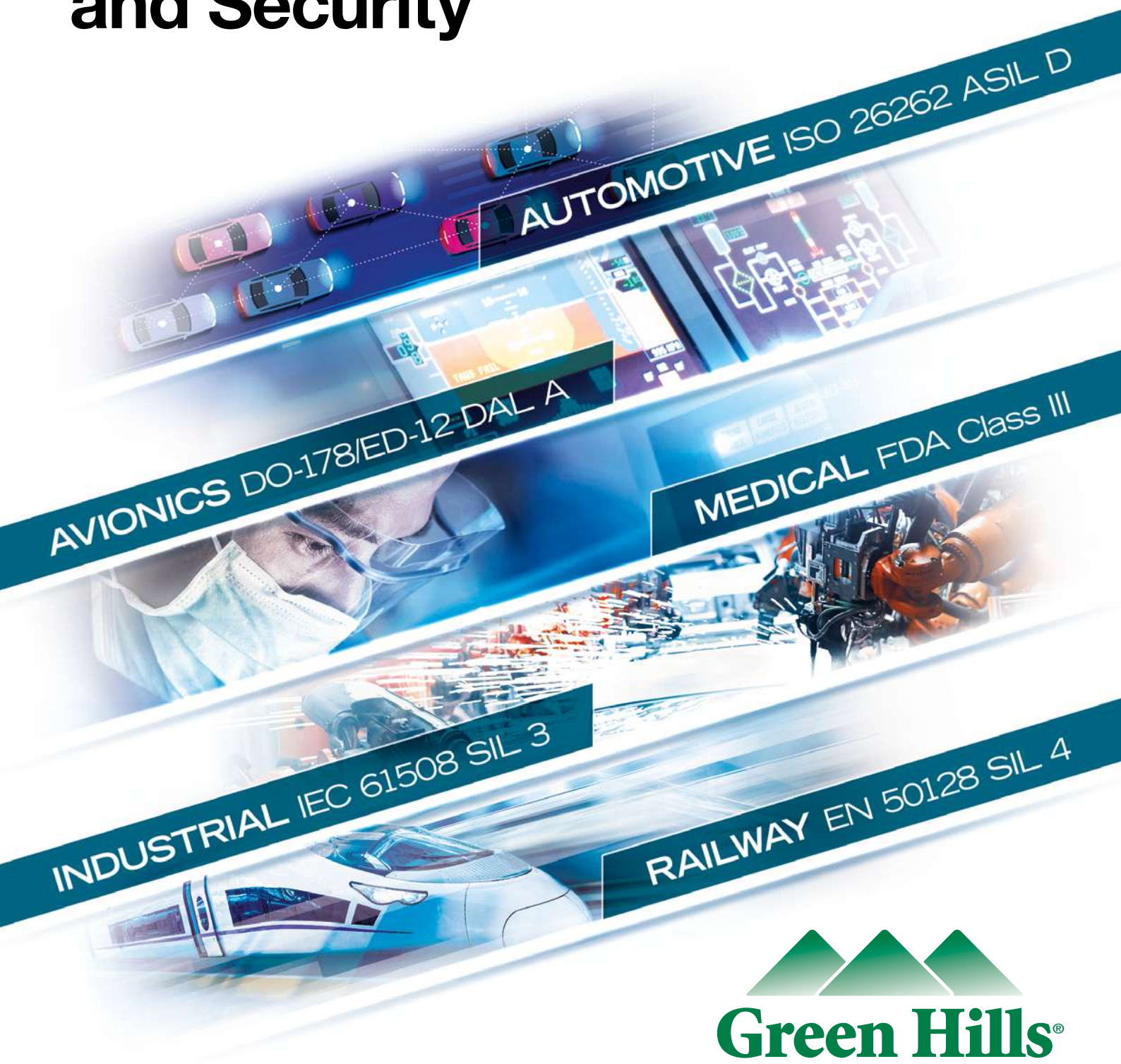
Tagungsband

Embedded Software Engineering Kongress 2023

www.ese-kongress.de

Embedded Software Engineering Kongress

Develop Your Software to the Highest Levels of Safety and Security



Green Hills® SOFTWARE

For over 40 years, world-class companies have trusted Green Hills Software's integrated software platforms, engineering services, and certification experts as the foundation to develop and deploy next-generation embedded systems with confidence to the highest levels of safety and security.

