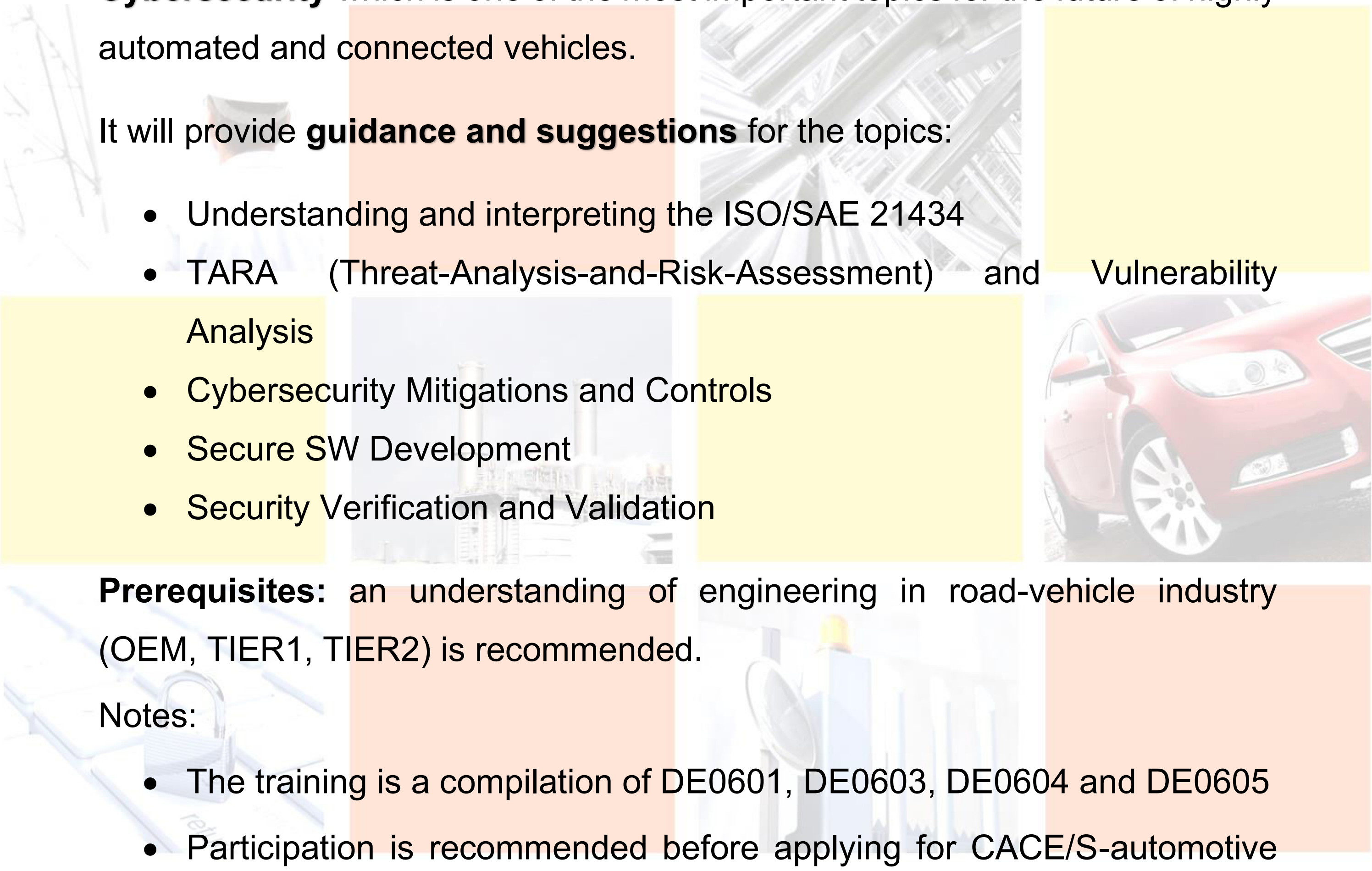
DE0610 Road Vehicle Cybersecurity in context of ISO/SAE 21434 – in depth

This training will support to lay a basis for the **understanding of Automotive Cybersecurity** which is one of the most important topics for the future of highly automated and connected vehicles.



It will provide **guidance and suggestions** for the topics:

- Understanding and interpreting the ISO/SAE 21434
- TARA (Threat-Analysis-and-Risk-Assessment) and Vulnerability Analysis
- Cybersecurity Mitigations and Controls
- Secure SW Development
- Security Verification and Validation

