Titel des Verbundprojektes	**Verhinderung von Angriffen auf Elektroniksysteme durch innovative Multisensorik (VE-SAFE)**
Projektleitung	HTV Halbleiter-Test & Vertriebs-GmbH Dipl.-Ing. Thomas Kuhn Robert-Bosch-Str. 28, D-64625 Bensheim
Projektpartner	Jenaer Leiterplatten GmbH (JLP) Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration IZM (IZM)
Verbundnummer	ME1ZEUS015
Förderkennzeichen	16ME0236K
Zeitraum	01.03.2021 – 29.02.2024
Projektträger	VDI/VDE Innovation + Technik GmbH
Anschrift	Steinplatz 1, 10623 Berlin
Forschungsziel	Entwicklung und Evaluation einer Überwachungselektronik zum Schutz einer bislang ungeschützten Kundenelektronik durch die Verpressung einer innovativen Multisensorik in ein Leiterplattenmodul

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor

Inhalt

1 Kurzbericht (Teil 1)

1.1 Aufgabenstellung sowie wissenschaftlicher und technischer Stand

Im täglichen Leben werden Menschen künftig noch mehr elektronischen Bauteilen vertrauen müssen, die beispielsweise in selbstfahrenden Autos, Servicerobotern oder unseren alltäglichen elektronischen Systemen und Geräten zum Einsatz kommen. Zusätzlich werden unter dem Stichwort Internet of Things (IoT) immer mehr Geräte miteinander vernetzt, die wiederum hard- und softwareseitig immer mehr angreifbare Schwachstellen in elektronischen Geräten und Netzwerken aufweisen.

Im Verbundvorhaben „Verhinderung von Angriffen auf Elektroniksysteme durch innovative Multi-Sensorik“ (VE-SAFE) fördert das Bundesministerium für Bildung und Forschung (BMBF) vom 01.03.2021 bis 29.02.2024 die Entwicklung einer Überwachungselektronik. Diese soll zusammen mit einer bislang ungeschützten Kundenelektronik in einer Leiterplatte vergossen werden, um mögliche Angriffe auf die Hardware (Kundenelektronik) des jeweiligen elektronischen Gerätes erkennen und passende Gegenmaßnahmen einleiten zu können. Hersteller elektronischer Geräte sollen durch diese zusätzliche adaptierbare Sensorhülle zukünftig in der Lage sein, das Sicherheitsniveau ihrer elektronischen Baugruppen im Bereich der Hardwaresicherheit (bzw. Hardware Security) komfortabel und kostengünstig erhöhen zu können.

Die Aufgabe von HTV umfasst die Zusammenstellung von möglichen **Schwachstellen und Angriffen** auf elektronische Hardware, die Entwicklung einer **schützenswerten Kundenelektronik** und die Entwicklung realer **Angriffe** auf die ermittelten Schwachstellen der realisierten Kundenelektronik zur praktischen Demonstration. Zusätzlich soll eine **Überwachungselektronik** entwickelt werden mit einer Dokumentation der enthaltenen **Schutzmaßnahmen** (Security-Target) und Schnittstellen für den Anschluss der vom Projektpartner IZM in diesem Forschungsprojekt entwickelten Überwachungs-sensoren. Die Überwachungselektronik soll in der Lage sein, aktiv **Gegenmaßnahmen** bei Angriffen einleiten zu können.

1.2 Ablauf des Vorhabens

Zu Beginn des Projektes wurde im Jahr 2021 ein erster Prototyp zu einer möglichen „schützenswerten“ Kundenelektronik als praktischer Anwendungsfall aufgebaut. Der Prototyp realisiert ein Sicherheits-schloss, dessen Schlüsselposition mittels AES-Verschlüsselung verschlüsselt zu einer Empfangs-station übertragen wird. Die Empfangsstation entschlüsselt das Signal und zeigt die Schlüsselstellung auf einem Display an. Im Bereich der Sicherheitstechnik wurde ein Messplatz aufgebaut, um den Stromverbrauch messen und analysieren zu können, zur Durchführung von Seitenkanalangriffen. Mit dem Messplatz können in kurzer Zeit hunderte von Messkurven aufgenommen werden. Durch eine Bewertung der Messkurven ist es möglich, den geheimen Schlüssel der AES-Verschlüsselung mittels DPA (Differential Power Analysis) zu ermitteln.

Im Jahr 2022 konnten die vom Projektpartner Fraunhofer IZM simulierten Sensoren erfolgreich in ein Leiterplatte bzw. PCB als Modul verpresst werden. Bei HTV erfolgte dann die weitere Qualifikation, Analyse und der elektrische Funktionstest der Module.

Im Jahr 2023 wurden die IZM-Sensoren, sowie weitere käufliche Sensoren und die Kundenelektronik in ein gemeinsames VE-SAFE-Modul V3 verpresset, in Betrieb genommen und die elektrische Funktion getestet.

Zum Projektabschuss wurden Anfang 2024 die unterschiedlichen Angriffe auf mögliche Schwachstellen der Elektronik wiederholt. Dabei zeigte sich, dass die realisierten Gegenmaßnahmen erfolgreich die Angriffe abschwächen oder sogar verhindern können. Ein signifikanter Anstieg der Sicherheit konnte damit nachgewiesen werden.

1.3 Wesentliche Ergebnisse und Zusammenarbeit mit anderen Forschungseinrichtungen

Das SAFE-Projekt greift die immer noch vorherrschenden Vulnerabilität heutiger Elektronik bezüglich physikalischer Nahbereichsangriffe auf. Um die Brisanz der Thematik zu demonstrieren, startete das VE-SAFE-Projekt mit einer Umfrage zum Stand der Technik und zum Marktbewusstsein über das Problem.

Im VE-SAFE-Projekt wird dann als Lösung der folgende Ansatz gewählt: Bekannte Angriffe auf elektronische Geräte werden zunächst zusammengestellt, anschließend werden Teststationen aufgebaut, die diese Angriffe auf die im Projekt entwickelten Demonstratoren durchführen können. Anschließend werden Schutzmechanismus evaluiert, selbst dem physikalischen Zugriff entzogen sind und die Angriffe erkennen können. Im VE-SAFE-Projekt wird dazu als aktiver Schutzmechanismus eine Sicherheitssensorik und -elektronik entwickelt, die einer beispielhaften, ungeschützten Kunden-elektronik hinzugefügt wird. Es werden auch passive Schutzmechanismen getestet (z. B. Metallflächen zur Reduktion von elektromagnetischer Abstrahlung). Im Projekt erfolgen dann Angriff auf die entwickelten Leiterplattenmodule und es wird getestet, ob die Angriffe sowohl erkannt als auch durch die implementierten Gegenmaßnahmen, wie z. B. das Löschen sensibler Daten, verhindert werden können. Die Einbettung des gesamten Elektronikpakets (Kundenelektronik + Überwachungselektronik) im PCB sorgt dabei für eine Unzugänglichkeit einzelner Komponenten und somit für schlecht identifizierbare und unzugängliche Angriffspunkte. Vom Schaltungs- und Layoutentwurf über die Schaltungsrealisierung in Prototypen und den elektrischen und Anwendungstests an den Prototypen wurde eine gesamte Entwicklungskette im Projekt realisiert, die das Thema an einem Anwendungsbeispiel veranschaulicht.

Die Projektpartner Fraunhofer IZM, Jenaer Leiterplatten GmbH und HTV Halbleiter Test & Vertriebs-GmbH vereinten alle nötigen Kompetenzen im VE-SAFE Projekte. Das Fraunhofer entwickelte, fertigte und validierte im Projekt eigene induktiven Näherungssensor mit Schnittstelle. Zusammen mit dem Projektpartner Jenaer Leiterplatten GmbH werden dann alle elektronischen Komponenten (Sensoren, ICs, …) in Leiterplattenmodule mit eingebetteten bzw. verpresst. Von HTV wurden kommerzielle Sensoren, wie Lichtsensoren, Hallsensoren, Bewegungssensoren ausgewählt und deren Einsatzmöglichkeiten evaluiert. HTV führte auch die anfängliche IT-Sicherheitsbefragung durch, entwickelt die Überwachungs- und Kundenelektronik für den Demonstrator, Baute Messplätze auf für die Durchführung der physikalischen Angriffe (z. B. Seitenkanalanalyse) und qualifizierte mit unterschiedlichen Verfahren (z. B. Röntgen, Mikroskopie, Schilffbilder, …) entwickelten Leiterplatten-module.

Die Arbeitspakete gliedern sich auf in:
AP1 Angriffsvektoren, Spezifikationen und Systemarchitektur: Definition von Angriffen, Schutzmaßnahmen und Spezifikationen mit Erstellung einer Lastenheftes für die gesamte Elektronik
AP2 Sensorentwicklung: Entwicklung und Auswahl von Sensoren für die Angriffsdetektion
AP3 Analog-/Digitale Interface: Entwicklung der Kommunikation und aller benötigten Schnittstellen
AP4 Sicherheitssystem: Realisierung des Sicherheitssystems als Ganzes
AP5 Packaging-Plattform: Entwicklung und Optimierung des Verpressungsprozesses (bzw. Embedding), Fertigung von Prototypen mit unterschiedlicher Komplexität, Auswahl und Integration aller elektronischer Komponenten in die Leiterplatte
AP6 Systemtests und -evaluierung. Das finale VE-SAFE-Modul V3 wurde entwickelt, produziert und evaluiert

Die Ergebnisse der einzelnen Arbeitspakete werden in den folgenden Kapiteln beschrieben.

2 Ausführlicher Schlussbericht (Teil II)

2.1 Der Verwendung der Zuwendung und der erzielten Ergebnisse im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele

Ziel des Projektes war die Entwicklung und Evaluation einer Überwachungselektronik zum Schutz einer bislang ungeschützten Kundenelektronik durch die Verpressung einer innovativen Multisensorik in ein Leiterplattenmodul. Die Abbildung 1 zeigt den Zusammenhang der einzelnen Arbeitspakete und Abbildung 2 den zeitlichen Ablauf des Projektes.

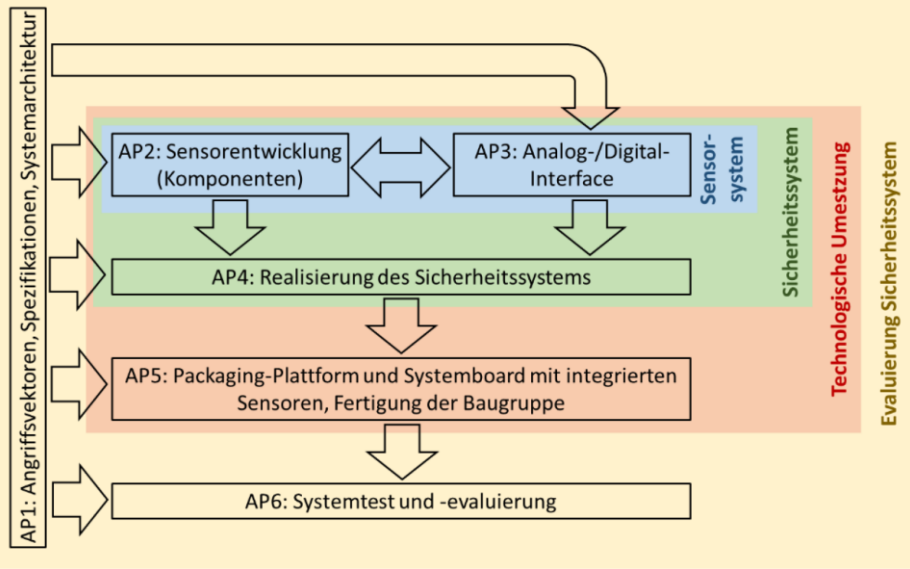


Abbildung 1: Projektaufbau nach Projektantrag des Verbundprojekts SAFE

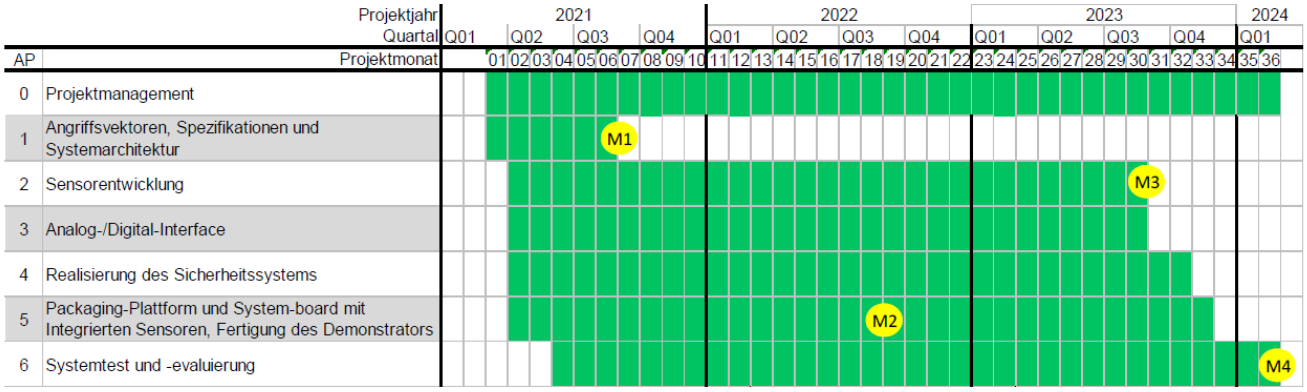


Abbildung 2: Arbeitspakete AP0 bis AP6 des VE-SAFE Projektes

2.1.1 AP1: Angriffsvektoren, Spezifikationen und Systemarchitektur

Ziele:

Mögliche Angriffsszenarien werden analysiert und Schutzmechanismen definiert, um die Elektronik vor Manipulationen zu schützen. Bedarfsanfragen an mögliche Kunden bzgl. derer Anforderungen zum Schützen deren spezifischer Elektronik werden gestellt. Außerdem wird eine Übersicht der Spezifikationen erstellt.

Ergebnisse aus 2021:

- Erste Version **von Security Target Dokument** wurde erstellt (mit Angriffsvektoren)
- **Lastenheft** wurde erstellt (Systemspezifikation und Systemarchitektur)
- Eine **Online-Befragung** von deutschen Unternehmen zur Lage der Hardwaresicherheit und zur Ermittlung von Wünschen und Anforderungen für das Verbundprojekt VE-SAFE wurde durchgeführt. Die gewonnenen Erkenntnisse aus den Befragungen wurden direkt an die Technik weitergegeben (Aufnahme in das Lastenheft des Forschungsprojektes), um die Bedürfnisse der Anwender bei der Technikentwicklung zu berücksichtigen. Eine Veröffentlichung erfolgte in der „velektronik“ Plattform.

Meilenstein M1 wurde erfolgreich abgeschlossen.

2.1.2 AP2: Sensorentwicklung

Ziele:

Es sollen ausgewählte Sensorprinzipien analysiert und Sensoren entwickelt werden. Diese grundsätzlichen Untersuchungen sollen für die spätere Integration in ein Package genutzt werden.

Ergebnisse aus 2021:

Mit dem Projektpartnern IZM wurde diskutiert, welche Angriffe von einem neuartigen, induktiven Sensor erkannt werden sollen. Anschließend wurden vom IZM unterschiedliche Simulationen zur Auslegung des Sensors durchgeführt (vgl. Abbildung 3). Für die Auswertung der Sensorsignale wurde der Baustein LDC1614 vorgeschlagen. Das Entwicklungsboard LDC1614EVM wurde angeschafft und evaluiert (vgl. Abbildung 4) und anschließend mit den Projektpartnern eine mögliche Integration der elektronischen Bauteile in ein Leiterplattenmodul besprochen (vgl. Abbildung 5). Für die Analyse zum Stand der Technik wurden zusätzlich Sicherheitschips aus Smartcards freigelegt und analysiert (vgl. Abbildung 6).

