT cybersecurity, control system cybersecurity is still a developing area. Control system cybersecurity is an interdisciplinary field encompassing computer science, industrial networking, public policy, and engineering control system theory and applications. Unfortunately, today's computer science curriculum often does not address the unique aspects of control systems. Correspondingly, the electrical engineering, chemical engineering, mechanical engineering, nuclear engineering, and industrial engineering curricula do not address computer security. Public policy has not addressed the unique issues with control system cybersecurity in cybersecurity policymaking. Consequently, there is a need to form joint interdisciplinary programs for control system cybersecurity. This paper discusses the needs for interdisciplinary programs in control system cybersecurity and provides recommendations for both addressing this serious challenge and training future multidisciplinary hardware and cybersecurity experts.

# CONTENTS

# INTRODUCTION

Control system cybersecurity, often referred to as Operational Technology (OT) cybersecurity, is an emerging, highly specialized yet integrated field combining engineering and network cybersecurity. It includes the disciplines of control system engineering, the specific engineering domain being protected, IT security, industrial networking, risk management, safety system engineering, and public policy.

Control system cybersecurity also requires an understanding of commercial platforms (e.g., Windows, UNIX, LINUX, SQL, etc.). The object is to develop, implement, and maintain policies and resilient technologies to reliably and safely secure:

1. Modern and legacy control systems.
2. Control system field devices that did not address cybersecurity in their initial design and may not have capabilities to upgrade for cyber security.
3. New control systems and control system field devices that are inherently secure by design.

There is also a need to educate the engineering technologists and engineering technicians who maintain control system field devices about cybersecurity considerations.

We stand at the crossroads of technological evolution and critical infrastructure security. The imperative to advance competencies and training in control system cybersecurity has never been more urgent. Control systems are the backbone of Critical Infrastructure—from energy grids and water treatment facilities to transportation networks and manufacturing plants, to defense. Control systems, vital to economic and national security, are increasingly interconnected, automated, and vulnerable to malicious cyberattacks and unintentional incidents. However, cybersecurity is generally viewed in the context of traditional IT systems.

Control systems field devices are frequently not viewed as “computers,” so cybersecurity is not a consideration. Control systems and control system field devices are often considered not to be susceptible to IT cybersecurity threats. Consequently, while cyber security is taught within the Computer Science Departments, it focuses on traditional IT concepts to the exclusion of control system issues. Control system theory and applications for control systems are addressed in the various engineering disciplines. However, those disciplines do not address cyber security.

The highly specialized nature of interconnected control system technologies demands a workforce that is constantly adapting, learning, and staying ahead of malicious and unintentional threats. The need for evolution is not solely driven by threats—it's also driven by innovation in automation, AI, Quantum, and Internet of Things (IoT). These will only increase the number, interconnectivity, and complexity of control systems.

We must take steps to equip the next generation of engineers and technicians, network security personnel, and policymakers with the skills they need to secure and optimize these systems. By fostering robust educational foundations and strategic industry partnerships, we can build a pipeline of control systems engineers, network security personnel, and policymaking professionals prepared to safeguard the systems of today and tomorrow. This will make our nation's infrastructure stronger, safer, more resilient, and more secure.

## CONTROL SYSTEMS

Control systems operate physical infrastructures world-wide including electric power, water, oil/gas, pipelines, chemicals, mining, pharmaceuticals, transportation, manufacturing, and defense. Control systems measure, control, and provide a view of the process once only the domain of the operator. Typical types of control systems include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), and control system field instrumentation (process sensors, actuators, analyzers, etc.). Most universities with engineering and technology programs offer courses in control systems.

Control system networks and workstations including the human-machine interface (HMI) are generally networked like IT systems and may be susceptible to IT cyber vulnerabilities and threats. Consequently, they utilize IT security technologies, where traditional IT education and training apply. The field instrumentation and controllers generally do not utilize commercial off-the-shelf operating systems and are computer resource-constrained, as the microprocessors don't have the capability to use passwords, keys, encryption, etc. They often use proprietary real time operating systems (RTOS) or embedded processors. These systems have different operating requirements and can be impacted by cyber vulnerabilities typical of IT systems in addition to cyber vulnerabilities unique to control systems. These cybersecurity gaps between IT/OT networks and control systems have led to incidents such as the 2023 hack of a poultry processor, leading to potential poisoning of the food supply.[i]

Control systems continue to be upgraded with advanced communication capabilities and networked to improve process efficiency, productivity, and regulatory compliance. This communication can be within a facility or even between facilities continents apart. When a control system does not operate properly or appears not to operate properly, it can result in impacts ranging from minor to catastrophic. Consequently, there is a critical need to ensure that cyber impacts do not cause or enable mis-operation of control systems. Additionally, there is a need for policymakers to understand the issues associated with control systems.

## Control Systems And Operational Technology (OT)

Prior to the 2006 timeframe, control systems were under the purview of engineering organizations. Networks and network devices such as firewalls, routers, and switches were under the purview of the IT organizations. The engineering organizations would reach out to IT as necessary to provide IT expertise, including cybersecurity, for instance, when integrating equipment which had to “talk to” outside vendors,. Policymakers, then as now, were not considering control system cybersecurity issues. The distinctions between different levels of OT and IT are identified in the Purdue Reference Model (Figure 1). Level 0 are control system field devices which are not part of the OT networks, Levels 1-3 include OT networks, and Levels 4 and higher are IT and the cloud.

