Verhinderung von Angriffen auf Elektroniksysteme durch innovative Multi-Sensorik (VE-SAFE)

T. Kuhn[1], K. Giapakras[1], A. Friedl[2], D. Sirkeci[3], U. Maaß[3], E. Bezer[3], R. Golinske[3], M. Spanier[3], I. Ndip[3]

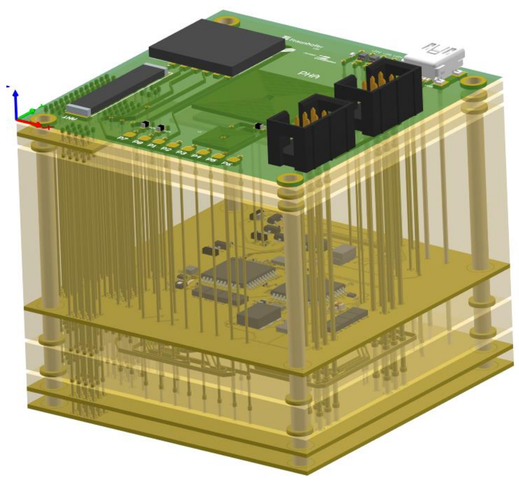
Zielstellung

Im Verbundvorhaben VE-SAFE wurde eine ungeschützte Kundenelektronik mit Sensoren zur Erkennung von Tamper-Angriffen in ein PCB-Embedding Package integriert. Die Sensorik soll Angriffe auf die Hardware (Kundenelektronik) des Moduls erkennen und passende Gegenmaßnahmen einleiten können. Durch die Entwicklungen im Forschungsprojekt sollen Hersteller elektronischer Geräte zukünftig in die Lage versetzt werden, das Sicherheitsniveau ihrer elektronischen Baugruppen im Bereich der Hardware Security komfortabel und kostengünstig zu erhöhen.

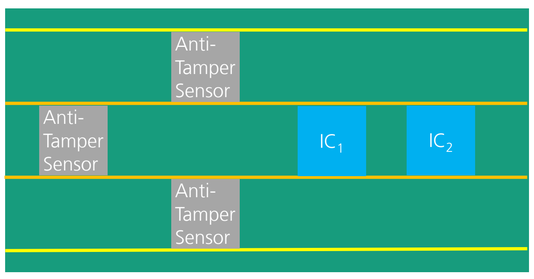
SAFE-Konzept

- Hardware-Angriffe auf elektronische Baugruppen ermöglichen Manipulation und Reverse Engineering
- Bauteilinformationen und Routing in SMD-Technologie z.T. direkt sichtbar
- Probing ermöglicht Messung von elektrischen Signalen an Pads
- Unbemerkte physikalische und chemische Angriffe möglich

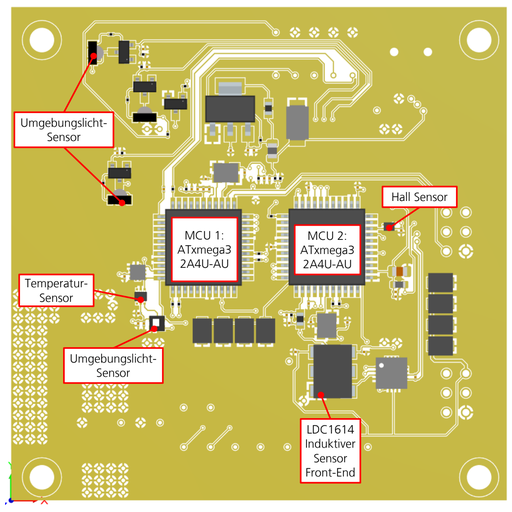
→ Zusätzlicher Schutz durch aktive Überwachung der Integrität des Elektronikmoduls mit Anti-Tamper Sensoren



Designmodell SAFE-Modul V3: Eingebettete sensitive Kundenelektronik, SAFE-Sensorik und weitere Komponenten

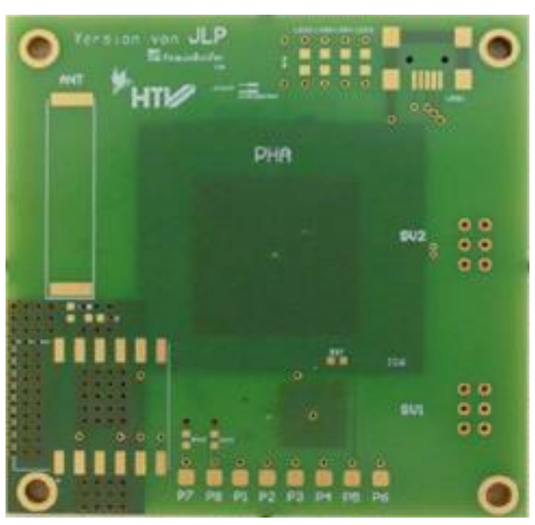


Querschnitt durch SAFE-Modul mit eigebetteten Komponenten der Kundenschaltung und Anti-Tamper Sensoren