Call us on **+49 228 4330 777** or contact us at **ghs.com/go/contact**

Tagungsband

Embedded Software Engineering Kongress 2023

4. bis 8. Dezember 2023

Preconference 1. Dezember 2023

Kongressbeirat 2023:

Stephan Ahrends
Jan Altenberg, Open Source Automation Development Lab (OSADL) eG
Thomas Batt, MicroConsult GmbH
Michael Bayer, The Happy Zebra Project
Maria Beyer-Fistrich, Vogel Communications Group GmbH & Co.KG
Roland Bickel, Hitex GmbH
Prof. Dr. Gert Bikker, Ostfalia Hochschule
Prof. Dr. Heinz-Peter Bürkle, Hochschule Aalen
Henning Butz
Raphael Dunker, SEW-EURODRIVE GmbH & Co. KG
Thomas Eisenbarth, Axivion GmbH
Dr. Carsten Emde, Open Source Automation Development Lab (OSADL) eG
Sebastian Gerstl, Heise Medien GmbH & Co.KG
Wolfram Gettert, Mixed Mode GmbH
Peter Gliwa, GLIWA embedded systems
Dr.-Ing. René Graf, Siemens AG
Rainer Grimm, Modernes C++
Martina Hafner, genua GmbH
Prof. Dr. Georg Hagel, Hochschule Kempten
Andreas Klinger, IT-Klinger
Maximilian Koller, intive automotive GmbH
Prof. Dr. Rainer Koschke, Universität Bremen
Caren Kresse, Open Source Automation Development Lab (OSADL) eG
Dr. Thomas Kuhn, Fraunhofer Institut IESE
Wolfgang Leimbach, SodiusWillert SAS
Prof. Dr. Jens Liebehenschel, Frankfurt University of Applied Sciences
Frank Listing, VoltStorage
Remo Markgraf, MicroConsult GmbH
Dr. Albrecht Mayer, Infineon Technologies
Prof. Dr. Jürgen Mottok, OTH Regensburg
Gudrun Neumann, SGS-TÜV Saar GmbH
Karl Nieratschker, SKT Nieratschker
Richard Oed, Richard Oed inelligent Engineering
Daniel Penning, embeff GmbH
Ingo Pohle, MicroConsult GmbH
Heiko Rießland, PLS Programmierbare Logik & Systeme GmbH
Stephan Roth, oose Innovative Informatik
Florian Schäffer, Grollmus München GmbH
Dr. Joachim Schlosser, Elektrobit Automotive GmbH
Marco Schmid, Schmid Elektronik AG
André Schmitz, Green Hills Software
Thomas Schütz, PROTOS Software GmbH
Prof. Dr. Christian Siemers, TU Clausthal
Peter Siwon, Systemisches Projektmanagement
Peter Sommerlad, Better Software
Andreas Stucki, Solcept AG
Klaus-Dieter Walter, SSV Software Systems GmbH
Siegfried Weigert, ibw industrieberatung
Johann Wiesböck
Andreas Willert, SodiusWillert SAS

Die Informationen in diesem Tagungsband werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

Die Texte und Abbildungen dieses Tagungsbandes wurden mit größter Sorgfalt zusammengestellt. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren übernehmen für fehlerhafte Angaben und deren Folgen weder eine juristische noch eine sonstige Haftung.

Für Verbesserungsvorschläge und Hinweise sind der Verlag und Herausgeber dankbar.