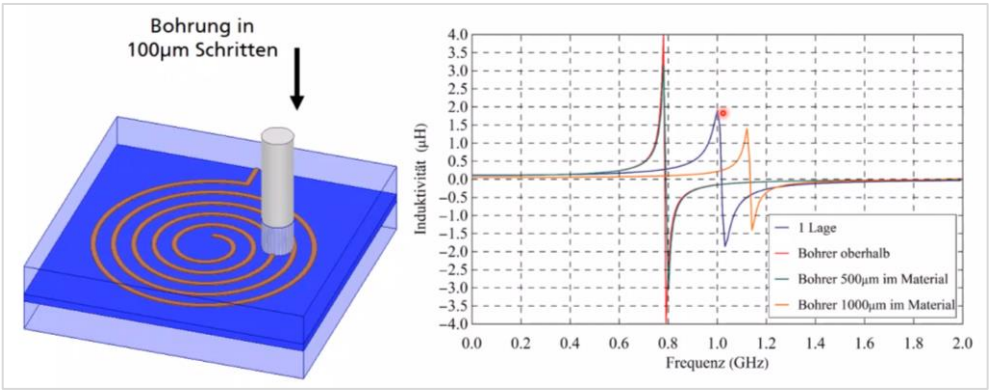


Abbildung 3: Simulation einer Bohrung in das Leiterplattenmaterial mit unterschiedlicher Eintauchtiefe

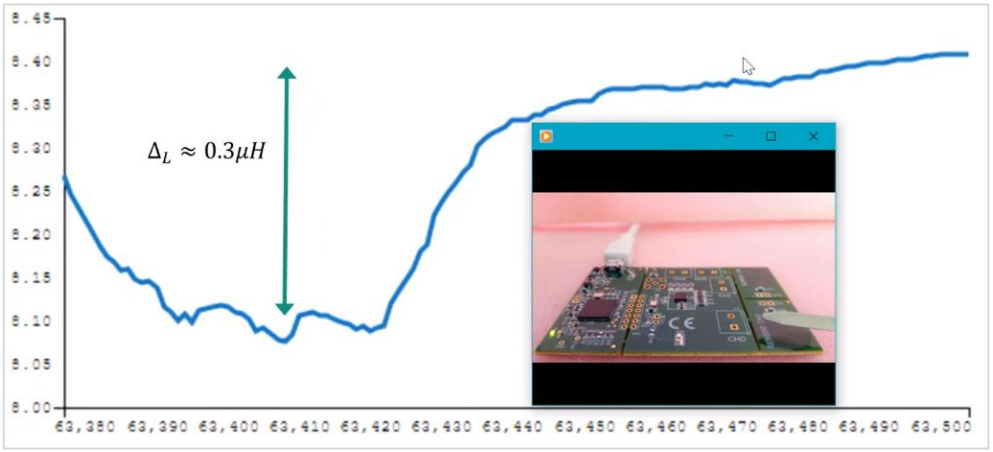


Abbildung 4: Versuche mit käuflich verfügbarem Sensorboard
(Änderung der Spuleninduktivität durch Annäherung eines metallischen Gegenstandes)

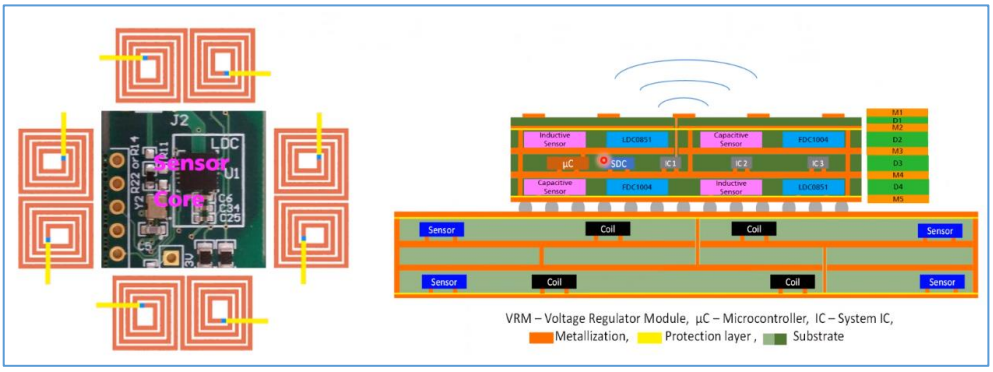
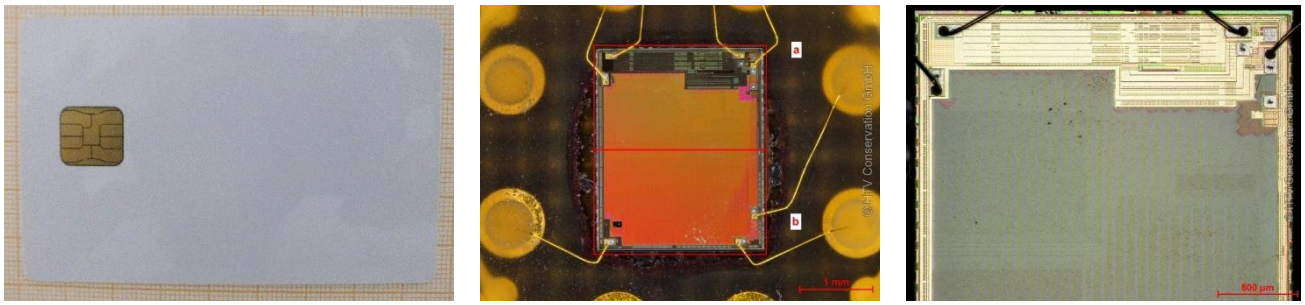


Abbildung 5: IZM – Vorstellung einer ersten Messschaltung zur Auswertung der Sensorsignale



Smartcard / Chip-Karte | Chip (chem. Öffnung) | Chip (Bildausschnitt)

Abbildung 6: Physikalische Analyse einer Smartcard

Ergebnisse aus 2022:

Aus den Simulationsergebnissen der IZM-Sensoren konnten gewünschte Eigenschaften für die Sensoren abgeleitet werden und eine Auswahl für die Realisierung getroffen werden. HTV entwickelte in Absprache mit den Projektpartnern eine Ansteuer- und Auswerte-Schaltung.

Die Projektpartner verpressten alle elektronischen Komponenten dann in ein erstes VE-SAFE-Modul V1. Dieses wurde von HTV elektrisch validiert und mit den Methoden Röntgen, Mikroskopie und Ultraschall-Mikroskopie nach thermischen Belastungen qualifiziert. Es zeigte sich eine große Übereinstimmung der Messwerte mit der Simulation.

Von HTV wurden dann weitere käufliche Sensoren auf einem Sensorboard in Betrieb genommen und mit den Projektpartnern eine Auswahl durchgeführt, welche davon in ein finales Modul verpresst werden sollen (vgl. Abbildung 7). In Abbildung 8 ist die GUI der Auswertesoftware des von HTV entwickelten Sensorboards abgebildet.

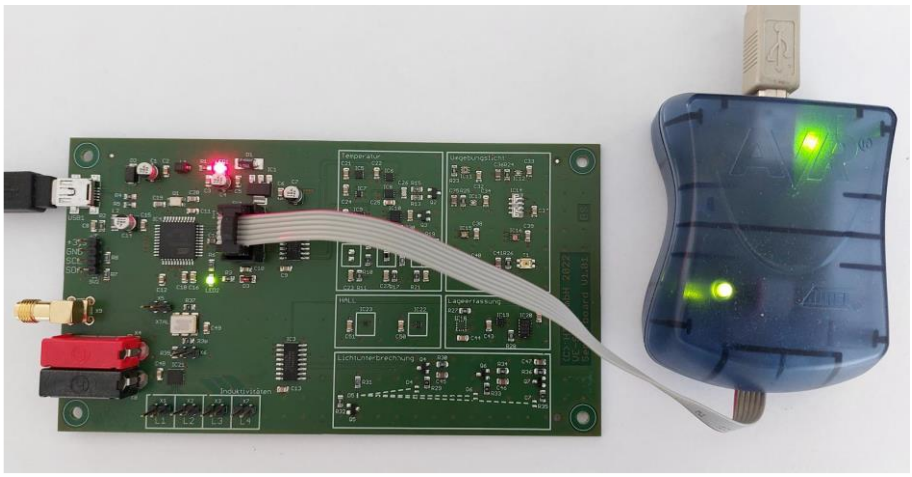


Abbildung 7: Realisiertes Sensorboard für die Evaluation käuflicher Sensoren

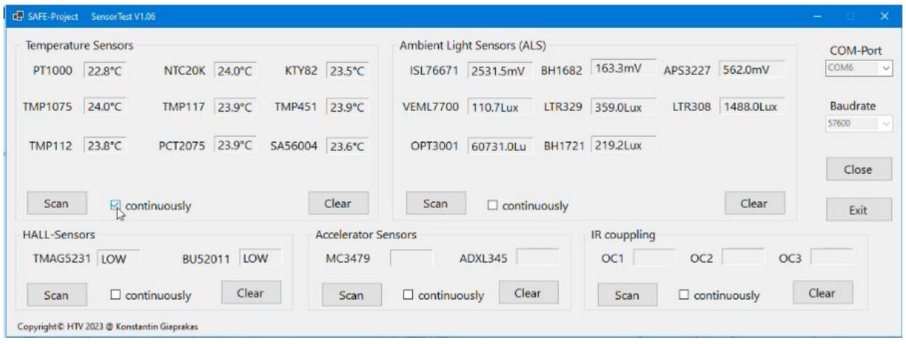


Abbildung 8: Auswertesoftware zur Evaluation käuflicher Sensoren

Ergebnisse aus 2023:

Im Jahr 2023 wurde die Sensorelektronik für die Überwachung der Kundenelektronik vollständig in Betrieb genommen und die finale Auswahl der Sensoren für das Gesamtsystem (SAFE-Modul V3) durchgeführt.

Meilenstein M3 konnte erfolgreich abgeschlossen werden.

2.1.3 AP3: Analog-/Digital Interface

Ziele:

Es soll eine Messschaltung aufgebaut werden. Außerdem werden die Messdaten aufbereitet und analysiert.

Ergebnisse aus 2021:

Erste Experimente mit käuflichen Sensorboards (vgl. Abbildung 4) und erste Absprachen zwischen den Projektpartnern zu möglichen Schnittstellen sind erfolgt. Passende elektronische Bausteine zur Wandlung der analogen Sensorsignale in digitale Signale wurden ausgewählt.

Ergebnisse aus 2022:

In den realisierten Modulen wurde eine Schnittstelle zwischen dem Mikrocontroller und den Sensoren des IZM realisiert.

Ergebnisse aus 2023:

In 2023 wurden für das Überwachungssystem weitere käufliche Sensoren zusätzlich zu den IZM-Sensoren mit dem Mikrocontroller des Überwachungssystems verbunden und der Controller mit dem Mikrocontroller der Kundenelektronik verbunden (vgl. Abbildung 9).

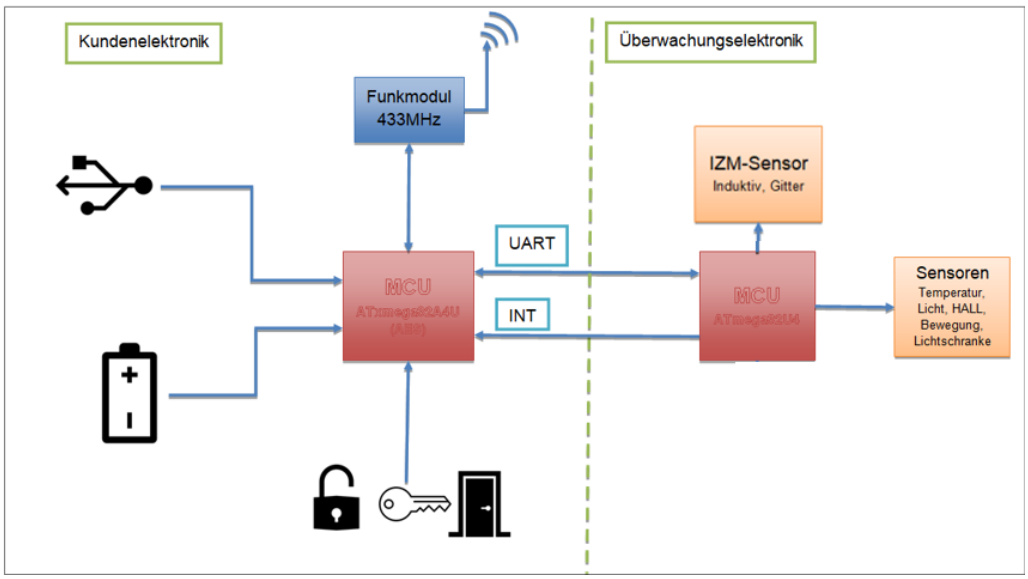


Abbildung 9: Gesamtsystem in SAFE Modul V3 (Mikrocontroller, Sensoren und Kundenelektronik)

Im Jahr 2023 wurde **Arbeitspaket AP3 erfolgreich abgeschlossen**.

2.1.4 AP4: Realisierung des Sicherheitssystems

Ziele:

Umsetzung eines Sicherheitssystems zur Erkennung von Manipulationsversuchen. Entwicklung eines Mechanismus zur Absicherung der ICs bzw. elektronischer Bauteile.

Ergebnisse aus 2021:

Um im späteren Verlauf des Projektes reale Angriffe auf eine Kundenelektronik mit Mikrocontroler demonstrieren zu können, wurden zunächst mit den Partnern unterschiedliche Anwendungsfälle und Themengebiete diskutiert. Ausgewählt wurde als Anwendungsfall ein elektronische überwachtes Sicherheitsschloss (Beispiel einer IoT-Anwendung) bei dem der Status des Schlosses per Funk übertragen wird. Die Leiterplatten dafür wurden bei JLP gefertigt. Nach der Bestückung und Inbetriebnahme konnte in 2021 die verschlüsselte (AES128-Verschlüsselung) Übertragung des Schlüsselzustandes (Tür offen / Tür geschlossen) und des Batteriestatus per Funk (433 MHz) realisiert werden. Auch eine Bildübertragung wurde realisiert. Im Empfangsmodul wurde die Entschlüsselung realisiert und die Darstellung der Schlüsselposition und des Batteriestatus auf einem Display.

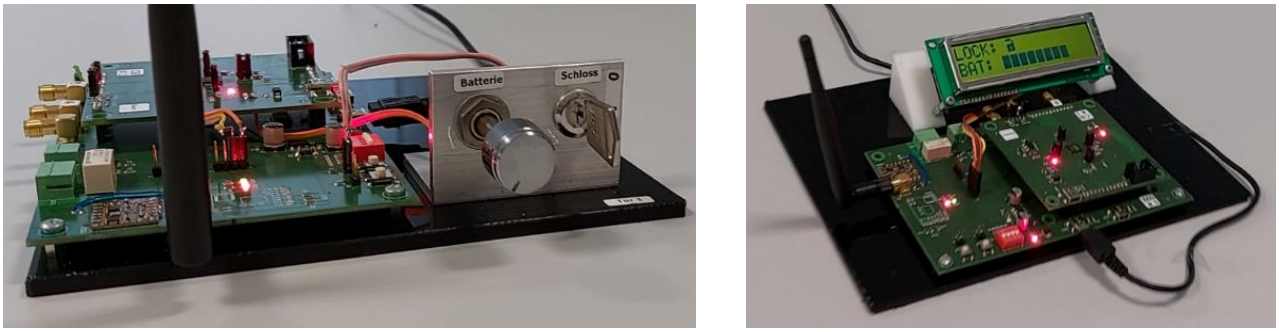


Abbildung 10: Prototyp „schützenswerten“ Kundenelektronik – Sicherheitsschloss mit Funkverbindung (Links: Sicherheitsschloss, Rechts: Empfangsstation)

Ergebnisse aus 2022:

In 2022 wurden käufliche Sensoren ausgewählt und mit dem Design und der Fertigung eines Sensorboards begonnen, auf dem unterschiedlichste käufliche Sensoren getestet werden können (z. B. Temperatur, Helligkeit, Beschleunigung).

Ergebnisse aus 2023:

Alle Sensoren des Sicherheitssystems wurden erfolgreich in Betrieb genommen und eine passende Auswertung dazu erzeugt, die auch Alarme auslöst, wenn ein bestimmter Schwellwert eines Sensors überschritten wird. Die Schwellwerte wurden durch praktische Versuche ermittelt.

Das **Arbeitspaket AP4 wurde erfolgreich abgeschlossen**.

2.1.5 AP5: Packaging-Technologie für Modul mit integrierten Sensoren

Ziel:

Es wird ein Package-Konzept mit entsprechender Aufbau- und Verbindungstechnik (AVT) entwickelt. Abschließend werden Baugruppen gefertigt, zu einem Demonstrator assembliert und in Betrieb genommen

Ergebnisse aus 2021:

In den regelmäßigen Treffen wurde mit den Projektpartnern mögliche Packaging-Technologie für die Integration von Sensoren in Leiterplattenmodule diskutiert und Anforderungen und technische Vorgaben für die Prototypenentwicklung abgeleitet. Die Projektpartner führten verschieden Verpressungsversuche durch und ermittelten z. B. Vorgaben für die maximale Bauhöhe elektronischer Bauteile, die noch verpresst werden können, damit die Leiterplatte nicht zu dick wird (vgl. Abbildung 11).

