Teil II - Eingehende Darstellung

Vorhabensbezeichnung	MEDGE - Secure Low Power Medical Edge Computing
Laufzeit des Vorhabens	01.11.2022 - 31.1.2026 (verlängert)
Berichtzeitraum	01.11.2022 - 31.1.2026

AP 4: Anforderungsanalyse, Use Cases und Systemkonzept

Im Rahmen von AP 4 wurden die technischen und sicherheitsbezogenen Anforderungen der drei im Projekt betrachteten medizinischen Anwendungsfälle systematisch erhoben und in ein gemeinsames Systemkonzept überführt. Dabei wurden alle Projektpartner eingebunden, um ein konsistentes Bild der Anforderungen aus Nutzersicht zu erhalten.

Die drei Use Cases — Neurostimulationsimplantat (AP 1), Kapselendoskopie (AP 2) und hybrider Ultraschall (AP 3) — wurden hinsichtlich Funktionsumfang, Rechenleistung, physischer Beschränkungen sowie Kommunikationsanforderungen analysiert. Das daraus abgeleitete Systemkonzept beschreibt ein System aus drei Akteuren (Sensor/Implantat, Access Point, Cloud) und zwei Kommunikationsstrecken:

Figure 1: Systemkonzept der MEDGE-Plattform

Die wichtigsten zu untersuchenden Attribute umfassen Funktionsumfang und Rechenleistung, physische und energetische Beschränkungen sowie Kommunikationsprotokolle und Sicherheitsanforderungen. Diese Anforderungen bildeten die Grundlage für alle nachfolgenden Arbeitspakete.

Anforderungsanalyse Use Case 1 — Hybrider Ultraschall (AP 3)

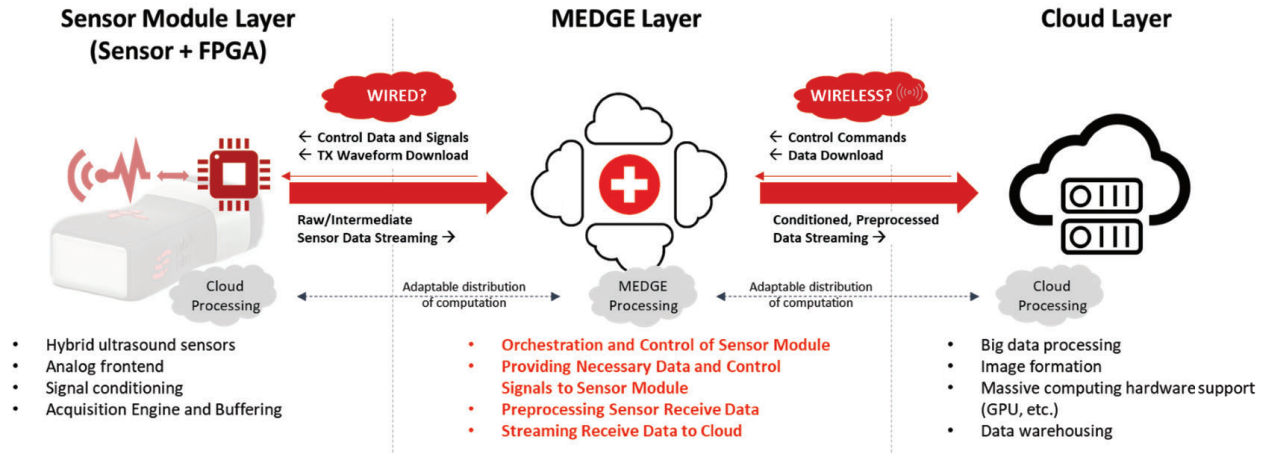

Figure 2: Hybrider Ultraschall Use Case

Der Ultraschall-Use-Case stellt die rechenintensivste der drei betrachteten Anwendungen dar. Die gesamte Verarbeitungskette umfasst die Transformation von Rohdaten in ein Bild (Fourier-Transformation, k-Raum-Koordinatentransformation, Interpolation, inverse Fourier-Transformation). Für die Vorverarbeitung auf dem MEDGE-Edge-Device sind Filterung, Demodulation, Fourier-Transformation, Kompression sowie KI-Vorverarbeitungsschritte vorgesehen.

Attribut	**Wert**
Architektur	RISC-V oder ARM, 1,0–1,5 GHz
Arbeitsspeicher	2 GB RAM
Sensoren TX	4×–16× Ultraschall-Transducer
Sensoren RX	64×–128× Kanäle
Rohdatenrate (RX)	250 Mbps/Kanal, bis zu 32 Gbps gesamt
Verarbeitungsmodus 0	4–205 Gbit/s (100 MSPS, 16 bit, 128 Kanäle)
Verarbeitungsmodus 1	2 Gbit/s (120 FPS, 128 Kanäle)
Verarbeitungsmodus 2	1 Gbit/s (30 FPS, 128 Kanäle)
Kommunikationsdatenrate	bis zu 5 Gbps
Latenz	< 200 ms
Reichweite	< 10 m

Aus sicherheitstechnischer Sicht wurde eingeschätzt, dass das Abfangen von Ultraschall-Rohdaten aufgrund der unmittelbaren Natur der Bildgebung unwahrscheinlich ist. Spezifische Authentifizierungs- und Verschlüsselungsanforderungen bestehen für diesen Use Case nicht; Jamming ist schwer zu verhindern, aber nicht sicherheitskritisch. Ein ASIC-Design bietet hier vor allem durch spezialisierte Beschleuniger Vorteile, die die hohe Rechenlast bei den geforderten Bandbreiten mit vertretbarem Energieaufwand bewältigen können. Zusammenfassend stehen beim Ultraschall-Use-Case hohe Datenraten und Energieeffizienz im Vordergrund, während Security-Anforderungen am MEDGE-Chip selbst nur eine untergeordnete Rolle spielen.

Anforderungsanalyse Use Case 2 — Kapselendoskopie (AP 2)