Copyright 2023
ELEKTRONIKPRAXIS
Vogel Communications Group GmbH & Co. KG
Max-Planck-Straße 7/9
97082 Würzburg

und

MicroConsult Microelectronics Consulting & Training GmbH
Charles-de-Gaulle-Straße 6
81737 München

ISBN 978-3-8343-6314-5

Analyse.
Automate.
Accelerate.
Assure Quality.

Statische Analyse- und dynamische Testing-Tools für zukunftssichere Software-Entwicklung

Squish | Coco | Test Center | Axivion Static Code Analysis | Axivion Architecture Verification

Squish

Plattformunabhängiges funktionales GUI Testing Tool für praktisch jede Desktop-, Mobile-, Web-Oberfläche oder integrierte Systeme

Coco

Dynamische Überprüfung der Code-Abdeckung um Test-Protokolle zu optimieren und ein neues Level von Produktqualität zu erreichen

Test Center

Zentralisierte Testergebnis-Management Plattform zur Verbindung von Testautomatisierung mit dem gesamten Entwicklungsprozess

Regelkonformität

+ ISO 26262
+ ISO 14971
+ IEC 61508
+ IEC 62304
+ EN 50128 / EN 50657
+ SPICE® / ASPICE

Sicherheit

+ MISRA C/C++
+ CERT®
+ AUTOSAR C++14
+ CWE
+ ISO/IEC TS 17961
+ FDA Vorgaben

Axivion Architecture Verification

Architektur-Wiedergewinnung und -Archäologie für langfristig zielgerichtete und geplante Entwicklung von Software

Optimierte Lösungen

+ reibungslose Integration in vorhandene Tool Chain, CI/DevOps und IDE
+ individualisierbar
+ Service, Support, Coaching und Schulungen

Axivion Static Code Analysis

Umfassende statische Analyse um Software Erosion zu stoppen, potentielle Runtime Fehler zu finden und ROI zu verbessern

www.qt.io/quality-assurance

Qt Quality Assurance

Inhaltsverzeichnis

KEYNOTE

ARCHITEKTUR

ECHTZEIT

IMPLEMENTIERUNG

TEST & QUALITÄT

VECTOR

Empowering Continuous Embedded Software Development and Testing

DevOps for System Testing

Set up your DevOps environment using Vector's virtual execution environments. Vector provides ready-to-run solutions for software-in-the-loop testing. Build the test platform based on open and partly free tooling without vendor lock-in. Depending on the use case, choose the appropriate building blocks from Vector and 3rd-party to test interactively or automated in virtual environments.

Increasing Software Quality, Minimize Technical Debt

The more complex software becomes, the more important it is to monitor its quality to identify weaknesses and take countermeasures in good time.
Vector offers tools to analyze and test embedded software, with and without safety requirements.

Embedded Software

Vector is shaping the future of the Software-Defined Vehicle with an open DevOps toolchain and modular software platform. OEMs and suppliers worldwide benefit from first-class basic software tools and solutions for the development of embedded systems. The Vector Software Factory supports and automates workflows to implement your SDV project quickly and effectively.

