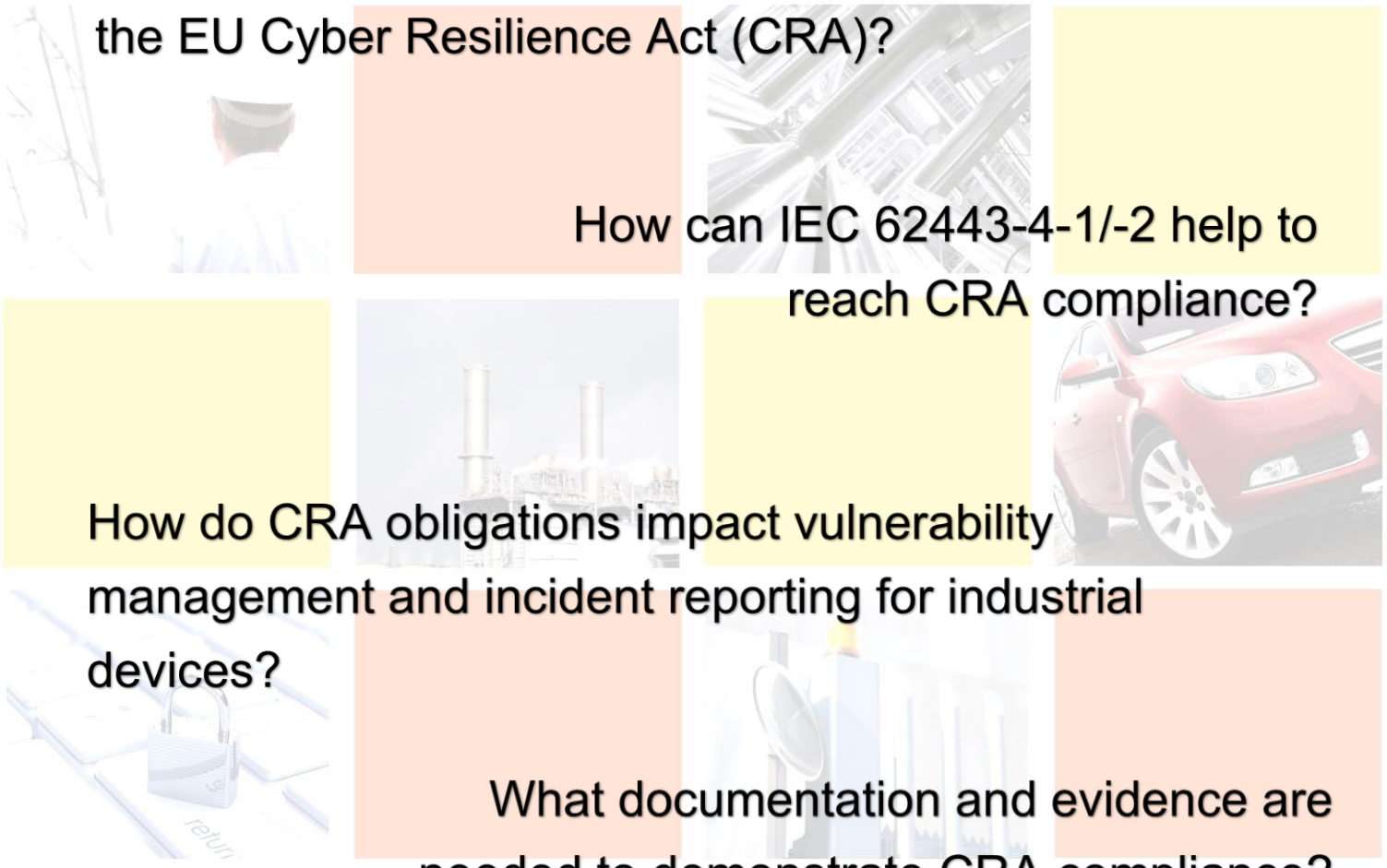
exida

www.exida.eu

DE0612 Navigating the Cyber Resilience Act with IEC 62443 Best Practices



Are your industrial components 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 confidently navigate the Cyber Resilience Act (CRA)

exida Excellence in *Dependable Automation*

Agenda and Content

- Cybersecurity Introduction & Threat Landscape
  Why the CRA exists: current threats, incidents, and industrial context
- CRA Basics for Engineers
  Scope, timeline, key principles and roadmap from product classification to CE marking and post-market activities
- CRA Structure, Obligations & Roles
  Legal structure, essential requirements, roles of manufacturers and authorities, and enforcement mechanisms
- Product Classification & Conformity Assessment Procedures
  Does your product fall under the EU Cyber Resilience Act?
- From CRA Requirements to Engineering Activities
  Translating regulatory requirements into engineering practices, controls, and evidence
  - Risk Assessment & Threat Modeling under the CRA
  - Using IEC 62443 as a CRA Enabler
  - CRA Annex I to IEC 62443 Mapping Proposal
  - Technical Documentation (CRA Annex VII)
- Vulnerability Handling & Incident Reporting
  Processes, coordinated disclosure, and CRA reporting obligations
- CRA vs Other EU Regulations
  Interaction with e.g., Machinery Regulation, NIS2, and GDPR

Industrial products are becoming smarter, more connected, and increasingly exposed to cyber threats. This expert-led training equips professionals with knowledge 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 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:	1 day
Language:	English or German in agreement with the participants. The training material will be in English.
Location:	Online 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
✉ trainings.germany@exida.com