INSTITUT FÜR
INNOVATION UND
TECHNIK

iit-kompakt 06 ▪ Selami Yilmaz, Johannes Rittner

Mikroelektronik – Eine Frage des Vertrauens

Kaum eine andere Technologie ist so omnipräsent wie die Elektronik. Wenn Elektronik nicht korrekt funktioniert, hat dies beispielsweise bei Herzschrittmachern oder Smartphones unmittelbaren Einfluss auf Leben oder mindestens Lebensqualität. Wenn Komponenten fehlerhaft funktionieren, kann dies für die kritische Infrastruktur, beispielsweise bei der Energieversorgung, verheerende Folgen haben. Während früher verschmorte Kabel Sinnbild für Fehlfunktionen in der Elektronik waren, ist das Problem heute viel größer.

Das Innenleben von einzelnen Komponenten ist nicht greifbar oder kaum zu verstehen: Ein Prozessor zum Beispiel, Hauptbestandteil eines jeden komplexen elektronischen Systems, besteht aus vielen Milliarden Transistoren auf einer sehr kleinen Fläche[1]. Der Versuch, sich das in Gedanken auszumalen und einen Fehler bzw. eine Manipulation zu entdecken, ist schlicht unmöglich. Da stellt sich zwangsläufig die Frage, wie Vertrauen in diese Systeme aufgebaut werden kann, wo doch Vertrauen evolutionär aus visuellen Reizen und Erfahrungen abgeleitet wird[2].

Vertrauen in Elektronik ist angesichts der Tatsache, dass sie den Alltag durchdringt, essenziell. Eine Grundlage für explizit vertrauenswürdige Elektronik ist, dass diese ausschließlich so funktioniert, wie man es erwartet.

Unwissenheit ist (k)ein Segen

Während der Ausfall von Elektronik am Ende des Lebenszyklus von Produkten absehbar und daher planbar ist, gibt es bereits über die gesamte Lebensspanne hinweg Gefahrenpotenziale, die unerwartete wirtschaftliche Schäden zur Folge haben können. Um diesen Gefahren zu begegnen, sind ein höherer Aufwand und Maßnahmen für einen adäquaten Umgang mit der Elektronik nötig. Elektronische Systeme können beispielsweise gewollte oder ungewollte Schwachstellen in der elektronischen Schaltung aufweisen, die zu Zugriffen unberechtigter Dritter führen können. Gewollte Schwachstellen betreffen u. a. sogenannte Hardware-Trojaner, die eine Art Hintertür auf Hardware-Ebene offen lassen[3]. Aber auch ungewollte Schwachstellen können dazu führen, dass Dritte sich Zugang zu betroffenen Systemen verschaffen. Ein Beispiel hierfür sind sogenannte Zero-Day-Exploits, also Schwachstellen, die nur den Entdecker:innen sowie wenigen anderen bekannt sind. Weitere Beispiele für Sicherheitslücken und deren Gefahrenpotenziale sind Meltdown und Spectre[4]. Fehler beim Design können, wie in einem Fall von Intel, auch zum Rückruf von im Umlauf befindlichen Prozessoren führen[5]. Weitere wirtschaftliche Schäden können Unternehmen durch mangelhafte Fälschungen oder Reverse Engineering, also den Nachbau des Produkts und dem damit verbundenen Diebstahl von geistigem Eigentum, erleiden. Den Schaden haben betroffene Anwender:innen – wenn das elektronische System in seiner Funktion ausfällt – aber auch die Hersteller, nämlich durch Imageverlust und entgangene Umsätze.

