

Kurzbericht

Verbundprojekt: Verhinderung von Angriffen auf Elektroniksysteme durch neuartige keramische Mehrlagensysteme – VE-CeraTrust

Teilprojekt: AVT Prozesse für die Herstellung vertrauenswürdiger Elektronik und Test der Schutzfunktionen.

Förderkennzeichen: 16ME0391

Projektlaufzeit: 01.08.2021 bis 31.07.2024

Projektleitung: Dr. Hartmut Stoltenberg

Aufgabenstellung sowie wissenschaftlicher und technischer Stand

Die Aufgabe bestand darin, Angriffe auf Elektroniksysteme, in unserem speziellen Fall Drucktransmitter, zu erkennen und, soweit möglich, zu verhindern. Das betrifft sowohl Angriffe auf in Funktion befindliche Geräte als auch Angriffe auf die IP durch Reverse Engineering. In diesem Zusammenhang ist die eindeutige Identifikation der Elektroniksysteme und ihrer Komponenten von großer Bedeutung.

Dieses Teilprojekt nutzte für diese Aufgaben neuartige keramische Mehrlagensysteme. Diese wurden von den Projektpartnern entwickelt, umgesetzt und zur Verfügung gestellt.

Die Schwerpunkte des Teilvorhabens liegen in der Erforschung der Integration von Sicherheitsbauelementen und ihrer Einbindung in die Elektronik und ihre Realisierung im Rahmen der AVT. Das gilt sowohl für aktive - als auch für passive Sicherheitskomponenten und die zu ihrer Implementierung notwendigen Prozessschritte. Aktive Sicherheitskomponenten müssen in Teilen in die Gerätesoftware eingebunden sein. Angriffe auf in Funktion befindliche Geräte können Meldungen an übergeordnete Systeme bewirken. Angriffsstrategien wurden identifiziert und die Wirkung der im Projekt entwickelten Schutzmaßnahme untersucht und bewertet.

Im Bereich der integrierten Schaltkreise gibt es bereits eine Vielzahl von hardware-basierten Lösungen für den Manipulationsschutz. Betrachtet man Geräte und Baugruppen, wie z.B. Drucktransmitter, sind hier keine Lösungen publiziert. In der Praxis bestehen verschiedene Gefahren. Es muss beispielsweise verhindert werden, Bauelemente zu verarbeiten, die von Angreifern implementierte Funktionen enthalten. Dabei könnte beispielsweise, der vom Gerät gesendete Wert verfälscht werden. Aus diesem Grund setzt VE-CeraTrust den Fokus auf die integrierte Entwicklung relevanter Schutzfunktionen in Kombination mit dem Einsatz der am Markt erprobten LTCC- und PCB-Technik.

Ablauf des Vorhabens

Ein Lastenheft für den Demonstrator: „Drucksensor für kritische Infrastruktur“ wurde erarbeitet und im Projektverlauf fortgeschrieben. Ausgehend von der Untersuchung möglicher Angriffsstrategien erfolgte die Erarbeitung von Gegenmaßnahmen. In diesem Zusammenhang geforderte Funktionen von Bauelementen zur Identifizierung von einzelnen Bauteilen und ganzen Transmittern waren ebenso Gegenstand der Diskussionen, wie Funktionen zum Schutz vor Manipulation und Schutz der IP. Im Ergebnis dieser Absprachen enthält das Lastenheft Parameter und Sicherheitsmerkmale unter Verwendung der Technologien der Kooperationspartner. Das Lastenheft geht auf die Struktur des Demonstrators und die möglichen Maßnahmen in den einzelnen Elementen dieser Struktur ein.

Ein erster Schwerpunkt waren Identifikationsstrukturen. Die erarbeitete Bandbreite reicht dabei von Kennzeichnungen im Bereich von Datamatrixcodes über die Identifikation von PUF (Physical Uncloneable Functions) bis zum Einbringen spezieller Identifikationsmerkmale, die auch im laufenden Betrieb überwacht werden können. Für diese Aufgabe wurden entsprechende Schaltungen und Technologien

entwickelt.

Die Untersuchungen zum Manipulationsschutz ergaben, dass die Bauweise unserer Transmitter schon einen weitgehenden Schutz gegen verschiedene Angriffsszenarien bietet. Als Schwachstelle erkannte das Konsortium hier die Möglichkeit der Öffnung des Gehäuses. Entsprechend wurden mit den Partnern Keramikbauelemente entwickelt und ihre Ansteuerung bzw. Auswertung untersucht, die an dieser Stelle wirksam werden.

Mit den verschiedenen Lösungen der Partner zu den vorgenannten Themen hat sich das Konsortium eine Technologische Plattform erarbeitet.

Für die Fertigungslinie der Zukunft wurden bei PMST exemplarisch zwei Stationen zur Erfassung von Geräteparametern und ihre automatische Zuordnung zu einer Teilenummer realisiert. Diese Teilenummer wird in der Station automatisch gelesen. Die Auswahl und die Bewertung von Codereadern zu diesem Zweck fanden gemeinsam mit KMS statt. Eine Tracer Software entstand, die die Verfolgung von Losen durch die Fertigung erlaubt.

Wesentliche Ergebnisse sowie Zusammenarbeit

Im Rahmen des Projektes entstanden Lösungen für die Identifikation von Baugruppen und Geräten, die es gestatten, diese im Feld bzw. im Reklamationsfall von Plagiaten zu unterscheiden. Das betrifft z.B. den Polymerleiterzug, umgesetzt von Andus, den Doppel-T-Filter, bearbeitet von IMST, chipless RFID, entwickelt von IMST und prozessiert von VIA, und den Datamatrixcode umgesetzt von VIA mit einer Technologie von KMS. Die Identifikation spielt auch während der Fertigung eine große Rolle, um eine eindeutige Zuordnung der verbauten Komponenten und Chargen zu den fertigen Geräten herbeizuführen. Die im Projekt beispielhaft entwickelten Lösungen für den Durchlauf werden in der Perspektive in der Produktion umgesetzt.

In permanenter Abstimmung zwischen den Projektpartnern entstanden im Rahmen des Projektes Lösungen für den aktiven und passiven Schutz von Baugruppen und Geräten vor Manipulation. Die von den Projektpartnern entwickelten Schutzbauelemente, z.B. der Heizer, entwickelt von IKTS und in die Leiterplatte einlaminiert durch Andus, konnten mit der notwendigen Ansteuerungs- und Überwachungselektronik erfolgreich in den Demonstrator integriert werden. Auf dieser Basis können die Lösungen nun Kunden vorgestellt und angeboten werden.

In gemeinsamer Arbeit entstand ein Katalog mit den betrachteten Sicherheitselementen. Es erfolgt eine Gegenüberstellung des Sicherheitsrisikos der verschiedenen Angriffsmöglichkeiten zunächst ohne und dann mit den im Projekt erarbeiteten Lösungen. Dieser Katalog ist erweiterbar und bietet eine Möglichkeit den gewünschten Schutzgrad im Entwurfsstadium zu planen und zu bewerten.

Zum Projekt fanden regelmäßig Projektmeetings statt, in denen die Aktivitäten der Partner unter Federführung des Verbundkoordinators VIA electronic abgestimmt und erfolgreich organisiert wurden.

Projekt-Abschlussbericht

Verbundprojekt:	Verhinderung von Angriffen auf Elektroniksysteme durch neuartige keramische Mehrlagensysteme – VE-CeraTrust -
Teilprojekt:	AVT Prozesse für die Herstellung vertrauenswürdiger Elektronik und Test der Schutzfunktionen.
Förderkennzeichen:	16ME0391
Projektlaufzeit:	01.08.2021 bis 31.07.2024
Berichtspflichtiger:	Prignitz Mikrosystemtechnik GmbH
Projektleitung:	Dr. Hartmut Stoltenberg

1. Übersicht der wichtigsten Ergebnisse

Die Motivation für die PMST sich an diesem Projekt zu beteiligen war, Erkenntnisse zu erlangen, die es ermöglichen, die eigenen Produkte gegenüber Angriffen und Fälschungen sicherer zu machen. Die Ergebnisse sollen in unsere Drucksensoren einfließen, um unseren Kunden geschützte Drucksensordlösungen anbieten zu können. Deshalb wurde ein Schwerpunkt auf die Entwicklung eines Demonstrators gelegt, der sich von einem vorhandenen Erzeugnis ableitet und möglichst viele der im Projekt entwickelten Schutzmechanismen umsetzt.

Ein weiterer wichtiger Punkt war die Nutzung von Codierungen nicht nur zur sicheren Identifikation des Erzeugnisses, sondern auch zur Umsetzung der Rückverfolgbarkeit in der Fertigung.

Im Einzelnen war PMST an folgenden Arbeitspaketen beteiligt:

1. Spezifikation des Gesamtkonzeptes
2. Identifikationsstrukturen (Entwicklung, Design und Musterbau)
3. Manipulationsschutz (Entwicklung, Design und Musterbau)
4. Verifikation und Angriffsstrategien
6. Technologische Plattform
7. Demonstratoren (Design, Herstellung und Test)
8. Fertigungslinie der Zukunft
9. Zertifikationsstrategien

Im Folgenden wird auf die Ergebnisse der einzelnen Arbeitspakete eingegangen.

1.1 AP 1. Spezifikation des Gesamtkonzeptes

In AP 1 wurde ein Lastenheft für den Demonstrator: „Drucksensor für kritische Infrastruktur“ erarbeitet und im Projektverlauf fortgeschrieben. Wichtig in diesem Zusammenhang war insbesondere AP4, in welchem Angriffsstrategien verifiziert wurden. In diesem Lastenheft wurden Parameter sowie Sicherheitsmerkmale unter Verwendung der Technologien der Kooperationspartner zur Umsetzung im Demonstrator definiert. Dabei wurden die einzelnen Baugruppen des Transmitters betrachtet und jeweils mögliche Maßnahmen beschrieben.

