Bundesministerium
für Bildung
und Forschung

Vertrauenswürdige Elektronik

Forschung und Innovation für technologische Souveränität

Vorwort

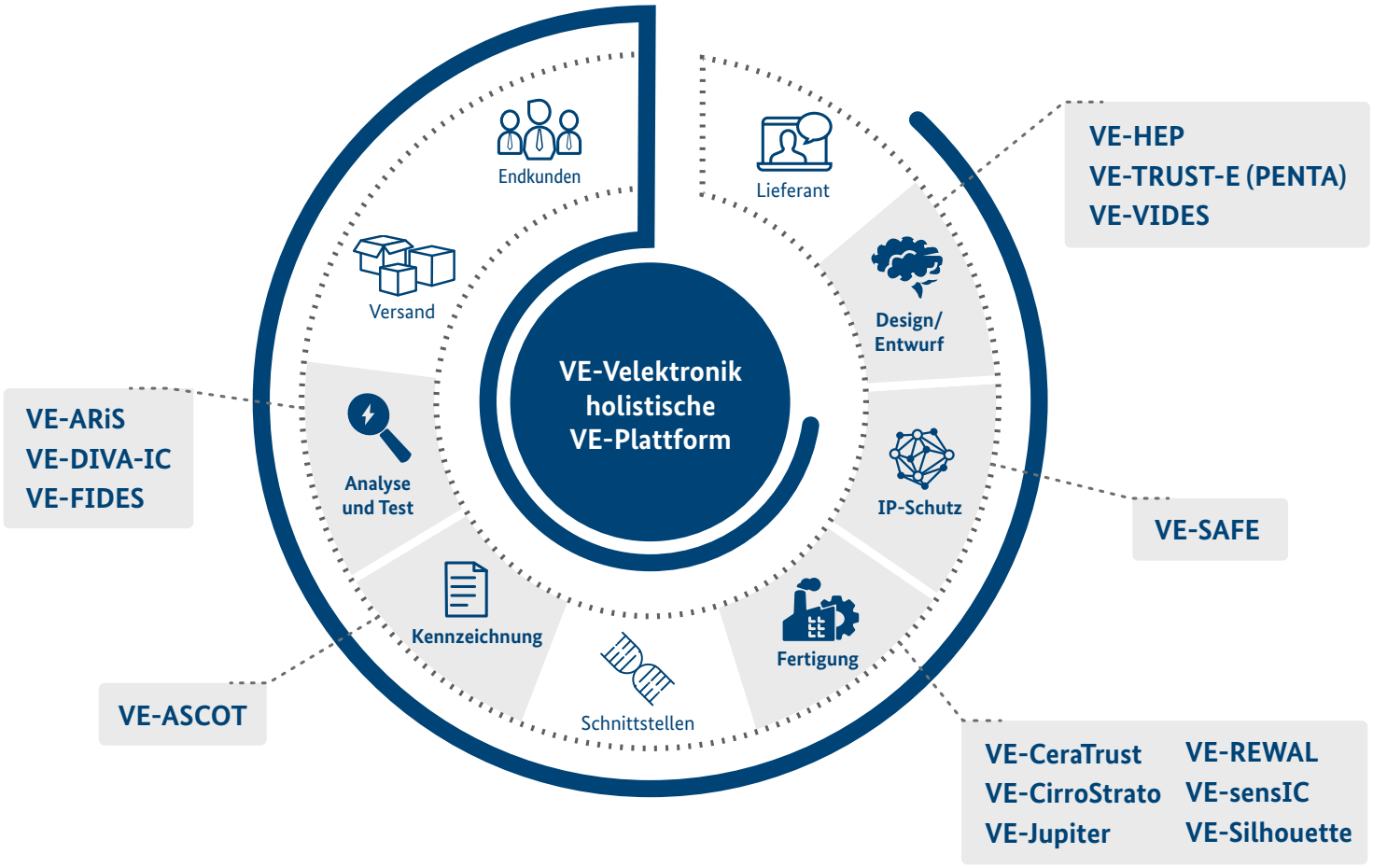
Mikroelektronik bildet den Kern jedes digitalen Systems und ist eine Schlüsseltechnologie der Digitalisierung. Im täglichen Leben wird die Gesellschaft künftig noch mehr elektronischen Bauteilen vertrauen müssen, die beispielsweise in selbstfahrenden Autos oder Servicerobotern zum Einsatz kommen. Deutschland und Europa sind im Bereich der Mikroelektronik und Elektroniksysteme intensiv in die globalen Wertschöpfungsketten und Partnerschaften eingebunden. Um Elektronik sicher und zuverlässig einzusetzen, muss Deutschland in den globalen Wertschöpfungsketten eine souveräne Position einnehmen können. Dazu gehört das Nachvollziehen der Funktionalitäten sowie eine Versorgungssicherheit. Deutschland braucht daher für seine technologische Souveränität Spitzenkapazitäten in der Erforschung, Entwicklung und Anwendung von vertrauenswürdiger Elektronik. Hier setzt die Leitinitiative für eine Vertrauenswürdige Elektronik der Digitalstrategie des BMBF an und baut auf Forschung und Entwicklung vom Design über Herstellung bis zur Prüfung.

Mit dem Rahmenprogramm „Mikroelektronik. Vertrauenswürdig und nachhaltig. Für Deutschland und Europa.“ und der Leitinitiative „Vertrauenswürdige Elektronik“ fördert die Bundesregierung Forschung und Innovation in der Mikroelektronik, um die technologische Souveränität in Deutschland und Europa zu stärken.

Diese Broschüre stellt Forschungsprojekte vor, die das Bundesministerium für Bildung und Forschung im Rahmen der Leitinitiative „Vertrauenswürdige Elektronik“ fördert.

Ihr Bundesministerium für Bildung und Forschung

Inhaltsverzeichnis



Projekte mit vertrauenswürdigen Technologien in den Bereichen Design, Fertigung und Analyse

Im täglichen Leben werden wir künftig noch mehr elektronischen Bauteilen vertrauen müssen, die beispielsweise in selbstfahrenden Autos oder Servicerobotern zum Einsatz kommen. Um Elektronik sicher und zuverlässig einzusetzen, müssen wir in den globalen Wertschöpfungsketten eine souveräne Position einnehmen können. Dazu gehört das Nachvollziehen der Funktionalität der verbauten Komponenten sowie die Versorgungssicherheit. Deutschland braucht daher für seine technologische Souveränität Spitzenkapazitäten in der Erforschung, Entwicklung und Anwendung von vertrauenswürdiger Elektronik. Um dies realisieren zu können, sollen die Projekte der Förderinitiative ZEUS im Rahmen der Leitinitiative „Vertrauenswürdige Elektronik“ neuartige Methoden, Lösungen und Prozesse erforschen und entwickeln, vom Design über die Herstellung bis zur Analyse und Prüfung.

Ansprechpartner
Dr. Roland Krüppel
Referat: Elektronik und autonomes Fahren; Supercomputing
E-Mail: Roland.Krueppel@bmbf.bund.de

Vertrauenswürdige Elektronik

Plattform für vertrauenswürdige Elektronik und sichere Wertschöpfungsketten (VE-Velektronik)

Ziele und Vorgehen

In dem Vorhaben wird eine Plattform für vertrauenswürdige Elektronik geschaffen. Dabei werden übergreifende Fragestellungen in den drei Säulen Design, Fertigung und Analyse der Mikroelektronik-Wertschöpfungskette bearbeitet. Die Plattform wird sich auf Beiträge zur notwendigen Standardisierung, auf die Vernetzung der Forschungsvorhaben zur Vertrauenswürdigen Elektronik sowie die Pflege und Bereitstellung des im Rahmen der einzelnen Vorhaben erzielten Know-how konzentrieren, um durch die Nutzung von Synergien den zunehmenden Bedarf nach höherer Vertrauenswürdigkeit in der Elektronik zu decken und konkrete einsatzreife Lösungskonzepte zur Verfügung zu stellen.

