Vertrauenswürdige Elektronik mit integrierter Sensorik zur Erkennung von Tamper-Angriffen (VE-SAFE)

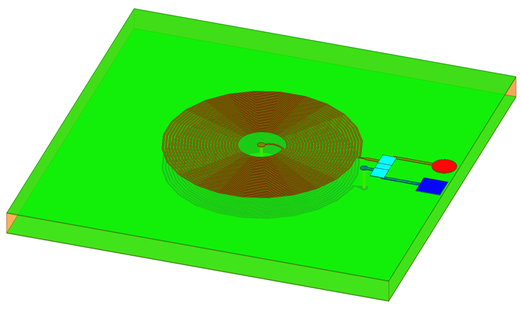
T. Kuhn[1], K. Giapakras[1], A. Friedl[2], D. Sirkeci[3], U. Maaß[3], E. Bezer[3], R. Golinske[3], M. Spanier[3], I. Ndip[3]

Zielstellung

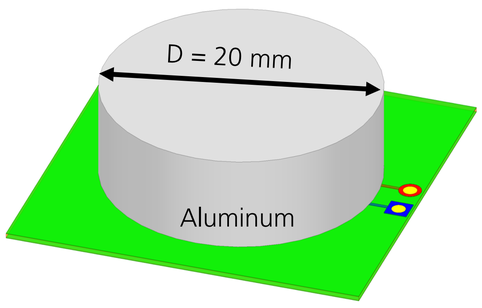
Es wurden verschiedene Sensoren zur Überwachung der Integrität sensitiver Elektronikmodule und Erkennung physkalischer Angriffe untersucht. Induktive Näherungssensoren sowie Sensoren für Umgebungslicht, Temperatur, Magnetfeld und Beschleunigung wurden durch Simulationen und Testaufbauten evaluiert. Darüber hinaus wurde die Wirksamkeit des PCB-Embedding gegen Seitenkanalangriffe evaluiert.

Induktive Sensoren

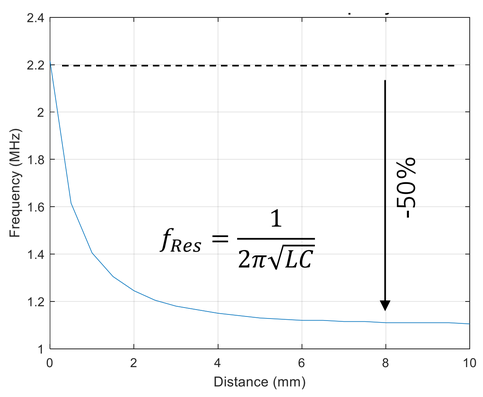
- Physikalische Angriffe durch metallische Werkzeuge (Bohrer, Fräser usw.) beeinflussen das Magnetfeld induktiver Näherungssensoren
- EM Feldsimulationen der Annäherung eines Metallwerkzeugs zeigt Änderung der Eigenschaften von Schwingkreis aus Sensorinduktivität und zusätzlicher Kapazität



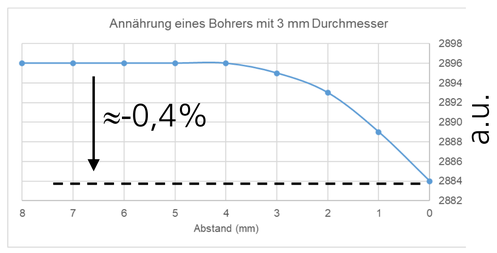
Simulationsmodell integrierte Induktivität (∅13mm, 25 Windungen, 2 Lagen, 100um Line/Space, 300um PCB-Höhe)



Simulationsmodell Sensorinduktivität mit metallischem Werkzeug (Al, ∅13mm) zur Analyse des Einflusses auf Induktivität

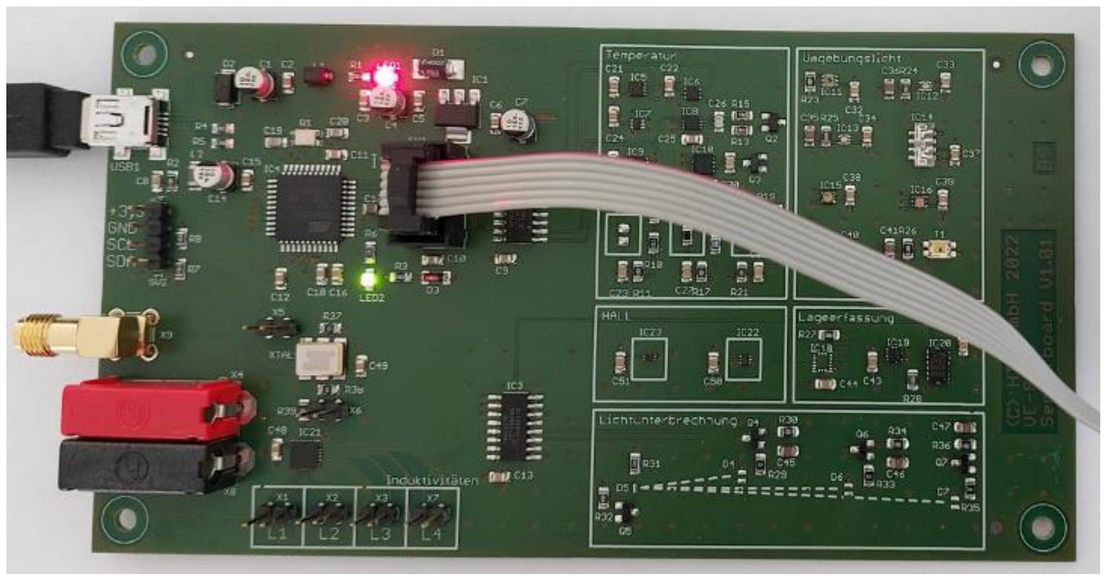


Simulationsergebnis zu Effekt der Annäherung eines metallischen Werkzeugs auf Resonanzfrequenz von Sensorspule



