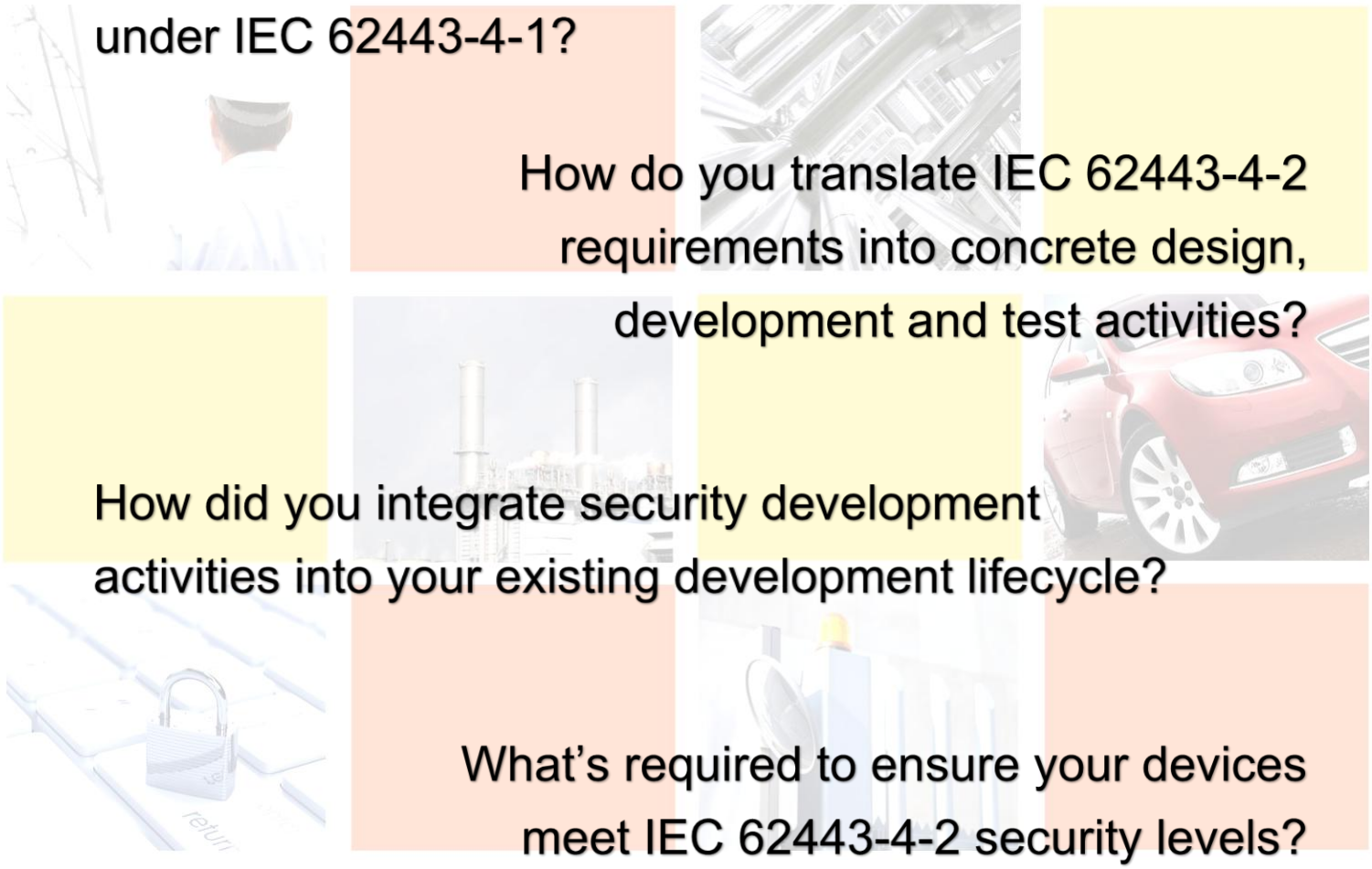
exida

www.exida.eu

DE0611 IEC 62443-4-1/-4-2 in Practice: Building and Verifying Secure Industrial Components



What does “secure by design” really mean under IEC 62443-4-1?

How do you translate IEC 62443-4-2 requirements into concrete design, development and test activities?

How did you integrate security development activities into your existing development lifecycle?

What’s required to ensure your devices meet IEC 62443-4-2 security levels?

Join our Training and learn about Building and Verifying Secure Industrial Components

exida excellence in *Dependable Automation*

DE0611 IEC 62443-4-1/-4-2 in Practice: Building and Verifying Secure Industrial Components

Agenda and Content

- Welcome, Introduction, Training Goals
- IACS Cybersecurity Introduction and Threat Landscape: Why It Matters for Industrial Components
- IEC 62443 Family incl. the link to the EU Cyber Resilience Act
- Security Development Lifecycle and Security Management Process acc. to IEC 62443-4-1 as part of the overall development lifecycle
- Threat Modelling, Risk Assessment & Security Levels
- IEC 62443-4-2 Technical Security Requirements
- Secure Software Development Fundamentals
- Hardware & Embedded Security
- Vulnerability Handling & Monitoring
- Security Verification and Validation Testing
- Incident Response Planning and Execution
- Q&A and Wrap-Up

Industrial products are becoming smarter, more connected - and more exposed to cyber threats. This expert-led training gives professionals the essential understanding and practical tools to build and assess secure industrial automation and control components in line with IEC 62443-4-1 and -4-2. Participants learn how to integrate cybersecurity into every stage of product development, from initial concept through validation and maintenance.

DE0611 IEC 62443-4-1/-4-2 in Practice: Building and Verifying Secure Industrial Components

You'll learn to apply the IEC 62443 standards hands-on - identifying risks, implementing secure design practices, and verifying technical security requirements. By thinking like both a developer and an attacker, you'll gain the insight needed to strengthen product resilience, demonstrate compliance, and prepare for upcoming regulatory demands such as the EU Cyber Resilience Act.

Who should attend?

This training is designed for professionals involved in the development, testing, and assessment of industrial automation and control system (IACS) products. It is particularly valuable for:

- **System and security engineers** responsible for applying IEC 62443 technical requirements.
- **Quality, compliance, and certification managers** seeking to align development processes with IEC 62443-4-1 and -4-2.
- **Cybersecurity specialists and assessors** supporting product security evaluations or audits.
- **Project managers and product owners** overseeing secure product development lifecycles.
- **Product and software developers** implementing secure design and coding practices.

DE0611 IEC 62443-4-1/-4-2 in Practice: Building and Verifying Secure Industrial Components

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