Innovationen und Perspektiven

Im Erfolgsfall wird die technologische Souveränität über vertrauenswürdige Elektronik für die Industrie deutlich gestärkt. Das mittelbare Ziel des Vorhabens ist es, Unternehmen effektiv zu unterstützen und die Versorgung mit vertrauenswürdiger Elektronik, speziell für Kleinserien, zu gewährleisten.

Verbundkoordinator

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Dr.-Ing. Johann Heyszl
Lichtenbergstr. 11
85748 Garching b. München
Tel.: +49 89 3229986-172
E-Mail: johann.heyszl@aisec.fraunhofer.de

Projektvolumen

6,01 Mio. Euro
BMBF-Förderung: 5,73 Mio. Euro (95 %)

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- Fraunhofer Gesellschaft (FhG) für Angewandte und Integrierte Sicherheit AISEC, Garching b. München
- Forschungsfabrik Mikroelektronik Deutschland (FMD), Berlin
- edacentrum GmbH, Hannover
- FhG für Mikrosysteme und Festkörper-Technologien EMFT, München
- Forschungsverbund Berlin e.V., Berlin
- FhG für Angewandte Festkörperphysik IAF, Freiburg
- IHP GmbH – Leibniz-Institut für innovative Mikroelektronik, Frankfurt/Oder
- FhG für Integrierte Schaltungen IIS, Erlangen
- FhG für Integrierte Schaltungen IIS, Dresden
- FhG für Integrierte Schaltungen IIS, Nürnberg
- FhG für Mikroelektronische Schaltungen und Systeme IMS, Duisburg
- FhG für Elektronische Nanosysteme ENAS, Chemnitz
- FhG für Mikrostruktur von Werkstoffen und Systemen IMWS, Halle (Saale)
- FhG für Photonische Mikrosysteme IPMS, Dresden
- FhG für Zuverlässigkeit und Mikrointegration IZM, Berlin

Vertrauen durch Transparenz: Methoden und Werkzeuge für das Design quelloffener, vertrauenswürdiger Prozessoren (VE-HEP)

Ziele und Vorgehen

Ziel des Projekts ist es, erstmals wesentliche Teile der gesamten Wertschöpfungskette im Bereich der Entwicklung und Fertigung von sicherheitsrelevanten Chips (Hardware Security Module) in Open Source zu realisieren. Dies bezieht sich sowohl auf die Entwicklung der Hardware als auch auf die Implementierung von Härtungsmechanismen, also dem Schutz vor Angriffen. Weiterhin werden Schwachstellen der Hardware-Wertschöpfungskette analysiert und offengelegt. Konkret soll ein gegen physikalische Angriffe geschützter RISC-V-Prozessor entwickelt werden. Als Anwendungsfall zur Evaluation der entwickelten Lösung wird die durch Hardware beschleunigte Ausführung von kryptographischen Operationen betrachtet. Erstmals sollen in einer quelloffenen Software für den Entwurf von Mikroelektronik – einem sogenannten Electronic Design Automation (EDA)-Tool – Härtungsmaßnahmen gegen Seitenkanalangriffe automatisiert werden. Die Forschenden werden offene Lösungen und Ansätze wählen, um die Verifizierbarkeit der entwickelten Hardware zu ermöglichen. Hierdurch wird eine vollständig transparente Zertifizierbarkeit erreicht. Am Ende des Projektes steht ein Demonstrator, der die Ergebnisse im Kontext der industriellen Praxis aufzeigt.

Innovationen und Perspektiven

Sind Prozessoren und Kryptobeschleuniger quelloffen, so erleichtert dies kleineren und mittleren Unternehmen den Markteinstieg. Dadurch werden Wertschöpfungs- und Lieferketten diversifiziert, was wiederum Abhängigkeiten reduziert und perspektivisch die Wettbewerbs- und Innovationsfähigkeit der deutschen und europäischen Industrie stärkt. Im Speziellen bewirkt das Projekt VE-HEP auch den Ausbau von Kompetenzen und Wertschöpfung im Bereich IT-Hardware, insbesondere bei Mikroprozessoren für die Automobilindustrie und für Geräte im Internet der Dinge (IoT). Die Ergebnisse des Projekts werden dazu beitragen, dass künftig sicherheitskritische Hardwaredesigns und formal verifizierte Härtungsmaßnahmen leichter umzusetzen sind. Eine Industrial Liaison Group, die durch die Projektpartner gegründet wird, analysiert, überwacht und lenkt die stetige industrienahe Weiterentwicklung der im Projekt gewonnenen Ergebnisse und entwickelt die rechtlichen Rahmenbedingungen und eine dauerhaft tragfähige Gesellschaft.

Verbundkoordinator

IHP GmbH – Innovations for High Performance Microelectronics / Leibniz-Institut für innovative Mikroelektronik
Herr Dr.-Ing. Norbert Herfurth
Postfach 14 66, 15204 Frankfurt/Oder
E-Mail: herfurth@ihp-microelectronics.com

Projektvolumen

4,07 Mio. Euro
BMBF-Förderung: 3,41 Mio. Euro (84 %) zzgl. 0,20 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- IHP GmbH – Innovations for High Performance Microelectronics/Leibniz-Institut für innovative Mikroelektronik, Frankfurt/Oder
- IAV GmbH Ingenieurgesellschaft Auto und Verkehr, Berlin
- Elektrobit Automotive GmbH, Erlangen
- Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI), Bremen
- Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt
- Hochschule RheinMain, FG Theoretische Informatik, Wiesbaden
- Ruhr-Universität Bochum, FG Security Engineering, Bochum
- Technische Universität Berlin, FG Security in Telecommunications, Berlin

Assoziierte Partner

- Bosch
- Hensoldt Cyber
- Volkswagen CSO

Ansprechpartner

Dr. Steffen Lohmann
Referat: Vernetzung und Sicherheit digitaler Systeme
Steffen.Lohmann@bmbf.bund.de

Vertrauenswürdige Sensorsysteme für mobile und industrielle Anwendungen (VE-TRUST-E)

Ziele und Vorgehen

Ziel des Projektes ist es, Sensoren mit eingebetteter Künstlicher Intelligenz (KI) zu entwickeln, welche die Erfassung und Bewertung von Situationen unmittelbar und autark vornehmen können. In dem Vorhaben werden hierfür ein Trägheitssensor, ein optischer Sensor zur Umgebungserfassung und ein Sensornetzwerk für die Zustandsüberwachung von industriellen Antrieben entwickelt. Dafür werden äußerst kompakte, modulare und vertrauenswürdige Elektronikchips mit großer Rechenleistung entwickelt, welche sich leicht an unterschiedliche Anwendungen anpassen lassen und kompakte und effiziente Baugruppen ermöglichen. Wesentliche Schwerpunkte des Projekts sind die Erforschung und Testung zuverlässiger KI-Methoden sowie die Entwicklung von vertrauenswürdigen Design- und Fertigungsmethoden der Elektronikbausteine.

Innovationen und Perspektiven

Die automatisierte und vertrauenswürdige Situationsbewertung auf Grundlage von Sensordaten ist in vielen künftigen Anwendungen, wie dem autonomen Fahren und der Überwachung von Produktionsanlagen, entscheidend. Eine KI direkt im Sensor verringert die Last in der Datenübertragung und von Manipulationsmöglichkeiten.

