Training Course

	Industrial Cyber Security 2 (IES-CS2)
Objective	In this training attendees will learn techniques to establish and test protection measures to increase network security.
Prerequisites	Strong networking experience is required, based on experiences in the field or previous attendance of the "Layer 2 Networking" (IES-L2), "Layer 3 Networking" (IES-L3) and "Industrial Cyber Security 1" (IES-CS1) courses. Preferably participants have reached Moxa Certified Engineer certification level.

Content	**Architecture of Cybersecurity**
	
	- IEC-62443
	   - Perdue Model
	   - Zones and Conduits
	   - Remote Access
	
	Network Attack Types
	
	- Attack Vectors Overview
	- Password Cracking
	   - Methodologies and Tools
	- DoS (Denial of Services)
	   - Methodologies and Tools
	- ARP Spoofing
	   - Methodologies and Tools
	- Port Scan
	   - Methodologies and Tools
	- Man in the Middle
	   - Methodologies and Tools
	- Modbus attacks
	   - Methodologies and Tools
	- Profinet Attacks
	   - Methodologies and Tools
	
	Forensics
	
	- Vulnerabilities
	- Network Intrusion Analyses
	
	Defense Mechanisms

	- Firewall
	
	    - Network Segmentation
	
	    - Zones
	
	    - Rule based protection.
	
	- IPS/IDS - Create
	
	    - Concepts
	
	    - Signature based protection.
	
	    - White listening
	
	    - Virtual Patching
	
	    - SA x Pro (SDC)
	
	- Anti-Virus – Create
	
	Secure Remote Connection
	
	- Concept
	
	- Applications
	
	Game
	
	- Cybersecurity Architecture Game
	
	- Game - Red/Blue

Duration	1.5 Day
Certification	Industrial Cyber Security 2 (IES-CS2)