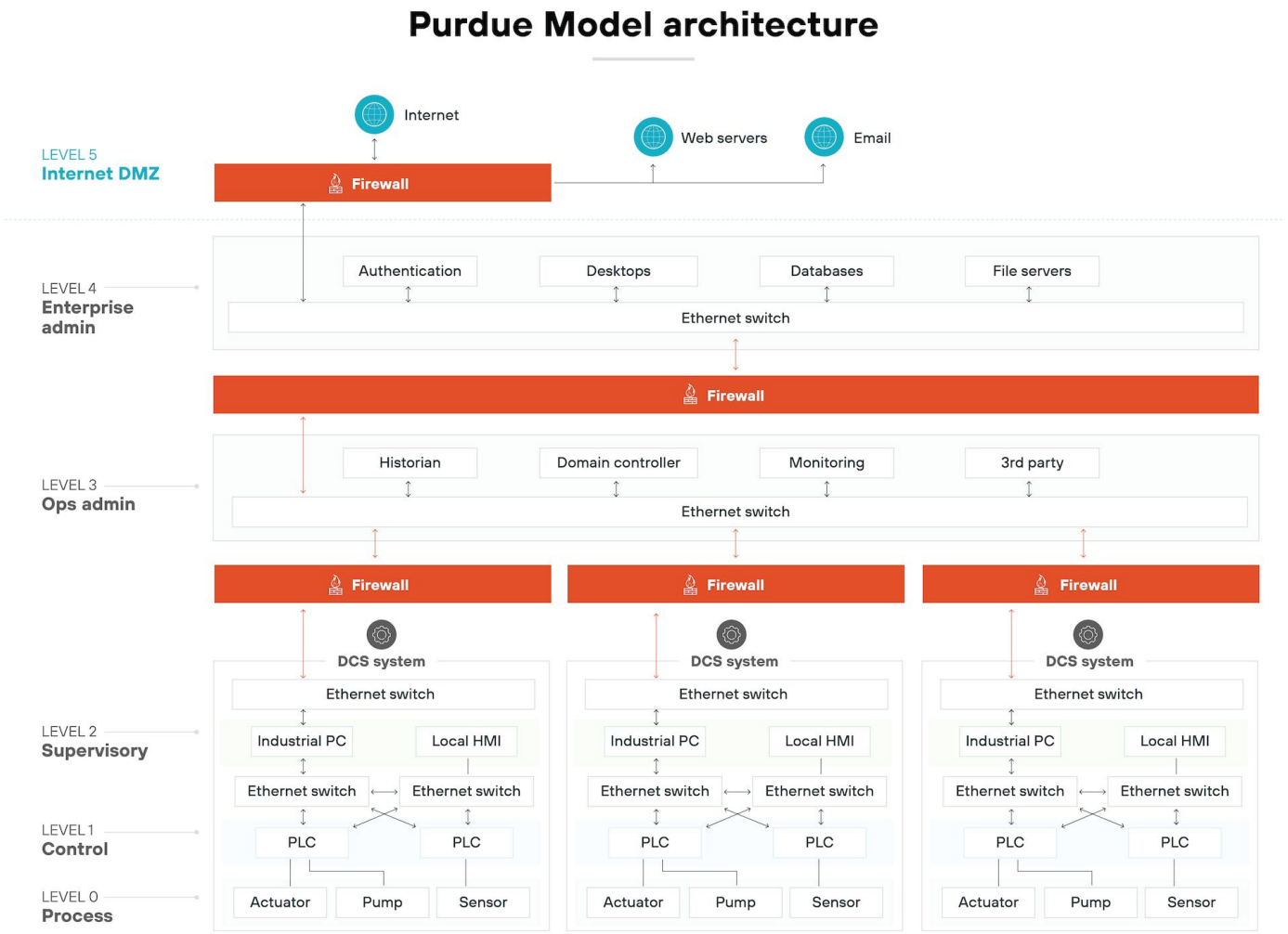


*Figure 1 Purdue Reference Model*[ii]

The term OT as applied to control systems was first published in a research paper from Gartner in May 2006 (Steenstrup, Sumic, Spiers, Williams) and presented publicly in September 2006 at the Gartner Energy and Utilities IT Summit.[iii] Initially the term was applied to power utility control systems, but over time was adopted by other industrial sectors and used in combination with Internet of Things (IoT).[iv] A principal driver of the adoption of the term was that the nature of OT platforms had evolved from isolated proprietary systems to complex software portfolios that rely on IT infrastructure. This change was termed IT-OT convergence. The concept of aligning and integrating the IT and OT systems of industrial companies gained importance as companies realized that physical assets and infrastructure was managed by OT systems and also generated data for the IT systems running the business. In May 2009 a paper was presented at the 4th World Congress on Engineering Asset Management Athens, Greece outlining the importance of this in the area of asset management [v]

According to the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST), OT encompasses the technologies used to operate, automate, and manage physical processes, including SCADA, DCS, PLC, control system field devices and OT networks. OT networks play a critical role in ensuring the continuous reliable and efficient operations of physical processes and is increasingly interconnected with IT systems to enable advanced functionality and data analysis.

One of the limitations and issues associated with the term OT is that people don't think of it as including the hardware (e.g., pumps, valves, turbines, transformers, relays, etc.) used in physical processes. The term "OT" is known within the cybersecurity community, but not as much outside of it**.**

> *Many engineers who design, operate, and maintain the processes and associated control systems do not understand cybersecurity. Many IT and OT network security personnel do not understand the physical processes associated with boilers, transformers, robotics, and other hardware.*