Verbundkoordinator

Siemens Aktiengesellschaft
Dr. Kai Kriegel
Otto-Hahn-Ring 6, 81739 München
Tel.: +49 89 636-634390
E-Mail: kai.kriegel@siemens.com

Projektvolumen

ca. 4,09 Mio. Euro
BMBF-Förderung: ca. 2,61 Mio. Euro (ca. 64 %)
zzgl. ca. 0,05 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.
Freistaat Sachsen: ca. 0,34 Mio. Euro

Projektlaufzeit

01.04.2021 bis 31.03.2024

Projektpartner

- Siemens Aktiengesellschaft, München
- Berliner Nanotest und Design GmbH, Berlin
- Chemnitzer Werkstoffmechanik GmbH, Chemnitz
- Fraunhofer-Institut für Integrierte Schaltungen IIS, Dresden
- Fraunhofer-Institut für Elektronische Nanosysteme ENAS, Chemnitz
- Nexperia GmbH, Hamburg
- Robert Bosch GmbH, Gerlingen
- scalable minds GmbH, Potsdam
- Universität Siegen, Siegen

Designmethoden und HW/SW-Co-Verifikation für die eindeutige dentifizierbarkeit von Elektronikkomponenten (VE-VIDES)

Ziele und Vorgehen

Ziel des Projekts ist es, ein ganzheitliches Sicherheitskonzept für Elektroniksysteme zu entwickeln, das sowohl das zugrundeliegende geistige Eigentum als auch die Integration von Elektronikkomponenten in ein Gesamtsystem gegen Sicherheitsrisiken, Angriffe und Manipulationen von Dritten absichert. Mit einer Art Fingerabdruck können einzelne Elektronikkomponenten eindeutig identifiziert und überwacht werden. Ein modularer Ansatz erlaubt zudem die einfache Integration von Tests, um das System gegen neue Schwachstellen und Angriffsszenarien abzusichern. Mit Anwendungsfällen aus den Bereichen autonomes Fahren und Industrie 4.0 werden die Ergebnisse validiert.

Innovationen und Perspektiven

Die im Projekt entstehenden Entwurfs- und Verifikationsmethoden, Werkzeuge und Testumgebungen bilden eine Grundlage für zukünftige Entwicklungsprozesse von vertrauenswürdiger Elektronik. Die Übertragung der Ergebnisse auf die Anwendungsbereiche Medizin- und Kommunikationstechnik sowie Luft- und Raumfahrt ist geplant.

Verbundkoordinator

Infineon Technologies AG
Dr. Djones Lettnin
Am Campeon 1 - 15
85579 Neubiberg
Tel.: +49 89 23489-730
E-Mail: djones.lettnin@infineon.com

Projektvolumen

16,28 Mio. Euro
BMBF-Förderung: 9,92 Mio. Euro (61 %) zzgl. 0,25 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- Infineon Technologies AG, Neubiberg
- Volkswagen car.SW Org Wolfsburg AG, Wolfsburg
- Fraunhofer-Institut für Integrierte Schaltungen IIS, Dresden
- IMMS gGmbH, Ilmenau
- OFFIS e.V., Oldenburg
- Onespin Solutions GmbH, München
- Robert Bosch GmbH, Reutlingen
- Siemens AG, München
- Synopsys Deutschland GmbH, Aschheim/ Dornach
- Technische Universität Chemnitz, Chemnitz
- Universität Ulm, Ulm
- X-FAB Global Services GmbH, Erfurt

Verhinderung von Angriffen auf Elektroniksysteme durch innovative Multi-Sensorik (VE-SAFE)

Ziele und Vorgehen

Im Verbundvorhaben wird ein Verfahren und ein Multisensorsystem entwickelt, welches wichtige Mikroelektronikschaltung vor Angriffen schützt. Das Gesamtsystem wird durch eine hierarchisch gestaffelte Überwachung, durch eingebettete Sensoren und einen Mikrocontroller geschützt. Die Entwicklung der Aufbau- und Verbindungstechnik wird ergänzt durch ein zerstörungsfreies Prüfverfahren, das die Integrität des Schutzmechanismus überwacht. Wird ein Manipulationsversuch erkannt, werden durch die Kontrollschaltung Maßnahmen zum Schutz des Systems ausgelöst. Ein Zugriff auf weitere Systemkomponenten wird unterbunden und die ggf. sensiblen Daten werden gelöscht.

Innovationen und Perspektiven

Der hier verfolgte Ansatz erfordert keine Modifikation des Aufbaus der zu schützenden Schaltkreise und ist mit allen sicherheitskritischen Anwendungsschaltungen kombinierbar. Durch diese kostengünstige Lösung sind auch Kleinserienfertigungen wirtschaftlich möglich.

Verbundkoordinator

HTV Halbleiter-Test & Vertriebs-GmbH
Thomas Kuhn
Robert-Bosch-Str. 28
64625 Bensheim
Tel.: +49 6151 869- 282
E-Mail: t.kuhn@htv-gmbh.de

Projektvolumen

2,87 Mio. Euro
BMBF-Förderung: 2,13 Mio. Euro (74 %)

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- HTV Halbleiter-Test & Vertriebs-GmbH, Bensheim
- Jenaer Leiterplatten GmbH, Jena
- Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration IZM, Berlin

Verhinderung von Angriffen auf Elektroniksysteme durch neuartige keramische Mehrlagensysteme (VE-CeraTrust)

Ziele und Vorgehen

Das Vorhaben VE-CeraTrust zielt auf die Entwicklung verschiedener Schutzmechanismen zur Abschirmung und Verschleierung sowie zur Nachverfolgbarkeit von Elektronikbaugruppen durch keramische Mehrlagentechnologie ab. Diese Technologie wird speziell bei großflächigen Bauteilen mit hohem Kühlvolumen eingesetzt. Das Konsortium wird die Ergebnisse nach Vertrauenswürdigkeit klassifizieren und in einer Baugruppenbibliothek zusammenfassen. Die Modularität des Ansatzes gewährleistet eine hohe Breitenwirksamkeit. Die Entwicklungen lassen sich zudem auch auf die Leiterplattentechnologie, den 3D-Druck oder die Dickschichttechnik übertragen.

Innovationen und Perspektiven

Die zu entwickelnde Bauteilbibliothek ist Grundlage für die Sicherung der Nachverfolgbarkeit und den Manipulationsschutz von Elektronikbauteilen in der Wertschöpfungskette der Zukunft. Die Projektergebnisse lassen sich in sicherheitskritischen Bereichen wie der Medizintechnik, Telekommunikation und der Industrie 4.0 einsetzen.

Verbundkoordinator

VIA electronic GmbH
Dr.-Ing. Uwe Krieger
Robert-Friese-Str. 3
07629 Hermsdorf
Tel.: +49 36601 9298-118
E-Mail: u.krieger@via-electronic.de

Projektvolumen

4,18 Mio. Euro
BMBF-Förderung: 2,64 Mio. Euro (63 %).
Im Förderschwerpunkt „Vertrauenswürdige Elektronik (ZEUS)“ gefördert.

Projektlaufzeit

01.05.2021 bis 30.04.2024

Projektpartner

- VIA electronic GmbH, Hermsdorf
- Fraunhofer-Institut für Keramische Technologien und Systeme IKTS, Dresden
- IMST GmbH, Kamp-Lintfort
- KMS Technology Center GmbH, Dresden
- ANDUS ELECTRONIC GmbH, Berlin

Neuartige rekonfigurierbare Transistoren für den Know-how-Schutz von Elektronikkomponenten (VE-CirroStrato)

Ziele und Vorgehen

Im Vorhaben wird der Einsatz von rekonfigurierbaren Transistoren erforscht, die dem Schutz des geistigen Eigentums bei Chiplayouts dienen. Dafür werden in erster Linie die benötigten Modelle der rekonfigurierbaren Transistoren für die Entwurfswerkzeuge erarbeitet und darauf aufbauend Schaltungsblöcke entwickelt, deren Funktionsweise nicht durch Dritte ermittelt werden kann. In der beispielhaften Umsetzung eines Chips wird das neue Verfahren getestet und unter Einbeziehung des Bundesamts für Informationssicherheit (BSI) auf seine Sicherheit hin überprüft.

Innovationen und Perspektiven

Die geplanten Projektergebnisse für rekonfigurierbare Transistoren bieten beim Schutz von geistigem Eigentum von Chips entscheidende Kostenvorteile. Die geplante Einfachheit bei der Verwendung wird insbesondere die KMU-geprägten Systemhäuser in Deutschland, aber auch deren Kunden im internationalen Wettbewerb, stärken.