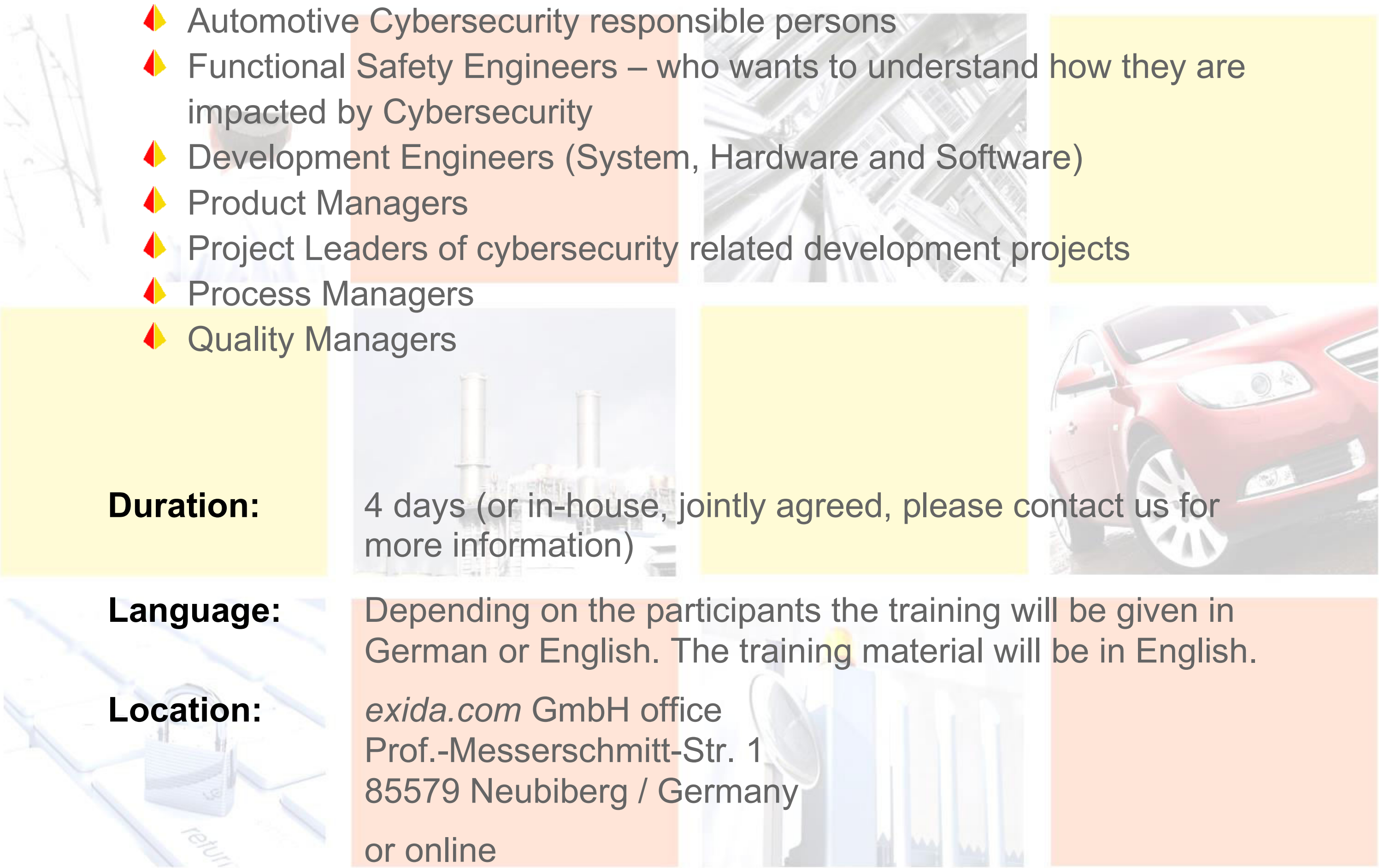
Prerequisites: an understanding of engineering in road-vehicle industry (OEM, TIER1, TIER2) is recommended.

Notes:

- The training is a compilation of DE0601, DE0603, DE0604 and DE0605
- Participation is recommended before applying for CACE/S-automotive speciality personal certification

DE0610 Road Vehicle Cybersecurity in context of ISO/SAE 21434 – in depth

Who should attend?



- Automotive Cybersecurity responsible persons
- Functional Safety Engineers – who wants to understand how they are impacted by Cybersecurity
- Development Engineers (System, Hardware and Software)
- Product Managers
- Project Leaders of cybersecurity related development projects
- Process Managers
- Quality Managers

Duration: 4 days (or in-house, jointly agreed, please contact us for more information)

Language: Depending on the participants the training will be given in German or English. The training material will be in English.

Location: *exida.com* GmbH office
Prof.-Messerschmitt-Str. 1
85579 Neubiberg / Germany

or online

Certificate: Each participant gets a letter of attendance.

