

Ensuring Cybersecurity and Digital trust across the entire digital value chain

Add value.
Inspire trust.



IoT

Ensuring consumer and industrial IoT (IIoT) cyber-resilience

- Ensuring security by design principles for IoT (smart watches, smart bulbs etc.)
- Enabling cyber-resilient factories through secure IIoT.
- Regulatory compliance for upcoming regulations and support with regulatory readiness.

Critical Infrastructure

Critical Infrastructure Protection (CIP) at factory and supply chain level

- Regulatory compliance for critical infrastructure entities (energy, data protection, food, healthcare, waste management etc.).
- Operational resilience through unbiased third-party risk assessment.

Mobility

Ensuring safer and secure mobility for our society

- Automotive cybersecurity and software update management systems .
- Regulatory compliance and adherence to standards (e.g. ISO21434, ISO 24089 etc.).
- Testing of automotive components and modules.

Medical Device

Enhanced cyber resilience and regulatory compliance for medical devices

- Cybersecurity of critical medical devices such as pacemakers, infusion pumps etc.
- Includes security by design and security by default evaluation of medical devices.

Office IT (ISMS)

Ensuring effective information security management systems (ISMS) across the entire value chain

- ISMS cybersecurity.
- Organisational risk management and risk mitigation.
- Information Security Management Systems Certifications.
- Payment Security

Training

Empowering the “human firewall” through education

- Standards-based training for cybersecurity practitioners (e.g. ISO 27001, TISAX, Industrial Security Foundation etc.).
- Data privacy related training
- Management level training for effective cybersecurity risk management and decision making.

Industrial

Enabling zero downtime through operational resilience

- Industrial cyber risk assessment & risk quantification.
- Industrial cybersecurity certifications.

