



## Maximaler Schutz für Embedded Systeme

„Security“ bezieht sich auf die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität von funktionssicheren Systemen. Sie soll nicht-autorisierte Datenmanipulationen oder aber auch die unbefugte Preisgabe sensibler Informationen verhindern.

Mixed Mode kann im Bereich Security bereits langjährige Erfahrung in Kundenprojekten vorweisen. Um das Thema IT- und Cyber-Sicherheit weiter voran zu treiben, engagiert sich Mixed Mode aktiv in Verbänden wie dem Sicherheitsnetzwerk München.

Zudem wurden bei Mixed Mode mehrere Forschungsprojekte wie TECOM, SecFutur und SIBASE zu dem Thema erfolgreich durchgeführt.

## Weitere Informationen

» [Projektüberblick](#)

## Projektbeispiele Security

### Security-Toolentwicklungen

Objektorientierte Applikations-Softwareentwicklungen für Security-Anwendungen inklusive Kryptokomponenten. Darunter schnelle Simulatoren und Emulatoren für Chipcard Processor Cores und die angeschlossene Peripherie.

### Secure Application

Sichere Kommunikationslösung auf Basis von Android Smartphones.

### TECOM

Internationales Förderprojekt zur Spezifizierung von Use Cases und Anwendungen für den Einsatz der TPM-Technologie. Entwicklung von Modulprototypen zur Anbindung von TPM in bestehende Anwendungen. Anbindung von Sensoren über gesicherte Datenleitung.

### Qualitätsberatung für sichere Software

Consulting zur Entwicklung spezifischer Entwicklungsrichtlinien für die Realisierung von sicherheitskritischer Software nach SIL und ISEC. Unterstützung bei der Vorbereitung für die Zertifizierung nach Bankenstandards.

### SafeBatt (Maßnahmen für eigensichere Lithium-Ionen-Batterien)

Ziel ist die Verbesserung der Betriebssicherheit von Lithium-Ionen-Batterien in Elektro- und Hybridfahrzeugen. Die sensiblen Betriebsdaten werden in einem „sicheren Batteriepass“ verschlüsselt gegen Fremdmanipulation gespeichert.

### SIBASE (Sicherheitsbaukasten für eingebettete Systeme)

Erforschung und Anwendung spezieller Hardware-Sicherheitselemente mit physikalisch eindeutigen Fingerabdrücken (PUF = Physical Unclonable Function) mit gesicherten Betriebssystemen. Entwicklung eines Demonstrators für die Anwendungsmöglichkeiten von Sicherheitselementen.

### Testautomatisierung für Smart Metering-Systeme

Analyse, Verbesserung des aktuellen Testprozesses sowie Einführung von Continuous Integration in der Entwicklung von Smart Meters für Strom und Wasser.

### Trusted Platform Module (TPM)

Entwicklung von Trusted Computing Applications. Entwicklung von Tools zur Funktions- und Ausgangsprüfung von hochsicherheitsfesten Kryptoprozessoren (Trusted Platform Modules). Treiberentwicklung für Linux und U-Boot.

### Tooling für Verbrauchsdatenerfassung

Softwareentwicklung für die exakte und sichere Abrechnung angefallener Kosten von Heizung sowie Warm- und Kaltwasser im privaten und gewerblichen Bereich.

### Validierung von Kryptoalgorithmen

Umsetzung komplexer Algorithmen wie DES und SHA in VHDL. Anschließende Verifikation und Validierung per Softwaresimulation und Freigabevorbereitung für den Kunden.