Velektronik
Vertrauen ist besser

Fraunhofer
AISEC

Referenzpapier Vertrauenswürdige Elektronik

Teil I: Definition, Bedrohungen und Bewertung von Lösungsansätzen

10. März 2022

Dr. Johann Heyszl, Prof. Dr. Georg Sigl,
Andreas Seelos-Zankl, Dr. Matthias Hiller

Fraunhofer Institut für Angewandte und Integrierte Sicherheit AISEC, Deutschland

REFERENZPAPIER

VERTRAUENSWÜRDIGE ELEKTRONIK

Teil I: Definition, Bedrohungen und Bewertung von Lösungsansätzen

Autoren

Dr. Johann Heyszl

Prof. Dr. Georg Sigl,

Andreas Seelos-Zankl

Dr. Matthias Hiller

Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Lichtenbergstraße 11, 85748 Garching bei München

Velektronik
Vertrauen ist besser

Projektname: Velektronik
Datum: 10.03.2022
Projektpartner: Bundesministerium für Bildung und Forschung

Danksagung

Die Arbeiten wurden vom BMBF im Förderprojekt Plattform Vertrauenswürdige Elektronik unter dem Kennzeichen 16ME0214K gefördert. Die Autoren bedanken sich bei allen Mitgliedern des Projekts, dem Industriebeirat, Workshop-Teilnehmern und bei allen Reviewern aus Wirtschaft und Forschung für ihre Beiträge.

Bundesministerium für Bildung und Forschung

Inhalt

Einleitung und Überblick

Das Referenzpapier „Vertrauenswürdige Elektronik“ wird im Rahmen des Projekts Velektronik[1] entwickelt, das vom Bundesministerium für Bildung und Forschung (BMBF)[2] gefördert wird. Das Projekt Velektronik hat zum Ziel, die Projekte des Förderprogramms Vertrauenswürdige Elektronik (ZEUS) zu begleiten, indem es die Inhalte erfasst, die Ergebnisse in einen ganzheitlichen Ansatz einordnet und Lücken identifiziert. Dieses Referenzpapier leistet dazu einen wichtigen Beitrag. Das Papier wird in mehreren, jährlich aufeinander folgenden Teilen erweitert. Teil 1 des Papiers enthält folgende Aspekte:

- Eine **Definition vertrauenswürdiger Elektronik** (Kapitel 1). Diese Definition hilft, das Thema abzugrenzen und den Zusammenhang sowohl zu IT-Sicherheit als auch zu technologischer Souveränität zu erklären.

- Danach wird eine **übersichtliche Darstellung der Elektronik-Wertschöpfungskette** gezeigt (Kapitel 2). Damit werden die **Bedrohungen für Vertrauenswürdigkeit** systematisch anhand dreier wesentlicher Kategorien erklärt. **Beispiele** illustrieren diese Kategorien auf verständliche Weise (Kapitel 2.2). Darauf aufbauend werden Prioritäten abgeleitet, welche Bedrohungen besonders relevant sind (Kapitel 3).

- Um die **positive Auswirkung** von Lösungsansätzen auf vertrauenswürdige Elektronik darzulegen, werden zudem **drei einfache Bewertungskriterien** definiert (Kapitel 4).

- Die vom BMBF im Rahmen der Förderbekanntmachung ZEUS geförderten Projekte werden in diesen Kontext untersucht, um Lücken in der abgedeckten Felder zu identifizieren (Kapitel 4.1 und 4.2).

- Nach einer Zusammenfassung folgt ein **Ausblick inklusive Forschungsimpulse** (Kapitel 5).

Zukünftig geplante Teile dieses Papiers werden die Überlegungen, welche Forschungsthemen einen stärkeren Fokus erhalten könnten, fortführen. Außerdem werden Themen adressiert, die häufig im Kontext mit vertrauenswürdiger Elektronik genannt werden. Unter anderem sind Kapitel zu den Themen Open-Source-Hardware, Echtheitsmerkmalen, der Messung von Vertrauenswürdigkeit sowie dem Bedarf an Standardisierung geplant. Praktische Fallstudien anhand repräsentativer, anonymisierter Unternehmen werden zeigen, wie Forschungsergebnisse die Vertrauenswürdigkeit elektronischer Produkte erhöhen.

[1] https://www.velektronik.de/
[2] https://www.bmbf.de

1 Eine Definition von vertrauenswürdiger Elektronik

Intelligente, vernetzte Produkte basieren in hohem Maß auf sicherer und vertrauenswürdiger Software. Die Realisierung solcher Software ist jedoch nur möglich, wenn die Hardware, auf der die Software ausgeführt wird, sicher und vertrauenswürdig ist. Auch andere Elektronikkomponenten wie Sensoren und Aktuatoren müssen vertrauenswürdig Messdaten liefern oder Aktionen umsetzen. Produkte hoher Qualität, wie sie für die deutsche Wirtschaft typisch sind, sind folglich nur mit vertrauenswürdiger Elektronik möglich.

Dieses Papier konzentriert sich deshalb auf die *Vertrauenswürdigkeit elektronischer Hardware*. Nur fest integrierte Software, sogenannte Firmware, ist dabei Teil der Betrachtung. Vertrauen in Elektronik bedeutet, dass Unternehmen Produkte und Systeme auf Basis elektronischer Hardware bauen und dabei möglichst ausschließen können, dass unerwartetes Verhalten und Sicherheitsvorfälle auftreten. Aufgrund der hohen Komplexität von High-Tech-Elektronikentwicklung und -fertigung und der dadurch erforderlichen Spezialisierung erstrecken sich entsprechende Wertschöpfungsketten von Entwicklung bis Produktion und Lieferketten über den gesamten Globus. Unter diesen Voraussetzungen ist es immens herausfordernd, Vertrauen in elektronische Hardware herzustellen.

Vertrauenswürdige Elektronik ist definiert durch das Erfüllen der folgenden Eigenschaften:

1. Die elektronische Hardware muss **hohen Qualitäts- und Zuverlässigkeitsanforderungen** genügen. Sie kann zuverlässig über die gesamte Lebenszeit im Feld betrieben werden.

2. Die elektronische Hardware muss eine **bekannte und vollständige Spezifikation** erfüllen.
   - Dies bedeutet, dass die Hardware in ihrer Funktion *exakt und ausschließlich* die Spezifikation erfüllt. Die Hardware enthält keine Funktionalität, die als Hintertür verwendet werden kann – weder absichtlich noch durch den Missbrauch von Funktionalität, die zu anderem Zweck spezifiziert war. Zu keinem späteren Zeitpunkt in der Wertschöpfungskette kann die Funktionalität der Hardware abweichend von der Spezifikation verändert werden.

3. Die elektronische Hardware muss **gegen Angriffe ausreichend gehärtet** sein, die das Verhalten oder die Funktion ohne Zustimmung des Besitzers verändern.
   - Dies erfordert einerseits **Sicherheitsmechanismen in der Spezifikation** und andererseits, dass die Hardware **keine weiteren relevanten Schwachstellen außerhalb der Spezifikation** zeigt, wenn sie im Feld mit realistischen Angriffen konfrontiert ist. Relevante Angriffe wie beispielsweise Seitenkanal- und Fehlerangriffe nutzen Betriebsumstände und Informationsquellen, die sich außerhalb der Spezifikation befinden. Vertrauenswürdige Elektronik erfordert daher immer ein ausreichendes Maß an Hardware-Sicherheit, geht aber darüber hinaus, wie die obigen Punkte zeigen.

Zusammenhang zu technologischer Souveränität. Technologische Souveränität bedeutet *innerhalb des Rahmens von vertrauenswürdiger Elektronik*, dass man aus eigenen Stücken in der Lage ist, ein ausreichendes Maß an Vertrauenswürdigkeit für die gesamte international eingekaufte Elektronik und die damit verbundenen Leistungen der Wertschöpfungskette sicherzustellen. Dabei ist wichtig festzustellen, dass dies nicht erfordert, dass all diese Leistungen unter vollständig eigener Kontrolle oder auf eigenem Territorium stattfinden müssen. Wesentlich ist, dass die obigen Ziele aus eigenen Bemühungen sichergestellt werden können. Dies kann im Allgemeinen mittels sowohl technologischer als auch organisatorischer Lösungen erfolgen.

Technologische Souveränität ist allerdings mehr als das: Sie impliziert auch die Möglichkeit, *zu jeder beliebigen Zeit und in beliebiger Menge* im Sinne der Versorgungssicherheit sowohl auf Elektronik als auch auf entsprechende (Design-)Werkzeuge und Produktionskapazitäten zugreifen zu können. Dies ist grundlegend, jedoch gleichzeitig schwierig sicherzustellen. Während der COVID-19-Pandemie kam es beispielsweise zu gravierenden Lieferengpässen elektronischer Komponenten. Während diese Thematik nicht unmittelbar unter den Begriff der vertrauenswürdigen Elektronik fällt, ist sie ein wesentlicher Teilaspekt von Technologiesouveränität und hat für die Wirtschaft eine immense Bedeutung. Sie hat eine Auswirkung auf vertrauenswürdige Elektronik, weil Lieferengpässe und hohe Preise das Aufkommen von Elektronik-Fälschungen begünstigen, was wiederum ein Teilproblem vertrauenswürdiger Elektronik ist.