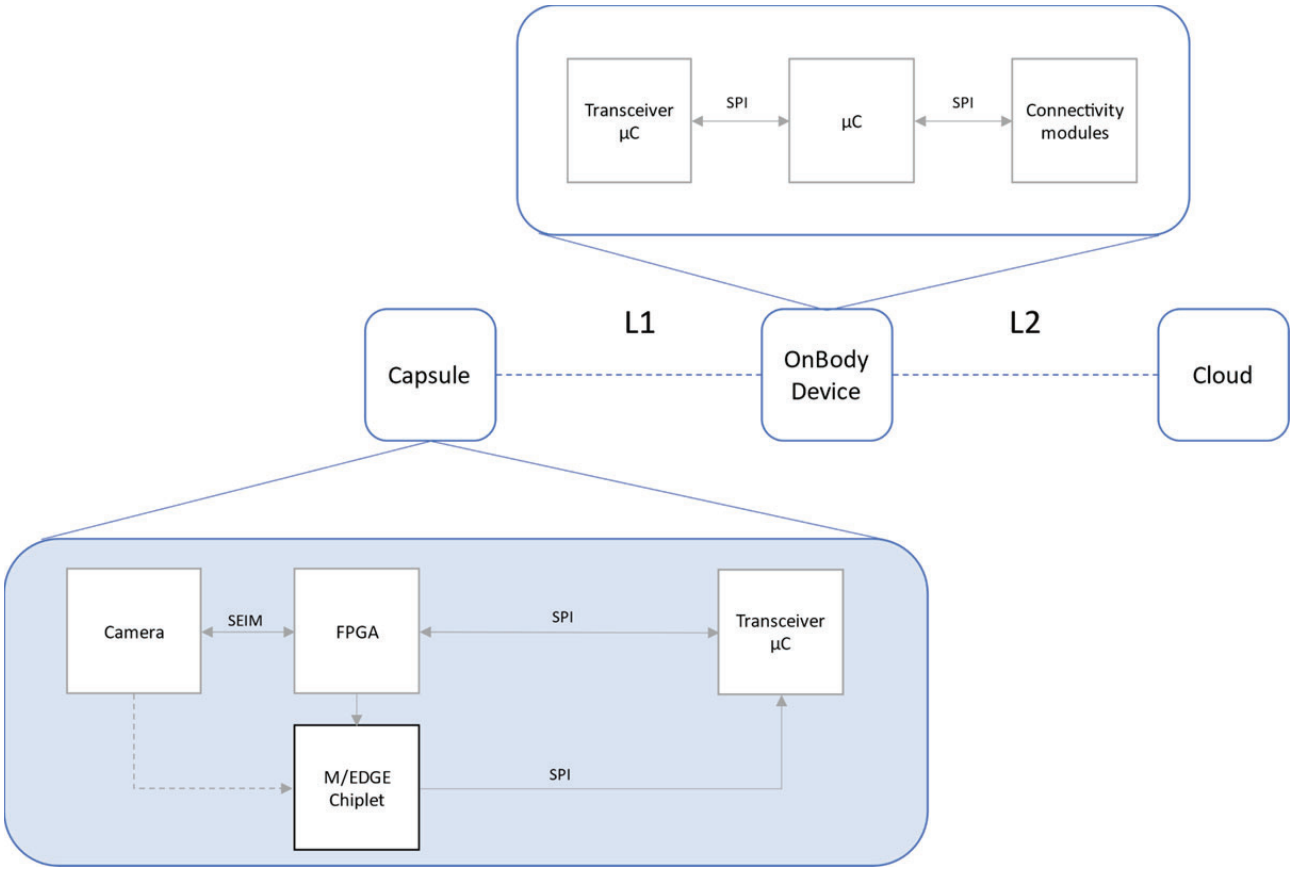

Figure 3: Kapselendoskopie Use Case

Die Kapselendoskopie stellt aufgrund ihrer extremen Größen- und Energiebeschränkungen einen der anspruchsvollsten Use Cases dar. Der Chip muss in eine Kapsel von weniger als 5 × 5 mm integrierbar sein und mit einem KI-Beschleuniger die Auswertung der aufgenommenen Kamerabilder direkt auf der Kapsel ermöglichen.

Attribut	**Wert**
Architektur	Mit KI-Beschleuniger
Taktfrequenz	24 MHz
Speicher (Bild)	mind. 102,5 kB (ein Bild)
Speicher (Sensordaten)	30 Byte
Größenbeschränkung	< 5 × 5 mm
Kommunikationsdatenrate	4 MHz
Latenz	< 0,5 s
Reichweite	1 m

Hinsichtlich Datenschutz und Sicherheit wurde festgestellt, dass die Bilddaten der Kapsel anonym sind und nicht mit dem Patienten verknüpft werden können. Ein Jamming-Angriff

gefährdet den Patienten nicht direkt, da der Arzt auch ohne Kapseldaten behandeln kann. Die Sicherheitsaspekte sind primär auf der Verbindung vom On-Body-Device zur Cloud relevant, nicht direkt am MEDGE-Chip. Für diesen Use Case ist ein ASIC insbesondere wegen extrem kleiner und effizienter Micro-KI-Beschleuniger interessant; Security-Aspekte an der Kapsel selbst sind hingegen nur von geringer Bedeutung.

Anforderungsanalyse Use Case 3 — Neurostimulationsimplantat (AP 1)

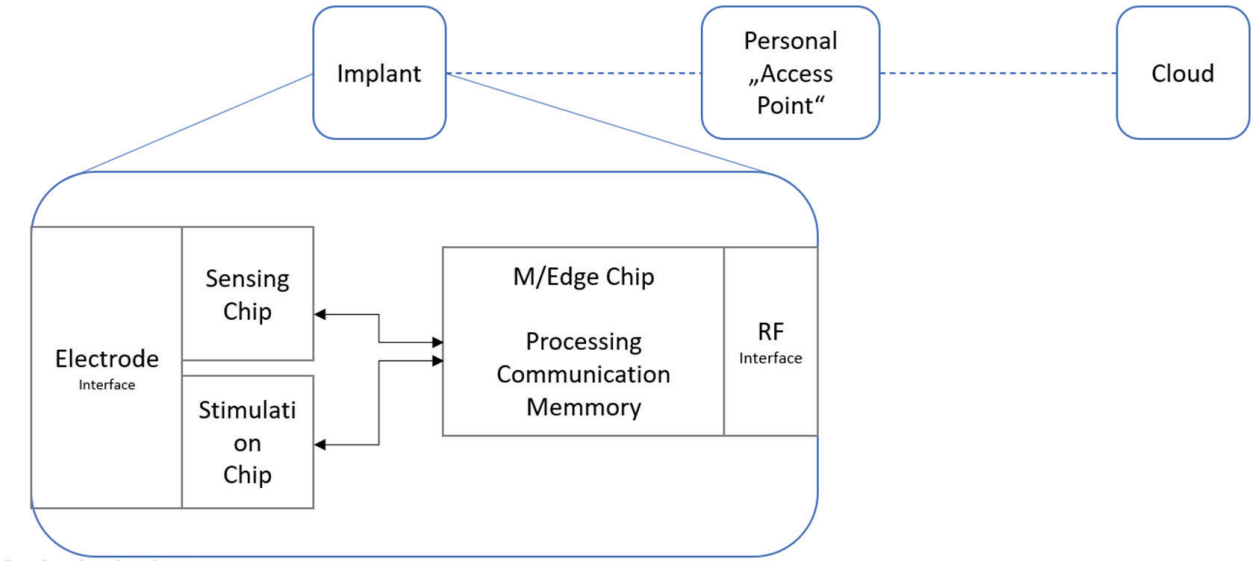

Figure 4: Neurostimulationsimplantat Use Case

Das Neurostimulationsimplantat teilt mit der Kapsel die starken physischen und energetischen Beschränkungen, unterscheidet sich jedoch in der Art der Sensorik und Verarbeitung. Bestehende Sicherheitskonzepte für implantierbare Geräte wurden als weitgehend unzureichend eingestuft und erfordern eine grundlegende Neubewertung im Kontext moderner Sicherheitsanforderungen. Ein ASIC ist hier aufgrund kleiner, effizienter KI-Beschleuniger ebenfalls interessant; zugleich ist Sicherheit besonders relevant, da das Implantat aktiv in den Körper eingreift und potenziell Schaden anrichten kann.

