LEVEL ZERO

OT CYBER SECURITY CONFERENCE

Date and Time

April 19 - 23
Times Vary

Location

Georgia Tech Exhibition Hall
460 Fourth St. N.W. Atlanta, GA 30332

Sunday, April 19	Faculty	Time
*** CambiOS Academy Live Courses** • Choose from 5 courses being taught in-person with access to 6 months of the online course. • www.CambiOSAcademy.com/LevelZero	Jonathan Pollet, Bryan Singer, Marc Visser, Mike Holcomb, Donovan Tindill, Vincent Seruch	9:00 am - 5:00 pm
*** Cyber-Informed Engineering Training for Infrastructure Resilience** • Program introducing a transformative framework to embed cybersecurity resilience directly into the design of critical infrastructure systems.	Ginger Wright Jeremy Jones	9:00 am - 5:00 pm
*Registration to the conference is not required to participate in these 2 training opportunities. Meals are not included.		
Game Night Shenanigans • Arrived in town early and looking to have some fun? Join some friends at the venue for a fun night of board games, pizza and drinks. Early check-in!	Clint Bodungen John Cloonan	5:00 pm - 8:00 pm

Monday, April 20	Faculty	Start Time
Full breakfast and lunch will be available every day of the conference. Snacks and gourmet coffee will also be available throughout the day.		
Main Stage Sessions • All sessions will be held on the main stage • 3 Ted-style talks will be offered during lunch	Clint Bodungen John Cloonan	7:30 am - 10:00 pm
Dinner and Cocktails and a Show . . . Oh My! • No need to change from the day . . . but stay on for a fun social evening where dinner, cocktails and "tv" game shows will entertain us for hours!	Host: Derek Harp & the LZ Team	6:30 pm

Tuesday, April 21	Faculty	Start Time
Full breakfast and lunch will be available every day of the conference. Snacks and gourmet coffee will also be available throughout the day.		
Panels, Sessions and Workshop Break-outs • With up to 4 simultaneous tracks, your entire team can find something • 3 Ted-style talks will be offered during lunch	Varied	8:00 am - 4:00 pm

Wednesday, April 22	Faculty	Start Time
Full breakfast and lunch will be available every day of the conference. Snacks and gourmet coffee will also be available throughout the day.		
Panels, Sessions and Workshop Break-outs • With up to 4 simultaneous tracks, your entire team can find something • 3 Ted-style talks will be offered during lunch	Varied	8:00 am - 3:00 pm
Type 3 or Type 4 ICS4ICS Credentials • **Prior to conference**: complete 6 FEMA courses (free of charge and available online) Details provided below. • Attend a special Table Top Exercise (requires pre-registration) at LZ	UTSI Megan Samford	8:00 am - 3:00 pm

Thursday, April 22	Faculty	Start Time
***Meeting: CIE Design Patterns Working Group** • Enhancing CIE guidance to integrate engineered controls into critical infrastructure (oil/gas, nuclear, power delivery) for cyber-resilience.	Benjamin Lampe Ginger Wright	8:00 am - 12:00 pm

*Registration to the conference is not required to participate in this meeting. Registration to the meeting is required. Meals are not included.

Info@LevelZeroConference.com
www.LevelZeroConference.com

LEVEL ZERO

OT CYBER SECURITY CONFERENCE

CambiOS ACADEMY™

Sunday, April 19

*** CAMBIOS ACADEMY LIVE COURSES**

- Choose from 5 courses being taught in-person with access to 6 months of the online course.
- Visit www.CambiOSAcademy.com/LevelZero for longer descriptions

Introductory(100)

AWARENESS TRACK (3 COURSES)

This track combines three different CambiOS courses into a day long learning experience providing participants with an awareness of the OT infrastructure and systems, the risks and challenges of protecting these systems from attack and the types of threats and risks in overall supply chain and how to manage them.

- **Introduction to OT ICS Fundamentals**
  - Introduction to OT/ICS Fundamentals (OTCS-0103) serves as an awareness-level overview of what Operational Technology is and its role in industrial environments.
- **OT Security Awareness**
  - Derived from the fundamentals course content, it focuses on building basic security awareness around OT systems, without delving into deep technical implementation details.
- **Product Security Awareness for Business Leaders**
  - An introductory level course educating product development teams, engineers, and management about cybersecurity considerations in industrial product design and manufacturing.

Intermediate (200)

OT MONITORING & SOC

This course builds on foundational OT and network architecture knowledge by providing best practices for deploying detection and monitoring sensors, extracting meaningful logs and security events from OT hardware and software, and aggregating this security context into an OT DMZ staging area.

INTRODUCTION TO OT REGULATIONS, STANDARDS, AND GUIDELINES

This course provides an introduction to regulations, standards, and guidance that applies to OT environments, as well as the application of maturity and security levels.

Advanced(300)

OT SECURITY ESSENTIALS

This course teaches students how to defend ICS systems. Students learn to design secure ICS architectures, implement proper firewall placement, position IDS/IPS systems effectively, deploy secure remote access, and implement centralized log aggregation and network monitoring solutions.

