



## Schlussbericht TVB Teil 1

BMBF-Verbundprojekt VE-VIDES:

Designmethoden und HW/SW-Co-Verifikation für die eindeutige Identifizierbarkeit von Elektronikkomponenten

<b>Zuwendungsempfänger:</b>	<b>Robert Bosch GmbH (RB)</b>
<b>Vorhabenbezeichnung:</b>	VE-VIDES
<b>Förderkennzeichen:</b>	16ME0249
<b>Projektlaufzeit:</b>	01.03.2021 bis 31.08.2024 (mit 6 Monaten Verlängerung)
<b>Fälligkeit:</b>	31.08.2024
<b>Erstelldatum:</b>	30.01.2025
<b>Autoren:</b>	Felix Lang, RB Michael Amann, RB Gregor Bracher, RB Rudolf Ritter, RB
<b>Ansprechpartner:</b>	Dr. Ing. Felix Lang Fon: +49 7121 35-18133 E-Mail: felix.lang@de.bosch.com

## I.1 Kurzbericht

### I.1.1 Motivation, Zielsetzung und Ausgangslage

Das gemeinsame Entwicklungsziel von VE-VIDES ist die systematische Identifikation von potenziellen Sicherheitslücken bereits in der Designphase. Weiterhin sollen Elektroniksysteme mithilfe automatisiert erzeugter, zuverlässiger Mechanismen vor Angriffen geschützt werden. Dazu konzentriert sich VE-VIDES auf die Vertrauenswürdigkeit der System-Hardware (HW) und berücksichtigt die unmittelbare Schnittstelle zu vertrauenswürdigen Software-/Firmware-Komponenten. Als wesentliche Angriffsszenarien führt die Gesamtvorhabenbeschreibung (GVB) die folgenden beiden Punkte auf:

1. Angriffe über das Internet („Hacking“), bei denen vorsätzlich eingebrachte Backdoors und Trojaner oder versehentlich verbliebene Schwachstellen genutzt werden, um die Funktionalität des Systems zu verändern bzw. darin gespeicherte Daten zu stehlen.
2. Elektronische, optische und physikalische Angriffe auf integrierte Schaltungen, um geistiges Eigentum (IP) zu stehlen oder Daten illegal auszulesen bzw. zu modifizieren.

Robert Bosch (RB) – bzw. dessen Entwicklungsbereich **Mobility Electronics** - Engineering Integrated Circuits (ME-IC) - bewegt sich bezüglich der Arbeitsumgebung bei Elektroniksystemen im Umfeld anwendungsspezifischer integrierter Schaltungen (ASIC) für Automotive Applikationen. Diese ASICs werden für die nächsten Generationen von PKW-Steuergeräten entwickelt und müssen diverse Anforderungen bezüglich Safety, Security und Zuverlässigkeit erfüllen. Ein wesentlicher Aspekt, der bei ASICs in Betracht gezogen werden muss, ist - im Gegensatz zu den zuvor genannten - der Stückpreis, welcher sich aus Testzeit-, Verpackungs- und natürlich den reinen Herstellungskosten der Halbleiter-Wafer ergibt.

Die Arbeiten von RB in VE-VIDES konzentrieren sich auf die in Abbildung 1 dargestellten Thematiken.

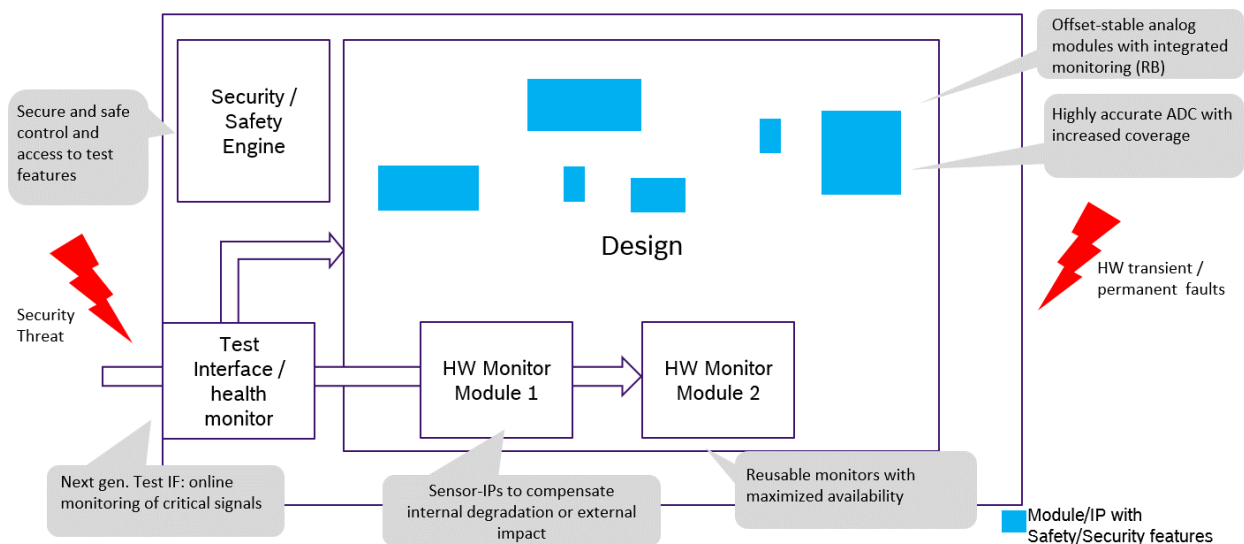


Abbildung 1: Gesamtdarstellung der RB-Arbeitspakete.

Basierend auf Anforderungsanalysen und Konzeptüberlegungen wird eine möglichst schlanke und universelle Plattformarchitektur abgeleitet, die die folgenden Themen abdeckt:

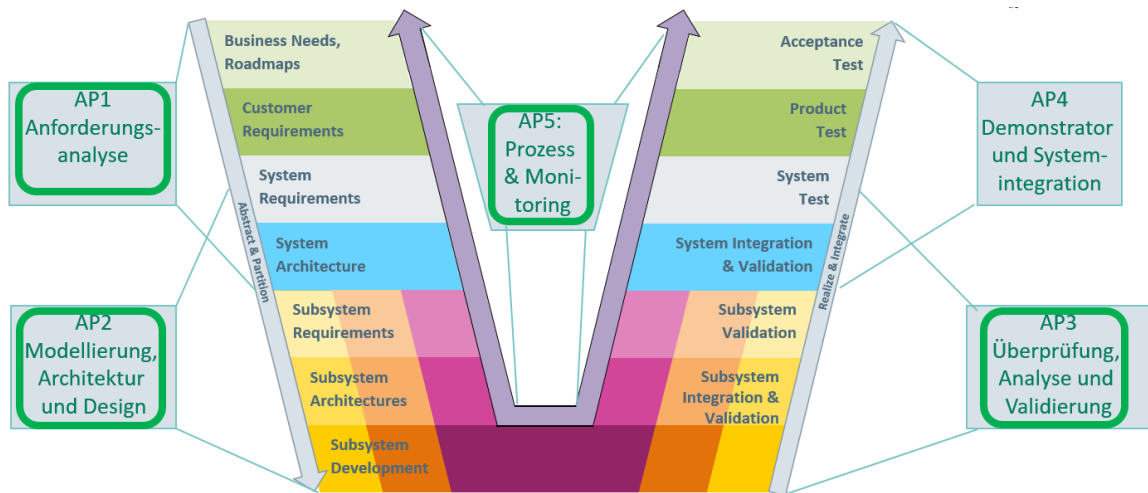
- Security → sicherer (Nicht-)Zugriff und Ablauf
- Safety → Ausfallsicherheit, durch Redundanz oder robuste Strukturen
- Test und Build-In-Self-Test (BIST) → sehr hohe Abdeckung, niedrige Testzeit
- Monitoring → on-Chip Health/Aging Monitoring

Auf Basis von ersten Strukturen (Test-Interface (IF) und Monitoren - siehe Vorarbeiten und Patente) wird in VE-VIDES ein kompletter Basissatz von Einzelkomponenten für eine Plattform zusammengestellt. Die Schaltungen wurden wo nötig funktional ergänzt, aufeinander abgestimmt oder durch völlig neuartige Strukturen erweitert. Die Gesamtstruktur wird zur Verifikation auf einem Testchip evaluiert.

Die Erkenntnisse und Ergebnisse aus dem Testchip werden in RB interne Schaltungs- und Modulplattformen überführt.

### I.1.2 Ablauf des Vorhabens, wesentliche Ergebnisse und Kooperationen

RB hat sich im Rahmen von VE-VIDES in allen Arbeitspaketen außer AP4 eingebracht, da auf ASIC-Ebene kein AP4-Demonstrator im Sinne von VE-VIDES erstellt werden kann. Die in den folgenden beschriebenen Ergebnisse und Beiträge orientieren sich am V-Diagramm in Abbildung 2. Die Teilbeiträge wurden weitgehend sequenziell wie in Abbildung 3 von oben nach unten bearbeitet, entsprechend wurden die Ergebnisse nacheinander erzielt und in den Deliverables des Projekts und in regelmäßigen Projekttreffen mit den VE-VIDES-Partnern geteilt.



**Abbildung 2** V-Modell für Produkt- und Systementwurf.

RB beteiligt sich in grün markierten Arbeitspaketen (AP1, AP2, AP3, AP5)

Vor allem in der Konzeptphase führte ein Abgleich mit den Partner aus AP1 und AP5 zu einem besseren Verständnis bezüglich Vertrauenswürdigkeit und die technischen Ziele in VE-VIDES wurden geschärft. Dies wurde im Rahmen der Projekttreffen und in direkten Abstimmungsrunden - beispielsweise der AP5-Partner - erreicht. Mit der Uni Ulm wurden des Weiteren das Thema Physical Unclonable Functions (PUF) als Unterthema der OnChip-Monitore für Security evaluiert.

AP/ A / B	Arbeitspaket-/Aufgaben-Titel
<b>AP1</b>	<b>Anforderungen an Vertrauenswürdigkeit von IP und Designflow</b>
A1.1	Sammlung der Anforderungen an die Vertrauenswürdigkeit
B1.1.6	Test-Anforderungen
B1.1.7	Anforderungen an Monitoring-Schaltungen
A1.2	Herunterbrechen der Anforderungen und Randbedingungen
B1.2.5	Analyse der Test-Anforderungen
B1.2.6	Umsetzungskonzept für Test-Anforderungen
B1.2.7	Untersetzung von Detektor-Anforderungen
<b>AP2</b>	<b>Design, Architektur und Modellierung</b>
A2.2	Integration und Entwurf vertrauenswürdiger IP
B2.2.9	Analyse des Integrationsaspekts für Vertrauenswürdiger IPs
B2.2.10	Definition und Implementierung von optimierten Schaltungen für Black-Box-IP
B2.2.11	Generierung einer Plattformarchitektur bzgl. Test und Monitoring
B2.2.12	Standardisierte Umsetzung von Cross-Domain-Interfaces
B2.2.13	Generierung von Ansteuer- und Auswerteschaltungen für on-chip Monitore (Test+BIST)
B2.2.14	Vorbereitung zur Integration ausgewählter Monitorkonzepte (Design, Simulation, Layout)
A2.3	Design u. Modellierung von Runtime-Monitoren zur Überprüfung d. V.
B2.3.7	Entwurf eines hochgenauen Delta-Sigma ADC mit integrierten Monitoren
B2.3.8	Definition und Entwurf von Monitoren zur Prüfung der Integrität der Signaleingänge.
B2.3.9	Definition und Design eines Monitors für die Funktion des Delta-Sigma ADCs
<b>AP3</b>	<b>Verifikation der Vertrauenswürdigkeit</b>
A3.4	Analyse und Validierung der Monitore und Fingerprints
B3.4.3	Definition und Entwurf einer Testumgebung für das Design aus A2.3 inklusive Laborevaluierung
B3.4.4	Einbindung neuer Monitorstrukturen und Erweiterung der Designkonzepte auf vorentwickelte IP-Blöcke
B3.4.5	Anwendung der Monitore in einem Zielprojekt oder für einen separaten Testchip
B3.4.6	Tests auf IP-Ebene
B3.4.7	Validierung der Designs aus A2.2. durch geeignete Labortests
B3.4.8	Auswertung der Teststrukturen verschiedener Monitorkonzepte
<b>AP5</b>	<b>Prozess und Monitoring über die Lieferkette</b>
A5.1	Gap-Analyse zum aktuellen Halbleiter-Entwicklungsprozess
B5.1.9	Gap Analyse entlang der Entwicklungen von AP1 bis AP3 aus Sicht eines Automotive Halbleiterherstellers
A5.2	Definition eines vertrauenswürdigen Entwicklungsprozesses
B5.2.4	Erstellen einer Handlungsempfehlung zur Integration vorentwickelter OnChip Test Module in Automotive ASIC

**Abbildung 3:** Inhalt der RB-Arbeitspakete



## Schlussbericht TVB Teil 2

BMBF-Verbundprojekt VE-VIDES:

Designmethoden und HW/SW-Co-Verifikation für die eindeutige Identifizierbarkeit von Elektronikkomponenten

<b>Zuwendungsempfänger:</b>	<b>Robert Bosch GmbH (RB)</b>
<b>Vorhabenbezeichnung:</b>	VE-VIDES
<b>Förderkennzeichen:</b>	16ME0249
<b>Projektlaufzeit:</b>	01.03.2021 bis 31.08.2024 (mit 6 Monaten Verlängerung)
<b>Fälligkeit:</b>	31.08.2024
<b>Erstelldatum:</b>	30.01.2025
<b>Autoren:</b>	Felix Lang, RB Michael Amann, RB Gregor Bracher, RB Rudolf Ritter, RB
<b>Ansprechpartner:</b>	Dr. Ing. Felix Lang Fon: +49 7121 35-18133 E-Mail: felix.lang@de.bosch.com

## I.1 Technische Ergebnisse

In den folgenden Kapiteln dieses Abschlussberichts werden die Beiträge mit den relevanten Ergebnissen zu den jeweiligen Arbeitspaketen bzw. Aufgaben mit Beteiligung von RB (siehe Abbildung 1) hierarchisch aufgeführt. Diese Reihenfolge passt gut zu der zeitlichen Sequenz, die sich in VE-VIDES am V-Modell orientiert und RB in allen AP außer AP4 beteiligt war.

AP/ A / B	Arbeitspaket-/Aufgaben-Titel
<b>AP1</b>	<b>Anforderungen an Vertrauenswürdigkeit von IP und Designflow</b>
A1.1	Sammlung der Anforderungen an die Vertrauenswürdigkeit
B1.1.6	Test-Anforderungen
B1.1.7	Anforderungen an Monitoring-Schaltungen
A1.2	Herunterbrechen der Anforderungen und Randbedingungen
B1.2.5	Analyse der Test-Anforderungen
B1.2.6	Umsetzungskonzept für Test-Anforderungen
B1.2.7	Untersetzung von Detektor-Anforderungen
<b>AP2</b>	<b>Design, Architektur und Modellierung</b>
A2.2	Integration und Entwurf vertrauenswürdiger IP
B2.2.9	Analyse des Integrationsaspekts für Vertrauenswürdiger IPs
B2.2.10	Definition und Implementierung von optimierten Schaltungen für Black-Box-IP
B2.2.11	Generierung einer Plattformarchitektur bzgl. Test und Monitoring
B2.2.12	Standardisierte Umsetzung von Cross-Domain-Interfaces
B2.2.13	Generierung von Ansteuer- und Auswerteschaltungen für on-chip Monitore (Test+BIST)
B2.2.14	Vorbereitung zur Integration ausgewählter Monitorkonzepte (Design, Simulation, Layout)
A2.3	Design u. Modellierung von Runtime-Monitoren zur Überprüfung d. V.
B2.3.7	Entwurf eines hochgenauen Delta-Sigma ADC mit integrierten Monitoren
B2.3.8	Definition und Entwurf von Monitoren zur Prüfung der Integrität der Signaleingänge.
B2.3.9	Definition und Design eines Monitors für die Funktion des Delta-Sigma ADCs
<b>AP3</b>	<b>Verifikation der Vertrauenswürdigkeit</b>
A3.4	Analyse und Validierung der Monitore und Fingerprints
B3.4.3	Definition und Entwurf einer Testumgebung für das Design aus A2.3 inklusive Laborevaluierung
B3.4.4	Einbindung neuer Monitorstrukturen und Erweiterung der Designkonzepte auf vorentwickelte IP-Blöcke
B3.4.5	Anwendung der Monitore in einem Zielprojekt oder für einen separaten Testchip
B3.4.6	Tests auf IP-Ebene
B3.4.7	Validierung der Designs aus A2.2. durch geeignete Labortests
B3.4.8	Auswertung der Teststrukturen verschiedener Monitorkonzepte
<b>AP5</b>	<b>Prozess und Monitoring über die Lieferkette</b>
A5.1	Gap-Analyse zum aktuellen Halbleiter-Entwicklungsprozess
B5.1.9	Gap Analyse entlang der Entwicklungen von AP1 bis AP3 aus Sicht eines Automotive Halbleiterherstellers
A5.2	Definition eines vertrauenswürdigen Entwicklungsprozesses
B5.2.4	Erstellen einer Handlungsempfehlung zur Integration vorentwickelter OnChip Test Module in Automotive ASIC

Abbildung 1: Übersicht der VE-VIDES Arbeitspakete mit Beteiligung und Beiträgen von RB.

## I.1.1 AP1 Anforderungen an Vertrauenswürdigkeit von IP und Designflow

### I.1.1.1 A1.1: Sammlung der Anforderungen an die Vertrauenswürdigkeit

In folgendem Abschnitt sind die Beiträge und Arbeitsschritte von RB in Arbeitspaket AP1, Aufgabe A1.1. aufgelistet. Die Nomenklatur der Beitragsnummerierung ist an der Zugehörigkeit eines Beitrages zu einer Aufgabe und einem Arbeitspaket orientiert. Zum Beispiel ist der Beitrag B1.2.4 der vierte Beitrag in der zweiten Aufgabe des Arbeitspakets 1.

#### Beitrag B1.1.6 Test-Anforderungen

##### Partnerbeitragsbeschreibung

Safety- und Security-Anforderungen von verschiedenen aktuell in Entwicklung und Vorbereitung befindlichen Projekten müssen analysiert, sortiert und zusammengefasst werden. Anschließend erfolgt eine Bewertung der Anforderungen hinsichtlich Abdeckung durch ein weiterentwickeltes Test-Interface Test-IF2.0.

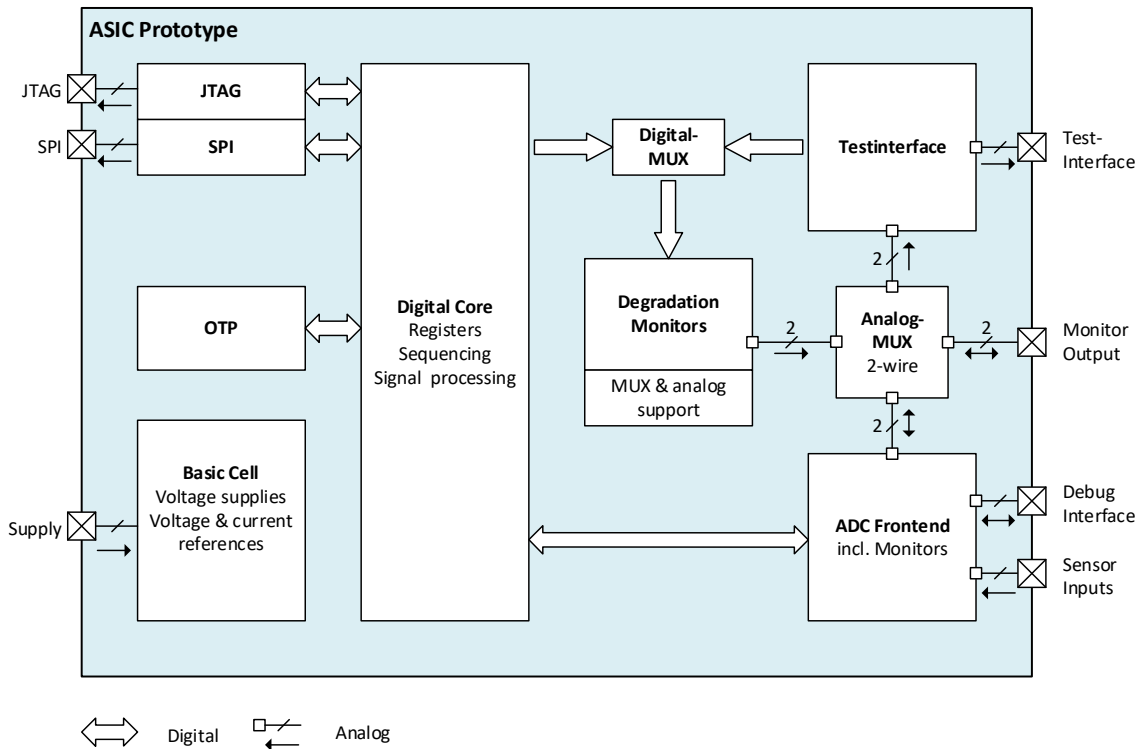
##### Aktuelle Arbeiten im Berichtszeitraum

Unter Einbindung verschiedener Experten von Bosch wurde eine einfache Übersicht erstellt und es wurden iterativ, basierend auf den Vorüberlegungen, die Anforderungen an ein Test-IF der nächsten Generation zur Ansteuerung der weiteren Arbeiten auf dem Testchip von RB aus VE-VIDES präzisiert.