2 Die Elektronik-Wertschöpfungskette und Bedrohungen

Die Elektronik-Wertschöpfungskette ist komplex und unterscheidet sich je nach betroffenen Bauteilen, Gruppen, Geräten, Technologien und beteiligten Unternehmen. Im Folgenden skizzieren wir trotzdem eine einheitliche und vereinfachte Wertschöpfungskette als Basis für alle weiteren Überlegungen zu Bedrohungen der Vertrauenswürdigkeit und den Lösungen dafür. Diese abstrahierte Darstellung beinhaltet Elemente, die spezifisch für Halbleiterfertigung sind, wie auch Elemente, welche weitere elektronische Komponenten und die Fertigung gesamter Geräte repräsentieren. Der Abstraktionsgrad ist bewusst nicht streng konsistent, sondern verfolgt die Absicht, die hier relevantesten Aspekte der Wertschöpfungskette für die weitere Diskussion darzustellen. Dabei wird beispielsweise auch die Software- bzw. Firmware-Entwicklung nicht explizit berücksichtigt.

Für jedes Element der Wertschöpfungskette identifizieren wir *Quellen für Bedrohungen*, die die angestrebte Vertrauenswürdigkeit untergraben bzw. zerstören.

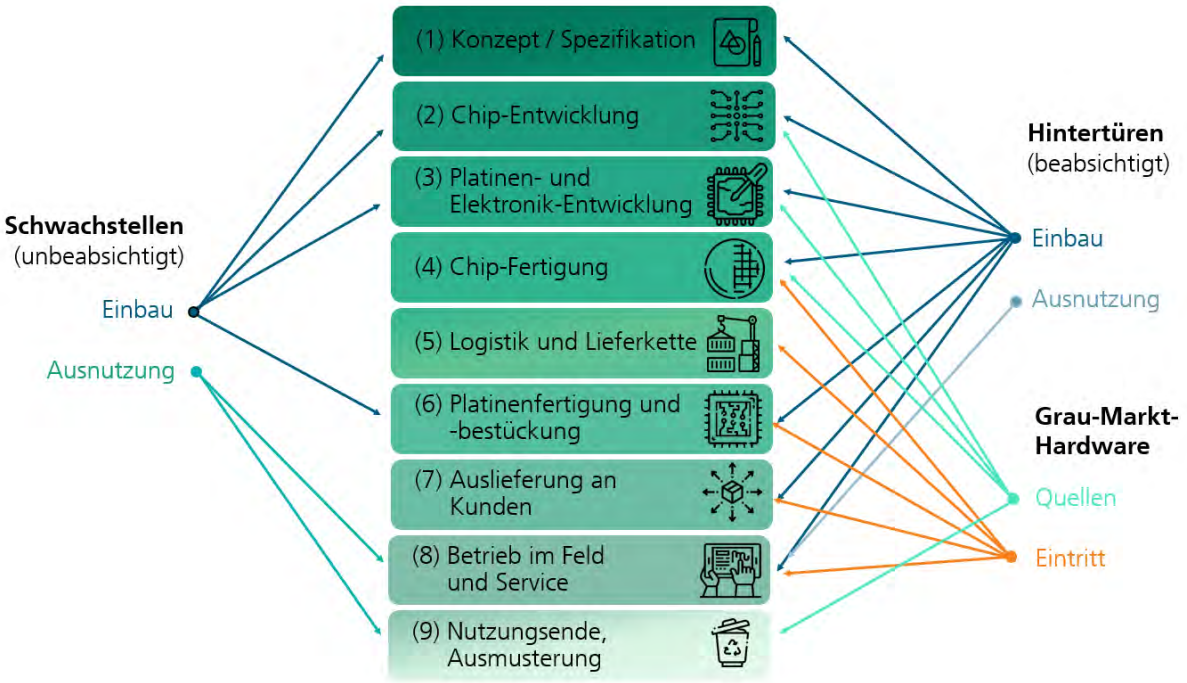

Abbildung 1: Abstrahierte Elektronik-Wertschöpfungskette und Zusammenfassung der Bedrohungen für Vertrauenswürdigkeit.

Abbildung 1 zeigt die Elemente der abstrahierten Wertschöpfungskette und fasst die Bedrohungen für Vertrauenswürdigkeit zusammen, die sich im Wesentlichen in drei Kategorien einteilen lassen:

1. **Schwachstellen**, die unabsichtlich in Chips und Elektronik eingebaut und später im Betrieb ausgenutzt werden.
2. **Hintertüren**, die absichtlich in Chips und Elektronik eingebaut und später ausgenutzt werden.
3. **Grau-Markt-Hardware** beschreibt eine Gruppe von Bedrohungen, wie das Aufkommen illegaler Chip-/Platinen-Fälschungen, -Kopien, minderwertiger und falsch gekennzeichneter Ausschussware sowie der Diebstahl geistigen Eigentums beispielsweise in Folge von Reverse-Engineering.

2.1 Bedrohungen entlang der Wertschöpfungskette

Im Folgenden werden die Elemente der Wertschöpfungskette aus Abbildung 1 detailliert aufgeführt. Zu jedem Element werden Bedrohungen bzw. deren Quellen genannt und diese den drei oben identifizierten Kategorien in Spalten zugeordnet. Bei manchen Elementen wie der Chip-Entwicklung werden Unterelemente aufgeführt, um die Bedrohungen verständlich zuzuordnen.

Tabelle 1: Bedrohungen für Vertrauenswürdigkeit entlang der Elektronik-Wertschöpfungskette

Schwachstellen (unbeabsichtigt)	Hintertüren (beabsichtigt)	Grau-Markt-Hardware
(1) Konzept / Spezifikation von Chips, Modulen, Gruppen und elektronischen Produkten		
Lücken/Fehler in Spezifikationen, die später missbraucht werden	Schwachstellen in Spezifikationenund Standards	
(2) Chip-Entwicklung analog / digital / mixed-signal		
- Eigene oder an Dritte ausgelagerte Entwicklung		
Implementierungsfehler, Funktionalität mit Missbrauchspotential, Implementierungsangriffe außerhalb der Spezifikation zur Zeit der Entwicklung	absichtlich eingebrachte Schwachstellen oder Hintertüren (HW-Trojaner) bei Eigenentwicklung oder ausgelagerten Entwicklungsleistungen	Diebstahl geistigen Eigentums für illegale Kopien und Fälschungen
- Design-Flow (Simulation, Synthese, Place&Route, Layout)		
Design-Tool-Optimierungen zum Entfernen funktional redundanter Sicherheitsmaßnahmen	Design-Tool-basierende Modifikationen für Schwachstellen / Hintertüren	(wie oben)
(3) Platinen- und Elektronik-Entwicklung (eigene und ausgelagert)		
Entwicklungsfehler erlauben Zugriff auf sensible Schnittstellen	Einbettung von HW-Trojaner-Chips / ungewünschten Trojaner-Schnittstellen	(wie oben)
(4) Chip-Fertigung		
- Designdatentransfer und Maskenproduktion		
	Manipulation von Design- oder Maskendaten	(wie oben)
- Wafer-Fertigung (Front-/Back-End of Line) und Packaging		
		Quellen für Grau-Markt aus illegalen Klonen (mit potenziell unterschiedlichen gestohlenen Designs), Fälschungen (Überproduktion) oder gebrauchten (Recycling) sowie defekten Chips (Wiedereintrag von Ausschussware)
(5) Logistik und Lieferkette		
		(wie oben)
(6) Platinenfertigung und -bestückung inkl. Einbringen von Firmware		
Unsichere Hardware-Root-Schlüssel oder Verlust von Schlüsseln	Einbettung von HW-Trojaner-Chips, Manipulation von Firmware (z. B. Bootlader-Missbrauch) oder manipulierte HW-Root-Schlüssel	(wie oben)
(7) Auslieferung an Kunden		
(wie oben)	(wie oben)	(wie oben)
(8) Betrieb im Feld durch Kunden und **Service im Feld**		
Ausnutzung von Schwachstellen (z. B. nach Analyse oder Reverse-Engineering)	Ausnutzung eingebrachter Hintertüren, Einbringung manipulierter Firmware-Updates	Einbringung von Grau-Markt-Elektronik, Reverse-Engineering zum Diebstahl geistigen Eigentums
(9) Nutzungsende, Ausmusterung von elektronischen Produkten, Chips, Mustern usw.		
z. B. illegales Reverse-Engineering anstatt Entsorgung / Zerstörung		Quelle für Grau-Markt als illegales Recycling, Reverse-Engineering zum Diebstahl geistigen Eigentums

2.2 Beispiele

Die folgenden Beispiele illustrieren die zuvor aufgelisteten Quellen für Bedrohungen für Vertrauenswürdigkeit in den drei identifizierten Kategorien entlang der Wertschöpfungskette.

2.2.1 Schwachstellen (unbeabsichtigt)

Konzept / Spezifikation und Chip-Entwicklung. Viele High-Tech-Chips wie CPUs für PCs und Server sind hoch-komplex. Obwohl immense Anstrengungen in Richtung einer hohen Sicherheit von Unternehmen wie Intel und AMD unternommen werden, führt die Komplexität der Chips unweigerlich zu unbeabsichtigten Schwachstellen. Die bekanntesten Beispiele aus den vergangenen Jahren sind die Angriffe Meltdown und Spectre[3] in CPUs [5, 4]. Die Angriffe nutzen komplexe Funktionen der CPU-Hardware aus, deren Implementierungsdetails nicht öffentlich dokumentiert waren. Die Folgen waren schwerwiegend, weil ten.