Vertrauenswürdige Elektronik: das notwendige Fundament für Cybersicherheit

Das skizzierte Problem nicht vertrauenswürdiger Elektronik hat starke Bezüge zur Cybersicherheit. Allerdings liegt dort der Schwerpunkt auf der Informations- sowie Kommunikationstechnik und Softwaresicherheit. Dagegen adressiert der Ansatz der vertrauenswürdigen Elektronik das Fundament des Hauses: Um diese essenzielle, unterste Schicht von elektronischen Systemen vertrauenswürdig zu machen, bedarf es daher intensivster Anstrengungen in Forschung und Entwicklung. Dabei ist ein gemeinsames und interdisziplinäres Verständnis aller Akteur:innen von besonderer Bedeutung, um geeignete Lösungsansätze entwickeln zu können. Vertrauenswürdigkeit bedeutet in diesem Zusammenhang, dass die Elektronik nur genau das tut, was sie soll – nicht mehr, und auch nicht weniger.

Wie kann die Vertrauenswürdigkeit von komplexer Elektronik hergestellt und anschließend dauerhaft gewährleistet werden? Es gelingt nur, wenn idealerweise die gesamte Wertschöpfungskette betrachtet wird. Dies bedeutet, dass die Methoden und Ansätze, die die Vertrauenswürdigkeit ermöglichen sollen, beginnend beim Design über die Fertigung und Integration bis hin zu Test und Analyse greifen können. Nur so kann über die gesamte Lebensdauer der Elektronik die Vertrauenswürdigkeit aufrechterhalten werden. Grundsätzlich ist es daher notwendig, dass in Deutschland für sämtliche Schritte in der Wertschöpfungskette von vertrauenswürdiger Elektronik ausreichend Kompetenz vorhanden ist. Nur dann könnten die beteiligten Unternehmen ihre Vertrauenswürdigkeit in einer Art Zertifizierung beweisen und den Endanwender:innen garantieren.

1 https://www.intel.com/content/www/us/en/newsroom/news/4th-gen-xeon-scalable-processors-max-series-cpus-gpus.html
2 z. B. https://www.mpg.de/Milinski_Laecheln_Vertrauen
3 Prominentes Beispiel ist die Crypto AG, die in den 70er bis 90er Jahren elektronische Kommunikationsgeräte zur verschlüsselten Kommunikation von Regierungen mit Hintertüren versehen und vertrieben hat.
4 https://meltdownattack.com
5 https://www.golem.de/1101/81091.html

Abbildung 1: Die Vertrauenswürdigkeit von Elektronik wird idealerweise entlang der Wertschöpfungskette adressiert und durch Standards vereinheitlicht. Die technologischen Ansätze zur Verankerung der Vertrauenswürdigkeit wirken insbesondere in den grau hinterlegten Schritten.

Leichter gesagt als getan: Vertrauen entlang der Wertschöpfungskette aufbauen

Die Entwicklungen, die Anfang der 2000er-Jahre begonnen haben und in deren Zuge Fertigungskapazitäten aus Europa nach Asien verlagert wurden, haben dazu geführt, dass Elektronik heutzutage mit Hilfe eines komplexen, globalen Wertschöpfungsnetzwerks entsteht. In der Folge sind nur sehr selten einzelne Länder, wie z. B. die USA, in der Lage sämtliche Schritte der Wertschöpfung selbst umsetzen zu können. In Europa ist das derzeit nicht vollumfänglich möglich. In einzelnen Stufen der Wertschöpfung ist daher die Gefahr gegeben, dass Funktionen in die Elektronik Einzug finden, die dort nichts zu suchen haben. Beispielsweise können im Entwurfsprozess Schaltungsblöcke integriert werden, die ungewollte Abhörfunktionen implementieren. Gleiches kann durch Hinzufügen von zusätzlichen Komponenten in der Zusammenbauphase erfolgen. Um derartige Gefährdungen rechtzeitig aufspüren und geeignete Gegenmaßnahmen ergreifen zu können ist es daher notwendig, die Kenntnisse und Kompetenzen für alle Stufen der Wertschöpfung auf- und auszubauen. Denn nur so gelingt es, Elektronik nach den eigenen Werten zu gestalten, auf Augenhöhe mit anderen Ländern zu agieren und technologisch souverän zu handeln.