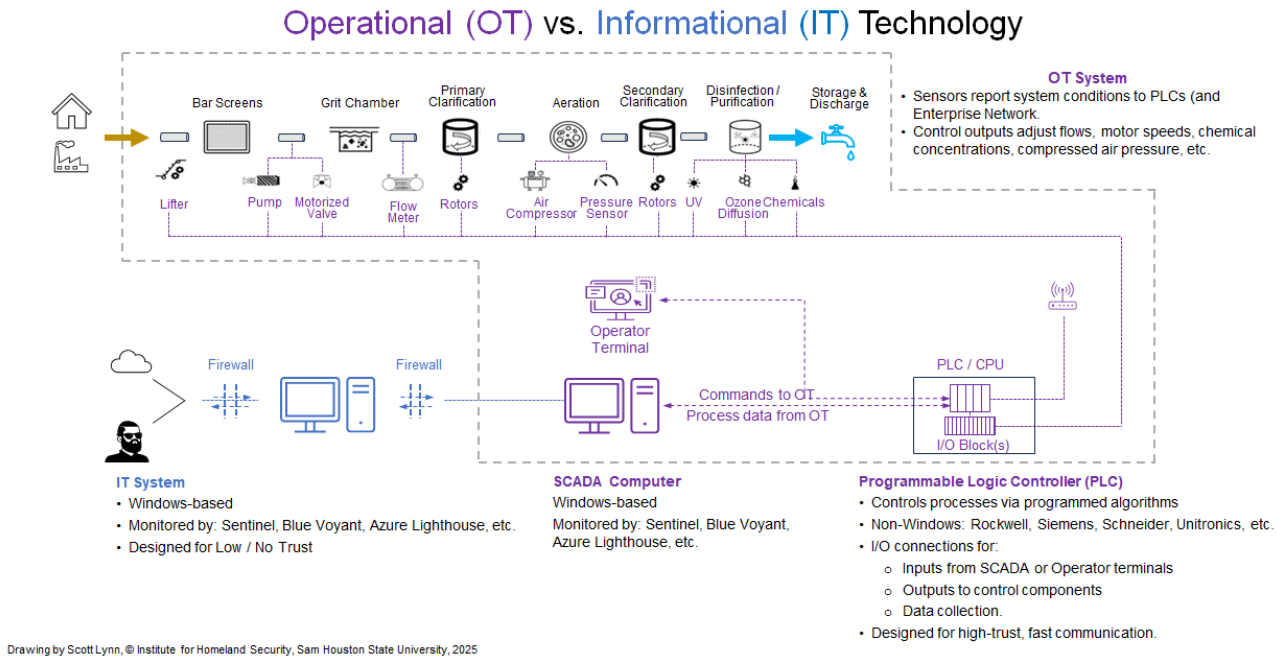


*Figure 2 Typical OT vs IT "Boundaries"*

## Control Systems and IT Systems

Securing control systems consists of physical security, IT security, and control system cybersecurity. Physical security is generally well-understood and often addressed by experts coming from the military or law enforcement. IT security generally deals with traditional commercial off-the-shelf (COTS) hardware and software and connections to the Internet with experts coming from IT and the military. IT security is necessary as IT systems are continuously being probed and hacked. The third aspect is unique to the engineering community, control system cybersecurity, which is much less understood and often not considered. Those working in this area are generally either from the IT security community with little knowledge of control systems or control system experts knowledgeable in the operation of systems, not cybersecurity. Policymakers understand IT and OT network security, but generally not control system cybersecurity.

## The Confidentiality, Integrity, Availability (CIA) Triad

The Confidentiality, Integrity, Availability (CIA) triad effectively defines the technologies needed for securing IT systems. In the IT domain, cyberattacks often focus on acquiring or modifying data (information Assurance). Consequently, the CIA triad results in Confidentiality being the most important attribute. This dictates an encryption requirement. However, in the control system domain, cyberattacks tend to focus on destabilization of physical assets (mission assurance). Moreover, many control system cyber incidents are unintentional and often occur because of a lack of effective process sensor data integrity and/or appropriate control system cybersecurity policies. Consequently, Integrity and Availability are much more important for control systems than Confidentiality. This significantly raises the importance of authentication and process measurement integrity. It lessens the importance of Confidentiality for the control systems though it is still critical for the information being sent from the control systems to the outside environment. For control system cybersecurity, research and education should focus on technologies that address Integrity and Availability (and Safety, even though it is not part of the CIA triad.).

Control system cybersecurity is an engineering problem requiring engineering solutions. Resilience and robustness are critical factors in the survivability of compromised control systems. Further, with industrial processes needing immediate responses to changing systems, fast responses to changes are critical. As control systems are deterministic (meaning the process is repeatable within a prescribed period of time), cybersecurity technologies can take too long to operate and can cause denial-of-service conditions to the control systems. Consequently, control system cybersecurity requires a balanced approach to technology design, product development and testing, development and application of appropriate control system policies and procedures, analysis of intentional and unintentional security threats, and proactive management of communications across view, command and control, monitoring and safety.  It is a lifecycle process beginning with conceptual design through the retirement of the systems

## Differences Between IT and Control System Communications

Control systems often are not viewed as “computers” or as susceptible to cybersecurity threats. Consequently, cybersecurity is generally viewed in the context of traditional business IT systems and Defense systems. IT systems are general purpose systems that use “best effort” in that they get the task complete without time constraints. On the other hand, control systems are purpose-built, not general-purpose systems. Again, they are deterministic in that they must act repeatably within a prescribed time. Unlike IT systems, control system design criteria include

performance and safety requirements, but generally not cybersecurity. This is particularly the case for control system field devices

The difference between network security and engineering can be seen by two 2025 job solicitations - one from a mid-sized water utility for Junior, Mid-level, and Senior Engineering positions and the second from large electric utility looking for a Senior OT Security Analyst. The engineering job description stated “Assist with or lead providing electrical engineering and technical support to ensure reliable operation of the utility’s SCADA controlled facilities including RTUs, PLCs, programmable automation controllers (PACs), associated industrial communications, networking equipment and protective relaying equipment.” Even though communications and networking were addressed, the term “security” was missing. The analyst job application stated: “the analyst would be part of a team consisting of skilled OT cybersecurity professionals to ensure the cybersecurity resilience and regulatory compliance of the utility’s industrial operational sites. The focus would be on identifying vulnerabilities and assessing risks to uphold and continuously improving the security posture of industrial control systems (ICS) and OT environments. There was no mention of ensuring the control systems accomplished their functions in a safe and reliable manner or working with the engineering organizations. The education requirement was computer science not engineering.

Reliable and timely communications are critical for maintaining the operations of control systems. Control system field device communication protocols originate as serial or analog communications and are then converted to Internet Protocol (IP) communications such as Ethernet packets. Legacy control systems were not designed to be cybersecure or have modern network monitoring. There is some signal validation, no authentication, no encryption, and adequate speed (that is, minimal latency is acceptable). The control system community has the knowledgebase to understand what physical parameters are required to perform a root-cause analysis of a physical incident. Consequently, the control system community has developed detailed forensics for physical parameters - temperature, pressure, level, flow, motor speed, current, voltage, etc. However, legacy/field device portions of control systems (e.g., process sensors, actuators, drives, etc.) have minimal to no cyber forensics. This area is ripe for research and development to determine what specific types of forensics are needed and how they would be performed in the least invasive manner possible.