Verbundkoordinator

NaMLab gGmbH
Dr.-Ing. Jens Trommer
Nöthnitzer Str. 64 A
01187 Dresden
Tel.: +49 351 2124990-35
E-Mail: jens.trommer@namlab.com

Projektvolumen

2,11 Mio. Euro
BMBF-Förderung: 1,76 Mio. Euro (83 %) zzgl. 0,18 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- NaMLab gGmbH, Dresden
- GLOBALFOUNDRIES Dresden Module One Limited Liability Company & Co. KG, Dresden
- Technische Universität Dresden, Dresden
- Universität Bremen, Bremen

Eindeutige Identifizierbarkeit für vertrauenswürdige Mikroelektronik mit Chiplets (VE-Jupiter)

Ziele und Vorgehen

Im Projekt wird eine Plattform für den Entwurf vertrauenswürdiger Elektronik in komplexen und unsicheren Fertigungsketten entwickelt. Dazu werden unter anderem direkt in den Chip Schutzmechanismen gegen Manipulationsversuche sowie speziell für Prüfbarkeit im Herstellungsprozess angepasste Schaltungselemente eingebracht. Diese werden mit anderen kritischen Komponenten zu sogenannten iTrustlets verbunden. Damit soll schon im Entwurf eine Absicherung gegen externe Einflüsse angelegt werden. Zusätzlich werden dedizierte On-Chip-Einheiten mit externen Messverfahren kombiniert, um mögliche Abweichungen vom Originalentwurf auch außerhalb von Laborumgebungen zu erkennen.

Innovationen und Perspektiven

Die im Projekt entwickelten Technologien im Chip-Design sowie Messverfahren zur Identifikation von Manipulationen liefern einen erheblichen Beitrag zur Steigerung der Vertrauenswürdigkeit der Elektronik. Das Vorhaben leistet damit einen wichtigen Beitrag zur Vermeidung von Manipulationen kritischer Komponenten und zur technologischen Souveränität.

Verbundkoordinator

NXP Semiconductors Germany GmbH
M.Sc. Marc Gourjon
Troplowitzstr. 20
22529 Hamburg
Tel.: +49 40 5613-3695
E-Mail: marc.gourjon@nxp.com

Projektvolumen

3,43 Mio. Euro
BMBF-Förderung: 2,33 Mio. Euro (68 %) zzgl. 0,20 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- NXP Semiconductors Germany GmbH, Hamburg
- DSI Datensicherheit GmbH, Stuhr
- Technische Universität Darmstadt, Darmstadt
- Universität zu Lübeck, Lübeck

Know-how-Schutz für vertrauenswürdige heterogene Elektroniksysteme mit Chiplets (VE-REWAL)

Ziele und Vorgehen

Sensorsysteme im Automobilbereich werden immer komplexer und vereinen unterschiedlichste Technologien, z. B. Sensoren, Signalverarbeitung und drahtlose Übertragung. Ziel des Projekts ist es, die Funktionalität des Gesamtsystems abzusichern und für den Endanwender vertrauenswürdig und sicher zu gestalten. Die Funktionen einzelner Chips werden auf mehrere sogenannte Chiplets verteilt und integriert. Dadurch werden sowohl die Funktionsweise und das Layout als auch das geistige Eigentum gegenüber Dritten verschleiert. Dafür werden neue Richtlinien für das Elektronikdesign sowie neue Integrations- und Kommunikationskonzepte erarbeitet. Die Funktionalität soll an einem Radarsystem für Fahrassistenzsysteme demonstriert werden.

Innovationen und Perspektiven

Mit diesem Ansatz werden die Funktionen der Signalverarbeitung auf verschiedene Chiplets verteilt, sodass einzelne Chiplets für Angreifer wertlos sind. So kann das IP für das Gesamtsystem geschützt werden und auf unterschiedliche Lieferanten zurückgegriffen werden.

Verbundkoordinator

Universität Bremen
Prof. Dr.-Ing. Steffen Paul
Postfach 33 04 40
28334 Bremen
Tel.: +49 421 218-62540
E-Mail: steffen.paul@me.uni-bremen.de

Projektvolumen

6,00 Mio. Euro
BMBF-Förderung: 5,16 Mio. Euro (86 %) zzgl. 0,28 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.
Im Förderschwerpunkt „Vertrauenswürdige Elektronik (ZEUS)“ gefördert.

Projektlaufzeit

01.05.2021 bis 30.04.2024

Projektpartner

- Universität Bremen, Bremen
- Conti Temic microelectronic GmbH, Nürnberg
- Infineon Technologies AG, Neubiberg
- Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration IZM, Moritzburg
- Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik FHR, Wachtberg
- Ruhr-Universität Bochum, Bochum
- Technische Hochschule Ingolstadt, Ingolstadt
- Viconnis, Hamburg (assoziiert)

Eindeutige Identifizierbarkeit für vertrauenswürdige Hybrid-Sensorelektronik mit Hilfe additiver Fertigung (VE-sensIC)

Ziele und Vorgehen

Ziel des Projekts ist es, elektronische Komponenten zu entwickeln, die direkt in Maschinenbauteile integriert werden und dort sicherheitsrelevante Sensordaten ermitteln. Im Vorhaben wird ein intelligenter Gummischlauch mit einem integrierten Temperatursensor für technische Batterien entwickelt. Die elektronische Sensorkomponente lässt frühzeitig Überlastungen und Beschädigungen erkennen und ermöglicht so einen sicheren Betrieb sowie einen Austausch des Schlauches vor einem Totalausfall. Ferner enthält der Schlauch nicht-kopierbare Identifikationsmerkmale, die ihn als hochwertiges Originalteil kennzeichnen.

Innovationen und Perspektiven

Das Projekt schafft Grundlagen, um Elektronik, Sensorik und deren Energieversorgung untrennbar in Kunststoff- und Gummibauteile zu integrieren. Die entwickelten Verfahren können auch in relevanten Komponenten von Treibstoffleitungen oder Leitungen in der Pharmaindustrie eingesetzt werden.

Verbundkoordinator

Benecke-Kaliko AG
Dr.-Ing. Tim Wolfer
Bötzinger Straße 31
79111 Freiburg im Breisgau
Tel.: +49 160 94828915
E-Mail: tim.wolfer@continental.com

Projektvolumen

4,32 Mio. Euro
BMBF-Förderung: 2,86 Mio. Euro (66 %) zzgl. 0,58 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.
Im Förderschwerpunkt „Vertrauenswürdige Elektronik (ZEUS)“ gefördert.

Projektlaufzeit

01.05.2021 bis 30.04.2024

Projektpartner

- Benecke-Kaliko AG, Freiburg im Breisgau
- Polysecure GmbH, Freiburg im Breisgau
- Sondervermögen Großforschung beim Karlsruher Institut für Technologie KIT, Eggenstein-Leopoldshafen
- Leibniz-Institut für Neue Materialien gemeinnützige Gesellschaft mit beschränkter Haftung INM, Saarbrücken
- Hochschule Offenburg
- Cyient GmbH, Stuttgart
- ContiTech MGW GmbH, Hann. Münden
- Elmos Semiconductor (assoziiert)

Heterogene Photonik-Elektronik-Plattform für vertrauenswürdige quelloffene Prozessoren (VE-Silhouette)

Ziele und Vorgehen

Ziel des Projekts ist es, eine Photonik-Elektronik-Plattform zu entwickeln, die über standardisierte optische und elektrische Schnittstellen die flexible Anbindung photonischer Komponenten an offene Prozessorsysteme erlaubt. Dadurch können Sicherheitsfunktionen photonisch implementiert werden, was dank der besseren Abhörsicherheit die Vertrauenswürdigkeit steigert. Die Integrität der sicherheitsrelevanten Funktionsblöcke wird durch sogenannte Built-In-Self-Test-Verfahren sichergestellt. Neben der Entwicklung grundlegender elektronischer und photonischer Komponenten werden auch Aufbau- und Verbindungstechnologien sowie Fertigungsprozesse für die elektrooptische Integration auf einer Fertigungslinie erarbeitet.

