Tel No:+97126654546 | Fax No:+97126654182 | Email: training@cmc-me.com | www.cmc-me.com

IE290:
Using ISA/IEC 62443 Standards to Secure Control Systems

Training Description:

Industrial Control Systems (ICS), including SCADA, DCS, PLC-based systems, and critical automation environments, are increasingly exposed to cyber threats due to connectivity, digital transformation and integration with enterprise networks. Traditional IT security approaches alone are insufficient for protecting operational technology (OT) environments, where safety, reliability and availability are paramount.

This intensive training course provides a comprehensive understanding of the ISA/IEC 62443 series of standards — the globally recognized framework for industrial cybersecurity. Participants will gain both conceptual and practical knowledge of how to apply these standards to design, implement, assess and maintain secure control system environments.

The training course bridges theory and real-world application by combining standard interpretation, risk-based thinking, architecture design, governance strategies, and hands-on exercises. Attendees will leave with a structured methodology for building and managing cybersecurity programs aligned with ISA/IEC 62443.

Training Objectives:

By the end of the training, participants will be able to:

- ✓ Understand the structure, purpose and components of the ISA/IEC 62443 standards family
- ✓ Explain the differences between IT security and OT/ICS security
- ✓ Identify threats, vulnerabilities, and risks specific to control systems
- ✓ Apply a risk-based approach to industrial cybersecurity
- ✓ Design secure ICS architectures using zones and conduits
- ✓ Define security requirements and target security levels
- ✓ Implement technical and organizational security controls
- ✓ Conduct security assessments and gap analyses
- ✓ Develop cybersecurity policies, procedures and governance frameworks
- ✓ Align industrial cybersecurity with compliance, safety and operational goals

Training Designed for:

This training course is intended for professionals responsible for the design, operation, management, or protection of industrial control systems, including; Control system engineers and automation engineers, SCADA, DCS, and PLC specialists, Cybersecurity and information security professionals, OT security practitioners, System integrators and solution architects, Maintenance and reliability engineers Plant managers and operations managers, Risk management and compliance personnel and Consultants working with industrial environments.

No deep prior cybersecurity expertise is required, although familiarity with industrial systems is beneficial.

Training Requirement:

"Hands on practical sessions, equipment and software will be applied during the course if required and as per the client's request."

Tel No:+97126654546 | Fax No:+97126654182 | Email: training@cmc-me.com | www.cmc-me.com

Contents can be adapted to your specific wishes. It is therefore possible to focus on specific modules of the training course as per client's learning needs and objectives. Further, it should be forwarded to us a month prior to the course dates.

Training Program:

DAY ONE:

FOUNDATIONS OF INDUSTRIAL CYBERSECURITY & ISA/IEC 62443 OVERVIEW

- Introduction to industrial cybersecurity challenges
  - Differences between IT and OT security priorities
  - Common ICS architectures and communication flows
  - Threat landscape for control systems
  - Consequences of cyber incidents in industrial environments
- Overview of ISA/IEC 62443 standards
  - Structure and organization of the 62443 series
  - Key terminology and concepts
  - Roles and responsibilities defined by the standards
  - Lifecycle approach to security
- Security principles for industrial systems
  - Defense-in-depth strategies
  - Safety vs. security considerations
  - Balancing availability, reliability and protection

DAY TWO:

RISK ASSESSMENT & SECURITY LEVELS

- Risk management fundamentals
  - Threats, vulnerabilities, and consequences
  - Risk identification techniques
  - ICS-specific risk considerations
- ISA/IEC 62443 risk-based approach
  - Asset identification and classification
  - Security zones concept
  - Conduits and communication control
- Security Levels (SL)
  - Definition and interpretation of SL 1–4
  - Mapping risks to security levels
  - Establishing target security levels
- Practical exercises
  - Sample risk scenarios
  - Defining zones and assigning security levels
  - Discussion of real-world case studies

DAY THREE:

SECURE ARCHITECTURE & SYSTEM DESIGN

- Secure ICS architecture principles

- Segmentation strategies
- Network separation and layering
- Trust boundaries

❖ Zones and conduits in depth
- Logical vs. physical segmentation
- Communication control strategies
- Minimizing attack surfaces

❖ Security requirements engineering
- Functional and technical security requirements
- System hardening concepts
- Secure remote access design

❖ Designing for resilience
- Redundancy and fail-safe mechanisms
- Incident containment strategies

❖ Workshop
- Designing a secure ICS architecture
- Applying segmentation and SL concepts
- Peer review and critique

DAY FOUR:

SECURITY CONTROLS & IMPLEMENTATION

❖ ISA/IEC 62443 control categories
- Technical controls
- Procedural controls
- Organizational controls

❖ Identity and access management in ICS
- Role-based access control
- Authentication mechanisms
- Privileged access management

❖ System and network protection
- Firewalls and industrial DMZ
- Whitelisting and application control
- Secure communication protocols

❖ System hardening techniques
- Patch management challenges in OT
- Configuration management
- Secure device management

❖ Monitoring and detection
- Security event monitoring in ICS
- Anomaly detection concepts
- Incident detection strategies

❖ Practical discussions
- Control selection based on SL
- Constraints of legacy systems

DAY FIVE:

GOVERNANCE, COMPLIANCE & SECURITY PROGRAM DEVELOPMENT

- Cybersecurity governance frameworks
  - Policies, procedures and standards
  - Roles, responsibilities and accountability
- ISA/IEC 62443 lifecycle approach
  - Continuous improvement
  - Security management systems
- Security assessments and audits
  - Gap analysis techniques
  - Compliance evaluation
  - Documentation requirements
- Incident response in industrial environments
  - Preparation and planning
  - Coordination with operations and safety teams
  - Recovery and lessons learned
- Building a cybersecurity roadmap
  - Prioritization strategies
  - Balancing cost, risk and operations
  - Integration with business objectives
- Final workshop
  - Developing a cybersecurity strategy aligned with 62443
- Course Conclusion
- POST-ASSESSMENT and EVALUATION

Training Methodology:

This interactive training course includes the following training methodologies as a percentage of the total tuition hours:

- 30% Lectures, Concepts, Role Play
- 70% Workshops & Work Presentations, Techniques, Based on Case Studies & Practical Exercises, Gamification, Software & General Discussions
- Pre and Post Test

Training Certificate(s):

CMCT Internationally recognized certificate(s) will be issued to each participant who completed the course.

Training Fees:

TBA as per the course location - This rate includes participant's manual, hand-outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Note: The 5% VAT (Value Added Tax), will be effective starting 01st of January 2018 as per the new regulation from the UAE Government. The VAT applies for all quotation both for local and abroad.

Training Timings:

Daily Timings:

07:45 - 08:00	Morning Coffee / Tea
08:00 - 10:00	First Session
10:00 - 10:20	Recess (Coffee/Tea/Snacks)
10:20 - 12:20	Second Session
12:20 - 13:00	Recess (Prayer Break & Lunch)
13:00 - 14:00	Last Session

For training registrations or in-house enquiries, please contact:

Aisha Relativo - Training & Career Development Manager
aisha@cmc-me.com / training@cmc-me.com
Tel.: +971 2 665 3945 or +971 2 643 6653 | Mob.: +971 52 2954615