

# OT Cybersecurity & IEC 62443 Fundamentals Workshop



Join the 10<sup>th</sup> Batch. Register Now.

Venue: Andheri, Mumbai

Date: 14<sup>th</sup> May 2026

## What is this training event all about?

This one day IEC 62443 Fundamentals Workshop covers the basics of OT Security and IEC 62443

OT is short for Operational Technology. These are computer-based systems that control physical objects and parameters in the real world. Although these systems process data, their main function is to monitor and control physical objects and parameters. Some examples of OT systems include:

- \* Industrial Automation and Control Systems (including DCS/PLC/SCADA/SIS)
- \* Building Automation Systems
- \* Heating, Ventilation & Airconditioning (HVAC) Control Systems
- \* Ship Steering & Control Systems, Marine Port cranes
- \* Electrical Grid Management/Electrical Distribution SCADA systems
- \* Automated Warehouse Stacking Systems

There are more such systems, and they are in many different industrial sectors.

## Real Life Exercises

This training event is not all talk. Participate in real life exercises in the workshop including the following:

- a) Evaluate an OT architecture for cyber resilience-spot weaknesses and vulnerabilities & modify it to become more resilient.
- b) Attack a PLC (actual hardware branded product-no simulation) via a network, manipulate the actual outputs, manipulate analog values shown on the SCADA/HMI without changing the PLC ladder program.



## Some Participants in earlier workshops & feedback



Earlier batches were conducted in Mumbai (multiple times), Baroda, Dahej & Bengaluru. Participants from marquee organizations from diverse sectors such as Space & Defence (e.g. ISRO, DRDO, Bharat Electronics), Manufacturing Industries (e.g. GACL, Yokohama Tire), EPC (e.g. Toyo Engineering, Thyssenkrupp, Worley), IT Consulting ( e.g. HCL Technologies, Deloitte), Industrial Automation (e.g. Schneider), Robotics ( e.g Addverb), Govt Bodies (e.g CPRI, DRDO) and others have participated in earlier workshops.

---

*Thanks to this workshop, I will now be able to define cybersecurity requirements & specifications very well for my client for the next project as well conduct risk assessments effectively*  
*Participant from Worley*

---



---

*Great knowledge gained about OT Security. It will help protect our DCS from cyber attacks*  
*Participant from Gujarat Alkalies and Chemicals*

---



---

*I was able to very well understand the different parts of IEC 62443 and how to apply the clauses of different parts-*  
*Participant from Thyssenkrupp*

---



---

*Exciting real life examples and Case Studies-*  
*Participant from Toyo Engineering*

---



---

*The workshop was very good and covered very important topics in OT Cybersecurity-*  
*Participant from DRDO*

---



Abhisam's OT Cybersecurity workshops and self-paced e-learning courses have seen participation from several hundreds of professionals from all over the world including from several marquee organizations.

### Why is OT Cybersecurity different from IT cybersecurity?

Both OT systems and IT systems are computer-based systems that may be vulnerable to cyberattacks. A cyber-attack on an IT system may result in loss of data, information and perhaps money; however, **an attack on an OT system may result in not only loss or theft of data but may also lead to physical consequences such as fires, explosions, loss of containment, equipment damage, harm to people and harm to the environment.**

Many OT systems that exist today are insecure from the design stage itself, since it was never envisaged that they would be the target of cyberattacks. Additionally, the priorities of defending OT systems and IT systems are different, so the strategies and techniques are also different. For IT systems confidentiality of data is a priority whereas for OT systems, availability & safety are priorities. Furthermore, OT systems may be a few generations older than IT systems and the cyber security tools commonly used to protect IT systems may not be suitable for protecting OT systems.

Additionally, the standards that govern OT systems (such as IEC 62443) are different from IT cybersecurity standards.