Innovationen und Perspektiven

Neben der Entwicklung vertrauenswürdiger Elektronik schafft die modulare Integration photonischer Komponenten eine Grundlage für zahlreiche neue Anwendungen wie beispielsweise die Datenverarbeitung mit photonischen neuronalen Netzen.

Verbundkoordinator

Fraunhofer-Institut für Photonische Mikrosysteme IPMS
Marcus Pietzsch
Maria-Reiche-Str. 2, 01109 Dresden
Tel.: +49 351 8823-355
E-Mail: marcus.pietzsch@ipms.fraunhofer.de

Projektvolumen

13,07 Mio. Euro
BMBF-Förderung: 11,78 Mio. Euro (90 %) zzgl. 0,60 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.
Im Förderschwerpunkt „Vertrauenswürdige Elektronik (ZEUS)“ gefördert.

Projektlaufzeit

01.05.2021 bis 30.04.2024

Projektpartner

- Fraunhofer-Institut für Photonische Mikrosysteme IPMS, Dresden
- Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration IZM-ASSID,Dresden-Moritzburg
- Technische Universität Dresden, Institut für Aufbau- und Ver-bindungstechnik der Elektronik, Dresden
- Technische Universität Dresden, Institut für Nachrichtentech-nik, Dresden
- OSRAM Opto Semiconductors GmbH, Regensburg
- Fraunhofer-Institut für Nachrichtentechnik, Heinrich-Hertz-Institut HHI, Berlin
- qutools GmbH, München

Neuartige sichere Elektronikkomponenten für die „Chain of Trust“ (VE-ASCOT)

Ziele und Vorgehen

Ziel des Projekts ist es, eine „Chain of Trust“ (COT) Plattform zu entwickeln, die eine vertrauenswürdige Produktionskette und eine sichere Inbetriebnahme von Halbleiterkomponenten ermöglicht. Sie basiert auf einem eingebetteten Vertrauensanker (dieser schützt vor unbefugtem Zugriff und speichert vertrauliche und kryptografische Daten) und weiteren, nicht kopierbaren Identitätsmerkmalen. Die Funktionalität soll im Bereich der Medizintechnik demonstriert werden.

Innovationen und Perspektiven

Der Vorteil dieser COT besteht darin, dass sie jederzeit aus der Hardwarekomponente ausgelesen und vor Ort auf Echtheit überprüft werden kann. Sie kann in allen kritischen Infrastrukturen, z. B. in hochautomatisierten Prozessen der Industrie 4.0 oder in der Verkehrstechnik eingesetzt werden. Damit könnte das Projekt wesentlich zur technologischen Souveränität Deutschlands beitragen.

Verbundkoordinator

WIBU-SYSTEMS Aktiengesellschaft
Ralf Fust
Rüppurrer Str. 52–54
76137 Karlsruhe
Tel.: +49 721 93172-34
E-Mail: ralf.fust@wibu.com

Projektvolumen

4,71 Mio. Euro
BMBF-Förderung: 3,15 Mio. Euro (67 %) zzgl. 0,15 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- WIBU-SYSTEMS Aktiengesellschaft, Karlsruhe
- Siemens Aktiengesellschaft, München
- Infineon Technologies AG, Neubiberg
- Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt
- Karlsruher Institut für Technologie (KIT), Karlsruhe
- Universität Bielefeld, Bielefeld

Elektronischer Know-how-Schutz für innovative Sensorsysteme (VE-ARiS)

Ziele und Vorgehen

Ziel des Vorhabens ARiS ist es, einen umfassenden Schutz vertrauenswürdiger, hochintegrierter Sensorsysteme zu entwickeln, der Nachbauten (Reverse Engineering) und Manipulationen verhindert. Neuartige Designmethoden sollen vor Fälschungen der Elektroniksysteme schützen und aktive Abwehrtechniken in Leiterplatten und Schaltkreise integrieren. Zusätzlich ermöglichen diese Designmethoden, die Echtheit der Bauteile zu verifizieren. Mit Hilfe von KI-Algorithmen wird die Sicherheit des Chip-Layouts gegenüber Reverse Engineering automatisch bewertet. Die Leistungsfähigkeit der Lösung soll am Beispiel eines Positionsgebers für die Anwendung in Aufzügen, Robotern oder für das autonome Fahren demonstriert werden.

Innovationen und Perspektiven

Die Projektergebnisse ermöglichen einen sehr guten IP-Schutz und können auf verschiedene Anwendungen übertragen werden. Dabei sind insbesondere sicherheitskritische Bereiche, wie z. B. die Automobil- oder die Luftfahrtindustrie hervorzuheben.

Verbundkoordinator

iC-Haus GmbH
Dr. Heiner Flocke
Am Kuemmerling 18
55294 Bodenheim
Tel: +49 6135 9292-0
E-Mail: Heiner.Flocke@ichaus.de

Projektvolumen

3,87 Mio. Euro
BMBF-Förderung: 2,26 Mio. Euro (59 %)

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- iC-Haus GmbH, Bodenheim
- Wachendorff Automation GmbH & Co. KG, Geisenheim
- IMMS Institut für Mikroelektronik- und Mechatronik-Systeme gGmbH, Ilmenau

Neuartige Designmethoden für vertrauenswürdige Elektronikschaltungen (VE-DIVA-IC)

Ziele und Vorgehen

Ziel des Projektes VE-DIVA-IC ist es, den Schutz von Integrität und Identität von elektronischen Bauteilen in den Bereichen Mobilität und Automatisierungstechnik zu stärken. Dazu wird beim Entwurf von integrierten Schaltungen ein zusätzlicher Schritt entwickelt, welcher die Planung sicherer, vertrauenswürdiger Bauteileigenschaften ermöglicht und die Integrität der Entwurfsdaten durch Modellierung verifiziert. Ein zusätzlicher Schutz ergibt sich dadurch, dass die Elektronikkomponenten auch im laufenden Betrieb kontinuierlich getestet werden, um den Sicherheitszustand zu überwachen und Angriffe mit gezielter Manipulationsabsicht zu detektieren. Durch dieses strukturierte Vorgehen wird Security-by-Design sichergestellt.

Innovationen und Perspektiven

Die angestrebte Modellierung und kontinuierliche Prüfung dient einer zertifizierungsfesten Planung und Dokumentation der Fertigungsprozesse. So können elektronische Bauteile, etwa in Fahrzeugen, vertrauenswürdig abgesichert werden.

Verbundkoordinator

Elmos Semiconductor AG
Dr. Roland Krumm
Heinrich-Hertz-Str. 1
44227 Dortmund
Tel.: +49 231 7549-585
E-Mail: roland.krumm@elmos.com

Projektvolumen

6,35 Mio. Euro
BMBF-Förderung: 4,10 Mio. Euro (65 %) zzgl. 0,56 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.
Im Förderschwerpunkt „Vertrauenswürdige Elektronik (ZEUS)“ gefördert.

Projektlaufzeit

01.05.2021 bis 30.04.2024

Projektpartner

- Elmos Semiconductor AG, Dortmund
- Cadence Design Systems GmbH, Feldkirchen
- DENSO AUTOMOTIVE Deutschland GmbH, Eching
- Giesecke+Devrient Mobile Security GmbH, München
- IMST GmbH, Kamp-Lintfort
- Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC, Garching b. München;
- Fraunhofer-Institut für Mikroelektronische Schaltungen und Systeme IMS, Duisburg;
- Universität Bielefeld, Bielefeld

Know-how-Schutz und Identifizierbarkeit von Elektronikkomponenten für vertrauenswürdige Produktionsketten (VE-FIDES)

Ziele und Vorgehen

Die lückenlose Rückverfolgbarkeit und der Nachweis der Echtheit einzelner Komponenten entlang der Produktionskette gestaltet sich zunehmend schwieriger. Im Projekt VE-FIDES werden Lösungen entwickelt, um eine eindeutige und vertrauenswürdige digitale Identität zu ermöglichen. Dazu werden elektronische Bauteile mit digitalen Echtheitsmerkmalen ausgestattet. Entlang der Produktionskette soll modular aus den einzelnen digitalen Eigenschaften ein umfassendes Gesamtsystem zur Identifikation des fertigen Produkts aufgebaut werden. Die Funktionalität soll anhand eines Tachographen-Systems, das oft Manipulationsversuchen ausgesetzt ist, demonstriert werden.