Schlussfolgerung

Implantat und Kapsel haben ähnliche Grundanforderungen: starke physische und energietechnische Beschränkungen, geringe benötigte Rechenleistung sowie unvollständige oder fehlende Sicherheitskonzepte. Der Ultraschall-Use-Case unterscheidet sich grundlegend: kaum physische oder Energiebeschränkungen, aber extrem hohe Rechenleistung erforderlich. Trotz der Ähnlichkeit von Use Case 2 und 3 ist die Definition einer gemeinsamen Chip-Architektur jedoch schwierig: Beide nutzen Micro-KI-Beschleuniger, die konkreten Anforderungen unterscheiden sich aber zu stark für eine einheitliche Architektur.

AP 5: Systemperformance-Analyse

Im Rahmen von AP 5 wurden die im Projekt entwickelten Hardware-Komponenten messtechnisch charakterisiert. Insgesamt wurden im Projektzeitraum drei Chip-Generationen in der GlobalFoundries 22 nm FDSOI-Technologie produziert und vermessen. Der letzte und für MEDGE zentrale Chip (Masur25) hatte folgenden Entwicklungszeitplan:

Meilenstein	Datum
RTL Freeze	01.10.2024
Code Freeze	30.10.2024
Tapeout	24.11.2024
Chip im Labor	September 2025

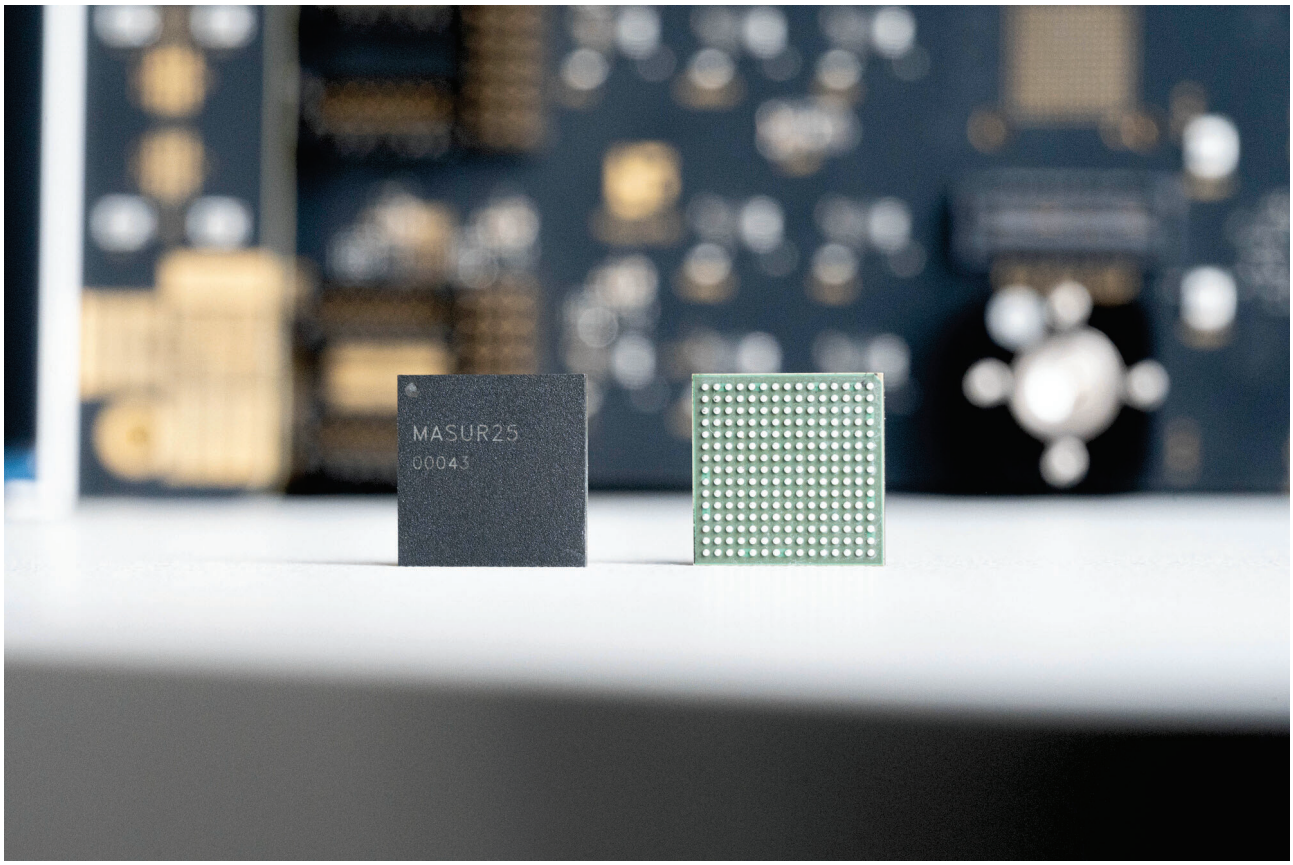

Figure 5: Masur25-Chip

Die iterative Weiterentwicklung über drei Chip-Generationen ermöglichte eine schrittweise Optimierung der Basiskomponenten und deren Energieverbrauch. Jede Generation lieferte Erkenntnisse, die direkt in das Design der nächsten einfließen konnten.

Chip-Inbetriebnahme

Die Inbetriebnahme des Chips umfasste den Aufbau und Test der Verbindungen zwischen Chip und Host-PC. Eine auf dem Host-PC laufende Software wurde entwickelt, die den Chip konfiguriert, initialisiert und Debug-Schnittstellen einrichtet. Die Leistungsaufnahme wird

mittels Messwiderständen (Shunt-Widerständen) erfasst; durch Ausführen typischer Anwendungsszenarien wird die Performanz der MPSoC-Basiskomponenten ermittelt.