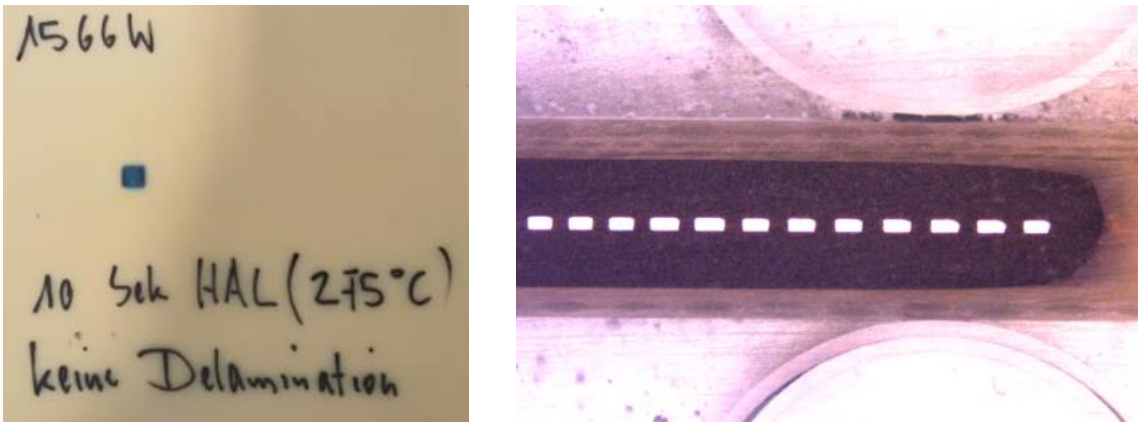


Abbildung 11: Versuche zu verpressten elektronischen Bauteilen beim Projektpartner JLP (Links: verpresstes Bauteil in Leiterplatte, Rechts: Querschliff des Bauteils)

Ergebnisse aus 2022:

In 2022 wurden nachfolgend an die Sensorsimulationen reale Module mit verpressten elektronischen Bauteilen gefertigt (vgl. Abbildung 12). Mit den Forschungspartnern wurde dann ein Qualifikationsablauf für die verpressten Module entwickelt (vgl. Abbildung 13). Dieser soll die Qualität der gefertigten Module bewerten. Nach einer Qualitätskontrolle der Module werden diese sowohl in einem Lotbad als auch zyklisch thermisch belastet. Nach der Belastung wurden dann die Module bei HTV auf Fehlerbilder analysiert und den Partnern die Ergebnisse für die Prozessverbesserung in Form eines Analyseberichtes zur Verfügung gestellt. In 2022 wurde die Qualifikation der IZM-Module vollständig durchgeführt und die Qualifikation der JLP Module begonnen. In der Qualitätskontrolle wurden im Röntgen z. B. defekte BT nach dem Verpressen gefunden (vgl. Abbildung 14). Als Ursache konnte das IZM eine Messungenauigkeit bei der Vermessung der bestückten Leiterplatte ermitteln. Die angestrebte Verpressung von elektronischen Komponenten in Leiterplatten konnte in 2022 von beiden Partnern erfolgreich durchgeführt werden.

Meilenstein M2 wurde erfolgreich abgeschlossen.

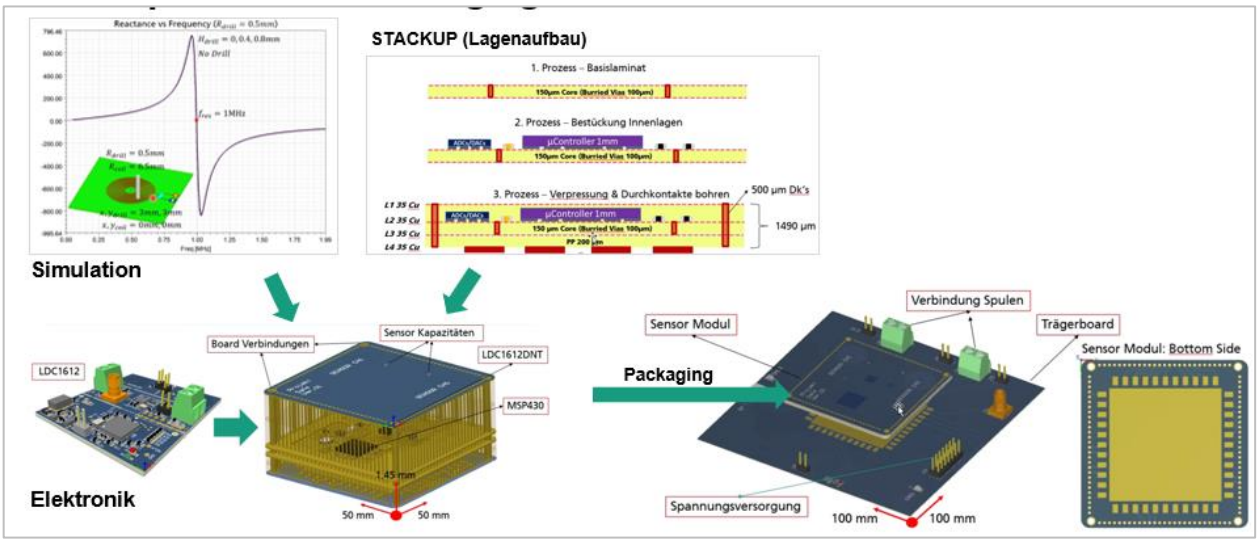


Abbildung 12: Prozess von der Sensor-Simulation bis zur Fertigung des realen Moduls

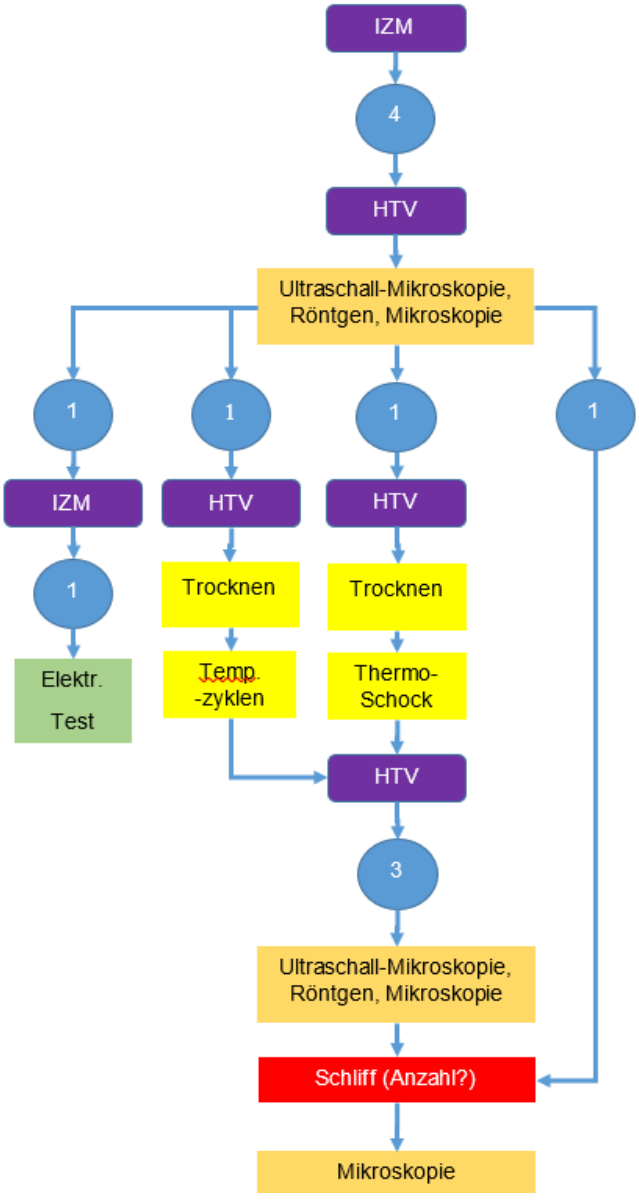


Abbildung 13: Qualifikationsablauf der verpressten Module

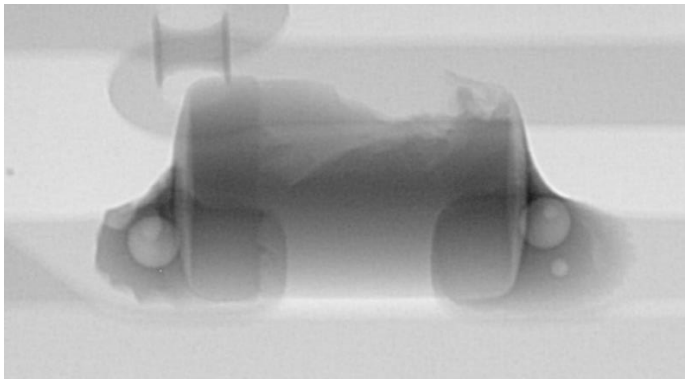


Abbildung 14: Röntgenbild von defektem Kondensator:
Die Qualitätskontrolle bei HTV analysiert die Qualität der verpressten Module

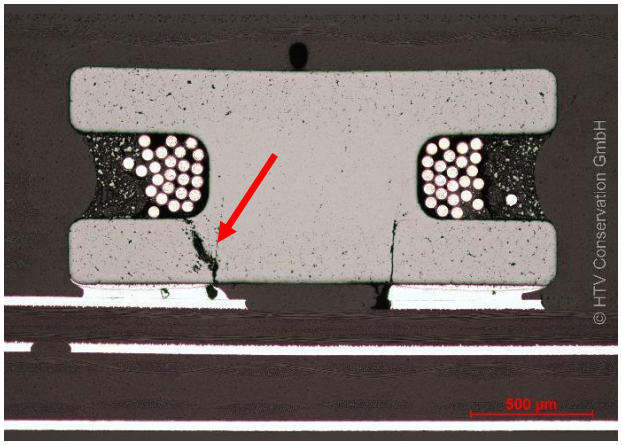


Abbildung 15: Risse in Spule (Schliffbild)

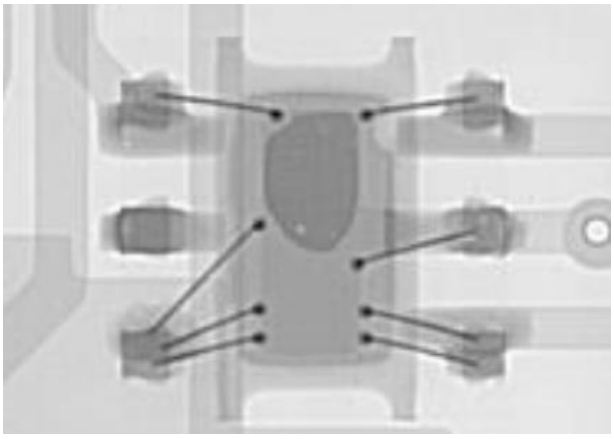


Abbildung 16: Falscher Footprint-Mismatch (Röntgen)

Ergebnisse aus 2023:

In 2023 wurde die gesamte Elektronik in ein finales SAFE-Modul V3 integriert und verpresst (vgl. Abbildung 17: CAD-Tool gesamtes Modul, Abbildung 18: CAD-Tool bestückte Innenlage, Abbildung 19: Zeitplan, Abbildung 20: gefertigte Module, Abbildung 21: Übersicht aller im Projekt entwickelten Module). Ende 2023 wurde bei HTV mit deren Qualifizierung begonnen, die bis zum Projektende in 2024 durchgeführt wird.

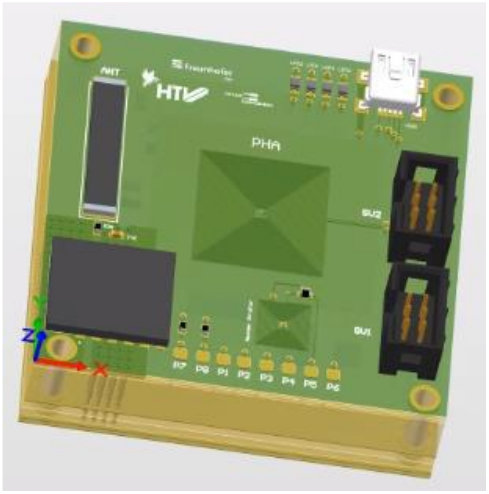


Abbildung 17: 3D Ansicht des Moduls V3

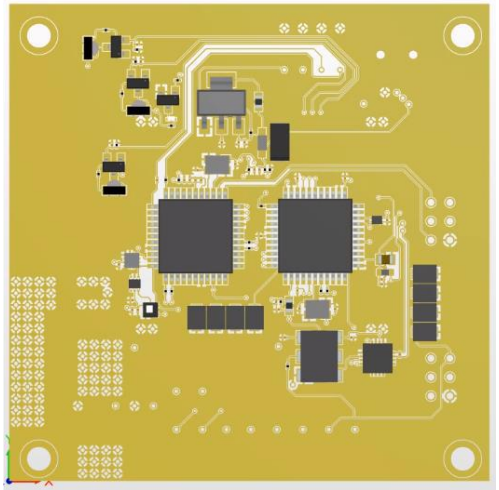


Abbildung 18: Übersicht der Innenlage des Moduls V3

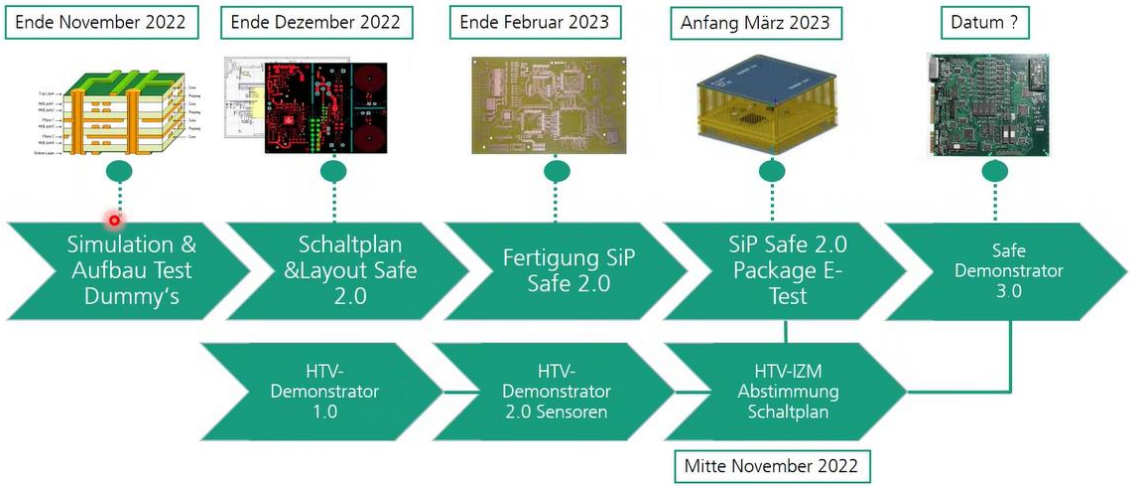


Abbildung 19: Zeitplan für die Herstellung von VE-SAFE-Modul V3

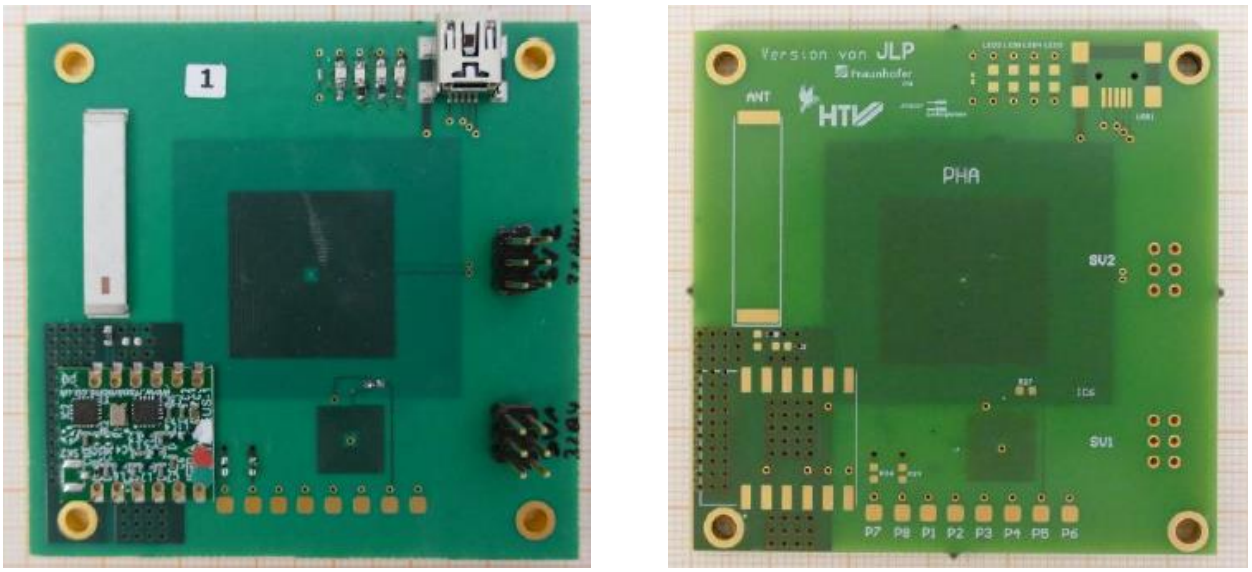


Abbildung 20: VE-SAFE-Modul V3 (link: IZM, rechtgs: JLP)