Dabei wurde klar, dass es zwei Aufgabenfelder gibt. Zum einen sind im Erzeugnis Sicherheitsmerkmale vorzusehen, die einen Angriff erschweren oder ihn leichter entdeckbar machen. Zum anderen muss sichergestellt werden, dass die verwendeten Teile rückverfolgbar sind und von vertrauenswürdigen Lieferanten kommen. In diesem Zusammenhang spielt die Kennzeichnung der Einzelteile eine große Rolle. Ebenso wichtig ist die Kennzeichnung des Produktes, so dass sein Durchlauf durch die Produktion verfolgt und Prozessparameter in der Produktion und auch im Nachgang noch überprüft werden können.

1.2 AP2. Identifikationsstrukturen

Identifikationsstrukturen haben im Kontext unseres Projektes zwei unterschiedliche Aufgaben:

Die erste Aufgabe ist die eindeutige Identifikation des Erzeugnisses im Feld bzw. auch im Reklamationsfall. Das soll auch dann noch möglich sein, wenn durch einen Angriff die Seriennummer verfälscht oder beschädigt wurde. Es kann auch notwendig werden, ein gefälschtes Bauteil zu identifizieren.

Die zweite Aufgabe besteht darin, eine Identifikation des Erzeugnisses vom ersten bis zum letzten Herstellungsschritt zu ermöglichen und die verwendeten Bauteile und Baugruppen diesem Erzeugnis zuzuordnen. Das ist eine Grundvoraussetzung um Traceability zu ermöglichen, kann aber auch helfen, verfälschte Produkte zu identifizieren.

Eine Idee war die Erzeugnisse mit kleinen, möglichst versteckten DMCs eindeutig zu kennzeichnen. Diese müssen aber herstell- und lesbar sein. Im Ergebnis unserer Testreihen liegt die aktuelle technologische Grenze für PMST hier bei 2mm Kantenlänge. Für den Demonstrator wurde durch die Partner VIA electronic und KMS Technology Center GmbH ein DMC mit 1mm Kantenlänge gestanzt. Das Stanztool hatte dazu einen Durchmesser von 50µm. Ein solcher DMC findet sich auf der Anschlussplatine des Demonstrators im Chipless-RFID-Tag.

Identifikationsstrukturen können in alle Bauteile des Sensors integriert werden. Im Rahmen des Projektes wurden sie in folgenden Strukturen umgesetzt:

- Druckaufnehmer
- Zelle
- Prozessorleiterplatte
- Anschlussleiterplatte

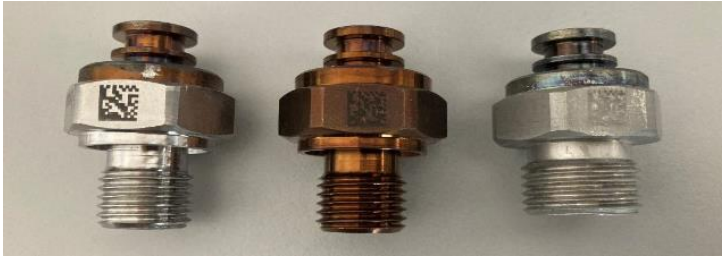


Abbildung 1: Lesbarkeit des 2D Barcodes Druckaufnehmer nach verschiedenen Fertigungsschritten

Als Identifikationsstruktur auf den Druckaufnehmern wurde ein DMC umgesetzt, der die Basis für die Rückverfolgbarkeit der Produktion ist.

Abbildung 1 zeigt die Druckaufnehmer nach verschiedenen Fertigungsschritten. Der 2D-Barcode konnte in allen abgebildeten Fertigungsschritten mit den, gemeinsam mit dem Partner KMS, getesteten Barcodescannern von Omron und Keyence sicher gelesen werden. Das trifft auch im ganz rechts in der Abbildung 1 dargestellten Zustand nach dem Laserreinigen zu. Der Code ist nach dem Laserreinigen sehr kontrastarm. In mehreren Versuchsreihen konnte ein Beleuchtungsszenario gefunden werden, das ein sicheres und reproduzierbares Lesen des Codes ermöglichte. Auch wenn der Leser über eigene Lichtquellen verfügt, ist die Nutzung externer Lichtquellen in einigen Fällen entscheidend für die Leseergebnisse.

Ein sehr interessanter Aspekt im Bereich Identifikation ergab sich aus einem Kontakt des Projektpartners Andus zur Chemitzer Werkstoffmechanik GmbH. Die Expertise dieser Firma erlaubt es, einen Fingerabdruck der Zelle im Sinne einer PUF (Physical Uncloneable Function) aufzunehmen und zu verifizieren

Die von PMST bereitgestellten Bilder in sieben verschiedenen Fertigungsstufen wurden dort analysiert. Die eingelesenen Muster konnten in jeder Stufe eindeutig erkannt werden. Dazu trug auch der mit den Glaspads eindeutig definierte Erkennungsbereich bei. Abbildung 2 zeigt die im letzten Fertigungsschritt erkannte Membranoberfläche. In Abbildung 3 ist das Ergebnis des Vergleiches einer anderen Zelle zu sehen. Es kann eindeutig festgestellt werden, dass das nicht die gesuchte Zelle ist. Mit der Aufnahme eines entsprechenden Bildes kann das Bauteil eindeutig identifiziert werden.

Damit steht eine weitere Methode zur Verfügung, die Identität der Zellen mit optischen Mitteln eindeutig festzustellen. Zum heutigen Zeitpunkt ist noch nicht entschieden, ob und in welchem Umfang solche Aufnahmen gemacht werden sollen. Es ist aber eine sehr interessante Option für sicherheitskritische Transmitter.

Geschliffene Stahloberfläche mit verschiedenen Fertigungsstufen

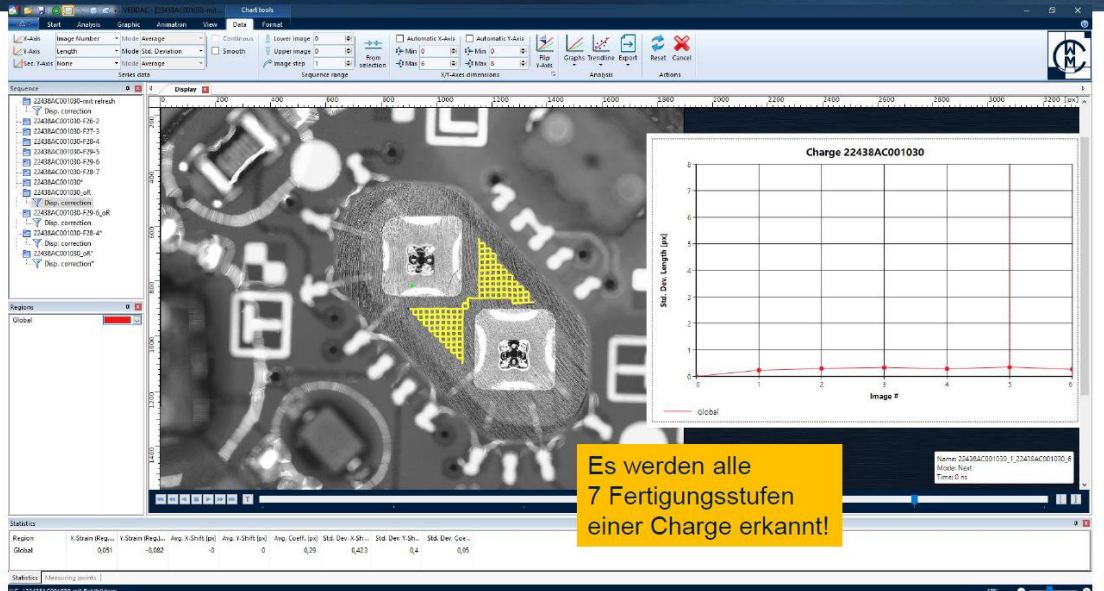


Abbildung 2: Zelle als übereinstimmend erkannt; Quelle: Bildanalyse mit DIC-Software VEDDAC 7 der Chemnitzer Werkstoffmechanik GmbH

Geschliffene Stahloberfläche mit verschiedenen Fertigungsstufen

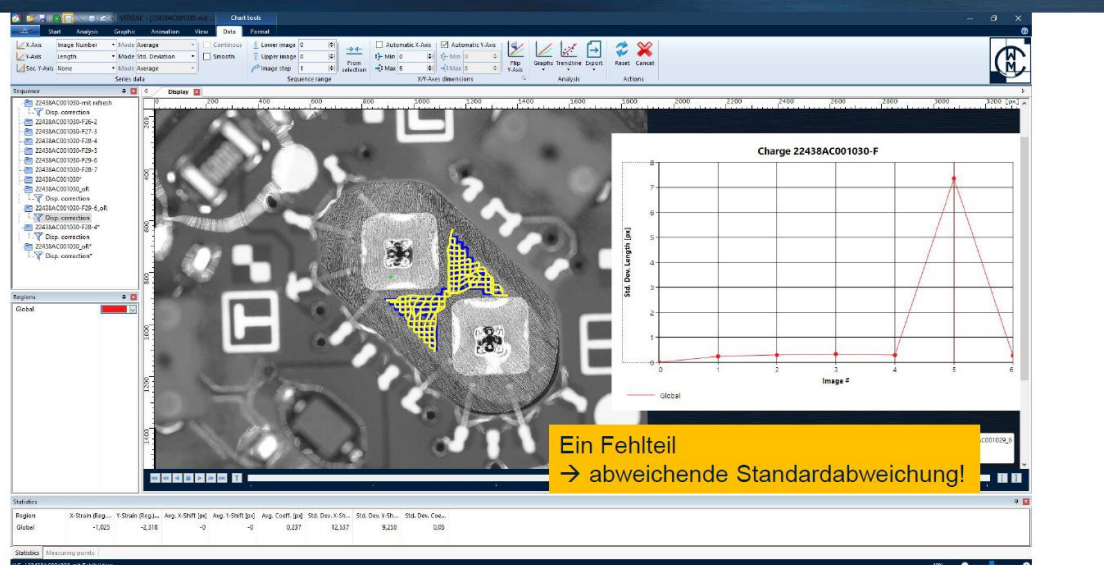


Abbildung 3: Zelle als nicht übereinstimmend erkannt; Quelle: Bildanalyse mit DIC-Software VEDDAC 7 der Chemnitzer Werkstoffmechanik GmbH

Die nächsten Identifikationsstrukturen finden sich auf der Bondleiterplatte. Durch den Partner Andus wurde ein Polymerleiterzug in der Bondleiterplatte realisiert, der für einen Angreifer nicht ohne weiteres sichtbar ist. Sein Vorhandensein ist aber ein Beleg dafür, dass die Leiterplatte nicht manipuliert wurde.

Es wurden verschiedene Ansätze verfolgt. Neben Lasergravuren, die insbesondere im Bereich der Traceability in der Fertigung große Bedeutung bekommen werden, wurde unsere Idee, ein modifiziertes Bauelement zu entwickeln und zu fertigen von der Firma IMST aufgegriffen. Entsprechende Bauelemente wurden gefertigt. Es zeigte sich aber, dass die technologischen Anforderungen so hoch sind, dass eine Umsetzung in diesem Projekt nicht möglich war. Es gibt Ideen, wie eine Umsetzung erfolgen kann. Zur Umsetzung dieser Ideen ist ggf. ein Folgeprojekt notwendig.

Für den Demonstrator wurde die vorgesehene Funktion diskret nachgebildet, um die Abfrage der Sicherheitsfunktion dieses Bauelements mit der dazu entwickelten Elektronik darstellen zu können.

Auch die Anschlussleiterplatte ist mit Identifikationsstrukturen ausgestattet. Dazu gehört ein Chipless-RFID-Tag, entwickelt durch den Partner IMST. Dieser ist zusätzlich mit einem 2D Barcode mit 1mm Kantenlänge ausgerüstet, der in dieses Keramiksubstrat gestanzt wurde. Die Technologie hierfür stammt vom Partner KMS.

Schaltungs- und Technologieentwicklung

Die Ergebnisse der Schaltungsentwicklung für die Identifikation gehen in die gleichen Baugruppen wie die Ergebnisse der Schaltungsentwicklung für den Manipulationsschutz ein. Gleichzeitig werden hier die Ergebnisse der Technologieentwicklung umgesetzt. Es entstanden bisher zwei Bondleiterplatten, ein Prozessor- und ein Interfaceboard sowie eine Anschlussleiterplatte. Das Interfaceboard realisiert die elektrische Schnittstelle zur Umwelt und sorgt für die Einhaltung der EMV-Normen. Die Anschlussleiterplatte ermöglicht es dem Kunden, den Transmitter an seine Hardware anzuschließen und erfüllt gleichzeitig Aufgaben des Manipulationsschutzes und der Identifikation.

Kern der Entwicklung ist das Prozessorboard. Die Grundidee ist, die Hardware und ihren Stromverbrauch so gering wie möglich zu halten, um den in der Automatisierungstechnik weit verbreiteten 4...20 mA 2-Leiter Ausgang realisieren zu können. Das bedeutet, dass die Schaltung mit 4 mA komplett funktionieren muss. Das ermöglicht eine breite Einsetzbarkeit, stellt aber hohe Anforderungen im Bereich des Stromverbrauches. Das betrifft die Druckmessung selbst aber auch die zusätzlichen Sicherheitsfunktionen im Bereich der Identifikation und des Manipulationsschutzes.

Diese Funktionen sind:

- Überwachung der Polymerfaser, die durch Andus in der Bondleiterplatte realisiert wird. Diese wird über eine 12 Bit ADC gemessen. Es erfolgt dabei eine ja/nein-Auswertung an einer festgelegten Schwelle.
- Überwachung des Fotosensors zur Detektion der Gehäuseöffnung. Der zu

diesem Zweck verwendete 16 Bit ADC kann darüber hinaus genutzt werden, um keramische Elemente, die in die Leiterplatte eingebettet sind (Anbohrschutz), zu überwachen.

- Der Doppel-T-Filter: Die für die Generierung des Druckmesswertes erforderliche Temperaturmessung erfolgt über einen Doppel-T-Filter. Seine, für einen potentiellen Angreifer offensichtliche Funktion, wird genau in der erwarteten Weise genutzt. Der Doppel-T-Filter kann aber auch in einen AC-Mode gebracht werden. Aktuell erfolgt der Test mit zwei Frequenzen, für die jeweils ein anderer Spannungsabfall über dem Element entsteht. Diese stehen zur Identifikation der Leiterplatte zur Verfügung.

1.3 AP3. Manipulationsschutz

Die Untersuchungen zum Manipulationsschutz, AP3, haben ergeben, dass die Bauweise unserer Transmitter schon einen sehr weitgehenden Schutz gegen verschiedene Angriffsszenarien bietet. Als Schwachstelle wurde hier die Möglichkeit der Öffnung des Gehäuses identifiziert. Daraus ergeben sich für AP3 drei Aufgabenstellungen:

1. Überwachung der Öffnung des Gehäuses,
2. Überwachung von Unterbrechungen der Stromversorgung,
3. Schaffung einer zusätzlichen Barriere unterhalb des Gehäusedeckels

Die Funktion für 1. ist im Demonstrator mit einer elektronischen Überwachung der Gehäuseöffnung realisiert. Ist der Sensor in Betrieb, wird die Öffnung erkannt und der übergeordneten Steuerung eine Alarmmeldung übermittelt. Gleichzeitig entsteht ein Eintrag im Sensortagebuch.

Die Funktion für 2. realisiert der Demonstrator über das Sensortagebuch.

Die zusätzliche Barriere für 3. entsteht mit der Leiterplatte, die den Anschlussblock trägt. Werden die Schrauben, mit der diese Leiterplatte fixiert ist, gelöst, wird ein vom IKTS entwickelter und von Andus in die Leiterplatte integrierter Heizer aktiviert, der für den Demonstrator eine Lotbrücke aufschmilzt. Es sind aber auch darüberhinausgehende Zerstörungen möglich.

Bei der Schaltungsentwicklung für diese Funktion erwies sich die Bereitstellung der erforderlichen Energie als problematisch. Eine Energiegewinnung aus dem Sensorsignal wurde untersucht, musste aber verworfen werden. Mit dem oben genannten Ausgangssignal ist nur eine Entnahme von sehr kleine Energiemengen möglich. Diese müssten in einem Kondensator oder einem Akkumulator gespeichert werden. Damit wäre die Betriebsbereitschaft der Schaltung erst nach geraumer Zeit möglich. Der Schutz würde erst nach entsprechender Betriebsdauer eintreten. Die

ersatzweise vorgesehene Batterielösung erwies sich auch als nur bedingt geeignet, weil der Innenwiderstand der ausgewählten Batterien die umsetzbare Leistung begrenzte. Die Lösung besteht zurzeit darin, die Schaltung mit vorgeladenen Akkumulatoren zu bestücken, die über einen geringen Innenwiderstand verfügen und so die erforderliche Leistung bereitstellen können. Die Selbstentladung muss aus dem Sensorsignal kompensiert werden.

Werden andere Sensorausgangssignale, bei denen eine Stromversorgung unabhängig vom Ausgangssignal besteht, verwendet, sind für diese Aufgabe einfachere Lösungen möglich. Diese Erkenntnis wird in zukünftige Entwicklungen einfließen.

Technologie für Strukturen zum Manipulationsschutz

Es wurden verschiedene Technologien und Konzepte zum Manipulationsschutz entwickelt und diskutiert. Als Drucksensorhersteller haben wir uns mit der Frage beschäftigt, ob und wie ein Drucksensorchip dazu verwendbar ist.

Wenn das zu schützende Gerät hermetisch verschließbar ist, kann man einen definierten Über- oder Unterdruck in dem Gehäuse einschließen, so dass eine im Gerät eingebaute Druckmessung, die Öffnung des Gerätes erkennen kann.

Für den Demonstrator ist das allerdings nicht umsetzbar, im Gehäuse muss funktionsbedingt Umgebungsdruck herrschen.

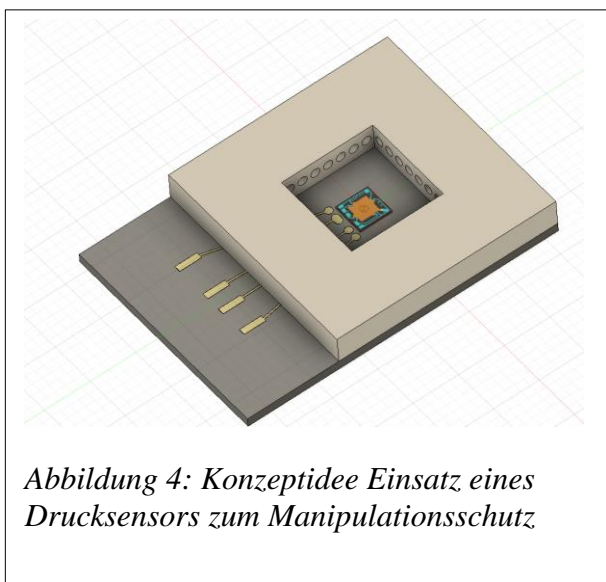


Abbildung 4: Konzeptidee Einsatz eines Drucksensors zum Manipulationsschutz

Eine weitere Idee, zum Einsatz eines Drucksensor im Bereich Manipulationsschutz, ist nach diesen Überlegungen trotzdem entwickelt worden.

Im Rahmen des Projektes wurde die Einbringung von Kavitäten zur Abschirmung von Angriffen mittels Ultraschalls untersucht. Wenn man die Kavitäten einer Schutzebene zu einem gemeinsamen Volumen verbindet, ist es möglich, den Druck in diesem Volumen mittels eines Sensorchips für Absolutdruck zu überwachen. Abbildung 4 stellt das Prinzip dar. Der Sensorchip (in der Mitte des Bildes) ist auf einer Keramiklage montiert und

durch Bonden elektrisch kontaktiert. Die Kontakte sind hier beispielhaft zur Seite herausgeführt. Es wäre auch möglich diese durch Vias nach unten herauszuführen. Die im inneren Quadrat sichtbaren Eingänge zu den Röhren verbinden alle Kavitäten in der Innenlage. Wenn man diese Anordnung mit einem keramischen Deckel unter Vakuum verschließt, ist ein effektiver flächiger Anbohrschutz gegeben.

Möglich ist auch die Einbettung piezoresistiver Strukturen in die Leiterplatte, um Spannungen im Material, die sich durch Anbohren oder das Lösen von Schrauben verändern, zu detektieren. Das IKTS hat entsprechende Sensorchips entwickelt.

Nachteilig bei allen diesen Überlegungen ist die Notwendigkeit einer Stromversorgung. Damit ist der Schutz nur während des Betriebes wirksam.

1.4 AP4. Verifikation und Angriffsstrategien

Aus Sicht der PMST geht es vorrangig immer um Angriffe auf die Erzeugnisse der PMST. Die Projektpartner haben hier nicht solch einen engen Focus. Im vorliegenden Bericht beziehen wir uns immer auf den Focus der PMST.

Es gibt zwei grundlegende Angriffsziele.

1. Manipulation der Sensorausgangssignale mit dem Ziel, Anlagenstörungen hervorzurufen.
2. Erlangung der IP zum Nachbau der Sensoren

Wege um das Ziel 1. zu erreichen sind:

- Manipulation der Zweidrahtleitung. Wird die Anschlussleitung aufgetrennt, wird das durch den Betriebsstundenzähler erkannt. Der Zeitpunkt dieser Unterbrechung kann ausgelesen werden. Wird parallel zum Transmitter ein Widerstand eingebaut, erhöht sich der Strom, was einem erhöhten Druckmesswert entspricht. Das ist durch den Transmitter nicht feststellbar.

Denkbar ist die zusätzliche zyklische Übertragung des Messwertes auf der Zweidrahtleitung in Form eines digitalen Wortes, um der Anlage eine Vergleichsmöglichkeit zu bieten.

Eine solche Manipulation ist erkennbar, wenn der Druck zu bestimmten Zeitpunkten auf Maximaldruck gefahren wird, in diesem Fall verlässt das Signal den zulässigen Wertebereich. Das ist ein Indiz für eine solche Manipulation, das allerdings nicht durch den Transmitter selbst detektierbar ist.

- Denkbar ist auch die Manipulation der Membran des Sensors durch gezielten Überdruck oder mechanisches Verbiegen der Membran. Das würde auch zu permanent verfälschten Messwerten führen. Einen solchen Angriff halten wir für unwahrscheinlich, weil er sehr spezielles Know how zum Verhalten des

Sensors erfordert und sehr präzise ausgeführt werden muss, um die Membran im plastischen Bereich zu verformen, ohne sie zu zerstören.

- Manipulation der Sensorelektronik bei laufendem Betrieb. Hierfür ist das Öffnen des Deckels erforderlich. Ein optischer Sensor überprüft laufend, ob der Deckel geschlossen ist. Wird der Sensor geöffnet, wird das der Anlage gemeldet, indem das Ausgangssignal in einen unzulässigen Bereich gefahren wird.
- Angriff auf die Firmware des Sensors bei laufendem Betrieb. Die Firmware des Transmitters ist mit einem 256 Bit Passwort gesichert. Wird ein unberechtigter Zugriffsversuch detektiert, sind Meldungen an die Anlage, aber auch ein Selbstlöschen der Firmware, vorgesehen.

Um das Ziel 2 zu erreichen, wird der Transmitter in stromlosem Zustand untersucht werden. Dadurch sind aktive Schutzmaßnahmen deutlich schwerer umzusetzen. Hier erweist sich die oben beschriebene Batterie - bzw. Akkumulatorlösung als hilfreich, denn ein solcher Angriff ist fast immer mit einer Öffnung des Transmitters verbunden.

- Öffnen des Sensors durch Abschrauben der Leiterplatte. Hier greift der oben beschriebene Mechanismus zur Zerstörung wesentlicher Bauelemente über den Heizer.
- Öffnen des Gehäuses oder der Leiterplatte durch einen mechanischen Eingriff. Hier kann ein Anbohrschutz greifen. Der Begriff Anbohrschutz umfasst dabei nicht nur Bohren, sondern jede Art der gewaltsamen Gehäuseöffnung. Entsprechende Strukturen sind keramisch oder in Leiterplattentechnologie umsetzbar. Sie können, dank der Bereitstellung der benötigten Energie durch die beschriebene Batterie - bzw. Akkumulatorlösung, die gleichen Reaktionen auslösen, wie die Überwachung der Verschraubungen. Entsprechend erfolgt über den Heizer auch hier eine Zerstörung wesentlicher Bauelemente. Im Demonstrator wurde das nicht umgesetzt.
- Angriff auf die Firmware: Um sie auszulesen, muss der Prozessor mit Betriebsspannung versorgt werden. Dadurch sind aktive Reaktionen bei falscher Passworteingabe, wie oben beschrieben, möglich. Im Demonstrator ist die Selbstlöschung der Firmware vorgesehen.

Sollte durch einen Angreifer Ziel 2 erreicht worden sein, ist die Unterscheidung der Originaltransmitter von entsprechenden Nachbauten auf Basis der unter 1.2 beschriebenen Identifikationsmaßnahmen von entscheidender Bedeutung.

1.5 AP6. Technologische Plattform

Unsere Projektpartner haben sich eine Technologische Plattform erarbeitet, die es ihnen gestattet, bestimmte Sicherheits- und Identifikationsmerkmale in Keramik bzw. Leiterplatten umzusetzen. Die Aufgabe von Prignitz Mikrosystemtechnik bestand in diesem Zusammenhang darin, Möglichkeiten der Auswertung dieser Merkmale zu schaffen.

Die gefundenen Lösungen sind:

- Überwachung der Polymerfaser, die durch Andus in der Bondleiterplatte realisiert wird. Diese wird über eine 12 Bit ADC gemessen. Es erfolgt dabei eine ja/nein-Auswertung an einer festgelegten Schwelle.
- Überwachung des Fotosensors zur Detektion der Gehäuseöffnung. Der zu diesem Zweck verwendete 16 Bit ADC kann darüber hinaus genutzt werden, um keramische Elemente, die in die Leiterplatte eingebettet sind (Anbohrschutz), zu überwachen.
- Die für die Generierung des Druckmesswertes erforderliche Temperaturmessung erfolgt über einen Doppel-T-Filter. Seine für einen potentiellen Angreifer offensichtliche Funktion wird genau in der erwarteten Weise genutzt. Der Doppel-T-Filter kann aber auch in einen AC-Mode gebracht werden. Das gemessene Antwortsignal wird im Prozessor hinterlegt, so dass jederzeit eine sichere Identifikation möglich ist.

Zur Technologischen Plattform zählen auch die Optionen zur Kennzeichnung und Identifikation, wie sie unter 1.2 beschrieben sind. Diese haben eine besondere Bedeutung bei der Umsetzung der Fertigungslinie der Zukunft.

1.6 AP7. Demonstratoren

Als Demonstrator wurde ein Drucksensor zum Einsatz im Bereich der kritischen Infrastruktur entwickelt und als Demonstrator umgesetzt.



Abbildung 5 Versuchsaufbau für den Demonstrator

Im Demonstrator wurden dazu folgende Funktionen umgesetzt:

- Überwachung der Hard- und Softwareintegrität
- Überwachung der Deckelöffnung
- Schutz vor Demontage
- Interne Protokollierung von Ereignissen
- Ausgabe von Alarmmeldungen
- Eindeutige Identifikation

Der Demonstrator besteht aus einer Druckmesszelle, einer Auswerte- und Überwachungselektronik, mehreren Gehäuseteilen und einer Anschlussleiterplatte.



Abbildung 6 Drucksensor für kritische Infrastruktur

Er ist in Abbildung 5 auf einer Halterung stehend zu sehen und in Abbildung 6 nochmals dargestellt.

Die Druckmesszelle übernimmt, neben der Umwandlung des anliegenden Druckes in ein elektrisches Signal, Zusatzfunktionen, die die Identifikation des Sensors und die Überwachung der Integrität der Zelle auch im Betrieb ermöglichen.

Bestandteile der Zelle sind unter anderem ein Druckaufnehmer und eine Bondleiterplatte.

Der Druckaufnehmer enthält mit seinem Schlibbild der Membranoberfläche ein eindeutiges Merkmal, das im Sinne eines PUF auswertbar ist. (siehe Abschnitt 2). Das Schlibbild ist in Abbildung 7 dargestellt.

Die Bondleiterplatte wurde vom Partner Andus gefertigt und mit einem Polymerleiterzug versehen, der von potentiellen Angreifern nicht ohne weiteres gefunden werden kann und der damit geeignet ist die Integrität der Zelle sicherzustellen. Ursprünglich sollte durch den Partner IMST ein Doppel-T-Filter realisiert werden. Dafür ist die größere Kupferfläche auf der Leiterplatte, zu sehen in Abbildung 8, vorgesehen. Leider ergaben sich im Zuge der Entwicklung technologische Herausforderungen, die im Rahmen dieses Projektes nicht gelöst werden konnten. Um die unter 2. beschriebene Funktion zu realisieren, wäre ein Folgeprojekt notwendig. Für den Demonstrator wurde ein diskreter Doppel-T-Filter realisiert, der zwar für einen Angreifer sichtbar wäre, aber die Möglichkeit eröffnet, die softwareseitige Abfrage zu demonstrieren.

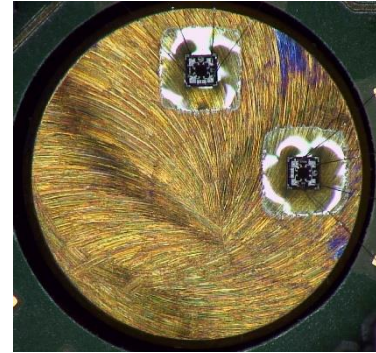


Abbildung 7 Membranoberfläche mit charakteristischem Schliffbild im Sinne einer PUF auswertbar

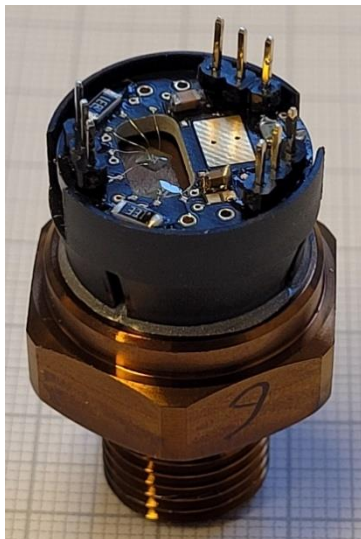


Abbildung 8 Druckmesszelle mit Sonderfunktionen

Um die oben beschriebenen Funktionen umzusetzen, wurde eine Sensorelektronik, bestehend aus Hard und Software, entwickelt. Abbildung 9 zeigt die Sensorelektronik montiert auf der Zelle. Auf der linken Seite ist das Interfaceboard erkennbar, das die Stromversorgung des Prozessorboards sicherstellt, die notwendigen Bauelemente für die Sicherstellung der EMV-Eigenschaften enthält und die Ausgabe des 4...20mA-Drucksignals realisiert. Bei der rechten Leiterplatte handelt es sich um das Prozessorboard, das neben der Verarbeitung des Zellensignals und der Erzeugung eines digitalen Ausgangssignals die Prüfung der Integrität der Zelle auf der Basis der Abfrage des

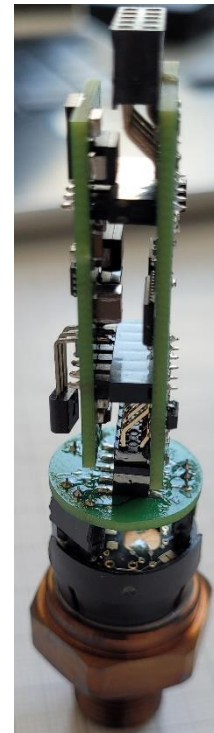


Abbildung 9 Zelle mit Sensorelektronik

Polymerleiterzuges und des Doppel-T-Filters übernimmt. Weitere Aufgaben des Prozessors bestehen in der Überwachung der Deckelöffnung, der Führung des Sensortagebuches und der Ausgabe eines Fehlersignals bei definierten Ereignissen.

Abbildung 10 zeigt einen Screenshot des Programms zur Sensorüberwachung. Auf der linken Seite werden Informationen zum Sensor, der kalibrierte Druckbereich etc. dargestellt. In der Mitte oben ist das Ergebnis des Integritätschecks zu sehen. In der Mitte unten sieht man die letzten 10 Einträge des Sensortagebuches und die Klartextinterpretation des gehighlighteten Ereignisses. Ganz oben wird der Status des Sensors dargestellt. Im vorliegenden Fall also ein Alarm, weil der Deckel geöffnet wurde.

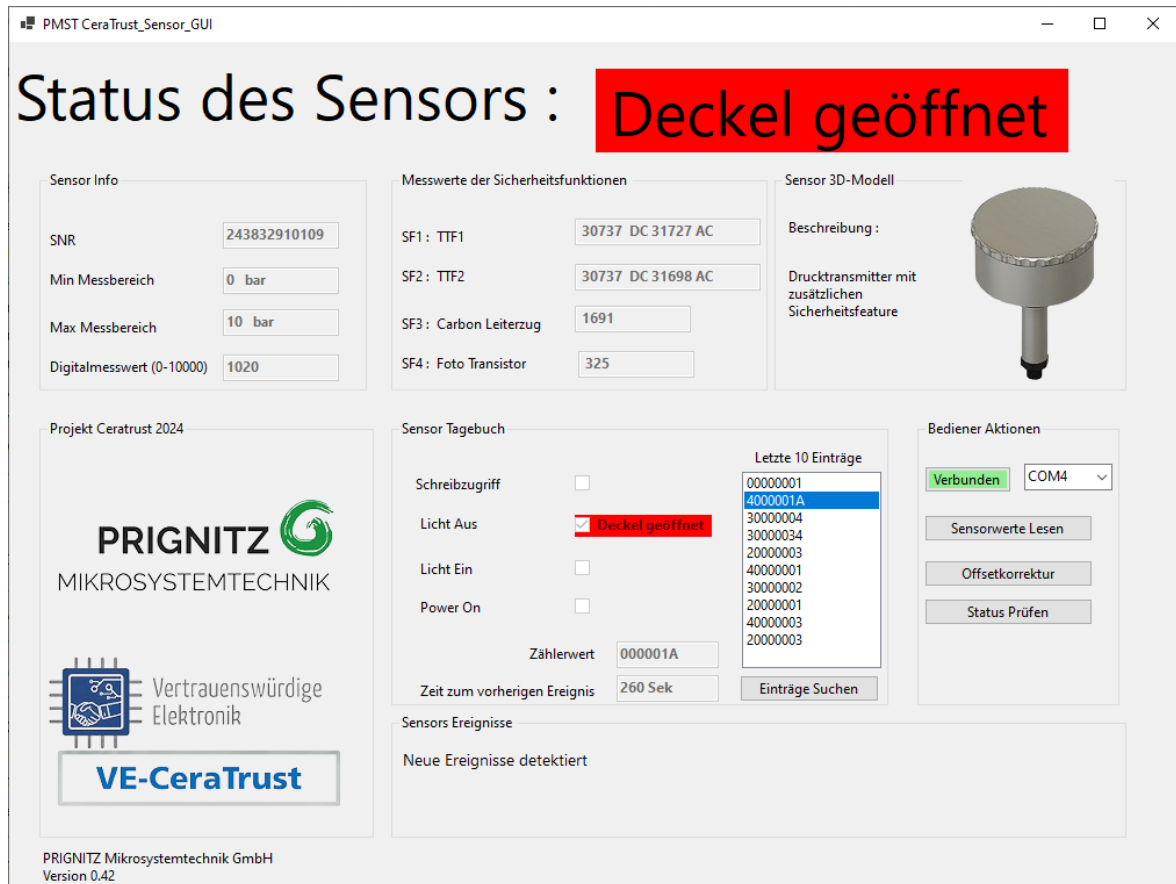


Abbildung 10 Screenshot des PC-Programms zur Sensorüberwachung

Im oberen Teil des Sensors ist in einem Feldgehäuse die Anschlussleiterplatte untergebracht. Diese ermöglicht dem Kunden den Sensor über einen Klemmblock mit seiner Automatisierungslösung zu verbinden. Neben dieser offensichtlichen Funktion werden hier aber auch zwei Sicherheitsebenen und zwei Identifikationsfunktionen realisiert.

Die erste Sicherheitsebene ist das Öffnen des Deckels des Feldgehäuses. Über einen Fototransistor wird überwacht, dass der Deckel geschlossen ist. Ist das nicht der Fall, erhöht der Prozessor das Ausgangssignal des Transmitters über 20 mA. Das kann von der Automatisierungslösung als Fehler ausgewertet werden.

Die zweite Sicherheitsebene ist die Überwachung der Leiterplatte selbst. Wird versucht die Leiterplatte zu demontieren, wird ein Selbstzerstörungsmechanismus in Gang gesetzt. Das funktioniert auch, wenn der Sensor von der Stromversorgung getrennt ist. Dafür ist eine separate Batterie implementiert worden. Zur Unterbringung der Batterien musste das Feldgehäuse vergrößert werden. Für den Demonstrator war 3-D-Druck die Technologie der Wahl, um die entsprechenden Muster herzustellen. Für Kundenprojekte soll das Feldgehäuse wieder in Edelstahl ausgeführt werden. Die Selbstzerstörungsfunktion wird über ein keramisches Heizelement, das vom Partner Fraunhofer IKTS entwickelt und gefertigt wurde, realisiert. Es ist durch den Partner Andus in die Anschlussleiterplatte einlaminiert worden, so dass es äußerlich nicht

sichtbar ist. Für den Demonstrator wurde eine „Zerstörung“ gesucht, die leicht reversibel ist, um eine mehrfache Vorführung zu ermöglichen. Die Lösung besteht hier in einer Lötbrücke die durch das Heizelement aufgeschmolzen wird.

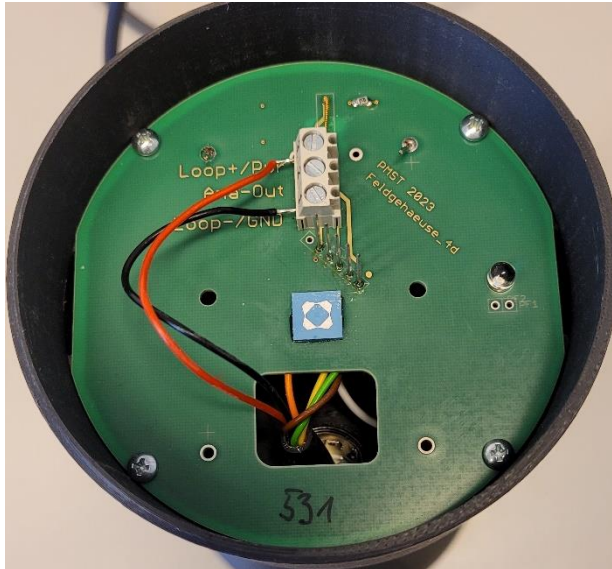


Abbildung 11 Anschlussleiterplatte mit Sicherheitsfunktionen

wurde.

Abbildung 11 zeigt die Anschlussleiterplatte mit den beschriebenen Funktionen. Im rechten Teil der Leiterplatte ist der Fototransistor zu sehen, der für die Erkennung der Deckelöffnung zuständig ist. Oberhalb des Klemmblocks, über den der Kunde den Transmitter anklemmt, ist die beschriebene Lötbrücke zu sehen. In der Mitte findet man das Identifikationselement. Dieses Element beinhaltet eine Chipless-RFID Funktion, die vom Partner IMST entwickelt und beim Partner VIA prozessiert wurde. Im Zentrum dieses Keramikelements ist ein Datamatrixcode eingepägt, der mit einer Technologie der Partner KMS und VIA umgesetzt

1.7 AP8. Fertigungslinie der Zukunft

Die Produktion von vertrauenswürdigen Transmittern setzt voraus, dass nachvollziehbar ist, welche Bauteile mit welcher Herkunft und Charge verbaut worden sind. Das war bisher im Unternehmen nur in wenigen Ausnahmefällen erforderlich und wurde dann händisch anhand der Fertigungsunterlagen nachvollzogen.

Die Fertigungslinie der Zukunft wird sich durch weitgehende Automatisierung der Produktionsprozesse, aber vor allem auch durch die Digitalisierung der Informationsprozesse auszeichnen. Dazu sind im Rahmen des Projektes verschiedene Vorarbeiten durchgeführt worden. U.a. sind verschiedene Varianten der Kennzeichnung von Produkten und Halbfertigerzeugnissen in der Produktion untersucht worden. Im Ergebnis entstand ein Konzept, das die Verknüpfung von Fertigungsaufträgen, Arbeitsschritten und abzulegenden Informationen berücksichtigte.

Schritt	Bezug	Information	abzulegendes Dokument
Wareneingang je Artikelnummer		Zeitstempel Lieferant Charge	Lieferschein Prüfzeugnisse
Wareneingangsprüfung		Zeitstempel Art der Prüfung Ergebnis Prüfer	Dokument
Kommissionierung je FA		Datum Kommissionierer Stückliste mit Info zu Lieferant und Charge Stahl Info zu Leiterplattencharge weitere Infos zu Ausgangsmaterialchargen?	
Beschriften Druckaufnehmer Bestücken Werkstückträger mit definierter SN Reihenfolge		Zeitstempel Werker Maschinennummer Parametersatz Seriennummernbereich? Ggf schon mit FA definiert? Nummer Werkstückträger?	
Tempern 1	Bezug FA	Zeitstempel Werker Position im Ofen	Logdatei des Ofens
Siebdrucken	Bezug FA	Zeitstempel Werker Maschinennummer Parametersatz Schablonennummer Pastentyp, Charge, Status	(Status heißt F
Anglasen1	Bezug FA	Zeitstempel Werker Position im Ofen	Logdatei des Ofens

Abbildung 12 zeigt einen Ausschnitt aus einem dieser Dokumente.

Um den Fertigungsauftrag informationstechnisch durch die Produktion zu begleiten und die Traceability zu gewährleisten, wurde ein so genannter Tracer entwickelt. Dazu wurden in der Produktion Terminals mit Handscannern installiert, die es gestatten, einen Fertigungsauftrag digital zu erfassen und dadurch zu verfolgen, sowie seinen Durchlauf durch die Fertigung einschließlich der beteiligten Mitarbeiter zu dokumentieren.

Abbildung 12 Ausschnitt aus einem Planungsdokument zur Fabrik der Zukunft

Dieses System wird in Zukunft flächendeckend in der Produktion eingeführt werden. Bild 13 zeigt einen Screenshot des Tracers. Damit ist der Fertigungsablauf be-

PMST Tracer - Legacy 5.3.8
FA: 231011417 | ArtikelNr: 94068034 | Kunde: Gefran Deutschland GmbH

Fertigungsauftrag: 231011417
Produktinformationen
Auftrag: 231202342
Kundenauftragsnummer: 3237702332
ArtikelNr: 94068034
Kunde: Deutschland GmbH
Beschreibung: Drucktransmitter SPT-H2-UR (-L...*)bar
Losgröße: 38

Zeitstempel	Bereich	Arbeitsplatz	Zusatzinformation	Produktionsmitarbeiter	Status	Anmerkung	Verantwortlich
08.01.2024 09:53:24	Endmontage	Eingangsregal			Auftrag wird bearbeitet		
08.01.2024 09:53:23	Kalibrierung	Eingangsregal			Bearbeitung ist abgesch		
12.12.2023 07:34:40	Kalibrierung	Eingangsregal			Auftrag wird bearbeitet		
12.12.2023 07:34:38	Lager	Regal Material fehlt			Bearbeitung ist abgesch		
07.12.2023 11:44:38	Lager	Regal Material fehlt			Material fehlt	70010000	
07.12.2023 09:26:04	Kalibrierung	Eingangsregal			Auftrag wird bearbeitet		
07.12.2023 09:26:03	Alterungsprozesse	Thermische Voralterung			Bearbeitung ist abgesch		
06.12.2023 14:06:21	Alterungsprozesse	Thermische Voralterung			Auftrag wird bearbeitet		
06.12.2023 14:06:20	Vormontage	Eingangsregal			Bearbeitung ist abgesch		
04.12.2023 13:09:40	Vormontage	Eingangsregal			Auftrag wird bearbeitet		
04.12.2023 13:09:38	Label	FOBA Laser			Bearbeitung ist abgesch		
01.12.2023 12:36:11	Label	FOBA Laser			Auftrag wird bearbeitet		
01.12.2023 12:36:10	Produktionsvorbereit	Materialbereitstellung			Bearbeitung ist abgesch		
30.11.2023 14:42:47	Produktionsvorbereit	Materialbereitstellung			Auftrag wird bearbeitet		

Abbildung 13 Durchlauf eines Fertigungsauftrages auf dem Bildschirm des Tracers

reits gut dokumentiert. An der weiteren Verbesserung wird gearbeitet.

Neben den Informationen aus dem Tracer und den Chargeninformationen für die verwendeten Materialien sind weitere Messdaten aus der Zellenproduktion, der Kalibrierung und der Endprüfung zu erfassen.

Die entsprechenden Informationen müssen mit dem Erzeugnis und dem entsprechenden Fertigungsauftrag sowie der aktuellen Fertigungsposition und den ausführenden Mitarbeitern verknüpft werden.

Das Konzept sieht vor, mit Beginn der Zellenfertigung eine Zellennummer zu vergeben. Diese wird kombiniert als Datamatrixcode und in Klarschrift auf eine Sechskantfläche der Zelle aufgebracht und gelesen, wenn Messungen an der Zelle oder am mit dieser Zelle aufgebauten Transmitter durchgeführt werden. Damit ist sichergestellt, dass Messungen immer dem richtigen Objekt zugeordnet werden. Die letzte derartige Messung ist der „End of Linie Test“ (EOL). Hat ein Transmitter diesen Abnahmetest bestanden, wird er in Zukunft in der Datenbank zum Labeln freigeschaltet. Geplant ist auch, den Laserbeschrifteter mit einem Codereader auszustatten, so dass nur Transmitter gelabelt werden und eine Seriennummer erhalten, die den EOL bestanden haben. Mit der zunehmenden Automatisierung der Arbeitsplätze, werden alle an-

fallenden Daten zum Prozess dann sofort in den Tracer übertragen, so dass vom Operator keinerlei weiteren losbezogenen Aktionen nötig sind. Selbstredend werden Prozessstart und -ende sowie der Operatorcode erfasst. Mit diesen Daten kann die Produktion noch kleinteiliger ausgewertet werden. Die automatisierten Systeme sind so angelegt, dass nur eingewiesene Operatoren die Arbeitsgänge durchführen können. Dies wird über personenbezogene Codekarten realisiert. Dazu verwalten die Arbeitsplätze eine Liste zugelassener Operatoren.

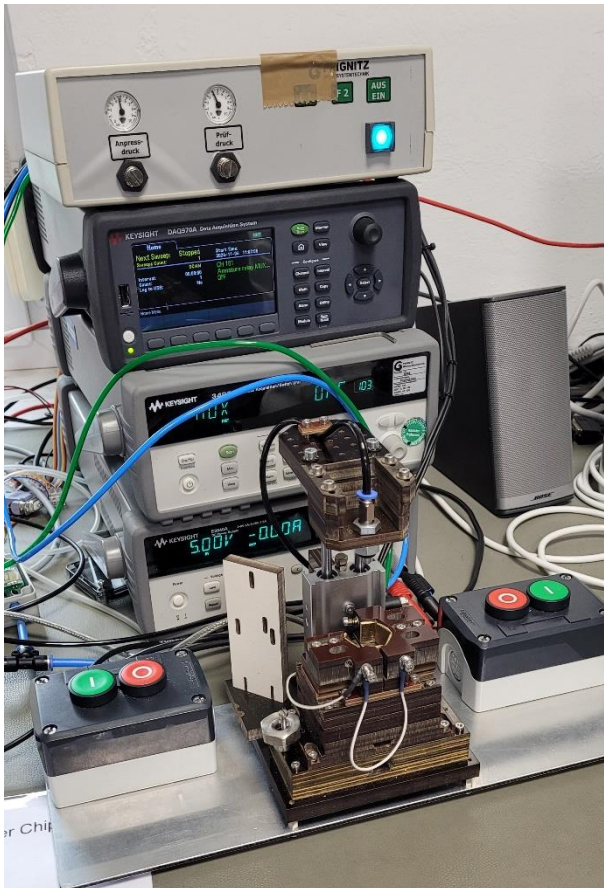


Abbildung 14 Prototyp Zellenprüfstand

worden. Die zu prüfende Zelle wird eingelegt. Der Vorgang startet nach Zweihandbedienung. Der Druckanschluss fährt nach unten und kontaktiert die Zelle. Das Messprogramm beginnt.

Ein ähnlicher Aufbau soll am EOL eingesetzt werden.

Abbildung 14 zeigt den aktuellen Stand des Prototypen für eine Messvorrichtung, mit der die Zellenparameter aufgenommen und in einer Datenbank abgelegt werden können. Die Aufnahme für den 2D Barcodeleser ist bereits vorhanden. Er wird es gestatten, automatisch die Zellennummer zu erfassen und damit die Gewinnung der Daten und ihre Zuordnung zu genau einer Messzelle zu automatisieren. Entsprechende Versuche sind bereits durchgeführt

Die Fragen der Identifikation und der Einsatz der entsprechenden Codereader wurden gemeinsam mit dem Partner KMS bearbeitet. Verschiedene Hersteller, verschiedene Konfigurationen und Beleuchtungen wurden gemeinsam getestet.

1.8 AP9. Zertifizierungsstrategie

In der nachfolgenden Tabelle haben die Projektpartner mögliche Angriffsszenarien zusammengestellt und ihre Auswirkungen bewertet. In Anlehnung an die Vorgehensweise bei der FMEA entstand die Risikobewertung anhand der drei Faktoren: mögliche Folgen des Angriffs, Wahrscheinlichkeit des Angriffs und Entdeckungswahrscheinlichkeit des Angriffs.

Die in diesem Projekt entwickelten Maßnahmen führen zu einer signifikanten Verringerung dieser Risiken. Damit konnte für jede Maßnahme ein Sicherheitslevel bestimmt werden.

Es ist möglich, wie im Demonstrator praktiziert, die einzelnen Schutzmaßnahmen zu kombinieren. Dabei ist mit dem Kunden zu bewerten, gegen welche Art des Angriffs ein Schutz aufgebaut werden muss und ob beim Angriff Aktivitäten ausgelöst werden sollen.

Katalog Sicherheitselemente														VE-CeraTrust	
Projekt: VE-CeraTrust		Index:34		Datum der Ersterstellung: 18.11.2023				Datum der letzten Änderung: 24.07.2024							
Nr.	Typ, Integrationslevel	Sicherheitsmaßnahme	Prüfverfahren	möglicher Angriff	Bewertung des Angriffsriskos					Bewertung der Sicherheitsmaßnahmen					
					mögliche Folgen des Angriffs (Bedeutung)	Auftritts-wahrscheinlichkeit Angriff	Entdeckungs-wahrscheinlichkeit	Risiko ohne weitere Maßnahmen	Entdeckungs-wahrscheinlichkeit	M	Umkehrbarkeit	II	Faktor der Risiko-reduzierung	Sicherheitslevel	Risiko nach eingetragener Maßnahme
					1...sehr geringe Beeinträchtigung	1...Angriff sehr unwahrscheinlich	1...Angriff wird entdeckt	6 bis 60 sehr geringes Risiko	1...Merkmal wird nicht entdeckt	1...Maßnahme kann nicht umgangen werden	0,01 bis 0,04 erhebliche Risikoreduktion durch Maßnahme	25 bis 100 sehr hohes Sicherheitslevel der Maßnahme	6 bis 60 sehr geringes Risiko		
					E...Beeinträchtigung Funktion & Sicherheit	E...gelegentlich auftretende Angriffe	E...Angriff wird wahrscheinlich über einen gewissen Zeitraum entdeckt	>60 bis <100 mittleres Risiko	E...Merkmal wird wahrscheinlich nach einem gewissen Zeitraum entdeckt	E...Maßnahme kann nur mit Aufwand umgangen werden	+0,04 bis +0,2 mittlere Risikoreduktion	6 bis 24 mittleres Sicherheitslevel	>60 bis <100 mittleres Risiko		
					10...Ausfall	10...häufig auftretende Angriffe	10...Angriff wird mit hoher Wahrscheinlichkeit nicht entdeckt	>100 sehr hohes Risiko	10...Merkmal wird sicher entdeckt	10...Maßnahme ist wirkungslos	+0,2 sehr geringe Risikoreduktion	1 bis 5 geringes Sicherheitslevel	>100 sehr hohes Risiko		
1	x x	C-ID	DC-Messung (Microprozessor)	Austausch einzelner Bauteile o. Komponenten	falsche Messwerte, Ausfall Baugruppe oder System	6 relativ häufig	6 elektrische Messung	2	72	Merkmal ist nur im 3D Röntgen entdeckbar.	2 elektrischer Leiter ist leicht zu überbrücken	7	0,14	7	10
2	x x	Abfrage kundenspez. Temperatursensor	AC-Messung (Microprozessor)	Austausch einzelner Bauteile o. Komponenten	falsche Messwerte, Ausfall Baugruppe oder System	6 relativ häufig	6 elektrische Messung	2	72	Merkmal ist durch Signalanalyse entdeckbar	2 Filterfrequenz nachzubilden setzt Know-how voraus und ist nicht leicht erkennbar	2	0,04	26	3
3	x x	Fingerprint Prägen LTC	Oberflächenprofil über AOI	Austausch einzelner Bauteile o. Komponenten	falsche Messwerte, Ausfall Baugruppe oder System	6 relativ häufig	6 optische Messung vor Ort oder nach Rücklauf intern	3	100	Merkmal kann gut getamt werden	3 Imitation nach Analyse der Komponenten	2	0,06	17	6
4	x x x	Fingerprint chem. Komponente	- RFA (XRF) - UV	Reverse Engineering	Plagiate	6 gelegentlich	5 Messung vor Ort oder nach Rücklauf intern	5	150	Merkmal kann sehr gut getamt werden	4 Imitation nach Analyse der Komponenten	4	0,08	18	12
5	x x	Versteckte RLC-Netzwerke	AC/DC-Messung	Reverse Engineering	Plagiate	6 gelegentlich	5 elektrische Messung	5	150	Merkmale können versteckt werden	5 Analyse und Imitation	5	0,25	4	38
6	x x	Chipless RFID	RF-Abfrage	Reverse Engineering	Plagiate	6 gelegentlich	5 RF-Messung	4	120	RFID Tags können versteckt werden	4 genaue Einordnung kundenspezifisch	3	0,12	8	14
7	x x	Elektromagnetische Schirmung Kabel und Board	Signalauswertung (Kabel)	Angriff von außen	Ausfall Baugruppe oder System, Abhören von Daten, Systembeeinträchtigung von außen	6 gelegentlich	5 elektrische Messung (nur bei Ausfall)	2	60	Schirmung ist offensichtlich	9 Schirmung umgehen	3	0,27	4	16
8	x x	Zerstörung (Heizerstruktur)	Zerstörung bei Sicherheitsrisiko	Reverse Engineering	Plagiate	6 gelegentlich	5 elektrische Messung	4	120	Merkmal ist nach Auslösung sichtbar	10 Wirkung von Beschädigung und Verfügbarkeit des zerstörten Bauelementes abhängig	3	0,3	5	36
9	x x x	Fingerprint - Zufallsmuster (z.B. Glasfaser, Bearbeitungsspuren, Membranoberfläche)	AOI, Mikroskop -Software	Reverse Engineering	Plagiate	6 gelegentlich	5 optische Messung oder nach Rücklauf	2	60	Merkmal ist offen sichtbar	5 optische Inspektion/ Bilderkennung	3	0,15	7	9
10	x x	Keramik als Bohrschutz- bzw. Knickschutzdektion	Röntgen-Mikroskopie, Ultraschall-Mikroskopie, optische Inspektion	mechan. Bohren, Reverse Engineering	Reverse Engineering, IP-Verlust	6 relativ häufig	6 Produktanalyse, Plagiate	5	180	Merkmale sind relativ leicht zu entdecken	10 Merkmal kann umgangen werden	5	0,5	2	90
11	x x	Seebeck-ID	DC-Messung (Microprozessor)	Reverse Engineering	Plagiate	6 gelegentlich	5 elektrische Messung	2	60	Merkmal ist nur im 3D Röntgen entdeckbar	2 Funktion kann evtl. übergangen werden	5	0,1	10	6

Abbildung 15 Bewertungsmatrix und Schutzgrad

Wenn weitere Schutzmaßnahmen entwickelt werden, können sie schon im Ideenstadium nach dieser Matrix bewertet und zertifiziert werden. Das ermöglicht es gezielt nach Schutzelementen bzw. Lösungen zu suchen, die hohe Schutzgrade versprechen.