Innovationen und Perspektiven

Die Projektergebnisse können in internationale Standards einfließen, wodurch branchenübergreifend die Vertrauenswürdigkeit und Integrität von Komponenten erhöht und die Produktpiraterie verhindert wird.

Verbundkoordinator

Siemens AG
Daniel Schneider
Werner-von-Siemens-Straße 1
80333 München
Tel.: +49 89 636-00
E-Mail: schneider.ds.daniel@siemens.com

Projektvolumen

5,99 Mio. Euro
BMBF-Förderung: 4,17 Mio. Euro (70 %) zzgl. 0,34 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.03.2021 bis 29.02.2024

Projektpartner

- Siemens AG, München
- Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC, München
- Technische Universität München, München
- Universität Ulm, Ulm
- Continental Automotive GmbH, Villingen-Schwenningen
- Infineon Technologies AG, Neubiberg
- Bischoff Elektronik GmbH, Oberstadt

Vertrauenswürdige Spezialprozessoren

Für Zukunftsaufgaben wie das autonome Fahren oder Industrie 4.0 müssen immer größere Mengen an Daten von einer steigenden Anzahl Sensoren mit Hilfe komplexer Algorithmen und künstlicher Intelligenz (KI) in kürzester Zeit analysiert werden. Die entsprechenden Prozessoren müssen aber nicht nur bei der Rechenleistung, sondern auch hinsichtlich Energieeffizienz, Zuverlässigkeit, Robustheit und Sicherheit hohe Anforderungen erfüllen, die über aktuelle Möglichkeiten weit hinausgehen. Die ZuSE-Projekte des BMBF sollen den dringenden Bedarf der Anwenderbranchen an zukunftsfähigen, vertrauenswürdigen Prozessoren decken, die auf ihre spezifischen Aufgaben zugeschnitten und hoch performant sind.

Ansprechpartner
Dr. Sebastian Jester
Referat: Elektronik und autonomes Fahren; Supercomputing
E-Mail: Sebastian.Jester@bmbf.bund.de

ZuSE

Anwendungsspezifischer KI-Prozessor für die intelligente Bildverarbeitung im autonomen Fahren (KI-AVF)

Ziele und Vorgehen

Ziel des Vorhabens ist die Entwicklung einer Vektorprozessorarchitektur für rechenintensive KI-Anwendungen in Fahrerassistenzsystemen. Dank anwendungsspezifischer Anpassungen und Skalierbarkeit der Rechenleistung soll der Prozessor flexibel für die Verarbeitung unterschiedlicher Sensordaten optimiert werden. Im Vorhaben werden kamera-, radar- und lidarbasierte KI-Anwendungen erforscht und dafür optimierte Prozessoren entwickelt. Für die optimale Abbildung der entwickelten KI-Algorithmen in einer Prozessorarchitektur wird ein spezieller Compiler erarbeitet. Eine breitbandige Speicheranbindung soll zudem die echtzeitfähige Datenverarbeitung gewährleisten. Zuletzt werden Aspekte der funktionalen Sicherheit sowie die Logikverschlüsselung zur Verhinderung eines Eingriffs durch Dritte erforscht und implementiert.

Innovationen und Perspektiven

Die flexible und skalierbare Prozessorarchitektur wird als Open-Source-Komponente veröffentlicht und bietet ein breites industrielles Nutzungspotenzial in der für Deutschland wichtigen Schlüsseltechnologien KI und dem Anwendungsbereich autonomes Fahren.

Verbundkoordinator

Gottfried Wilhelm Leibniz Universität Hannover
Prof. Dr. Holger Blume
Appelstr. 4
30167 Hannover
Tel.: +49 511 762-19640
E-Mail: blume@ims.uni-hannover.de

Projektvolumen

6,43 Mio. Euro
BMBF-Förderung: 3,58 Mio. Euro (58 %) zzgl. 0,28 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.10.2020 bis 30.09.2023

Projektpartner

- Gottfried Wilhelm Leibniz Universität Hannover, Hannover
- Dream Chip Technologies GmbH, Garbsen
- Robert Bosch GmbH, Gerlingen-Schillerhöhe
- Cadence Design Systems GmbH, Feldkirchen
- Rheinisch-Westfälische Technische Hochschule Aachen, Aachen
- Technische Universität Kaiserslautern, Kaiserslautern

Plattform für energieeffiziente KI-Prozessoren in mobilen Anwendungen (KI-mobil)

Ziele und Vorgehen

Ziel des Vorhabens ist die Entwicklung einer Prozessorplattform für die Entwicklung hoch performanter Elektronik für rechenintensive KI-Anwendungen. Als Kernkomponente wird ein KI-Beschleuniger mit einer flexiblen, erweiterbaren und skalierbaren System-on-Chip-Architektur (SoC) entwickelt. Um einen niedrigen Energieverbrauch zu erreichen, wird der Beschleuniger für KI-Algorithmen im Bereich des autonomen Fahrens optimiert und in der energieeffizienten 22-nm-FDX-Halbleitertechnologie gefertigt. Darüber hinaus wird ein Ökosystem aufgebaut, das ein Entwicklungssystem sowie ein deutsches Partnernetzwerk mit Know-how im KI-Hardware-Entwurf vereint. Die Flexibilität und Skalierbarkeit der Leistungsdaten der Prozessorplattform wird anhand von Demonstratoren verifiziert.

Innovationen und Perspektiven

Der rechenstarke KI-Beschleuniger, die flexible und skalierbare SoC-Architektur sowie das Ökosystem bilden eine Plattform für die kostengünstige Entwicklung anwendungsspezifischer KI-Hardware in Deutschland und sind für zukünftige Innovationen breit einsetzbar.

Verbundkoordinator

Bayerische Motoren Werke Aktiengesellschaft
Dr. Hans-Jörg Vögel
Petuelring 130
80788 München
Tel.: +49 89 382-68874
E-Mail: hans-joerg.voegel@bmwgroup.com

Projektvolumen

9,99 Mio. Euro
BMBF-Förderung: 6,26 Mio. Euro (63 %) zzgl. 0,43 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.05.2020 bis 30.04.2023

Projektpartner

- Bayerische Motoren Werke AG, München
- Technische Universität Dresden, Dresden
- Karlsruher Institut für Technologie, Karlsruhe
- Infineon Technologies AG, Neubiberg
- T3-Technologies, Dresden
- Gottfried Wilhelm Leibniz Universität Hannover, Hannover

Entwicklungsplattform für KI-basierte und hochdynamische Regelungsverfahren für die Leistungselektronik (KI-Power)

Ziele und Vorgehen

Ziel des Projektes ist es, eine modulare und skalierbare Entwicklungsplattform für leistungselektronische Systeme zu entwerfen. Die Steuereinheiten dieser Systeme benötigen eine Rechenleistung, die immer stärker durch das komplexe Zusammenspiel von Datenerfassung, -übertragung, -interpretation und Speicherzugriffen bestimmt wird. Dafür sind KI-Algorithmen besonders geeignet. Im Projekt werden auf Basis der neuen Entwicklungsplattform System-on-Chip-Lösungen mit KI-Prozessoren entwickelt. Diese Prozessoren haben eine hohe Rechenleistung und können die Berechnungen für KI-Algorithmen zur Steuerung von leistungselektronischen Systemen schnell und effizient durchführen.

Innovationen und Perspektiven

Die neue Plattform soll Hardwarebeschleuniger für die heterogene Berechnung von KI-Algorithmen für ein möglichst breites Anwenderspektrum im industriellen Umfeld, insbesondere kleiner und mittelständischer Unternehmen, zugänglich machen. Die geplanten Ergebnisse sollen auch in andere KI-Anwendungen übertragen werden.