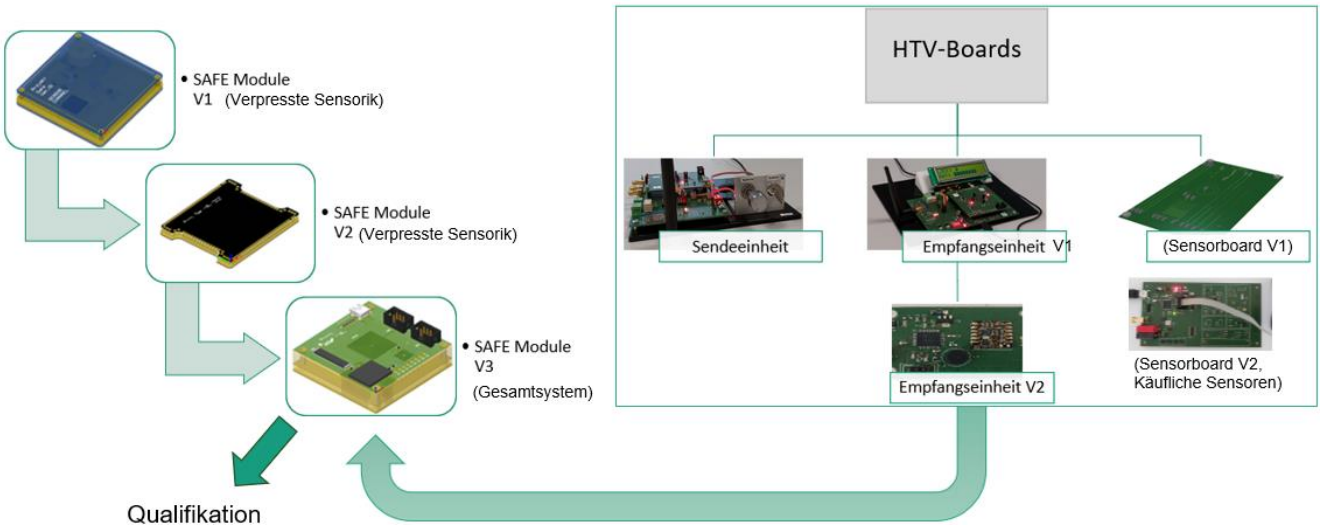


Abbildung 21: Übersicht aller im Projekt entwickelten Module

2.1.6 AP6: Systemtest und Systemevaluierung

Ziel:

Zu IT-Sicherheitsanalysen sollen Prüfplätze entwickelt und umgesetzt werden. Es sollen Evaluierungen für die Schutzmechanismen bezüglich der definierten Angriffsklassen definiert. Die Ergebnisse des gesamten Projektes werden dokumentiert.

Ergebnisse aus 2021:

Im Bereich der Systemevaluierung unterstützte HTV die Projektpartner mit Informationen im Bereich technischer Fragestellungen (z. B. bei der Ermittlung passender elektronischer Bauteile). Der Obsoleszenz-Status elektronischer Bauteile wurde ermittelt. Alle aufkommenden Fragen im Bereich der Hardware-Sicherheit wurden mit den Partnern diskutiert und wenn möglich geklärt.

Die als Softwarealgorithmus realisierte AES-Verschlüsselung des in AP4 aufgebauten Demonstrators wurde über den Stromverbrauch angegriffen. Dazu wurden zu unterschiedlichen Schlüsselbytes Messkurven aufgezeichnet und mit der internen Verarbeitung digitaler Daten im Mikrocontroller korreliert. Durch die Analyse gelang es den gewünschten Seitenkanalangriff durchzuführen und den geheimen Schlüssel mit einer Länge von 128 Bits zu extrahieren (vgl. Abbildung 22).

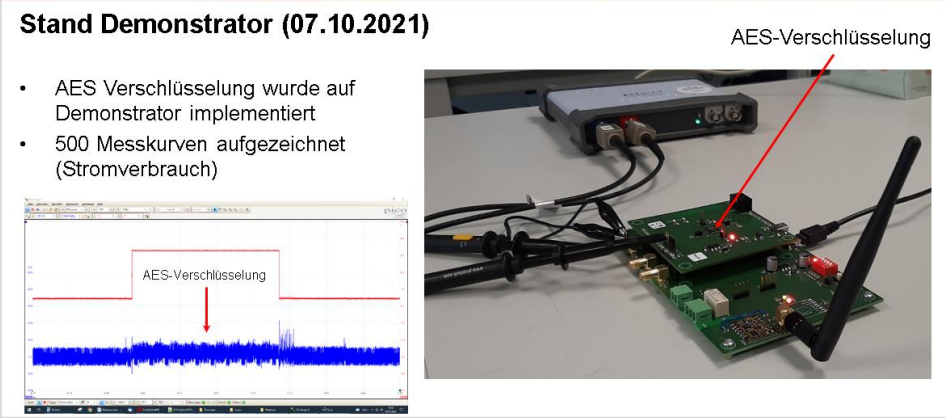


Abbildung 22: DPA-Angriff über die Stromverbrauchsmessung auf eine AES-Verschlüsselung (Schlüssellänge: 128 Bit) als Software-Algorithmus war erfolgreich

Ergebnisse aus 2022:

In 2022 wurde die Analyseplattform ChipWhisperer erfolgreich in Betrieb genommen und Seitenkanalangriffe konnten damit erfolgreich auf die AES-Verschlüsselung durchgeführt werden.

Ergebnisse aus 2023:

Im Bereich der Passwortentschlüsselung der AES-Verschlüsselung wurden in 2023 weitere Analysen an der unverpressten Kundenelektronik durchgeführt. Schwerpunkt war der Versuche aus aufgenommenen Messkurven und verschlüsselten Daten „rückwärts“ das Passwort der AES-Verschlüsselung zu ermitteln als auch das Passwort allein aus der elektromagnetischen Strahlung des Mikrocontrollers zu extrahieren. Dies Versuche war sowohl mit den Messkurven aus dem Stromverbrauch als auch der elektromagnetischen Strahlung erfolgreich. Es zeigte sich bei den Versuchen, dass der Analyse-Aufwand steigt, wenn Messkurven der elektromagnetischen Strahlung verwendet werden oder verschlüsselte Ausgangsdaten statt unverschlüsselter Eingangsdaten der AES-Verschlüsselung (vgl. Tabelle 2).

Ergebnisse aus 2024:

Anfang 2024 wurden am finalen VE-SAFE-Module V3 die final entwickelten Sicherheitsanalysen durchgeführt. Die Tabelle 1 enthält Beispiele zu möglichen Angriffen, der eine Elektronik ausgesetzt sein kann. Zu jedem Angriff sind ein oder mehr Sicherheitsfunktionen für die Angriffserkennung im VE-SAFE-Module V3 vorhanden. Die Ergebnisse der DPA-Analyse, die am finalen verpressten Modul durchgeführt wurden, zeigt, dass eine deutlich höhere Sicherheit gegen diese Art von Angriffen in diesem Forschungsprojekt erzeugt werden konnte (vgl. Tabelle 2).

Anfang 2024 wurde ebenfalls die Qualifikation der SAFE-Module V3 abgeschlossen sowohl für das IZM als auch JLP abgeschlossen. Bei den Modulen von IZM konnte der elektrische Funktionstest erfolgreich durchgeführt werden. Bei JLP wurde auch das VE-SAFE-Module V3 gefertigt eine fehlerfreie elektrische Funktion der Module konnte bei JLP aber nicht nachgewiesen werden.

Tabelle 1: Passive und aktive Maßnahmen zur Erkennung und Verhinderungen von Angriffen auf elektronische Hardware

	Angriffserkennung						
Bedrohungen	**Lichtsensor (extern)**	**Magnetsensor**	**IZM-Spule**	**IZM-Gittersensor**	**Bewegungssensor**	**Modul sendet nicht**	**Metalllage in LP**
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
	2	**1**	**2**	**3**	**4**	**1**	**1**

Tabelle 2: DPA-Analyse an verpresster Elektronik (VE-SAFE-Modul V3)

DPA-Analyse:

			Ergebnis 2023
			Elektronik ohne Verpressung
Angriffsart auf AES	**Angriffstyp**	**Richtung**	**Anzahl Messkurven**
Softwareimplementierung	Stromverbrauch	vorwärts	2.000
Softwareimplementierung	Stromverbrauch	rückwärts	5.000
Hardwareimplementierung	Stromverbrauch	vorwärts	15.000
Hardwareimplementierung	Stromverbrauch	rückwärts	25.000
Softwareimplementierung	Sonde	vorwärts	4.000
Softwareimplementierung	Sonde	rückwärts	6.000
Hardwareimplementierung	Sonde	vorwärts	30.000
Hardwareimplementierung	Sonde	rückwärts	160.000

Ergebnis 2024

Verpresse Elektronik (VE-SAFE-Modul V3)

Wird durch aktive Sensoren verhindert

Mit 25.000 nicht möglich

Mit 100.000 nicht möglich (Test erfolgt)

Mit 300.000 nicht möglich (Annahme)

Tabelle 3: Qualifikation der VE-SAFE-Module V3.0

Qualifikation der VE-SAFE-Module V3.0:

	IZM	JLP
Elektrische Funktion	1 Module: volle Funktion 5 Module: fehlerhaft	1 Modul (Jan.): 1 Controller in Betrieb 3 Module (Dez.): fehlerhaft (Bohrung) 2 Module (Jan.): fehlerhaft (elektrische Funktion)
Delamination	vorhanden (nach Belastung)	keine
Risse in Laminat	vorhanden	vorhanden
Risse in Lötstellen	Keine	vorhanden
Sonstiges	Bohrversatz, Bauteilposition	Doppelung der Lochwand

Meilenstein M4 wurde erfolgreich abgeschlossen.

2.1.7 AP0: Projektmanagement

Ziel:

Planung, Durchführung und Abschluss aller folgenden Arbeitspakete.

Ergebnisse aus 2021:

Die Projekttreffen erfolgten in 2021 aufgrund der Pandemie virtuell. HTV lud die Projektpartner dazu ein, leitete deren Ablauf und protokollierte diese im Nachgang.

31.03.2021 – Kick-off-Meeting:

- Vorstellung des Forschungsprojektes
- Austausch zu den Arbeiten in 2021
- Besprechung erster Planungen zu: Sensorprinzipien, Anwendungsfälle (Kundenelektronik), Security-Target

13.04.2021 – Projekttreffen:

- Detailvorstellung der Unternehmen der einzelnen Projektpartner
- Mehr Details zu IZM-Sensoren
- Klären erster Details für die Befragung späterer Anwender
- Kooperationsvertrag und gemeinsame Arbeitsweise in der HTV-Cloud

14.04.2021 – Konferenz „Vertrauenswürdige Elektronik“

- HTV stellt das Verbundprojekt VE-SAFE auf der Konferenz des Projektträgers vor.

27.05.2021 – Projekttreffen:

- JLP bespricht mit HTV Details zur Fertigung eines ersten Prototypen
- IZM stellt Sensor Simulation vor (vgl. Abbildung 3)

24.06.2021 – Projekttreffen:

- IZM stellt erste Messschaltung vor (vgl. Abbildung 5).
- JLP trägt Details zum Einbetten vor (z. B. mögliche Bauteilhöhen)

09.08.2021 – Projekttreffen:

- Vorstellung der Befragung zum Stand der Hardwaresicherheit
- Vorstellung einer bestückten Controller-Platine
- Vorstellung physikalische Analyse von Smartcards (vgl. Abbildung 6)
- **Meilenstein M1 wurde abgeschlossen.**

09.09.2021 – Projekttreffen:

- HTV: Vorstellung der bestückten Controller-Platinen und Trägerboards

- IZM: Vorstellung von Erkannten Annäherungsversuchen metallischer Gegenstände (vgl. Abbildung 4)
- HTV: Vorstellung einer ausgewählten Obsoleszenz Software

07.10.2021 – Projekttreffen:

- HTV ist es gelungen den geheimen Schlüssel im Controller-Board des Demonstrators über die Messung von dessen Stromverbrauch zu extrahieren (DPA-Angriff) (vgl. Abbildung 22).
- Das IZM stellt weitere Details zum Design der verpressten Leiterplatte vor.
- JLP stellt Versuchsergebnisse zu verpressten Bauteilen vor (vgl. Abbildung 11).

09.11.2021 – Projekttreffen:

- HTV: Information zum Ende der Befragung
- IZM: Besprechung weitere Details bezüglich des Designs der vergossenen Leiterplatte

14.12.2021 – Projekttreffen:

- Besprechung zu Lastenheft und Security Target Dokument
- Besprechung weiterer Details bezüglich Sensoren und der verpressten Leiterplatte

Ergebnisse aus 2022:

2022-01-25 - Projekttreffen:

- Weitere Inbetriebnahme der Kundenelektronik (Ton- und Bildübertragung)
- Start der Entwicklung eines für Angriffe wie (Bohren, Ätzen, Fräsen, Lasern)
- IZM: Weitere Simulationen für die Sensoren

2022-02-02 - Projekttreffen:

- Vorstellung aller aktuellen Ergebnisse dem VDI/VDE

2022-03-10 - Projekttreffen:

- Vorstellung der aktuellen Ergebnisse auf Fachkonferenz "Vertrauenswürdige Elektronik 2022"
- Unterstützung des IZM bei der Entwicklung eines Moduls mit verpressten elektronischen Bauteilen mit Ansteuerung und Auswertung (mit LDC1614) der vom IZM entwickelten Sensoren.

2022-03-31 - Projekttreffen:

- Durchführung weiterer Angriffe mit EM-Sonden auf die AES-Verschlüsselung
- Verpressungen von elektronischen Bauteilen bei IZM und JLP

2022-06-09 - Veröffentlichung:

- Veröffentlichung bei Velektronik zum Chipmangel und welche Lösungen im VE-SAFE Projekt genutzt werden, um im Zeitplan in der Elektronikentwicklung zu bleiben.
- Entwicklung einer Leiterplatte für physikalische Angriffe.

2022-07-14 – Projekttreffen bei JLP in Jena:

- PCB-Modul beim IZM fertiggestellt (Auswerteelektronik + Sensoren)
- Entwicklung eines Qualifikationsablaufs für die verpressten Module vom IZM und JLP bei HTV (vgl. Abbildung 13)

2022-08-23 – Projekttreffen bei HTV in Bensheim):

- Vorstellung erster Analyseergebnisse an den verpressten Modulen des IZM (vgl. Abbildung 14)

2022-09-13 (beim IZM in Berlin mit dem Projektträger):

- Vorstellung des aktuellen Projektstandes
- JLP hat seine Module auch erfolgreich fertigen können.
- Vorstellung der Qualifikationsergebnisse der IZM-Module
- **Meilenstein M2 wurde abgeschlossen**

2022-10-17:

- Vorstellung und Diskussion zu möglichen käuflichen Sensoren

2022-11-03:

- Besprechung des Projektfortschritts und Klärung der Aufgaben in 2022 und 2023

2022-12-13:

- Vorstellung des Sensorboards (Layout und Leiterplatte)

Ergebnisse aus 2023:

Auch in 2023 fanden in monatlichem Abstand regelmäßige Projekttreffen statt. An den Workshops der Velektronik wurde teilgenommen (z. B. am 14.02.2023). Der Projektstand des VE-SAFE-Projektes wurde beim „Tag der vertrauenswürdigen Elektronik“ am 10. Mai 2023 mit einem Vortrag vorgestellt. HTV nahm als Teilnehmer einer Podiumskonferenz bei der Systems Integration Conference am 28.03.2023 in Brügge online teil. Im Oktober 2023 wurden Ergebnisse aus dem VE-SAFE-Projekt in der Veröffentlichung „D. Sirkeci, U. Maaß: Inductive Sensors with integrated components“ auf dem Mikrosystemtechnik-Kongress veröffentlicht.

Die verpressten Leiterplatten (Modul V2) von JLP und IZM mit den Sensoren vom IZM wurden Anfang 2023 analysiert und in umfangreichen Analyseprozessen den Partnern die aufgetretenen Auffälligkeiten in Analyseberichten übermittelt. Es zeigten sich bei beiden Partnern unterschiedliche Fehlerbilder (vgl. Abbildung 15 und Abbildung 16) in den verpressten Modulen. Trotz der Defekte war ein Teil der Module aber elektrisch funktionstüchtig und die Verpressung konnte damit als erfolgreich bewertet werden.