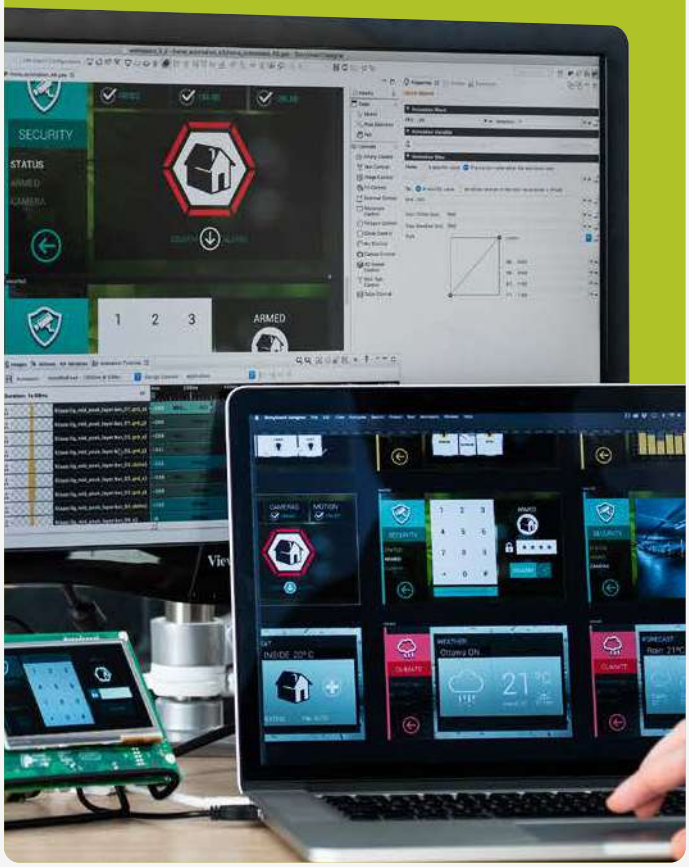
KI & MACHINE LEARNING

OPEN SOURCE

SAFETY

CRANK®
AMETEK

Make Embedded GUI Development Effortless With **Crank Storyboard**



Embedded Software Engineering Kongress

December 4th - 8th, 2023

Visit our Booth at ESE Kongress to Learn More!

SECURITY

AUTOMOTIVE

IOT & INDUSTRIE 4.0

TECHNOLOGIE – FORSCHUNG – INNOVATION

AGILE TRANSFORMATION

SOFTWARE ENGINEERING MANAGEMENT

MENSCH – TEAM – MANAGEMENT

PROJECT STORIES

TIPPS – TRICKS – LÖSUNGEN – VORTRAG-ABSTRACTS DER PRECONFERENCE

LACHMANN & RINK | PARTNER FOR SMART INDUSTRIAL SOLUTIONS

Digitale Lösungen für die Smart Industry.

Kundenspezifische Softwareentwicklung für die Industrielle Interoperabilität.

Wir sind Ihr verlässlicher Partner für Smart Industrial Solutions. Als Südwestfalens größtes Beratungs- und Entwicklungszentrum für Industriesoftware realisieren wir individuelle Lösungen des Maschinen- und Anlagenbaus sowie des produzierenden Gewerbes. Wir machen Industrie smart und intelligent, verleihen Maschinen neue Funktionalitäten, vernetzen sie, optimieren Prozesse und kreieren innovative Geschäftsmodelle.

Mit Stolz verhelfen wir Technologie- und Weltmarktführern durch die Entwicklung von Maschinensoftware, IIoT, Embedded, IT/OT, Cloud-Diensten, Digitalen Zwillingen u.v.m. zu ihrem Projekterfolg.

- ✓ Über 100 Entwickler an zwei Standorten
- ✓ Eigenes großes Hardware- und Maschinenlabor
- ✓ Seit 40 Jahren zuverlässiger Entwicklungsprofi
- ✓ Seit 1998 durchgängig DIN EN ISO 9001 zertifiziert
- ✓ Mitglied u. a. in der OPC Foundation, EtherCAT Technology Group, VDMA
- ✓ Consulting, Software, Embedded aus einer Hand
- ✓ Unterstützung bei Ressourcen-Engpässen
- ✓ Über 100 Kunden aus rund 50 Branchen
- ✓ Breites, industrielles Branchenwissen und Umsetzungs-Know-how

LACHMANN & RINK | PARTNER FOR SMART INDUSTRIAL SOLUTIONS

Lachmann & Rink GmbH
Hauptsitz Freudenberg | Hommeswiese 129 | 57258 Freudenberg
Standort Dortmund | Otto-Hahn-Straße 18-20 | 44227 Dortmund
+49 2734 2817-0 | info@lachmann-rink.de

www.lachmann-rink.de

IoT-Sicherheit und vertrauenswürdige Elektronik

Eine Perspektive aus der Forschung zu aktuellen Risiken und zukünftigen Technologien