Hierbei stehen vor allem Safety-, Test-, Reliability- und Verfügbarkeitsanforderungen im Vordergrund, da die mit den anderen Partnern erarbeiteten sonstigen Gesichtspunkte der Vertrauenswürdigkeit - wie beispielsweise Security – bei Bosch Semiconductor aktuell weniger Relevanz für reine Mixed-Signal-ASICs haben oder auf höheren Applikationsebenen abgedeckt werden. In Abbildung 2 ist ein erstes Blockdiagramm des anvisierten ASIC-Prototyps zu sehen der die verschiedenen Anforderungen und Möglichkeiten, die innerhalb von VE-VIDES erarbeitet wurden, anschaulich darstellt.

Diese sind unter anderem:

- 1) Sicherer Serientestzugriff über das Test-Interface mit hoher Testabdeckung und Testtiefe bei gleichzeitiger Optimierung der Testzeiten.
- 2) Sehr genaues und fehlerfreies Analysieren von internen Signalen mit einem ADC.
- 3) Alterungseffekte und andere Effekte, die in kleinen Technologieknoten verstärkt auftreten, sicher erkennen und entsprechende Maßnahmen einleiten.
- 4) Built-in-Self-Test-Features (BIST) die sich flexibel in verschiedenen ASICs anwenden lassen.
- 5) Analyse- oder Echtzeitzugriff auf ASIC-interne Monitor-Signale über Standardchnittstellen bei gleichzeitiger Nichtbeeinflussung der Funktionalität.



**Abbildung 2:** Erstes Blockdiagramm zur Ermittlung von potenziellen Use-Cases.

## Beitrag B1.1.7 Anforderungen an Monitoring-Schaltungen

### Partnerbeitragsbeschreibung

Aus einer Vielzahl möglicher Monitorstrukturen müssen, durch geeignete Wahl von Kriterien, die am besten geeigneten Konzepte ausgewählt werden. Geeignete Kriterien und Anforderungen müssen aus Applikationssicht formuliert werden.

### Aktuelle Arbeiten im Berichtszeitraum

Das Grundproblem von Defekten in Siliziumchips ist in Abbildung 3 dargestellt: In der Regel führen die Safety-Analysen auf Basis von fixen Mission-Profiles (MP; zum Beispiel 1000h in einer bestimmten Sequenz von Eingangsgrößen) bei schlechten Fehlerraten zur Implementierung einer redundanten Struktur zur Absicherung. Dies ist oft gar nicht nötig, da hier von einem im Verhältnis zur Realität eher schlechten Umfeld oder Fahrverhalten ausgegangen wird.

Durch Stresssensoren können diverse Effekte wie Alterung (z.B. NBTI, PBTI, HCI bei MOSFETs), Packaging-Stress etc. zur Laufzeit mit gemonitored werden. Dadurch kann bei Überschreitung einer bestimmten absoluten Grenze oder relativ bezüglich eines ungealterten Referenz-Devices eine Warnung ausgegeben werden.

Dies ermöglicht u.a. folgende Optionen:

- 1) Anpassung des Mission-Profiles und somit ggf. längere Nutzungszeiten nach Datenblatt durch echte Daten aus dem Feld.
- 2) Reduktion von redundanten Strukturen durch Ersetzen des kompletten ASIC bei Überschreitung einer bestimmten Grenze – also nur für besonders beanspruchte Devices.

Die Anforderungen für die Detektion kritischer Kombinationen von Belastung und Belastbarkeit in Abbildung 4 wurden erarbeitet. Ziel für Bosch ist es in VE-VIDES, eine möglichst große

Anzahl von potenziellen Fehlermechanismen abdecken zu können. Die dabei benutzten Alterungs- und Stresssensoren können in abgewandelter Form ebenfalls zur „Eindeutigen Identifikation“ des Systems als „Physical Unclonable Functions“ (PUF) genutzt werden.

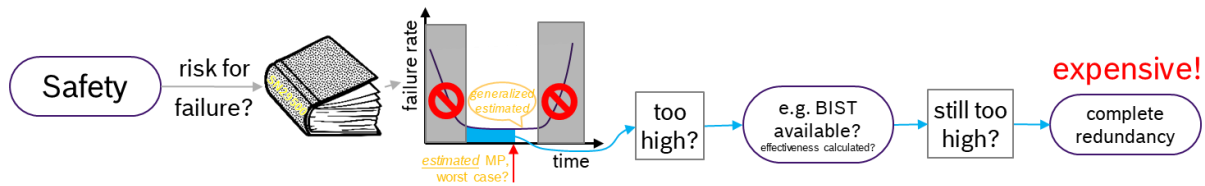


Abbildung 3: Vereinfachte Darstellung der Sicherheitsbewertung.



Abbildung 4: Kritische Kombination aus Stress und Festigkeit (engl.: Strength).

### I.1.1.2 A1.2: Herunterbrechen der Anforderungen und Randbedingungen

In folgendem Abschnitt sind die Beiträge und Arbeitsschritte von RB in Arbeitspaket AP1, Aufgabe A1.2. aufgelistet. Die Nomenklatur der Beitragsnummerierung ist an der Zugehörigkeit eines Beitrages zu einer Aufgabe und einem Arbeitspaket orientiert. Zum Beispiel ist der Beitrag B1.2.4 der vierte Beitrag in der zweiten Aufgabe des Arbeitspakets 1.

### Beitrag B1.2.5 Analyse der Test-Anforderungen

#### Partnerbeitragsbeschreibung

Neben den vorhandenen Schaltungsstrukturen können auch onChip-Testhilfen, wie Analog-zu-Digitalumsetzer (Analog to Digital Converter – ADC), Online-Monitore und andere BIST-Strukturen, Redundanzen – zum Beispiel durch eine klassische Dopplung von Über- und Unterspannungs-Monitoren und Bandabstands-Referenzen - reduzieren. Neben Verfügbarkeitsanforderungen lassen sich so ggf. Safety-Anforderungen mit einem reduzierten Aufwand abbilden.

#### Aktuelle Arbeiten im Berichtszeitraum

Generell sind auf den meisten ASICs bereits einfache Monitoring-Strukturen oder komplette Analog-zu-Digital-Wandler (engl.: ADCs; Analog-to-Digital-Converter) implementiert die diverse Signale überwachen. Dies erfolgt meist auf Basis einer FMEDA und anderen Safety-Analysen.

Oft sind diese Strukturen aber nicht aus „einem Guss“ und werden nach und nach je nach Bedarf mit ins Design übernommen. In VE-VIDES wird von RB auf Basis von Vorarbeiten eine vollständige flexible Monitoring-Matrix implementiert, die sich beliebig für zukünftige ASIC-Produkte reduzieren lässt. Sie ist durch die Verwendung von sehr einfachen Strukturen und einem modularen Ansatz einfach in freie Flächen auf dem Ziel-ASIC implementierbar und ermöglicht zunächst nur ein teileindividuelles Process-Control-Monitoring (PCM) und eine Offline- oder Online-Messung der jeweiligen Monitore.

Durch die Kombination mit einem ADC auf dem ASIC oder in einem uC lassen sich diese Signale zur Überwachung nutzen. Damit kann dann z.B. die echte Alterung gemessen werden und ein Auswechseln in der Werkstatt angestoßen werden durch übergeordnete Systeme.

In diesem Beitrag wurden die o.g. Anforderungen analysiert, sortiert und in eine einfache Übersicht überführt. Auf dieser Basis wurden die Testchipstruktur in Abbildung 2 bzw. dessen Blockschaltbild (BSB) inkl. seiner Beziehungen erarbeitet. Neben den Monitoren in der Matrix wurden weitere BIST-Strukturen definiert, diese sind für die Integrität, Performance und Funktionalität des DSM in „Beitrag B2.3.7 Entwurf eines hochgenauen Delta-Sigma ADC mit integrierten Monitoren“ essenziell und werden in diesem Beitrag näher erläutert.

## **Beitrag B1.2.6 Umsetzungskonzept für Test-Anforderungen**

### **Partnerbeitragsbeschreibung**

Die Arbeitspakete aus den Konzeptüberlegungen aus den verschiedenen Themengruppen bei RB müssen zusammengetragen und abgestimmt werden. Das Test-Interface und weitere Komponenten spielen hier eine zentrale Rolle da es die Ansteuerung, Auswahl und zum Teil auch Ausgabe und Auswertung der anderen Funktionalen Module ermöglichen soll.

### **Aktuelle Arbeiten im Berichtszeitraum**

Die Ergebnisse aus B1.2.5 wurden in diesem Beitrag zum finalen Blockschaltbild nach Abbildung 2 weiterverarbeitet. Hierbei wurden Details wie Spannungsversorgung, Interfaces, etc. abgestimmt und in Richtung der weiteren Teilpakete festgelegt.

Beispielsweise waren die meisten bis dato bei RB genutzten Test-Interfaces entweder unter- oder überdimensioniert, sie konnten also entweder nicht genug abdecken oder waren zu genau und umfangreich. Auf Basis eines Vergleichs von derzeitigen und zukünftigen Serientester-Plattformen wurde daher in Absprache mit den Testexperten die Auflösung bzw. Genauigkeit des Basismoduls reduziert, die Geschwindigkeit für den Testzugriff optimiert und für verschiedene Komplexitätsgrade von Testzugriffen flexibler gestaltet. Dies äußert sich unter anderem in einem modularen Ansatz, welcher mehr oder weniger Signale durch einfache Verdopplung oder Halbierung eines Teiles des Digitalteils des Test-IF ermöglicht. Auch wurden bestehende Anforderungen bzw. deren Umsetzung hinterfragt und zum Teil entfernt.

Weiterhin sind die Supply-Anforderungen der Test-Strukturen an die internen Standardversorgungsmodule angepasst worden, sind flexibel auf zukünftige Technologien übertragbar und ermöglichen die Ansteuerung mit Mikrokontrollern der nächsten Generationen.

## **Beitrag B1.2.7 Untersetzung von Detektor-Anforderungen**

### **Partnerbeitragsbeschreibung**

Aus den in AP1.1 definierten Anforderungen muss eine eindeutige Beschreibung der von den Monitor- und Sensor-Strukturen zu leistenden Funktion erfolgen. Wichtige Randbedingungen sind dabei die eigentliche Funktion der Applikation, die möglichst nicht gestört werden sollte und die Art der zu erfolgenden Überwachung.





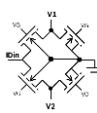
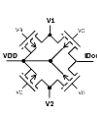

### **Aktuelle Arbeiten im Berichtszeitraum**

Bosch entwickelte in VE-VIDES ein Selektionstool für die Degradations-, Stress- und ESD-Sensoren bzw. „Physical Unclonable Functions“ (PUF). Das Tool, wie in Abbildung 5 dargestellt, beinhaltet sowohl Priorität der Sensoren, Technologieoptionen und Stromverbrauch. Anforderungen an die Genauigkeit der Auswerte-Schaltung wurden hergeleitet und der in „Beitrag B2.3.7 Entwurf eines hochgenauen Delta-Sigma ADC mit integrierten Monitoren“ beschriebene Delta-Sigma-Wandler (DSM) ist mit 20 Bit Auflösung für die meisten Monitore, wie zum Beispiel die in Abbildung 6, mehr als ausreichend.

In einem auf den Arbeiten aufbauenden Folgeprojekt mit Seriencharakter kann daher der DSM nach Bedarf auch in der Auflösung reduziert oder durch eine einfachere Struktur ersetzt werden. Die Monitoring-Matrix nach Abbildung 2, die in den folgenden Beiträgen detaillierter beschrieben wird, ist vollständig unabhängig von den eigentlichen Schaltungen auf dem Ziel-ASIC implementiert. Bei Bedarf lässt sie sich ebenfalls bzgl. Versorgung und räumlicher Nähe zu gewissen Schaltungen im Layout entkoppeln. Ein Stören oder Fehlzugriff auf funktionale Elemente des ASICs wird dadurch vollständig verhindert. Temperatur- und mechanisches Stresssensoren ermöglichen eine Plausibilisierung der anderen Sensorergebnisse durch eine zeitnahe gemeinsame Messung.

Im der Anforderungs- und Konzeptphase wurden für alle integrierten Sensoren und deren Ansteuerschaltung Verifikationsziele abgeleitet. Beispielsweise muss die Schaltung sicherstellen, dass Stress-Signale mit nur geringen Verlusten an die zu stressenden Elemente weitergeleitet werden, es aber auch keine fehlerhaften Stress-Signale gibt. Diese Überlegungen und Vorgaben wurden auch in einem Verifikations-Konzept abgebildet und in den folgenden AP durch Simulationen abgesichert.



Element	Mode	measured signal	signal Vds/V12 (typical, 25°C) [mV]	Variation over Ambient (-40-150°C) or mech. stress	expected change of signal over lifetime	Measurement accuracy requirements		proposal for IDrain	rough potential estimation	
						absolute (of signal Vabs)	relative (to a similar reference signal)		V <sub>Dout</sub> (typical, 25°C) [mV]	V <sub>Sout</sub> (typical, 25°C) [mV]
NMOS 1.8V/5V 	Ron	V(DS) with gate fully open	100	-40°C: -75mV +150°C: -140mV	<15%	<8%	<500µV (<0.5% of signal)	100µA (might differ from device to device)	125	25
	Vth	MOS device as diode	600	approx. constant	100mV	<8%	<1mV	100µA (might differ from device to device)	625	25
PMOS 1.8V/5V 	Ron	V(DS) with gate fully open	-100	-40°C: -75mV +150°C: -140mV	<15%	<8%	<500µV	-100µA (might differ from device to device)	1650 4850	1775 4975
	Vth	MOS device as diode	-600	approx. constant	100mV	<8%	<1mV	-100µA (might differ from device to device)	850 4250	1775 4975
Resistors 	Ron	Voltage drop over resistor	1000	resistor type specific, e.g. -40°C: 1400mV +150°C: 800mV	<5%	<8%	<5mV	100µA (might differ from device to device)	1050	25
Bipolar C=Idrain B= +1µA E=GND 	Ron	not yet defined	not yet defined	not yet defined	not yet defined	not yet defined	not yet defined	not yet defined	not yet defined	25
	Vth	EB-forward diode voltage	800	-40°C: -900mV +150°C: -560mV	<5% (never observed degradation)	<2%	<1mV	100µA	850	25
NMOS Wheat-Stone Bridge  (mech. sensor or PUF)	Ron	Voltage drop V12: V1=V <sub>Dout</sub> V2=V <sub>Sout</sub>	0	in typical stress ranges of MC package +100mV	none expected	<500µV	-	5V	950mV (alternatively 2.55V)	950mV (alternatively 2.55V)
	Vth	Voltage drop V12: V1=V <sub>Dout</sub> V2=V <sub>Sout</sub>	0	in typical stress ranges of MC package +100mV	none expected	<500µV	-	100µA	950mV (alternatively 2.55V)	950mV (alternatively 2.55V)
PMOS Wheat-Stone Bridge  (mech. sensor or PUF)	Ron	Voltage drop V12: V1=V <sub>Dout</sub> V2=V <sub>Sout</sub>	0	in typical stress ranges of MC package +100mV	none expected	<500µV	-	0V	950mV (alternatively 2.55V)	950mV (alternatively 2.55V)
	Vth	Voltage drop V12: V1=V <sub>Dout</sub> V2=V <sub>Sout</sub>	0	in typical stress ranges of MC package +100mV	none expected	<500µV	-	-100µA	950mV (alternatively 2.55V)	950mV (alternatively 2.55V)
PUF non-matching MOS 	Ron	V(DS) with gate fully open	300	-40°C: -225mV +150°C: -420mV	none expected	<8%	<500µV	100µA (might differ from device to device)	325	25
	Vth	MOS device as diode	1000	approx. constant	none expected	<8%	<500µV	100µA (might differ from device to device)	1025	25

**Abbildung 6:** Zusammenfassung der Anforderungen an die Signal- und Messgenauigkeit.

## I.1.2 AP2 Design, Architektur und Modellierung

### I.1.2.1 A2.2. Integration und Entwurf vertrauenswürdiger IP

In folgendem Abschnitt sind die Beiträge und Arbeitsschritte von RB in Arbeitspaket AP2, Aufgabe A2.2. aufgelistet. Die Nomenklatur der Beitragsnummerierung ist an der Zugehörigkeit eines Beitrages zu einer Aufgabe und einem Arbeitspaket orientiert. Zum Beispiel ist der Beitrag B2.2.4 der vierte Beitrag in der zweiten Aufgabe des Arbeitspakets 2.

#### Beitrag B2.2.9 Analyse der Integrationsaspekte für vertrauenswürdiger IPs

##### Partnerbeitragsbeschreibung

Das erste Konzept in Form eines Blockschaltbildes (BSB) muss weiter detailliert und hinsichtlich Safety- und Security Anforderungen abgeglichen werden. Dazu wird auf Basis der Ergebnisse der Beiträge aus A1.2 eine weitere Detaillierung der Komponenten hinsichtlich Integration mit Abgleich gegen die Safety und Security Anforderungen; Konzeptanalyse verschiedener Monitoransätze und Vorbereitung zur Integration für eine Zielapplikation, mit den vorher definierten Safety und Security-Anforderungen, durchgeführt.

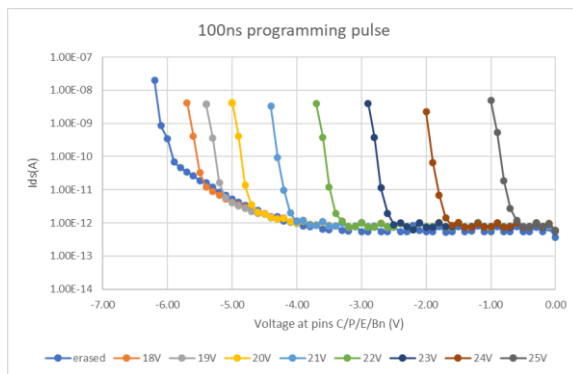
##### Aktuelle Arbeiten im Berichtszeitraum

Die Arbeiten zu B2.2.9 wurden im Laufe des Jahres 2023 abgeschlossen. Die genannten Schaltungskonzepte für die Auswertung der integrierten Sensoren wurden entwickelt und skizziert, in

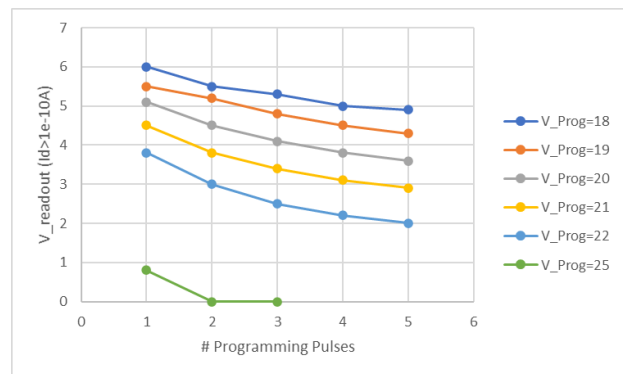
Folge-Beiträgen werden diese dann in finale Schaltungen und schließlich Layouts für die Fertigung übersetzt. Die Konzepte für PUF und ESD-Detektoren wurden ebenfalls erstellt, diese sind mittlerweile integriert in das Gesamtkonzept und somit ein modularer Teil des Monitormoduls aus Abbildung 2.