Abbildung 2: Spectre und Meltdown Angriff.
Quelle: https://meltdownattack.com/

Obwohl es sich um *unbeabsichtigte* Schwachstellen handelt, sind die Folgen gravierend. Die Implementierungsdetails elektronischer Produkte sind üblicherweise nur begrenzt zugänglich, sodass nur wenige die Chance haben, Schwachstellen im Zuge einer Begutachtung zu identifizieren. Im Falle von zertifizierten Produkten (z. B. Common-Criteria-Zertifizierung) wird der Kreis der Begutachter zwar größer, bleibt allerdings nichtsdestotrotz stark beschränkt. Interessanterweise wird diese Art von Schwachstelle häufig erst im Feld während des Betriebs oder nach der Ausmusterung von Exemplaren beispielsweise mittels Reverse-Engineering erkannt. Die Ausnutzung der Schwachstellen erfolgt anhand der Exemplare, die sich im Feld in Betrieb befinden.

Ähnliche schwerwiegende Schwachstellen sind auch in weniger komplexen Chips, z. B. in Mikrokontrollern, zu finden. Beispielsweise wurde gezeigt, dass USB-Authentisierungstokens aufgrund solcher Schwachstellen während des Betriebs im Feld oder bereits bei der Auslieferung an den Kunden manipuliert werden können, sodass sie komplett unsicher werden [9]. Schwachstellen in Elektronik ermöglichen leider Manipulationen an vielen Punkten der Wertschöpfungskette.

Abbildung 3: Unbeabsichtigte Schwachstellen in USB-Tokens.
Quelle: Schink, Fraunhofer AISEC

[3] https://meltdownattack.com/

Ein weiteres signifikantes Beispiel kommt aus dem Automobilbereich: Ein populäres CPU-Produkt wies einen gravierenden Fehler in der fest eingebrannten Firmware (also in der Hardware) auf, der es zu jedem Zeitpunkt möglich machte, den grundlegenden Schutz der Anwendungssoftware zu umgehen und Software beliebig zu manipulieren[4].

2.2.2 Hintertüren (beabsichtigt)

Konzept / Spezifikation. Es gibt öffentlich bekannte Beispiele für Hintertüren und Schwachstellen, die absichtlich in Spezifikationen und Produkte eingebaut wurden. In einem Fall wurde eine jahrelang unerkannte Hintertür in den Standard für einen Zufallszahlengenerator integriert, den sogenannten Dual_EC_DRBG im NIST Standard SP 800-90A. Dieser wurde in vielen Produkten, wie beispielsweise der SW-Kryptographie-Bibliothek der RSA Security Inc., eingesetzt.

Chip-Entwicklung. Viele akademische Veröffentlichungen beschäftigen sich damit, auf welche Arten Hardware-Trojaner in unterschiedlichen Schritten in Chips integriert werden *könnten* [2]. Der Trade-Off zwischen Kosten und Nutzen für die meisten solcher Manipulationen insbesondere in späten Fertigungsschritten ist relativ hoch. Das Einbringen von Hardware-Trojanern scheint vor allem in frühen Schritten der Chip-Entwicklung relevant zu sein [3], doch sind keine konkreten Fälle aus der Wirtschaft bekannt. In einem öffentlich dokumentierten Fall wurde eine Passwort-gesicherte Hintertür in einem FPGA beschrieben [10], allerdings scheint unklar, ob es sich tatsächlich um eine Hintertür oder vielmehr um eine nicht-dokumentierte Debug-Schnittstelle handelt. In beiden Fällen können schwerwiegende Angriffen im Feld die Folge sein.

Elektronik-Entwicklung. Ein Beispiel sind die Hintertüren, die in den 70er, 80er und 90er Jahren in von der Crypto AG vertriebene elektronische Kommunikationsgeräte zur verschlüsselten Kommunikation von Regierungen eingebaut wurden.

Chip-Fertigung. Es gibt keine Berichte über Vorfälle von Manipulation von Maskendaten für die Chip-Fertigung. Akademische Forschung zeigt, dass solche Manipulationen sehr gut versteckte und schwerwiegende Hintertüren öffnen können. Beispielsweise wurde gezeigt, dass bereits die Manipulation weniger Transistoren (im Zufallszahlengenerator) sämtliche Verschlüsselungsfunktionen eines elektronischen Gerätes vollständig aushebeln kann [1].

Platinenfertigung und -bestückung. Eine stark beachtete Veröffentlichung von Bloomberg [7] (sowie später [8]) beschrieb die Beobachtung von Hardware-Trojanern und Hintertüren in Form von sehr kleinen, kaum detektierbaren auf Platinen implantierten Chips in Server-Mainboards eines bestimmten Herstellers. Komplette Server-Systeme können anhand solcher kleinen Chips, die unter normalen Umständen nicht erkannt werden, aus der Ferne kompromittiert werden. Obwohl Beweise für diesen konkreten Fall nie öffentlich wurden, ist das Szenario angesichts des notwendigen Aufwands und der zu befürchtenden Auswirkung hoch-realistisch. Berichte über gefälschte Netzwerkkomponenten von CISCO[5] zeigen sehr ähnliche Manipulationen – in diesem Fall allerdings zum Zweck der Fälschung anstatt einer Hintertür. Auch dort wurden kleine Chips auf der Platine implantiert.

[4] https://blog.quarkslab.com/vulnerabilities-in-high-assurance-boot-of-nxp-imx-microprocessors.html
[5] https://www.servethehome.com/fake-cisco-switches-in-the-supply-chain-uncovered/

Auslieferung an Kunden. Es gibt umfangreiche Berichte über die Installation von Hintertüren in unterschiedlichen elektronischen Geräten anhand kleiner Manipulationen und implantierter Chips in der Lieferkette und während der Auslieferung als Teil größer angelegter nachrichtendienstlicher Unterfangen[6]. Ein davon unabhängiges Beispiel zeigt ein USB-Kabel[7] mit einem in den Plastikstecker implantierten WiFi-Chip, der Daten über weite Strecken an einen Angreifer ausleiten kann. Auf Röntgenbildern ist der implantierte Chip detektierbar[8].

2.2.3 Grau-Markt-Hardware

Gefälschte/geklonte Chips. Es gibt zahlreiche Berichte zu gefälschten und geklonten Chips populärer Produkte, die sich weit verbreiten. In solchen Fällen sind die konkrete Spezifikation und Qualität ausgesprochen unsicher, sodass Einsatz dieser Chips ein hohes Risiko birgt. Beispielsweise werden die Mikrokontroller der Firma STMicroelectronics, die hochvolumig in IoT-Geräten und eingebetteten Geräten eingesetzt werden, häufig gefälscht und geklont[9]. Teilweise werden sie als kompatible Ersatz-Chips vertrieben, teilweise mit gefälschten Markierungen als Originale [6]. Beispiele für solche gefälschten und geklonten STM32F1-Chips finden sich in [6] [Abbildung 1 und Abbildung 2].

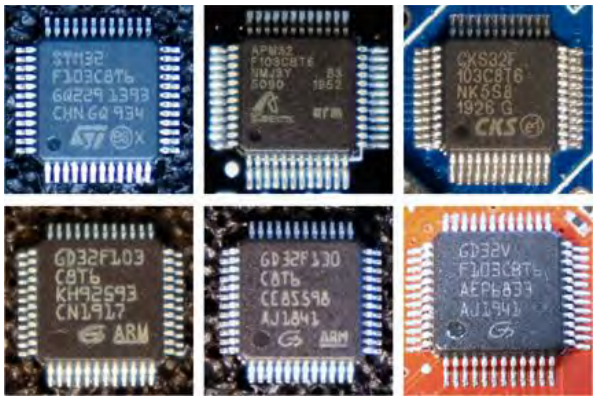

Abbildung 4: Funktional geklonte Chips.
Quelle: Obermaier, Schink, Moczek [6]

Geklonte Chips können entweder auf Basis von Reverse-Engineering oder durch Kopie der Funktion entstehen. Das Beispiel der geklonten FTDI-Chips[10] zeigt, dass das zugrundeliegende Design ein gänzlich anderes, aber dennoch funktionskompatibel war. Ein weiteres Beispiel ist ein Chip der Firma Nordic Semiconductor[11], der mittels exaktem Reverse-Engineering auf einem anderen Halbleiterprozess geklont wurde. Gefälschte und geklonte Chips aus dem Grau-Markt infiltrieren und beeinträchtigen die Elektronik-Wertschöpfungskette an verschiedenen Stellen, wie in Abbildung 1 dargestellt.

[6] https://en.wikipedia.org/wiki/NSA_ANT_catalog
[7] https://shop.hak5.org/products/o-mg-cable-usb-c
[8] https://www.vice.com/en/article/k789me/omg-cables-keylogger-usbc-lightning
[9] https://hackaday.com/2020/10/22/stm32-clones-the-good-the-bad-and-the-ugly/
[10] https://zeptobars.com/en/read/FTDI-FT232RL-real-vs-fake-supereal
[11] https://zeptobars.com/en/read/Nordic-NRF24L01P-SI24R1-real-fake-copy

Gefälschte/geklonte elektronische Geräte. Es werden sogar ganze elektronische Geräte illegal geklont. Beispielsweise wurden illegale Fälschungen von CISCO-Netzwerkkomponenten bekannt[12], die bei Unternehmen im Einsatz waren. Der Bericht[13] enthält Bilder von gefälschten Geräten, in denen die Unterschiede der gefälschten Platinen teils detektierbar sind. Teilweise wurden implantierte Chips verwendet, die theoretisch Hintertüren einbringen könnten. In jedem Fall ist die Vertrauenswürdigkeit solcher Geräte höchst fragwürdig. Interessanterweise war die Produktfälschung im beschriebenen Fall auch deswegen möglich, weil einer der verwendeten Hauptprozessoren eine unbeabsichtigte Hardware-Schwachstelle enthielt, die erlaubte, Software illegal zu klonen. Das Beispiel illustriert daher mehrere Bedrohungen für vertrauenswürdige Elektronik sehr deutlich.