Ansatzpunkte für vertrauenswürdige Elektronik von Verifikation bis Obfuskation

Betrachtet man die Stufen der Wertschöpfungskette im Einzelnen, ergeben sich verschiedene Ansatzmöglichkeiten, um die Vertrauenswürdigkeit der Elektronik zu verankern. Im Entwurfsprozess kommt der formalen Verifikation eine zentrale Bedeutung zu, um die Vertrauenswürdigkeit des in Entstehung befindlichen Systems zu validieren. Dabei kommen mathematische Methoden zum Einsatz, die die korrekte Funktion des Systems nachweisen und dadurch helfen, ungeplantes Fehlverhalten auszuschließen. Um den Diebstahl sensibler Daten oder des geistigen Eigentums zu verhindern, eignet sich der sogenannte Tamperschutz. Er kann zum Beispiel derart ausgelegt werden, dass der Versuch eines Zugriffs auf das Innenleben eines Chips im Rahmen des Reverse Engineerings dazu führt, dass Maßnahmen zur Zerstörung der Schaltung und zum Löschen von Daten ausgelöst werden. Für den Fertigungsprozess liefern Chiplets gleich mehrere Möglichkeiten, um geeignete Maßnahmen zu ergreifen. Chiplets ermöglichen die physische Unterteilung eines Chips nach Funktionen und werden mit anderen Bauteilen zu einem Gesamtchip zusammengebaut. Es können dabei Sicherheitselemente in Chiplets implementiert werden, die bei Fertigern des Vertrauens hergestellt werden, wogegen Standardfunktionen mit Chiplets von weniger vertrauenswürdigen Herstellern realisiert werden können. Zum anderen besteht die Möglichkeit, die eigentliche Schaltung zu schützen, indem Funktionsteile clever auf mehrere Chiplets verteilt werden. Die Kenntnis des Innenlebens eines Chiplets reicht dann nicht aus, um das Zusammenspiel aller integrierten Chiplets und die eigentliche Funktion des Gesamtchips zu ermitteln. Um die Echtheit von Elektronikkomponenten nachvollziehen zu können, sind Ansätze geeignet, die eine Art Wasserzeichen in Schaltungen innerhalb der Chips oder auf Leiterplatten integrieren. Ein weiterer Ansatz ist die sogenannte Hardware-Obfuskation, die es erlaubt, zum Beispiel mittels Ergänzung der eigentlichen Schaltung um zusätzliche Schaltungsblöcke, die tatsächliche Funktion der Schaltung zu verschleiern. Der Vorteil dieser Methoden ist, dass ein gewisser Schutz realisiert werden kann, auch wenn der Zugriff auf das Innenleben von Chips, z. B. mit sogenannten Chipscanner, durch schichtweises abtragen und abbilden der Schaltung nicht verhindert werden kann.