Die ESD-Logger wurden auf Basis der Ergebnisse aus Beitrag B1.2.7 „Untersetzung von Detektor-Anforderungen“ mit drei verfügbaren, aber verschiedenen Speicherzellen analysiert und in ersten Testschaltungen in der Simulationsumgebung bei Bosch umgesetzt.

Abbildung 7 und Abbildung 8 zeigen die Auslesespannung für eine der Strukturen bei unterschiedlichen Spannungs-Leveln nach einem kapazitiven Manipulieren bzw. in Abhängigkeit der Anzahl der einwirkenden Strom-Pulse am Eingang. Durch diese Analysen lassen sich einerseits die mögliche und nötige Auflösung des analogen Auslesevorgangs aber auch die Nutzbarkeit der jeweiligen Struktur für verschiedene Spannungsanforderungen an den Eingängen des nutzenden ASIC ableiten. Das Vorgehen und die technischen Details wurden u.a. in [13] vorgestellt.



**Abbildung 7:** Auslesen der Spannungs-Verschiebung durch kapazitives Manipulieren des floatenden Gate-Anschlusses. Durch die Erhöhung der Programmierspannung kommt es zu einer deutlichen Schwellenverschiebung.



**Abbildung 8:** Lesen der Spannung, während 100pA durch den Sensortransistor forciert werden.

Für alle der in der Monitormatrix implementierten Monitore ist wie zuvor beschrieben eine Selektionsmatrix – die jeweils für die Zieltechnologie erstellt werden muss – auf Basis der Arbeiten in VE-VIDES vorhanden. Abbildung 9 zeigt einen Ausschnitt der Matrix für die „Front end of line“ (FEOL) Bauelemente und die jeweils abgedeckten und relevanten Effekte. Dafür lässt sich dann der jeweilige Stress-Strom der permanent oder auch nur temporär nach Bedarf angelegt wird – z.B. auf Basis einer bestimmten Sequenz oder zu einem gewissen Zeitpunkt – ableiten.

In Abbildung 10 und Abbildung 11 sind zwei der Physical Unclonable Functions (PUF) bzw. die diese realisierenden Bauelemente abgebildet mit ihren Verteilungen. Diese werden durch den Device-Mismatch der Minimal-Transistoren erzeugt und lässt sich vor allem für zukünftige Security-Anforderungen nutzen. Die Single-Ended-Struktur in Abbildung 10 hat den Nachteil das die Mess-Signale sehr stark von der Temperatur abhängen bei der gemessen wird. Dies lässt sich durch verschalten von mehreren Transistoren sehr stark reduzieren, da die differentielle Messung über einer Brücke den Mismatch weitgehend eliminiert.

In Summe wird für den angedachten modularen Ansatz eine Monitormatrix mit 255 Tabs erstellt, diese sind dann beliebig mit ESD-Loggern, BEOL-Devices mit Stress und z.B. PUFs nutzbar.

Device	Type / Position	RB Baseline (w/o flavors, PLDD2)	70	Priority (1-3)			Stress current			all	allowed
				Reference	HCI [EM]	HCI (antenna)	HTRB, EB-Stress	NBTI	NBTI (antenna)		
1.5V NMOS	digital			1	2	3	4			5	6
1.8V NMOS	analog	x		15	16						
1.8V NMOS	analog			17	18						
3.3V NMOS	analog	x		21	22		23			24	25
5V NMOS	analog	x		26	27						
5V NMOS	analog	x		28	29						
5V NMOS	analog	x		30	31					32	33
1.5V PMOS	digital			34	35		36	37	38	39	
1.8V PMOS	digital			46				47			
1.8V PMOS	analog	x		50				51			
1.8V PMOS	analog			52				53			
3.3V PMOS	analog			56			57	58			
3.3V PMOS	analog	x		59				60	61		
5V PMOS	analog	x		62				63			64
5V PMOS	power			65				66			
Drain extended NMOS 1.8V				67	68						
NPN		x		71			72				
VPNP		x		73			74				
Resistors	Poly silicided	x		75							76
Resistors	Poly P+	x		77							78
Resistors	Poly N+			79							80
Resistors	Poly P+	x		81							82
Resistors (W=min, W=3xmin)	Metal (500µA)	x		83							84
Resistors (W=min, W=3xmin)	Metal	x		85							86
Resistors (W=min, W=3xmin)	Metal	x		87							88
Resistors	high precision TFR			91							
Resistors	high precision TFR			92	93						
DCM	Outer - 2			106							

Abbildung 9: Multiplexer-Bauelementmatrix für relevante FEOL-Bauelemente.

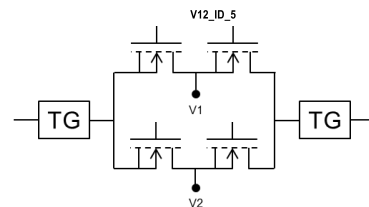
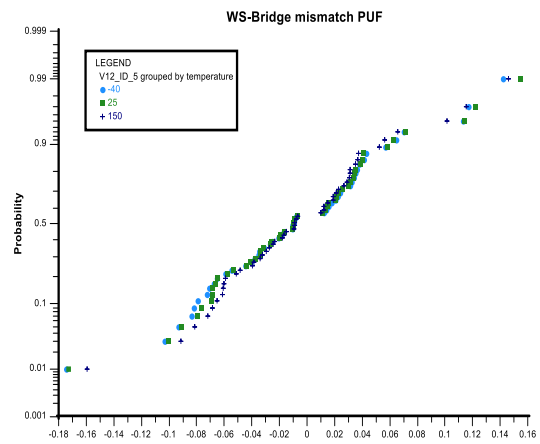
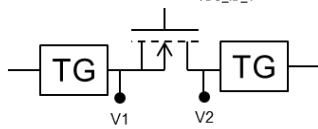
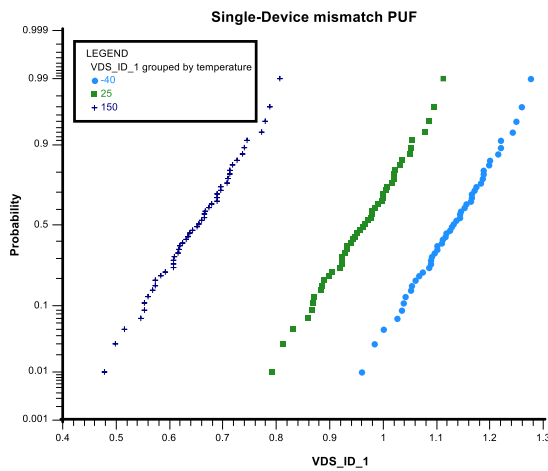


Abbildung 10: Das Signal der einzelnen Elemente wird maßgeblich von der Temperatur beeinflusst. Das Mismatch-Signal für

Abbildung 11: Bei der Konfiguration mit Wheatstone-Bridge ist der Temperatureinfluss gering, insbesondere bei Strukturen im Zentrum der Mismatch-Verteilung.

die PUF liegt in der gleichen Größenordnung.

## Beitrag B2.2.10 Definition und Implementierung von optimierten Schaltungen für Black-Box-IP

### Partnerbeitragsbeschreibung

In diesem Beitrag werden optimierte Schaltungsstrukturen oder Kombinationen für Black-Box-Strukturen, mit möglichst geringem Doppeln von Funktionen, definiert und implementiert. Dazu wird ein Standardhandling bzw. ein Ablauf (engl. Flow) skizziert. Die zuvor in anderen AP von RB internen Partnern erarbeiteten Monitore müssen hinsichtlich definierten Safety und Security-Anforderungen ausgewählt und funktional integriert werden.

### Aktuelle Arbeiten im Berichtszeitraum

Auf Basis der vorhandenen Monitore in der verwendeten Halbleiter-Zieltechnologie und den darüberhinausgehenden neuen Konzepte aus Beitrag B2.2.9 Analyse der Integrationsaspekte für vertrauenswürdiger IPs“ wurden verschiedene Möglichkeiten der Integration diskutiert und Möglichkeiten zur Reduktion der Safety-Konzepte skizziert. In dem Schaltplan des Testchips CO110 sind einige zusätzliche Schaltungs-Elemente wie die in Abbildung 12 dargestellten Einzelemente vorgesehen. Neue Anforderungen bzw. Features von TEST-IF, ADC; MUX etc. wurden festgelegt und umgesetzt - diese ermöglichen ein optimiertes Testen und Messen.

Entsprechend den kritisch bewerteten Elementen einer Schaltung - welche zum Beispiel durch eine Sensitivitätsbetrachtung ermittelt werden – definiert der Ingenieur eine Gruppe von Elementen, die den betreffenden Ausfallmechanismus abbilden. Durch das Selektionstool kann das oder die entsprechenden Referenzelemente ausgewählt werden für die Monitoring-Matrix. Die Einzel-Monitore können sowohl lokal Teil der Schaltung/Blackbox als auch externe Elemente neben der Schaltung sein die von mehreren Schaltungsblöcken gemeinsam genutzt werden.

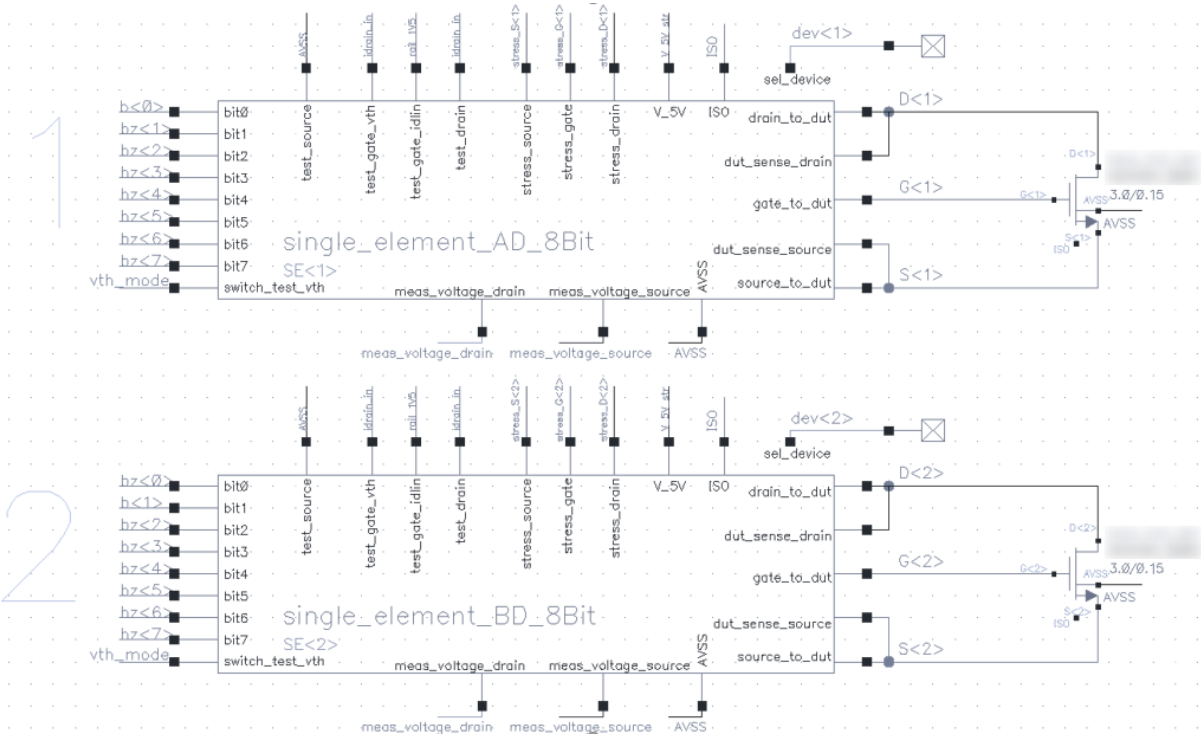
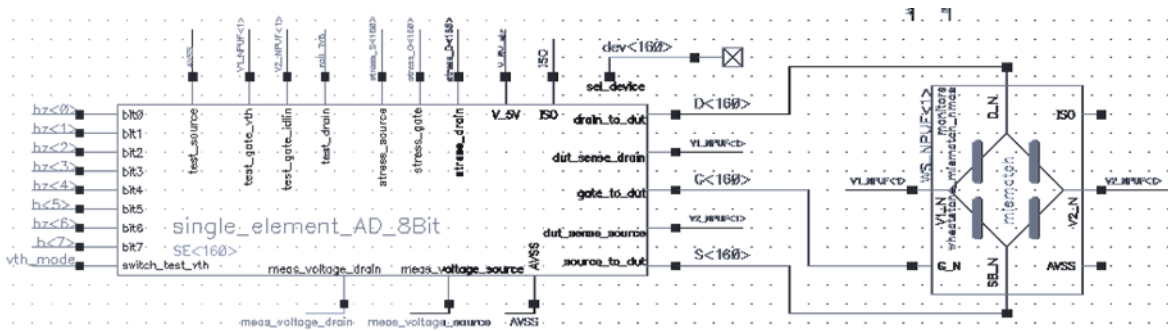


Abbildung 12: Snapshot der Einzelemente der Multiplexer-Struktur für einfache Monitore.

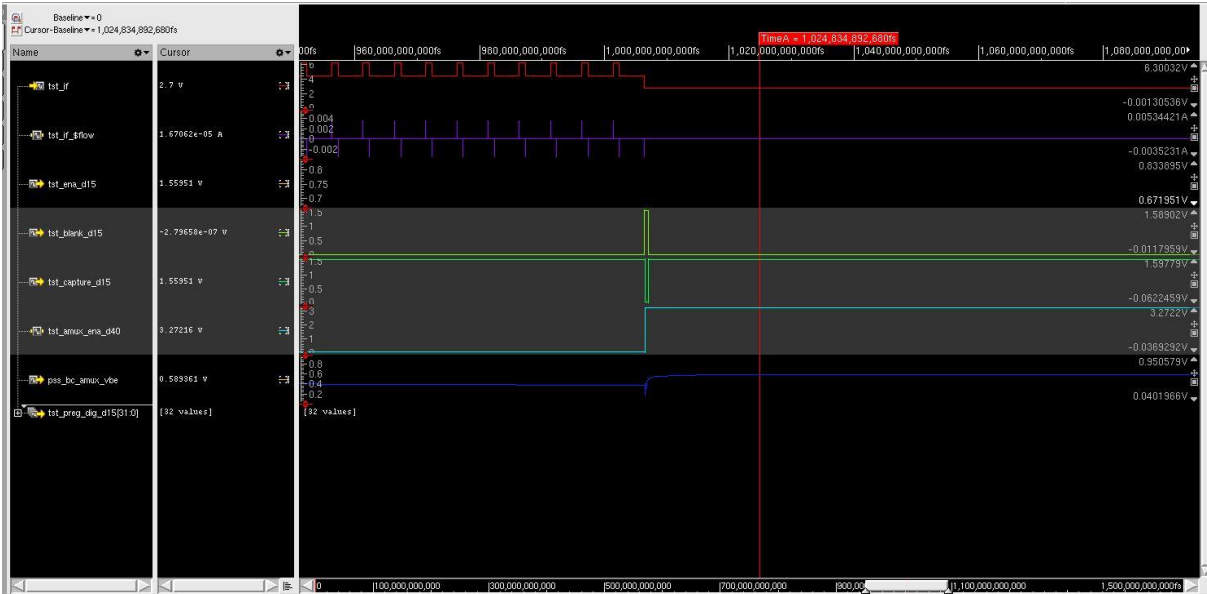
Ist beispielsweise Hot Carrier Injection bei einer Schaltung besonders kritisch bezüglich des Designaufwandes und somit auch der Fläche, lässt sich dieser Effekt bewusst in Kauf nehmen und zur Laufzeit mit beobachten. Bei einer Annäherung an einen bestimmten vorher definierten Wert, wird der ASIC bzw. das auf ihm implementierte System in einen sicheren Zustand versetzt oder schaltet das entsprechende kritische Device auf Ersatz-Elemente, die bisher nicht betrieben worden sind, um.

Der Ablauf muss im Anschluss an dieses Forschungs-Projekt in einem „echten Beispiel“ mit den Safety-Experten vertieft und final hinsichtlich seinem Effizienzgewinn bewertet werden. Einfacher ist hingegen das Beobachten des Einflusses eines Mission-Profiles auf die einzelnen Transistoren zur Laufzeit. Damit lässt sich dann die Laufzeit mit Einhaltung der Spezifikationsgrenzen verlängern. Dies hilft vor allem bei zukünftigen verlängerten oder intensiveren Laufzeiten der Fahrzeuge im ADAS-Kontext.

Die Einzelelemente der Matrix aus Abbildung 12 für BEOL lassen sich modular auch für die anderen Strukturen wie die PUFs in Abbildung 13 nutzen. Abbildung 14 zeigt eine erste Analog-Mixed-Signal-Simulation (AMS), bei der ein Signal aus der Matrix ausgewählt wird und dann über einen analogen Multiplexer (AMUX) an einen Mess-Ausgang geschaltet wird.



**Abbildung 13:** Snapshot Einzelelement-Multiplexer-Struktur für Brückensensorelemente, z.B. PUFs.



**Abbildung 14:** Schnappschuss aus der analogen Mixed-Signal-Simulation (AMS); Hier wird die Testschnittstelle aktiviert und ein Signal ausgewählt, das auf die AMUX-Leitung umgeschaltet werden soll.

## Beitrag B2.2.11 Generierung einer Plattformarchitektur bzgl. Test und Monitoring

### Partnerbeitragsbeschreibung

Anforderungen an Erhöhung der Testabdeckung [on- und offline] und Reduzierung der Testzeit erfordern, dass bisher nicht testbare Zustände durch ein dediziertes Konzept, u.a. mit Low-Voltage/Power Schaltungen beobachtbar gemacht werden. Dies muss unter Berücksichtigung der Sicherheitsaspekte erfolgen.

### Aktuelle Arbeiten im Berichtszeitraum

In den vergangenen Jahren ist bei Bosch und auch anderen wachsenden Unternehmen die Organisations- und Entwicklungskomplexität durch größere, interdisziplinäre und internationale Teams in Kombination mit herausfordernden Arbeitsmodellen wie bei externen Dienstleistern gestiegen. Während es früher einfach war, gemeinsam mit einem oder zwei Kollegen zu diskutieren und zu definieren, bestehen die aktuellen Teams fast immer aus mehr als 10 Mitarbeitern und vielen Fachgebieten. Um die Wiederverwendung zu gewährleisten und Missverständnisse oder Fehler zu reduzieren, werden Standarddefinitionen durch Design- oder Schaltplaneingabegerichtlinien festgelegt.

Die in diesem Beitrag erstellten Schaltungen basieren im Wesentlichen auf dem im Antrag genannten bereits bei Bosch vorhandenen Test-Interface mit Messfunktion der ersten Generation. Als Design-for-Test Verbesserungen stellten sich im Laufe dieses Projekts, neben höherem Messumfang und höherer Genauigkeit, vor allem viele kleine Optimierungen für den Testablauf als zentral heraus. So wurden diverse Änderungen wie beispielsweise ein „Blanking“ von Übergängen implementiert, was zu wesentlich schnelleren Testsequenzübergängen und so einer Verbesserung der Testzeit beiträgt.

Ergänzend dazu wurden auf dem Testchip einzelne neue Module implementiert, die sich in Kombination mit dem verbesserten Test-IF - welches mittlerweile aus einer modularen kleinen Familie von Modulen besteht – beliebig kombinieren lassen.