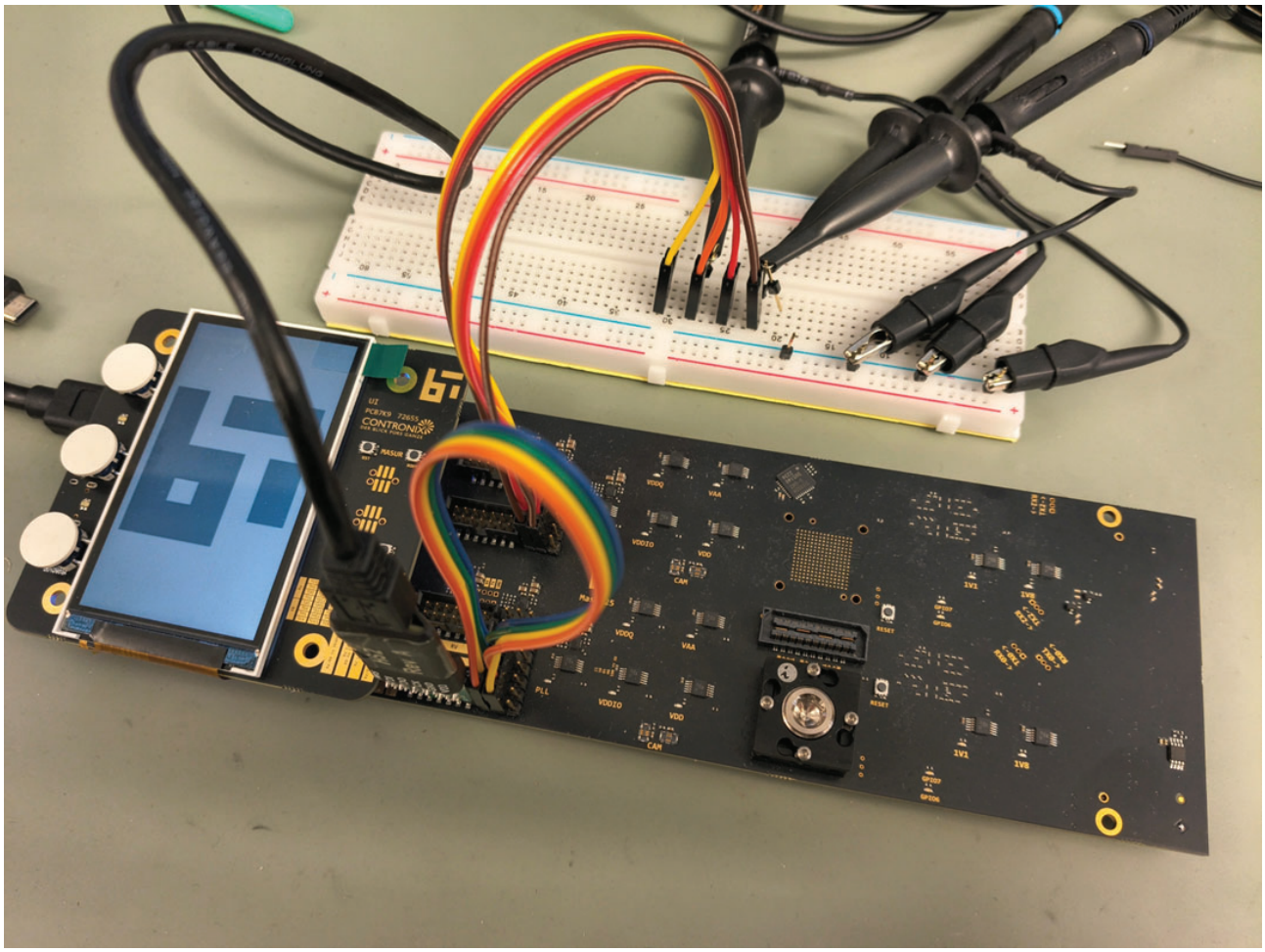

Figure 6: Chip-Inbetriebnahme: Laboraufbau

Um aus dem Gesamtchipverbrauch auf die Einzelverbräuche der Komponenten schließen zu können, kommen De-Embedding-Methoden zum Einsatz, die auf Hardwareemulationsartefakte aus AP 7 zurückgreifen. Dieses Vorgehen ermöglicht eine präzise Charakterisierung einzelner Funktionsblöcke auch im integrierten Systemkontext.

Trusted Communication Units (TCUs)

Die TCUs bilden das Sicherheitsfundament der Plattform und wurden in drei Größenvarianten realisiert, um unterschiedlichen Anforderungen hinsichtlich Fläche, Speicherbedarf und Sicherheitsfunktionalität gerecht zu werden:

Variante	Gesamtfläche	SRAM-Fläche
Full TCU	0,104 mm²	0,053 mm²
Mid TCU	0,036 mm²	0,008 mm²
Small TCU	0,008 mm²	—

Die Full TCU wird bei rechenintensiven Einheiten wie den RISC-V-Rechenkernen (Rocket Core) eingesetzt, wo viele separate Kommunikationskanäle verwaltet werden müssen. Die Mid TCU findet sich bei Beschleunigern wie dem Krypto- und dem Micro-KI-Beschleuniger, die eine beschränkte Anzahl von Kanälen haben. Die Small TCU kommt dort zum Einsatz, wo minimaler Overhead gefordert ist und Daten hauptsächlich durchgereicht werden, wie in IO-Komponenten (DRAM-Interface, GPIO-Komponenten) und der Chip-to-Chip-Kommunikation. Die Zuordnung der TCU-Größe zu den jeweiligen Kacheln ist Teil des Systemkonzepts und folgt dem Prinzip der minimalen notwendigen Vertrauenszone.

Basiskomponenten: Einzelmessungen

Die Einzelkomponenten wurden hinsichtlich Fläche und Leistung charakterisiert. Die Messergebnisse zeigen, dass die Basiskomponenten des Chips mit einem sehr geringen Flächen- und Leistungsbudget realisiert werden können. Insbesondere die Chip-to-Chip-Kommunikation (Aurora Link) erweist sich als äußerst kompakt, weist jedoch einen hohen Energieverbrauch auf. Dieser ist durch die großen Strukturen bedingt, die getrieben werden müssen, um aus dem Chip-Gehäuse heraus über das PCB in das Nachbargehäuse hinein zu kommunizieren. Für die geplante Erweiterung auf chiplet-basierte Systeme ist das eine wichtige Erkenntnis, da die Chiplet-to-Chiplet-Kommunikation deutlich energieeffizienter sein wird und damit die Leistungsaufnahme des Gesamtsystems maßgeblich reduzieren kann. Die beiden implementierten Krypto-Beschleuniger (AES und Keccak) zeigen, dass effiziente Kryptographie mit einem sehr kleinen Flächen- und Leistungsbudget umsetzbar ist. Die Messergebnisse für die Basiskomponenten im Überblick:

Komponente	Fläche	Leistung
Rocket Core (processing)	0,88 mm²	3,4 mW
Chip-to-Chip Interface (Aurora Link)	0,019 mm²	4,2 mW
AES (Krypto)	0,138 mm²	1,5 mW
Keccak (Krypto)	0,0028 mm²	2,5 mW

Krypto-Beschleuniger

Der auf dem Chip integrierte Krypto-Beschleuniger unterstützt die Algorithmen AES und Keccak. Die Messergebnisse zeigen, dass effiziente Kryptographie sowohl mit etablierten (AES) als auch mit modernen Verfahren (Keccak) realisierbar ist. Die Kosten der Kryptographie hängen von vielen Faktoren ab; grundsätzlich ist sie mit kleinem Flächen- und Leistungsbudget umsetzbar:

Kennwert	AES	Keccak
Fläche	0,107 mm²	0,0028 mm²
Leistung @ 100 MHz	2 mW	4,6 mW
Komplexität	22 Zyklen / 16 Byte (1,375 Zyklen/Byte)	638 Zyklen / 512 Byte (1,24 Zyklen/Byte)

Durchsatz	72 MB/s	80 MB/s
Energie	27,5 pJ/Byte	57,04 pJ/Byte
Area-Time-Energy (ATE)	$40{,}31 \cdot 10^{-21}$ mm²Js/Byte	$19{,}8 \cdot 10^{-21}$ mm²Js/Byte

Keccak erweist sich mit einem doppelt so günstigen ATE-Wert als die energieeffizientere Wahl und ist für die meisten Anwendungen zu bevorzugen. AES bietet demgegenüber eine deutlich höhere Flächeneffizienz. Die Wahl des Algorithmus hängt vom konkreten Use Case und den dominierenden Optimierungszielen (Fläche vs. Energie) ab. Auch die für den Use-Case erforderliche Sicherheitsstufe spielt eine Rolle, da AES eine viel geringere Sicherheitsgarantie bietet als Keccak.