Verbundkoordinator

Technische Hochschule Nürnberg Georg Simon Ohm
Prof. Dr. Armin Dietz
Postfach 21 03 20
90121 Nürnberg
Tel.: +49 911 5880-1814
E-Mail: armin.dietz@th-nuernberg.de

Projektvolumen

1,63 Mio. Euro
BMBF-Förderung: 1,46 Mio. Euro (79 %) zzgl. 0,16 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

15.06.2020 bis 14.06.2023

Projektpartner

- Technische Hochschule Nürnberg Georg Simon Ohm, Nürnberg
- Technische Universität München, München
- Kübrich Ingenieurgesellschaft mbH & Co. KG, Priesendorf
- Trenz Electronic GmbH, Hüllhorst
- Afag GmbH, Ambach

Entwicklungsplattform und Ökosystem für skalierbare Spezialprozessoren im Edge-Computing (ZuSE-Scale4Edge)

Ziele und Vorgehen

Das Vorhaben Scale4Edge erforscht, wie Entwicklungszeit und -kosten anwendungsspezifischer Edge-Prozessoren signifikant reduziert werden können. Solche Prozessoren führen meist mobil und nahe an Sensoren, an der Schnittstelle von der realen zur virtuellen Welt, entscheidende erste Berechnungen aus. Sie müssen deshalb nicht nur besonders zuverlässig, performant und robust, sondern auch energieeffizient arbeiten. Darüber hinaus müssen sie ein hohes Maß an Vertrauenswürdigkeit bieten. Mit der entstehenden skalierbaren und flexibel erweiterbaren Entwicklungsplattform auf Basis des lizenzfreien, quelloffenen RISC-V-Befehlssatzarchitektur können individuelle Prozessoren mit diesen Eigenschaften effizient und kostengünstig entwickelt werden.

Innovationen und Perspektiven

Die Entwicklungsplattform soll ein vollständiges, kommerziell zugängliches Ökosystem mit allen nötigen Entwicklungskomponenten bieten. Speziell KMU können davon profitieren und kostengünstig performante, innovative Edge-Geräte für verschiedene Anwendungen wie das Autonome Fahren oder die Industrie 4.0 entwickeln.

Verbundkoordinator

Infineon Technologies AG
Prof. Dr. Wolfgang Ecker
Am Campeon 1 – 15, 85579 Neubiberg
Tel.: +49 89 234-45334
E-Mail: wolfgang.ecker@infineon.com

Projektvolumen

24,44 Mio. Euro
BMBF-Förderung: 15,97 Mio. Euro (65 %) zzgl. 1,32 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen.

Projektlaufzeit

01.05.2020 bis 30.04.2023

Projektpartner

- Infineon Technologies AG, Neubiberg
- concept engineering GmbH ASIC- und Softwaretechnologie, Freiburg
- TU Kaiserslautern, Kaiserslautern
- AbsInt Angewandte Informatik GmbH, Saarbrücken
- FZI Forschungszentrum Informatik, Karlsruhe
- Universität Bremen, Bremen
- Robert Bosch GmbH, Gerlingen-Schillerhöhe
- Eberhard-Karls-Universität Tübingen, Tübingen
- OFFIS e.V., Oldenburg
- TU München, München
- Albert-Ludwigs-Universität Freiburg, Freiburg
- Universität Paderborn, Paderborn
- IHP GmbH - Innovations for High Performance Microelectronics/Leibniz-Institut für innovative Mikroelektronik, Frankfurt/Oder
- MINRES GmbH, Neubiberg
- TU Dresden, Dresden
- ARQUIMEA Deutschland, Frankfurt/Oder
- SYSGO GmbH, Klein-Winternheim
- TU Darmstadt, Darmstadt
- EPOS GmbH, Duisburg

Europäische Projekte mit einem vertrauenswürdigen Forschungsschwerpunkt

Europa und vor allem Deutschland besitzen in der Mikroelektronik besondere Stärken in der Automobil-, Energie-, Sicherheits- und Industrieelektronik. Um die Mikroelektronikkompetenz im Hinblick auf eine breite Digitalisierung zu stärken, fördert die Europäische Kommission gemeinsam mit Mitgliedsstaaten in der Initiative ECSEL Forschungsvorhaben und Pilotlinien. Deutsche Schwerpunkte liegen dabei auf multifunktionalen Elektroniksystemen, energiesparender Leistungselektronik, Design komplexer Systeme sowie Produktionstechnologien.

Ansprechpartner
Dr. Sebastian Jester
Referat: Elektronik und autonomes Fahren; Supercomputing
E-Mail: Sebastian.Jester@bmbf.bund.de

KI für neue Elektroniksysteme und Edge-Computing-Technologien (ANDANTE)

Ziele und Vorgehen

Neuronale Netze oder andere Methoden Künstlicher Intelligenz stellen besonders hohe Anforderungen an die Vertraulichkeit, Informationssicherheit, Echtzeitfähigkeit und Energieeffizienz. Anwendungsspezifische, multifunktionale Elektroniksysteme, die auf dedizierten Halbleiterchips aufbauen, sind ein vielversprechender Ansatz zur Lösung dieser Herausforderungen. Solche Chips implementieren maßgeschneidert die Funktionen neuronaler Netze und ermöglichen so eine effizientere Berechnung spezieller Aufgaben im Vergleich zu Universalprozessoren. Im Vorhaben ANDANTE wird neuartige, performante Hardware für neuronale Netze entwickelt. Dazu gehören Elektronikbausteine wie Speicher oder spezifische Rechenblöcke, um die Vertrauenswürdigkeit sicherzustellen. Zudem sollen Schnittstellen für die Integration von bestehenden Sensoren entwickelt werden.

Innovationen und Perspektiven

Das Konsortium bündelt auf europäischer Ebene die Kompetenzen von Forschungseinrichtungen und Industriepartnern. Mit der anwendungsorientierten Forschung an KI-basierten Hardwarelösungen für die Datenauswertung in den Bereichen autonomes Fahren, Industrieautomation und Gesundheit leistet es einen wesentlichen Beitrag zur Sicherung der deutschen Wettbewerbsfähigkeit und zum Ausbau der technologischen Souveränität Europas.

Verbundkoordinator

Infineon Technologies AG
Holger Schmidt
Am Campeon 1 - 15
85579 Neubiberg
Tel.: +49 89 234-23417
E-Mail: holger.schmidt2@infineon.com

Projektvolumen

40,58 Mio. Euro
Gesamtfördersumme (EU und Mitgliedsstaaten): 23,95 Mio. Euro
Nationale Fördersummen:
BMBF: 3,09 Mio. Euro (zzgl. 0,02 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen)
Freistaat Sachsen: 1,22 Mio. Euro

Projektlaufzeit

01.07.2020 bis 31.05.2023

Projektpartner

- Infineon Technologies AG, Neubiberg
- Ferroelectric Memory GmbH, Dresden
- Valeo Schalter und Sensoren GmbH, Bietigheim-Bissingen
- eesy-innovation GmbH, Unterhaching
- Fraunhofer-Institut für Photonische Mikrosysteme IPMS, Dresden
- Fraunhofer-Institut für Integrierte Schaltungen IIS, Erlangen
- Fraunhofer-Einrichtung für Mikrosysteme und Festkörper-Technologien EMFT, München
- Technische Universität Dresden, Dresden
- Friedrich-Alexander-Universität Erlangen-Nürnberg, Erlangen
- Heimann Sensor GmbH, Dresden

Robuste Elektroniksysteme für quantifizierbare Sicherheit im autonomen Fahren (ArchitectECA2030)

Ziele und Vorgehen

Ein höherer Automatisierungsgrad bei Fahrzeugen geht nur mit einer erhöhten Zuverlässigkeit und Sicherheit der einzelnen Komponenten. Ziel im Projekt ArchitectECA2030 ist es, einen Rahmen für die valide Entwicklung elektronischer Komponenten zu schaffen. Damit soll ein akzeptables Restrisiko erreicht und neue internationale Standards vorangetrieben werden, die für die Genehmigung autonomer Fahrzeuge erforderlich sind. Der neue methodische Ansatz beinhaltet Sicherheitsfunktionen im Design elektrischer Komponenten zu verankern sowie akzeptable Risikoniveaus für elektronische Systeme zu definieren. Hierfür wird u. a. ein fahrzeuginternes Überwachungsgerät entwickelt, mit dem der Zustand der Funktionselektronik bestimmt werden kann.