Für die Plattformkonzepte auf dem Testchip und darüber hinaus hat sich Bosch vor allem auf die folgenden vier Hauptaspekte konzentriert:

- 1) Naming- und Design-Entry-Guidelines
- 2) Definition / Standardisierung von Modulschnittstellen insbesondere für Test- und BIST-Funktionen
- 3) Anpassung der ASIC-Prüffunktionalitäten an moderne Serienprüfmittel
- 4) Schließen der Lücken zwischen bestehenden Modulen

Die Architekturanpassungen wurden für alle neuen Module des Testchips von Bosch direkt implementiert.

Ein einfaches Beispiel für den Punkt „Naming- und Design-Entry-Guidelines“ kann mit der Benennung eines Signals im Schaltplan gegeben werden. Dies folgt in Zukunft einer einheitlichen Struktur wie

modulename\_signalname\_postfix → e.g., module1\_signal234\_a31a.

Über die Hierarchie werden Informationen wie die Spannungsdomäne, der Typ des Signals und ein eindeutiger Name unmittelbar ersichtlich – ergänzen lässt sich dies durch weitere Design-Constraints und durch das Hinzufügen von Informationen im Postfix oder ersetzen bei einer Veränderung des Signals. Durch eine klare automatisiert prüfbare Anweisung lässt sich das Naming leicht verstehen, verbessern und für neue Module gleich richtig anwenden. Die Module

können per Drag and Drop in neue Designs übernommen werden und passen dort auch zur Namensstruktur.

## Beitrag B2.2.12 Standardisierte Umsetzung von Cross-Domain-Interfaces

### Partnerbeitragsbeschreibung

In ASICs mit unterschiedlichen Anforderungen wird die Schnittstelle Analog-Digital immer wieder gemäß verschiedenen Anforderungen neu definiert und erfordert viel Abstimmung.

Um die Entwicklungskosten auch in Zukunft gering zu halten, muss die Integration von vertrauenswürdigen IPs durch eine einheitliche Schnittstelle geregelt werden. Ziel ist eine universelle Sprache in Form einer Interface-Definition über alle bei RB erstellten und zu erstellenden ASICs, die dazu führt, dass die Schnittstelle einmal beschrieben wird und später durch Tausch von technologieabhängigen Sub-Komponenten - wie beispielsweise Levelshiftern - universell einsetzbar ist.

### Aktuelle Arbeiten im Berichtszeitraum

Im Rahmen von VE-VIDES wurde diese doch sehr zentrale Themenstellung angegangen und es wurden diverse Stakeholder aus den Entwicklungsbereichen und den an der Designmethodik beteiligten Gruppen eingebunden. Es wurde ein struktureller Rahmen für die Interfaces definiert und anhand von den unterschiedlich komplexen Funktionsmodulen in Abbildung 15 auf seine Tauglichkeit hin evaluiert.

Diese Standardisierung wurde an einigen neuen Modulen des Testchips umgesetzt und getestet, wird jedoch erst in einem Folgeprojekt – wenn in voller Breite für alle Module umgesetzt – ihre Wirkung entfalten. Neben den im vorherigen Beitrag B2.2.11 „Generierung einer Plattformerarchitektur bzgl. Test und Monitoring“ dargestellten Architekturelementen kommt noch eine klare Separierung von verschiedenen Signaltypen über die Domänengrenzen Analog und Digital hinzu.

So werden beispielsweise Konfigurationssignale klar von anderen Signalen unterschieden, sie werden nur selten zur Laufzeit umgeschaltet und haben in der Regel auch wesentlich geringere Anforderungen als andere Signale wie Clocks oder Interrupts. Dadurch lassen sie sich ggf. sogar sequenziell in einem Bussystem führen, wenn dies zu einer relevanten Verdrahtungsreduktion führt.

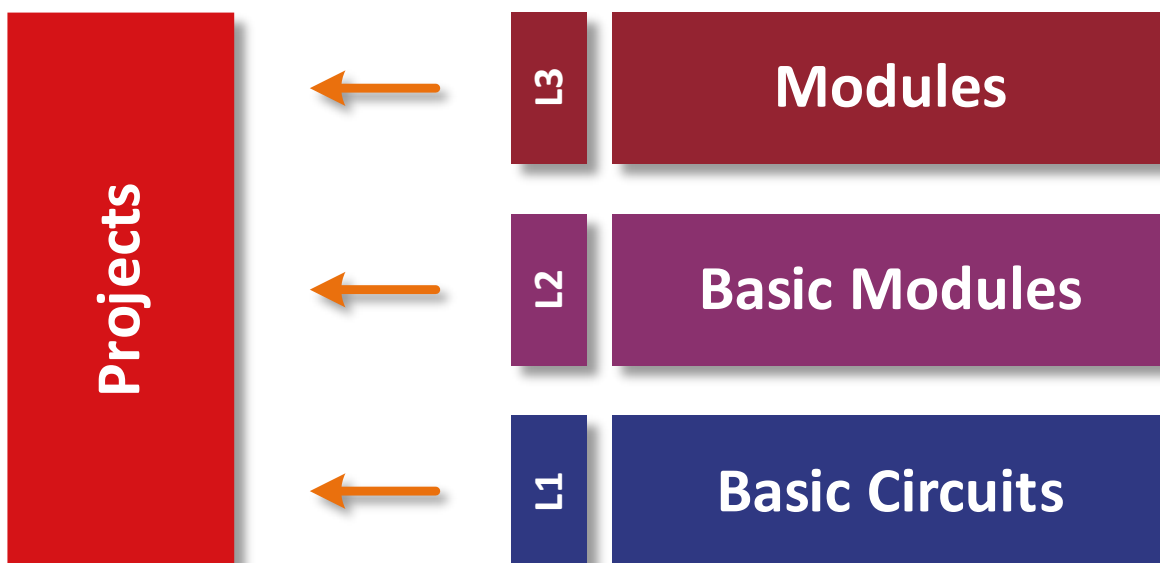


Abbildung 15: Modulebenen L1, L2 und L3 in den RB-Designplattformen.

## **Beitrag B2.2.13 Generierung von Ansteuer- und Auswerteschaltungen für on-chip Monitore (Test+BIST)**

### **Partnerbeitragsbeschreibung**

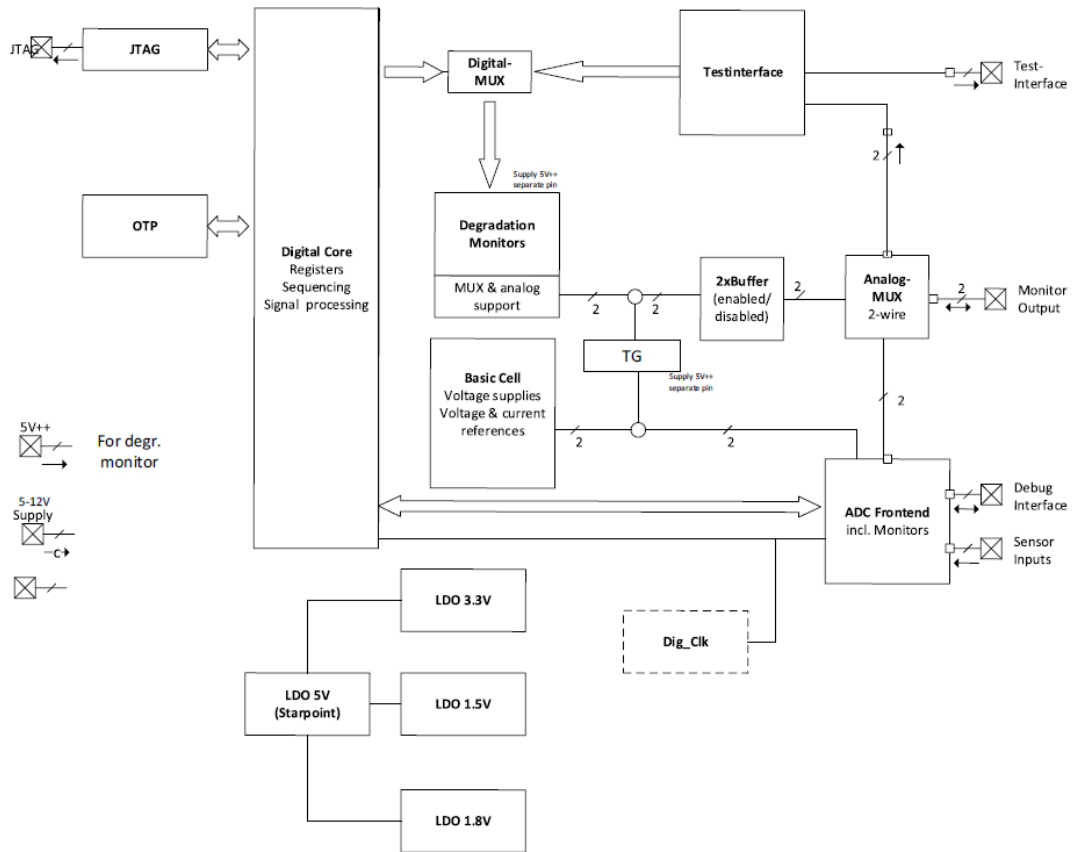
In diesem Beitrag wird eine gemeinsame Nutzung von BIST- und Testimplementierungen vorgestellt, was sowohl eine Reduzierung der Komplexität, des Designaufwands als auch eine höhere Fehlerabdeckung für beide Aspekte ermöglicht. Kompliziert ist hierbei die Vereinbarung der verschiedenen Anforderungen, weiterhin darf der Test von Signalen im BIST-Fall keinen Einfluss auf die eigentliche Funktionalität des ASIC haben.

### **Aktuelle Arbeiten im Berichtszeitraum**

Zusammen mit den weiteren Beiträgen wurden hier Ansteuerschaltungen final konzipiert und erstellt die eine Auswertung der onChip-Monitore aus der Monitormatrix sowohl für Testzwecke als auch zur Laufzeit des ASICs im Feld für BIST-Zwecke ermöglichen.

Sie ermöglichen einerseits die Ausgabe und Auswertung mit dem verfügbaren ADC oder über einen externen Pin, und andererseits die Ansteuerung der Stressmonitore durch „selbst generierten definierten Stress“ in Form von Strom und Spannungswerten.

Die Module wurden erstellt und in die Gesamtstruktur integriert. Die gemeinsame Nutzung für BIST und Serientest wird primär durch gemeinsame Nutzung der AMUX-Signale auf dem Chip erzielt. Diese lassen sich im Testchip nach Abbildung 16 relativ flexibel schalten, eine sichere Umschaltung mit Buffern und einer Transfegatter-Struktur (TG) wurde implementiert. Die Freigabe von kritischen Signalen zur Laufzeit kann durch verschiedene Optionen erfolgen zur Laufzeit. Entweder wird der Zugriff nur durch das Testinterface gegeben oder er lässt sich nach dem Test auf dem Serientester durch Setzen von OTP-Bits für die folgenden Lebenszyklen des ASICs sicher unterbinden. Im finalen Produkt ließen sich die AMUX-Signale je nach Safety-Anforderungen auch separieren oder gar nicht mehr auf externe Pads schalten – im CO110 wurden dies jedoch modular offengelassen und die maximale gemeinsame Funktionalität umgesetzt die sich dann reduzieren oder separieren lässt.



**Abbildung 16:** Abschließendes Top-Level-Blockdiagramm des RB-Test-ASIC mit Ein- und Ausgangspads.

## Beitrag B2.2.14 Vorbereitung zur Integration ausgewählter Monitorkonzepte (Design, Simulation, Layout)

### Partnerbeitragsbeschreibung

Von den zuvor erarbeiteten Monitoren werden die Konzepte ausgewählt und vollständig entwickelt, welche die Safety und Security-Anforderungen am effizientesten erfüllen können. Dabei werden auch Ansteuer-, Signalaufbereitungs- oder Versorgungsfunktionen mit einbezogen.

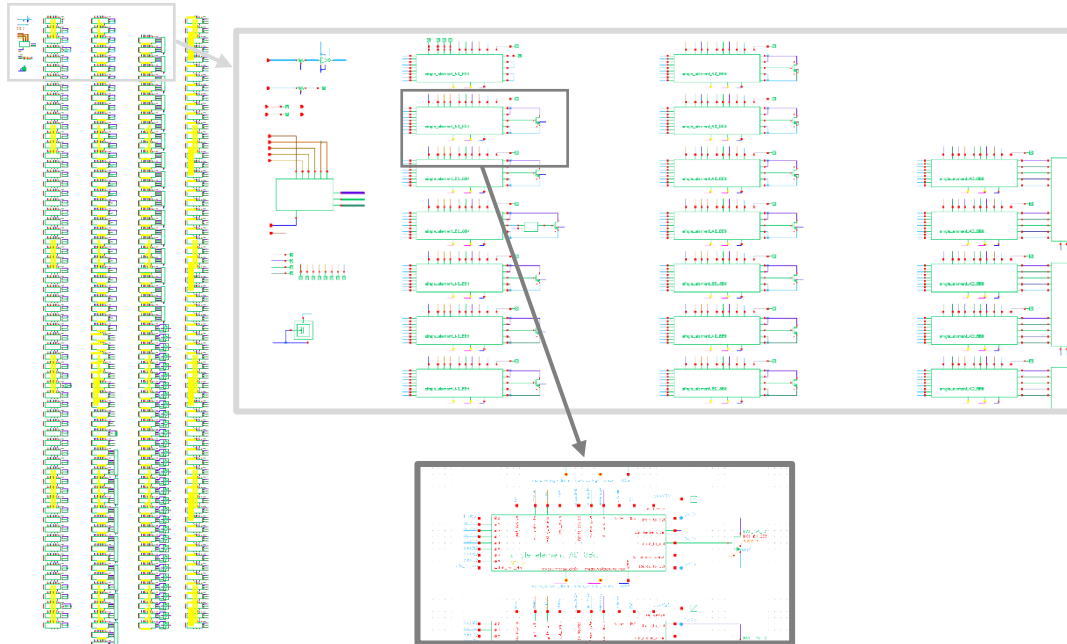
Die Entwicklung beinhaltet Design, Layout, Verifikation auf IP-Ebene und Dokumentation/Modell. So entsteht aus den Teststrukturen eine in der Design-Infrastruktur einsetzbare Library-Zelle mit eindeutigem Symbol, Design, Layout und Modell.

### Aktuelle Arbeiten im Berichtszeitraum

Die Entwicklung des finalen Sensor-Matrix-Modules wurde in diesem Beitrag in der verfügbaren Zieltechnologie abgeschlossen. Dieses wird es unter anderem ermöglichen, Performance und Alterung der Schaltkreise zu monitoren, analoge PUF-Werte zu erzeugen und elektrischen oder mechanischen Stress an kritischen Stellen des Schaltkreises zu erfassen.

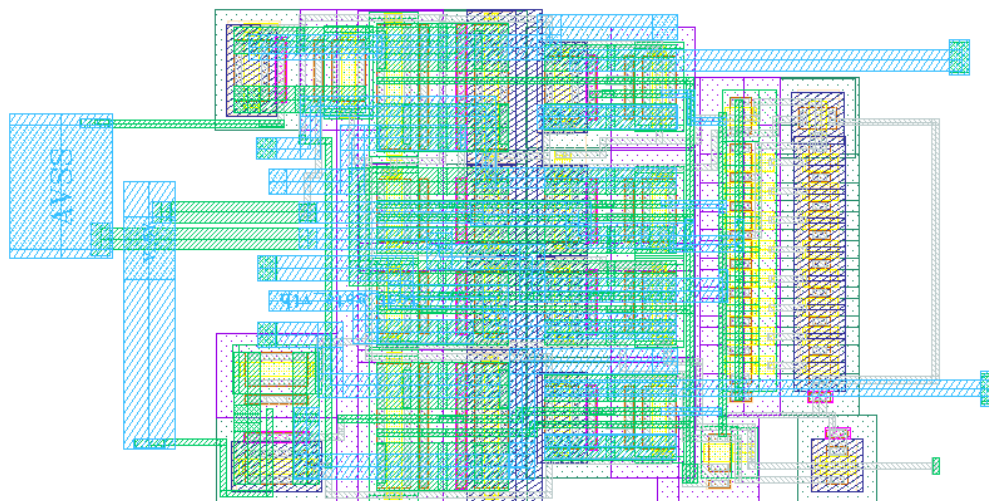
Das Testkonzept für das Gesamtmodul und für die einzelne Sensoren wurde entwickelt. Es erfüllt einerseits die klassische und recht simple Anforderung, die Funktionalität aller Sensoren in Summe und einzeln zu verifizieren. Darüber hinaus können typische Defekte identifiziert werden, die sich durch zum Beispiel durch einen erhöhten Leckstrom äußern. Eine Problematik hierbei ist, dass die Degradation des Schaltkreises nicht schon im Test vorweggenommen werden darf. Trotzdem muss sichergestellt sein, dass alle Stresssignale während der Applikation im Feld korrekt anliegen und auch an das jeweilige DUT/Element weitergegeben werden. Auch diese Anforderung an das Testkonzept konnte erfüllt werden.

Abbildung 17 zeigt hierarchisch die 255 Tab Gesamtmatrix basierend auf dem Einzelement aus Abbildung 12. Die Adressvergabe findet für den Testchip hart über die Verdrahtung statt, kann jedoch auch anders erfolgen. Geringere Zahlen von Sensorelementen lassen sich durch einfaches binäres halbieren der Struktur erzeugen, die dargestellte Matrix entspricht einer Maximalausbaustufe mit vielen Plätzen, die im Testchip mit Subvarianten zu Evaluierungszwecken gefüllt wurden – z.B. durch verschiedene PUF-Wheatstonebrücken-Kombinationen.

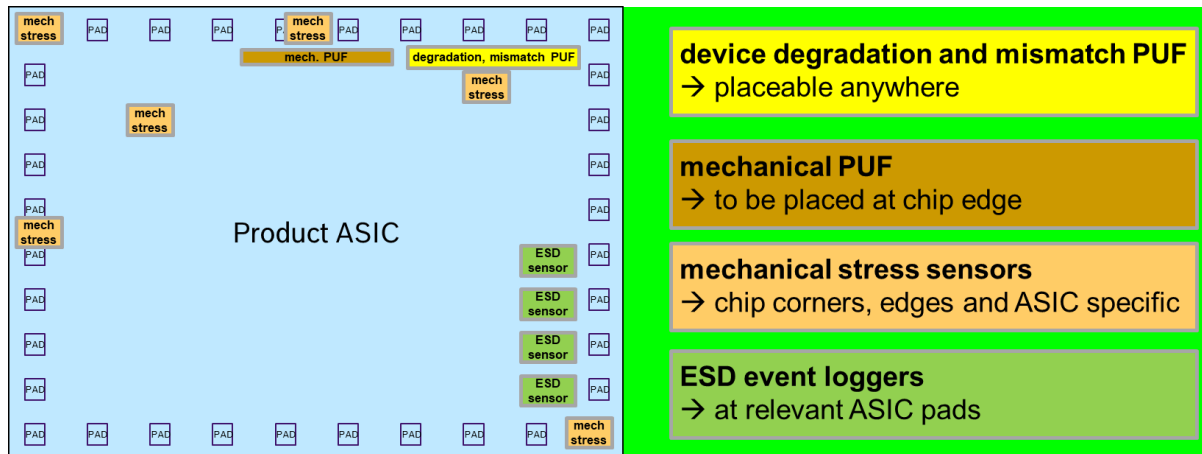


**Abbildung 17:** Übersicht über die Monitoring-IP mit 255 einzelnen Sensoren, die die Fehlermodi aller Prozess- und Device-Optionen abdecken.