User Datagram Protocol (UDP) is one of the core communication protocols of the IP suite used to send messages (transported as datagrams in packets) to other hosts on an IP network. Within an IP network, UDP does not require Transmission Control Protocol (TCP)/IP and is not deterministic. Consequently, TCP/IP is used for non-process or safety critical communications. Since there is a movement to utilize TCP/IP protocols from RTUs or PLCs to SCADA or DCS, there is a common look and feel between the IT community and the control system community.

The use of TCP/IP and Windows was also a natural progression to the Internet. There are now many instances where control systems have been connected directly to the Internet using TCP/IP through Windows or other commercial-off-the-shelf operating systems. Control systems can also connect to the Internet through serial-to-Ethernet converters. These direct connections to the Internet create significant cyber vulnerabilities and have been exploited similarly to the 2015 Russian cyberattack of the Ukrainian power grid. There are programs such as Shodan that publicly identify Internet-connected systems. In the future, TCP/IP will be used for control and even safety applications. This really needs to be done with great care.

In the IT community, software security and secure software are often discussed in the context of software assurance. Software assurance is broader than software security as it encompasses the additional disciplines of software safety and reliability. Software assurance aims to provide justifiable confidence that the software is free of vulnerabilities, that it functions in the intended manner, and that the intended manner does not compromise the security and other required properties of the software, its environment, or the information it handles. Software assurance also aims to provide justifiable confidence that the software will remain dependable under all circumstances. These include the presence of unintentional faults in the software and its environment; exposure of the operational software to accidental events that threaten its dependability; and exposure of the software to intentional threats to its dependability in development and operation. Software assurance addresses trustworthiness, predictable execution, and conformance where trustworthiness means no exploitable vulnerabilities exist, whether intentional or unintentional. Predictable execution provides confidence processes will function as designed. Conformance means the software and products conform to applicable standards and requirements. To date, the control system community has not formally applied all these principles.

Certain mainstream IT security technologies can adversely affect the operation of control systems or result in operator confusion. Examples include using port scanning tools resulting in components freezing-up - or worse. Encryption can slow down control system operation, resulting in denial-of-service events. Locking out a system after a specified number of password failures should not apply to critical control system workstations, as that can have devastating consequences.

The current state of IT insures a high degree of intelligence and processing capability on the part of the various devices within an IT system. The standard implementation provides centralized control points for authentication and authorization of IT activities. The lifetime of the equipment in an IT network, typically, ranges from 3 to 7 years before anticipated replacement and often does not need to be in constant operation. By the very nature of control system devices and their intended function, control system devices may have 15-to-20-year lifetimes, perhaps more, before replacement. Since security was not an initial design consideration,

control system devices do not have available computing capacity for what would have originally been considered unwanted or unneeded applications.

In both IT and control system domains, communication is of considerable importance. Control systems are intended to always operate, whether connected to other systems or not. This independence makes the control system very flexible. However, the lack of microprocessor capabilities makes it difficult to authenticate communications properly, not just between workstations and devices, but between devices and other devices, workstations and devices, workstations and people, and devices and people. By want of adequate operating systems and microprocessor capabilities, legacy control system field devices do not have the ability to access centralized authentication processes.

Patching or upgrading control systems has many pitfalls. Patches need to be verified to determine if the patch is really the same as the one that was sent and to determine that the patch really fixes a bug and won't adversely affect the system performance. This is not as easy as it seems. The field device must be taken out of service which may require stopping the process being controlled. This in turn may cost thousands of dollars and impact thousands of people. An important issue is how to protect non-patchable, non-securable workstations such as those still running NT, and Windows 7 (or even earlier versions). Many of these older workstations were designed as part of plant equipment and control system packages and cannot be replaced without replacing the large mechanical or electrical systems that accompany the workstations. Additionally, many Windows patches for control systems are not standard Microsoft patches but have been modified by the control system supplier. Implementing a generic Microsoft patch can potentially do more harm than the virus or worm against which it was meant to defend. As an example, in 2003 when the Slammer worm was in the wild, one DCS supplier sent a letter to their customers stating that the generic Microsoft patch should not be installed as it WOULD shut down the DCS. In another case, a water utility patched a system at a water treatment plant with a patch from the operating system vendor. Following the patch, they were able to start pumps but were unable to stop them! The recent CrowdStrike update incident resulted in millions of systems (IT and control systems workstations) being impacted.[1]

The perceived distinctions between IT and control systems are starting to blur with grave consequences. Various digital upgrade initiatives have provided real case histories of what happens when those without an understanding of the control system domain try to set the rules for systems they do not understand. Table 1 below provides a comparison between key

[1] CrowdStrike

characteristics of IT and control systems. These differences can have very dramatic impacts on control system operation and education.

## IT/ OT and Control System Characteristics

| Attributes | Network IT/OT | Control Systems |
|---|---|---|
| Confidentiality | High | Low |
| Integrity | Low-Moderate | Very High |
| Availability | Low-Moderate | Very High |
| Authentication | Moderate-High | High |
| Time Criticality | Delays tolerated | Critical |
| Security Education | Good | Usually Poor |
| Certifications | CISSP (Certified Information Systems Cybersecurity Professional) | PE (Professional Engineer) |
| Life Cycle | 3-5 years | 15-25 years |
| Automated Tools | Widely Used | Limited |
| Interoperability | Not critical | Critical |
| Protocols | TCP/IP, UDP | ICS-specific |
| Communications | Telco, Wi-Fi | Telco, Wi-Fi, satellite, radio, other |
| Resources | Unlimited | Very limited |
| Bandwidth | High | Limited |
| Forensics | Available | Minimal |
| Administration | Centralized | Localized |
| Operating Systems | COTS (Windows, etc.) | COTS at HMI; RTOS, Embedded Kernels |