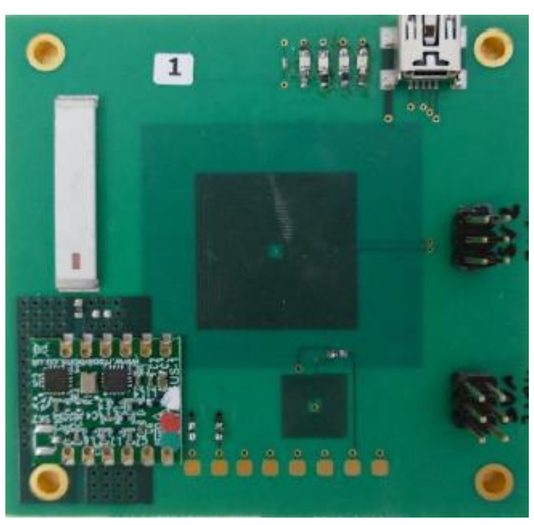


Layout eingebettete Komponentenlage in SAFE-Modul V3

Gefertigte SAFE-Module



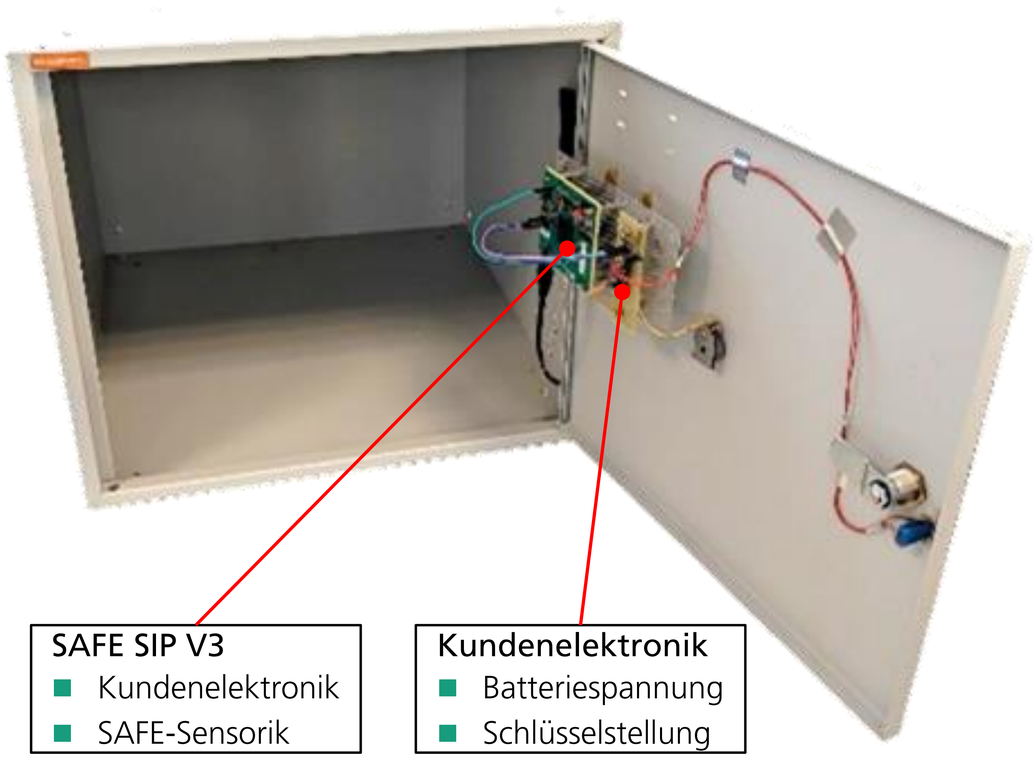
SAFE-Modul V3 in PCB-Embedding Technologie (SMD-Komponenten nicht bestückt)



SAFE-Modul V3 vollständig bestückt

Demonstration

- Evaluation SAFE-Modul mit Kundenschaltung in Metallschrank
- Kundenelektronik überwacht Batteriespannung und Schlüsselstellung
- Test auf Erkennung von Angriffsszenarien durch SAFE-Sensorik



Messaufbau zur Evaluation des SAFE-Konzepts mit Kundenelektronik und SAFE-Modul in Metallschrank

Angriff	Lichtsensor	Hallsensor	Induktivität	Gittersensor	Beschleunigung	Funkverbindung	Abschirmungslage
Tür wird unerlaubt geöffnet	X	X			X		
Annäherung (Körperteil, Werkzeug)			X				
Bewegung des Gehäuses (Vibration)					X		
Bohrung in Gehäuse	X			X	X		
Bohrung in Oberfläche der LP			X	X	X		
Trennung Stromversorgung						X	
Seitenkanalanalyse (Stromverbrauch)				X			
Seitenkanalanalyse (EM-Strahlung)							X

Fazit

- SAFE-Technologien können erhöhte Sicherheit gegen physikalische Angriffe auf elektronische Module bieten
- PCB-Embedding erschwert optische Analysen und galvanisches Probing
- Anti-Tamper Sensoren zur Überwachung von sensitiven Kundenschaltungen durch Erkennung von Umgebungsveränderungen können in PCB-Embedding Modul integriert werden
- Eine Kombination von Messwerten verschiedener Sensoren kann zur Verbesserung von Sensitivität und Trennschärfe genutzt werden
- PCB-Embedding erfordert Erfahrung in der PCB-Herstellung und erschwert dadurch Kopien und Fälschungen elektronscher Module

1 HTV Halbleiter-Test & Vertriebs-GmbH
Robert-Bosch-Str. 28
D-64625 Bensheim

2 Jenaer Leiterplatten GmbH
Prüssingstraße 31
07745 Jena

3 Fraunhofer IZM
Gustav-Meyer-Allee 25
13355 Berlin

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung