Vertrauenswürdigkeit sicherheitskritischer elektronischer Komponenten in einer global verflochtenen Liefer- und Wertschöpfungskette

Dirk KOSTER [1], Udo NETZELMANN [1], Steven QUIRIN [1], Jan OSWALD [1], Christian JUNGMANN [1], Rainer RICK [1], Philipp STOPP [1], Nico BROSTA [1], Horst GIESER [2], Nico KOVAC [2], Leo MEIXNER [2], Frank ALTMANN [3], Sebastian BRAND [3]

[1] Fraunhofer-Institut für Zerstörungsfreie Prüfverfahren IZFP, Saarbrücken

[2] Fraunhofer-Einrichtung für Mikrosysteme und Festkörper-Technologien EMFT, München

[3] Fraunhofer-Institut für Mikrostruktur von Werkstoffen und Systemen IMWS, Halle (Saale)

Kontakt E-Mail: dirk.koster@izfp.fraunhofer.de

Kurzfassung. Die Mikroelektronik ist zu einem unverzichtbaren Bestandteil unseres Lebens geworden und eine Schlüsseltechnologie der fortschreitenden Digitalisierung und Vernetzung unserer Gesellschaft. Der rasant zunehmende Einsatz von Elektroniksystemen in kritischen Infrastrukturen, für Industrie 4.0 oder Anwendungen im Internet of Things (IoT), der Kommunikationstechnik, im Automobilbereich oder bei medizinischen Geräten erhöht das Risiko für digitale Angriffe mit hohem Schadpotential. Zusätzlich ist durch die Globalisierung der Herstellerketten für elektronische Systeme die Gefahr von Fälschungs- und Manipulationsversuchen gewachsen. Als Hardware-Trojaner wird die Manipulation in der Verschaltung von Elektronikkomponenten bezeichnet, um unerlaubten und versteckten Zugriff z. B. auf persönliche Daten und Firmengeheimnisse zu erhalten oder Kontrolle über Produktionsprozesse oder sicherheitsrelevante Infrastruktur zu erlangen. Die Manipulation kann dabei an unterschiedlichen Stellen der Wertschöpfung erfolgen und lange Zeit unbemerkt bleiben. Neben der Implementierung in der Entwicklungsphase von mikroelektronischen Schaltkreisen können Hardware-Trojaner auch unbemerkt innerhalb der Chip- oder Baugruppenfertigung eingesetzt werden. Ein weiterer Angriffspunkt ist der Transport, bei dem gefälschte oder manipulierte Bauelemente eingeschleust werden können. Daher ist die Gewährleistung der Vertrauenswürdigkeit auf Ebene der integrierten Schaltkreise, der Bauelemente und Elektroniksysteme durch geeignete Prüfmethoden zum Nachweis von Hardware-Trojanern von zunehmender Bedeutung.

Im Rahmen des Fraunhofer-internen Projektes „Trusted resource aware ICT – TRAICT“ wurden verschiedene Angriffsszenarien analysiert und mögliche Detektionsmechanismen identifiziert. Mit den gewonnenen Erkenntnissen wurden danach Hardware-Trojaner-Ansätze in eine Demonstrator-Baugruppe implementiert. In diesem Beitrag werden die erzielten Ergebnisse besprochen, die jeweiligen Nachweisempfindlichkeiten und Einsatzgrenzen für die Hardware-Trojaner-Detektion diskutiert und ein erstes multimodales Prüfkonzept vorgestellt.

1. Einführung

1.1 Globaler Kontext und die Notwendigkeit für vertrauenswürdige Mikroelektronik

Das weltweite Bestreben nach Digitalisierung im zivilen und industriellen Umfeld, sowie der Wunsch einer vernetzten Welt, sorgen für einen globalen Anstieg des Bedarfs an elektronischen Bauteilen. Lösungen für aktuelle Megatrends wie z. B. Smart Mobility/City sowie IoT und 5G/6G sind hierbei starke Technologietreiber. Durch den vermehrten Einsatz von mikroelektronischen Bauelementen und deren abzusichernden Datenverkehr zu übergeordneten Cloudsystemen steigt jedoch der weltweite Energieverbrauch signifikant. Um dieser Entwicklung entgegenzuwirken kann die Entscheidungsfindung von der Cloudebene in Richtung des Endgeräts verlagert werden (Edge Computing) [1]. Die Konsequenz ist der Einsatz leistungsstarker mikroelektronischer Schaltungen in den unterschiedlichsten Bereichen des täglichen Lebens. Dadurch eröffnen sich aber auch vielfältige Möglichkeiten von Schadangriffen. Grundsätzlich können mit Schadangriffen unterschiedliche Ziele wie z. B. das Ausspähen von persönlichen Daten oder Firmengeheimnissen, Manipulation oder Löschen von Dateien oder das Sabotieren von Produktionsprozessen und sicherheitsrelevanter Infrastruktur verfolgt werden. Neben den seit vielen Jahren etablierten Software-Technologien wie z. B. dem Computervirus, Trojanischen Pferd oder Computerwurm wird der Einsatz von sogenannten Hardware-Trojanern (HT) immer relevanter. Als HT wird die Manipulation an Hard- oder Firmware von integrierten Schaltungen und Elektronikmodulen bezeichnet. Die Manipulation kann dabei an unterschiedlichen Stellen der Wertschöpfung erfolgen und lange Zeit unbemerkt bleiben [2]. Neben der Implementierung in der Entwicklungsphase von mikroelektronischen Schaltkreisen können HT auch unbemerkt innerhalb der Chip- oder Baugruppenfertigung eingesetzt werden. Ein weiterer Angriffspunkt ist der Transport der elektronischen Komponenten. Field Programmable Gate Array (FPGA) Bausteine bieten hierbei besondere Angriffsmöglichkeiten durch die Manipulation des Programmiervorgangs [3]. Die potentielle Angriffsgefahr wird durch die weltweit verflochtenen Liefer- und Wertschöpfungsketten verschärft. Stehen Produkte aus dem Consumer-Bereich – mit Ausnahme von Kommunikationsgeräten wie Handy, Router etc. [4] – bisher weniger im Fokus, so müssen Bauteile in sicherheitsrelevanten Bereichen wie z. B. Kraftwerken, Internet-Knoten oder Kommunikationssystemen in nachrichtendienstlichen Behörden und der Verteidigung verlässlich und vertrauenswürdig sein. Sensorsysteme der zerstörungsfreien Prüfung und Analyse können einen wichtigen Beitrag zur Detektion von HT leisten und so die Sicherstellung der Vertrauenswürdigkeit von elektronischen Systemen gewährleisten [5].

1.2 Stand der Technik zur Hardware-Trojaner-Detektion

Mikroelektronische Schaltungen und Baugruppen können auf Vorhandensein von HT untersucht werden. Zur Klassifizierung der Modifikationen kann die Charakterisierung der physikalischen Implementierung, die Art der Aktivierung sowie die Handlung während der aktiven Phase des HT herangezogen werden [6]. Zur Detektion können verschiedene zerstörende und zerstörungsfreie Analyseverfahren angewendet werden. Die Mechanismen zur Detektion unterschiedlicher Typen von HT unterscheiden sich deutlich. Jedes Analyseverfahren hat deshalb Vor- und Nachteile und ist nur für spezielle HT unter bestimmten Randbedingungen geeignet [2]. Die strukturelle Analyse zur Detektion von manipulierten Schaltungsteilen auf Chipebene kann unter Zuhilfenahme von schrittweisem Delayern und mikroskopischen Abbildungsverfahren (scanning optical microscopy (SOM), scanning electron microscopy (SEM) u. a.) bis in den Bereich von wenigen Nanometern

erfolgen [6]. Mit hochauflösender scanning acoustic microscopy (SAM) [7] und IR-Abbildung können größere Strukturen und Blöcke zerstörungsfrei abgebildet werden. Funktionale Tests nutzen z. B. definierte Testpattern an den Eingangspins, welche durch den Vergleich der Ausgangssignale auf Produktionsfehler oder HT hinweisen können. Ähnliche Analysefähigkeiten versprechen integrierte Testschaltungen, sogenannte Built-in self-tests (BIST). Seitenkanalanalysen sind in der Lage verschiedene Signale, die durch die elektrische Aktivität in den elektronischen Schaltungen verursacht werden, zu analysieren. Zu den Seitenkanalsignalen zählen elektromagnetische Abstrahlung, Timing-Informationen, Wärmeabstrahlung und Energieaufnahme [2, 6,]. Die Verwendung bildgebender Thermografie wird als vielversprechend angesehen [8, 9]. Automatische optische Inspektionssysteme (AOI) werden seit vielen Jahren zur Kontrolle von sichtbaren Qualitätsmerkmalen eingesetzt. So z. B. die Einhaltung von Fertigungstoleranzen von Leiterplatten oder die richtige Bestückung und Lötung von elektronischen Baugruppen [10]. Röntgen- und Röntgen-CT Systeme werden zur Qualitätskontrolle aber auch zur Untersuchung von Modifikationen auf unterschiedlichen Ebenen (Chip, Bauelement, Leiterplatte, Baugruppe) erfolgreich eingesetzt [11]. Zum Betrieb von Röntgeneinrichtungen sind jedoch die Vorgaben aus der Strahlenschutzverordnung einzuhalten. Zur Erhöhung der Detektionswahrscheinlichkeit verschiedener Klassen von HT wird der Kombination mehrerer Detektionsverfahren ein hohes Potential zugeschrieben. Zur vorsorglichen Abwehr von Manipulationen werden aktuell z. B. quelloffene Prozessorstrukturen wie der RISC-V verwendet. Dessen Vorteil ist der Open-Source-Charakter, der es durch Transparenz und Offenheit jedem erlaubt, Sicherheitslücken zu identifizieren und zu schließen. Eine Manipulation kann dadurch deutlich erschwert werden.

2. Ergebnisse

2.1 Zielstellung und Vorgehensweise

Die Detektion von HT ist durch die vielfältigen Varianten der Integration, sei es der Ort in der Wertschöpfungskette oder die Komplexität des Trojaners selbst, keine triviale Herausforderung. In dieser Arbeit wurden hauptsächlich Techniken eingesetzt, welche einen HT-Nachweis durch Strukturanalyse oder Analyse von Emissionssignalen aktiver Bauelemente/Baugruppen (Seitenkanalanalyse) leisten können, siehe Abbildung 2.1.

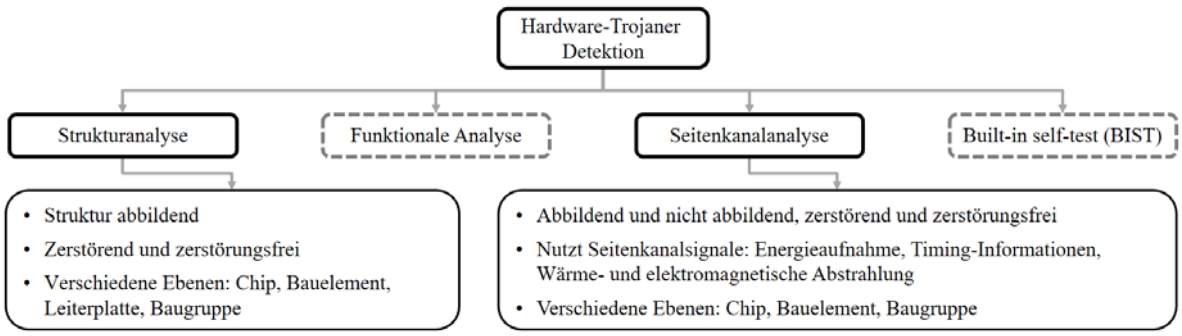

Abbildung 2.1: Verschiedene Arten der Hardware-Trojaner Detektion

In einer Versuchsreihe wurden unter Zuhilfenahme verschiedener Analysemethoden an einem kommerziell verfügbaren elektronischen Gerät (WLAN Router) erste Ergebnisse erarbeitet. Die Verwendung zweier gleicher Gerätetypen mit unterschiedlichen Versionsständen (Baugruppe-A und -B), welche sich durch Unterschiede in Layout und Bestückung auszeichneten, wurde als Grundlage für die prinzipielle Nachweisfähigkeit von potentiellen HT verwendet. Ein HT bedeutet hierbei ein zusätzliches aktives

Schaltungselement, welches Aufgaben der Datengenerierung und –übertragung übernimmt, ein passives Bauteil oder eine veränderte Leiterbahn. So kann ein HT z. B. ein zusätzliches Bauelement auf einer Baugruppe bis hin zur Veränderung einer im integrierten Schaltkreis (IC) implementierten Funktion oder eines Schlüssels sein. Die unterschiedlichen geometrischen Größenordnungen der Funktionsstrukturen auf Baugruppen-, Leiterplatten-, Bauelement- und Chipebene samt entsprechender Randbedingungen und Größenordnungen erzwingen den Einsatz verschiedener angepasster Analyseverfahren.

2.2 Strukturanalyse auf Baugruppen-, Leiterplatten-, Bauelement- und Chipebene

Um auf Baugruppenebene zusätzliche Funktionsstrukturen nachweisen zu können, müssen Analyseverfahren verwendet werden, welche mit den erschwerten Bedingungen einer unebenen Oberfläche zurechtkommen. Ein scannendes Verfahren wie die Wirbelstromprüfung kann deshalb nur partiell verwendet werden. Der Einsatz von bildgebenden Verfahren, wie z. B. die blitzlichtangeregte Thermografie und die Oberflächeninspektion mittels Laser-Profilometrie, bieten sich dadurch an. Mit der blitzlichtangeregten Thermografie kann eine komplette Baugruppe auf Veränderungen untersucht werden. Dazu wird die Baugruppe mit einem starken Lichtblitz kurzzeitig an den Oberflächen erwärmt. Eine Infrarotkamera nimmt den nachfolgenden Abkühlungsprozess als Bildsequenz auf. Ziel ist hierbei nicht die absolute Bestimmung der Temperaturen, sondern vielmehr die Extraktion zeitbezogener Größen wie Temperaturabklingraten. Üblich ist die sogenannte Puls-Phasen-Thermografie, bei der Störungen wie ungleichmäßige Beleuchtung oder lokale Unterschiede des Emissionsgrads unterdrückt werden. Abbildung 2.2 d) und e) zeigt zwei dadurch entstehende Phasenbilder zweier Baugruppen-A und -B. In dem Differenzbild f) werden die Unterschiede zwischen den Baugruppen deutlich hervorgehoben. Wichtig dabei ist, dass im Gegensatz zur Inspektion im sichtbaren Bereich der elektromagnetischen Strahlung a) und b) sowie bei der Laser-Triangulation c), durch Störung der inneren Wärmeströme auch verborgene Strukturen, z. B. durch HT in der Leiterplatte, gefunden werden können. Die schwarz gestrichelte Ellipse markiert eine Stelle, bei der im Differenzbild zusätzliche Leiterbahnen in Baugruppe-B unterhalb der Oberfläche detektiert wurden. Die orange gestrichelte Ellipse markiert einige Bestückungsunterschiede.

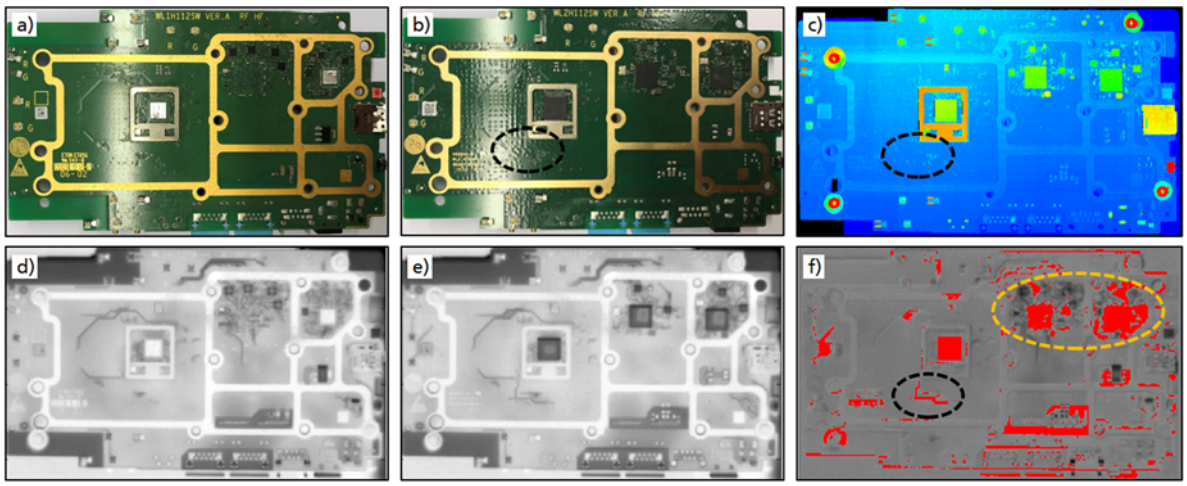

Abbildung 2.2: a) Baugruppe-A, b) Baugruppe-B, c) Laser-Profilometriebild von Baugruppe-B, d) thermisches Phasenbild bei 0,92 Hz von Baugruppe-A, e) und Baugruppe-B, f) Differenzbild des thermischen Phasenbildes von Baugruppe-A und -B

Auf Ebene der unbestückten Leiterplatte unterliegt die Prüfung auf versteckte Funktionsstrukturen anderen Randbedingungen. Leiterplatten (LP) fungieren als passiver Träger für elektronische Bauelemente und sind für die mechanische Befestigung und elektrische Verbindung verantwortlich. Sie bestehen aus Leiterbahnen aus Kupfer, welche in

elektrisch isolierend wirkenden faserverstärktem Kunststoff eingebettet sind. Die Implementierung von passiven und aktiven Bauelementen in eine LP ist aktuell ein etabliertes Verfahren zur Miniaturisierung von Elektronik und kann auch für HT Angriffe verwendet werden. An den ebenen LP können neben der Thermografie und Laser-Profilometrie auch scannende Verfahren wie die Wirbelstromprüfung, welche auf elektrisch leitfähige Materialien empfindlich wechselwirkt, durchgeführt werden. Abbildung 2.3 a) zeigt eine LP mit nachträglich implementierten Bauelement, welches eine HT Signatur simulieren soll. Im Vergleich zum Wirbelstrombild ohne zusätzliches Bauelement b) kann in c) durch Schwellwertauswertung ein deutlicher Kontrast (rote Anzeige innerhalb der blau gestichelter Ellipse) festgestellt werden und somit die zusätzliche Struktur detektiert werden. Dies basiert auf der Annahme, dass HT aus elektrisch leitfähigen Materialien bestehen. Das Wirbelstromverfahren ist jedoch nur an der für den Sensor ersten Kupferschicht empfindlich, unterhalb dieser ersten Schicht sind HT weitestgehend nicht detektierbar.

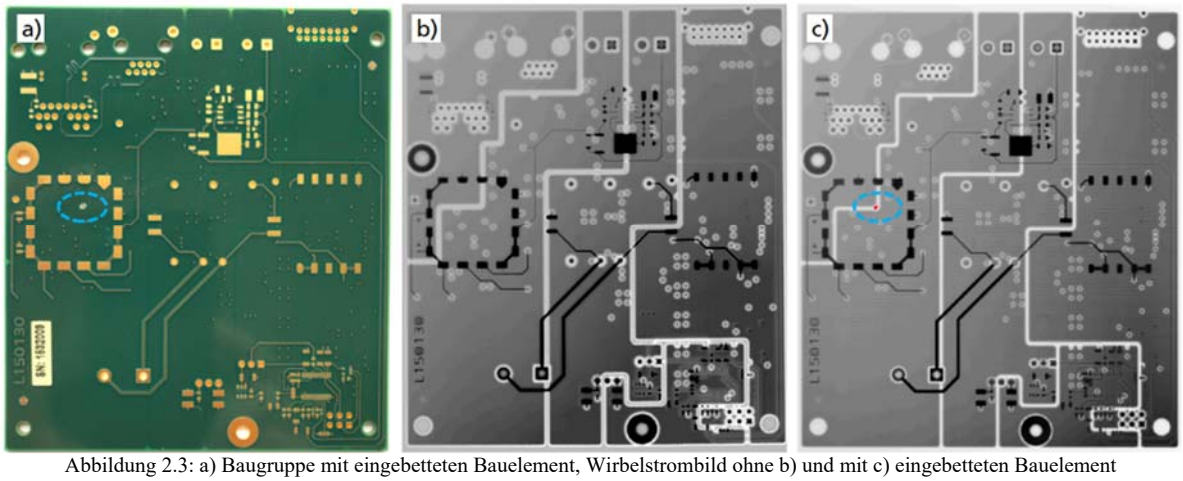

Abbildung 2.3: a) Baugruppe mit eingebetteten Bauelement, Wirbelstrombild ohne b) und mit c) eingebetteten Bauelement

Zur Analyse der Chip-Strukturen steht die Erfassung von Leitbahn- und Transistorstrukturen mit µm- und nm-Skalen im Vordergrund. Als zerstörungsfreier Ansatz erlaubt die akustische GHz-Mikroskopie eine hochauflösende Abbildung im einstelligen Mikrometerbereich. Hochfrequente akustische Wellen können entsprechend fokussiert werden, um sowohl oberflächennah, als auch durch einzelne Verschaltungsebenen des Chips hindurch abzubilden. Eindringtiefe und laterale Auflösung konteragieren hierbei jedoch, weshalb im Einzelfall ein Kompromiss gefunden werden muss. Je nach akustischer Frequenz und Materialzusammensetzung der Probe können Strukturen bis in eine Tiefe von etwa 10 µm abgebildet werden. Dadurch ist auch die Erfassung von größeren Chipstrukturen unterhalb von optisch nicht transparenten Metallbahnen möglich. Abbildung 2.4 zeigt exemplarisch einen Chip des WLAN Routers in 7nm fin field-effect transistor (FinFET) Technologie der mittels akustischer GHz-Mikroskopie in der Draufsicht abgebildet wurde. Die Mäanderstrukturen unter der oberen weitestgehend geschlossenen Metallebene sind optisch nicht zugänglich, können jedoch mittels akustischer Wellen im GHz-Band hochauflösend detektiert und abgebildet werden. Auf diese Weise können auch verdeckte, größere Chip-Strukturen mit ausreichender Sensitivität und Abbildungsauflösung erfasst werden. Diese Methode ist besonders dann relevant, wenn Strukturen durch metallische Leitbahnebenen hindurch zu untersuchen sind, da diese auch im optischen Spektralbereich von elektromagnetischen Wellen nicht durchdrungen werden können. Aufgrund der extremen Fokussierungen, welche bei hochfrequenten akustischen Analysen zum Einsatz kommen, ist die Durchdringung größerer Materialstärken nicht oder nur mit Einschränkungen möglich. Eine Alternative bietet die mikroskopische Abbildung der Chip-Struktur durch das Silizium-Substrat. Insbesondere im für die Thermografie genutzten

Wellenlängenbereich ist Silizium transparent, so dass die unteren Chip-Strukturen, insbesondere die Transistorebene, direkt abgebildet werden kann.

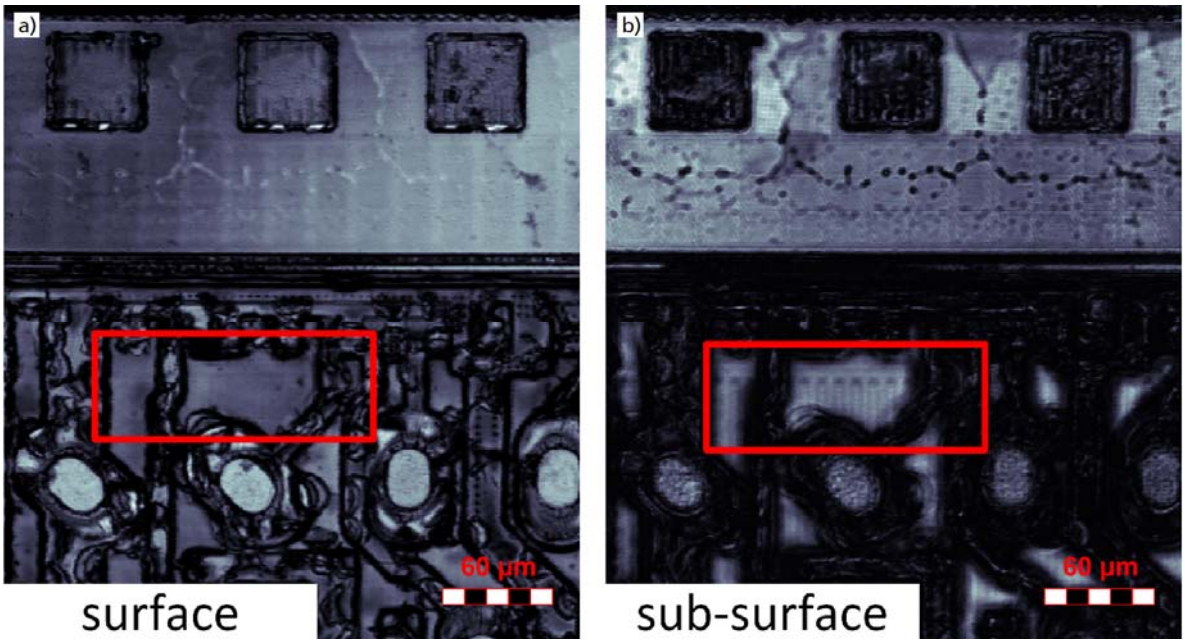

Abbildung 2.4: Hochauflösende akustische Abbildung im GHz-Band. a) Abbildung der Probenoberfläche, welche auch optisch zugänglich ist. b) Abbildung verdeckter Strukturen unterhalb der Probenoberfläche. Verdeckte Mäanderstruktur ist rot markiert.

In Abbildung 2.5 ist eine thermographische Aufnahme der aktiven Chip-Strukturen durch das Silizium des 7 nm FinFET Chips zu sehen. Die hohe Detailtreue ist der Verwendung eines stark vergrößernden Infrarot (IR)-Objektives zu verdanken. Abweichungen in der Größe und Anordnung von Funktionsblöcken können durch Bildanalyse im Vergleich zu einer Referenzprobe gefunden werden. Die Auflösung lässt sich weiter erhöhen, wenn zusätzlich eine Festkörper-Immersionslinse zur Anwendung kommt, siehe Abbildung 2.5 b).

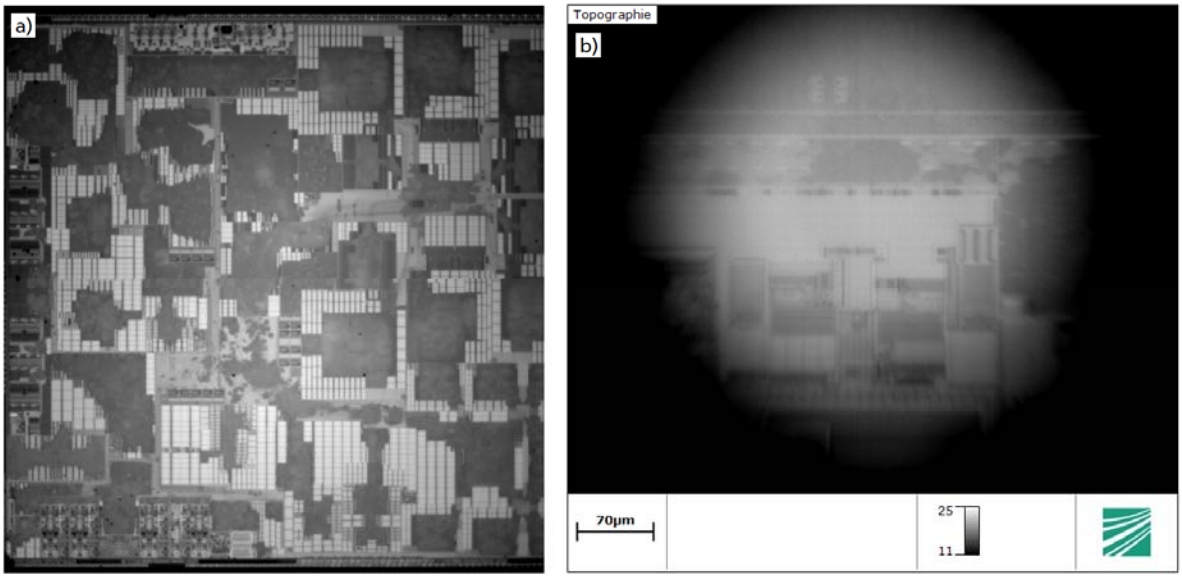

Abbildung 2.5: a) Abbildung im infraroten Spektrum. Mittels Thermografiekamera können die unteren aktiven Ebenen eines Chips zerstörungsfrei durch das Siliziumsubstrat hindurch abgebildet werden. Eine Bildanalyse ermöglicht die Detektion kleinster Strukturabweichungen ohne das Bauelement zu zerstören. Die Anwendung einer Festkörper Immersionslinse b) erlaubt es die laterale Auflösung weiter zu erhöhen, um auch feinere Strukturen detektieren zu können, die aber deutlich über der Größe der Transistoren 7 nm liegen.

2.3 Seitenkanalanalyse auf Chip- Bauelement- und Baugruppenebene

Eine Möglichkeit der Analyse von Seitenkanalsignalen auf Baugruppenebene besteht in der zeitaufgelösten Verfolgung der Erwärmung auf einzelnen Bauelementen einer Baugruppe mittels direktabbildender Thermographie. In Abbildung 2.6 sind Temperaturbilder von der Oberfläche eines FPGA-Bausteins d) zu verschiedenen Zeiten nach Anlegen der Versorgungsspannung dargestellt (a, b, c). An unterschiedlichen Orten treten Temperaturkontraste zu verschiedenen Zeiten auf und verschwinden teilweise auch wieder. Dies zeigt eine Zeitanalyse der mittleren Temperatur (Abbildung 2.6 f) auf ausgewählten Auswerteflächen (Abbildung 2.6 e). Die genauen Zeitverläufe stellen gewissermaßen einen "Fingerabdruck" der Aktivität des Bausteins dar. Es konnte gezeigt werden, dass bestimmte Periodizitäten bei der Erwärmung mit der Länge von Schleifendurchläufen in der Software korrelieren. Da die meisten Vorgänge im Chip aperiodisch ablaufen, können statistische Signalanalyseverfahren für eine Charakterisierung genutzt werden. Vorteil der Thermografie ist die berührungsfreie Arbeitsweise auf größere Distanz und die im Gegensatz zu rasternden Verfahren gleichzeitige, schnelle Prüfung einer größeren Fläche. Die laterale Auflösung in größerer Materialtiefe ist jedoch begrenzt und normalerweise nicht besser als die Tiefe selbst.

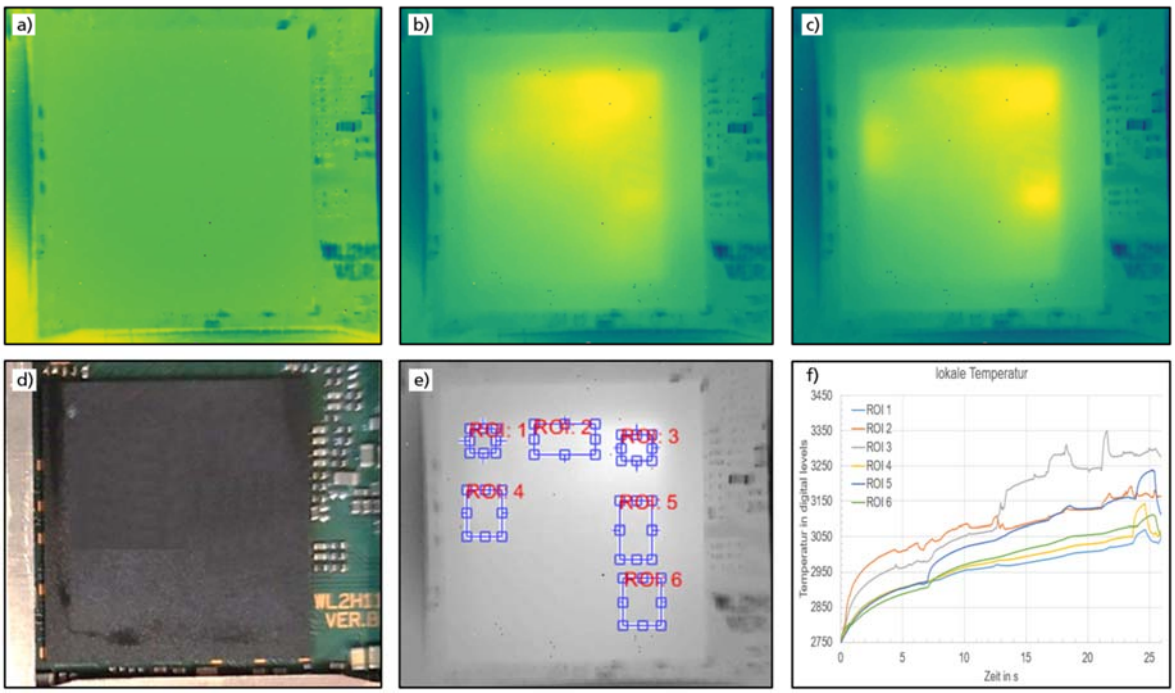

Abbildung 2.6: Aufheizvorgang auf einem FPGA a) zu Beginn, b) nach 10 s, c) nach 30 s, d) Foto des Bauelements, e) Lage der Auswerteregionen 1 bis 6, f) Temperaturverläufe in Einheiten von Digitalwerten auf den Auswerteregionen 1 bis 6

Mit solchen zeitaufgelösten thermographischen Analysen kann man zum einen auf transiente Vorgänge z. B. während des Boot-ups oder spezieller Sequenzen des Betriebes fokussieren. Zum anderen ist es aber auch möglich, die aktiven Regionen eines Schaltkreises zu lokalisieren, indem dieser periodisch beschaltet wird und die aus der Verlustleistung resultierende Wärmestrahlung erfasst wird. Um Zugang zur Chipebene für die hochauflösende Beobachtung der IC-Strukturen zu erhalten, ist es notwendig, die Vergussmasse des Bauelements lokal zu entfernen. Anschließend ist je nach Aufbautechnik die Chip-Oberfläche oder -Unterseite durch das Silizium Substrat hindurch thermographisch abbildbar. Abbildung 2.7 a) zeigt die Präparation eines Bauelements, bei der die Vergussmasse entfernt wird sowie die Ergebnisse der hochauflösenden aktiven Thermografieanalyse (Abbildung 2.7 b, c). In Abbildung 2.7 b) ist die IC-Struktur des Chips zu sehen. Der Kontrast resultiert dabei aus den Emissivitäten der einzelnen Materialien. Die

Probe ist in diesem Zustand nicht aktiv betrieben. In Abbildung 2.7 c) ist das Ergebnis einer Lock-In Messung zu sehen. Hierbei wird die Probe periodisch elektrisch angeregt und die gemessenen thermischen Signale mit der Anregung korreliert. Auf diese Weise lassen sich selbst schwächste thermische Signale der Chip-Aktivität messen und lokalisieren. Diese Ergebnisse können dann im Vergleich zu einer Referenzprobe analysiert werden, um etwaig eingebrachte HT-Strukturen auf IC-Ebene zu identifizieren.

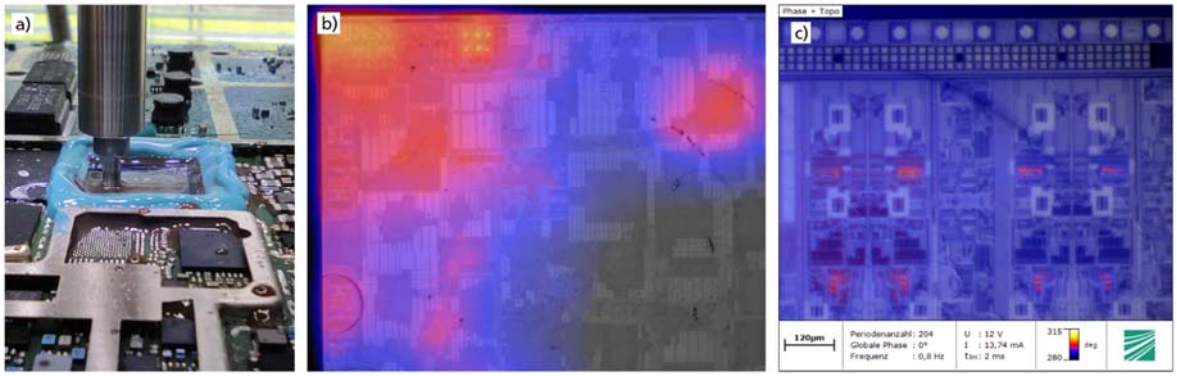

Abbildung 2.7: a) Vorpräparation zur Entfernung der Moldmasse und zum Rückdünnen des Si-Kristalls, um einen direkten Zugang für die aktive Thermografie zu schaffen. Thermografiebilder des geöffneten Chips durch den Si-Kristall hindurch, b) IR-Bild aufgrund des reinen Emissivitätskontrastes der Chiprückseite, c) Überlagerung des Topographiebildes (b) mit den im Lock-in Modus gemessenen Wärmequellen, welche die thermisch aktiven Bereiche lokalisieren.

3. Demonstrator-Baugruppe und erstes Prüfkonzept

In Kapitel 2 konnten erste Ergebnisse verschiedener Prüf- und Analyseverfahren auf unterschiedlichen Elektronikebenen vorgestellt werden. Diese hatten zur Aufgabe eine prinzipielle Nachweisfähigkeit zu demonstrieren. Um im nächsten Schritt einem realistischen Szenario näher zu kommen, muss zuerst eine Eingrenzung auf ein relevantes Anwendungsszenario erfolgen. Elektronische Baugruppen werden heutzutage häufig von weltweit agierenden spezialisierten Unternehmen gefertigt. Diese Fertigungsvorgänge sind kaum einsehbar und können einfach zur unbemerkten Implementierung von HT genutzt werden. Die Überprüfung auf Modifikationen von elektronischen Baugruppen im Wareneingang ist deshalb von großem Interesse, weshalb eine Demonstrator-Baugruppe (Abbildung 3.1 c) mit verschiedenen Modifikationen (HT) aufgebaut wurde.

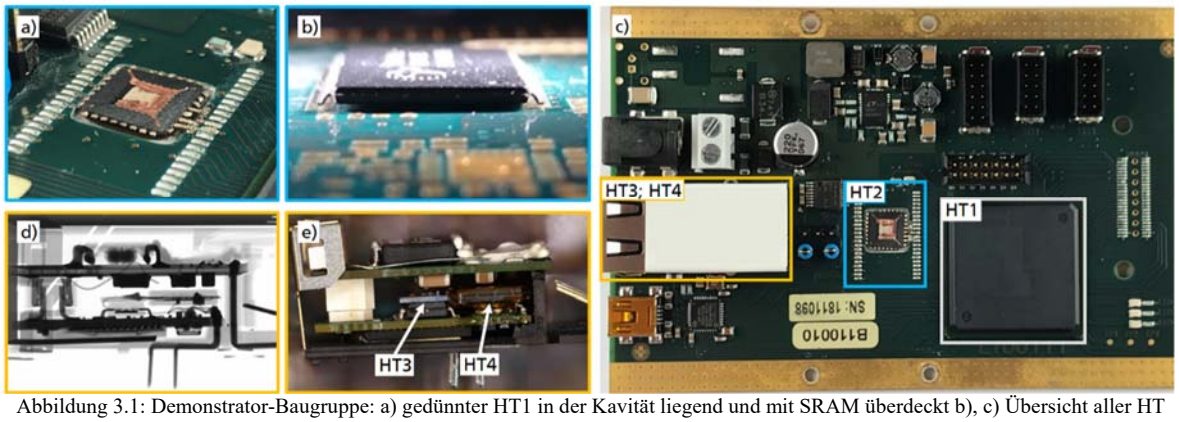

Abbildung 3.1: Demonstrator-Baugruppe: a) gedünnter HT1 in der Kavität liegend und mit SRAM überdeckt b), c) Übersicht aller HT auf der Demonstrator-Baugruppe, d) Röntgenbild und Implementierung e) von HT3 und HT4

Hierzu zählt ein veränderter Programmcode im FPGA (HT1), ein gedünnter Mikrocontroller (HT2) der unter einem static random-access memory (SRAM) Bauelement b) in eine in die Leiterplatte eingebrachte Kavität eingebettet wurde a) sowie ein RISC-V Mikroprozessor (HT3) und ein weiterer Mikrocontroller (HT4), welche in ein

Kommunikationsmodul integriert wurden. Die Modifikationen können optisch nicht und mit Röntgenverfahren nur HT2, HT3 und HT4 erschwert detektiert werden. Die Modifikationen sind an die Versorgungsspannung angeschlossen, funktionsfähig und können zukünftig zur Validierung von verschiedenen multimodalen Prüfkonzepten verwendet werden. Dabei sollen die zu überprüfenden Baugruppen mit einer Referenzbaugruppe ohne HT verglichen werden. Die Ergebnisse aus Kapitel 2 haben einige Vorteile bei der Verwendung von thermografischen Systemen gezeigt. So sind die Möglichkeiten einer HT-Detektion mit der blitzlichtangeregten Thermografie in der Leiterplatte sowie unter bestimmten Voraussetzungen unter Bauelementen gegeben. Wird die Baugruppe aktiv betrieben, so können zusätzlich Unterschiede von örtlich veränderlichen thermischen Merkmalen erfasst werden. Die Erfassung der Stromaufnahme und Vergleich mit der Referenzbaugruppe kann bei Auftreten eines Variationsereignisses auf einen aktiven HT hinweisen. Durch zeitliche Korrelation mit den Thermografiedaten könnte man auf den Ort der zusätzlichen Energieumsetzung hinweisen. Eine Möglichkeit der Detektion von zusätzlich eingebrachten Bauelemente kann die Fusion von optischen Daten mittels Laser-Profilometrie mit dem 3D-Modell der Baugruppe ermöglichen. Ein erstes Prüfkonzept beinhaltet diese Technologien und wird für zukünftige Untersuchungen aufgebaut.

