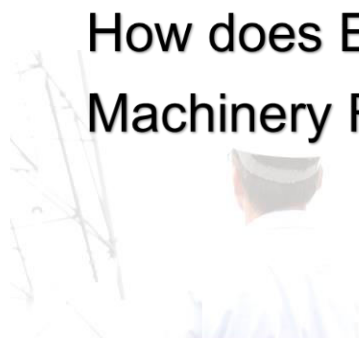
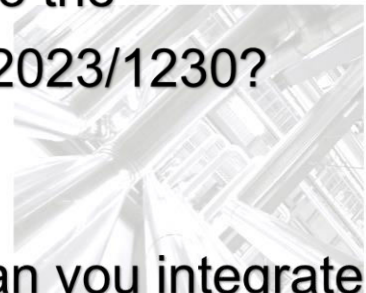


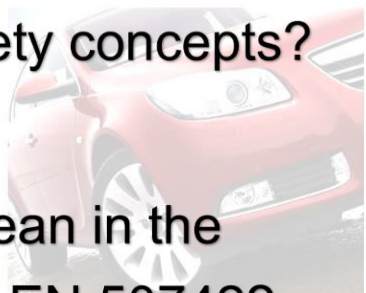
# DE0613 EN 50742 in Practice - Cybersecurity for Machinery and Regulatory Compliance



How does EN 50742 relate to the Machinery Regulation (EU) 2023/1230?



How can you integrate cybersecurity into machinery safety concepts?



What does “protection against corruption” mean in the context of the Machinery Regulation and the EN 50742?



How can you leverage IEC 62443 for efficient compliance?

## Join our Training

and gain practical insight into EN 50742 and regulatory requirements

# Agenda and Content

- ◆ Cybersecurity for Machinery – Why It Matters and Regulatory Requirements (Machinery Regulation and Cyber Resilience Act)
- ◆ Overview of EN 50742 and its key concepts
- ◆ Risk-Based Approach to Safety & Security
- ◆ Two Implementation Paths of EN 50742
  - Approach A: Standalone methodology
  - Approach B: Integration with IEC 62443
- ◆ Leveraging IEC 62443
  - Mapping EN 50742 to IEC 62443-3-3 / 4-1 / 4-2
  - Secure development lifecycle integration
  - Efficient reuse of existing cybersecurity processes
- ◆ Relation to the EU Machinery Regulation (EU) 2023/1230
  - Essential requirements for cybersecurity
  - How EN 50742 supports presumption of conformity
  - Practical compliance strategy
- ◆ Q&A and Wrap-Up

Machinery is becoming connected more and more – and therefore exposed to cyber threats. EN 50742 provides a structured, risk-based approach aiming to ensure that cybersecurity vulnerabilities do not compromise safety.

At the same time, it serves as a bridge between safety standards, IEC 62443, and the EU Machinery Regulation, enabling manufacturers to demonstrate compliance efficiently and future-proof their products.



***Current Status of EN 50742 & Harmonisation:*** EN 50742 is currently being finalized as a key European standard addressing cybersecurity for machinery in the context of the EU Machinery Regulation (EU) 2023/1230.

*It is currently in draft stage (prEN 50742) and harmonisation is not yet completed. It is expected to provide presumption of conformity with relevant cybersecurity requirements.*

*Early adoption of EN 50742 enables manufacturers to prepare for the 2027 regulatory application.*

## Who should attend?

This training is designed for professionals involved in the development, testing, and assessment of machinery. It is particularly valuable for:

- ◆ **System and safety engineers** working on machinery design
- ◆ **Cybersecurity specialists** in industrial environments
- ◆ Compliance and certification managers
- ◆ **Machine manufacturers, integrators, and product owners**
- ◆ **Project managers** responsible for regulatory compliance

**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](mailto:trainings.germany@exida.com)