Masur25-Chip

Die Gesamtmessung des Masur25-Chips ergibt folgendes Bild der Kachelgrößen und -leistungen:

Kachel	**Fläche**	**Leistung**
Gesamt	11,3 mm²	52,6 mW
RISC-V	1,383 mm²	5,5 mW
Chip-to-Chip Interface	0,176 mm²	7,9 mW
AES	0,421 mm²	2,0 mW
Keccak	0,343 mm²	4,6 mW
Kamera Interface	0,15 mm²	– nicht einsetzbar –

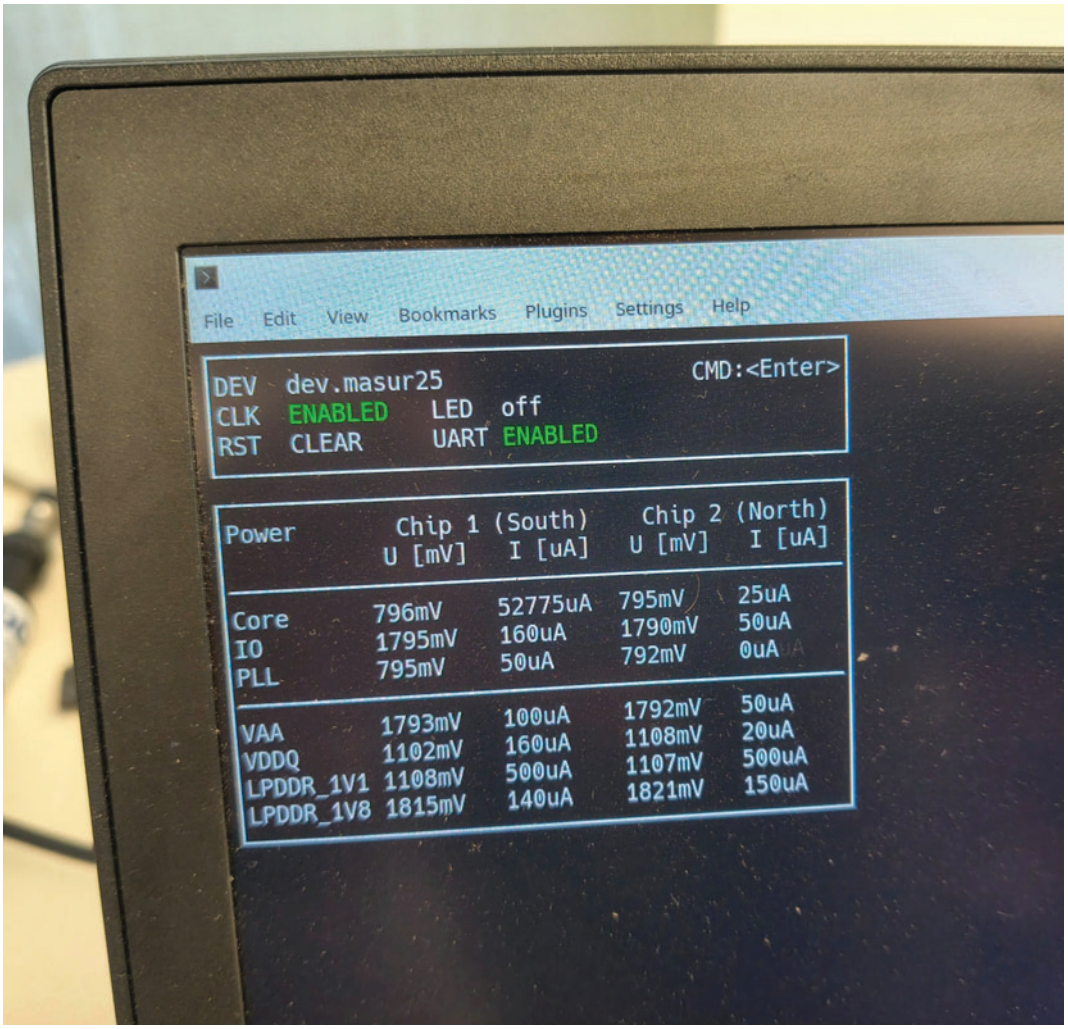

Figure 7: Chip-Inbetriebnahme: Leistungsmessung

Die in Betrieb genommenen Kacheln zeigen, dass die angestrebten Leistungsziele erreicht werden. Das Kamera-Interface weist einen RTL-Fehler auf und konnte daher nicht in Betrieb genommen werden. Solche Fehler lassen sich im Chipdesign nicht vollständig vermeiden und werden typischerweise durch iterative Verbesserungen über mehrere Generationen behoben. Dass die übrigen Komponenten funktionieren, ist auch auf die schrittweise Reifung über mehrere Chip-Generationen zurückzuführen; das Kamera-Interface wurde in dieser Chipserie erstmals integriert.

Publikationen

Die im Projekt erzielten Ergebnisse wurden in einer breiten wissenschaftlichen Publikationsaktivität disseminiert. Insgesamt umfasst die Publikationsliste (Table 1) 16 Beiträge, davon 10 bereits veröffentlichte und 6 angenommene Arbeiten. Inhaltlich decken die Veröffentlichungen ein breites Themenspektrum ab, darunter sichere und energieeffiziente Chip-Architekturen, kryptographische und systemnahe Hardwarekonzepte, KI-Methoden für medizinische Bild- und Sensordaten, sowie wissensbasierte Verfahren für Risiko- und Sicherheitsmanagement in der Medizintechnik.

Nr.	Abbr.	Partners	Title
1	MLMI[1]	UTU	Precise localization within the GI tract by combining classification of CNNs and time-series analysis of HMMs.
2	IJCNN[2]	UTU	Energy-Efficient Seizure Detection Suitable for low-power Applications
3	MobiHealth[3]	IfN	Evanescent Wave Filtering for Ultrasound RF-Data Compression
4	Medical Imaging[4]	IfN	Adoption and Evaluation of a Multistatic Fourier-based Synthetic Aperture Radar Method for Ultrasound Imaging
5	NorCAS[5]	BI	Trustworthy Silicon: An MPSoC for a Secure Operating System
6	EMBC[6]	UTU, TUD (EKFZ)	Enhanced Anomaly Detection for Capsule Endoscopy Using Ensemble Learning Strategies
7	KR[7]	ICCL	Pushing the Boundaries of Tractable Multiperspective Reasoning: A Deduction Calculus for Standpoint EL+
8	LPNMR[8]	ICCL	Consequence Operators of Characterization Logics – The Case of Abstract Argumentation
9	EMBC[9]	UTU	Systematic Hardware Integration Testing for Smart Video-based Medical Device Prototypes
10	ISOCC[10]	BI	Trust-minimized Integration of Third-Party Intellectual Property Cores
11	ISOCC[11]	BI	Integration of IP-Cores for the M Architecture with Low Area Overhead: Accelerator Support Module
12	AMAI[12]	UTU, TU Dresden (EKFZ)	Seeing More with Less: Video Capsule Endoscopy with Multi-Task Learning
13	ICONIP[13]	UTU	Smart Video Capsule Endoscopy: Raw Image-Based Localization for Enhanced GI Tract Investigation
14	FNINS[14]	CHA	Critical dynamics and interictal epileptiform discharges: a comparative analysis with respect to tracking seizure risk cycles
15	IJCAI[15]	ICCL	Approximation Fixpoint Theory as a Unifying Framework for Fuzzy Logic Programming Semantics
16	SEMANTICS[16]	ICCL, EKFZ	Supporting Risk Management for Medical Devices via the Riskman Ontology and Shapes

Table 1: Publikationsliste

[1]Machine Learning in Medical Imaging (at MICCAI)
[2]IEEE International Joint Conference on Neural Networks
[3]Wireless Mobile Communication and Healthcare (MobiHealth 2023)

AP 7: Sichere Low-Power Drahtlosvernetzung

In AP 7 wurde ein Systemkonzept für die sichere Kommunikation der MEDGE-Plattform erarbeitet. Ausgangspunkt war die Anforderung, die Sicherheitsbedürfnisse der drei Use Cases abzudecken und gleichzeitig einen energieeffizienten Betrieb zu ermöglichen. Die Anforderungsanalyse umfasste die Zusammenführung aller Projektpartnerbeiträge sowie weitere verbreitete medizinische Use Cases für Edge-Devices.