Expert (400)

INCIDENT RESPONSE FOR OT

This is a condensed 1-day course focused on physical safety and operational resilience in Industrial Control Systems (ICS). Learn to manage the full IR lifecycle—from prep to hardening—while maintaining mission-critical systems under fire.

LEVEL ZERO
OT CYBER SECURITY CONFERENCE

Cyber-Informed Engineering

Idaho National Laboratory

*Registration to the conference **is not** required to participate. Separate registration **is** required. Meals **are not** included.

Sunday, April 19

Suitable for all levels, student to advanced practitioner

* CYBER-INFORMED ENGINEERING TRAINING FOR INFRASTRUCTURE RESILIENCE

- This 6-hour training introduces participants to the foundational principles and practical applications of Cyber-Informed Engineering (CIE), a transformative framework developed to embed cybersecurity resilience directly into the design of critical infrastructure systems.
- Unlike traditional cybersecurity approaches that focus on digital perimeter defenses, CIE empowers engineers and technicians to design systems that can withstand and mitigate the process impacts of cyber sabotage and digital technology failure.
- Participants will explore how CIE integrates engineered controls, consequence-focused design, and planned resilience to protect essential functions and reduce adversary opportunities for degrading them. The session will cover the 12 core CIE principles, illustrated through real-world use cases in energy, water, and manufacturing sectors. Attendees will engage in interactive exercises to apply CIE concepts to operational technology environments. Participants will receive access to tools to speed and focus the application of CIE for specific functions and a database of engineering controls to incorporate in their own designs.

Thursday, April 23

Suitable for all levels, student to advanced practitioner

*MEETING: CIE DESIGN PATTERNS WORKING GROUP

- This working group meeting will focus on reviewing and enhancing guidance for creating Cyber-Informed Engineering (CIE) design patterns that integrate engineered controls and the larger body of CIE principles into engineered architectures and technologies within oil and natural gas, advanced nuclear, power delivery, and other critical infrastructure systems.
- The effort aims to define criteria, decisions, and constraints that guide engineering design to ensure safety, reliability, and performance while under cyberattack conditions. The approach will be validated through testing and analysis and mapped with the Engineering Controls Database recently released by the Idaho National Laboratory's CIE program (GitHub - idaholab/CIE_EC_Database: Cyber-Informed Engineering addresses how cyberattacks on engineered systems threaten physical safety and reliability beyond data loss. This database provides guidance on defining and applying engineered controls, explaining their distinction from information security measures and their integration into system design.).
- Building on the database of over 62,000 examples of engineered controls across national critical sectors, this initiative seeks to identify recurring patterns that help organizations reduce digital risk. As stated, while engineered controls represent one of twelve CIE principles, incorporating insights from all principles will enable the creation of this comprehensive catalog of design patterns—a powerful tool for national resilience conversations. This workshop invites participants to engage in this Thursday discussion and review the current efforts toward defining this catalog.
- Key activities include:
  - Reviewing existing design patterns and technologies across targeted energy sectors.
  - Creating any new design patterns that embed engineered controls into system architectures to enforce safety and operational requirements despite digital risks.
  - Linking guidance to opportunities identified in the Engineering Controls Database.

LEVEL ZERO

OT CYBER SECURITY CONFERENCE

ICS4ICS CREDENTIALS

- ICS4ICS credentials allow an individual to demonstrate that they have obtained the required training, skills, and experience to perform specific ICS4ICS roles during a cyber incident.

This opportunity is embedded in the main conference agenda , however, to maximize the Table Top Exercise, we are asking people to sign up for it and choose a role ahead of time.

Wednesday, April 22

TYPE 3 OR TYPE 4 ICS4ICS CREDENTIALS (ONLINE FEMA COURSES REQUIRED PRIOR TO LEVEL ZERO)

For those attending and looking to maximize their professional development, we highly recommend completing the FEMA courses beforehand. By arriving pre-qualified, you can leverage the event's experiential opportunities — to immediately pursue your Type 4, or potentially Type 3, credentials. Imagine the value of leaving this conference with your credentialing application essentially complete, a direct result of preparing in advance!

- **Type 4 Credentials**
  - For exercise participants to receive the base level ICS4ICS credentials, they would need to complete the 6 FEMA courses identified below. (free of charge and available online).
  - No application is required but participants should notify the individuals at ics4ics@isa.org after completion of the courses, below.

- **Type 3 Credentials**
  - Participant need to:
    - take the training
    - attend the exercise
    - submit an application for Type 3 (https://www.ics4ics.org/credentials)

- **Required FEMA courses (to be taken prior to the Level Zero Conference)**
  - IS-100: INTRODUCTION TO THE INCIDENT COMMAND SYSTEM, ICS-100
  - IS-200: INCIDENT COMMAND SYSTEM FOR SINGLE RESOURCES AND INITIAL ACTION INCIDENTS
  - IS-700: NATIONAL INCIDENT MANAGEMENT SYSTEM, AN INTRODUCTION
  - IS-800: NATIONAL RESPONSE FRAMEWORK, AN INTRODUCTION
  - IS-706: NATIONAL INCIDENT MANAGEMENT SYSTEM INTRASTATE MUTUAL AID – AN INTRODUCTION
  - IS-201: FORMS USED FOR THE DEVELOPMENT OF THE INCIDENT ACTION PLAN