*Table 1 Comparison of IT and ICS Characteristics*

## CURRENT STATUS CONTROL SYSTEM AND IT SYSTEMS

Figure 3 below characterizes the relationships of the different types of special technical skills and certifications needed for control system cyber security, and the relative quantities of each at work in the industry today. Most people now becoming involved with OT (not control system) cyber security typically come from a mainstream IT security background and not a control system background. The training that would make them "OT security experts" is from a network not control system focus. This trend is certainly being accelerated by digital transformation initiatives, where the apparent lines between IT and control systems are blurring creating the

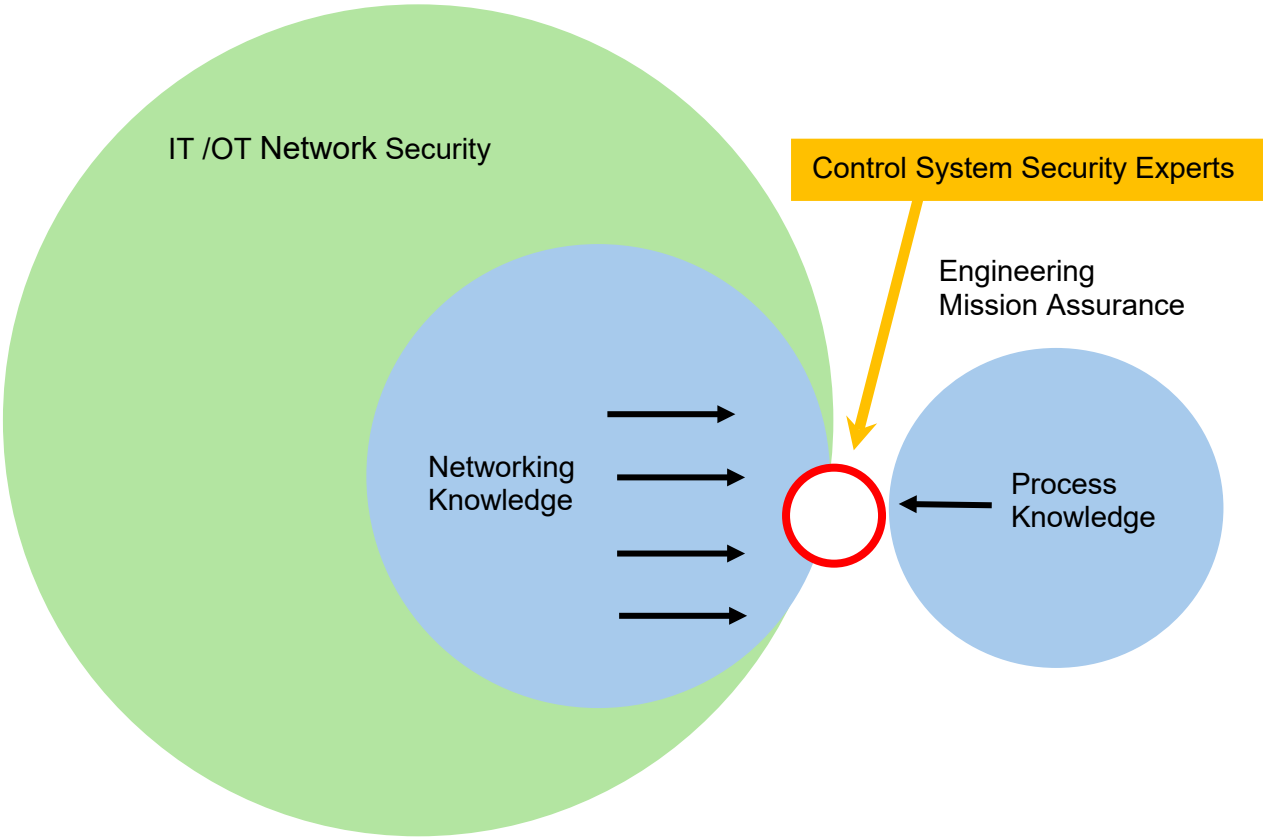


*Figure 3:* Computer Science (Information Assurance) vs Control Systems (Mission Assurance)

term "IT/OT convergence". Many of the entities responsible for control system cyber security including end-users, equipment suppliers, system integrators, consultants, and government personnel do not fully appreciate the difficulties created by this trend.

Lack of understanding extends to both network security (IT and OT) and Engineering, And this lack of understanding means that, while you may not see the threats you are used to seeing, this does not mean the system isn't vulnerable to (OT) attacks of an entirely different type.

***Just because part of the system is not vulnerable to the threats you are used to seeing does not mean the system isn't vulnerable.***

As can be seen in Figure 3, IT encompasses most network cybersecurity but does not include control system processes. The arrows indicate that most people coming into the control system cybersecurity domain (from academia and the work force) come from the IT domain. This needs to change. It does not take rocket science to compromise a control system; however, it does take engineers and IT personnel working together to be able to protect a control system and still have it perform its functions. Being able to do that is what makes people control system cybersecurity experts. Arguably, on the cyber defense side, there are only hundreds worldwide who fit into the tiny dot called control system cybersecurity. This obviously needs to grow exponentially.

There are a couple of reasons for this imbalance.

First, there are simply more trained IT (now also OT) network security personnel than control system security personnel. There is an old adage: "to a carpenter with a hammer, everything looks like a nail". As control systems get more of an IT-look, network security (IT and OT) view them as IT systems and want to apply their expertise to them.

Second, there is often little funding or desire for training control system personnel in cybersecurity as Engineering often does not view this area as under their purview or concern. Is there any question as to why there are so many more IT and OT network security personnel than control system personnel? The timing is ripe for the academic community to address the need to educate more control system cybersecurity technologists, researchers, and experts.