Architekturkonzept und Sicherheitsmodell

Das entwickelte Konzept basiert auf dem Prinzip der Isolation der Recheneinheiten:

- **Chip-interne Kommunikation** wird als sichere Kommunikation behandelt und durch die TCU-Architektur abgesichert.
- **Chip-externe Kommunikation** (z.B. zwischen Sensor und Access Point) wird kryptographisch verschlüsselt.

Die Chip-Recheneinheiten gliedern sich in drei Kategorien, um die benötigte hohe Energieeffizienz durch spezialisierte Einheiten zu gewährleisten:

[4] SPIE Medical Imaging, 2023
[5] IEEE Nordic Circuits and Systems Conference
[6] IEEE Engineering in Medicine and Biology Society
[7] Proceedings of the 20th International Conference on Principles of Knowledge Representation and Reasoning, KR 2023, Rhodes, Greece, September 2-8, 2023
[8] Logic Programming and Nonmonotonic Reasoning – 17th International Conference, 2024, Dallas, TX, USA, October 11–14, 2024
[9] IEEE Engineering in Medicine and Biology Society
[10] 20th International SoC Design Conference
[11] 21th International SoC Design Conference
[12] Applications of Medical AI
[13] 32nd International Conference on Neural Information Processing
[14] Frontiers in Neuroscience
[15] 34th International Joint Conference on Artificial Intelligence
[16] Proceedings of the 21st International Conference on Semantic Systems

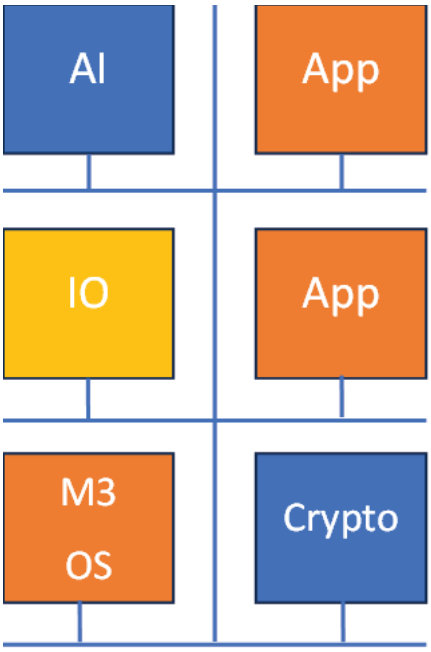

Figure 8: Architekturkonzept der MEDGE-Plattform

- **Universelle Recheneinheiten** (orange): RISC-V-basierte Prozessorkerne für generelle Berechnungen
- **Spezialisierte Beschleuniger** (blau): KI- und Krypto-Beschleuniger für rechenintensive, wiederkehrende Aufgaben
- **Ein-/Ausgabe-Blöcke** (gelb): Peripherieschnittstellen für Sensoren und Kommunikation

Jede Einheit enthält mindestens eine funktionale Komponente, einen lokalen Speicher und eine Trusted Communication Unit (TCU).

Universelle Recheneinheiten

Die universellen Recheneinheiten basieren auf quelloffenen RISC-V-Prozessoren. Jede Einheit enthält einen Cache als lokalen Speicher sowie eine TCU für die sichere Kommunikation:

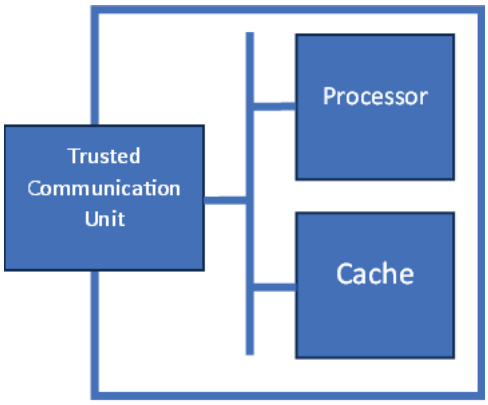

Figure 9: Universelle Recheneinheiten der MEDGE-Plattform

Im System sind drei verschiedene Prozessorvarianten geplant, die unterschiedliche Leistungs-/Effizienz-Trade-offs abdecken:

- **Rocket Core**: kleiner, einfacher Kern für ressourcenschonende Aufgaben
- **BOOM Core**: leistungsfähiger, großer Out-of-Order-Kern für rechenintensive Anwendungen
- **Ariane + Ara**: Vektorprozessor, geeignet für Signalverarbeitung und besonders nützlich für den Hybrid-Ultraschall-Use-Case

Beschleunigereinheiten

Beschleunigereinheiten erweitern die Kachelstruktur um ein zusätzliches Element, das Accelerator Support Module (ASM):

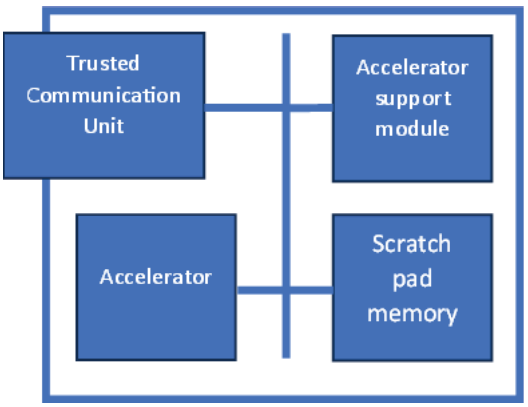

Figure 10: Beschleunigereinheiten der MEDGE-Plattform

Das ASM hat die Aufgabe, eine einfache Integration beliebiger Beschleuniger in die Plattform zu ermöglichen. Die Aufgabenteilung zwischen ASM und Beschleuniger ist klar definiert: Das ASM übernimmt die gesamte Kommunikation mit dem restlichen System (einschließlich Betriebssystem-Kompatibilität), während der Beschleuniger ausschließlich die Datenverarbeitung durchführt. Dieses Prinzip erlaubt es, neue Beschleuniger mit minimalem Integrationsaufwand einzubetten.