Die Schaltung an sich ist hierarchisch in einem Schaltungsmodul gebündelt, lässt sich aber später auf dem Chip im Layout auch verteilen. Ein Einzelementlayout ist wie in Abbildung 18 dargestellt überschaubar und in einem komplexen ASIC von der Fläche her weitgehend vernachlässigbar. Es kann an die empfohlenen Platzierungen in Abbildung 19, die in VE-VIDES von Bosch erarbeitet wurden, für den jeweiligen Sensortyp genutzt werden. Dies muss auch in Abhängigkeit der jeweiligen Nutzung erfolgen, wird ein BEOL-Sensor zur Lifetime-Erhöhung für eine Subschaltung genutzt, sollte er physikalisch in der Nähe oder Teil der Schaltung sein.

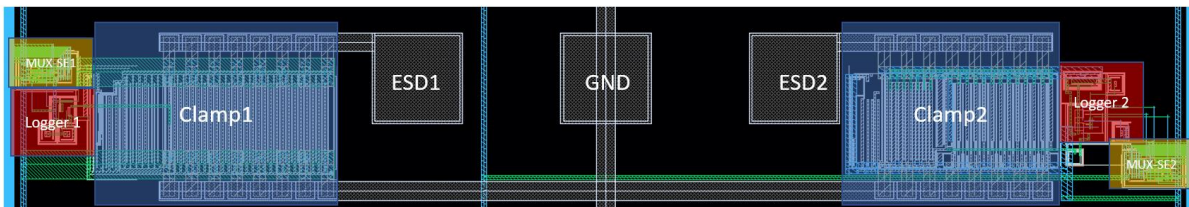


**Abbildung 18:** Layout-Beispiel einer "Single Element"-Instanz, die zum Verbinden eines Sensorelements verwendet wird.



**Abbildung 19:** Übersicht über die Position der wichtigsten Überwachungsblöcke.

Die vorgestellten ESD-Logger werden im Zielprojekt in der Nähe der zu schützenden Schaltung platziert, da der Schutz der Schaltung das eigentliche Ziel der ESD-Schaltung ist. Abbildung 20 zeigt das Layout von zwei verschiedenen Zellen, die hier aufgrund von ESD-Wafertest-Anforderungen der Testchip nebeneinander an den Pads angeordnet wurden. Dadurch sollen die späteren Charakterisierungsmessungen bezüglich ESD - die im Randbereich auch zur Zerstörung der jeweiligen Logger-Schaltung führen können - möglichst isoliert nur einen Teil des Testchips schädigen. Die ESD-Logger (Logger1/2) und die Selektionselemente (MUX-SE1/2) sind im Layout von der Fläche her so klein, dass sie verglichen mit den eigentlichen ESD-Klammern (Clamp1/2) wenig zusätzliche Kosten für das neue Feature erzeugen. Auch lassen sie sich unter den Pads (hier ESD1/2) oder im Randbereich des ASICs platzieren, um freie Flächen zu nutzen.



**Abbildung 20:** Beispiel für eine ESD-Klammer und eine Logger-Schaltung.

### I.1.2.2 A2.3 Design und Modellierung von Runtime-Monitoren zu Überprüfung der Vertrauenswürdigkeit

In folgendem Abschnitt sind die Beiträge und Arbeitsschritte von RB in Arbeitspaket AP2, Aufgabe A2.3. aufgelistet. Die Nomenklatur der Beitragsnummerierung ist an der Zugehörigkeit eines Beitrages zu einer Aufgabe und einem Arbeitspaket orientiert. Zum Beispiel ist der Beitrag B2.2.4 der vierte Beitrag in der zweiten Aufgabe des Arbeitspakets 2.

### Beitrag B2.3.7 Entwurf eines hochgenauen Delta-Sigma ADC mit integrierten Monitoren

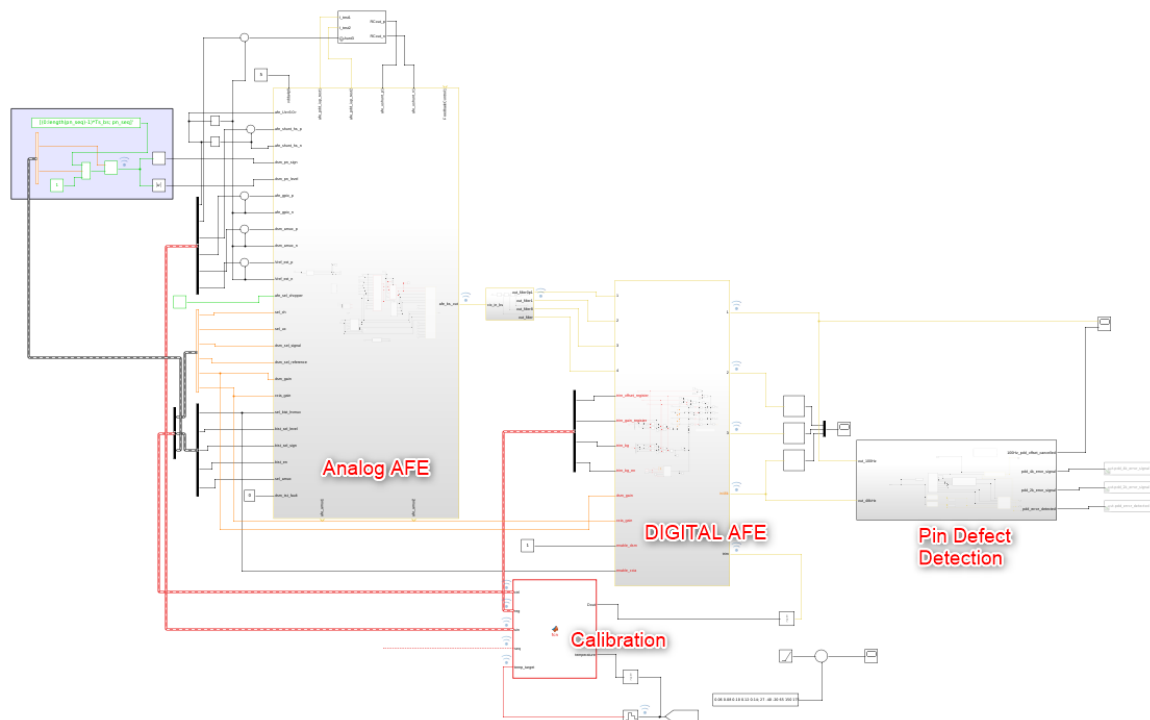
#### Partnerbeitragsbeschreibung

In diesem Beitrag wird ein ADC mit hochgenauen Signaleingängen entworfen, welche mit Monitorfunktionen ausgestattet werden können. Gleichzeitig muss Rücksicht auf eine möglichst hohe „Testability“ genommen werden, um einen ausgiebigen Test der zusätzlichen Monitorstrukturen zu ermöglichen.

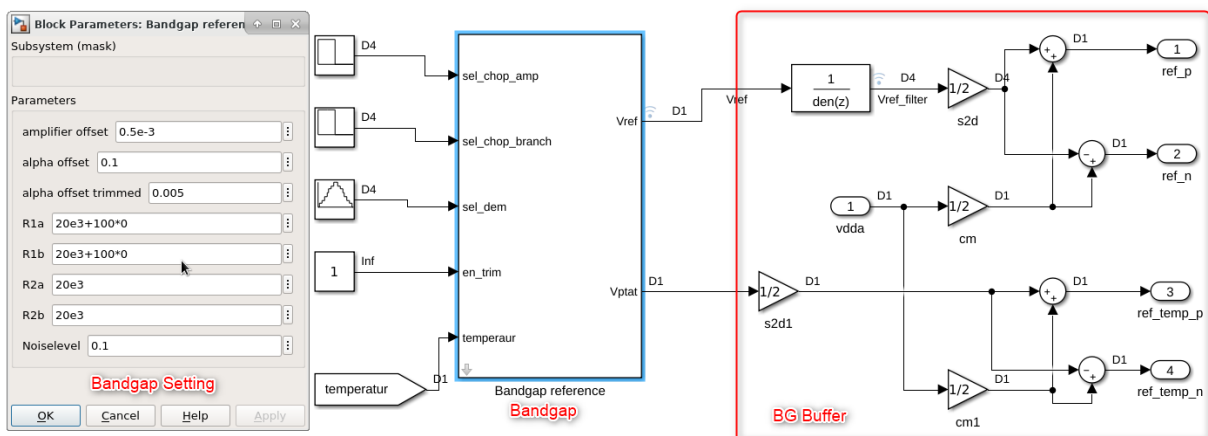
## Aktuelle Arbeiten im Berichtszeitraum

Auf Basis der Anforderungen der Monitoring-Beiträge und generellen Vorüberlegungen wurden als Ziele für den ADC unter anderem eine Auflösung von ca. 20 Bit, eine Hochvoltschnittstelle bis ca. 35V zur Überwachung von externen Signalen und diverse Kalibrier- und BIST-Funktionalitäten vorgegeben. Basierend darauf wurde das Delta-Sigma-Wandler-Konzept für die Implementierung des ADC ausgewählt, um die hohen Anforderungen erfüllen zu können.

Die komplette analoge Schnittstelle einschließlich Multiplexer, programmierbarem Verstärker, programmierbarem Delta-Sigma-Modulator (DSM) mit seiner Referenzspannungserzeugung und seiner Sicherheitsfunktionen wurde zunächst in Matlab Simulink, wie in Abbildung 21 dargestellt, modelliert. Die Subkomponenten wie die Bandgap-Referenz in Abbildung 22 wurden dazu schrittweise erstellt, verifiziert und erst dann in den DSM integriert.



**Abbildung 21:** AFE modelliert mit seinem Kalibrierungsprozess, der in Matlab Simulink modelliert wurde.



**Abbildung 22:** Matlab Simulink-Modell des BG und des BG-Puffers.

Nach einer erfolgreichen Evaluierung in Matlab wurde jeder Block separat in Cadence Virtuoso, zunächst über VerilogA-Modelle, implementiert. Abbildung 23 zeigt beispielhaft die

Kalibriersequenz des DSM in Simulink, die initial bei Aktivierung des Moduls auf dem Chip erfolgen muss, um die gegebene Performance zu erreichen.

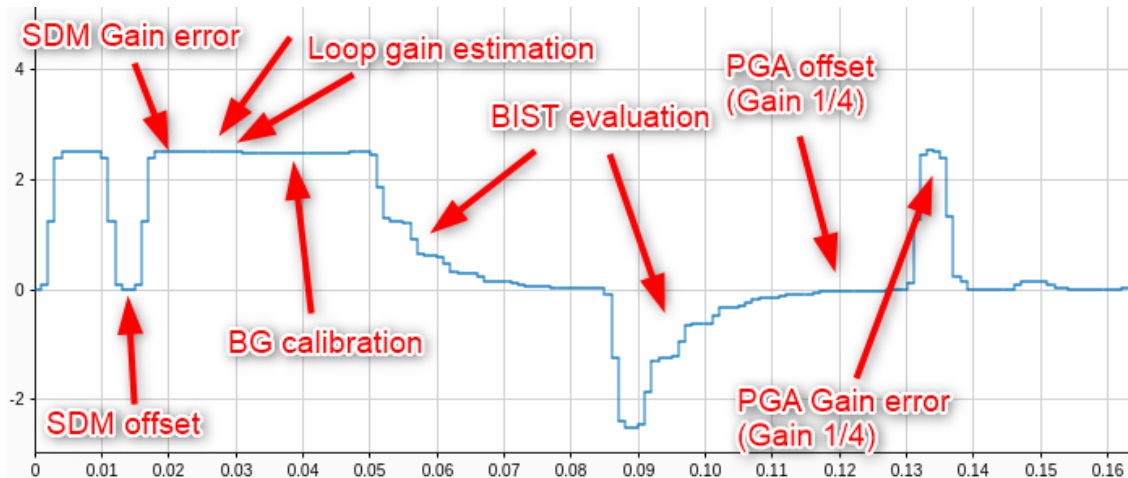


Abbildung 23: Ausgabe der Kalibriersequenz des AFE in Matlab Simulink implementiert.

Die Umsetzung auf Transistorebene wurde anschließend schrittweise abgeschlossen für den vollständigen DSM in Abbildung 24. Der vollständige DSM wurde dann gegen die Simulink-Modelle verifiziert. Abschließend erfolgte für den Testchip CO110 das physikalische Layout der Transistorebenen-Modelle welches mit PEX und PLS (PEX=Post Layout Extraktion; PLS=Post Layout Simulation) optimiert wurde. Dieses kann dann in den Testchip integriert und hinsichtlich Funktionalität simulativ abgesichert werden.

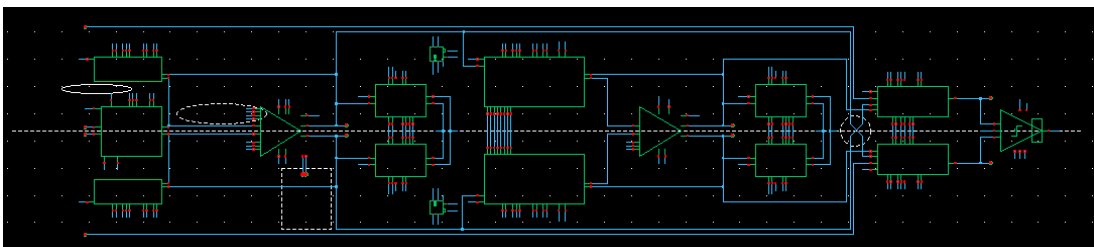


Abbildung 24: Der Delta-Sigma Modulator DSM.

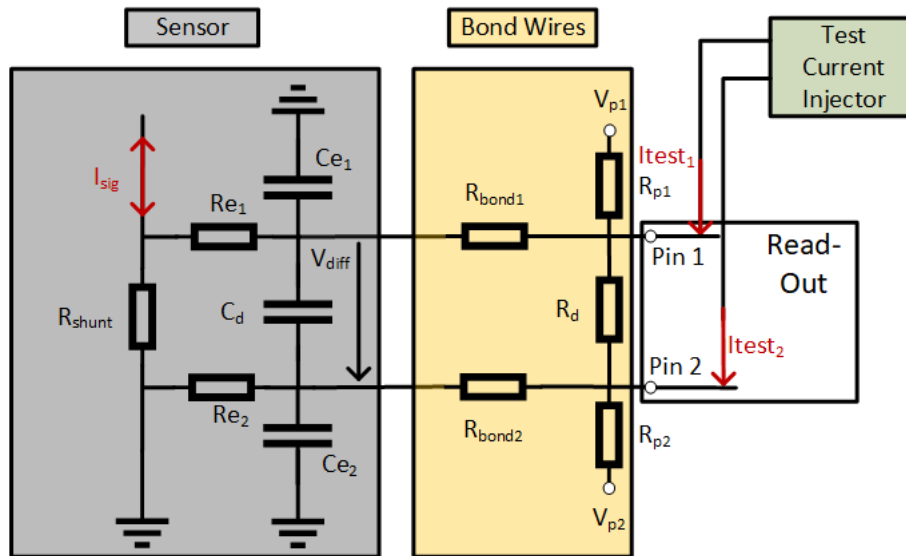
### Beitrag B2.3.8 Definition und Entwurf von Monitoren zur Prüfung der Integrität der Signaleingänge

#### Partnerbeitragsbeschreibung

In diesem Beitrag wird ein Monitorkonzept entworfen und realisiert, um die Integrität von Signaleingängen zu bewerten, wie z.B. die Detektion von defekten Bonds oder defekter externer Beschaltung. Diese Monitore sollen ohne Beeinträchtigung der eigentlichen Messfunktion gleichzeitig durchführbar sein und sie sollen die eigentliche Messfunktion nicht beeinträchtigen.

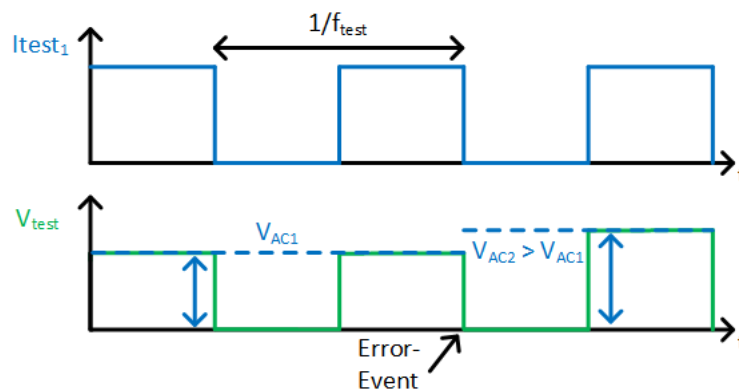
#### Aktuelle Arbeiten im Berichtszeitraum

Als Ergänzung der Funktionalität in automotive Produkten im Beitrag B2.3.7 Entwurf eines hochgenauen Delta-Sigma ADC mit integrierten Monitoren“ ist die Funktionalität der Detektion von Bondabrissen und anderen ähnlichen physischen Problemen erforderlich.



**Abbildung 25:** Modellierung der Bonddrhte und des externen RC-Filternetzwerks zur Erzeugung von Defekten.

Die Monitorschaltung in Abbildung 25 die dazu entworfen wurde, ist in Simulink Matlab modelliert (s. Abbildung 27) und erfolgreich evaluiert worden. Der Entwurfsprozess inklusive Schaltungskonzept auf Transistorebene in Cadence wurde anschlieend fur den DSM durchgefuhrt. Die Layouts der Module, inklusive PEX und PLS sind erstellt (PEX=Post Layout Extraktion; PLS=Post Layout Simulation) und wurden optimiert. Anschlieend wurde die erstellten Module in den ADC aus B2.3.7 integriert und hinsichtlich gemeinsamer Funktionalitat simulativ abgesichert.

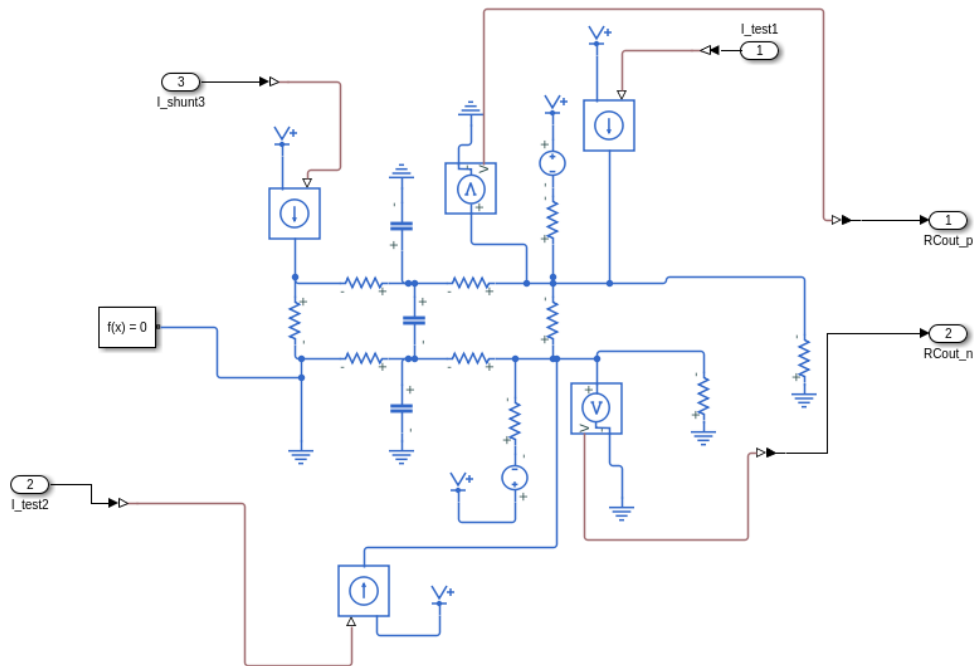


**Abbildung 26:** Einspeisung eines AC-Prufstroms an einem Pin zur Erkennung von Defekten durch die AC-Spannungsantwort.

Das Konzept ist mit Abbildung 26 recht einfach nachvollziehbar:

- 1) Zu bestimmten Zeitpunkten wird ein Teststrom injiziert ohne das ein zu messendes Signal extern anliegt  $\rightarrow$  Referenzwert
- 2) Dies wird sequenziell zu bestimmten Zeitpunkten, z.B. beim Startup der Schaltung, durchgefuhrt
- 3) Durch einen Bondabriss oder andere externe anderungen andert sich der Spannungshub zwischen Pin 1 und Pin 2  $\rightarrow$  Fehlerfall erkannt durch Vergleich mit Referenz

Hierbei ist jedoch auf die genaue Sequenz zu achten und zu verhindern das der „Test Current Injector“ die eigentliche Messung spater verfalscht.