The lack of control system cyber security understanding in the industrial community is also often reflected in the academic community. Having given lectures at National Defense University, the Naval Postgraduate School, the University of Washington, the University of Illinois, Mississippi State University, Stanford, and UC Berkeley among others, I found the lack of interdisciplinary focus and coordination evident. Unfortunately, today's computer science curriculum generally does not address the unique aspects of control systems. Correspondingly, electrical engineering, chemical engineering, mechanical engineering, nuclear engineering, and industrial

engineering curricula rarely if ever address cybersecurity. Consequently, there is a need to form joint interdisciplinary programs for control system cybersecurity. One book used for a critical infrastructure class at the University of Washington had to be rewritten as its focus was IT. [vi] This is not just academic - there have been numerous cases where control system performance has been impacted by inappropriate use of IT security policies, procedures, and/or testing. Conversely, there have been many control system cyber incidents including shutdowns of nuclear power plants, pipeline ruptures, plane and train crashes that did not violate IT cybersecurity policies. Consequently, there is a need to educate engineers and security professionals on how to better cybersecure physical infrastructure. There are many examples of this problem. The first example of this gap occurred in October 2008 when the author gave two lectures on control system cyber security at Mississippi State University. The first lecture was to the computer security class. There was only one engineer taking the class. The second lecture was open to the university. There were approximately 120 attendees. When asked how many were from departments other than IT or the Computer Science Department, fewer than ten raised their hands. In April 2010, I gave a presentation in San Antonio to a local organization. The audience included a senior in Computer Science from the University of Texas-San Antonio who wanted to specialize in critical infrastructure security. When asked how many engineering classes he had taken the answer was “none, why?” When asked how many engineering students were in his computer security classes, he could not recall any.

Cybersecurity is usually taught as a track of study within computer science baccalaureate degree programs, but those programs typically do not include courses on engineering except as electives, whereas baccalaureate degrees in electrical, mechanical, chemical, nuclear, systems, and other engineering disciplines treat courses in cybersecurity as electives (although there are few trends on concentration, certificate or emphasis areas in cybersecurity). And from there, the die is cast, with a small subset of graduates of these programs having become knowledgeable (or at least familiar) in both engineering and cybersecurity. The situation is similar for vocational training, with a heavy emphasis on either engineering or cybersecurity.

However, there do exist undergraduate and graduate-level certificate and degree programs that treat engineering and cybersecurity in a unified manner, such as the University of Pittsburgh’s undergraduate certificate in Cybersecurity in Emerging Engineering Systems.[2] For instance, in addition to completing two courses in cybersecurity and one in artificial intelligence, a student in the certificate program could take the course ECE 1773 ~~,~~ Power Generation, Operation, and Control which covers the topic of power system security. As another example, the Naval Postgraduate School offers the interdisciplinary Cyber Systems and Operations program, with one of the tracks leading to a Master of Electrical Engineering Science (with an emphasis on Electrical Engineering). [3] Five of the core courses in that track focus on cybersecurity and cyber-

physical systems:  Introduction to Cybersecurity, Introduction to Cyber Systems and Operations, Cyber Network and Physical Infrastructures, Network Security, and Introduction to Cyber Physical Systems. The students in that program have plenty of electives that they can take in engineering related to cyber-physical systems and control.

At the September 2001 International Society of Automation (ISA) Expo in Houston, ISA held two sessions on control system cybersecurity on September 10th. Participants represented the spectrum of industrial and manufacturing organizations including electric power, oil/gas, chemicals, water, food, automotive, and even a pet food manufacturer. On September 10th, the sessions were focused on business because “you can’t make things if the control systems don’t work.” National security was not yet an issue (the next day was 9/11 and everything changed) as there were very few known control system cyberattacks. In 2001, the engineers were focused on the control systems and control system field devices including process sensors. In 2001, the term “OT” hadn’t been coined yet (Gartner did that in 2006). Consequently, almost all attendees were from engineering with very few IT attendees. These sessions ultimately led to the formation of ISA99[vii] and the resulting ISA/IEC 62443[viii] series of control system cyber security standards.

Fast forward to September 24, 2024. The HouSecCon security conference was held in the same building as the ISA Expo in 2001. Eugene Spafford from Purdue gave the opening keynote. He agreed that we haven’t got very far in addressing control system cyber security since I spoke at the National Information Assurance Partnership (NIAP) Security Summit in Indianapolis in March 2001. Paul Veeneman and I gave a presentation, “OT security – the cure is worse than the disease”. There were approximately 90 people in our OT session. By raising of hands, there was one engineer present with the rest being network security people – a 180-degree change from 2001. This should be a flashing red light that cyber security of control systems in critical infrastructures is no longer about the control systems but the networks. In fact, I was asked what security conferences engineers would attend. The unfortunate answer is that most engineers don’t attend cyber security conferences because they don’t believe cyber directly affects them.

At the October 2009 Applied Control Solutions Control System Cybersecurity Conference, Professor John Saunders from the National Defense University provided a presentation on the status of education and training in ICS cyber security. The focus of cybersecurity training was on networks while the focus on control system training was on safety, ultra-high reliability, and maintaining aging equipment using low bandwidth communication links.

Policy discussions at the 2018 Air Force Cyber Policy Conference were based on IT considerations. The technical issues associated with control system cybersecurity issues were not addressed

Granted these are small real-life samples, but they are representative of the author's experience in industry and academia.

## Government and Industry

NIST's National Initiative for Cybersecurity Education (NICE) is to prepare, grow, and sustain a cybersecurity workforce that safeguards and promotes America's national security and economic prosperity. However, control system cybersecurity is not part of that effort.

The SANS Institute is a for-profit cybersecurity training institute. They have an ICS training set of courses but does not address control system field devices.

The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program is managed by NSA's National Cryptologic School. Federal partners include the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST)/National Initiative on Cybersecurity Education (NICE), the National Science Foundation (NSF), the Department of Defense Office of the Chief Information Officer (DoD-CIO), and U.S. Cyber Command (USCYBERCOM).[ix]

The NCAE-C program has over 400 institutions all over the Nation with designations in Cyber Defense (CAE-CD), Cyber Research (CAE-R), and Cyber Operations (CAE-CO).[x]

Today, the NCAE-C program has over 400 institutions all over the Nation with designations in Cyber Defense (CAE-CD), Cyber Research (CAE-R), and Cyber Operations (CAE-CO).