Chip-Toplevel und Kommunikationsarchitektur

Das vollständige Chip-Toplevel enthält neben den Rechen- und Beschleunigereinheiten zusätzliche Ein-/Ausgabe-Optionen für externe Konnektivität:

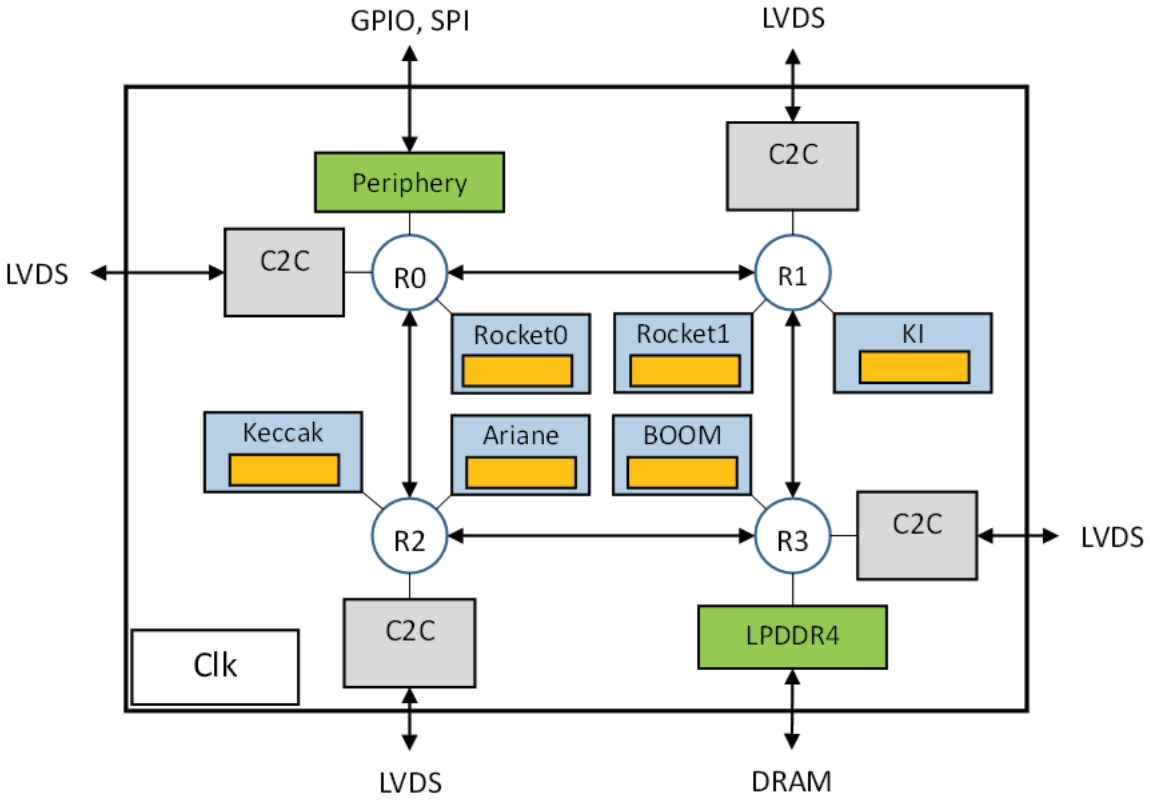

Figure 11: Chip-Toplevel und Kommunikationsarchitektur

Authentifizierungs- und Verschlüsselungsverfahren

Für die Kommunikation mit chip-externen Systemkomponenten wurden energieoptimierte kryptographische Algorithmen (AES, Keccak) analysiert, ausgewählt und als Hardware-Beschleuniger implementiert. Die Analyse umfasste einen Vergleich verfügbarer Verfahren hinsichtlich Eignungsgrad für die Use Cases, insbesondere Energieverbrauch und anfallenden Datenmehrverbrauch.

Mittels Hardwareemulation (FPGA-basierte Prototyping-Plattform) wurden Performanz und Energieverbrauch der Authentifizierungs- und Verschlüsselungsverfahren vorab abgeschätzt. Im Gegensatz zur software-basierten Verifikation erlaubt die Hardwareemulation die Evaluierung großer Designs in kurzer Zeit sowie das Profiling von dynamischer und statischer Leistungsaufnahme einschließlich der darauf simulierten Softwarekomponenten. Die Trade-offs zwischen Sicherheitsniveau und Energiebedarf wurden so für beide Algorithmen quantifiziert.

Der KI-Beschleuniger der Universität Tübingen wurde parallel auf die Systemeigenschaften des BI-Chips angepasst und für die Integration in das Design vorbereitet. Gleichzeitig wurden die Erfahrungen aus den vorangegangenen BI-Chip-Tapeouts genutzt, um den MEDGE-Tapeout-Prozess so reibungslos wie möglich zu gestalten.

AP 8: Hardware-Plattform für Edge-Computing im Patienten

AP 8 bildete den zentralen Entwicklungsschwerpunkt des Projekts. Auf Basis des 2023 erstellten Systemkonzepts wurde 2024 ein vollständiger Mikrochip entwickelt und zur Fabrikation bei GlobalFoundries in Dresden (22 nm FDSOI) eingereicht. Die Entwicklung profitierte dabei von zwei vorangegangenen BI-Chip-Generationen: Der erste Digitalchip des BI wurde 2023 in Betrieb genommen und stellte einen wichtigen Meilenstein auf dem Weg zum MEDGE-Chip dar. Der zweite digitale BI-Chip kam 2024 im Labor an, ähnelt dem MEDGE-Chip deutlich und testete weitere geplante Funktionalitäten vorab.

Integrierte Komponenten

Das digitale Design des MEDGE-Chips umfasst folgende Komponenten:

- **2× Rocket Core** — allgemeiner Applikationsprozessor (256 kB Cache, DDR-Speicheranbindung), generiert mit dem Chipyard-Framework; führt Betriebssystemkern und Applikationslogik aus
- **BOOM Core** — leistungsfähiger Out-of-Order-Applikationsprozessor für rechenintensive Aufgaben, ebenfalls via Chipyard generiert
- **Pico Core** — sehr kleiner Prozessor mit SRAM statt Cache für Tests ohne externe Speicheranbindung
- **KI-Beschleuniger** — Zuarbeit der Universität Tübingen, via ASM (Accelerator Support Module) in das System integriert; für den Kapsel-Use-Case ausgelegt, um Bildauswertung direkt auf dem Gerät zu ermöglichen
- **Krypto-Beschleuniger** — BI-Eigenentwicklung, wiederverwendet aus vorherigen BI-Chips und für das MEDGE-Design optimiert (angepasste SRAM-Größe für optimale Leistung, ASM-Integration für Betriebssystem-Kompatibilität)
- **Peripherie-Controller** mit Kamerainterface und SPI (Zuarbeit Universität Tübingen); ein zusätzlicher Pico Core steuert die Peripheriemodule
- **LPDDR4-Speicherinterface** — Synopsys-Modul, analog zur bewährten Integration aus dem vorherigen BI-Chip wiederverwendet

Das Accelerator Support Module (ASM) übernimmt die Kommunikation zwischen Beschleuniger und dem restlichen System, während der Beschleuniger selbst ausschließlich die Datenverarbeitung durchführt. Zur Reduktion der benötigten Chip-Pins wurden Peripheriemodule über Selektionsschalter zur Mehrfachnutzung an die Ein-/Ausgabe-Pins angebunden.

Verifikation

Alle Komponenten wurden zunächst einzeln funktional verifiziert, um deren grundlegende Funktionalität sicherzustellen. Nach der Integration zum Gesamtsystem bestätigten einfache Applikationstests die korrekte Zusammenarbeit der Komponenten. Nach der Synthese zur Netzliste wurden ausgewählte Tests wiederholt, um sicherzustellen, dass auch nach diesem Verarbeitungsschritt die Funktionalität gewährleistet ist. Mit zunehmendem Entwicklungsfortschritt und steigendem Rechenaufwand wurden aus praktischen Gründen weniger Tests durchgeführt.