4 Zusammenfassung

Verteilte Sensorik, Edge Computing und Cloud Computing verbinden die Erfassung lokaler Daten mit der Möglichkeit des weltweiten Abrufs über das Internet. Dies eröffnet jedoch die Möglichkeit der Implementierung von versteckten Firm- oder Hardwaremanipulationen an elektronischen Bauteilen (Hardware-Trojanern) zum Ausspähen, Beeinflussen oder Löschen von Daten oder dem Sabotieren von technischen Prozessen. Das Auffinden manipulierter Schaltungsteile stellt deshalb eine hohe Relevanz für eine vertrauenswürdige und sichere Umwelt für industrielle und gesellschaftliche Prozesse dar. Detektionsmechanismen und der Einsatz von Prüf- und Analyseverfahren zum Auffinden der verschiedensten HT-Implementierungen ist aktueller Forschungsgegenstand. Zerstörungsfreie Prüf- und Analyseverfahren können hierbei einen entscheidenden Beitrag zur HT-Detektion leisten.

Soll ein Auffinden über eine Strukturanalyse erfolgen, so konnten gute Ergebnisse auf Baugruppen-, Leiterplatten- und Bauelementebene mit der blitzlichtangeregten Thermografie und der Wirbelstromprüfung erzielt werden. Möchte man HT auf Chipebene detektieren, so wurde gezeigt, dass neben den lichtmikroskopischen Abbildungsverfahren die akustische GHz-Mikroskopie sowie mikroskopische Thermografie mit hochvergrößernden Festkörper-Immersionslinsen Strukturen im unteren µm-Bereich auflösen können. Dazu müssen die Chips jedoch durch Entfernung des Gehäuses optisch zugänglich gemacht werden. Für die Überprüfung von kleineren Strukturen bis hin zu wenigen nm müssen nach der lagenweisen Rückpräparation rasterelektronenmikroskopische Chipscanner und geeignete Software eingesetzt werden.

Die Analyse von Seitenkanalsignalen ist eine weitere Möglichkeit der HT-Detektion. Es konnte gezeigt werden, dass man auf Baugruppen- und Bauelementebene einen „thermischen Fingerabdruck“ aus der Wärmeabstrahlung ermitteln kann. Zusätzliche Wärmequellen durch manipulierte Strukturen können somit detektiert werden. Mittels hochauflösender Lock-In Thermografie kann die Funktionalität einzelner Chipstrukturen anhand ihrer thermischen Emission untersucht und durch Referenzvergleich entsprechende Abweichungen detektiert werden, die auf HT hinweisen. Hierzu müssen die Chips jedoch freigelegt werden.

Zur Validierung zukünftiger Prüfkonzepte wurde eine Demonstrator-Baugruppe mit verschiedenen HT ausgestattet. Ein erstes multimodales Prüfkonzept konnte erarbeitet

werden. Die technische Umsetzung ist aktuell in der Bearbeitung und kann zukünftig wertvolle Erkenntnisse für an die verschiedenen Randbedingungen angepasste Prüf- und Analysesysteme liefern.

5 Danksagung

Diese Arbeit wurde durch das Projekt „Trusted resource aware ICT - TRAICT“ der Fraunhofer Gesellschaft gefördert. Wir danken Carsten Rolfes für wertvolle Diskussionen und die Programmierung der Mikrocontroller sowie Kevin Becker für die Beiträge zu vorsorglichen Abwehrmöglichkeiten.

Referenzen

[1] J. Hartmann, Global Trends in Microelectronics and how Europe can address them, ESSCIRC/ESSDERC 2020 Conference, Sep 2020, Grenoble (France), https://www.ipcei-me.eu/wp-content/uploads/2020/11/13ahartmannslides1598725993144.pdf (as consulted online on 10 December 2021)
[2] J. Francq and F. Frick, Introduction to Hardware Trojan Detection Methods, Design, Automation & Test in Europe Conference & Exhibition (DATE), 9-13 March 2015, Grenoble (France), https://doi.org/10.7873/DATE.2015.1101
[3] P. Swierczynski, M. Fyrbiak, P. Koppe, A. Moradi and C. Paar, Interdiction in Practice – Hardware Trojan Against a High-Security USB Flash Drive, J Cryptogr Eng 7, pp. 199 - 211, Sep 2017, https://doi.org/10.1007/s13389-016-0132-7
[4] SPIEGEL Staff: Inside TAO: Documents reveal top NSA hacking unit (2013). http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html (as consulted online on 09 December 2021)
[5] B. Valeske, R. Tschuncky, F. Leinenbach, A. Osman, Z. Wei, F. Römer, D. Koster, K. Becker, T. Schwender, Cognitive sensor systems for NDE 4.0: Technology, AI embedding, validation and qualification, tm – Technisches Messen, vol. 89, no. 4, 2022, pp. 253-277, https://doi.org/10.1515/teme-2021-0131
[6] B. Sanno, Detecting Hardware Trojans, Ruhr-University Bochum, July 2009, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.8582&rep=rep1&type=pdf (as consulted online on 14 April 2022)
[7] J. Flannery, G.M. Crean, S.C.O. Mathuna, Imaging of Integrated Circuit Packaging Technologies Using Scanning Acoustic Microscopy, Ermert H., Harjes HP. (eds) Acoustical Imaging. Acoustical Imaging, vol 19. Springer, 1992, Boston, MA, https://doi.org/10.1007/978-1-4615-3370-2_113
[8] C. Rooney, A. Seeam, X. Bellekens, Creation and Detection of Hardware Trojans Using Non-Invasive Off-The-Shelf Technologies, Electronics 7, 2018, https://doi.org/10.3390/electronics7070124
[9] H. Liu, L. Tinsley, W. Lam, S. Addepalli, X. Liu, A. Starr, Y. Zhao, A Novel Inspection Technique for Electronic Components Using Thermography (NITECT), Sensors 2020, 20, 5013, https://doi.org/10.3390/s20175013
[10] A. A. R. M. A. Ebayyeh, A. Mousavi, A Review and Analysis of Automatic Optical Inspection and Quality Monitoring Methods in Electronics Industry, in IEEE Access, vol. 8, pp. 183192-183271, 2020, doi: 10.1109/ACCESS.2020.3029127
[11] M. T. Rahman, Q. Shi, S. Tajik, H. Shen, D. L. Woodard, M. Tehranipoor, N. Asadizanjani, "Physical Inspection & Attacks: New Frontier in Hardware Security," 2018 IEEE 3rd International Verification and Security Workshop (IVSW), 2018, pp. 93-102, doi: 10.1109/IVSW.2018.8494856.