[12] https://www.servethehome.com/fake-cisco-switches-in-the-supply-chain-uncovered/
[13] https://labs.f-secure.com/publications/the-fake-cisco/

3 Prioritäten in vertrauenswürdiger Elektronik

Die in Abschnitt 2.1 entlang der Wertschöpfungskette identifizierten Bedrohungen für Vertrauenswürdigkeit sind in Tabelle 2 im Überblick dargestellt, allerdings nun anhand der drei Kategorien gruppiert. Bedrohungen, die in mehreren Elementen der Wertschöpfungskette ähnlich sind, wurden zur besseren Übersichtlichkeit zusammengefasst.

Darauf aufbauend wurde eine vereinfachte Risikoanalyse durchgeführt, um nachzuvollziehen, welche Bedrohungen besonders relevant sind. Dies dient dazu, Prioritäten zu definieren, an welchen Stellen die Forschung vorrangig ansetzen sollte. Die Einschätzung wird anhand der folgenden Eigenschaften abgeleitet:

- Das geschätzte **Schadensausmaß** misst den voraussichtlichen Schaden erfolgreicher Angriffe bzw. Bedrohungen. Ein hohes Schadensausmaß bedeutet, dass eine große Anzahl elektronischer Geräte nach der Definition für vertrauenswürdige Elektronik beeinträchtigt werden.
- Die geschätzte **Eintrittswahrscheinlichkeit** für Unternehmen beschreibt, ob eine Bedrohung eine hohe praktische Relevanz im Feld hat oder es sich eher um ein aus akademischer Sicht interessantes Risiko handelt. Hier wird auch darauf hingewiesen, ob es zu einer Bedrohung bereits beobachtete Fälle in der Wirtschaft gab (wie zum Teil in Kapitel 2 beschrieben).
- Das geschätzte **Nutzen-Kosten-Verhältnis** für den Angreifer beschreibt, ob eine Bedrohung attraktiv für Angreifer ist. Wenn beispielsweise der wirtschaftliche oder strategische Nutzen im Vergleich zu den dafür benötigten Ressourcen wie Aufwand, Know-How oder Kosten hoch ist, fällt auch die Einschätzung hoch aus. Hohe Aufwände bei geringem Nutzen reduzieren das Nutzen-Kosten-Verhältnis entsprechend.

Die drei Eigenschaften werden jeweils in drei Stufen als **hoch/mittel/niedrig** bewertet. Anhand der drei Kategorien wird zusammenfassend eine **geschätzte Priorität** ermittelt. Diese Bewertung erfolgte durch Fachexperten und wurde durch Vertreter aus Forschung und Wirtschaft im Rahmen des Projekts Velektronik begutachtet. Naturgemäß handelt es sich um eine abstrahierte Betrachtung nach bestem Wissen und Gewissen.

Tabelle 2: Einschätzung der Prioritäten von Bedrohungen für vertrauenswürdige Elektronik.

Gruppierte Bedrohungen nach Elementen der Wertschöpfungskette		Geschätztes **Schadensausmaß**	Geschätzte **Eintrittswahrscheinlichkeit** für Unternehmen (konkrete Berichte vorhanden: Ja/Nein)	Geschätztes **Nutzen-Kosten-Verhältnis** für Kontrahenten	Geschätzte **Priorität**
Schwachstellen (unbeabsichtigt) in Wertschöpfungskette:					
(1)	**Konzept/Spezifikation** und **Chip-Entwicklung**	hoch	hoch (Ja)	hoch	**hoch**
(2)	**Platinen- und Elektronik-Entwicklung**	niedrig	mittel (Nein)	mittel	mittel
(3)	**Betrieb im Feld** (Angriffe)	hoch	hoch (Ja)	mittel	**hoch**
Hintertüren (beabsichtigt) in Wertschöpfungskette:					
(4)	**Konzept/Spezifikation** (z. B. Standardisierung)	hoch	mittel (Ja)	nieder	mittel
(5)	**Chip-Entwicklung** (z. B. ausgelagert)	hoch	mittel (Nein)	mittel	mittel
(6)	**Chip-Entwicklung** (Design-Flow) und **Chip-Fertigung** (z. B. Tool-basiert, Maskenmanipulation)	mittel	niedrig (Nein)	niedrig	niedrig
(7)	**Platinen- und Elektronik-Entwicklung**, **Platinenfertigung und -bestückung**, **Auslieferung** und **Betrieb im Feld** (z. B. implantierte HW-Trojaner und FW)	hoch	hoch (Nein)	hoch	**hoch**
Grau-Markt-Hardware in Wertschöpfungskette:					
(8)	**Chip-Entwicklung** und **Platinen- und Elektronik-Entwicklung** (z. B. Diebstahl von geistigem Eigentum)	mittel	hoch (Ja)	mittel	mittel
(9)	**Chip-Fertigung** und **Nutzungsende** (z. B. Überproduktion, Nutzung von Ausschussware und Recycling sowie Diebstahl geistigen Eigentums)	hoch	hoch (Ja)	hoch	**hoch**
(10)	**Logistik und Lieferkette**, **Platinenfertigung und -bestückung**, **Auslieferung** und **Betrieb im Feld** (Eintritt aus Grau-Markt)	hoch	hoch (Ja)	hoch	**hoch**

Zusammenfassend sind die wichtigsten Bedrohungen für vertrauenswürdige Elektronik anhand der Bewertung in Tabelle 1 wie folgt:

- **Unbeabsichtigte Schwachstellen in Chips**, die in frühen Entwicklungsschritten (**Konzept / Spezifikation** und **Chip-Entwicklung**) entstehen und **im Feld** ausgenutzt werden.
- **Beabsichtigte Hintertüren** in Form von implantierten Chips als Hardware-Trojaner oder manipulierter Firmware, die in späten Schritten der Wertschöpfungskette eingebracht werden (von **Platinen- und Elektronik-Entwicklung, Platinenfertigung und -bestückung,** bis **Auslieferung** und **Betrieb im Feld**).
- **Grau-Markt-Hardware** aus der **Chip-Fertigung** durch Überproduktion und Verwendung von Ausschussware sowie nach **Nutzungsende** durch illegales Recycling, welche an vielen Stellen in die Wertschöpfungskette eintritt.

4 Bewerten von Lösungsansätzen anhand von Kriterien

Es ist nicht immer klar ersichtlich, ob Lösungsansätze positive Auswirkungen auf die Vertrauenswürdigkeit von Elektronik entfalten können. Die folgenden Kriterien helfen bei der Bewertung:

- Wird eine **Bedrohung mit hoher Priorität** gemäß der Bewertung im vorangegangenen Abschnitt adressiert?
- Werden **signifikante Verbesserungen** erzielt?
- Was sind die dazu **notwendigen Aufwände**, wie beispielsweise zusätzliche nötige Prozesse oder Systeme, oder sich wiederholende Kosten und Entwicklungsaufwände bzw. Design-Komplexität (abgesehen von einmaligen Forschungsaufwänden)?

Die Bewertung anhand dieser Kriterien und deren Zusammenfassung erlaubt einen (positiven) **Gesamteffekt** einzelner Lösungsansätze auf vertrauenswürdige Elektronik zu schätzen.

4.1 Einordnung von ZEUS-Forschungsprojekten

Im Folgenden werden die im Rahmen der Förderbekanntmachung ZEUS vom BMBF geförderten Forschungsprojekte kurz dargestellt und anhand der obigen Kriterien diskutiert. An dieser Stelle ist hervorzuheben, dass die Darstellung ausschließlich anhand der hier definierten Gesichtspunkte der Vertrauenswürdigkeit erfolgt und Forschungsprojekte naturgemäß häufig darüber hinaus in andere Richtungen wertvolle Beiträge liefern.

Die Diskussion erfolgte durch Fachexperten nach bestem Wissen und Gewissen und wurde durch Vertreter der Forschungsprojekte begutachtet. Die Darstellung ist abstrahiert, sodass naturgemäß nicht jede Facette der Projekte detailliert dargestellt wird. Die Forschung an diesen Lösungsansätzen ist zudem noch nicht abgeschlossen und Themen werden unterschiedlich breit durch die Ansätze abgedeckt. Das gewählte Abstraktionsniveau soll trotzdem helfen, einen Überblick darüber zu erlangen, welche Bedrohungen für vertrauenswürdige Elektronik noch nicht ausreichend adressiert sind und gewissermaßen Lücken darstellen.

VE-FIDES: Know-how-Schutz und Identifizierbarkeit von Elektronikkomponenten für vertrauenswürdige Produktionsketten. Das Projekt VE-FIDES[14] beschäftigt sich mit der Verbesserung der Lieferkettensicherheit, indem Echtheitsmerkmale in Platinen und in Chips eingebracht werden, sodass diese jeweils einzeln, aber auch nach dem Zusammenfügen als System eindeutig identifiziert werden können. Außerdem werden neue Logic-Locking- und Chip-Obfuskations-Methoden erforscht und deren Robustheit gegen Reverse-Engineering untersucht.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierten Bedrohungen für Vertrauenswürdigkeit durch Grau-Markt-Hardware in allen Schritten der Wertschöpfungskette nach Chip-Fertigung (inkl. Diebstahl geistigen Eigentums) (Bedrohungen (9) und (10) in Tabelle 2).