Bei HTV wurde ein Sensorboard mit unterschiedlichen Sensoren (z. B. Bewegung, Helligkeit, Magnetfeld, Temperatur und Infrarotstrahlung) erfolgreich in Betrieb genommen, eine Auswertesoftware entwickelt und Sensoren für die weitere Verpressung in ein finales Modul (V3) ausgewählt (vgl. Abbildung 7, Abbildung 8).
Von HTV wurde der Schaltplan für das Gesamtsystem entworfen. Dieser wurde vom IZM in ein verpresstes Layout für das finale Gesamtsystem (VE-SAFE-Modul V3) überführt und enthält die ausgewählten Sensoren mit deren Auswerteelektronik und die Kundenelektronik (vgl. Abbildung 17, Abbildung 18).
Ende 2023 konnte dann sowohl von JLP als auch dem IZM ein VE-SAFE Modul V3 gefertigt werden (vgl. Abbildung 21). Es konnte auch ein verbesserter Empfänger für die Signale der Kundenelektronik von HTV entwickelt werden (Empfangseinheit V2).

In 2023 konnte der **Meilenstein M3 erfolgreich abgeschlossen** werden.

Ergebnisse aus 2024:
In 2024 wurde die Qualifikation der SAFE-Module V3 abgeschlossen sowohl für das IZM als auch JLP abgeschlossen. Bei den Modulen von IZM konnte der elektrische Funktionstest erfolgreich durchgeführt werden. Bei JLP wurde auch das VE-SAFE-Module V3 gefertigt eine fehlerfreie elektrische Funktion konnte aber nicht nachgewiesen werden.
HTV konnte bei den Sicherheitsfunktionen der IZM-Module zeigen, dass die IT-Sicherheit bei den verpressten Modulen deutlich gesteigert ist (vgl. Tabelle 2).

Damit konnte **Meilenstein M4 erfolgreich abgeschlossen** werden.
Die Arbeitspakete wurden wie geplant durchgeführt und die Meilensteine planmäßig erzielt.

2.2 Der wichtigsten Positionen des zahlenmäßigen Nachweises
Vertraulicher Inhalt

2.3 Der Notwendigkeit und Angemessenheit der geleisteten Arbeit
Das Projektziel war von der Durchführung wissenschaftlich-technischer Tätigkeiten abhängig, deren erfolgreiches Ergebnis innerhalb des zur Verfügung stehenden Zeitraums risikobehaftet war. Die Messverfahren benötigten eine hohe Empfindlichkeit gegenüber Manipulationsversuchen und durften zugleich keine falsch-positiven Interpretationen bei bestimmungsgemäßer Nutzung verursachen. Dies stellt hohe Anforderungen an die verwendeten Sensoren und die Erkennungsalgorithmen. Zur Systemintegration musste eine AVT entwickelt werden, die sich für unterschiedlichste Bauteile, Funktionen und Anwendungsbedingungen eignet und erschwinglich bleibt. Durch eine Auswahl an Anwendungen konnten im Laufe des Projekts lediglich die technischen Grundlagen demonstriert werden, die im Nachgang zum Forschungsprojekt noch weiter an einen realen Anwendungsfall angepasst werden müssen. Auch für eine erfolgreiche Verpressung von elektronischen Bauteilen mussten bestimmte Bedingungen eingehalten werden, die auch weiter für zukünftige Projekte analysiert und optimiert werden müssen. Die F&E-Aufwendungen dieses Projektes durch eigene Finanzierung abzudecken war nicht möglich.

2.4 Des voraussichtlichen Nutzens, insbesondere der Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans
Ein Mangel an IT-Sicherheit in elektronischen Baugruppen konnte durch eine Befragung, die im Jahr 2021 durch das VE-SAFE-Projekt durchgeführt wurde, bestätigt, werden.

Die im VE-SAFE-Projekt entwickelte Technologie kann vielseitig, z. B. bei IoT-Geräten eingesetzt werden, die eine wachsenden Verbreitungsgrad auszeichnet. Auch die Vertrauenswürdigkeit von Trusted Plattform Module (TPM) kann durch die Verpressung in eine Leiterplatte erhöht werden. Darüber hinaus kann die Sensorik des SAFE-Projektes flankierend auch die Zuverlässigkeit von Produkten innerhalb der Lieferkette erhöhen, wenn die Sensorik aktiv die Umgebung der verpressten Leiterplatte innerhalb eines Gerätes überwacht (z. B. durch Helligkeits- und Bewegungssensoren).
Die wirtschaftlichen Erfolgsaussichten nach Projektende sind sehr gut, da aus den Prototypen (verpresste Leiterplattenmodule), die in diesem Projekt entstanden sind und den gewonnenen Erfahrungen, unterschiedlichste elektronische Geräte zukünftig mit einer höheren IT-Sicherheit ausgestattet werden können. Eine kommerzielle Verwertung kann sich jedoch als problematisch herausstellen, da sich im Verbundprojekt gezeigt hat, dass die Produktion von verpressten Leiterplatten z. T. sehr aufwändig ist. Weitere Forschung und eine deszendierte Prozessentwicklung könnte hier Abhilfe schaffen.
Zusätzlich kann das Wissen und die Analyseergebnisse aus dem VE-SAFE-Projekt auch in weiteren Forschungsarbeiten integriert werden. Die Firma HTV wurde im Jahr 2023 vom TÜV Nord Konzern gekauft. Dieser hat einen eigenen Bereich mit zertifizierten Laboren für IT-Sicherheitsprüfungen (TÜV Informationstechnik GmbH). Im Anschluss an das SAFE-Projekt laufen dort aufbauend auf den Ergebnissen aus dem VE-SAFE-Projekt weitere Datenanalysen unter dem Einsatz neuronaler Netze, die in 1-3 Jahren Kunden eine verbesserte Analysetechnik zur Aufdeckung von Schwachstellen und Bewertung der IT-Sicherheit bieten können.
Zielkunden der Technologie aus dem VE-SAFE-Projekt finden sich allgemein im Bereich der Fertigung von elektronischen Geräten und Komponenten mit erhöhter IT-Sicherheit. Ein Beispiel wäre dafür z. B. die Swissbit AG die für Kunden USB-Speicher mit erhöhten Sicherheitseigenschaften fertigt. Diesen Unternehmen Analyse-Möglichkeiten anbieten zu können, erschließt für HTV einen neuen Marktbereich. Mittel- bis langfristig sind dadurch Umsatzsteigerungen von 2-5 % pro Jahr zu erwarten.

2.5 Des während der Durchführung des Vorhabens dem ZE bekannt gewordenen Fortschritts auf dem Gebiet des Vorhabens bei anderen Stellen

Während der Durchführung des Vorhabens sind dem ZE keine relevanten Fortschritte auf dem Gebiet des Vorhabens bei anderer Stelle bekannt geworden.

2.6 Der erfolgten oder geplanten Veröffentlichung des Ergebnisses nach Nr. 5 der NKBF

Im Rahmen des Projektes wurden keine Patente angemeldet. Die Erfindungshöhe der entwickelten Verfahren ist nicht ausreichend für Patente, so dass zum derzeitigen Stand auch keine Patentanmeldung geplant ist. Die Analyseergebnisse und erstellten Testprogramme können in zukünftigen Projekten aber weiterentwickelt werden und stellen damit eine wichtige Grundlage für weitere Forschungen da.

Befragung zur Lage der Hardwaresicherheit in Deutschland 2021 und Anforderungen an eine separate Schutzelektronik

HTV Halbleiter-Test & Vertriebs-GmbH, Bensheim, Deutschland

Kurzfassung

Im täglichen Leben werden Menschen künftig noch mehr elektronischen Bauteilen vertrauen müssen, die beispielsweise in selbstfahrenden Autos, Servicerobotern oder unseren alltäglichen elektronischen Systemen und Geräten zum Einsatz kommen. Zusätzlich werden unter dem Stichwort Internet of Things (IoT) eine steigende Anzahl von Geräten miteinander vernetzt, die wiederum hard- und softwareseitig immer mehr angreifbare Schwachstellen aufweisen.

Das diesem Bericht zugrundeliegende Vorhaben „Verhinderung von Angriffen auf Elektroniksysteme durch innovative Multi-Sensorik“ (VE-SAFE)“ wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16ME0236K vom 01.03.2021 bis 29.02.2024 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren. Im Vorhaben wird eine Überwachungselektronik entwickelt, die zusammen mit einer bislang ungeschützten Kundenelektronik in einer Leiterplatte verpresst wird. Die Überwachungselektronik ist anschließend in der Lage, mögliche Angriffe auf die Hardware (Kundenelektronik) des jeweiligen elektronischen Gerätes zu erkennen und passende Gegenmaßnahmen einzuleiten. Hersteller elektronischer Geräte sollen durch diese zusätzliche adaptierbare Sensorhülle zukünftig in der Lage sein, das Sicherheitsniveau ihrer elektronischen Baugruppen im Bereich der Hardwaresicherheit (bzw. Hardware Security) komfortabel und kostengünstig zu erhöhen.

Die HTV Halbleiter-Test & Vertriebs-GmbH ist einer der weltweiten Marktführer für Dienstleistungen rund um elektronische Komponenten und Spezialist in den Bereichen Test, Programmierung, Langzeitkonservierung und -lagerung, Analytik sowie Bearbeitung elektronischer Bauteile und Baugruppen und führt das Verbundvorhaben zusammen mit dem Fraunhofer IZM und der Jenaer Leiterplatten GmbH durch.

Im Rahmen des VE-SAFE Verbundprojektes führte HTV eine Online-Befragung im Bereich der Hersteller von elektronischen Geräten vom 13.08.2021 bis 12.11.2021 durch, um die Lage der Hardwaresicherheit in Deutschland 2021 zu erfassen und Anforderungen der Nutzer für die in diesem Projekt geförderte separate Schutzelektronik zu ermitteln.

1 Erstellung, Freigabe und Veröffentlichung der Befragung

Die Befragung wurde als Online-Befragung durchgeführt. Der erstellte Fragebogen enthielt vier Abschnitte mit insgesamt 31 Fragen.

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) (vgl. [1]) wurde der finale Fragebogen vor dem Beginn der Befragung für mögliche Korrektureingaben vorgelegt. Das BSI war mit den vorgeschlagenen Inhalten einverstanden und stufte den Detailierungsgrad des Fragebogens als passend ein, um ein gutes Feedback im Bereich der Hardwaresicherheit zu erhalten.

Die Veröffentlichung der Online-Befragung erfolgte über den Newsletter der HTV [2] und des Verbands der Automobilindustrie e.V. (VDA), sowie über unterschiedliche Webseiten der Forschungspartner und der Velektronik-Plattform [3].

Abbildung 1: Titelseite der Online-Befragung

2 Informationen zu den teilnehmenden Unternehmen

Von den angesprochenen Unternehmen füllten insgesamt 10 den Fragebogen zu diesem speziellen, komplexen und Geheimhaltungsanforderung unterliegenden Themenbereich vollständig aus (vgl. Abbildung 2). Die Unternehmen stammten aus den Branchen: Verteidigung, Sicherheitssysteme, Industrie, Großhandel & Entwicklungsdienstleitung, Industrieelektronik, Elektrotechnik, industrielle Automation, Elektronikfertigung, Luft- und Raumfahrt, Automatisierungstechnik und Halbleitertechnologie. Es handelt sich bei den meisten Unternehmen um KMUs (kleine und mittlere Unternehmen), gefolgt von Konzernen und Großunternehmen.

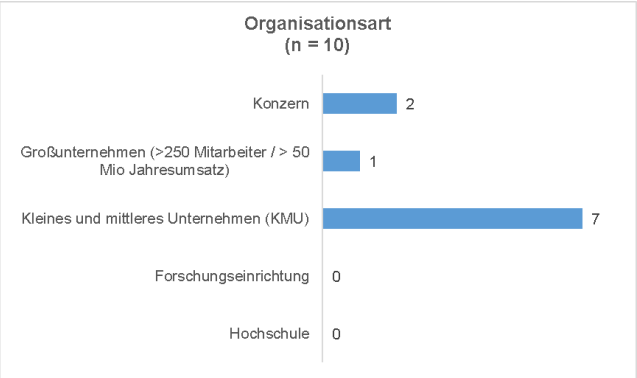


Abbildung 2: Organisationsart der teilnehmenden Unternehmen

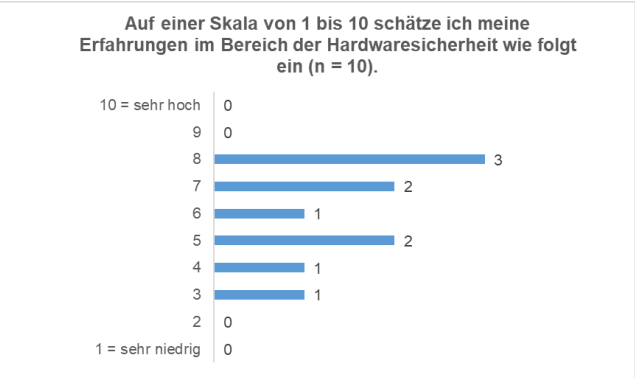


Abbildung 3: Expertise der Umfrageteilnehmer

3 Fragen zur Expertise der Teilnehmenden

Im ersten Abschnitt des Fragebogens wurden die Expertise im Bereich der Hardwaresicherheit befragt. Die Ergebnisse können wie folgt zusammengefasst werden:

- Die Teilnehmenden wiesen eine hohe Expertise im Bereich der Hardwaresicherheit elektronischer Baugruppen auf (vgl. Abbildung 3).
- Auf die Frage an welchen Konferenzen, Wettbewerben, Netzwerken und Arbeitsgruppen, die Teilnehmenden im Bereich der Hardwaresicherheit teilnehmen, wurden das „Infineon Security Partner Netzwerk“ und die „International Microelectronics Assembly and Packaging Society (IMAPS)“ genannt.
- Über Sicherheitslücken informieren sich die Teilnehmenden am häufigsten beim Bundesamt für Sicherheit in der Informationstechnik (BSI), bei Heise.de und über die firmeninterne Kommunikation.
- Die Hardwaresicherheit bei elektronischen Geräten hat für die Teilnehmenden einen hohen Stellenwert.
- Den Teilnehmenden sind im Bereich der Hardwaresicherheit als Standards und Normen am häufigsten die Common Criteria für IT-Sicherheit (CC) bekannt, gefolgt von den Federal Information Processing Standards (FIPS) und der IEC 62443 (Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme) (vgl. Abbildung 4).
- Nur 10% der Teilnehmenden stimmten der Aussage zu, dass die aktuell zur Verfügung stehenden Standards und Normen im Bereich der Hardwaresicherheit ausreichend sind für die Entwicklung sicherer elektronischer Geräte (vgl. Abbildung 5).

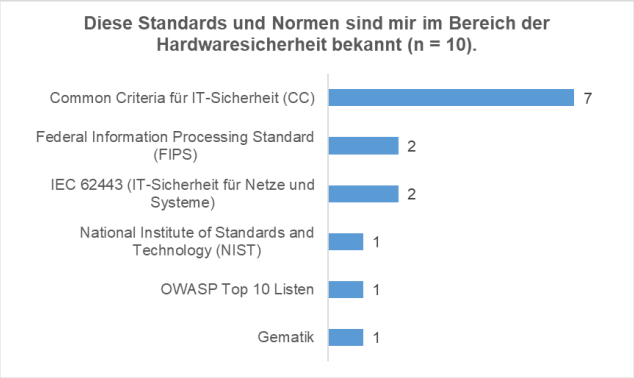


Abbildung 4: Bekannte Normen und Standards im Bereich der Hardwaresicherheit

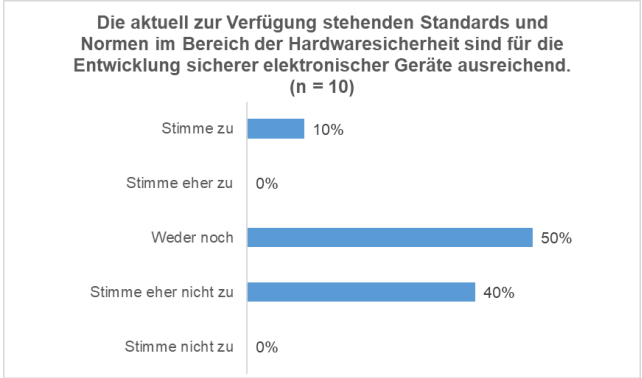


Abbildung 5: Normen und Standards zur Entwicklung sicherer elektronischer Geräte

4 Stand der Hardwaresicherheit in den teilnehmenden Unternehmen

Im zweiten Abschnitt wurden Fragen zur Hardwaresicherheit von Produkten aus dem eigenen Unternehmen gestellt. Die Ergebnisse können wie folgt zusammengefasst werden:

