Jan 2025 Isssue 01

THE CENTER FOR DATA ANALYTICS AND CYBERSECURITY (CDAC) NEWSLETTER

Vision

To be the leading regional hub for industrial cybersecurity and data-driven innovation, driving technological progress and safeguarding Southeast Texas' critical industries. We aim to be the trusted resource where businesses, educators, and government turn for expertise in cybersecurity and data solutions. By fostering collaboration, offering advanced training, and promoting innovation, we will strengthen the digital resilience of the entire region.

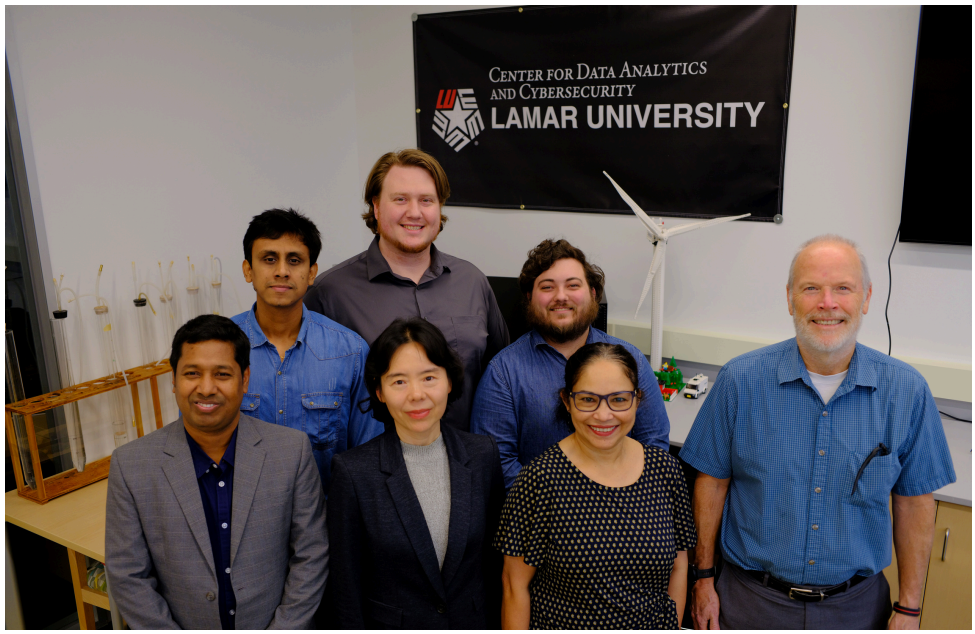
Mission

CDAC strives to drive digital transformation, secure vital infrastructure, and support regional economic development. Through research, talent development, and collaborative efforts with industry, academia, government, and community stakeholders, the center is committed to strengthening industrial capabilities, fostering innovation, and enhancing resilience in the energy, petrochemical, and port sectors. By addressing both current and emerging challenges, CDAC aims to ensure a safer and more prosperous future for Southeast Texas.

Helen Lou
Director
helen.lou@lamar.edu

Adam Loucks
Program Manager
aloucks@lamar.edu

Joseph Raymer
Cyber Research Scientist
jraymer1@lamar.edu



Click here to access our new website!

CDAC'S STRATEGIC GOALS

1. PROVIDE DATA ANALYTICS AND CYBERSECURITY SOLUTIONS TO THE ENERGY, PETROCHEMICAL AND PORT INDUSTRIES IN THE REGION.

2. Develop Cyber-Physical Systems (CPS) technologies, and threat detection and response techniques for industrial control systems.

3. Build the capacity of the workforce in industrial data analytics and cybersecurity.

4. Develop data analytics and cybersecurity education materials for college-level and continuing education in engineering, computer science, management information systems, and process operations.

5. Disseminate program results via seminars, workshops, publications, and stakeholder engagement.

Cybersecurity In-person Training for Industrial Control Systems

The United States Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) is pleased to offer Cybersecurity for Industrial Control Systems. There is no fee to attend the courses. Accommodation, time, travel, and food are the responsibility of the individual attendee.

Who Should Attend

This live training is provided specifically for members of the industrial control systems community associated with IT and process control network operations and security (Operations Technology, OT), operations or management of critical infrastructure (CI) assets and facilities, as well as those who provide CI components and software development.

Prerequisite: Every student attending the courses must bring a laptop computer (no tablets) with wireless capability (to connect to the internet and exercise networks) and a minimum of 8GB of RAM. A modified Kali distribution containing additions to support classroom exercises will be used during the course along with a modified Security Onion VM. Each student must arrive with a VMware® software virtualization package (Workstation, Player, or Fusion) installed on their laptop. You must have administrator privileges to install the VM player.

EVENT DETAILS

DATES April 15 - 18th, 2025

TIME 8:00 am to 5:00pm
Including 1hr lunch

LOCATION Lamar University
4400 S. MLK Jr PKWY
Beaumont, TX 77705

FREE REGISTRATION

Please register for this event at: https://ics-training.inl.gov/learn/courses/315/region-6-beaumont-registration

Course Description:

Tuesday, April 15th, 8:00 am – 4:00 pm
Introduction to Control Systems Cybersecurity (101): The purpose of this course is to introduce students to the basics of industrial control systems security. This includes a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.

Wednesday, April 16th , 8:00 am – 5:00 pm
Intermediate Cybersecurity for Industrial Control Systems, Lecture Part 1 (201): This course provides technical instruction on the protection of industrial control systems using offensive and defensive methods. Students will understand how cyber-attacks could be launched, why they work, and mitigation strategies to increase the cybersecurity posture of their control system. Demonstrations will include the use of software tools to establish a baseline of your network(s), and to monitor and analyze its traffic.

*Two courses (202 and CyberStrike) will be presented alternately on Thursday and Friday, with 50 seats available for each class.

Thursday, April 17th and Friday April 18th 8:00 am – 5:00 pm
Intermediate Cybersecurity for Industrial Control Systems, Part 2 (202) Hands-on:
Because this course is hands-on, students will get a deeper understanding of how the various tools work. Accompanying this course is a sample process control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the many

hands-on exercises that will help the students develop control systems cybersecurity skills they can apply when they return to their jobs.

Thursday, April 17th and Friday, April 18th 8:00 am – 5:00 pm
CyberStrike: Hands-on workshop for defending against an OT cyberattack
[No laptop required]This course offers a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine. The instruction platform challenges course participants to defend against a cyberattack on the equipment they routinely encounter within their industrial control systems.

A certificate of completion and CEUs will be offered to those who complete each session of the course.

Questions:

For additional information please contact:

Idaho National Laboratory
ICSTraining@inl.gov

For additional scheduled ICS events see:

https://us-cert.cisa.gov/ics/Calendar