

Executive Summary

Southeast Texas drives a substantial share of the nation's fuel, chemical, and LNG production and logistics. At the Center for Data, AI and Cybersecurity (CDAC) at Lamar University, our mission is straightforward: **maximize digital capacity, minimize cyber risk**, and prepare the regional workforce to defend the critical infrastructure our economy depends on.



This issue highlights our latest achievements since the last edition: a three-day Cybersecurity In-person Training for Industrial Control Systems; a live demonstration of CDAC's in-house midstream testbed; and peer-reviewed research spanning integrated risk assessment in chemical process industries, PLC code testing, ICS anomaly detection, and LEO satellite networks. We also celebrate the graduate pathways producing the next generation of OT and enterprise security professionals.

A note on our name. Following discussions with Lamar University leadership, CDAC has updated its name to the *Center for Data, AI, and Cybersecurity* (formerly the *Center for Data Analytics and Cybersecurity*) to better align with its strategic plan and the evolving technological landscape.

Looking ahead, CDAC is launching three new business-focused training programs:

AI for Business — Empower your team to harness Agentic AI in everyday business operations — drafting communications, organizing information, and accelerating workflow — grounded in human oversight and responsible use.

SMB Cybersecurity — Right-sized, plain-language protection built for small and mid-sized teams. Defend against phishing and breaches, navigate HIPAA/PCI and cyber-insurance, and leave with a 90-day action plan your team can deploy on day one.

AI & Cybersecurity — Get ahead of the AI threat curve: defend against AI-driven phishing and deepfakes, deploy AI-powered detection, and adopt AI safely with a clear use policy and 90-day roadmap.



Ready to elevate your team? Contact us today to bring CDAC's high-caliber training to your organization or to join our upcoming cohort.

POINT OF CONTACT

Helen H. Lou, Ph.D., P.E., AIChE Fellow

Director, Center for Data, AI and Cybersecurity (CDAC)
Professor, Dan F. Smith Department of Chemical & Biomolecular Engineering
Faculty Advisor, Center for Midstream Management and Science (CMMS)
✉ hhlou@lamar.edu ☎ (409) 880-8207 🏠 lamar.edu/cdac

IN THIS ISSUE

- 01 Welcome & Issue Overview
- 02 Impactful Training & Industry Engagement
- 03 Research Highlights & Publications
- 04 MBA in Cybersecurity Management
- 05 Graduate Certificates & Looking Forward

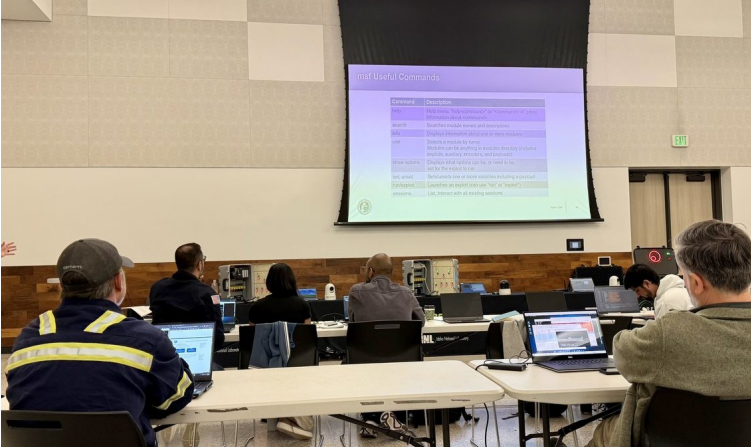
Cybersecurity In-person Training for Industrial Control Systems — April 6-8, 2026

CDAC hosted a three-day Cybersecurity in-person ICS Training at Lamar University in early April, drawing professionals, educators, and students from multiple states. Delivered by the world-renowned Idaho National Laboratory (INL) Industrial Control Systems (ICS) training team, this program was held in partnership with CISA Region 6. The curriculum successfully combined lectures, hands-on technical labs, and adversary simulations. We extend our heartfelt gratitude to the DOE for their grant support, to our corporate sponsor, ExxonMobil, and to our break sponsor, Valero, to our institutional partners Sul Ross State University and the Center for Advances in Port Management at Lamar University for making this workshop possible, as well as our wonderful featured speaker, Mr. Jeevan Sakti of ExxonMobil.