- *Werden signifikante Verbesserungen erzielt?*

  Die Kombination aus verschiedenen Echtheitsmerkmalen in unterschiedlichen elektronischen Teil-Komponenten bietet ein hohes Maß an Sicherheit, da viele Teile eines Geräts darin eingeschlossen sind. Erkenntnisse zu den Möglichkeiten durch Reverse-Engineering helfen, die Bedrohung besser einzuschätzen.

- *Sind hohe Aufwände zu erwarten?*

  Die Integration von Echtheitsmerkmalen in alle relevanten Chips und ihren Designs erhöht die Entwicklungs- und Qualitätssicherungsaufwände (insbesondere für Echtheitsmerkmale durch Physical Unclonable Functions) eines jeden Teils signifikant.

  Logic-Locking verhindert den Diebstahl geistigen Eigentums nur, wenn man voraussetzt, dass Kontrahenten mit nötigen Reverse-Engineering-Fähigkeiten keinen Zugang zu Exemplaren aus dem Feld haben, die entsprechende Schlüssel enthalten. Das Szenario scheint unrealistisch. Es scheint aber sinnvoll, die Grenzen solcher Methoden auszumachen.

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Der mögliche positive Gesamteffekt ist hoch, aber Aufwände für notwendige Echtheitsmerkmale scheinen ebenso signifikant.

VE-HEP: Vertrauen durch Transparenz: Methoden und Werkzeuge für das Design quelloffener, vertrauenswürdiger Prozessoren. Im Projekt VE-HEP[15] wird ein Open-Source-Mikrokontroller entwickelt, der gegen physikalische Implementierungsangriffe mittels weiterentwickelten Open-Source-EDA-, Härtungs- und Verifikations-Tools gehärtet wird.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierten Bedrohungen für Vertrauenswürdigkeit durch unbeabsichtigte Schwachstellen in den Schritten Konzept / Spezifikation und Chip-Entwicklung (Bedrohung (1) in Tabelle 2).

- *Werden signifikante Verbesserungen erzielt?*

  Jegliche Open-Source-Designs und -Tools verbessern die Aussichten auf Vertrauenswürdigkeit, weil sie jederzeit eingehend begutachtet werden können. Darüber hinaus ist ein positiver Effekt auf technologische Souveränität zu verzeichnen, da außerdem die Abhängigkeiten von kommerziellen Anbietern einen Schritt reduziert wird.

[14] https://www.elektronikforschung.de/projekte/ve-fides
[15] https://www.elektronikforschung.de/projekte/ve-hep

- *Sind hohe Aufwände zu erwarten?*

  Die Ergebnisse reduzieren Entwicklungsaufwände durch Tools und Automatisierung sowie durch zugängliche Designs, sodass generell die Auswahlmöglichkeiten steigen. Die Anwendung von Open-Source-EDA-Tools könnte in einigen Fällen allerdings zu Mehraufwänden aufgrund geringerer Reife führen.

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Der mögliche positive Gesamteffekt ist hoch.

VE-CirroStrato: Neuartige rekonfigurierbare Transistoren für den Know-how-Schutz von Elektronikkomponenten. Das Projekt VE-CirroStrato[16] strebt an, in Chip-Fertigungsprozessen konfigurierbare Transistoren bzw. logische Zellen zu entwickeln, sodass die Funktionalität einer Schaltung selbst vor der Fabrik geheim gehalten werden kann, die naturgemäß alle Maskendaten sieht, solange der entsprechende Konfigurationsschlüssel erst im Feld hineingeladen wird.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierte Bedrohung der Vertrauenswürdigkeit durch Diebstahl geistigen Eigentums während der Chip-Fertigung (Bedrohung (9) in Tabelle 2).

- *Werden signifikante Verbesserungen erzielt?*

  Ähnlich wie Logic-Locking ist das Design (Maskendaten) ohne Schlüssel im besten Fall wertlos.

- *Sind hohe Aufwände zu erwarten?*

  Der Schutz verliert jegliche Wirkung, sobald ein einziges Gerät aus dem Feld inklusive des Konfigurationsschlüssels einem Kontrahenten wie einer Chip-Fabrik zugänglich ist, da dieser dann in der Lage ist, den Schlüssel zu extrahieren (ähnlich wie Logic-Locking). Der Lösungsansatz erfordert die zusätzliche Entwicklung von dedizierten Transistoren und Zellen in jeder neuen zu schützenden Technologie, was einen hohen Aufwand erfordert (ähnlich zur Entwicklung einer CMOS-Bibliothek).

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Eine relevante Bedrohung wird adressiert. Die Ergebnisse der Forschung werden zeigen, ob die Aufwände im Verhältnis zum Nutzen den Ansatz attraktiv machen.

VE-REWAL: Know-how-Schutz für vertrauenswürdige heterogene Elektroniksysteme mit Chiplets. Das Projekt VE-REWAL[17] beschäftigt sich damit, die Funktionalität von Chips in mehrere Teile, sogenannte Chiplets, aufzuteilen, die innerhalb eines Chip-Package anhand von Interposern verbunden werden. Die Aufteilung soll helfen, den Diebstahl geistigen Eigentums zu verhindern, da kein Teil allein die gesamte Funktionalität abbildet und ein Angreifer beispielsweise nur Zugriff auf eine Fabrik hätte.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierte Bedrohung für Vertrauenswürdigkeit durch Diebstahl geistigen Eigentums während der Chip-Fertigung (Bedrohung (9) in Tabelle 2).

[16] https://www.elektronikforschung.de/projekte/ve-cirrostrato
[17] https://www.elektronikforschung.de/projekte/ve-rewal

- *Werden signifikante Verbesserungen erzielt?*

  Die Integration von Teil-Chips im Chip-Package ist aufgrund der starken Spezialisierung von Fabriken vorteilhaft und nimmt an Bedeutung zu. Es können Teil-Chips aus unterschiedlich spezialisierten Technologien integriert werden.

- *Sind hohe Aufwände zu erwarten?*

  Um signifikante Auswirkungen auf den Schutz des geistigen Eigentums zu erzielen, müsste Funktionalität voraussichtlich auf unterschiedliche Fabriken mit ähnlichen Technologien aufgeteilt werden, sodass der Vorteil der ursprünglichen Motivation für die Aufteilung entfiele. Die entsprechende Hinzunahme weiterer Fabrikationsstätten würde signifikante Aufwände erfordern.

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Eine relevante Bedrohung wird adressiert. Ein Mehrwert besteht nur, solange Angreifer nicht auf das finale Produkt zugreifen können.

VE-ASCOT: Neuartige sichere Elektronikkomponenten für die Chain of Trust. Das Projekt VE-ASCOT[18] strebt einen Beitrag zur Lieferkettensicherheit und zur Inbetriebnahme von Elektronik an, indem Vertrauensanker-Chips integriert werden, sodass diese authentisch identifiziert und anhand eines Hintergrundsystems verfolgt werden können. Dazu wird eine Software-Infrastruktur inklusive Datenbank erstellt.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierten Bedrohungen für Vertrauenswürdigkeit durch Grau-Markt-Hardware (Bedrohung (10) in Tabelle 2).

- *Werden signifikante Verbesserungen erzielt?*

  Die Möglichkeit, Authentizität von elektronischen Geräten anhand kryptographischer Methoden und mithilfe einer Hintergrundinfrastruktur verlässlich prüfen zu können, erschwert Fälschungen.

- *Sind hohe Aufwände zu erwarten?*

  Ein dedizierter zusätzlicher Vertrauensanker-Chip muss auf der Platine in jedes Gerät integriert werden. Die benötigte Infrastruktur muss betrieben werden und alle Beteiligten in Platinen-Fertigung und -bestückung müssen vertrauenswürdig sein, da dort der Zusatzchip mit dem Gerät verbunden wird. Dies trägt nach der Integration dazu bei, Fälschungen von Geräten zu unterbinden, verhindert davor allerdings keine Grau-Markt-Chips.

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Der Ansatz ist überzeugend auf Geräte-Ebene, deckt aber Bedrohungen durch Grau-Markt-Chips nicht ab.

VE-SAFE: Verhinderung von Angriffen auf Elektroniksysteme durch innovative Multi-Sensorik. Das Projekt VE-SAFE[19] strebt an, elektronische Geräte gegen Tampering-Angriffe und Seitenkanalangriffe zu schützen, indem mehrere Sensoren in Platinen anhand fortschrittlicher Fertigungsverfahren integriert werden. Außerdem werden Möglichkeiten zur gezielten Zerstörung im Angriffsfall untersucht.

[18] https://www.elektronikforschung.de/projekte/ve-ascot
[19] https://www.elektronikforschung.de/projekte/ve-safe

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierten Bedrohungen für Vertrauenswürdigkeit durch Ausnutzung von unbeabsichtigten Schwachstellen im Feld (Bedrohung (3) in Tabelle 2) u.a. durch das Erschweren von Reverse-Engineering von Exemplaren aus dem Feld.

- *Werden signifikante Verbesserungen erzielt?*

  Die Sensorik verspricht Schutz gegen Angriffe. Anstatt in der aufwändigen Chip-Entwicklung anzusetzen, müssen nur die Platinen modifiziert bzw. ergänzt werden. Funktionen zum Löschen sensibler Daten im Angriffsfall bedürfen aber Vorkehrungen im Chip.