- Die Mehrzahl der Teilnehmenden (90%) gab an, dass die Hardwaresicherheit in ihrem Unternehmen einen hohen Stellenwert hat.
- Von den Teilnehmenden gaben 60% an, dass die Hardwaresicherheit der im eigenen Unternehmen produzierten Geräte hoch ist (vgl. Abbildung 6).
- Zu den schützenswertesten Inhalten in elektronischen Geräten zählten die Teilnehmenden unter anderem die Firmware, die erzeugten und gespeicherten Anwendungsdaten (z. B. auch Schlüssel) und das Design/Layout der elektronischen Baugruppe.
- Die Hälfte der Teilnehmenden schätzte, dass die implementierten Sicherheitsfunktionen der im eigenen Unternehmen hergestellten elektronischen Geräte eine ausreichende Qualität aufweist.
- Die Mehrzahl der Teilnehmenden (70%) hielt es für wahrscheinlich, dass Angriffe auf die elektronischen Geräte der eigenen Organisation erfolgen. Staaten wurden dabei am häufigsten als mögliche Angreifer genannt, gefolgt von Hackern und Mitbewerbern.
- Angriffe können von den Geräten der befragten Unternehmen in 30% der Fälle erkannt werden (vgl. Abbildung 7).
- Von den Befragten hielten es 70% für gefährlich, wenn Daten aus den elektronischen Geräten der eigenen Organisation in den Besitz eines Angreifers gelangen.
- Die Mehrzahl der Teilnehmenden (70%) machte keine Aussagen darüber, welche Zeit einem Angreifer für einen Angriff auf ein elektronisches Gerät der eigenen Organisation zur Verfügung steht.
- Die Teilnehmenden schätzten, dass die Angriffe auf elektronischen Geräte ihrer Organisation am häufigsten auf eine „Manipulation der Funktion“ und das „Abhören der Kommunikation“ abzielen und am häufigsten Oszilloskope, Analysesoftware und Logikanalysatoren für die Angriffe eingesetzt werden (vgl. Abbildung 8).
- Als Schwachstellen, die am häufigsten von Angreifern ausgenutzt werden, gaben die Teilnehmenden eine „Manipulation der Stromversorgung“, „offene Programmierschnittstellen“ und die Ausnutzung von „Schwankungen in der elektromagnetischen Abstrahlung“ an.
- Bei den befragten Unternehmen gaben 40% an, dass ihre elektronischen Geräte gegen Angriffe über „offene Programmierschnittstellen“ und „unverschlüsselte Kommunikation“ geschützt sind. Nur 30% der Teilnehmenden gaben an vor Angriffen in Bezug auf den Stromverbrauch oder das Timing von Signalen geschützt zu sein (vgl. Abbildung 9).
- Ein Großteil der befragten Unternehmen (80%) gab an, seinen Entwicklern Vorgaben zu machen, Gegenmaßnahmen zum Schutz vor Angriffen in die elektronischen Geräte zu integrieren.
- Die am häufigsten vorgegebenen Gegenmaßnahmen gegen Angriffe sind in den Produkten der befragten Unternehmen: „Deaktivierung von Debug-Schnittstellen“, „Verschlüsselung der Anwendungsdaten“,

„Siegel oder Plomben“, „Verwendung von Security Chips, die ein bestimmtes EAL-Level der CC aufweisen“ und „Verschlüsselung der Firmware/Bitstrom“.

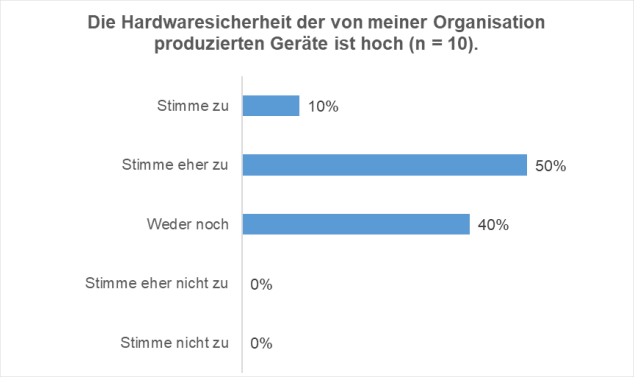


Abbildung 6: Hardwaresicherheit der im Unternehmen produzierten Geräte

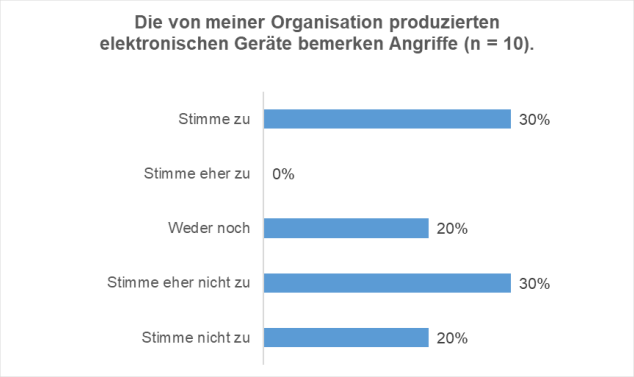


Abbildung 7: Aktive Erkennung von Angriffen

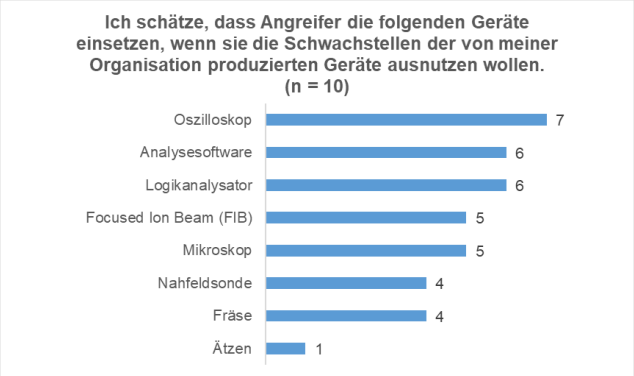


Abbildung 8: Häufig verwendete Werkzeuge für den Hardware-Angriff

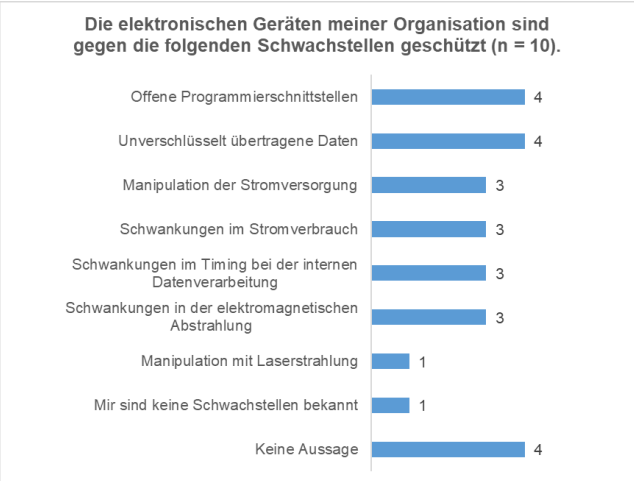


Abbildung 9: Gegenmaßnahmen

Die folgenden Wünsche wurden von den Teilnehmenden in Bezug auf die Hardwaresicherheit aktuell verfügbarer elektronischer Bauteile und Geräte geäußert:

- Stromsparendere Versionen für bisherige Versionen
- Mehr innovative Security Chips, bzw. deutliche Weiterentwicklung
- Leitungslängenmessung bei Mäander in Platinen, zum Schutz vor Anbohren
- Ultraschall oder lasergestützte Gehäuseöffnungserkennung für batteriebetriebene Geräte

5 Anforderungen an die im Verbundvorhaben VE-SAFE entwickelte Schutzhülle

Im dritten Abschnitt wurden befragt, welche Eigenschaften der im Verbundvorhaben VE-SAFE entwickelten Schutzhülle für den praktischen Einsatz gefordert oder gewünscht sind. Die Ergebnisse können wie folgt zusammengefasst werden:

- Ein Großteil der Teilnehmenden (80%) war der Ansicht, dass eine separate Elektronik zur Erkennung und Abschwächung von Angriffen sinnvoll ist (vgl. Abbildung 10).

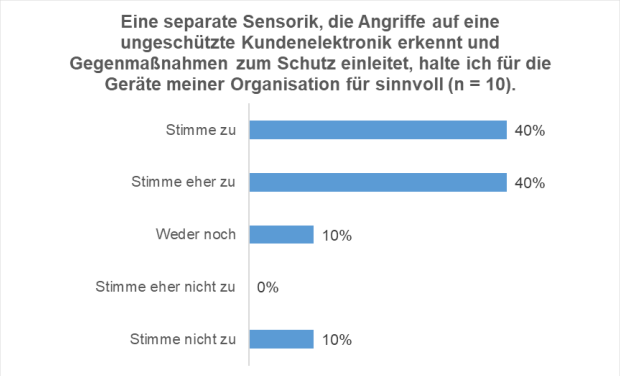


Abbildung 10: Eine separate Elektronik zum Erkennen von Angriffen ist sinnvoll.

- Eine separate Sensorik, die Angriffe auf eine ungeschützte Kundenelektronik erkennt und Gegenmaßnahmen zum Schutz einleitet, hielten die Teilnehmenden bei den folgenden Produkten oder Anwendungsbereichen für sinnvoll:
  - Wenn sensible Kundendaten sicher gelöscht werden müssen (z. B. Geräte für die Verteidigung)
  - IoT-Sensoren und IoT-Gateways
  - Für Bereiche wie z. B.: Telekommunikation, Medizintechnik, autonomes Fahren, Automatisierungstechnik, usw.
  - Geräte mit Kommunikationsschnittstellen und insbesondere, wenn diese funkbasierend sind

- Eine separate Sensorik, die Angriffe auf eine ungeschützte Kundenelektronik erkennt und Gegenmaßnahmen zum Schutz einleitet, darf die Baugruppe nach Aussage der Teilnehmenden nur um den folgenden Faktor vergrößern:
  - Allgemein:
    - so klein wie möglich
    - Vergrößerungsfaktor: 0 - 10%
    - einfach und unauffällige Integration der Sensorik bei einem Redesign im Rahmen der Produktpflege
    - Integration ohne signifikante Erhöhung des Platzbedarfs der elektronischen Baugruppe
    - extrem niedrigen Stromverbrauch
  - IoT-Sensoren: 10 x 20 mm^2
  - IoT Gateway: egal

- Eine separate Sensorik, die Angriffe auf eine ungeschützte Kundenelektronik erkennt und Gegenmaßnahmen zum Schutz einleitet, darf die Baugruppe nach Aussage der Teilnehmenden nur um den folgenden Faktor verteuern:
  - Verteidigung:
    - nicht relevant
  - Sicherheitssysteme / Elektronik:
    - 0 - 10%
  - Industrie, Großhandel & Entwicklungsdienstleitung:
    - IoT-Sensoren bis ca. 5,- Euro
    - IoT-Gateway bis ca. 9,- Euro
  - Industrielle Automation & Automatisierungstechnik:
    - Am besten gar nicht.

„Viele Kunden verstehen nicht, warum sie für etwas mehr Geld ausgeben sollen, was ihnen erstmal keinen Nutzen bringt.
Hier fehlt m.E. noch viel Verständnis und Hintergrundwissen bei den Endanwendern.“
(Zitat eines Teilnehmenden)

- Eine separate Sensorik, die Angriffe auf eine ungeschützte Kundenelektronik erkennt und Gegenmaßnahmen zum Schutz einleitet, muss nach Aussage der Teilnehmenden die folgenden Eigenschaften aufweisen, damit sie in der Praxis eingesetzt wird:
    - BSI-Zulassung
    - stromsparend
    - leicht konfigurierbar
    - kompaktes Modul (z. B. LGA)
    - geringe Eingriffe in Hardware bei Integration
    - unauffällig
    - kostengünstig
    - keine Quereffekte (z. B. „Fehlalarme“)
    - robust gegen Erschütterungen
    - Erkennung erfolgter Manipulationen beim Gerätestart
    - lange Lagerzeit (ca.10 Jahre).
    - Eignung für industriellen Temperaturbereich (-40°C bis +100°C)
    - selbstständige Manipulationserkennung

6 Fazit

Durch die durchgeführte Online-Befragung zur Lage der Hardwaresicherheit in Deutschland in 2021 konnten viele wertvolle Erkenntnisse gewonnen werden.

Aus Sicht der Teilnehmenden gibt es ein großes Verbesserungspotential der zur Verfügung stehenden Standards und Normen im Bereich der Hardwaresicherheit für die Entwicklung sicherer elektronischer Geräte. Nur 10% hielten den aktuellen Umfang der zur Verfügung stehenden Normen und Standards für ausreichend (vgl. Abbildung 5). Die Teilnehmenden nannten aber z. B. Standards wie den ISO/SAE 21434 „Road vehicles – Cybersecurity engineering“ nicht. Dies zeigt, dass bestehende Sicherheitsstandards noch weiter in der deutschen Industrie bekannt gemacht werden sollten.

Vorgaben für die sichere Entwicklung elektronischer Geräte, geben 80% der an dieser Umfrage teilnehmenden Unternehmen.

Nur 30% der Geräte der teilnehmenden Unternehmen verfügen bis jetzt über eine separate Elektronik zur aktiven Angriffserkennung (vgl. Abbildung 7)

Bei den befragten Unternehmen geben lediglich 40% an, dass ihre elektronischen Geräte gegen häufige Angriffe (z. B offene Programmierschnittstellen) geschützt sind (vgl. Abbildung 9).

Zusammenfassend ist daher ein Großteil der Teilnehmenden (80%) der Ansicht, dass eine separate Elektronik zur Erkennung und Abschwächung von Angriffen für die Geräte ihrer Organisationen, wie sie im Rahmen des Verbundprojektes VE-SAFE entwickelt wird, sinnvoll ist (vgl. Abbildung 10). Im Rahmen der Online-Befragung wurden viele Details zu Anforderungen, die eine solche separate Schutzelektronik in den unterschiedlichen Industrieanwendungen aufweisen sollte, mitgeteilt.

7 Literatur

[1] BSI. Bundesamt für Sicherheit in der Informationstechnik. www.bsi.bund.de, 2021.

[2] HTV. Das Hochleistungszentrum für elektronische Bauelemente. www.htv-gmbh.de, 2022.

[3] Velektronik. Vertrauenswürdige Elektronik. https://www.velektronik.de/bmbf-gefoerdertes-projekt-safe-befragung-zum-thema-hardwaresicherheit/, 2021.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Der aktuelle Chipmangel trifft alle Industriezweige – auch deutsche Forschungsprojekte sind betroffen

HTV Halbleiter-Test & Vertriebs-GmbH, Bensheim, Deutschland, 2022

Kurzfassung

Im täglichen Leben werden Menschen künftig noch mehr elektronischen Bauteilen vertrauen müssen, die beispielsweise in selbstfahrenden Autos, Servicerobotern oder unseren alltäglichen elektronischen Systemen und Geräten zum Einsatz kommen. Zusätzlich werden unter dem Stichwort Internet of Things (IoT) eine steigende Anzahl von Geräten miteinander vernetzt, die wiederum hard- und softwareseitig immer mehr angreifbare Schwachstellen aufweisen.

Das diesem Bericht zugrundeliegende Vorhaben „Verhinderung von Angriffen auf Elektroniksysteme durch innovative Multi-Sensorik“ (VE-SAFE)“ wird mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16ME0236K vom 01.03.2021 bis 29.02.2024 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren. Im Vorhaben wird eine Überwachungselektronik entwickelt, die zusammen mit einer bislang ungeschützten Kundenelektronik in einer Leiterplatte verpresst wird. Die Überwachungselektronik ist anschließend in der Lage, mögliche Angriffe auf die Hardware (Kundenelektronik) des jeweiligen elektronischen Gerätes zu erkennen und passende Gegenmaßnahmen einzuleiten. Hersteller elektronischer Geräte sollen durch diese zusätzliche adaptierbare Sensorhülle zukünftig in der Lage sein, das Sicherheitsniveau ihrer elektronischen Baugruppen im Bereich der Hardwaresicherheit (bzw. Hardware Security) komfortabel und kostengünstig zu erhöhen.

Die HTV Halbleiter-Test & Vertriebs-GmbH ist einer der weltweiten Marktführer für Dienstleistungen rund um elektronische Komponenten und Spezialist in den Bereichen Test, Programmierung, Langzeitkonservierung und -lagerung, Analytik sowie Bearbeitung elektronischer Bauteile und Baugruppen und führt das Verbundvorhaben zusammen mit dem Fraunhofer IZM und der Jenaer Leiterplatten GmbH durch.

Im Rahmen des VE-SAFE Verbundprojektes führte HTV eine Obsoleszenzanalyse der benötigen elektronischen Bauteile durch, um diese in ausreichender Zahl trotz aktueller Lieferengpässe im Halbleitermarkt zur Verfügung zu stellen. Lieferschwierigkeiten wurden analysiert und Lösungsansätze realisiert.

1 Hintergründe zum aktuellen Chipmangel

Einkäufer stehen aktuell vor großen Herausforderungen bei der Beschaffung dringend benötigter elektronischer Bauteile bzw. Halbleiter. Der Halbleitermangel beschäftigt weltweit nahezu alle Industriezweige. Lange Lieferzeiten und erhöhte Preise sind die Folge. Eine wirkliche Entspannung ist in 2022 nicht in Sicht. In einigen Fällen kommt es sogar vor, dass bereits zugesagte Preise nachverhandelt oder bereits bestätigte Aufträge an besser zahlende Unternehmen vergeben werden (vgl. Abbildung 1). Preise und Lieferzeiten sind für langfristige Projekte aktuell schwer kalkulierbar.