The curriculum delivered three cornerstone courses: **Intermediate Cybersecurity for ICS Part 1 (ICS 201)**, **Part 2 (ICS 202)**, and **CyberStrike Nemesis**. Through rigorous, hands-on exercises, participants gained practical experience detecting, mitigating, and responding to sophisticated attacks against industrial control systems. They also earned professional certificates and continuing education credits upon completion.



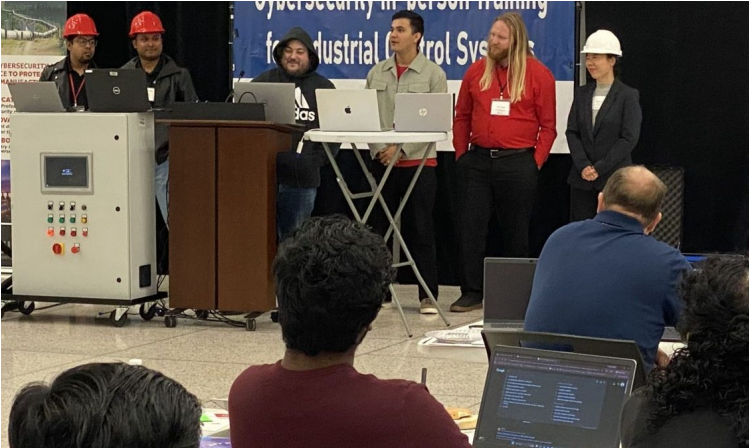
INL instructors and CDAC Director at the Opening Ceremony



ICS 202 instruction in session

Live Demonstration of CDAC's Midstream Testbed

On day one, to showcase CDAC's in-house cyber-physical midstream pipeline testbed, the CDAC and CMMS teams conducted a live demonstration for participants. The walkthrough featured normal SCADA operations, simulated cyberattacks targeting the control loop, and real-time attack detection through CMMS's software. Through a combination of live demonstrations on the CDAC midstream testbed and interactive exercises, attendees observed real-world threats to critical infrastructure, gaining a level of practical insight unavailable in a lecture-only setting.



Live midstream testbed demonstration — Day 1, April 6, 2026



CyberStrike Nemesis lab station — adversary simulation against ICS targets

3

DAYS OF TRAINING

3

COURSES

Multi-State

PARTICIPANT REACH

CEUs

EARNED BY ATTENDEES

BRING HIGH-CALIBER TRAINING TO YOUR TEAM. CDAC delivers specialized cybersecurity training, including hands-on ICS, wireless security, tailored defense strategies, and AI for Business. Contact us today to discuss a customized session for your organization or to join an upcoming cohort.

RESEARCH HIGHLIGHTS & PUBLICATIONS

Our 2025–2026 research output spans four active threads: integrated cyber-risk frameworks for chemical process industries, ICS anomaly detection, LEO satellite networks for port and maritime operations, and reproducible open-source datasets for PLC code testing and Starlink performance prediction.

01 PROCESS SAFETY AND CYBERSECURITY • PLC CODE TESTING

- ▶ M. A. Sabuj, D. Robertson, P. Richmond, H. H. Lou. "An Integrated Cyber-Risk–Based Process Safety Framework for Cybersecurity Risk Assessment in Chemical Process Industries," *Smart Sustainable Manufacturing Systems*, vol. 10, no. 1, 2026. doi.org/10.1520/SSMS20250033
- ▶ S. Daida. "Integrating Cybersecurity Risk Assessment with Process Safety in Chemical Process Industries," *PhD Dissertation*, Lamar University, May 2026.
- ▶ M. H. Kabir. "On the Effectiveness of LLMs in Unit Test Generation for Structured Text Programs," *MS Thesis*, Lamar University, December 2025.