- *Sind hohe Aufwände zu erwarten?*

  Die Modifikationen der Platinen erfordern moderate Aufwände und es werden zusätzliche Sensoren benötigt. Diese Sensoren müssen initial und wahrscheinlich während des Betriebs laufend kalibriert werden, um effektiv gegen Angriffe zu schützen.

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Das Projekt adressiert wichtige Angriffe im Feld. Die Forschungsergebnisse werden zeigen, inwieweit das Erkennen von Angriffen tatsächlich effektiv ist. Aufwände für zusätzliche Komponenten und Modifikationen sowie Kalibrierung usw. sind zu beachten.

VE-DIVA-IC: Neuartige Designmethoden für vertrauenswürdige Elektronikschaltungen. Das Projekt VE-DIVA-IC[20] beschäftigt sich mit sicheren analogen und digitalen Designs (z. B. gehärtete offene Prozessoren, geschützte analoge Schnittstellen und Systemsicherheitsmaßnahmen wie Software-Attestierung) und mit Tools für formale und empirische Verifikation z. B. gegen Seitenkanalangriffe und Hardware-Trojaner.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierte Bedrohung für Vertrauenswürdigkeit durch unbeabsichtigte Schwachstellen während Konzept / Spezifikation und Chip-Entwicklung und ihrem Betrieb im Feld (Bedrohungen (1) und (3) in Tabelle 2)

- *Werden signifikante Verbesserungen erzielt?*

  Fortschritte in Form von offenen Designs und Tooling können zielführend unbeabsichtigte Schwachstellen reduzieren.

- *Sind hohe Aufwände zu erwarten?*

  Tool-basierte Verifikation in der Entwicklung erfordert relativ geringe Zusatzaufwände.

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Der mögliche positive Gesamteffekt ist hoch, da Tooling und offene Designs breit eingesetzt werden könnten.

VE-CeraTrust: Verhinderung von Angriffen auf Elektroniksysteme durch neuartige keramische Mehrlagensysteme. Das Projekt VE-CeraTrust[21] will einzigartige Identifikationsmerkmale in verschiedene Arten von Platinen, Subsysteme und Packages einbringen, die teilweise mit neuen keramischen Verfahren aufgebaut sind. Das ermöglicht, die darauf aufbauenden Teile und Geräte an verschiedenen Stellen der Lieferkette authentisch zu identifizieren.

[20] https://www.elektronikforschung.de/projekte/ve-diva-ic
[21] https://www.elektronikforschung.de/projekte/ve-ceratrust

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierten Bedrohungen für Vertrauenswürdigkeit durch Grau-Markt-Hardware entlang der Lieferkette (Leiterplatten, Subsysteme, Packages) (Bedrohungen (9) und (10) in Tabelle 2).

- *Werden signifikante Verbesserungen erzielt?*

  Die genannten Bauteile sind integrale Bestandteile von Elektronik, sodass das Sicherstellen ihrer Authentizität Fälschungen in der Lieferkette erschwert.

- *Sind hohe Aufwände zu erwarten?*

  Der Lösungsansatz erfordert Modifikationen in allen genannten Bauteilen und die Integration entsprechender Merkmale sowie Möglichkeiten, diese auszulesen. Die Stabilität der Merkmale zu garantieren, erfordert Aufwand in der Qualitätssicherung. Das initiale Auslesen muss in vertrauenswürdiger Umgebung vorgenommen werden. Ein Hintergrundsystem zum Abgleich der Merkmale muss betrieben und gesichert werden.

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Der Schutz von Platinen, Subsystemen und Packages gegen Fälschungen entlang der Lieferkette ist vorteilhaft, wenn auch mit gewissen Aufwänden verbunden. Andere Bedrohungen durch den Grau-Markt wie gefälschte Chips sind nicht Teil der Betrachtung.

VE-Jupiter: Eindeutige Identifizierbarkeit für vertrauenswürdige Mikroelektronik mit Chiplets. Das Projekt VE-Jupiter[22] zielt darauf ab, Echtheitsmerkmale in der Form von Physical Unclonable Functions in Chips zu integrieren, um ihre Authentizität nachzuweisen und um Design-Manipulationen zu erkennen. Außerdem integriert das Projekt Vertrauensanker und weitere Isolationsmechanismen in Designs, um Angriffe zu verhindern.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Das Projekt adressiert die mittel priorisierte Bedrohung für Vertrauenswürdigkeit durch Hintertüren in späten Phasen der Chip-Entwicklung (Bedrohung (6) in Tabelle 2) und die hoch priorisierten Bedrohungen durch Grau-Markt-Hardware für alle Schritte nach der Chip-Fertigung (Bedrohungen (9) und (10) in Tabelle 2) sowie die hoch priorisierte Bedrohung durch Ausnutzen von unbeabsichtigten Schwachstellen im Feld (Bedrohung (3) in Tabelle 2).

- *Werden signifikante Verbesserungen erzielt?*

  Die Zusatzschaltungen der Echtheitsmerkmale erlauben das Prüfen der Authentizität in der Wertschöpfungskette nach dem initialen Auslesen. Vertrauensanker und Isolationsmechanismen erhöhen die Sicherheit.

- *Sind hohe Aufwände zu erwarten?*

  Die Echtheitsmerkmale in Form von Physical Unclonable Functions setzen signifikante Aufwände für die Qualifizierung und das Sicherstellen der korrekten Funktionalität und Qualität voraus. Außerdem wird ein Hintergrundsystem mit Datenbank zum Hinterlegen und Vergleich der Merkmale benötigt, die für alle relevanten Akteure in der Wertschöpfungskette gesichert zugänglich ist. Das initiale Auslesen muss in einer sicheren Umgebung stattfinden. Ein Schutz gegen Design-Manipulationen würde sehr präzise Simulationen erfordern.

[22] https://www.elektronikforschung.de/projekte/ve-jupiter

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Die Lösungsansätze gegen unbeabsichtigte Schwachstellen sind vielversprechend. Die Lösungsansätze gegen Bedrohungen durch Grau-Markt-Hardware bringen nicht unerhebliche Aufwände mit sich.

VE-ARiS: Elektronischer Know-how-Schutz für innovative Sensorsysteme. Das Projekt VE-ARiS[23] hat zum Ziel, geistiges Eigentum in Chips und Platinen gegen Diebstahl durch Reverse-Engineering und darauffolgendes Klonen zu schützen. Dazu werden Obfuskations-Methoden von Chip-Designs und Möglichkeiten der Zersetzung sowie Wasserzeichen für die Produktion untersucht.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierten Bedrohungen für Vertrauenswürdigkeit durch Grau-Markt-Hardware in allen Phasen nach Chip-Fertigung (Bedrohungen (9) und (10) in Tabelle 2), indem der Diebstahl geistigen Eigentums erschwert wird.

- *Werden signifikante Verbesserungen erzielt?*

  Das Erschweren von Reverse-Engineering ist positiv zu bewerten, wenn auch unklar bleibt, wie hoch der Schutz letztlich ist.

- *Sind hohe Aufwände zu erwarten?*

  Die Maßnahmen erfordern signifikante Modifikationen am Chip-Design-Flow und der Platinenfertigung.

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Die Lösungsansätze erschweren den Diebstahl geistigen Eigentums, wobei dies in Abhängigkeit von den Fähigkeiten der Kontrahenten steht. Andere Bedrohungen durch Grau-Markt-Chips wie Überproduktion werden nicht betrachtet.

VE-VIDES: Designmethoden und HW/SW-Co-Verifikation für Identifizierbarkeit von Elektronikkomponenten. Das Projekt VE-VIDES[24] beschäftigt sich damit, EDA-Tools und Design-Flows, wie beispielsweise formale Verifikationsmethoden, zu verbessern, um Schutzmaßnahmen gegen Angriffe automatisiert zu integrieren. Außerdem werden elektronische Echtheitsmerkmale in MEMS Chips betrachtet.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Ja, das Projekt adressiert die hoch priorisierten Bedrohungen für Vertrauenswürdigkeit durch unbeabsichtigte Schwachstellen während Konzept / Spezifikation und Chip-Entwicklung (Bedrohung (1) in Tabelle 2). Die Echtheitsmerkmale adressieren die hoch priorisierten Bedrohung durch Grau-Markt-Hardware (Bedrohung (9) in Tabelle 2).

- *Werden signifikante Verbesserungen erzielt?*

  Automatisierte und tool-basierte Ansätze können viele Designs positiv beeinflussen.

- *Sind hohe Aufwände zu erwarten?*

  Die mit der Anwendung von Tools verbundenen Aufwände sind verhältnismäßig gering. Die Echtheitsmerkmale erfordern Aufwände zur Qualitätssicherung, Hintergrundsysteme und das initiale Auslesen in einer sicheren Umgebung.

[23] https://www.elektronikforschung.de/projekte/ve-aris
[24] https://www.elektronikforschung.de/projekte/ve-fides

- *Gesamteffekt auf vertrauenswürdige Elektronik*: Die Lösungsansätze auf Basis automatisierter Tools adressieren hoch priorisierte Bedrohungen für Vertrauenswürdigkeit. Die Echtheitsmerkmale stehen im Spannungsfeld zwischen Aufwand und Nutzen (siehe auch VE-FIDES und VE-Jupiter).