Gemeinsame Anstrengungen für Forschung, Entwicklung und Standards

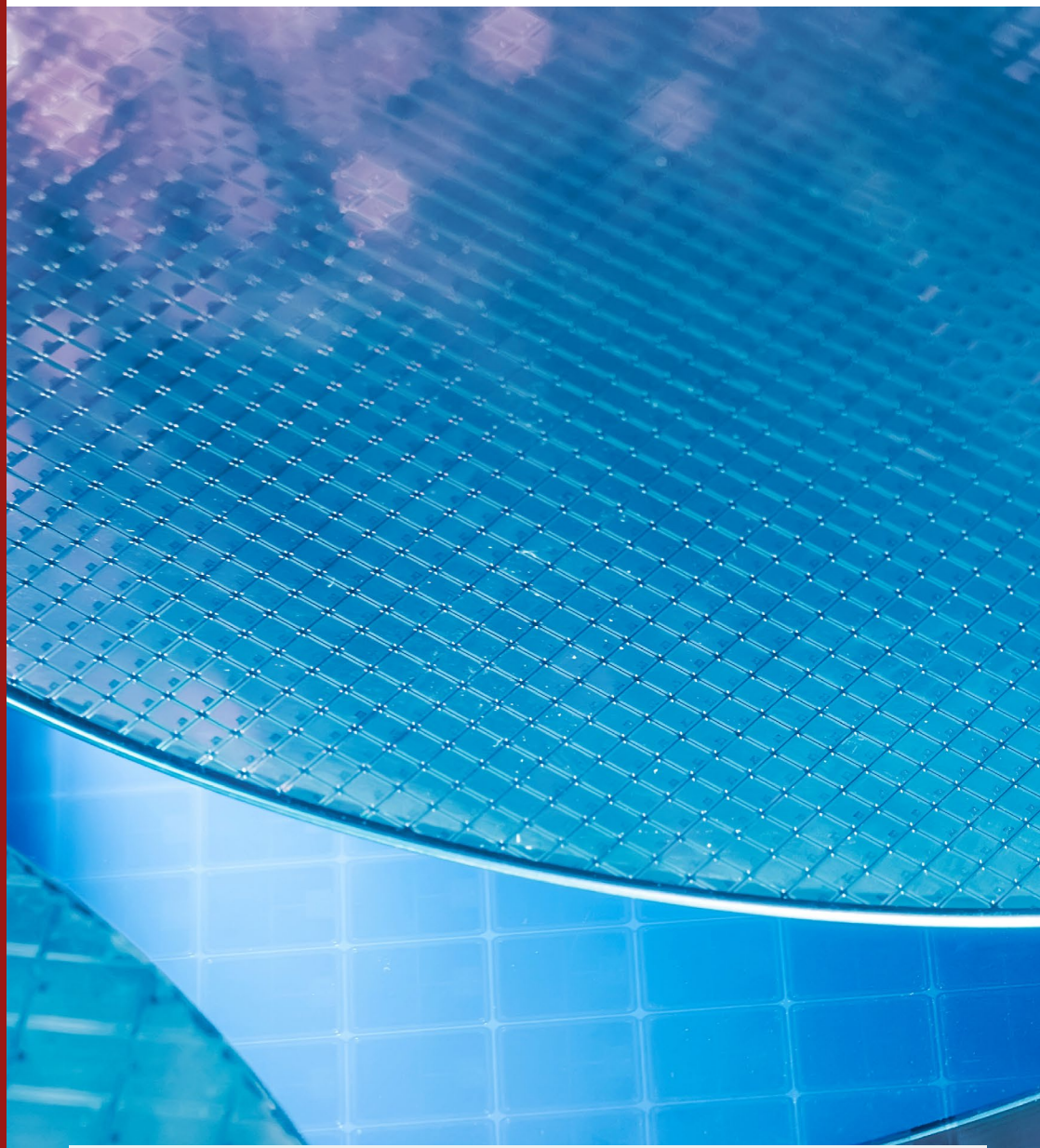
Viele der möglichen Ansätze befinden sich noch nicht in der Serienreife und erfordern Forschungs- und Entwicklungsaufwände. Im Alleingang wir es nicht gelingen, die notwendigen Lösungen zu entwickeln und anzubieten. Daher sind geförderte Verbundprojekte von besonders hoher Bedeutung, damit sich die Forschung und Entwicklung in diesem Bereich an den Bedarfen der Gesellschaft und der Anwender:innen orientiert. Darüber hinaus kann die einhergehende, enorme finanzielle Belastung Einzelner bei der Umsetzung und Realisierung von Lösungen reduziert werden. Vorreiter in Europa ist das deutsche Bundesministerium für Bildung und Forschung (BMBF), das Projekte in diesem Bereich fördert[6]. Auch in den USA gibt es seit einiger Zeit intensive Aktivitäten, die hauptsächlich durch die Defense Advanced Research Projects Agency (DARPA) des Verteidigungsministeriums koordiniert und gefördert werden[7]. Um eine möglichst weite Verbreitung der Ansätze zur Realisierung vertrauenswürdiger Elektronik erreichen zu können, bedarf es einer Kooperation über Ländergrenzen hinweg.