Neben der funktionalen Verifikation wurde eine Coverage-Analyse des Chipdesigns durchgeführt, die die Abdeckung der Testcases bestimmt (Code-Blöcke, Signalwechsel, Zustandsübergänge). Ein Regressionstest wurde erzeugt, der durch regelmäßige Wiederholung aller Testcases fehlerhafte Modifikationen im Chipdesign erkennt.

Physical Design und Tapeout

Zur Vorbereitung der Fabrikation wurden folgende Verarbeitungsschritte iterativ in mehreren Runden durchgeführt, um das Ergebnis hinsichtlich Chipfläche und erreichbarer Basisfrequenz zu optimieren:

1. **Platzierung von Hard-Makros** — große Module fester Abmessung wie Teile des Speicherinterfaces und SRAMs (On-Chip-Speicherzellen)
2. **Synthese** — Übersetzung der Logikbeschreibung (RTL) in eine Netzliste (Netzwerk von Standardzellen) in der 22 nm-Technologie von GlobalFoundries
3. **Place & Route** — Verteilen und Verdrahten der Standardzellen der Netzliste auf der Chipfläche

Das resultierende Layout wurde in mehreren Prüfschritten auf technologische Herstellbarkeit verifiziert (DRC, ERC, LVS). Nach abschließender Überprüfung durch mehrere Personen und verschiedene Werkzeuge wurde das fertige Chipdesign fristgerecht an GlobalFoundries in Dresden übergeben (Tapeout: 24.11.2024):

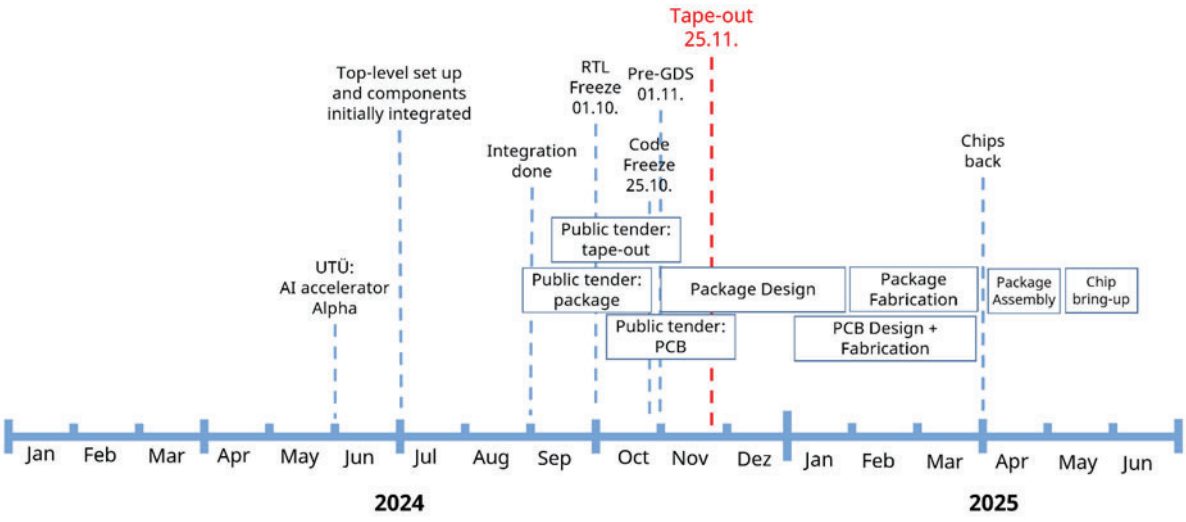

Figure 12: Chip-Tapeout der MEDGE-Plattform

AP 9: Chiplet-Integration, Systemintegration & Packaging

In AP 9 wurden Konzepte für die Miniaturisierung und Integration der MEDGE-Plattform in Chiplet-basierten sowie monolithischen Systemen untersucht. Ziel war die Erarbeitung von Handlungsempfehlungen für eine kommerzielle Umsetzung der Technologie in den drei medizinischen Anwendungsfeldern.

Übertragbarkeit der Sicherheitsarchitektur auf Chiplet-Systeme

Das Kachelungs- und Isolationsprinzip der TCU-Architektur ist gleichermaßen für monolithische Chips wie für Chiplet-Systeme anwendbar. Das Network-on-Chip (NoC) kann über Chiplet-Grenzen hinweg erweitert werden, um die Kommunikation zwischen den Chiplets zu ermöglichen, ohne dass dies Auswirkungen auf die Sicherheitsarchitektur hat. Ob ein Kommunikationspartner sich auf demselben Chiplet befindet oder nicht, ist für die Sicherheitslogik irrelevant — alle Komponenten werden unabhängig von ihrer physischen Lage durch TCUs isoliert.

Funktionale Einheiten wie KI- und Krypto-Beschleuniger lassen sich in beiden Integrationsformen unterbringen und profitieren in gleicher Weise von der TCU-basierten Isolation.

Wirtschaftliche Bewertung

Aus wirtschaftlicher Perspektive (untersucht insbesondere durch IFX) sind maßgeschneiderte ASICs für medizintechnische Anwendungen aufgrund der geringen Stückzahlen nicht wirtschaftlich rentabel. Chiplet-basierte Ansätze verbessern die Wirtschaftlichkeit grundsätzlich, da standardisierte Chiplets häufiger eingesetzt werden können; in den in MEDGE betrachteten Anwendungsfällen reicht dies jedoch ebenfalls nicht aus, da die Stückzahlen insgesamt zu gering bleiben.

Zusätzlich erschwerend wirkt die kompakte und abgeschlossene Natur der betrachteten Implantate und Kapseln: Die Systeme sind so klein und abgeschlossen, dass sich eine vollständig gekachelte Sicherheitsarchitektur bei den gegebenen Stückzahlen und Systemgrößen wirtschaftlich nicht lohnt.

Schlussfolgerung

Die im Projekt entwickelten Konzepte und Technologien sind technisch sowohl für monolithische als auch Chiplet-basierte Systeme geeignet. Für eine kommerzielle Umsetzung in den betrachteten medizinischen Anwendungen (Implantat, Kapsel, Ultraschall) sind jedoch weitere Schritte zur Kostenreduktion oder eine Ausweitung auf Anwendungsfelder mit höheren Stückzahlen erforderlich.

Mit anderen Use Cases und größeren Stückzahlen könnte eine medizinische Chip-Plattform wirtschaftlich sinnvoll werden. Zudem kann die Weiterentwicklung in Richtung Chiplet-Design das Stückzahlproblem teilweise umgehen, da sich aus einem kleinen Set von Chiplets eine Vielzahl unterschiedlicher Systeme für verschiedene Anwendungsfelder zusammensetzen lässt. Die im Projekt gewonnenen Erkenntnisse liefern dafür eine solide technologische Grundlage.

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Forschung,Technologie und Raumfahrt unter dem Förderkennzeichen 16ME0527 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der Autorin/beim Autor.

Gefördert durch:

Bundesministerium für Forschung, Technologie und Raumfahrt