VE-Silhouette: Heterogene Photonik-Elektronik-Plattform für vertrauenswürdige quelloffene Prozessoren. Das Projekt VE-Silhouette[25] beschäftigt sich damit, die Schnittstellen zwischen Photonik-Elektronik und elektronischen Schaltungen (beispielsweise Open-Source-Prozessoren) zu schaffen, um diese zu integrieren. Das Projekt behandelt auch die gemeinsame Fertigung der beiden unterschiedlichen Technologien.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Während die Inhalte sinnvoll scheinen, werden Bedrohungen für die Vertrauenswürdigkeit von Elektronik (siehe Tabelle 2) nicht adressiert.

- *Werden signifikante Verbesserungen erzielt?* (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)
- *Sind hohe Aufwände zu erwarten?* (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)
- *Gesamteffekt auf vertrauenswürdige Elektronik*: (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)

VE-sensIC: Eindeutige Identifizierbarkeit für vertrauenswürdige Hybrid-Sensorelektronik mit Hilfe additiver Fertigung. Das Projekt VE-sensIC[26] beschäftigt sich mit der Integration von Sensoren (z. B. für Temperatur) in Plastikschläuchen zur Detektion von Betriebsfehlern. Dabei werden auch Identifikationsmerkmale in Schläuche integriert.

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Während die Inhalte sinnvoll scheinen, werden Bedrohungen für die Vertrauenswürdigkeit von Elektronik (siehe Tabelle 2) nicht adressiert.

- *Werden signifikante Verbesserungen erzielt?* (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)
- *Sind hohe Aufwände zu erwarten?* (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)
- *Gesamteffekt auf vertrauenswürdige Elektronik*: (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)

VE-TRUST-E: Vertrauenswürdige Sensorsysteme für mobile und industrielle Anwendungen. Im Rahmen des Projekts VE-TRUST-E[27] befasst man sich damit, maschinelle Lernverfahren in Chips für Sensoren zu integrieren, sodass in verschiedenen Anwendungsdomänen Daten direkt am Sensor verarbeitet werden können, dort Entscheidungen getroffen werden können und die notwendige Datenübertragung reduziert wird.

[25] https://www.elektronikforschung.de/projekte/ve-silhouette
[26] https://www.elektronikforschung.de/projekte/ve-sensic
[27] https://www.edacentrum.de/trust-e/

- *Wird eine Bedrohung mit hoher Priorität adressiert?*

  Während die Inhalte sinnvoll scheinen, werden Bedrohungen für die Vertrauenswürdigkeit von Elektronik (siehe Tabelle 2) nicht adressiert.

- *Werden signifikante Verbesserungen erzielt?* (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)
- *Sind hohe Aufwände zu erwarten?* (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)
- *Gesamteffekt auf vertrauenswürdige Elektronik*: (Nicht relevant, da Vertrauenswürdigkeit nicht direkt adressiert wird.)

4.2 Vorläufige Identifikation von Lücken

Die beschriebenen Projekte werden im Folgenden den Bedrohungen zugeordnet, die sie adressieren. Dies erlaubt eine Identifikation von Bedrohungen mit hoher Priorität, die bisher in geringem Maße durch ZEUS-Forschungsprojekte adressiert werden. Dazu wird Tabelle 2 entsprechend ergänzt, sodass daraus Tabelle 3 folgt. Die Analyse dieser Tabelle 3 zeigt:

1. **Die meisten hoch priorisierten Bedrohungen für vertrauenswürdige Elektronik werden sogar durch mehrere Projekte adressiert**. Die ZEUS-Projekte adressieren fast ausschließlich Bedrohungen, die anhand der Analyse als hoch und damit sehr relevant eingestuft wurden.
2. Die Bedrohung (7) „beabsichtigte Hintertüren z. B. durch implantierte HW-Trojaner-Chips und FW“ in späten Schritten der Wertschöpfungskette, **Platinen- und Elektronik-Entwicklung, Platinenfertigung und -bestückung, Auslieferung** und **Betrieb im Feld** wird nur in einem der Projekte adressiert. Hier zeigt sich trotz der stark abstrahierten Betrachtung eine potenzielle Lücke in der Abdeckung der Bedrohungen.
3. Außerdem sind einige Lücken bei Bedrohungen festzustellen, die als mittel priorisiert wurden. Diese Bedrohungen sollten weiterhin beobachtet werden, um festzustellen, ob sich beispielsweise die Einschätzung der Rahmenbedingungen (z. B. notwendige Aufwände der Kontrahenten) und damit die Bewertung in Zukunft ändern.

Naturgemäß ist diese Sicht abstrahiert und es kann an dieser Stelle nicht im Detail analysiert werden, inwiefern einzelne Lösungsansätze eine ausreichende Abdeckung gewähren oder ob Lösungen aus anderen Forschungsvorhaben alternativ ausreichend wirken. Außerdem wird in dieser abstrahierten Ansicht nicht berücksichtigt, ob Lösungsansätze beispielsweise besonders aufwändig sind. Nichtsdestotrotz liefert die Übersicht erste Ansätze, welche Bedrohungen stärker adressiert werden könnten.

Tabelle 3: Einschätzung der Prioritäten von Bedrohungen für vertrauenswürdige Elektronik

Gruppierte Bedrohungen nach Elementen der Wertschöpfungskette	Geschätzte **Priorität**	Adressiert in ZEUS-Projekt
Schwachstellen (unbeabsichtigt) in Wertschöpfungskette:		
(1) **Konzept / Spezifikation** und **Chip-Entwicklung**	**hoch**	VE-VIDES VE-DIVA-IV VE-HEP
(2) **Platinen- und Elektronik-Entwicklung**	mittel	
(3) **Betrieb im Feld** (Angriffe)	**hoch**	VE-Jupiter VE-DIVA-IC VE-SAFE
Hintertüren (beabsichtigt) in Wertschöpfungskette		
(4) **Konzept / Spezifikation** (z. B. bei Standardisierung)	mittel	
(5) **Chip-Entwicklung** (z. B. ausgelagert)	mittel	
(6) **Chip-Entwicklung** (Design-Flow) und **Chip-Fertigung** (z. B. Tool-basiert, Maskenmanipulation)	nieder	VE-Jupiter
(7) **Platinen- und Elektronik-Entwicklung**, **Platinenfertigung und -bestückung**, **Auslieferung** und **Betrieb im Feld** (z. B. implantierte HW-Trojaner und FW)	**hoch**	VE-FIDES
Grau-Markt-Hardware in Wertschöpfungskette:		
(8) **Chip-Entwicklung** und **Platinen- und Elektronik-Entwicklung** (z. B. Diebstahl geistigen Eigentums)	mittel	
(9) **Chip-Fertigung** und **Nutzungsende** (z. B. Überproduktion, Nutzung von Ausschussware und Recycling sowie Diebstahl geistigen Eigentums)	**hoch**	VE-Aris VE-Jupiter VE-CeraTrust VE-REWAL VE-CirroStrato VE-FIDES
(10) **Logistik und Lieferkette**, **Platinenfertigung und -bestückung**, **Auslieferung** und **Betrieb im Feld** (Eintritt aus Grau-Markt)	**hoch**	VE-ARis VE-Jupiter VE-CeraTrust VE-ASCOT VE-FIDES

5 Zusammenfassung und Ausblick

Der Vertrauenswürdigkeit von Elektronik wird häufig eine große Bedeutung zugemessen. Dabei werden verschiedene Themen wie Vertrauenswürdigkeit, IT-Sicherheit, technologische Souveränität und weitere Forschung im Zuge des allgemeinen technologischen Fortschritts manchmal vermengt. Die Definition in Kapitel 1 sowie die systematisierte Darstellung der Bedrohungen für Vertrauenswürdigkeit einschließlich der Beispiele in Kapitel 2 helfen bei der begrifflichen Einordnung.

Welche Forschungsansätze können die Vertrauenswürdigkeit von Elektronik verbessern? Forschung kann unter verschiedenen Gesichtspunkten Beiträge zur *Vertrauenswürdigkeit von Elektronik* leisten. Dabei helfen die drei Kriterien aus Kapitel 4, die Wirksamkeit von Ansätzen einzuschätzen:

- *Wird eine **hoch priorisierte Bedrohung** für Vertrauenswürdigkeit adressiert (gem. Kapitel 2)?*
- *Werden **signifikante Verbesserungen** erzielt?*
- *Was sind die dazu **notwendigen Aufwände** wie beispielsweise zusätzlich nötige Prozesse oder Systeme oder sich wiederholende Kosten und Entwicklungsaufwände bzw. Design-Komplexität (abgesehen von einmaligen Forschungsaufwänden)?*

Die sich wiederholenden Kosten von Lösungsansätzen in der Produktion oder für den Betrieb zusätzlicher IT-Infrastruktur werden in der Forschung häufig zu wenig beachtet, sind aber für eine Umsetzung in der Wirtschaft ausschlaggebend. Denn Vertrauenswürdigkeit ist für Elektronik und Unternehmen zwar grundlegend, dennoch bleibt es schwierig, die damit verbundenen Kosten am Markt angemessen einzupreisen. Insofern ist es ratsam, immer zumindest eine oberflächliche Abschätzung der Aufwände und Kosten anzustellen, insbesondere wenn Forschungsansätze miteinander verglichen werden. Besonders attraktiv sind Forschungsrichtungen, die auf der einen Seite die Vertrauenswürdigkeit steigern und auf der anderen Seite zusätzlich auch einen Beitrag zu technologischer Souveränität oder dem allgemeinen technologischen Fortschritt leisten. Die Forschung an Open-Source-Tools und -Designs ist ein Beispiel dafür.

Welche Bedrohungen finden zu wenig Beachtung? Die Analyse der Bedrohungen in Tabelle 2 und der Vergleich mit den ZEUS-Projekten zeigt:

- **Unbeabsichtigte Schwachstellen in Chips** stellen Bedrohungen dar, aber **hauptsächlich in frühen Entwicklungsschritten**.

