exida

www.exida.eu

DE0612 Navigating the Cyber Resilience Act with IEC 62443 Best Practices

Are your IACS compliant to the EU Cyber Resilience Act (CRA)?

How can IEC 62443-4-1/-2 help to reach CRA compliance?

How do CRA obligations impact vulnerability management and incident reporting for industrial devices?

What documentation and evidence are needed to demonstrate CRA compliance?

Join our Training to learn about best practices for building and verifying secure industrial components in a CRA context

Agenda and Content

- Overview of the EU Cyber Resilience Act (CRA) and its Implications
- Introduction to Industrial Automation and Control Systems (IACS) Cybersecurity
- Introduction to IEC 62443 Family and its relevance for CRA
- Essential Cybersecurity Requirements of the CRA
- Concepts of IEC 62443-4-1 and IEC 62443-4-2
- Creating CRA-Compliant Documentation
- Threat Modeling and Risk Assessment
- Cybersecurity Security Requirements for IACS
  - Secure Software Development Fundamentals
  - Hardware & Embedded Security Basics
  - Security Verification and Validation Testing
- Vulnerability Handling and Monitoring under CRA Obligations
- Incident Response Planning and Execution under CRA Obligations

Industrial products are becoming smarter, more connected, and increasingly exposed to cyber threats. This expert-led training equips professionals with the knowledge and practical tools to **meet the cybersecurity requirements of the EU Cyber Resilience Act (CRA)** for industrial automation and control components.

Participants will learn how to integrate security throughout the entire product lifecycle - from concept and development to validation and ongoing maintenance - ensuring that products are resilient, safe, and compliant with CRA obligations making use of **IEC 62443 concepts**.

You will gain hands-on experience in identifying risks, implementing secure design practices, handling vulnerabilities, and preparing for incidents, giving you the insight needed to **demonstrate compliance and strengthen product resilience in the face of regulatory and cyber challenges**.

Who should attend?

This training is designed for professionals involved in the design, development, testing, and technical assessment of industrial automation and control system (IACS) products, with a focus on building cyber-resilient components in a CRA context. It is particularly valuable for:

- **Quality, product, and certification managers** aiming to integrate cybersecurity best practices into product development and lifecycle processes.
- **Cybersecurity specialists and technical assessors** supporting product security evaluations, internal reviews, or third-party assessments.
- **System, hardware, and security engineers** responsible for implementing technical cybersecurity measures in industrial products.
- **Project managers and product owners** overseeing secure product development and cyber-resilience activities.

Duration: 2 days

Language: English or German in agreement with the participants.

The training material will be in English.

Location: Online or Onsite @ Neubiberg *exida* Office

Customer specific on-site or online training is also possible. We will adjust the training content to your specific needs - just get in touch!

Certificate: Each participant can voluntarily take an exam and earn a Cybersecurity Practitioner (CSP) certificate, or receive a confirmation of attendance listing the covered topics.

For more information, please contact:

Kerstin Tietel
+49 89 44118232
kerstin.tietel@exida.com