Dr.-Ing. Matthias Hiller, Fraunhofer AISEC[1]

Innovationen im Bereich der Hardware erweitern ständig die Grenzen von Embedded-Systemen in Bezug auf Rechenleistung, Kommunikation und Effizienz. Dies ermöglicht ihren Einsatz in immer neuen Anwendungen, z.B. in den Bereichen Internet der Dinge (IoT), Edge Computing oder eingebettete KI. Allerdings vergrößert sich dadurch auch die Angriffsfläche – und damit das Sicherheitsrisiko für das Gerät an sich, die verarbeiteten Daten, und die darauf ausgeführte Anwendung.

Eine Bestandsaufnahme: Embedded Devices im IoT aus Hardware-Sicht

Eingebettete Systeme und insbesondere vernetzte Systeme im IoT interagieren mit ihrer Umwelt durch eine Anwendung, die als Applikationssoftware auf dem System ausgeführt wird. Darunter liegen das Betriebssystem, die Systemsoftware, wie Firmware und Treiber, und schließlich auf unterster Ebene die Hardware. Fehler und Sicherheitslücken in der Applikations- und Systemsoftware können dazu führen, dass eine große Anzahl von Geräten durch remote Schnittstellen kompromittiert wird. Diese Fehler können durch Updates behoben werden. Die darunterliegende Hardware verhält sich aufgrund mehrerer Aspekte anders: sie bildet den Vertrauensanker auf dem alle weiteren Sicherheitsfunktionen, und damit die Sicherheit und Vertrauenswürdigkeit des Gesamtsystems aufbauen, und kann ohne Hardwareaustausch im Allgemeinen nicht verändert werden.

Es gibt eine Vielzahl von Gründen, warum die Hardware unter Umständen nicht ausreichenden Schutz für eine Anwendung und die verarbeiteten Daten bieten kann, wie schlichtweg das Fehlen der nötigen Features, unzureichende oder fehlerhafte Spezifikation und Implementierung, kompromittierte oder fehlerhafte Hardware, oder Angriffe durch Dritte oder auch den eigentlichen Nutzer. Um die Sicherheit eines Gerätes über die ganze Lebensdauer hinweg zu gewährleisten, ist es wichtig, dass zu Beginn sichere Hardware ausgewählt oder entwickelt wird und vertrauenswürdige Komponenten in den Systemen verbaut werden.

In einer Studie für das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden z.B. am Fraunhofer AISEC Mikrocontroller im IoT Umfeld auf ihre Sicherheit gegen

[1] Teile der vorgestellten Forschungsarbeiten wurden vom Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie durch das Projekt Trusted Electronik Center Bayern gefördert.

Seitenkanal- und Fehlerangriffe untersucht und es wurden für verschiedene Chips Möglichkeiten für Angriffe gezeigt[2].