**Abbildung 27:** RC-Block der in Matlab (Sub-Block als Beispiel) über die „Simscape Toolbox“ modelliert wurde.

### Beitrag B2.3.9 Definition und Design eines Monitors für die Funktion des Delta-Sigma ADCs

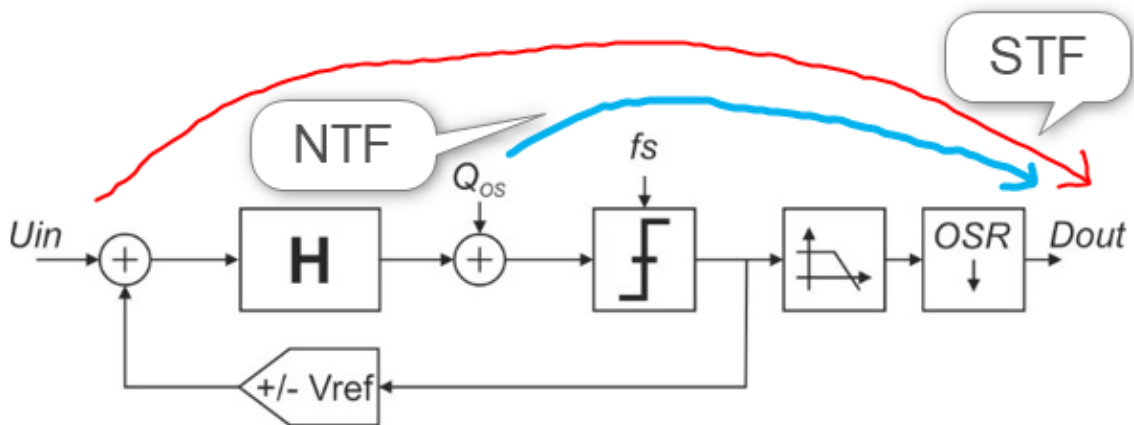
#### Partnerbeitragsbeschreibung

Klassische Monitorkonzepte nutzen Stichprobentests zur Funktionsprüfung von Delta-Sigma ADCs mit der sich daraus ergebenden Einschränkungen der Zuverlässigkeit. Mit der geplanten Erweiterung werden spezifische Eigenschaften des Delta-Sigma ADCs geprüft, um die Fehlererkennung mit gleichzeitig niedriger Test- und Selbsttestzeit nachzubessern.

#### Aktuelle Arbeiten im Berichtszeitraum

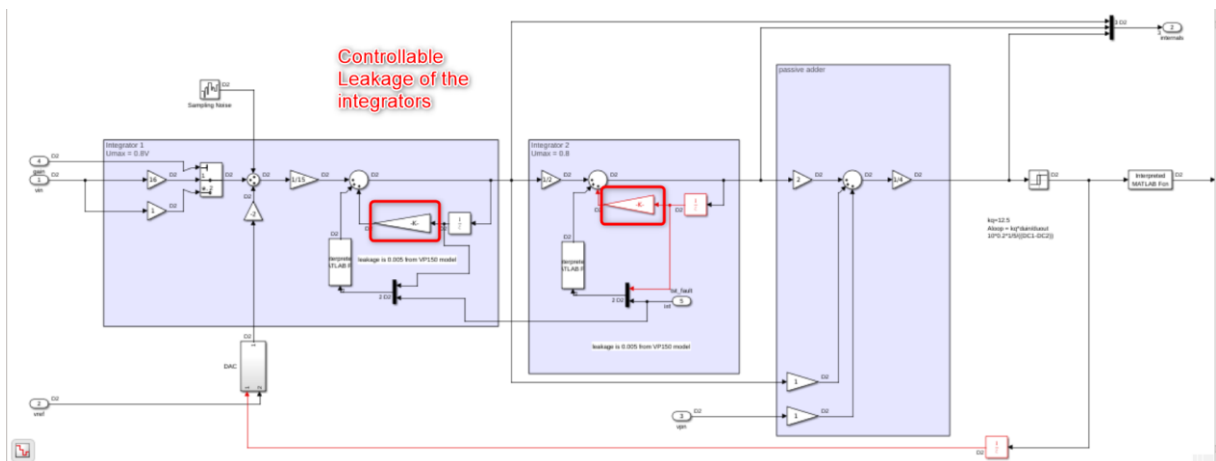
Neben der Verlässlichkeit der Verbindung an die Signaleingänge im vorherigen Beitrag ist für den DSM in „Beitrag B2.3.7 Entwurf eines hochgenauen Delta-Sigma ADC mit integrierten Monitoren“ auch die Performanz des DSM und dessen Testbarkeit sehr wichtig. Dazu wurde in VE-VIDES von RB diese Erweiterung konzipiert und Schritt für Schritt umgesetzt.

Abbildung 28 zeigt den DSM vereinfacht mit der herleitbaren „Signal Transfer Function“ (STF) und der „Noise Transfer Function“ (NTF). Mit Kenntnis dieser Funktionen lässt sich ein zusätzlicher definierter Leakage-Strom (engl.: Leakage Current) in den Rückkopplungen nutzen um den DSM in Simulink wie in Abbildung 29 dargestellt zu testen oder zu kalibrieren. Das Ausgangssignal verhält sich dann wie in Abbildung 30 dargestellt, die frequenzabhängige Leakage verursacht eine relevante Veränderung des DSM-Ausgangs.



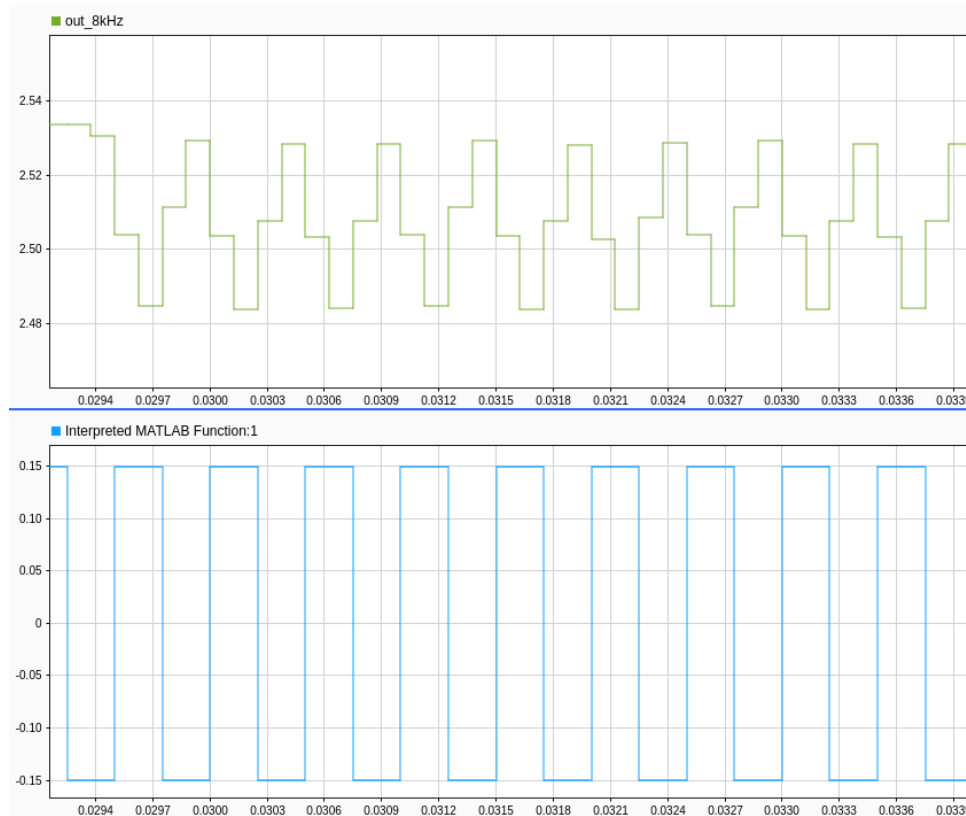
**Abbildung 28:** Der DSM ADC mit seinen Übertragungsfunktionen.

Wie im vorherigen Beitrag wurde bei Bosch der Monitor zunächst modelliert. Anschließend erfolgte die Bewertung der Sicherheitsfunktion und ihres Algorithmus im Simulink-Modell, woraufhin eine Schaltungsimplementierung in Cadence über VerilogA-Modelle erfolgte. Das Schaltungsdesign auf Transistor-Ebene in der Designumgebung Cadence Virtuoso wurde durchgeführt und in der nächsthöheren Ebene und auf CO110 Top-Level in Verbindung mit dem gesamten Analogen Frontend abgesichert.



**Abbildung 29:** Der in diesem Projekt verwendete DSM - die Integratoren beziehen steuerbare Leakage-Faktoren in die Rückkopplungen ein, um die Schleifenverstärkung zu Testzwecken zu verschlechtern.

Die Implementierung der Leakage-Tests konnte mit recht wenig schaltungstechnischem Aufwand und Komplexität durchgeführt werden. Die Layouts der Module, inklusive PEX und PLS sind erstellt (PEX=Post Layout Extraktion; PLS=Post Layout Simulation) und wurden abschließend optimiert.



**Abbildung 30:** Der Ausgang des DSM mit einem modulierten Offset, der mit einer Frequenz von  $f_{\text{qos}}=4\text{kHz}$  in den Quantizer eingespeist wird. Es ist ein Leckstrom vorhanden und somit bewegt sich der Ausgang des DSM merklich.

## I.1.3 AP3 Verifikation der Vertrauenswürdigkeit

### I.1.3.1 A3.4 Analyse und Validierung der Monitore und Fingerprints

In folgendem Abschnitt sind die Beiträge und Arbeitsschritte von RB in Arbeitspaket AP3, Aufgabe A3.4. aufgelistet. Die Nomenklatur der Beitragsnummerierung ist an der Zugehörigkeit eines Beitrages zu einer Aufgabe und einem Arbeitspaket orientiert. Zum Beispiel ist der Beitrag B3.2.4 der vierte Beitrag in der zweiten Aufgabe des Arbeitspakets 3.

#### Beitrag B3.4.3 Definition und Entwurf einer Testumgebung für das Design aus A2.3 inklusive Laborevaluierung

##### Partnerbeitragsbeschreibung

Verschiedene Testszenarien sollen z.B. mit „fault injection“ ermöglicht werden. Ziel ist es eine möglichst vollständige Prüfung der Monitorfunktionen zu erzeugen.

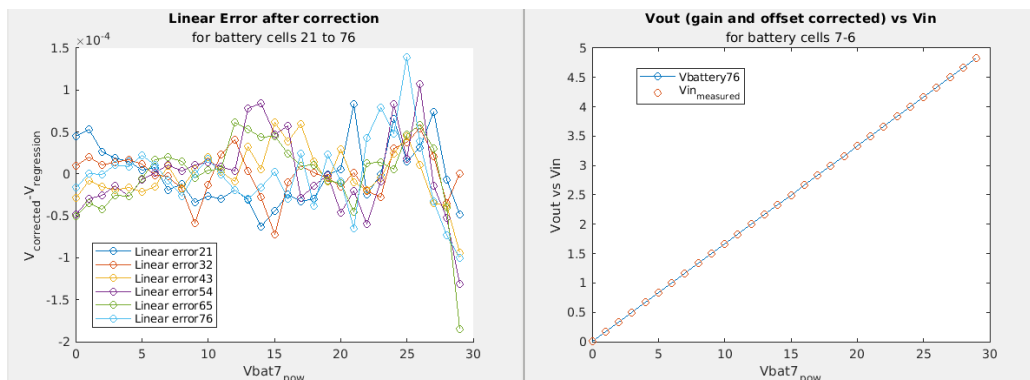
Die entwickelten ADC-Front-End Monitorstrukturen aus A2.3 werden in einem Testchip realisiert und müssen auf ihre Einsetzbarkeit geprüft werden.

##### Aktuelle Arbeiten im Berichtszeitraum

Im Laufe der Arbeit zu B2.3.9 wurden alle relevanten Fehlerbilder in Delta-Sigma ADCs analysiert und dazugehörige Testmöglichkeiten implementiert. Um die ADCs hinreichend in Serienproduktion bei hohen Stückzahlen zu testen, wurden in das Zieldesign aktivierbare und kontrollierbare Fehler nach B2.3.8 und B2.3.9 eingebaut. Diese können von außerhalb des DSM-



Ist der ASIC vollständig hochgefahren muss als Teil der Startsequenz (engl.: Bootloading) eine Kalibrierung des DSM erfolgen, damit lassen sich für den DSM aus VE-VIDES sehr niedrige lineare Restfehler wie in Abbildung 33 dargestellt erzielen.



**Abbildung 33:** Beispiel für eine Signalpfadkalibrierung für die Low-Side-Shunts.

### Beitrag B3.4.4 Einbindung neuer Monitorstrukturen und Erweiterung der Designkonzepte auf vorentwickelte IP-Blöcke

#### Partnerbeitragsbeschreibung

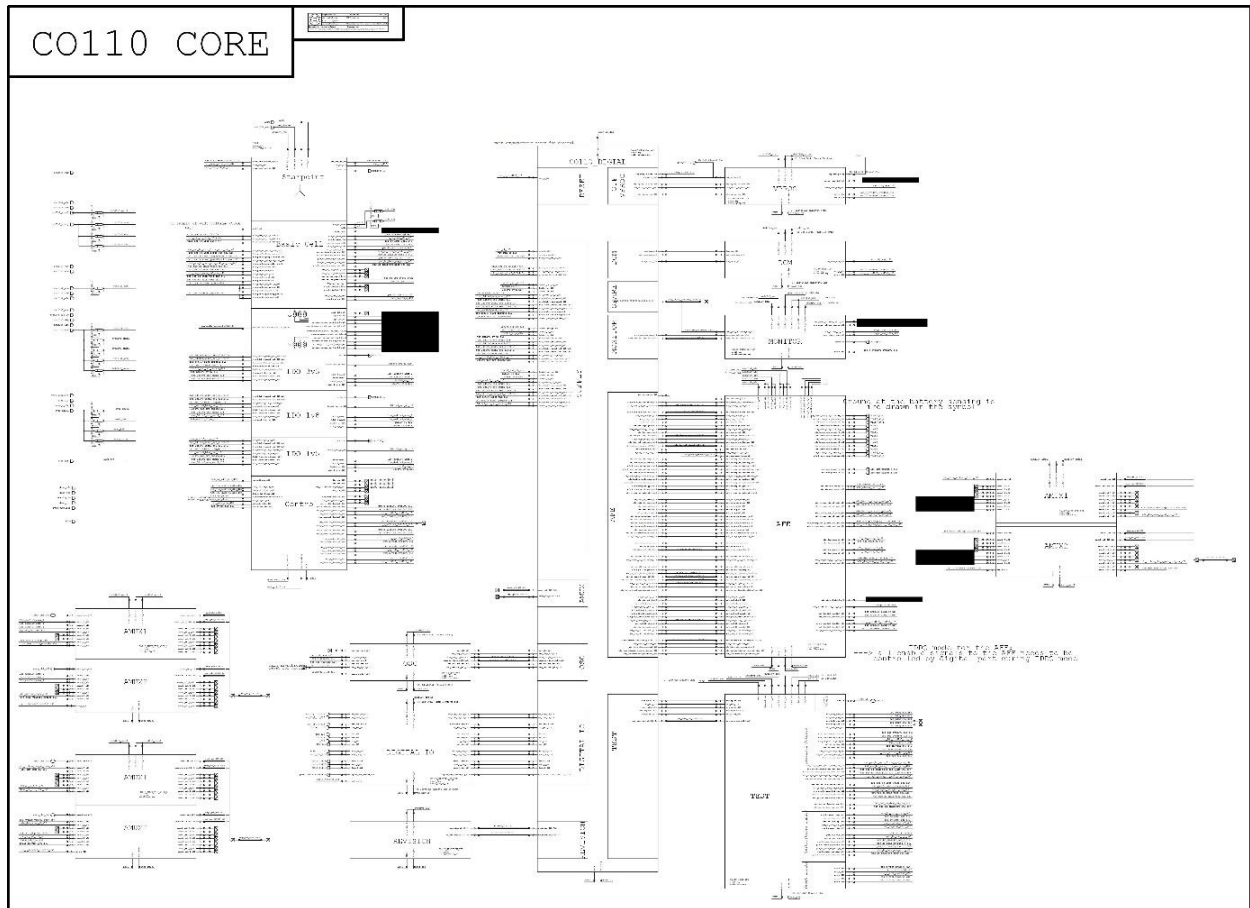
In diesem Beitrag werden die entwickelten Strukturen aus A2.2 in den Testchip und die Gesamtstruktur integriert. Dies beinhaltet verschiedene Monitore, Teststrukturen und fehlerunterdrückende Schaltungen. Zusätzlich werden die entwickelten Schaltungen und Konzepte konsolidiert um eine Auswahl von vorentwickelten Schaltungen als IP-Block bereitzustellen.

Zur Erstellung eines Testvehikels müssen die zuvor erstellten Schaltungen und Modelle in einer verfügbaren und vom Aufwand und Nutzen her optimalen Technologie zusammengeführt werden

#### Aktuelle Arbeiten im Berichtszeitraum

Die in Abbildung 2 definierten Monitore wurden im Rahmen der Projektlaufzeit um weitere Submodule ergänzt und konsolidiert, so wurden beispielsweise sogenannte ESD-Logger mit ins Portfolio aufgenommen. Die Module wurden konzeptionell so umgesetzt das man die im Testchip (Schaltplan in Abbildung 34) umgesetzte Vollausbaustufe nach Bedarf reduzieren kann. Entsprechend wurden die Monitore als Matrix mit 256 Tabs (255 Monitore und Default-Adresse Ausgang=AMUX=GND) in eine Schaltung umgesetzt und um die Ansteuerschaltungen ergänzt. Dazu wurde ebenfalls eine digitale Ansteuerung im Digitalteil des Testchip-ASICs implementiert.

Anschließend wurden die Layouts ebenfalls modular erstellt und nach Bedarf der Monitore – v.a. um die physikalischen Größen v.a. bezüglich mechanische Stress effizient auch im Labor zu sehen – auf dem Testchip verteilt. Die Funktionalität wurde durch AMS-Simulationen sichergestellt.