There has been a joint effort from the Idaho National Laboratory (INL), Idaho State University, and ISA to address control system cyber security training needs in the document, "Industrial Cybersecurity Knowledge".[xi, xii] The document provided a review of cybersecurity workforce development literature and cybersecurity curricular guidance documents from leading English language sources. The report found 1) A lack of "industrial" or "OT" specific cybersecurity guidance; 2) No clear description of what is meant by "industrial" or "OT" cybersecurity; 3) No documentation describing what methodology was used to create the guidance [2]. The "Curricular Guidance: Industrial Cybersecurity Knowledge" document presents the results of a collaborative multi-year research effort to address those needs.

The Curricular Guidance document was intended to provide course authors, instructors, education administrators, and students with a clear description of what "industrial" cybersecurity includes that distinguishes it from traditional cybersecurity programs. The document approaches the challenge from the perspective of "what is missing from traditional cybersecurity curricula?" As a result, the document does not cover all the knowledge that must be included within an industrial cybersecurity curriculum – just those parts that which make industrial cybersecurity different. For example, host and server operating systems and networking fundamentals should be taught, but are not specifically listed in this document. They are outside the document's defined scope. The document is good in explanation but does not address the control system cybersecurity aspects of field devices.

I sent an e-mail to CISA on February 7, 2025, asking if CISA's control system cybersecurity training included specific training on control system field devices such as process sensors, actuators, and drives. As CISA could not answer the question, my e-mail was forwarded to INL for response. INL's response to me dated February 10, 2025, was "The training does not have specific training on field controllers or field devices.  We do look at HMI creation, and an overview of the types of programming done on controllers including a short lab on ladder logic."

## Selected Texas Universities Approach to Engineering, Cybersecurity, and Public Policy

Many universities and colleges provide cyber security tracks within the Computer Science programs. Engineering departments provide control system theory and practice. A review of the course catalogues from University of Texas-Austin, University of Texas-San Antonio, Texas Tech, Sam Houston State University, and Lamar University demonstrate the lack of a unified approach to teaching control system cyber security. The author reviewed the course catalogues for Chemical Engineering, Computer Science, and Public Policy for each university to identify if there were existing cross-departmental programs. Nothing was evident in the engineering courses that included cybersecurity. However, UT-Austin and UT-San Antonio each had a course through computer science on control systems. UT-Austin was Introduction to Cyberphysical Systems, and UT-San Antonio was Industrial Control Systems Security. Without the course details, it was not possible to identify the efficacy of the course. That is, is the course being taught from a network or engineering perspective?

## Impact of the Current Approach[xiii]

The 2006 Gartner research paper introducing the term OT created a hybrid between engineering and IT that still hasn't been properly connected. Engineers come from a "physics-based" discipline whereas IT comes from a data-centric discipline. The term OT is known within the cyber security community but not necessarily outside. That is, electrical, mechanical,

chemical, nuclear, industrial, systems, and other engineers and technicians often do not consider themselves to be OT and may not be aware of the term. That was evident at the 2025 IEEE Power and Energy Society Summitt in San Jose, CA.[xiv]

The previous mention of job solicitations from water and electric utilities bears repeating here. Neither the engineering or the network security offering mentioned the other – clearly overlooking the technology being protected or vulnerabilities in how the OT/control systems communicate.

This gap in mutual understanding has prevented critical plant processes and control system equipment from being cybersecure and safe. The paper written for the Institute for Homeland Security at Sam Houston State University: Who's in Charge of OT Security?[xv] explores these cultural challenges in greater detail.

# RECOMMENDATIONS

## A Case History of What Can be Done

The benefits of combined IT / OT training became clear in 2022 when I supported a Masters-level course in the Computer Science Department at the Missouri University of Science and Technology. The course was CS 6001: Industrial Control Systems for Computer Scientists. The course covered the basics of industrial control systems, their importance, interactions between ICSs and standard IT networks, the cybersecurity of ICSs, case studies of cyberattacks, and the Internet of Things (IOT). The course discussed how to model and verify the behavior of industrial control systems.

The instructor was a computer security scientist. None of the students were engineers or had a computer science background. I gave two lectures on industrial control system cyber security and the difference between industrial control system cyber security and IT cyber security

The capstone project for the course was each student selected an electric utility to investigate how the utility met the intent of the NIST Cybersecurity Framework. The investigation only used public sources. The students' focus appeared to be on IT functions because there was not much publicly available about industrial control systems. However, in some cases, there was information available on control systems/hardware issues..

An indication of the success of the course was that, in at least three cases, students found NIST cybersecurity framework failures of which the utilities did not appear to be aware.

The first student found the utility's history on NERC CIP cybersecurity compliance. The student also found the utility operated a critical Chinese-made grid control device in a critical substation.

A second student found a document outlining Cyber Security Requirements for third party vendors working with the second utility. The document was marked “Internal Use Only” which showed that this document was mistakenly located on the public not private side of the utility’s firewall and should not have shown up in the Google search. The document showed the maintenance of the policy and confirmation of adherence fell to the utility’s Information Security Analysts. Additionally, the student found that many of the utility’s substations had no form of physical barrier to entry, and several only had chain link fences. The physical security for some substations seemed to only be that they were “hidden” in remote parts of the countryside. However, the student was able to remotely assemble a list of addresses and identify vulnerable substations. Additionally, lack of discoverable information in the public domain indicates that the utility did not publicly disclose a cyber incident at a nuclear power plant the year it occurred.

The third student couldn’t find substantial information about the utility’s IT assets but surprisingly found information regarding their operational assets. The student found the utility had an active contract with one vendor and a multi-million-dollar asset management contract with another vendor. The utility deployed this vendor’s transformers and software services for their generation, transmission, and distribution assets. Even though the student did not find any public indications of direct cyberattacks on the utility, the student found one of utility’s supplier was a victim of a ransomware data breach in which hackers accessed schematics and drawings related to the utility’s powerplants. The student also found the utility procured uranium from a Russia company for its nuclear plant.