Besonders wichtig sind daher Standards, die einen internationalen Rahmen für die wissenschaftlichen und wirtschaftlichen Aktivitäten in diesem Bereich bieten. Möglich wäre dabei die Definition von Stufen der Vertrauenswürdigkeit. Allerdings gibt es bisher keine Standards, da eine gesonderte Betrachtung der relevanten Aspekte eine neue Herangehensweise darstellt. Denkbar wäre die Anwendung der Common Criteria for Information Technology Security Evaluation (kurz Common Criteria[8]) als Blaupause für die vertrauenswürdige Elektronik. Das Europäische Komitee für elektrotechnische Normung (CENELEC) entwickelt aktuell eine Strategie für eine Standardisierung im Bereich der Vertrauenswürdigen Elektronik, die sich in weiten Teilen an den Prinzipien der Common Criteria orientiert. In 2023 wird die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (DKE[9]) gemeinsam mit der CENELEC ein Projekt zur Erarbeitung einer Roadmap starten, mit dem Ziel, ab 2025 mit den Arbeiten zur Standardisierung anfangen zu können.

6 https://www.elektronikforschung.de/fokusthemen/vertrauenswuerdigkeit
7 https://www.darpa.mil/program/automatic-implementation-of-secure-silicon
8 https://www.commoncriteriaportal.org *
9 https://www.dke.de

Ohne vertrauenswürdige Elektronik keine technologische Souveränität

Die genannten Anstrengungen und Aktivitäten sind von besonderer strategischer Bedeutung für Deutschland und Europa: Vertrauenswürdige Elektronik ist ein Grundpfeiler für Technologische Souveränität, da es möglich wird, die allgegenwärtige Elektronik nach den eigenen Werten zu gestalten und vor dem Ein- und Zugriff Dritter zu schützen. Vor allem stellt sie ein Alleinstellungsmerkmal dar, das den Unternehmen in Europa einen signifikanten Wettbewerbsvorteil verschaffen kann. Ein interessantes Beispiel dafür sind rekonfigurierbare Feldeffekttransistoren, die eine reversible Programmierbarkeit der digitalen Schaltungsfunktion ermöglichen und daher besonders gut für die Realisierung von Verschleierungsschaltungen geeignet sind. Mit den Forschungs- und Entwicklungsaktivitäten ist Deutschland Vorreiter in Europa und hätte daher bereits Lösungen parat, die zukünftigen, gesetzlichen Vorgaben entsprechen. Denkbar sind Anforderungen, wie sie beispielsweise im Bereich der Informationssicherheit bereits legislativ verankert sind. Auch für Europa wäre die Fähigkeit, vertrauenswürdige Elektronik zu produzieren und als europäisches Kennzeichen zu etablieren von besonderem Wert. Denn das Ziel der Europäischen Kommission, perspektivisch 20 Prozent Marktanteil bei der Herstellung von Mikroelektronik zu erreichen, wird nicht nur durch Aufbau von Fertigungskapazitäten zu erreichen sein, sondern bedarf auch zusätzlicher Anreizeffekte, wie die Vertrauenswürdigkeit sie bietet.



Herausgeber
Prof. Dr. Volker Wittpahl
Institut für Innovation und Technik (iit)
in der
VDI/VDE Innovation + Technik GmbH
Steinplatz 1, 10623 Berlin

Zitation
Yilmaz, Selami; Rittner, Johannes (2023): Mikroelektronik – Eine Frage des Vertrauens. iit-kompakt Nr. 06. Hrsg. vom Institut für Innovation und Technik (iit), Berlin.

iit-kompakt Nr. 06
Mai 2023
Layout: VDI/VDE-IT
Bildnachweis: xiaoliangge/AdobeStock

Autoren
Dr. Selami Yilmaz
Tel: +49 (0)89 51089630 24
E-Mail: selami.yilmaz@vdivde-it.de

Johannes Rittner
Tel: +49 (0)30 310078 230
E-Mail: johannes.rittner@vdivde-it.de

ISBN: 978-3-89-750253-6