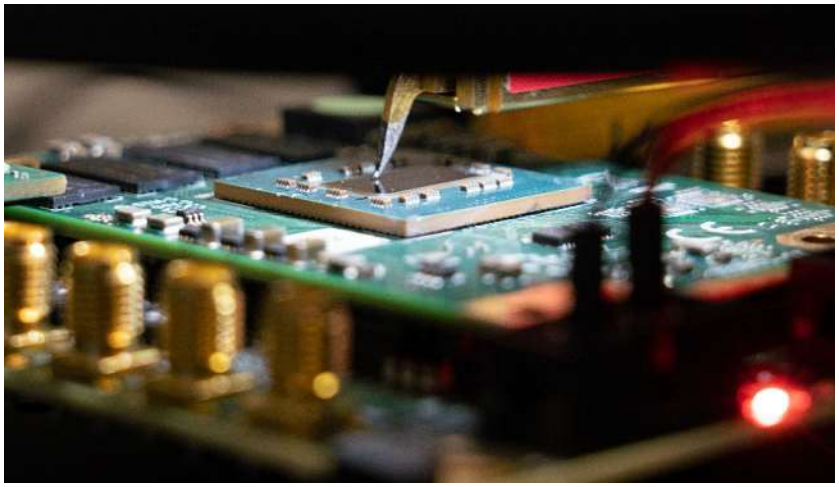


Abbildung 1: Seitenkanalangriff durch lokale EM-Abstrahlung von ICs

Durch Risikoanalysen können über alle Geräte und Anwendungen hinweg die möglichen Angriffe und dazu nötigen Schutzmaßnahmen bewertet, und so ein anwendungsspezifisches Sicherheitskonzept erstellt werden.

Technologien für resiliente Embedded-Systeme und die zugehörige Software

Zentrale Merkmale sind sichere Schlüsselspeicher, eine Umgebung zur sicheren Ausführung von Code sowie eine Implementierung kryptografischer Algorithmen, z.B. als Software-Bibliothek oder über Hardware-Beschleuniger sowie ein Zufallszahlengenerator. Wie z.B. im Projekt Keystone[3] gezeigt wurde, ist es mit diesem minimalen Set an Features möglich, grundlegende Sicherheitsfunktionalitäten bereitzustellen. Tiefer im System verankerte sichere Ausführungsumgebungen (Trusted Execution Environments) verbinden eine stärkere Separierung auf Hardware-Ebene und spielen eine immer wichtigere Rolle.

Attestierung ermöglicht, die Eigenschaften des Systems und seine Unversehrtheit gegenüber der auf dem System ausgeführten Software und nach Außen gegenüber Dritten nachzuweisen. Secure Boot und secure Update sind essenziell, um sicherzustellen, dass das System nur authentischen Code ausführt und dieser nicht verändert wurde. Weiter ist secure Update notwendig, um die Sicherheit auch langfristig zu gewährleisten. Neben sicheren Designs sind Tool-basierte Analysen und praktische Penetrationstests eine Voraussetzung, um die Effektivität der eingesetzten Maßnahmen sicherzustellen.

[2] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/Hardware-Angriffe/Hardware-Angriffe_node.html
[3] https://keystone-enclave.org/

Ausblick Forschungsthemen

Um Systeme aufbauend auf der Hardware auch langfristig abzusichern, werden in der Forschungscommunity neue Sicherheitstechnologien erforscht, die über einen Transfer in die Industrie auch nach und nach in Produkten verwendet werden. Einige Beispiele aus der aktuellen Forschung sind:

Post-Quanten-Kryptografie (PQC)

Asymmetrische kryptografische Verfahren wie RSA und ECC bilden die Grundlage unserer heutigen Kommunikation. Die Komplexität der darunter liegenden mathematischen Probleme ist für einen Quantencomputer drastisch reduziert, sodass Kommunikation, die z.B. durch ECC und RSA gesichert wurde, ggfs. durch einen Quantencomputer entschlüsselt werden kann. In den vergangen 10 Jahren wurden deshalb neue Verfahren entwickelt und werden derzeit durch verschiedene Sicherheitsbehörden, wie NIST, standardisiert[4]. Sind Daten langfristig relevant oder Systeme über Jahrzehnte im Feld, ist es wichtig, jetzt den Wechsel zu PQC-Algorithmen vorzubereiten und zu vollziehen. So wird derzeit z.B. ein Branch der Krypto-Bibliothek Botan im Auftrag des BSI um PQC-Algorithmen erweitert[5].

Durch Unterschiede in den mathematischen Verfahren, ist es nötig, Wissen und Erfahrung zu PQC zu transferieren und zu nutzen, und andererseits die grundlegenden Unterschiede weiter zu erforschen.