### What Should be Done

Many universities and colleges provide cyber security tracks within the Computer Science programs. Engineering departments provide control system theory and practice. There is a need to form interdisciplinary programs from experts drawn from Computer Science and the various Engineering departments. This also extends to public policy programs.

As a minimum, develop a one semester (quarter) course, “Control Theory and Applications for Non-Engineers” as a pre-requisite for the cyber security track in the Computer Science Department. The course would identify the different types of control systems, their computing resource limitations, the technical and administrative differences between control systems and IT systems, and the technologies that would be relevant to control systems. The course should be taught by faculty from Computer Science and various Engineering Departments.

The parallel course would be a one semester (quarter) course, “Cyber Security for Engineers” as a pre-requisite for engineering control theory and application courses. This course would identify the different types of cyber security threats, the different types of IT cyber security technologies, and address the potential impacts of these security systems and technologies on

control system design and operation. The course also should be team-taught by faculty from various Engineering and Computer Science Departments.

1. **Statewide Assessment of ICS Training Needs & Industry Gaps**

   Action: Conduct a comprehensive statewide assessment to evaluate the current workforce demand for ICS experts, identifying gaps in both training programs and skilled personnel.

   Outcome: A comprehensive report that outlines industry needs and proposes solutions to address workforce gaps.

2. **Define Key Positions and Core Competencies for ICS Workforce**

   Action: Develop a clear framework for identifying key industrial positions in ICS and the core competencies required for each role, ensuring alignment with industry needs.

   Outcome: A competency model for ICS positions that can be used to guide educational programs, certifications, and industry recruitment.

3. **Establish SHSU's Role in ICS Workforce Development**

   Action: Develop a recommendation for Sam Houston State University (SHSU) to take a leadership role in the development of ICS experts, creating an integrated educational program and industry partnership

   Outcome: A well-defined strategy for SHSU to become a center for ICS training, attracting students, researchers, and industry professionals to advance the field.

4. **Establish in-service training courses for engineers and computer scientists in the workforce.**

   Action:Create an on-line training course for those in the workforce who are responsible for cyber-physical assets.

   Outcome: This would support existing organizations in helping them come "up to speed" on OT cybersecurity.

## CONCLUSION

IT and control systems are both susceptible to cyber threats (those treats may be different from each other) which need to be addressed.  Industry and academia recognize the need to secure IT systems. However, the same can't be said for control systems.  This is a new field that requires the best and brightest from both IT and engineering to solve these critical problems and provide a new generation of trained control system cybersecurity experts.

## AUTHOR BIOGRAPHY

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.

# REFERENCES


[i] Pilet Jonan, South Carolina Chicken Plant Sabotage Case Exposes Food Safety Gap, Food Safety News, May 2, 2025, https://www.foodsafetynews.com/2025/05/south-carolina-chicken-plant-sabotage-case-exposes-food-safety-gaps/

[ii] https://www.paloaltonetworks.com/cyberpedia/what-is-the-purdue-model-for-ics-security

[iii] Steenstrup, Sumic, Spiers, Williams. "IT and OT Interaction Gives Rise to New Governance". *Gartner from https://en.wikipedia.org/wiki/Operational_technology#cite_note-2*

[iv] Arlen, James, Integrity and Compliance Monitoring, July 15, 2015, The IoT Convergence: How IT and OT Can Work Together to Secure the Internet of Things, https://www.tripwire.com/state-of-security/the-iot-convergence-how-it-and-ot-can-work-together-to-secure-the-internet-of-things.

[v] Koronios, A., Haider, A., Steenstrup, K. (2010). Information and Operational Technologies Nexus for Asset Lifecycle Management. In: Kiritsis, D., Emmanouilidis, C., Koronios, A., Mathew, J. (eds) Engineering Asset Lifecycle Management. Springer, London. https://doi.org/10.1007/978-0-85729-320-6_13.

[vi] Ted Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, ISBN: 978-0-471-78628-3.

[vii] ISA99, Industrial Automation and Control Systems Security, International Society of Automation, 1999

[viii] Cybersecurity Certificate Program, International Society of Automation

[ix] National Security Agency/Central Security Service, https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

[x] CAE in Cybersecurity Community, About Us  What Is a CAE In Cybersecurity? , https://caecommunity.org/about-us/what-cae-cybersecurity#:~:text=In%201999%2C%20the%20National%20Security,rigorous%20curriculum%20and%20program%20requirements.

[xi] Ida Ngambeki, Sean McBride, and Jill Slay “Knowledge Gaps in Curricular Guidance for ICS Security” (2022). Journal of the Colloquium for Information Systems Security Education. https://doi.org/10.53735/cisse.v9i1.149

[xii] “Building and Industrial Cybersecurity Workforce: A Managers’ Guide” (2021). Idaho National Laboratory and Idaho State University, https://inl.gov/content/uploads/2023/07/ICS_Workforce-ManagersGuide2021.pdf.

[xiii] Control Global, Unfettered Blog, OT and engineering are not the same and are creating dangerous conditions, https://www.controlglobal.com/blogs/unfettered/blog/55278622/ot-and-engineering-are-not-the-same-and-are-creating-dangerous-conditions

[xiv] 2025 IEEE Power & Energy Society (PES) Summit: Achieving a More Reliable and Resilient Energy Future, https://ieee-pes.org/events/2025-ieee-pes-summit-achieving-a-more-reliable-and-resilient-energy-future/

[xv] Weiss, Joseph, Who's In Charge Of OT Security?, Institute for Homeland Security, Sam Houston State University, https://ihsonline.org/Portals/0/Tech%20Papers/2024_Papers/Weiss_Whos_in_Charge_of_OT_Security.pdf?ver=dDp8PytV0TTz8Uqlu687gg%3d%3d

# INSTITUTE FOR HOMELAND SECURITY

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. (2025). The Need for Interdisciplinary Programs for Control System Cybersecurity (Institute for Homeland Security Report No. 2025-1018). Institute for Homeland Security.

https://doi.org/10.17605/OSF.IO/AZGW6