€TRAINING

Securing Intelligent Transportation Systems

Securing Intelligent Transportation Systems

Introduction:

This training program offers a comprehensive curriculum aimed at enhancing participants' proficiency in safeguarding digital infrastructure within transportation systems. Through it, individuals are equipped with the knowledge and skills necessary to mitigate cyber threats and ensure the resilience of intelligent transportation systems against cyber attacks.

Program Objectives:

At the end of this program, participants will be able to:

- List and describe major ITS Cybersecurity Threats and Vulnerabilities Understanding the ITS environment and its architecture
- Create mitigation methods after doing an ITS Cybersecurity Risk Assessment.
- Create an incident response and ITS monitoring plan.
- List and evaluate the most significant present-day and future defensive strategies.
- List and understand the most significant ITS and Cybersecurity Standards.

Targeted Audience:

- Project Managers.
- Technology Engineers, Chief Technology Officers CTOs and Chief Information Officers CIOs.
- Strategic Development Personnel.
- Transport Operators, Engineers, Managers, and Researchers.
- ITS and Cybersecurity Industry Consultants.
- IT and Cybersecurity Professionals.
- Operators and Professionals of Transport Systems.
- City governments Involved in Transport Systems.
- Enterprises involved in the design of Transport System.

Program Outline:

Unit 1:

ITS Cybersecurity Risk Assessment and Mitigation:

- Cybersecurity Risk assessment in ITS.
- Cybersecurity challenges.
- Approaches in ITS cybersecurity.
- Cybersecurity protection frameworks: NIST and others.
- Cybersecurity Controls.

Unit 2:

Cybersecurity & The Intelligent Transportation ITS System Environment:

- How cyber-attacks happen.
- Industries affected.
- The Intelligent Transportation System ITS Environment.
- Role of Autonomous vehicles.
- ITS Architecture.
- New mobility platforms.
- A Need to Secure ITS.

Unit 3:

ITS Monitoring and Incident Response:

- Penetration Testing for ITS.
- Cybersecurity Monitoring.
- Event Management.
- Incident Response.
- Best practices for first responders.

Unit 4:

ITS & Cybersecurity Standards - Current and Future Practices:

- ITS & Cybersecurity Standards.
- Good Practices.
- Gap Analysis.
- Plan of action.
- Innovative approaches: AI, blockchain.

Unit 5:

ITS models, Infrastructure, Cybersecurity Threats & Vulnerabilities:

- Overview of Cybersecurity.
- ITS Models: Operators.
- ITS systems and infrastructure.
- Communication systems, wired, wireless.
- Data management, sharing, and governance.
- Threats & vulnerabilities in ITS.