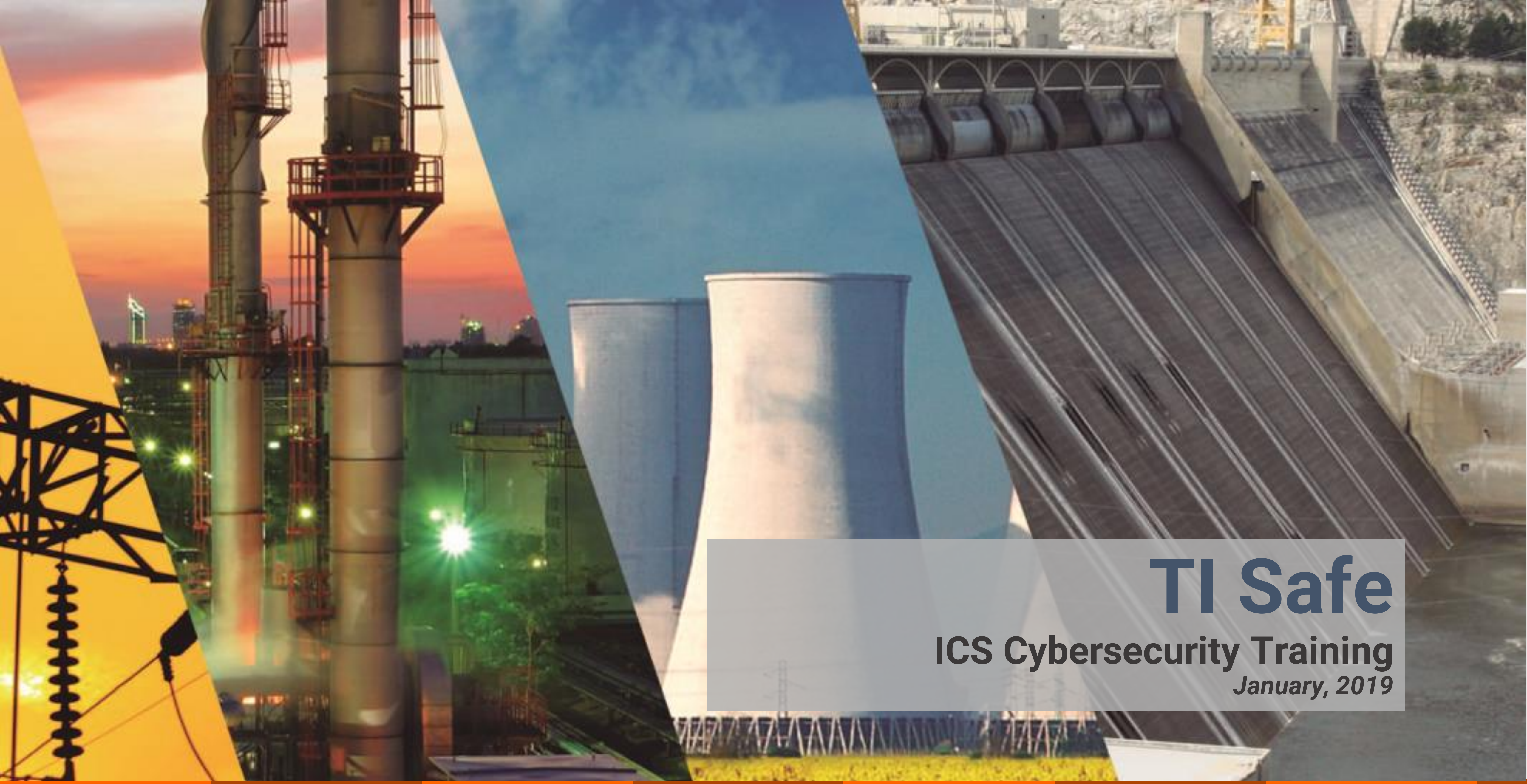


TI Safe

ICS Cybersecurity Training

January, 2019

TI Safe Academy

ICS Cybersecurity - Classroom Training

Theory and practices on how to identify industrial cyber threats, evaluate risks and plan security measures according to TI Safe´s ICS.SecurityFramework.

ICS Cybersecurity – Online Training

The same content of the classroom training available in our virtual environment.
There are 10 modules of video lessons with tests at the end of each module.

CASE Certification

The CASE exam determines whether a professional has the appropriate knowledge to protect an industrial network.

CERTIFIED AUTOMATION SECURITY ENGINEER

ICS Cybersecurity Training - Goals

- Educate professionals to be capable of identifying risks in industrial networks, as well as recommend the main countermeasures for them, according to the main international security standards and the ICS.SecurityFramework methodology developed by TI Safe.
- To capacitate professionals to design and deploy the CSMS (Cyber Security Management System) in critical infrastructure automation networks.
- Teach professionals how to implement monitoring and management controls for the industrial cyber security solutions implemented in automation plants and control systems.