Abbildung 2: Arbeiten an einem Lasermessplatz für Fehlerangriffe auf eingebettete Systeme und darauf ausgeführte kryptografische Implementierungen

[4] https://csrc.nist.gov/Projects/post-quantum-cryptography
[5] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html

RISC-V

Der offene Befehlssatz RISC-V wurde in den letzten Jahren immer weiterentwickelt, um eine Alternative zu bestehenden Befehlssätzen bereitzustellen[6]. Der weitere Ausbau des Befehlssatzes und des Tool- und Software-Ökosystems wird an vielen Stellen vorangetrieben, um unterstützende Prozessoren in System-on-Chip Systemen, aber auch die eigentlichen Applikationsprozessoren zu ermöglichen. Dies ermöglicht, leichter Anpassungen an Prozessoren durchzuführen und so angepasste Chip zu fertigen.

Open-Source HW

Open-Source Software ist inzwischen ein essenzieller Baustein der IT-Landschaft geworden (z.B. Linux). RISC-V und andere offene Implementierungen stehen an der Schwelle, ähnliche Rollen einzunehmen. Das Hardware-Ökosystem stellt jedoch andere Herausforderungen, sodass sowohl die Technik als auch ihre Nutzung vorangetrieben werden müssen.

Sichere Lieferketten und Vertrauenswürdige Elektronik

Elektronik ist nur sicher, wenn sie frei von unbeabsichtigten Schwachstellen und bewusst eingebrachten Hintertüren ist, und außerdem korrekt gefertigt wurde. In der international vernetzten Lieferkette ist es derzeit unmöglich, diese Vertrauenswürdigkeit herzustellen und nachzuweisen. Initiativen wie der EU Chips Act haben das Ziel, die europäische Souveränität zu stärken und bieten Möglichkeiten für vertrauenswürdigere Lieferketten[7]. Dies setzt aber auch die Verfügbarkeit und technische Reife der eingesetzten Technologien voraus[8]. Dazu sind z.B. neue Vertrauensmerkmale - wie Hardware Fingerprinting -nötig, um einzelne Chips und Geräte über die Lieferkette nachverfolgbar zu machen und ihre Authentizität nachzuweisen. Effiziente Analysetechniken sind erforderlich, um nachzuweisen, dass Geräte frei von Trojanern und Backdoors sind; sowie Tools, um nachzuweisen, dass Tools, Designs und Software frei von Schwachstellen und Hintertüren sind.

Zusammenfassung und Ausblick

Die Sicherheit der Hardware ist Voraussetzung für die Sicherheit von Eingebetteten Systemen, aller darauf ausgeführter Software und der verarbeiteten Daten. Über die letzten Jahre wurden immer mehr Sicherheitsfeatures in Chips und Geräten implementiert, sodass das Thema Sicherheit einen breiteren Stellenwert einnimmt. Wichtig ist, dass die Features korrekt umgesetzt und verwendet werden. Dazu werden konstant neue Sicherheitsfeatures und Analysemethoden entwickelt, die ermöglichen die Sicherheit von eingebetteten Systemen und ihrer Lieferketten zu erhöhen.

Wichtige Trends dabei sind z.B. die Migration zu Post-Quanten Kryptografie, RISC-V Prozessoren und sicherer Hardware.

[6] https://riscv.org/
[7] https://digital-strategy.ec.europa.eu/de/policies/european-chips-act
[8] https://www.velektronik.de/en/referenzpapier-vertrauenswurdige-elektronik/

Autor

Dr.-Ing. Matthias Hiller leitet die Abteilung Hardware Security am Fraunhofer AISEC in Garching bei München. Vor seiner Tätigkeit am Fraunhofer AISEC studierte Matthias Hiller an den Universitäten Ulm und Portland State University, und arbeitete als Wissenschaftlicher Mitarbeiter an der Technischen Universität München.
In seiner Forschung beschäftigt er sich mit sicheren eingebetteten Systemen und vertrauenswürdiger Elektronik.