For more information, please contact:
Kerstin Tietel ☎ +49 89 44118232
✉ kerstin.tietel@exida.com

DE0610 Road Vehicle Cybersecurity in context of ISO/SAE 21434 – in depth

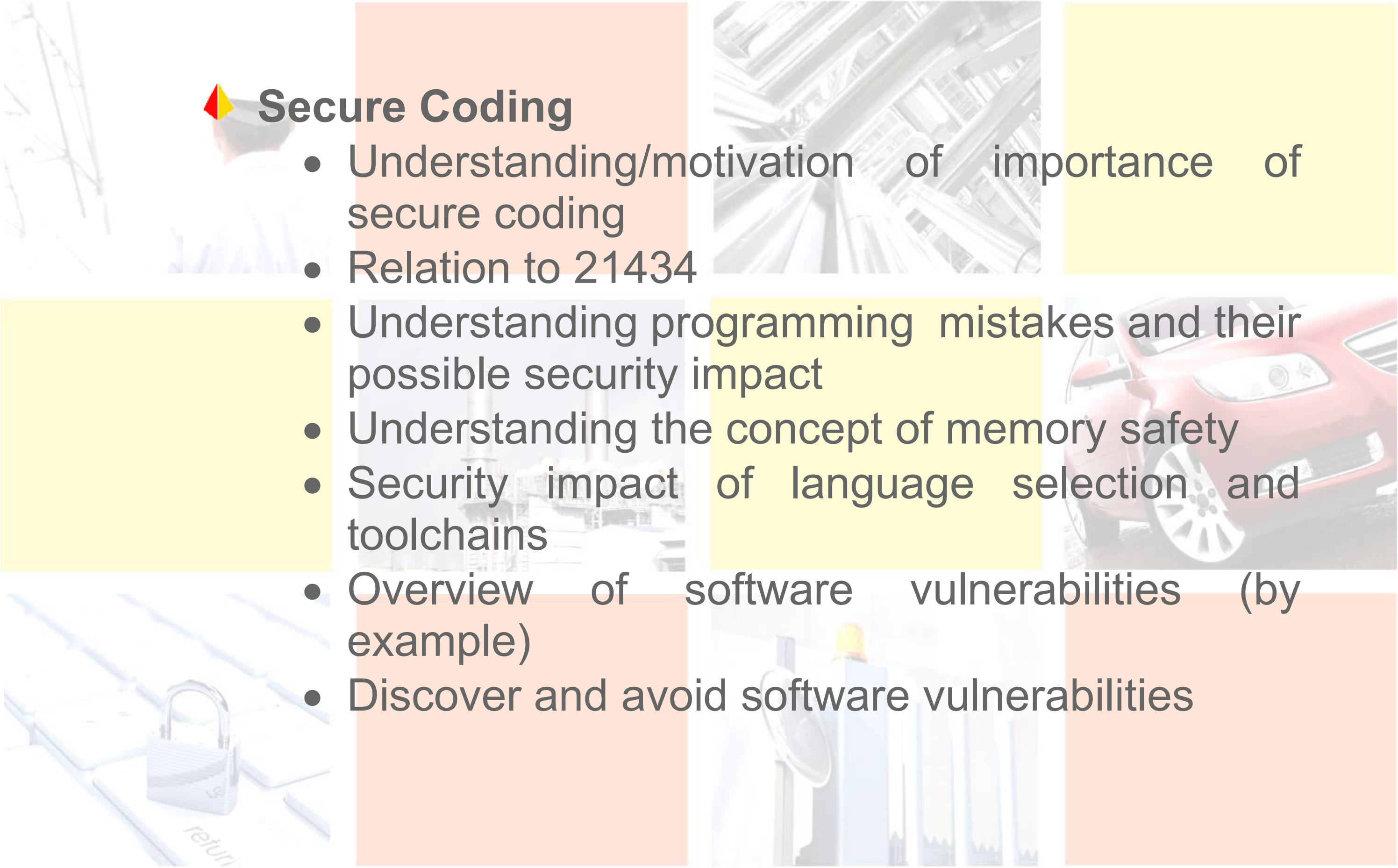
Agenda and Content

- Awareness & Motivation
- Cybersecurity & Functional Safety
- Standards overview
- Cybersecurity Management
  - Organizational
  - Project dependent
  - Post-development related
- Concept Phase
- Product Development Phase

- Intro
- Assets/Properties/Impacts -> Goals
- TA-RA
- TARA-Vs VA
- ATA vs TMEA
- TARA-ISO-Head-Lamp
- Measures & Mitigations

Secure Software Design

- Understanding/motivation secure software design
- Relation to 21434
- Secure design principles
- Supply-chain security (SBOM, Monitoring)
- Language selection
- Toolchains



Secure Coding

- Understanding/motivation of importance of secure coding
- Relation to 21434
- Understanding programming mistakes and their possible security impact
- Understanding the concept of memory safety
- Security impact of language selection and toolchains
- Overview of software vulnerabilities (by example)
- Discover and avoid software vulnerabilities

Software Testing for security

- Awareness & Motivation: Why is verification so important?
- Test Planning and Infrastructure
- SW Security Verification Overview: Get to know security relevant test methods and their application

Pen Testing

- Introduction to Pentesting: What is pentesting? Which testing methods are relevant for pentesting? Pentesting approach, attach types and surfaces ans so on.
- Pentesting – Needs brainstorm on attacks: Get to know different kind of cybersecurity attacks