ICS Cybersecurity Training - Contents

Curricular Unit	Goals	Contents
Initial Presentations	Presentation of training objectives and rules, instructors and students.	• Presentation of training objectives and bibliography • Short presentation of instructors and students
Chapter I – Introdution to Industrial networks and SCADA	Overview of a SCADA system, its elements, protocols and typical architecture.	• Overview of an ICS • Industrial control systems architecture. The Purdue model (ISA-95) • Industrial networks and protocols • SCADA systems • Industry 4.0
Chapter II - Critical Infrastructures and Cyberterrorism	Definition of critical infrastructures, their importance and presentation of recent cyberterrorism cases. Presentation of the types of attackers, the market that feeds the cyber attacks and the main challenges for implementation of cyber security in critical infrastructures.	• What are Critical Infrastructures? • Cyber warfare – the 5th dimension of war • Characteristics of the new attackers • The cybercrime market • Vulnerabilities in industrial systems • History of cyber attacks to industrial networks • Malware, the main hacker´s weapon • Cyber security challenges for industrial control systems
Chapter III – Risk Analysis	Presentation of techniques for elaboration of risk analysis in industrial networks according to ISA/IEC-62443 standard and the TI Safe´s ICS.SecurityFramework methodology.	• Concepts • Risk Scenarios • Classification of critical infrastructure networks • Classification methods • Risk analysis • Static analysis – evaluated controls • Physical security analysis • Dynamic analysis • Risk analysis report

ICS Cybersecurity Training - Contents

Chapter IV - Governance for industrial networks	Presentation of the main international standards that guide the implementation of cyber security policies and procedures in industrial networks. Presentation of concepts of governance in industrial networks and the basic concepts for the development of a business continuity plan (BCP).	• Reference standards • The ANSI/ISA 99 | ISA/IEC 62443 standard • The NIST 800-82 Guide • The NERC-CIP standard • Automation security policites • Business Continuity Plan (BCP)
Chapter V - Perimeter security in automation networks	Presentation of Next Generation Firewalls and other solutions for perimeter security in automation networks. Security strategies fo wireless networks security in industrial environments.	• Firewall architectures and DMZ deployment • Firewall policies • Next-generation firewalls for use in industrial networks • Industrial WiFi security
Chapter VI - Industrial networks protection	Details of the defense in depth strategy recommended by ANSI/ISA-99 / ISA 62443 and presentation of the zones and conduits model Presentation of cyber security solutions used for internal automation networks protection.	• Defense in depth model • Zones and Conduits model • VLANs and Zero Trust • Industrial firewalls • Security gateways • Unidirectional security gateways • Inventory and assets visibility with Machine Learning
Chapter VII – Malware Control	Presentation of the weaknesses of solutions traditionally used for protection in automation networks. Malware control in OT networks and presentation of modern solutions to prevent malware attacks.	• Considerations about the use od of antivirus and patches in automation networks • Blacklisting x Whitelisting • Solution for protection against malware infections in automation networks

ICS Cybersecurity Training - Contents

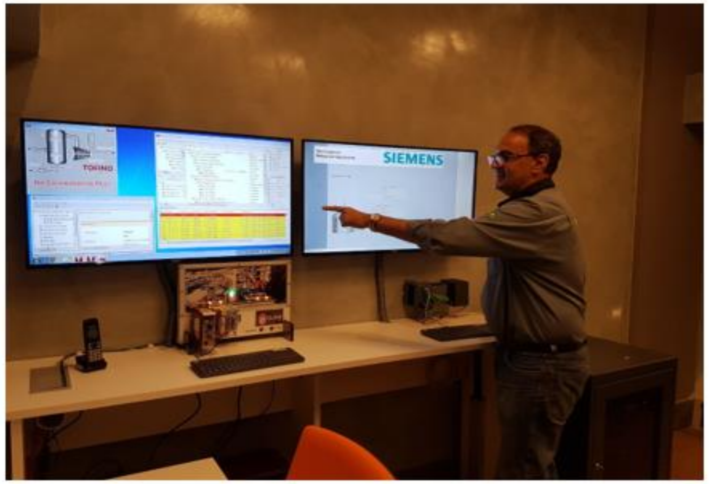
Chapter VIII - Data Security in industrial networks	Presentation of threats to industrial networks access control and the weaknesses of remote access to industrial networks. Presentation of encryption fundamentals and their applications in industrial network security (VPNs).	• Threats to the access control • Access control: concepts, Methodologies and Techniques • Main authentication mechanisms • Remote access to industrial networks and SCADA • Cryptography in industrial networks and VPNs
Chapter IX - Education and Awareness	Presentation of concepts to build an education and awareness plan aiming at establishing the culture of cyber security for automation networks.	• Education and awareness plan • Training and certifications available on the market • Awareness-raising methods • Main Events
Chapter X – Planning and Monitoring	Presentation of methods for the implementation of continuous monitoring in automation plants, including SIEM technologies and managed security services. Presentation of new technologies for ICS Cybersecurity.	• Planning for deployment of security controls in an industrial network • Continuous monitoring and trends • SIEM and ICS-SOC • New technologies for ICS cybersecurity
Laboratory Practicies	Ensure that the student has contact with the main attack tools used by hackers and also the main ICS Cybersecurity countermeasures presented during the training.	• Presentation of environment for hacking based on Kali Linux 2017 V3 • PLC variable scan using Wireshark • Attack by manipulating PLC TAG values • Internal DOS attack against PLC • Development of a cyberweapon • APT attacks to the PLC; • External hacking via Shodan • Practice with Malware Control Solution

ICS Cybersecurity Training - Training Apostilles

- The training apostilles are available in English and distributed in digital format (PDF file).
- They are constantly updated and improved. In addition to the mentioned bibliographical references, we have the important support of the leading companies in the ICS Cybersecurity arena to ensure that we have the insights on the latest industrial systems defense technologies used today.
- One week before the start date of each training, TI Safe will send a link to download the training apostiles to the enrolled students.

ICS Cybersecurity Training – Pratical Classes

- During the training will be held practical classes and technical demonstrations of attacks and defenses against simulated automation networks.
- For the demonstration of attacks against industrial networks we count on simulators of automation networks industrial plants shown in the figure below:



ICS Cybersecurity Training - Duration

- The training is formatted to be performed within 20 hours of class.
- TI Safe is open to discuss any changes or enhancements that may be necessary for the execution of the ICS Cybersecurity training according to the customer´s demands.

Thank You!

contato@tisafe.com

@tisafe