  Ansätze wie Open-Source-Hardware-Designs und tool-basierte Schutzmaßnahmen adressieren diese Risiken, verursachen wenig Zusatzaufwände und haben einen positiven Einfluss auf technologische Souveränität. Einige ZEUS-Projekt behandeln diese Aspekte.

- **Grau-Markt-Hardware** scheint insbesondere aufgrund illegaler Überproduktion, Nutzung von Ausschussware und illegalem Recycling hoch problematisch. Dazu wird illegales Klonen nach Reverse-Engineering auch häufig im Feld beobachtet.

  Einige Lösungsansätze adressieren diese Risiken. Ein Beispiel ist die Einbringung von Echtheitsmerkmalen. Allerdings sind die damit verbundenen Aufwände (z .B. Qualitätssicherung eines zusätzlichen Merkmals oder Kosten eines Zusatzchips) und die Einschränkungen (z. B. Notwendigkeit einer vertrauenswürdigen Fabrik) nachteilig. Hier sollte der Fokus auf Lösungsansätzen mit möglichst geringen Aufwänden liegen.

- **Beabsichtigte Hintertüren** sind ausgesprochen relevant, **aber erst in späten Schritten der Wertschöpfungskette** (z. B. als implantierte Hardware-Trojaner Chips).

Dieses Thema wird von den laufenden ZEUS-Projekten weniger intensiv adressiert. Existierende Bildgebungsverfahren eigen sich zwar für die automatisierte Prüfung von Elektronik, erfordern allerdings hohe Aufwände. Echtheitsmerkmale schützen bisher kaum vor Implantaten und sind auch mit erheblichen Aufwänden verbunden.

Welche Impulse ergeben sich darüber hinaus? Die Diskussionen in den Gremien und Workshops des Projekts Velektronik mit Teilnehmern aus Forschung und Wirtschaft ergaben zusätzliche Impulse:

- **Open-Source-Hardware / RISC-V**: Die zunehmende Popularität der Open-Source RISC-V Architekturspezifikation und der darauf aufbauenden Hardware-Designs und Tools sind wahrscheinlich stark getrieben von Gesichtspunkten wie dem allgemeinen technologischen Potential, der Technologiesouveränität und dem Willen zur Abkehr von proprietären Prozessortechnologien, die in der Hand einzelner Unternehmen sind. Wie im Bereich der Betriebssysteme, wo Open-Source-Linux eine ausgesprochen hohe Bedeutung erlangt hat, scheint sich nun im Bereich der Hardware-Prozessoren etwas Grundlegendes zu verändern. Der potenzielle Gewinn an Vertrauenswürdigkeit durch Open-Source-Hardware-Designs (bessere Möglichkeiten der Begutachtung von Designs und schnellere Entwicklungszyklen für Sicherheitsverbesserungen) steht zwar weniger im Vordergrund, die gesamte Entwicklung ist – aus eben diesen Gründen – jedoch in hohem Maß vorteilhaft für die Vertrauenswürdigkeit von Elektronik. Forschung in diese Richtung ist daher aus vielen Gründen attraktiv.
- **Fertigungsprozesse, analoge Open-Source-Hardware und Design-Tools**: Digitale Open-Source-Hardware, beispielsweise auf der Basis der Open-Source RISC-V Architektur, wird an vielen Stellen in den Vordergrund gestellt. Darüber hinaus sind für einen funktionierenden Chip aber eine Reihe zusätzlicher Schaltungsblöcke notwendig, wie Analog/Digital-Wandler, Schnittstellen, Speicher, Sensoren usw. In diesem Bereich werden bisher wenige Forschungsergebnisse als Open-Source veröffentlicht. Die Forschung ist in dem Bereich zudem dahingehend allgemein eingeschränkt, dass sowohl Tool-Lizenzen als auch die für die Designs notwendigen Fertigungsparameter der Chip-Technologien, sogenannte *Process Design Kits,* üblicherweise einer Geheimhaltung unterliegen und daher keine Ergebnisse veröffentlicht werden dürfen. Eine eventuell geförderte Veränderung dieser Rahmenbedingungen, beispielsweise durch offenere *Process Design Kits* sowie Open-Source-Design-Tools, würde mehr Forschung an diesen wesentlichen Schaltungsteilen ermöglichen.
- **Lücke zwischen Open-Source-Design und gefertigtem Chip:** Selbst wenn ein (digitales) Design Open-Source ist, bleiben wesentliche darauffolgende Schritte in der Wertschöpfungskette aus den zuvor genannten Gründen geschlossen. Es gibt bisher wenig attraktive Lösungen, um einen Nachweis zu führen, dass gefertigte Chips wirklich bestimmten Open-Source-Designs entsprechen. Bildgebung und Stichproben-basierte Lösungen sind sehr aufwändig und scheinen daher nicht besonders attraktiv. Hier besteht eine Lücke, die bisher zu wenig adressiert wird. Offene Chip-Fertigungsprozesstechnologien (*Process Design Kits*) würden erlauben, Informationen wie Maskendaten offenzulegen und mehr Möglichkeiten zur Nachweisführung schaffen.
- **Heterogene Integration, Chiplets und Split-Manufacturing**: Heterogene Integration, also die Integration von Silizium-Chip-Teilen (Chiplets) aus verschiedenen Technologien und Fabriken ist aus wirtschaftlichen Gründen sehr relevant. Hier scheint ein stärkerer Forschungsfokus zur Steigerung der Vertrauenswürdigkeit und IT-Sicherheit vorteilhaft.

  Split Manufacturing als Ansatz, um Vertrauenswürdigkeit zu steigern, indem der Diebstahl geistigen Eigentums und das Einbringen von Hintertüren erschwert wird, scheint erhebliche negative Auswirkungen auf die Wirtschaftlichkeit von Elektronikfertigung zu haben. Die Schutzwirkung ist auch begrenzt, da der fertige Chip im Feld zugänglich ist

und die Aufteilung der Fertigung auch neue Angriffspunkte in Organisationen und Prozessen bietet. Der Ansatz scheint vorwiegend für Nischenanwendungen attraktiv.

- **Echtheitsmerkmale**: Die Forschung an Echtheitsmerkmalen klammert häufig die erheblichen Aufwände aus, die mit der Umsetzung derselben verbunden sind. Das Gewährleisten der Qualität von Merkmalen, die aus Fertigungsschwankungen abgeleitet werden, erfordert wiederholt große Aufwände. Abgesehen davon scheint für eine praktische Umsetzung die Standardisierung und internationale Vereinheitlichung von Hintergrundinfrastruktur zum Ablegen und Abgleich von Merkmalen notwendig zu sein. All dies stellt eine große Hürde dar.
- **Zero Trust**: Eine Übertragung des zunehmend populären Begriffs ‚Zero Trust' auf den Bereich der Elektronik könnte bedeuten, dass die Vertrauenswürdigkeit hauptsächlich durch technologische Maßnahmen – seien es wirkungsvolle Schutzmaßnahmen oder aussagekräftige Prüfverfahren – gesichert werden sollte und weniger durch organisatorische Maßnahmen wie beispielsweise vertragliche Garantien geschützt ist. In diesem Zusammenhang könnte man interpretieren, dass IT-Sicherheit als Teil der Vertrauenswürdigkeit möglichst wenig durch das vorgeschriebene Geheimhalten von Information gewährleistet werden sollte. Wichtige Zertifizierungsverfahren wie Common Criteria messen der Geheimhaltung bisher aber eine hohe Bedeutung bei und stützen sich stark auf organisatorischen Aspekten und Prozessen. Open-Source-Designs versuchen hingegen, IT-Sicherheit bei voller Transparenz zu gewährleisten, was langfristig vorteilhafter sein könnte.

6 Referenzen

[1] Georg T Becker, Francesco Regazzoni, Christof Paar, and Wayne P Burleson. Stealthy dopant-level hardware trojans. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 197–214. Springer, 2013.

[2] Swarup Bhunia, Michael S. Hsiao, Mainak Banga, and Seetharam Narasimhan. Hard- ware trojan attacks: Threat analysis and countermeasures. *Proceedings of the IEEE*, 102(8):1229–1247, 2014.

[3] Nisha Jacob, Dominik Merli, Johann Heyszl, and Georg Sigl. Hardware trojans: current challenges and approaches. *IET Comput. Digit. Tech.*, 8(6):264–273, 2014.

[4] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, et al. Spectre attacks: Exploiting speculative execution. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1–19. IEEE, 2019.

[5] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. Meltdown: Reading kernel memory from user space. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 973–990, Baltimore, MD, August 2018. USENIX Association.

[6] Johannes Obermaier, Marc Schink, and Kosma Moczek. One exploit to rule them all? on the security of drop-in replacement and counterfeit microcontrollers. In *14th {USENIX} Workshop on Offensive Technologies ({WOOT} 20)*, 2020.

[7] Jordan Robertson and Robertson Riley. How china used a tiny chip to infiltrate u.s. companies, 2018.

[8] Jordan Robertson and Robertson Riley. The long hack: How china exploited a u.s. tech supplier, 2021.

[9] Marc Schink, Alexander Wagner, Florian Unterstein, and Johann Heyszl. Security and trust in open source security tokens. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(3):176–201, 2021.

[10] Sergei Skorobogatov and Christopher Woods. Breakthrough silicon scanning discovers backdoor in military chip. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 23–40. Springer, 2012.