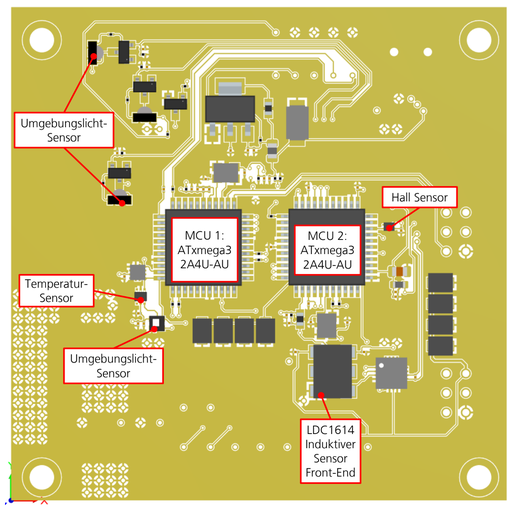
Messung der relativen Abnahme der Induktivität der Sensorspule bei Annäherung von metallischem Werkzeug

Weitere Sensoren

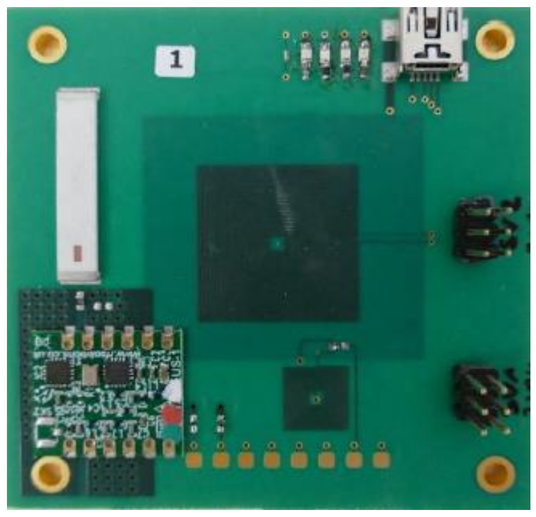


Entwickeltes Sensorboard zur Evaluierung der Erkennung von Tamper-Angriffen mit Sensoren für Umgebungslicht, Temperatur, Beschleunigung und Magnetfeld

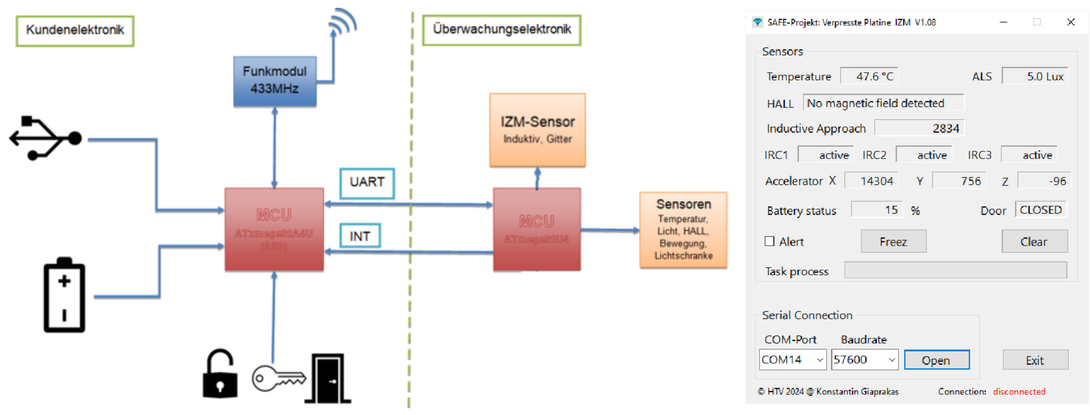
Integration der Sensoren in PCB-Embedding Modul



Einbettungslage SAFE-Modul V3 mit verschiedenen Anti-Tamper Sensoren, LDC Sensor Front-End zur Auswertung der Sensorinduktivität und Mikrocontrollern für SAFE-Sensorik und Anwendungsschaltung



Gefertigtes SAFE-Modul V3 mit Anti-Tamper Sensorik, sensitiver Kundenelektronik sowie weiteren Komponenten



Blockschaltbild Demonstrationsszenario (links) und GUI zur Auslesung der Messwerte (rechts)

Evaluation von SAFE-Technologien gegen DPA-Angriffe

			PCB	SAFE Modul V3
Angriffsart	**Angriffstyp**	**Richtung**	**Messungen**	**Messungen**
Software	Strom	Vorwärts	2.000	Verhinderung durch aktive Sensoren
Software	Strom	Rückwärts	5.000	
Hardware	Strom	Vorwärts	15.000	
Hardware	Strom	Rückwärts	25.000	
Software	EM-Sonde	Vorwärts	4.000	> 25.000
Software	EM-Sonde	Rückwärts	6.000	> 25.000
Hardware	EM-Sonde	Vorwärts	30.000	>100.000
Hardware	EM-Sonde	Rückwärts	160.000	>300.000

Fazit

- Induktive Näherungssensoren sowie Sensoren für Umgebungslicht, Temperatur, Beschleunigung und Magnetfeld können zur Erkennung von Veränderungen der Umgebung sensitiver elektronischer Module genutzt werden
- Eine Kombination von Messwerten verschiedener Anti-Tamper Sensoren kann zur Verbesserung der Sensitivität und Trennschärfe gegen physikalische Angriffe genutzt werden

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
Förderkennzeichen 16ME0239