### Who Should attend?

Any technical professional who has some work experience in working with any IT system or OT system can attend. Participants should have a basic understanding of computers, networking and preferably be familiar with typical industrial operations. Some typical attendee profiles are:

- \* Instrumentation & Industrial Automation, Control System Professionals from any industry
- \* IT Heads (CIOs) from manufacturing or Critical Infrastructure, Marine Transportation, Defence, Manufacturing, Oil & Gas, Chemicals or similar organizations having cyber-physical systems

- \* IT Cybersecurity Professionals including CISOs who wish to understand OT security in more detail
- \* IT Cybersecurity Auditors
- \* Smart OT Device Developers & Evaluators
- \* OT related Software & application developers
- \* Process Safety Professionals
- \* Industrial Plant or Process Engineers, Plant Managers
- \* Electrical Engineers involved in Electrical SCADA/ Electrical Grid/ Distribution/Load Dispatch/ Sub stations
- \* Government Regulatory authorities
- \* Cybersecurity Management consultants

## What will be covered?

The following topics will be covered.

1. Introduction to Operational Technology (OT) systems.
2. Differences between OT security and IT security.
3. Basic Concepts of OT security- Threats, Vulnerabilities & Attacks
4. Case Study of an OT attack
5. Evaluating OT System architectures for vulnerabilities and weaknesses
6. Overview of different standards & practices related to OT cybersecurity (IEC 62443, NIST 800-82)
7. Introduction to IEC 62443 & **Changed Structure in 2026**
8. Overview of following (published) parts of IEC 62443
  - IEC 62443-1-1
  - IEC 62443-2-1 (updated version)
  - IEC 62443-2-3
  - IEC 62443-2-4 (updated version)
  - IEC 62443-3-1
  - IEC 62443-3-2
  - IEC 62443-3-3
  - IEC 62443-4-1
  - IEC 62443-4-2

9. Hardware Demo: Attacking a branded PLC in a network with Open-Source Tools, manipulating the actual PLC outputs as well as values seen on SCADA/HMI without modifying the PLC program.

## About Abhisam

Abhisam is a global provider of e-learning courses & certifications for technical professionals in the Manufacturing, Oil & Gas, Chemicals, Power, Electronics, EPC, Logistics, IT, Industrial Automation sectors, with many marquee organizations as customers. Since 2003, Abhisam has pioneered the use of technology in skill upgradation and competency management. Abhisam's CICIP® (Certified Industrial Cybersecurity Professional) program is used by leading companies such as IBM, FLSmidth, SASOL, Black & Veatch, CEMEX and many others to build competency of their employees in OT cybersecurity worldwide.

## How to Register?

(Limited Seats, book early to get in before doors close).

The investment is Rs. 11,800/- per participant all inclusive (Taxes, Lunch/Tea/Coffee, printed training material and Certificate).

**Note:** Cost is decided based on location, dates, number of seats and may vary widely from Country to Country. Make your payment via UPI code here

For organizations wishing to nominate, & requiring a GST Invoice, please contact us for Invoicing.

## Will I get a Certificate?

A Certificate of Participation in the IEC 62443 Fundamentals Workshop will be provided. If you would like to have a Certificate of Competency and a title, then you can consider joining the CICIP® program.



## What is the CICP® program?

The CICP® program is our flagship Professional Certification program. The **Certified Industrial Cybersecurity Professional (CICP®)** is a self-paced fully online course that is popular all over the world. It has been taken by hundreds of professionals from all over the world, including those from different areas such as Asset Owners, EPC companies, IT consultants, Automation vendors, independent cybersecurity companies and more.

On completion of all modules of this course, you will earn the title of CICP® that you can affix to your name such as for example John Q. Public, CICP® . You also earn a Certificate of Competency, the CICP® certificate and electronic badge that you can display on LinkedIn.

## Where can I get more information about OT Cybersecurity?

Please visit the Abhisam website at <https://www.abhisam.com/cybersecurity-information/> for more information about OT Cybersecurity and IEC 62443

## More Information?

Contact us at [sales@abhisam.com](mailto:sales@abhisam.com) or Call us/SMS/Whatsapp on +91 9664404771