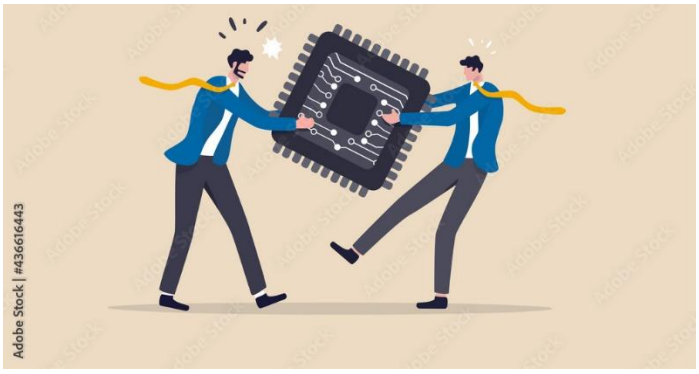


Abbildung 1: Unternehmen streiten aktuell um elektronische Bauteile

Der Halbleitermangel führt bei einigen Unternehmen zu einem Produktionsrückgang oder sogar Produktionsstopp. In der Automobilbranche führt es z. B. dazu, dass einige Fahrzeuge nur mit großen Lieferverzögerungen oder mit einer abweichenden Ausstattung (z. B. analoger Tachometer statt digitaler Version) ausgeliefert werden [5]. Im Anlagenbau werden Anlagen teilweise ohne Steuerungstechnik beim Kunden aufgebaut und können erst nach Wochen in Betrieb genommen werden, wenn die elektronischen Steuereinheiten verzögert zur Verfügung stehen.

Die weltweite Knappheit von Halbleiterbauelementen wird unter anderem derzeitig durch die folgenden Faktoren verursacht.

Hohe Nachfrage:

Die Digitalisierung und damit ein wachsender Bedarf an elektronischen Bauelementen hält in allen Bereichen des Lebens Einzug. Da elektronische Bauteile häufig aus Halbleitermaterialien gefertigt werden, verzeichnet die Halbleiterbranche große Wachstumsraten. Die World Semiconductor Trade Statistics (WSTS) hatte daher Ende November 2021 prognostiziert, dass der weltweite Halbleitermarkt im Jahr 2021 um 25,6 % und im Jahr 2022 weiter um 8,8 % wachsen wird [9]. Trotz des steigenden Angebots kann die gegenwärtige Nachfrage nicht gedeckt werden und ein großer Mangel an elektronischen Bauteilen ist die Folge.

Geopolitische Spannungen und Kriege:

Geopolitische Spannungen zwischen USA und China, aber auch die Ukraine-Krise 2022 und damit verbundene Handelsbeschränkungen, wie z. B. die ITAR-Regeln (International Traffic in Arms Regulations), führen zu Beschränkungen der weltweiten Lieferketten im Halbleitermarkt (vgl. [3] und [8]). Arbeitsgruppen aus Verbänden der Halbleiterindustrie versuchen dem entgegen zu wirken [7]. Distributoren elektronischer Bauteile bringen bei der Bauteilsuche z. B. folgenden Hinweis: „Die Lieferung in die Ukraine sowie nach Russland und Weißrussland wurden aufgrund der jüngsten Ereignisse in der Region gestoppt (Stand: 07.03.2022).“

Extreme Wetterbedingungen:

Extreme Wetterbedingungen (z. B. ungewöhnlich starke Kälte und Schneefälle) führten 2021 im US-amerikanischen Texas zu einem Aufruf an die Chipproduktionsstätten von Samsung, NXP und Infineon deren Betrieb einzustellen, um einer drohenden Überlastung des Stromnetzes entgegen zu wirken [6].

Erdbeben:

Der weltweit größte Hersteller von Silizium-Wafern in Japan, Shin Etsu, musste am 14.02.2021 aufgrund eines Erdbebens der Stärke 7,3 in Japan die Produktion herunterfahren [6].

Brand:

Brände in einer Fabrik in Taiwan, die dringend benötigte Chipträger produziert, führten zu einem Chip-Produktionsausfall bei großen Halbleiterfirmen, wie z. B. dem führenden FPGA-Hersteller Xilinx [6].

Pandemie:

Durch die Corona-Pandemie wurden weltweit Lieferketten durch Lockdown-Maßnahmen oder Arbeitsverbote empfindlich gestört. Hochseehäfen wurden z. T. wochenlang geschlossen und Produktionen gedrosselt. Dies führte zu längeren Lieferzeiten und höheren Preisen auf dem Halbleitermarkt [2].

Mangel bzw. Rationierung von elektrischer Energie:

In China kam es 2021 zur Rationierung von elektrischer Energie. Unternehmen waren hierdurch gezwungen ihre Produktion herunterzufahren. Als Grund wurden die gestiegenen Kosten für Kohle genannt, die auf die

Nutzer aufgrund strenger Regulierungen nicht weitergegeben werden durften und so zu einer Reduktion der Stromproduktion führten [1].

Obsoleszenz:

Ein elektronisches Bauteil gilt dann als obsolet, wenn es nicht mehr nach der originalen Spezifikation beim Originalhersteller hergestellt wird. Ein Blick in den Halbleitermarkt im Bereich der programmierbaren logischen Schaltungen (engl. programmable logic device, PLD), zu denen unter anderem die häufig eingesetzten FPGAs (Field Programmable Gate Array) gehören, zeigt, dass viel der in der Vergangenheit gegründeten Firmen heute nicht mehr am Markt vertreten sind. Selbst die beiden größten FPGA-Hersteller Xilinx und Altera wurden in den letzten Jahren von AMD und Intel aufgekauft (vgl. rote Pfeile in Abbildung 2). Die beiden Prozessorhersteller benötigten die FPGA-Technologie dringend für eine zusätzliche Beschleunigung ihrer Prozessoren.

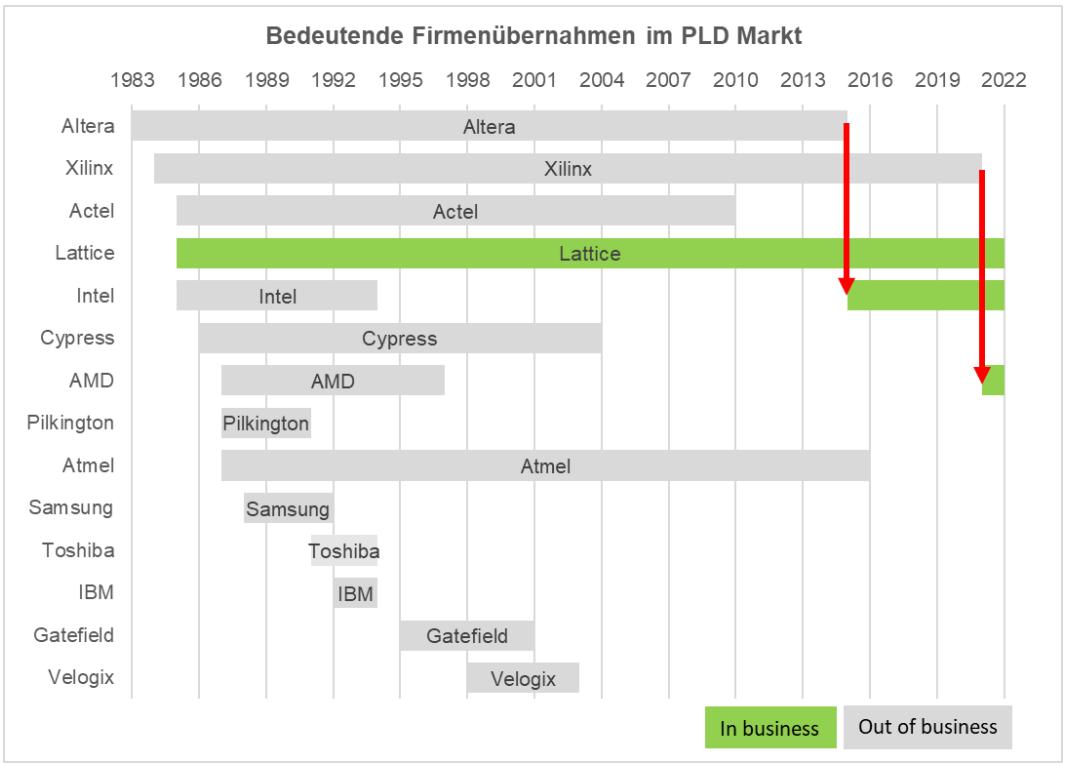


Abbildung 2: Beispiele zu Firmen die im PLD-Markt tätig waren oder noch tätig sind.

2 Stücklisten-Obsoleszenzanalyse beim Forschungsprojekt VE-SAFE

Um die Versorgungssicherheit bei den benötigten elektronischen Komponenten für das Forschungsprojekt VE-SAFE sicherzustellen, wurden eine Obsoleszenzanalyse der Stückliste (engl. Bill of materials, BOM) mit dem Life Cycle Management Tool der Firma Amsys bei HTV durchgeführt [4]. Diese Datenbankanwendung prüft in internationalen Bauteildatenbanken den Obsoleszenz-Status elektronischer Bauteile und ist in der Lage alternative elektronische Bauteile bei Bedarf vorzuschlagen. Für die Bauteilsuche wird dabei die exakte MPN (manufacturer part number) und der Herstellername benötigt.

Die Datenbank zeigte im Jahr 2021 keine Anzeichen für Obsoleszenz oder eine Bauteilverknappung bei den geplanten elektronischen Bauteilen für die nächsten 4 Jahre (vgl. Abbildung 3 und Abbildung 4).

Aufgrund der aktuellen Herausforderungen am Halbleitermarkt wurde zu Beginn des Forschungsprojektes beschlossen, die benötigten Bauteile bereits im Jahr 2021 in ausreichender Höhe zu beschaffen, um deren Verfügbarkeit über den gesamten Projektverlauf hinweg sicherstellen zu können.

Kundenteilenummer (KTN)	Bezeichnung / Hersteller	Aktueller Obsoleszenzstatus	Vorhersage 2 Jahre	Vorhersage 4 Jahre	Vorhersage 6 Jahre
SAFE	SAFE	Active	Active	Active	Obsolete
ControllerBoard V1.00	ControllerBoard V1.00	Active	Active	Active	Obsolete
Safe Mainboard V1.00	Safe Mainboard V1.00	Active	Active	Active	Obsolete

Abbildung 3: Stücklisten-Obsoleszenzanalyse elektronischer Bauteile im Forschungsprojekt VE-SAFE

Aktualisiert am: 2022-03-02

Kundendaten (Import)

Datenbankabgleich

Obsoleszenzdaten

Technische und weitere Daten

Kundenteilenummer (KTN)	556-ATXMEGA32A4U-AU
Herstellerteilenummer (HTN) (raw)	ATXMEGA32A4U-AU
Hersteller (raw)	MicroChip
Hersteller Bezeichnung der Einheit (raw)	Atmel AVR XMEGA Mikrocontroller ATXMEGA32A4U-A
Herstellerteilenummer (HTN) (clean)	ATxmega32A4U-AU
Hersteller (clean)	Microchip Technology
Hersteller Bezeichnung der Einheit (clean)	MCU 8-bit/16-bit AVR RISC 32KB Flash 1.8V/2.5V/3.3V
Hersteller CAGE Code	60991
Anzahl der Hersteller	1
Aktueller Obsoleszenzstatus	Active
Lebenszykluscode	Mature
Beginn der Produktion (SOP)	2011-07-12
Einstellung des Vertriebs (EOS) (Last Time Buy - LTB)	
Vorhersage Einstellung der Produktion (EOP)	2027-04-11
Vorhersage Jahre bis Einstellung der Produktion (YTEOP)	5.1
Obsoleszenzwahrscheinlichkeit	Low
PCN/PDN Historie	

Abbildung 4: Daten zu einem elektronischen Bauteil im Life Cycle Management Tool

3 Lieferschwierigkeiten und Lösungen

Da im Forschungsprojekt VE-SAFE zu Beginn des Jahres 2021 nicht alle über den Projektverlauf benötigten Bauteile bekannt waren, konnte nur ein Teil der benötigten Bauteile bestellt und eingelagert werden.

Im März 2022 war die zeitnahe Lieferbarkeit der zusätzlich benötigten elektronischen Bauteile nicht mehr gegeben. Bei allen großen Distributoren elektronischer Bauteile lag die Lieferzeit bei mehr als 72 Wochen oder konnte z. T. nur geschätzt werden (vgl. Tabelle 1).

Tabelle 1: Verfügbarkeit des Mikrocontrollers STM32F417VGT6 bei unterschiedlichen Distributoren (15.06.2022)

Distributor	Auf Lager	Lieferzeit für STM32F417VGT6
1	0	Nicht verfügbar
2	0	Lange Lieferzeit für dieses Produkt
3	0	Das Produkt ist zurzeit nicht verfügbar und kann derzeit nicht vorbestellt werden.

Im Forschungsprojekt wird daher eine Recycling-Ansatz zur Bauteilbeschaffung verfolgt. Bei diesem werden benötigte Bauteile von bereits bestückten Baugruppen durch ein spezielles Rework-Verfahren entlötet, gereinigt und anschließend auf die Rohleiterplatten der Prototypen des Forschungsprojektes aufgebracht. Durch dieses Vorgehen hoffen die Verbundpartner von VE-SAFE, das Forschungsprojekt fristgerecht durchführen zu können.

4 Fazit

Einkäufer stehen aktuell vor großen Herausforderungen bei der Beschaffung dringend benötigter elektronischer Bauteile bzw. Halbleiter. Viele Komponenten sind von langen Lieferzeiten und erhöhten Preisen betroffen. Kosten und Termine werden dadurch z. T. schwer kalkulierbar.

Der aktuelle weltweite Halbleitermangel hatten nicht nur Auswirkungen auf viele Industriezweige, auch Forschungsprojekte können davon betroffen sein.

Durch eine Stücklisten-Obsoleszenzanalyse kann sichergestellt werden, dass für die Prototypen eines Forschungsprojektes keine obsoleten Bauteile ausgewählt werden. Eine Chip-Knappheit kann aber nie 100%ig ausgeschlossen werden.

Daher sollten Forschungsprojekte den Bauteilbedarf frühestmöglich ermitteln und die Bauteile anschließend bestellen und einlagern. HTV verwendet für die Einlagerung das TAB®-Langzeitlagerungsverfahren.

Für elektronische Bauteile, die inakzeptabel lange Lieferzeiten aufweisen, sollte geprüft werden, ob diese durch einen Recycling-Prozess von einer bestehenden Baugruppe entlötet werden können. Im Forschungsprojekt VE-SAFE verwendet HTV dafür einen speziellen Rework-Prozess.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

5 Literatur

[1] Dana Heide. China stellt Unternehmen den Strom ab - auch deutsche Firmen leiden. *https://www.handelsblatt.com/politik/international/energieversorgung-china-stellt-unternehmen-den-strom-ab-auch-deutsche-firmen-leiden/27721118.html*, 20.10.2021.

[2] Joachim Hofer. Samsung und Micron schränken Chip-Produktion ein - Sorge vor Lieferengpässen wächst. *https://www.handelsblatt.com/technik/it-internet/corona-lockdown-in-xian-samsung-und-micron-schraenken-chip-produktion-ein-sorge-vor-lieferengpaessen-waechst/27931874.html*, 29.12.2021.

[3] Lars Hoffmann. US-Exportkontrolle - ITAR-Regeln werden in Deutschland zunehmend kritisch gesehen. *ES&T, https://esut.de/2019/01/fachbeitraege/ruestung/10119/us-exportkontrolle-itar/*, 24.01.2019.

[4] HTV. Stücklisten-Obsoleszenzanalyse - Überwachung und Vorhersage der Verfügbarkeit elektronischer Komponenten. *https://www.htv-gmbh.de/dienstleistungen/langzeitkonservierung/stuecklisten-obsoleszenzanalyse*, 07.03.2022.

[5] Christiane Köllner. Das müssen Sie zur Halbleiter-Krise wissen. *SpringerProfessional, https://www.springerprofessional.de/halbleiter/halbleitertechnik/das-muessen-sie-zur-halbleiter-krise-wissen/19356172*, 07.01.2022.

[6] Mark Mantel. Chip-Produktionsausfall: Extremes Wetter, Erdbeben und Brände verstärken Mangel. *https://www.heise.de/news/Chip-Produktionsausfall-Extremes-Wetter-Erdbeben-und-Braende-verstaerken-Mangel-5059076.html*, 18.02.2021.

[7] Ronald Matta. Halbleiter: Chipindustrie Chinas und der USA diskutieren Handel und Zusammenarbeit. *https://www.notebookcheck.com/Halbleiter-Chipindustrie-Chinas-und-der-USA-diskutieren-Handel-und-Zusammenarbeit.527541.0.html*, 12.03.2021.