02 ICS ANOMALY DETECTION

- ▶ K. F. Rabbi, H. H. Lou, X. Liu. "The Impact of Time-Aware Design Choices in ICS Anomaly Detection," *Proc. IEEE CCWC 2026*, Las Vegas, NV, pp. 890–899. doi.org/10.1109/CCWC67433.2026.11393705
- ▶ K. F. Rabbi. "Design Choices in Anomaly Detection for Industrial Control Systems: Insights from Gas Pipeline Data," *MS Thesis*, Lamar University, December 2025.
- ▶ P. Paul. "Towards Secure Autonomous Vehicles: An Integrated Edge and Multi-Modal Machine Learning Framework for Intrusion Detection," *MS Thesis*, Lamar University, December 2025.
- ▶ M. S. Paran. "Control and Data Acquisition in a Cyber-Physical Midstream Testbed," *MS Thesis*, Lamar University, May 2026.

03 LEO SATELLITE NETWORKS FOR PORT & MARITIME OPERATIONS

- ▶ M. M. Hossain, X. Liu, H. H. Lou, R. Wang, K. F. Rabbi. "Predictive Model for Starlink Maritime Performance Using Multi-Horizon Random Forest," *Proc. IEEE CCWC 2026*, Las Vegas, NV, pp. 1464–1473. doi.org/10.1109/CCWC67433.2026.11393745
- ▶ LEO SatLink Observatory — a self-contained operational tool with continuous 30-second polling, dual-task ML inference, health scoring, and early-warning boundaries for Starlink maritime links. Developed at CDAC.
- ▶ M. M. Hossain. "Predictive Modeling and Operational Monitoring of Starlink LEO Satellite Network Performance in Maritime Environments," *MS Thesis*, Lamar University, May 2026.

04 OPEN-SOURCE DATASETS

- ▶ M. H. Kabir, M. R. Islam, H. H. Lou. "STMutants: A Benchmark Dataset for Mutation Testing of Structured Text Programs," *Figshare Dataset*, 2026. doi.org/10.6084/m9.figshare.31724761.v1
- ▶ M. M. Hossain, X. Liu, H. H. Lou, R. Wang. "Experimental Dataset of Starlink Performance Across Different Weather Conditions in Southeast Texas Coastal Areas," *Figshare Dataset*, 2026. doi.org/10.6084/m9.figshare.30929588

