



## Expert- and Engineering-Services for Cybersecurity according to ISO/SAE 21434

Due to the increasing risks of cyber attacks on vehicles and because the infrastructure for online vehicle updates (OTA), fleet management, communication between vehicles (Car2x/V2X) and other requirements for vehicles open up new attack surfaces, ISO/SAE 21434 requires measures for development.

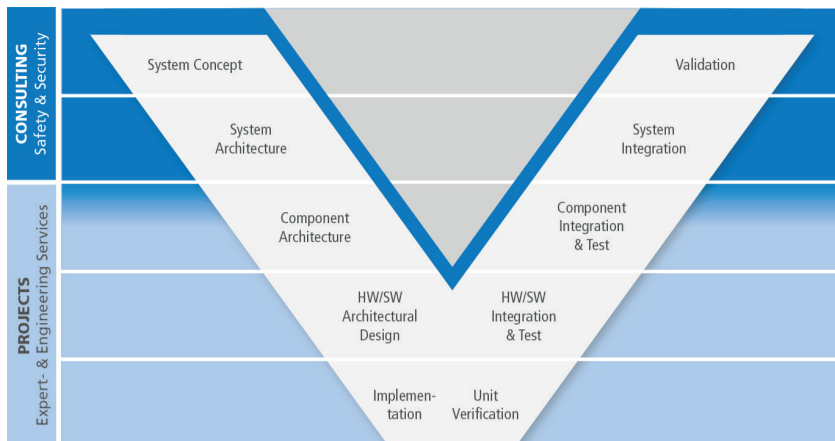
NewTec offers various methods and techniques based on ISO/SAE 21434 and beyond to develop secure software from analysis to concept, development, commissioning and end-of-life. Structured processes ensure that cybersecurity is in focus during the entire product development process.

### Expert- und Engineering-Services:

- System analyses (requirements analyses, static code analysis)
- Hazard and risk analyses (TARA, HARA, STPA)
- Security defense-in-depth concepts
- Public key infrastructure concepts (PKI)
- Security goal definition
- Update concepts
- Secure boot
- Software bill of materials (SBOM) Management
- Security requirements
- Security reviews
- Security robustness tests (penetration tests (internal/external), fuzzing)
- Implementation of secure SW modules

### Managed-Services for securing the operation:

- Continuous monitoring for weak points due to new threat situations
- Continuous monitoring for conformity with current security standards
- Continuous maintenance of the desired level of protection
- Incident management
- Obsolescence management for security-related system parts



NewTec provides support and guidance throughout the entire product development cycle.