**Abbildung 34:** Schaltplan des CO110 (auf Core-Modul Ebene + ESD).

### Beitrag B3.4.5 Anwendung der Monitore in einem Zielprojekt oder für einen separaten Testchip

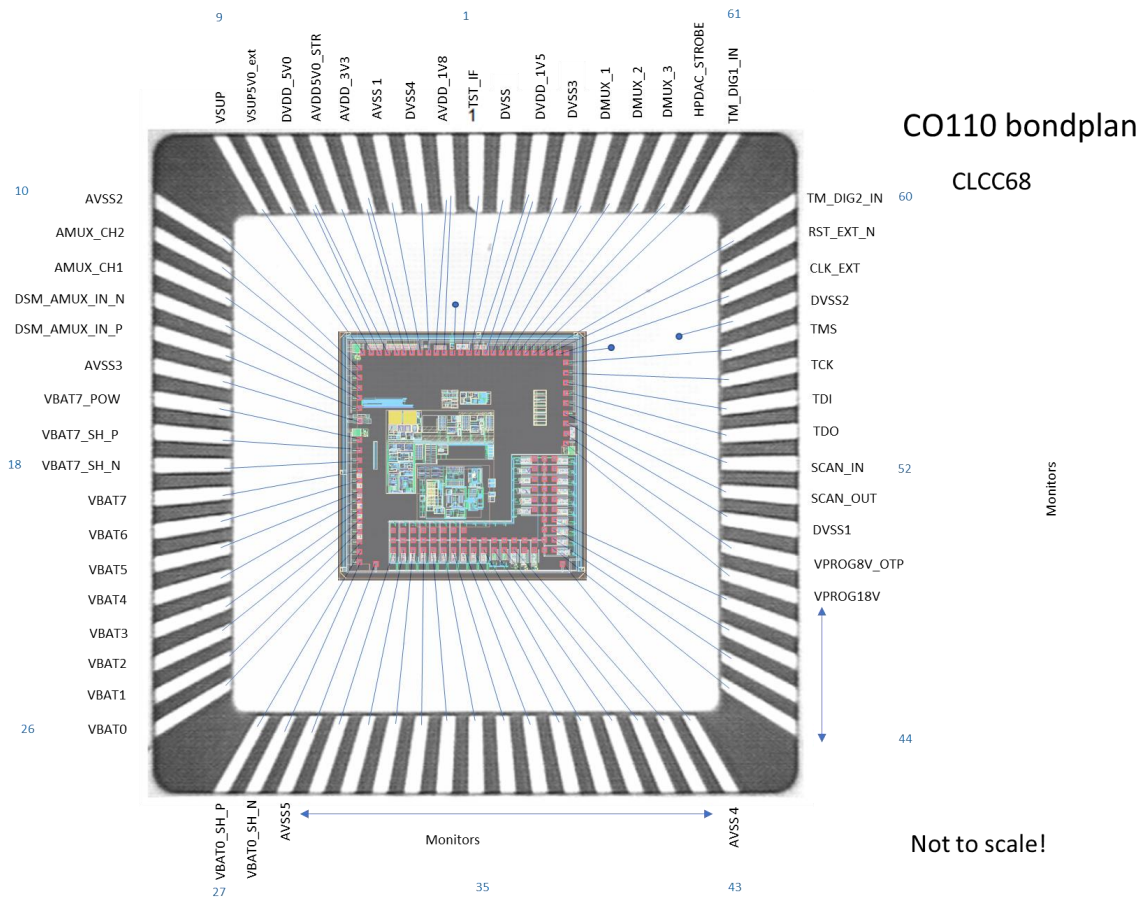
#### Partnerbeitragsbeschreibung

Es muss überprüft werden, ob die in AP2.2 entwickelten Monitor- und Sensor-IPs im Rahmen eines normalen Design-Flows eingesetzt werden können. Das zuvor erstellte Design bzw. die Module müssen in ein Layout überführt und im Rahmen eines Testchips eingesetzt werden.

#### Aktuelle Arbeiten im Berichtszeitraum

Zu Beginn des Teilprojekts bei RB war noch nicht klar, ob die entwickelten Module in ein separates Test-Silizium oder sogar zum Teil gleich als Unterstruktur in ein Serien-Silizium bzw. Produkt von RB implementiert werden (vgl. TVB). Relativ schnell wurde hier aufgrund von Risikobetrachtungen und dem Grad der Neuerungen ein separates Silizium als Zwischenziel definiert. Der wesentlich größere Funktionsumfang der RB-IPs aus den Arbeiten in VE-VIDES führte ebenfalls zur Entscheidung eines eigenen Testchips, ein Seriensilizium würde diesen Umfang nicht benötigen, was zu viel ungenutzte Funktionen (engl.: Overhead) in einem Produkt-ASIC bedeuten würde.

Das Design und Layout wurden abgeschlossen, das finale und verifizierte Einzelchip-Tapeout (Maskenbeauftragung) wurde im Juni 2023 im Rahmen eines Multi-Projekt-Wafers (MPW) in Auftrag gegeben. Das finale Layout im Zielpackage für die Beauftragung des Bondings zeigt Abbildung 35. Die Schaltungen nehmen aufgrund der Anzahl der benötigten Testpads und der gewünschten mechanischen Effekte nicht die komplette Fläche ein.



**Abbildung 35:** Finaler Bondplan inkl. Layout von CO110 in einem CLCC68-Gehäuse.

Der höhere Aufwand im Umfang und der Absicherung des größeren Testvehikels führt jedoch durch eine höhere Simulationsabdeckung im Nachgang zu einer Reduktion des Untersuchungsaufwands und zur Sicherstellung der Projektziele wurden die Messungen zusätzlich im Labor automatisiert. Damit konnten alle relevanten Erkenntnisse bis zum Projektabschluss erzielt werden.

### Beitrag B3.4.6 Tests auf IP-Ebene

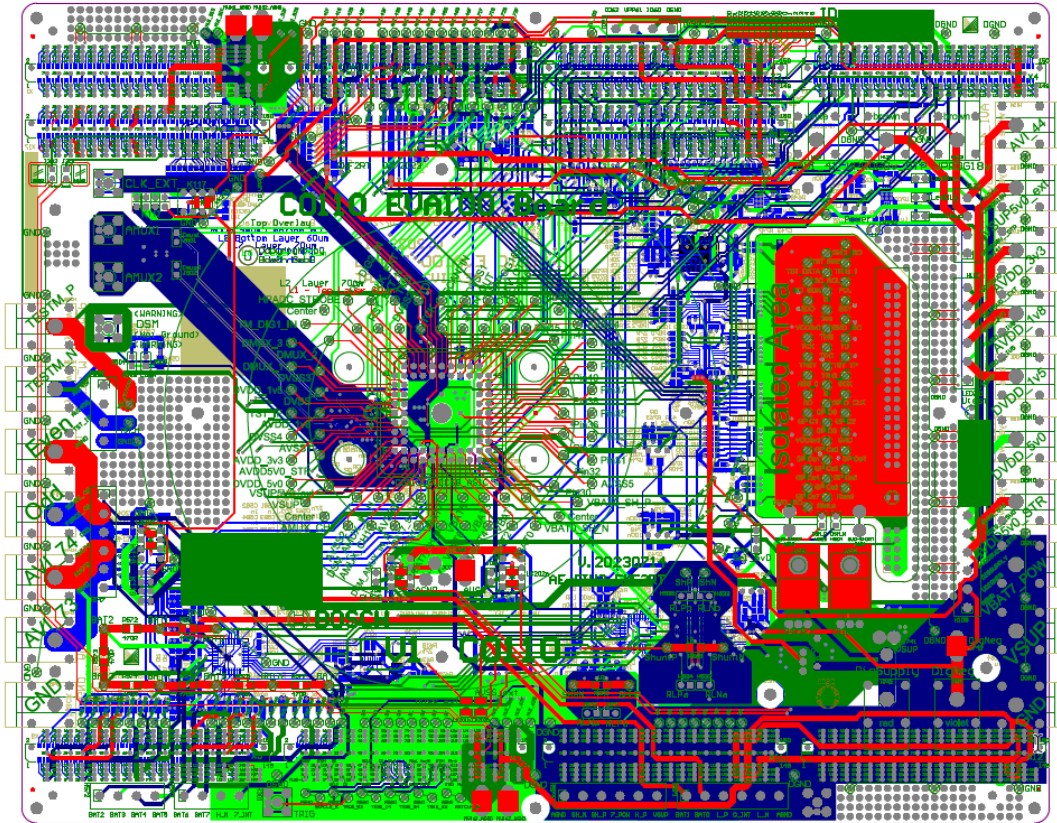
#### Partnerbeitragsbeschreibung

Die entwickelten Monitor- und Sensor-IPs müssen im Zusammenspiel mit der Zielapplikation auf ihre tatsächliche Funktion verifiziert werden.

Ziele: Elektrische Charakterisierung der Monitor-IPs; es muss gewährleistet sein, dass die Monitore die überwachten physikalischen Parameter unter verschiedenen vorher definierten Stressarten zuverlässig über die Lebensdauer des Produktes überwachen.

#### Aktuelle Arbeiten im Berichtszeitraum

Die Messungen am Testchip konnten aufgrund der Prozessierung des MPW erst Ende Q3/2023 starten. In der Zwischenzeit wurde der Messaufbau nach Abbildung 31 erstellt und optimiert, einzelne automatisierte Testsequenzen wurden ebenfalls vorab erstellt. Abbildung 36 zeigt das finale Multi-Layer-Board-Layout (vereinfacht in Abbildung 31, grün und mittig).



**Abbildung 36:** Layout der Leiterplatte für das Charakterisierungslabor für CO110 – mit allen Schichten.

Die Automatisierung mit dem Labortestsystem führt zu einer großen Datenmenge, die im Rest der Projektlaufzeit mit den Annahmen und Simulationsergebnissen abgeglichen wurde. Teilergebnisse finden sich u.a. in den Berichten zu den Folgebeiträgen.

Grundsätzlich ist die volle anvisierte Funktionalität von CO110 gegeben, u.a.:

- 1) Interne Versorgung und Hochlauf inkl. OTP read+write und JTAG sind funktional
- 2) Alle 255 Monitore lassen sich über AMUX und ADC auslesen
- 3) Das Test-Interface lässt sich zum Setzen der Testmodes und zum Auslesen von internen Signalen nutzen, die Ergänzungen sind voll funktional.
- 4) ESD-Logger, PUFs und weitere Monitore lassen sich automatisiert evaluieren und zeigen Ergebnisse im Erwartungsbereich

### Beitrag B3.4.7 Validierung der Designs aus A2.2 durch geeignete Labortests

#### Partnerbeitragsbeschreibung

Die einwandfreie Funktion der Monitore im Testchip bzw. Produkt muss nicht nur über einen begrenzten Zeitraum, sondern über die Produktlebensdauer gewährleistet sein. Dabei muss das zuvor erstellte Konzept –auch für nicht spezifizierte Zustände– sicher gegenüber beabsichtigter und unbeabsichtigter Fehlbedienung sein bzw. hinsichtlich seiner Grenzen evaluiert werden.

Aus diesem Grund sind erweiterte Produktcharakterisierungen im Labor notwendig. Außerdem müssen Langzeittests (sog. Erprobung) hinsichtlich verschiedener Fehlermechanismen mit einer abschließenden (Delta-)Untersuchung durchgeführt werden. Bei dieser wird geprüft, ob und mit welchem Fehlermechanismus das Bauteil ausgefallen ist, ob der Ausfall vorausgesagt wurde

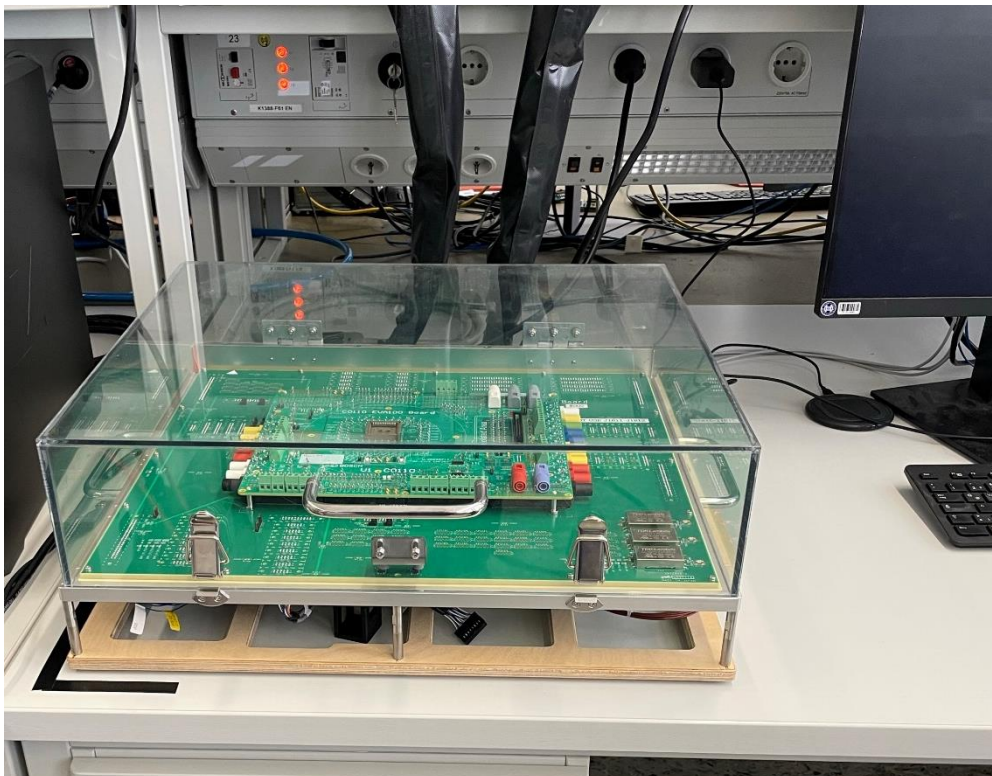
bzw. ob die Monitorfunktion bis zum Lebensdauerende mit der geforderten Präzision zur Verfügung stand.

### Aktuelle Arbeiten im Berichtszeitraum

Der in den vorherigen Beiträgen skizzierte (siehe u.a. Abbildung 2) und bis hierhin final implementierte Testchip CO110 ist so weit gekapselt, das zur Laufzeit nur über die digitalen Schnittstellen Zugriff auf die Module erfolgen kann. Entsprechend müssen im späteren Zielsystem diese Schnittstellen zusätzlich auf höheren Integrationsebenen abgesichert werden – z.B. durch Maßnahmen auf Protokollebene. Eine Beeinflussung der Monitore kann so nur indirekt und im Rahmen der stark eingegrenzten Features erfolgen.

Die Messungen im Labor erfolgen weitgehend mit einem automatisierten Labtester. Abbildung 37 zeigt die finale Platine für die Charakterisierung auf dem Labor-Testsockel. Dieser Aufbau ermöglicht eine sehr breite Charakterisierung über weiter Parameterranges an allen Pins und sich wiederholende Sequenzen.

Da eine vollständige Erprobung nach AEC-Standard sehr aufwändig, langwierig und kostenintensiv ist, wurden im Rahmen von VE-VIDES für den Testchip Langzeitmessungen mit dem Labor-Testsystem mit Simulationsergebnissen inkl. Alterung abgeglichen. Dies bildet eine Teilerprobung nach, die meiste Alterung von Devices findet ohnehin am Anfang der Badewannenkurve nahe der Inbetriebnahme statt. Die Schnittstellen werden bzgl. externen Einflüssen und Mis-Use ebenfalls im Labor untersucht, allerdings an einem frei nutzbaren Platz ohne Automatisierung.



**Abbildung 37:** CO110 Evaluierungsboard im Labor-Testsystem.

Die Ergebnisse der Langzeituntersuchungen folgten weitgehend dem Modellverhalten des in diesem Projekt verwendeten PDKs und wurden im Rahmen der Sample Verification mit den anderen Parameterschwankungen bewertet.

## Beitrag B3.4.8 Auswertung der Teststrukturen verschiedener Monitorkonzepte

### Partnerbeitragsbeschreibung

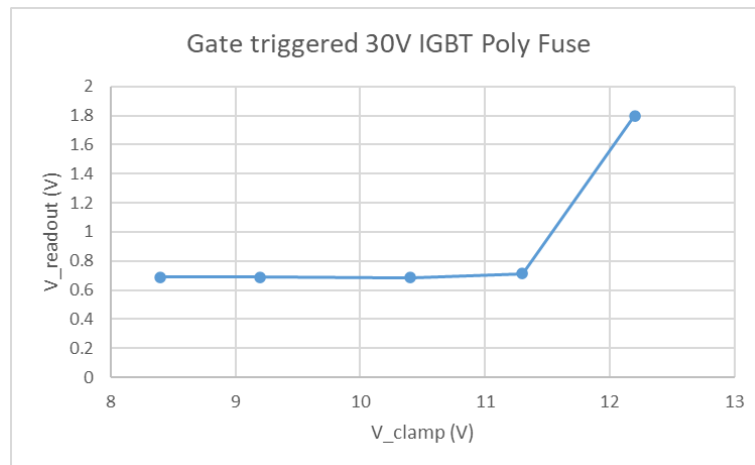
Produkte können verschiedenen Alterungsprozessen unterworfen sein. Zur Überwachung des Alterungsprozesses sind ein oder unter Umständen verschiedene Monitore notwendig, deren Daten korreliert werden müssen, um Fehlermodi exakt zu identifizieren.

Ebenso sollen unerwünschte Wechselwirkungen der Sensoren ausgeschlossen werden. Außerdem sollte geprüft werden, ob eindeutige und über die Lebensdauer stabile Signaturen aus den Monitoren extrahiert werden können, die für eine sichere Identifikation des Chips und Kommunikation über die Systemgrenzen hinaus genutzt werden können. In diesem Zusammenhang müssen auch die in AP2.2 entwickelten Kompensationsmethoden für ungewollte externe Störgrößen validiert werden.

### Aktuelle Arbeiten im Berichtszeitraum

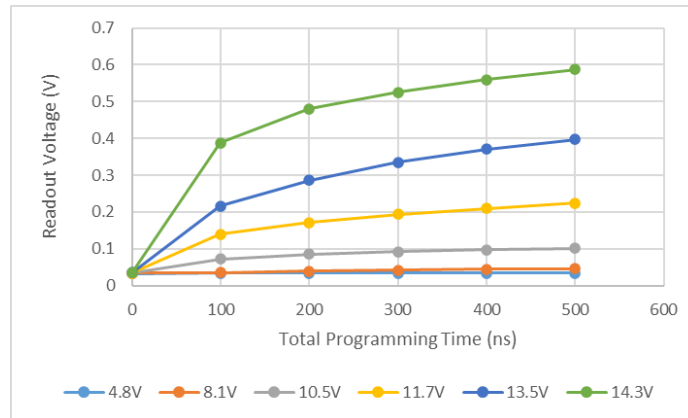
In diesem Beitrag wurden die Monitore aus den vorherigen Beiträgen automatisiert oder zum Teil auch manuell im Labor verifiziert und ausgewertet. Dabei werden die implementierten Stressmonitore, die ESD-Logger-Zellen und die Physical Unclonable Functions (PUFs) hinsichtlich ihrem Verhalten, v.a. über Temperatur und Zeit, verifiziert.

Abbildung 38 zeigt beispielhaft das Verhalten von einer implementierten Poly-Fuse als Teil eines ESD-Loggers. Wird eine bestimmte Klammerspannung überschritten wird die Sicherung (engl. Fuse) aktiviert und die Auslesespannung verändert sich. Mithilfe des DSM auf dem Testchip oder mithilfe von anderen analogen Testhilfen lässt sich diese Veränderung einfach erkennen und somit eine Spannungsüberschreitung über einem gewissen Level detektieren. Je nach Konfiguration und je nach verwendeten Elementen konnte gezeigt werden das sich alle drei implementierten Speicherzellentypen in den verschiedenen Teststrukturen sicher verwenden lassen. Dabei zeigen die Typen verschiedene Charakteristika, die Poly-Fuses lassen durch den Brennvorgang nur eine Detektion „ESD-Event Ja oder Nein“ zu.



**Abbildung 38:** Auslesespannung einer Poly-Fuse in Abhängigkeit von der Klammerspannung eines 30 V IGBT basierten ActFET.

Anders verhalten sich die beiden anderen implementierten Zelltypen. Abbildung 39 zeigt das analoge Verhalten der OTP-ESD-Logger, hier ist die analoge Readout-Spannung abhängig von der applizierten Spannung und der jeweiligen Dauer der ESD-Pulse auf dem TLP-Tester. Die Ergebnisse wurden detailliert in [13] beschrieben.



**Abbildung 39:** Auslesen eines OTP-basierten ESD-Loggers, der an einen 20 V LDMOS-basierten ActFET angeschlossen ist. Unterschiedliche Farben beziehen sich auf unterschiedliche TLP-Vorladespannungen und den daraus resultierenden Spannungsabfall über das ESD-Element.