RESEARCH AT A GLANCE

2025 – 2026 Academic Year

2

PEER-REVIEWED PAPERS

2

OPEN DATASETS

1

PHD DISSERTATION

5

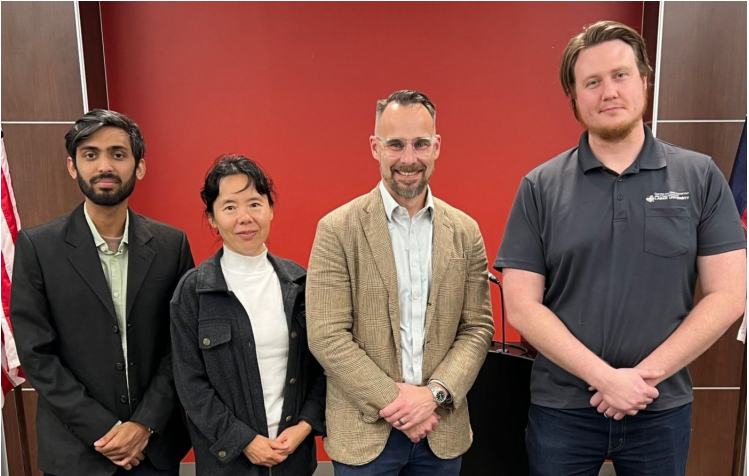
MS THESES COMPLETED

4

ACTIVE RESEARCH THREADS

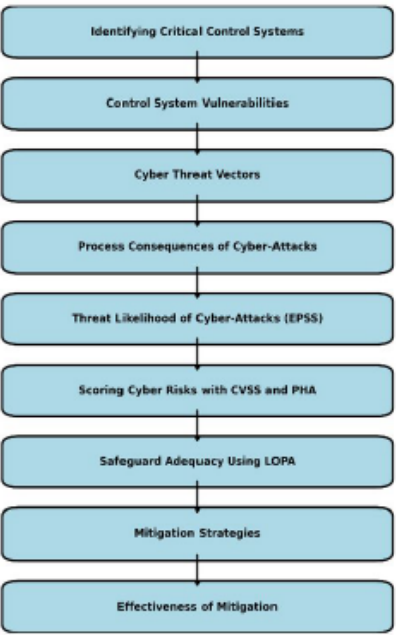
7

PRESENTATIONS AT INTL. CONFERENCES



SBDC AI Startup Pitch Competition — 2nd Place Winner, Beaumont TX
(solving real-world problems in shipping & port sector with cutting-edge AI)

FEATURED: CYBER-RBPS FRAMEWORK



A 9-step methodology spanning vulnerability identification through mitigation effectiveness, designed for chemical process industries. Published in *Smart Sustainable Manufacturing Systems*, 2026.

MBA in Cybersecurity Management

30 CREDIT HRS

COLLEGE OF BUSINESS · AACSB-ACCREDITED · ONLINE / ON-CAMPUS / HYBRID

PROGRAM OVERVIEW

Prepare to lead digital security teams and fortify any organization against cybercrime with the Master of Business Administration in Cybersecurity Management degree from Lamar University. This AACSB-accredited master's program will help you develop essential expertise for corporate, government and consulting roles, as well as entrepreneurial opportunities, in this high-growth industry. Sharpen your strategic leadership skills with an advanced business curriculum and specialized courses aligned with National Centers of Academic Excellence in Cyber Defense (CAE-CD) standards.

CORE MBA COURSES (21 HOURS / 7 COURSES)

- ACCT 5370: Managerial Accounting
- BUAL 5380: Managerial Decision Making or MISY 5340: Intelligent Enterprise Systems
- ECON 5370: Managerial Economics
- FINC 5310: Financial Management
- MGMT 5340: International Business
- MKTG 5310: Marketing Management
- MGMT 5380: Strategic Management

CYBERSECURITY CONCENTRATION (9 HOURS / 3 COURSES)

- MISY 5320: Information Assurance and Security
- MISY 5345: Cybersecurity Networking
- MISY 5355: Cybersecurity Programming Fundamentals
- MISY 5365: Intrusion Detection / Prevention Systems
- MISY 5385: Cybersecurity Governance

CAREER OPPORTUNITIES

- Chief Information Security Officer
- Cybersecurity Program Manager
- Cybersecurity Consultant
- IT Security Manager
- Governance, Risk & Compliance (GRC) Manager

LEARN MORE



Scan to access the MBA in Cybersecurity Management catalog page.
[catalog.lamar.edu / mba-cybersecurity](https://catalog.lamar.edu/mba-cybersecurity)

Contact

College of Business — Graduate Programs
[✉ cobmba@lamar.edu](mailto:cobmba@lamar.edu)
☎ (409) 880-8604
🏠 lamar.edu/mba

WHY LAMAR'S MBA IN CYBERSECURITY

01 AACSB-Accredited

Less than 6% of business schools worldwide hold AACSB accreditation — the gold standard for business education. Lamar's MBA does.

02 CAE-CD Aligned

Curriculum aligned with the National Centers of Academic Excellence in Cyber Defense standards — the federal benchmark for cybersecurity education.

03 Flexible Delivery

Online, on-campus, and hybrid formats designed around working professionals. Complete the program at your pace without leaving your current role.

04 Strategic Leadership Track

Combines business depth with cybersecurity governance — prepares candidates for CISO, GRC Manager, and executive security leadership roles.

READY TO ADVANCE YOUR CAREER IN CYBERSECURITY LEADERSHIP?