2. Wichtigste Positionen des zahlenmäßigen Nachweises

Die im Antrag kalkulierten Materialkosten wurden nicht ausgeschöpft. Die Ursachen dafür sind, dass die kalkulierten Iterationen bei der Herstellung der Demonstratoren nicht in dem Umfang notwendig waren, moderne Rapidprototypingtechnologien eingesetzt wurden und Teile des Materials durch die PMST ohne Anrechnung auf das Projekt zur Verfügung gestellt wurden. Die Iterationen fanden im Wesentlichen auf der Baugruppenebene statt. Damit konnten auch hier Kosten im Vergleich zum Aufbau kompletter Demonstratoren gespart werden. Durch den Verzicht auf geplante Stahlteile und ihren Ersatz durch 3-D-Druckteile aus Kunststoff, konnten Kosten reduziert und eine höhere Flexibilität erreicht werden.

Auch die Reisekosten wurden nicht ausgeschöpft. Messebesuche fanden u.a. auf Grund der Pandemie nur in geringerem Umfang statt. Wenn sie durchgeführt wurden, wurden Eintrittskartengutscheine von Kunden oder Lieferanten genutzt. Übernachtungen wurden vermieden.

Die Überziehung der kalkulierten Personalkosten resultiert im Wesentlichen aus der kostenneutralen Verlängerung des Projektes. Die in der Begründung des Antrages auf kostenneutrale Verlängerung aufgeführten Energieversorgungsthemen benötigten entsprechende Arbeitszeit und auch die oben beschriebenen Prototypen für die Fabrik der Zukunft waren in dieser Phase nochmal sehr arbeitsintensiv.

In Summe konnte das Projekt innerhalb des kalkulierten Kostenrahmens umgesetzt werden.

3. Verwertung der Ergebnisse und fortgeschriebener Verwertungsplan

Prignitz Mikrosystemtechnik hat begonnen, die im Projekt untersuchten Identifikationsmaßnahmen in Teilen des Portfolios umzusetzen. Das betrifft zunächst alle Produkte, die auf der im Hause PMST gefertigten Zelle beruhen. Perspektivisch ist geplant auch Zukaufteile miteinzubeziehen. Erste Pilotlösungen zur Erfassung und Verfolgung unserer Produkte und derer Daten in der Produktion wurden umgesetzt. Die Identifikation und das Tracing unserer Produkte in der Produktion wird in den nächsten zwei Jahren vervollkommen. Ziel ist es, zu jedem Zeitpunkt über alle erforderlichen Informationen über die eingesetzten Grundmaterialien und Zulieferteile, ihre Lieferanten und Chargen zu verfügen.

Wir bieten unseren Kunden gerade auch im Bereich der kritischen Infrastruktur die Einführung der im Projekt erarbeiteten Sicherheitsmaßnahmen an. Die Reaktionen

sind derzeit noch verhalten. Da die Sensoren üblicherweise in Stationen eingesetzt werden, denkt man dort eher nicht über die Sicherheit eines einzelnen Sensors nach. Die Sicherheit der Station steht im Focus. Ob wir mit unseren Lösungen hier einen Beitrag leisten können, wird noch zu diskutieren sein.

Im Projekt ist eine Reihe von Ideen entwickelt worden, die im Rahmen dieses Projektes nicht umgesetzt werden konnten. Ein Beispiel ist der Doppel-T-Filter. Dieses oder ähnliche Bauelemente und die Technologie zu ihrer Herstellung zu entwickeln, könnte in einem entsprechenden Konsortium umgesetzt werden.

4. Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Es gibt eine Reihe von Veröffentlichungen, die sich auf sichere Elektronik beziehen. Diese beziehen sich meist auf Halbleiterbauelement selbst, ihre Beschaffung aus sicheren Quellen und ihre Identifikation als Originalbauelemente. Traceability spielt hier eine wichtige Rolle.

Veröffentlichungen, die die Sicherung von Baugruppen unter Einbeziehung keramischer Sicherheitselemente oder auch die Anwendung von PUF in ähnlicher Weise beschreiben, wie sie in unserem Projekt umgesetzt wurden, sind uns nicht bekannt.

5. Veröffentlichungen der Ergebnisse

Die im Projekt erfolgten Veröffentlichungen sind in der Übersicht Abbildung 16 dargestellt. Neben der standardmäßigen Präsentation auf der Website wurden die Öffentlichkeit auf verschiedenen Fachtagungen und Messen informiert. Die Beteiligung der Projektpartner wechselte mit der Thematik der Veranstaltungen. Die Prignitz Mikrosystemtechnik beteiligte sich vor allem im Bereich der Vorstellung des Demonstratorkonzeptes. Dazu waren wir an der Präsentation zum Tag der vertrauenswürdigen Elektronik 2024 und der Fachtagung Sensoren und Messsysteme 2024 beteiligt. Letztere fand anlässlich der Sensor und Test in Nürnberg statt. Diese Messe ist für uns als Sensorhersteller besonders wichtig.

#	Autoren	Firma	Date	Titel / Detail	Kategorie (Bezug zu VE-CeraTrust)	Institution/ Firma	Konferenz / Messe	Ort	Link
1	Peter Uhlig, Uwe Krieger, Franz Bechtold, Stefan Körner, Christian Lenz	IMST, VIA, IKTS	22.10.2021	„VE-CeraTrust“ –Verhinderung von Angriffen auf Elektroniksysteme durch neuartige keramische Mehrlagensysteme	Projektübersicht, Lösungsansätze	IMAPS de	IMAPS Herbstkonferenz 2021	München	https://imaps.de/
2	L. Krieger / Z. Uhlig / J. Lenz		09. – 10.03.2021	öffentlicher Workshop: 1. Pitch - 09.03.2021 - VE-CeraTrust: U. Krieger 2. 10.03.: Workshop - Fertigung: P. Uhlig 3. 10.03.: Workshop - Analyse: C. Lenz		BMBF	ZEUS - öffentlicher Workshop		https://www.elektronikforschung.de/vertrauenswuerdige/it/konferenz
3	VE-CeraTrust	alle	02.12.2021	Austausch mit VE-FIDES gestartet 02.12.2021, gemeinsame Interessen hinsichtlich Identifikation, weiterer Austausch im Vorfeld des öffentlichen Workshops vereinbart	Austausch mit Herrn Schneider (SIEMENS, München)	SIEMENS	VE-FIDES	online/Berlin	https://elektronikforschung.de/projekt/ve-fides
4	Uwe Krieger, Franz Bechtold, Christoph Lehnberger, Christian Lenz, Peter Uhlig	VIA; IKTS; ANDUS; IMST	14. – 15.06.2022	Vertrauenswürdige Elektronik – Keramikmodule und Baugruppen gegen Fälschung und Manipulation sichern	Projektübersicht, Lösungsansätze	EBL	EBL 2022	Fellbach	https://www.dvs-home.de/events/dgetail/ebel2022
5	Uwe Krieger, Franz Bechtold, Thomas Herbst, Gunter Hagen	VIA, KMS	13. – 15.07.2022	Individual Surface Profiles in LTCC-based Ceramic Substrates for Identification of Trustworthy Electronics		IMAPS	CICMT	Wien	https://imapseurop.e.org/event/cicmt-2022/
6	Uwe Krieger und Harald Klaubert	VIA	25. – 30.09.2022	Präsentation am VIA-Messestand			European Micro Wave Week 2022	Milano, Italy	
7	Uwe Krieger und Annett Schroeter	VIA	20. – 21.10.2022	Präsentation über Table Top-Ausstellung		IMAPS de	IMAPS Herbstkonferenz 2022	München	
8	Uwe Krieger, Annett Schroeter, Franz Bechtold, Gunter Hagen, Adrian Goldberg	VIA, KMS, IKTS	11. – 14.09.2023	LTCC-based Ceramic Substrates for Identification of Trustworthy Electronics			EMPC 2023	Cambridge	https://empc2023.org/
9	Annett Schroeter, Uwe Krieger, Christoph Lehnberger, Peter Uhlig, Adrian Goldberg	VIA, ANDUS, IMST, IKTS	25.10.2023	Integration of LTCC into Printed Circuit Boards	Projektübersicht, Lösungsansätze	VDE e. V.	MST Kongress 2023	Dresden	https://www.mikrosystemtechnik-kongress.de/de/nachrichten/bericht-2023
10	Uwe Krieger, Annett Schroeter, Peter Uhlig, Christoph Lehnberger, Hartmut Stoltenberg, Gunter Hagen, Adrian Goldberg, Steffen Ziesche	VIA, KMS, ANDUS, IMST, PMST, IKTS	04. – 05.06.2024	Verhinderung von Angriffen auf Elektroniksysteme durch neuartige keramische Mehrlagensysteme	Projektübersicht, Lösungsansätze		Tage der vertrauenswürdigen Elektronik 2024	München	
11	Annett Schroeter, Uwe Krieger, Gunter Hagen, Christoph Lehnberger, Peter Uhlig, Hartmut Stoltenberg, Adrian Goldberg	VIA, KMS, ANDUS, IMST, PMST, IKTS	12.06.2024	Auswahl geeigneter Sicherheitselemente aus LTCC für eine vertrauenswürdige Elektronik	Projektübersicht, Lösungsansätze	AMA Service GmbH	Fachtagung Sensoren und Messsysteme 2024	Nürnberg	https://www.ama-science.org/process/links/details/4955
12	Enrico Tollin, Achim Bahr, Andreas Wien und Peter Uhlig	IMST GmbH	11. – 13.06.2024	LTCC Back-scattered Polarization Duplexing Chipless RFID for Nearfield Interrogation		IMAPS Nordic	NordPac 2024	Tampere, Finnland	DOI: 10.23919/NordPac1094.2024.10582265

Abbildung 16 Übersicht über die im Projekt erfolgten Veröffentlichungen