[8] Matthias Sander. China subventioniert seine Halbleiterindustrie massiv. Die USA sehen darin eine mögliche Verletzung von WTO-Regeln. *https://www.nzz.ch/technologie/halbleiter-usa-verdaechtigen-china-wegen-subventionen-ld.1629525*, 09.06.2021.

[9] WSTS. WSTS Semiconductor Market Forecast Fall 2021. *https://www.wsts.org/76/Recent-News-Release*, 30.11.2021.

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]

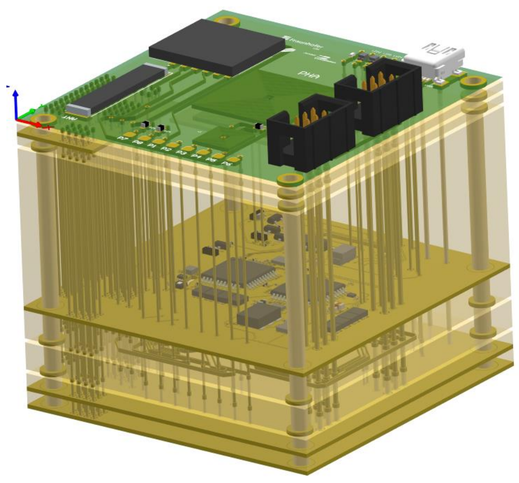
Zielstellung

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.

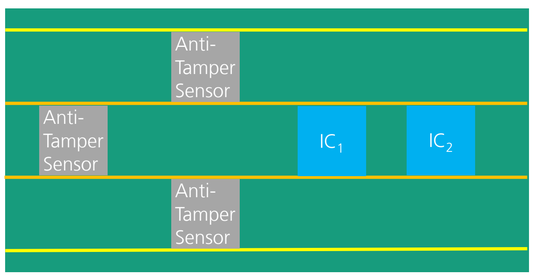
SAFE-Konzept

- 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

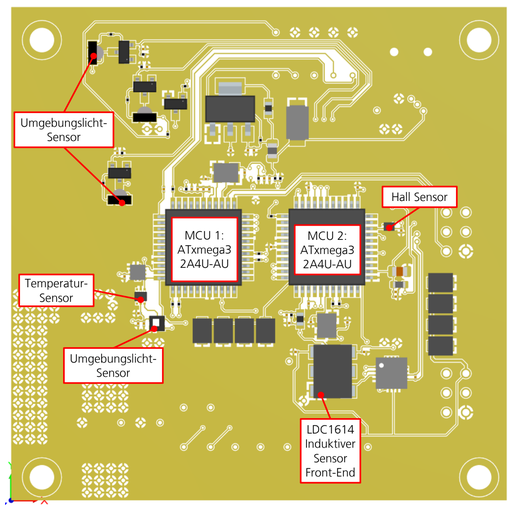
→ Zusätzlicher Schutz durch aktive Überwachung der Integrität des Elektronikmoduls mit Anti-Tamper Sensoren



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

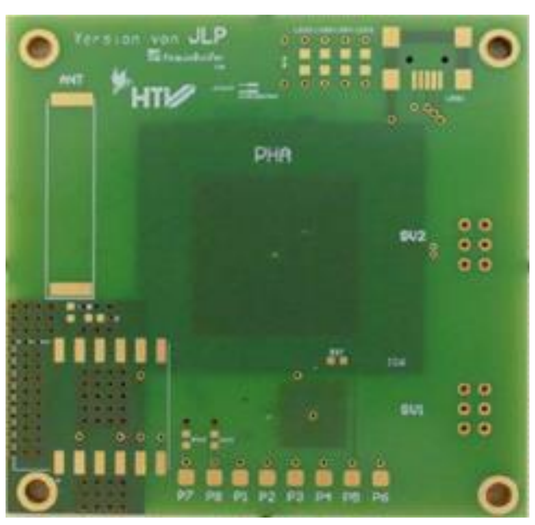


Querschnitt durch SAFE-Modul mit eigebetteten Komponenten der Kundenschaltung und Anti-Tamper Sensoren

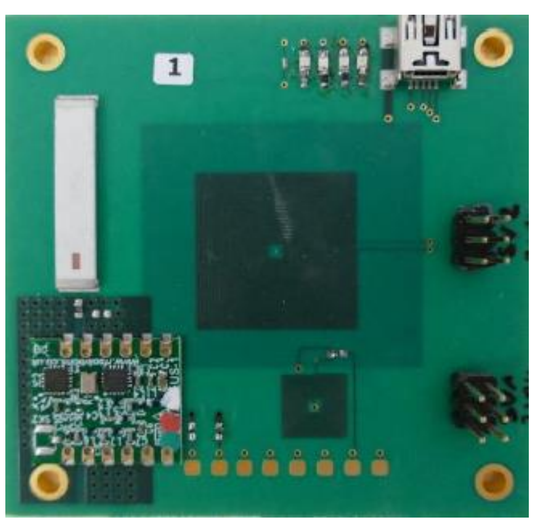


Layout eingebettete Komponentenlage in SAFE-Modul V3

Gefertigte SAFE-Module



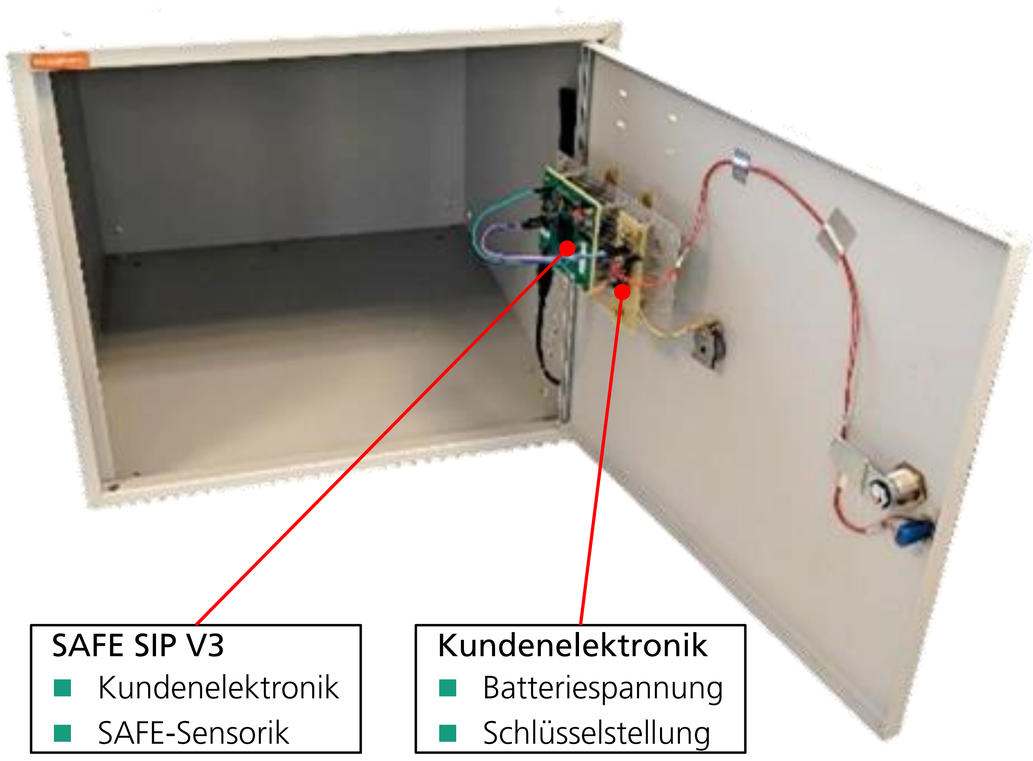
SAFE-Modul V3 in PCB-Embedding Technologie (SMD-Komponenten nicht bestückt)



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

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

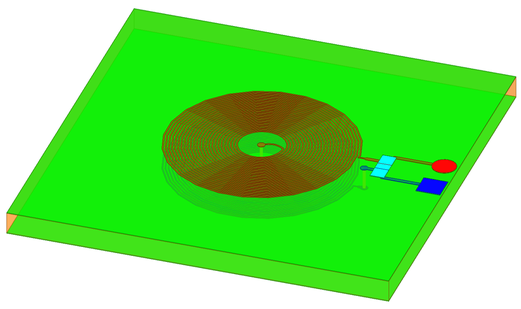
T. Kuhn[1], K. Giapakras[1], A. Friedl[2], D. Sirkeci[3], U. Maaß[3], E. Bezer[3], R. Golinske[3], M. Spanier[3], I. Ndip[3]

Zielstellung

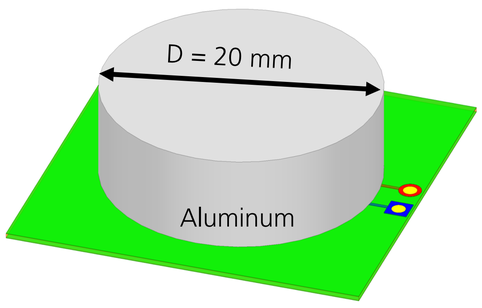
Es wurden verschiedene Sensoren zur Überwachung der Integrität sensitiver Elektronikmodule und Erkennung physkalischer Angriffe untersucht. Induktive Näherungssensoren sowie Sensoren für Umgebungslicht, Temperatur, Magnetfeld und Beschleunigung wurden durch Simulationen und Testaufbauten evaluiert. Darüber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

Induktive Sensoren

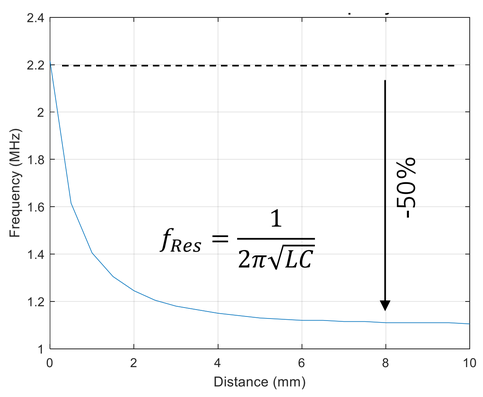
- Physikalische Angriffe durch metallische Werkzeuge (Bohrer, Fräser usw.) beeinflussen das Magnetfeld induktiver Näherungssensoren
- EM Feldsimulationen der Annäherung eines Metallwerkzeugs zeigt Änderung der Eigenschaften von Schwingkreis aus Sensorinduktivität und zusätzlicher Kapazität



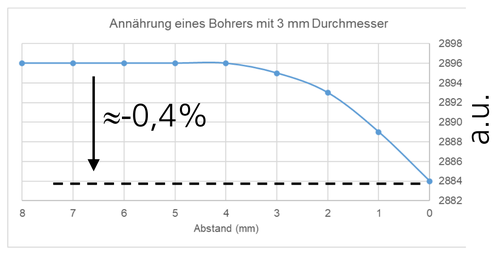
Simulationsmodell integrierte Induktivität (∅13mm, 25 Windungen, 2 Lagen, 100um Line/Space, 300um PCB-Höhe)



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

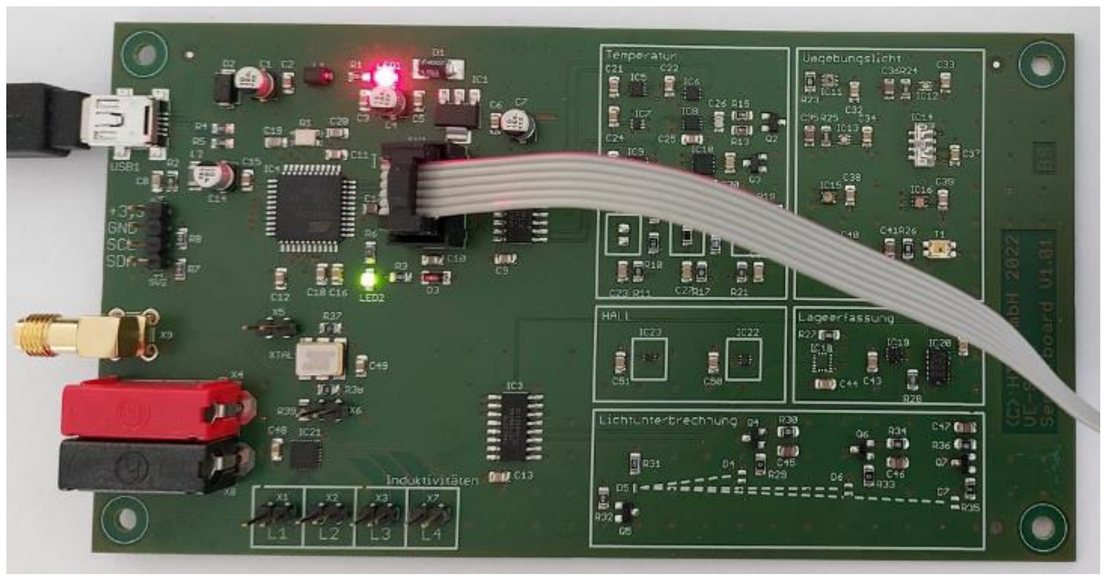


Simulationsergebnis zu Effekt der Annäherung eines metallischen Werkzeugs auf Resonanzfrequenz von Sensorspule



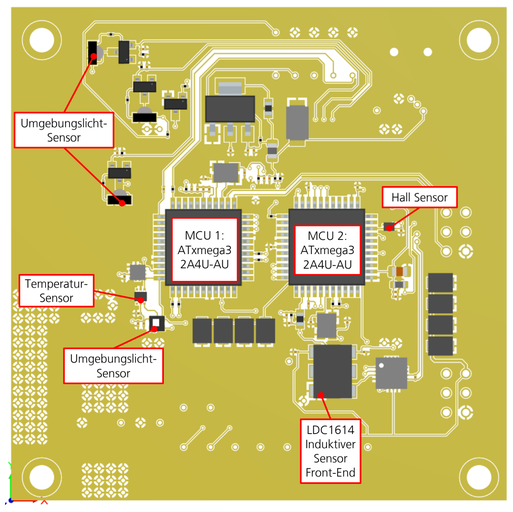
Messung der relativen Abnahme der Induktivität der Sensorspule bei Annäherung von metallischem Werkzeug

Weitere Sensoren

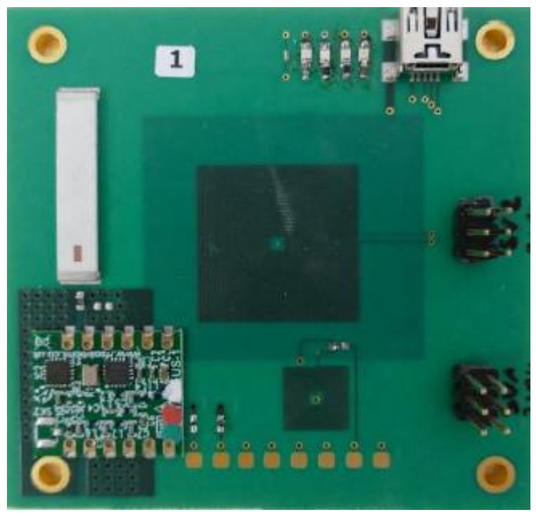


Entwickeltes Sensorboard zur Evaluierung der Erkennung von Tamper-Angriffen mit Sensoren für Umgebungslicht, Temperatur, Beschleunigung und Magnetfeld

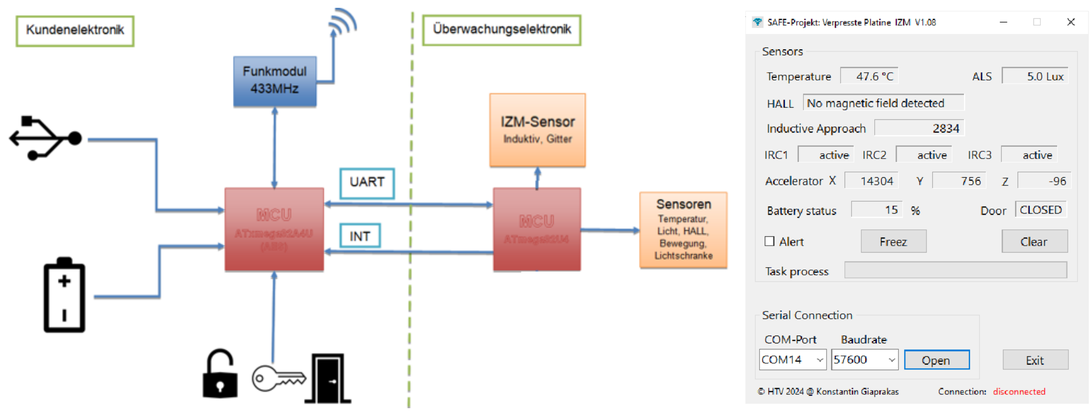
Integration der Sensoren in PCB-Embedding Modul



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