Lamar University's MBA in Cybersecurity Management prepares professionals to lead security teams and protect critical infrastructure.

Contact the College of Business Graduate Programs at cobmba@lamar.edu or (409) 880-8604 to learn more about admissions, financial aid, and upcoming cohort start dates.

Center for Data, AI and Cybersecurity
Lamar University

4

Graduate Certificate in Industrial Cybersecurity

12 CREDIT HRS

DEPARTMENT OF COMPUTER SCIENCE • COLLEGE OF ENGINEERING

This specialized 12-hour program bridges the gap between traditional IT security and Operational Technology (OT) or Industrial Control Systems (ICS). Manufacturing, energy, utilities, and infrastructure now rely on automation and the Industrial IoT — and demand for professionals who can protect cyber-physical systems is higher than ever.

CURRICULUM (12 HRS) — 1 COURSE FROM EACH CATEGORY

- 1. Industrial Fundamentals:** PLC Programming, Instrumentation, or Automated System Engineering
- 2. Network Fundamentals:** Computer Network Analysis, Computing Networks, or Advanced IoT Networking
- 3. System Security:** Ethical Hacking, Systems Cybersecurity, or Cyber Crime Analysis
- 4. Network Security:** Cyber-Physical Systems Security, Network Cybersecurity, or Wireless Sensor Networks

KEY CAREER PATHWAYS

- Industrial / OT Cybersecurity Analyst
- ICS / SCADA Security Specialist
- Cyber-Physical Systems Security Engineer
- Critical Infrastructure Risk & Compliance Analyst

WHO SHOULD APPLY?

B.S. or B.E. in a STEM field. No CS or Engineering background? An accessible workforce-aligned path is offered via **INEN 5396**, **COSC 5328**, **CPSC 5363**, and **COSC 5345**. Free online resources such as Harvard's CS50 and Cisco Networking Academy are also recommended.



Scan for
program page

Contact — Dept. of Computer Science

Dr. Xingya Liu, Ph.D., Chair

[✉ xliu@lamar.edu](mailto:xliu@lamar.edu) ☎ (409) 880-8677

Graduate Certificate in Enterprise Cybersecurity

18 CREDIT HRS

DEPARTMENT OF INFORMATION SYSTEMS • DEPARTMENT OF COMPUTER SCIENCE

This 18-hour Graduate Certificate in Enterprise Cybersecurity is designed to help working professionals and students protect organizational assets. Organizations face evolving threats to their proprietary systems — the program covers enterprise technology needs, infrastructure vulnerabilities, practical and strategic defenses, and leadership and strategic risk management.

CURRICULUM (18 HRS)

- 1. Foundations** cover physical security, intrusion detection, and related areas to build both technical and governance strengths. *CPSC 5363 – Cybersecurity: Systems.*
- 2. Technical Electives (choose two):** cybersecurity networking, programming fundamentals, intrusion detection, Python for data analysis, ethical hacking, management, governance, or cybercrime analysis.

KEY CAREER PATHWAYS

- Security Operations Center (SOC) Analyst
- Risk Management & Compliance Specialist
- Network Defense & Incident Responder
- Cybersecurity Architect / CISO

Contact — Dept. of Information Systems

Dr. Kakoli Bandyopadhyay, Ph.D.

[✉ k.b@lamar.edu](mailto:k.b@lamar.edu)

☎ (409) 880-8627



Scan for
program page

INDUSTRIAL TRACK (OT / ICS)

12 credit hours • 4 courses

For engineers protecting refineries, pipelines, utilities, manufacturing — the cyber-physical frontier.

ENTERPRISE TRACK (IT / GOVERNANCE)

18 credit hours

For corporate IT and security professionals leading SOCs, GRC programs, and incident response.

PARTNER WITH CDAC

Industry Partners

Sponsor training, evaluate detection tools on our testbeds, or shape curriculum to your sector's needs.

Workforce Pipeline

Recruit our students; upskill/reskill your team.

Sponsor / Research and Development

Co-fund projects for technology innovation.