Innovationen und Perspektiven

Der Erfolg des autonomen Fahrens hängt stark von der Zuverlässigkeit und Sicherheit sowie der gesellschaftlichen Akzeptanz ab. Durch neue Standards können die Risiken quantifiziert und hochautomatisierte Fahrzeuge genehmigt werden. Dies ist nur durch eine internationale Zusammenarbeit und Abstimmung möglich.

Verbundkoordinator

Infineon Technologies AG
Reiner John
Am Campeon 1 - 15
85579 Neubiberg
Tel.: +49 89 234-41310
E-Mail: reiner.john@infineon.com

Projektvolumen

13,69 Mio. Euro
Gesamtfördersumme (EU und Mitgliedsstaaten): 7,38 Mio. Euro.
Nationale Fördersummen:
BMBF: 0,57 Mio. Euro (zzgl. 0,02 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen)

Projektlaufzeit

01.07.2020 bis 30.06.2023

Projektpartner

- Infineon Technologies AG, Neubiberg
- VOLKSWAGEN AKTIENGESELLSCHAFT, Wolfsburg
- Technische Universität Dresden,Dresden
- SafeTRANS e. V., Oldenburg

Cyber-Sicherheit für hochautomatisierte Systeme und das autonome Fahren (SECREDAS)

Ziele und Vorgehen

Ziel des Projektes SECREDAS ist, eine umfassende Sicherheitsplattform für hochautomatisierte vernetzte Systeme aus den Bereichen Automobil, Schienenverkehr und Gesundheitsversorgung aufzubauen. Um die Betriebssicherheit des Systems und die Sicherheit von Personen und deren Privatsphäre lückenlos zu gewährleisten, werden anhand konkreter Risikoszenarien neue Sicherheitskonzepte entwickelt. Diese fließen sowohl in den Aufbau von System- und Netzwerkarchitekturen als auch in die Erfassung und Verarbeitung von Sensordaten mit ein. Die Sicherheitskonzepte können später in autonom fahrenden Automobilen oder bei der Überwachung des Gesundheitszustands des Fahrers eingesetzt werden.

Innovationen und Perspektiven

In den Bereichen Automobil, Schienenverkehr und Gesundheit werden künftig immer mehr Systeme automatisiert und vernetzt. Für eine breite gesellschaftliche Akzeptanz dieser Entwicklungen müssen die Betriebssicherheit und die Privatsphäre der Nutzer gewährleistet werden und in Industriestandards und Gesetze einfließen. Das Projekt liefert dazu einen wichtigen Beitrag, indem es Sicherheitsaspekte von Beginn an als feste Bestandteile von technischen Komponenten und Systemarchitekturen berücksichtigt.

Verbundkoordinator

senetics healthcare group GmbH & Co. KG
Dr. Michael Wiehl
Eyber Straße 89, 91522 Ansbach
Tel.: 0981 9724 7954
E-Mail: michael.wiehl@senetics.de

Projektvolumen

51,50 Mio. Euro.
Gesamtfördersumme (EU und Mitgliedsstaaten): 24,07 Mio. Euro.
Deutsches Projektvolumen: 10,25 Mio. Euro.
Nationale Förderung:
BMBF: 2,41 Mio. Euro (zzgl. 0,04 Mio. Euro sog. Projektpauschale an die beteiligte Hochschule)

Projektlaufzeit

01.06.2018 bis 30.04.2021

Projektpartner

- senetics healthcare group GmbH & Co. KG, Ansbach
- NXP Semiconductors Germany GmbH, Hamburg
- AVL Software and Functions GmbH, Regensburg
- Roche PVT GmbH, Waiblingen
- Fraunhofer Institut für Experimentelles Software Engineering IESE, Kaiserslautern
- Giesecke+Devrient Mobile Security GmbH, München
- ZF Friedrichshafen AG, Friedrichshafen
- Technische Universität Kaiserslautern, Kaiserslautern
- Merantix GmbH, Berlin

Technologie und Hardware für neuromorphe Computersysteme (TEMPO)

Ziele und Vorgehen

Nichtflüchtige Speicher sind ein zentraler Baustein der modernen Mikroelektronik. Sie werden für Anwendungen in der künstlichen Intelligenz, beim Maschinellen Lernen und beim neuromorphen Rechnen stark an Bedeutung gewinnen. Dies gilt insbesondere für das autonome Fahren, smarte Heimanwendungen und spezielle Industrieanwendungen, die aufgrund der hohen zu bearbeitenden Datenvolumen einen großen Speicherbedarf haben. Im Projekt werden neuartige Speicher-Chips entworfen und gefertigt. Sie sollen hauptsächlich für Klassifikationsaufgaben in Bilderkennungssystemen für das autonome Fahren, aber auch für die Verarbeitung weiterer Sensordaten z. B. von Radarsystemen eingesetzt werden.

Innovationen und Perspektiven

Mikroelektronik-Systeme für aktuelle gesellschaftliche Herausforderungen, wie das autonome Fahren oder eine intelligente Servicerobotik, erfordern eine stetig steigende Anzahl von Sensoren und anderer elektronischer Bauteile zur Datenaufnahme und Datenverarbeitung, mit entsprechend steigenden Datenmengen. Die innovative Mikroelektronik und neue Algorithmen aus TEMPO ermöglichen eine Vorverarbeitung, mit der trotz zunehmender Datenmengen der Bedarf an Speicher- und Übertragungskapazität reduziert werden kann. Dies ist eine zentrale Voraussetzung für die breite Nutzung hochkomplexer autonomer Systeme.

Verbundkoordinator

Infineon Technologies AG
Holger Schmidt
Am Campeon 1 – 15, 85579 Neubiberg
Tel.: +49 89 234-23417
E-Mail: holger.schmidt2@infineon.com

Projektvolumen

35,08 Mio. Euro
Gesamtfördersumme (EU und Mitgliedsstaaten): 20,03 Mio. Euro.
Deutsches Projektvolumen: 18,96 Mio. Euro.
Nationale Fördersummen:
BMBF: 2,76 Mio. Euro (zzgl. 0,01 Mio. Euro sog. Projektpauschale an beteiligte Hochschulen)
Freistaat Sachsen: 0,58 Mio. Euro

Projektlaufzeit

15.06.2019 bis 30.04.2022

Projektpartner

- Infineon Technologies AG, Neubiberg
- Fraunhofer-Institut für Integrierte Schaltungen IIS, Erlangen
- Fraunhofer-Einrichtung für Mikrosysteme und Festkörper-Technologien EMFT, München
- Robert Bosch GmbH, Gerlingen-Schillerhöhe
- InnoSenT GmbH, Donnersdorf
- Valeo Schalter und Sensoren GmbH, Bietigheim-Bissingen
- Fraunhofer-Institut für Photonische Mikrosysteme IPMS, Dresden
- Technische Universität Dresden, Dresden

Impressum

Herausgeber
Bundesministerium
für Bildung und Forschung (BMBF)
Referat Elektronik und Autonomes Fahren; Supercomputing
53170 Bonn

Stand
Mai 2021

Text
BMBF

Gestaltung
VDI/VDE-IT, Berlin

Bildnachweise
Titelbild, S. 19, S. 24: Gorodenkoff/AdobeStock
S. 3: VDI/VDE-IT

@BMBF_Bund
@bmbf.de
@bmbf.bund

bmbf.de