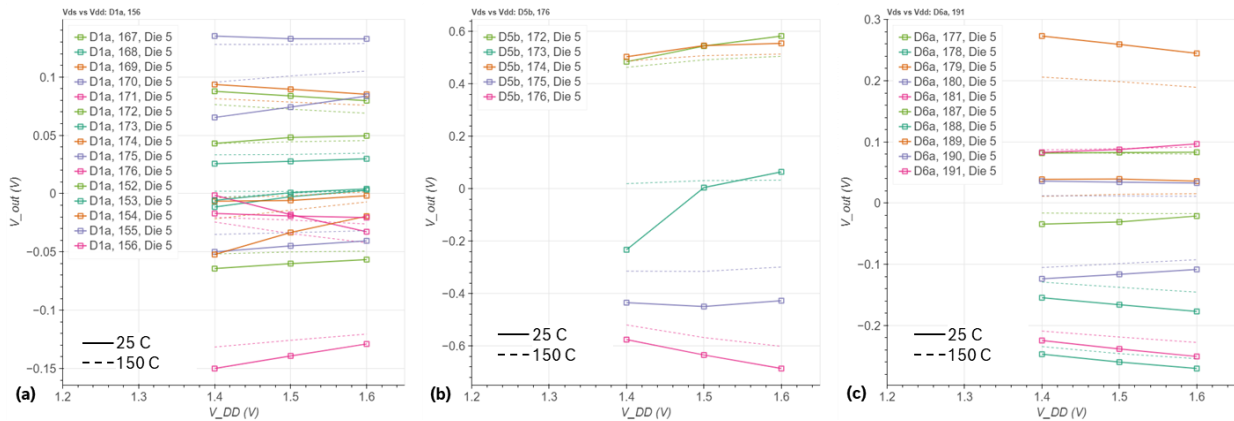
Unter Kenntnis dieses Verhaltens, und mit vielen Messungen an verschiedenen Devices, um die Reproduzierbarkeit sicherzustellen, lässt sich eine Grafik wie in Abbildung 40 erstellen. Der orange Bereich ließe sich so recht einfach eingrenzen durch Verwendung einer harten Ausfallschwelle von zum Beispiel 95mV.

Time(ns) \ V_clamp(mV)	8	8.5	9	9.5	10	10.5	11	11.5	12	12.5	13	13.5	14
0	28	29	31	34	34	34	34	34	34	34	35	35	35
50	28	29	33	38	48	61	77	95	117	142	170	200	234
100	28	30	34	42	56	74	97	124	154	189	228	271	318
150	28	30	35	45	62	84	110	141	176	217	262	312	367
200	28	31	37	48	67	90	119	153	192	236	286	341	401
250	29	31	38	51	71	96	126	163	204	252	304	363	427
300	29	32	39	54	74	101	133	171	214	264	320	381	448
350	29	32	41	56	77	105	138	178	223	275	333	396	466
400	29	32	42	58	80	109	143	184	231	285	344	410	483
450	29	33	43	60	83	112	148	190	238	293	355	423	497
500	30	33	45	62	85	115	152	195	245	302	365	435	511

**Abbildung 40:** Übersichtstabelle zur Korrelation der Auslesespannung mit der Belastungszeit und der Klemmspannung.

In den vorherigen Beiträgen wurde das Konzept für die PUF-Strukturen auf dem Testchip schon schrittweise eingeführt, zur Kompensation von Temperatureffekten der verwendeten Minimaltransistoren, werden Wheatstone-Brücken genutzt und das differentielle Signal über den Mittelabgriffen ausgewertet. Abbildung 41 zeigt für drei der neun implementierten Brücken das differentielle Ausgangssignal über der Versorgungsspannung und für zwei verschiedene Temperaturen. Klar zu erkennen ist die gewünschte Streuung der Signale, die sich mit dem 20 Bit DSM für alle Strukturen gut auflösen lässt. Je nach Devices und Verschaltung schwanken jedoch die Werte stark über den Randbedingungen wie Temperatur und Versorgungsspannung. Somit lassen sich manche nur unter bestimmten fixen Bedingungen bei einer guten Fehlerrate nutzen.

Vorteil der MOSFET Implementierung ist hingegen die kosten- bzw. flächenarme Implementierung – eine hohe Fehlerrate beim Auslesen lässt sich teilweise durch mehr Information – also mehr PUF-Strukturen – ausgleichen.



**Abbildung 41:**  $V_{out}$  vs. Versorgungsspannungs-Variationen ( $V_{DD}$ ) in einem Sample-Device (a) WS-Brücke, (b) WS-Brücke kreuzgekoppelt und (c) Stromspiegelkonfiguration.

## I.1.4 AP5 Verifikation der Vertrauenswürdigkeit

### I.1.4.1 A5.1 Gap-Analyse zum aktuellen Halbleiter-Entwicklungsprozess

In folgendem Abschnitt sind die Beiträge und Arbeitsschritte von RB in Arbeitspaket AP5, Aufgabe A5.1 aufgelistet.

#### Beitrag B5.1.9 Gap-Analyse entlang der Entwicklungen von AP1 bis AP3 aus Sicht eines Automotive Halbleiterherstellers

##### Partnerbeitragsbeschreibung

Mithilfe der Analyse der Sicherheitsanforderungen in Bezug auf on-chip Testinfrastrukturen, die in AP1 bis AP3 untersucht und implementiert werden, bewertet RB die erzielten Ergebnisse hinsichtlich des am Ende der Projektlaufzeit gültigen Standes der Technik und trägt so zur Gap-Analyse in 5.1 bei.

Das Projekt hat eine Gesamtdauer von mehreren Jahren, dadurch ist in der finalen Phase ein Abgleich der zu Beginn aufgestellten Erwartungen und der dann aktuellen Anforderungen nötig.

##### Aktuelle Arbeiten im Berichtszeitraum

Die Gap-Analyse erfolgte begleitend parallel zur Projektlaufzeit in vielen Gesprächen und im Rahmen der Abgleichtreffen mit den Partnern. Dabei wurde in der Konzeptphase auch vieles am RB-Testsystem angepasst. Die finalen Ergebnisse aus dem Labor wurden in den vorherigen Beiträgen skizziert, sie zeigen auch die Nutzbarkeit der Strukturen und des Gesamtkonzeptes auf ASIC-Ebene.

Für zukünftige Produkte sind vor allem die folgenden in VE-VIDES definierten Use-Cases relevant:

- 1) Testmode
- 2) BIST-Mode
- 3) Communication of analog signals in normal mode
- 4) Communication of health data in off-state

Lediglich der letzte Use-Case 4) mangelt aktuell konkreter Nachfrage aus den Projekten. Technisch bietet sich hier viel Potential und der Testchip zeigt die erforderliche Funktionalität – allerdings sind die meisten ASICs im Off-State „tatsächlich“ ausgeschaltet. Somit fehlt es hier

entweder an Abnehmern der Information oder die Information wird einem anderen Zustand über die anderen Use-Cases abgedeckt.

### I.1.4.2 A5.2 Definition eines vertrauenswürdigen Entwicklungsprozesses

In folgendem Abschnitt sind die Beiträge und Arbeitsschritte von RB in Arbeitspaket AP5, Aufgabe A5.2 aufgelistet.

### Beitrag B5.2.4 Erstellen einer Handlungsempfehlung zur Integration vorentwickelter on-Chip-Test-Module in Automotive ASICs

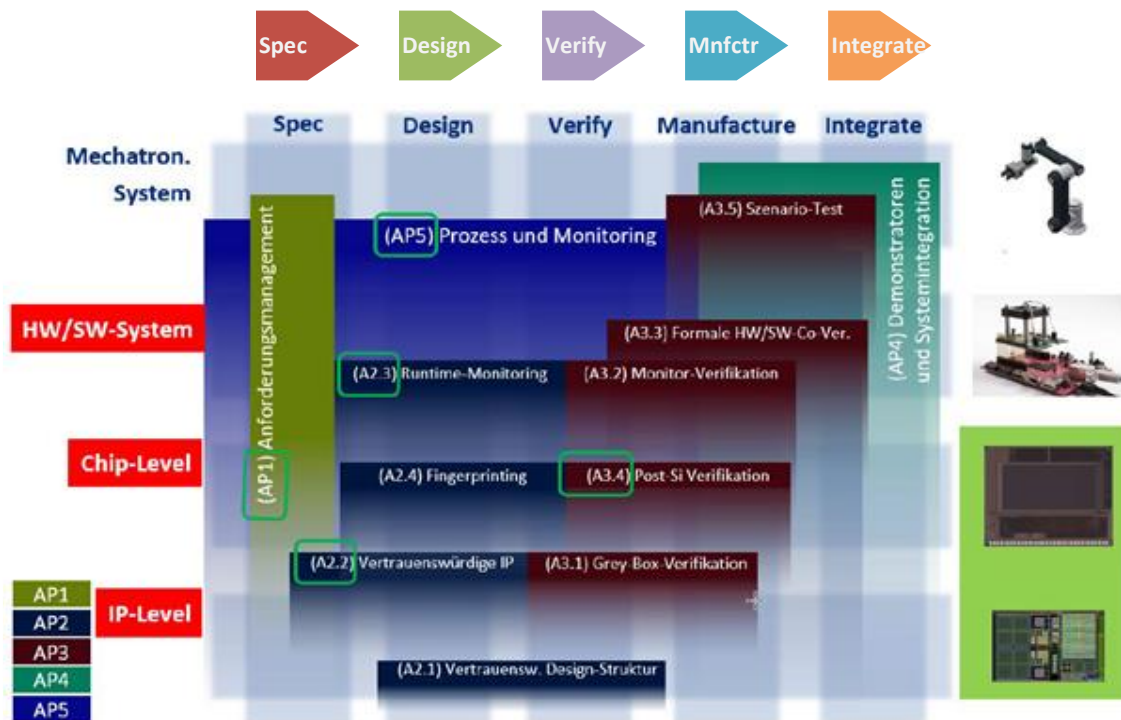
#### Partnerbeitragsbeschreibung

Anhand der Ergebnisse aus der Gap-Analyse aus AP5.1, sowie der Anforderungsanalyse und den implementierten Monitorstrukturen aus AP1 bis AP3 erstellt RB eine Handlungsempfehlung in Form eines Standard-Flows für die Entwicklung von onChip-Test-Modulen zur Integration in Automotive ASICs. Dieses beinhaltet Anforderungen (engl. Requirements), eine Konzeptübersicht, Designmodule und ggf. Layouts in der Mustertechnologie.

Die Dokumente müssen ebenfalls innerhalb der RB-Prozesse platziert werden und im RB-Management muss der Nutzen und die Notwendigkeit vermittelt und weitergetragen werden.

#### Aktuelle Arbeiten im Berichtszeitraum

Die Schaltungs-Konzepte sind vorhanden und wurden im Rahmen der vorhergehenden APs erstellt. Dieser Beitrag schließt entsprechend dem in VE-VIDES genutzten V-Diagramm zur Einordnung der Arbeitspakete die Beiträge von Bosch ab – in Abbildung 42 sind dazu die von Bosch mit bearbeiten Aufgaben farblich markiert.



**Abbildung 42:** V-Shape von VE-VIDES TVB - Arbeitspakete mit RB-Beteiligung grün markiert.

Nach Abgleich mit den erzielten Ergebnissen aus A3.4 wurde eine finale Version der Handlungsempfehlungen zusammengestellt und für zukünftige Nachfolgearbeiten bereitgestellt. Weiterhin

werden die Guideline-Dokumente und erstellten Module in die Plattformbibliotheken von RB überführt.

Einzelne Module des Testchips wurden bereits zur Projektlaufzeit von VE-VIDES in weitere Projekte übernommen, da diese einen direkten Mehrwert darin sehen und die simulative Absicherung zu diesem Zeitpunkt des Projekts hinreichend. Entsprechend erfolgte so auch ein direkter Abgleich mit den Kollegen hinsichtlich Vollständigkeit der Anforderungen etc.

Die in den ersten Arbeitspaketen erstellten Konzepte wurden für die neu erstellten Module umgesetzt und auch beispielsweise zur Bewertung der Verfügbarkeit und des Zustandes der Plattformmodule (siehe Tabelle 1) ausgerollt.

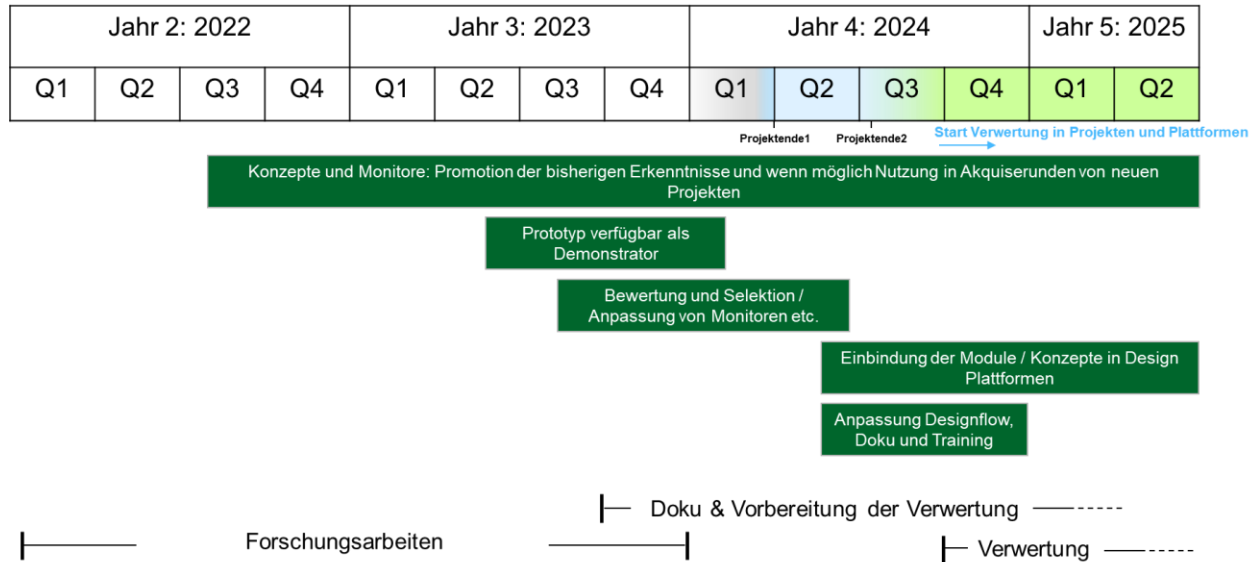
**Tabelle 1: RB Platform Maturity Levels**

1	Requirements Spec available
2	Architecture / Concept available
3	Design Specification ready
4	Design complete
5	Design Report / Verification done
6	Post-Si / Sample Verification done
7	Release of Platform module / function incl. all documentation

Zur Nutzung der neuen Module und Konzepte im Gesamt-Entwicklungs-Flow von Bosch wurden entsprechende Einstiegspunkte im Rahmen der Requirements-Engineering-Phase („Spec“ in Abbildung 42) für die Projekte formuliert. Damit lassen sich die kundenseitigen Anforderungen mit den vorhandenen Konzepten abgleichen und zu den Technologiegegebenheiten mappen, woraufhin das vollständige Konzept aus diesen Arbeiten reduziert oder auch leicht modifiziert umgesetzt werden kann.

## I.2 Fortschreibung des Verwertungsplans

Die Verwertung der Ergebnisse aus den zuvor beschriebenen Beiträgen ist in Abbildung 43 dargestellt. Aufgrund der kostenneutralen Verlängerung um 6 Monate sind das zwischenzeitliche Projektende 1 und das verzögerte Projektende 2 im Verwertungsplan dargestellt. Die Verschiebung hat keinen wesentlichen Einfluss auf die Verwertung, da die relevanten Erkenntnisse weitgehend schon zuvor verfügbar waren. Kleinere Anpassungen konnten im Anschluss adaptiert werden.



**Abbildung 43:** Verwertungsplan RB - Status und nächste Schritte

### I.2.1 Gemachte Erfindungen, vorgenommene Schutzrechts-Anmeldungen, erteilte Schutzrechte

Es wurden seit Beginn und im Rahmen des Projekts bei RB die folgenden Erfindungsmeldungen gemacht:

Titel	Status
Verfahren zur Detektion von elektrostatischen Entladungen (ESD) sowie der Speicherung von analogen Kenngrößen in digitalen Speicherzellen	Angemeldet
Verfahren zur Detektion von elektrostatischen Entladungen und deren zeit-abhängigen Analyse	Angemeldet
Method for online fault detection in differential read-out applications	Angemeldet

### I.2.2 Wirtschaftliche Erfolgsaussichten

Durch die in VE-VIDES entstehenden Ergebnisse bestehend aus Hardware-IP, HW/SW-Co-Verifikationsverfahren und Methoden zur Identifizierung von Elektronikkomponenten wird es für RB möglich, hocheffiziente Sensoren, ASICs und SoCs mit höchster Sicherheit für automatisiertes Fahren zu geringen Kosten und damit wirtschaftlich wettbewerbsfähig zu entwickeln.

Hiermit können elektronische Komponenten entwickelt werden, die smart und sicher aber gleichzeitig auch günstig und energieeffizient sind. Durch neue Möglichkeiten, maßgeschneiderte, konfigurierbare Komponenten mit hoher Energieeffizienz und Fehlerabdeckung zu entwickeln, wird die Grundlage für vertrauenswürdige elektronische Komponenten verschiedenster Applikationen geschaffen. Dies wird verschiedenen Halbleiterprodukten für die Automobilindustrie zugutekommen. Diese sind z.B. Sensor-ASICs für sicherheitskritische Anwendungen wie ABS oder ESP, System-Basis-ASICs für das Power-Management von Steuergeräten oder auch Power-ASICs für

die Ansteuerung elektrischer Fahrzeugkomponenten. Auf diese Weise werden RB-Produkte, welche sich bereits heute durch höchste Qualität in Bezug auf die Themen Funktionalität und Sicherheit gekennzeichnet sind, auch bei zukünftig immer stärker steigenden Anforderungen bzgl. Komplexität und Kosten höchsten Ansprüchen entsprechen.

Die Ergebnisse und die Ziele des Teilvorhabens wurden mit diversen Kontakten innerhalb RB geteilt und stießen dort auf ein breites Interesse. Module, die im Rahmen des Testchip CO110 verbessert oder erstellt wurden, sind aktuell teilweise schon in neu gestarteten Projekten im Einsatz oder Teil des Konzepts.

### **I.2.3 Wissenschaftliche und/oder technische Erfolgsaussichten**

Verschiedene Entwicklungsabteilungen des Geschäftsbereichs „Mobility Electronics“ an dem Standort Reutlingen waren in diesem Projekt aktiv beteiligt. Dadurch wird sichergestellt, dass aktuelle und zukünftige Anforderungen an Automotive ASICs mit hohe Sicherheitsanforderungen schnell und wirkungsvoll in die Entwicklungsmethoden in VE-VIDES eingehen. Auf diese Weise können Aufbau und Bewertung der Designmethoden im Kontext aktueller und relevanter Fragestellungen im Bereich der Vertrauenswürdigkeit erfolgen. Durch diese breite Beteiligung wird ein effektiver Transfer der Projektergebnisse in den industriellen Entwurfsablauf der Entwicklung bei RB sowie entlang der Lieferkette bis zur Entwicklung bei den jeweiligen Kunden bestmöglich vorbereitet, dessen Abschluss innerhalb eines Zeitraums von zwei Jahren nach Projektende angestrebt wird.

Wie bei den wirtschaftlichen Erfolgsaussichten wurden auch hier die Ergebnisse und die Ziele des Teilvorhabens mit diversen technischen Experten innerhalb RB geteilt und stießen dort auf ein breites Interesse. Ebenfalls erreichten uns Rückfragen von RB-Kundenteams zu den Ergebnissen, da sie von ihren jeweiligen Kunden darauf angesprochen wurden. Erste Module aus dem Testchip wurden als sinnvoll identifiziert und mit einem gewissen Pull-Effekt aus VE-VIDES in Projekte übernommen.

### **I.2.4 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit**

Die Forschungsergebnisse von VE-VIDES bilden die notwendige Voraussetzung für den Aufbau hoch-verfügbare Sensoren und ASICs. Dabei können bis zum Ende der Projektlaufzeit wichtige Ergebnisse erzielt, jedoch nicht alle Aspekte erschöpfend behandelt werden. Die erzielten Forschungsergebnisse liefern dafür die Grundlage für weitere Forschungsarbeiten und interne Entwicklungen, die in den darauffolgenden zwei bis vier Jahren bearbeitet werden. So werden mit dem Projekt die erhöhte Testbarkeit der bisher nicht testbaren Zustände durch einheitliche cross-domain Schnittstellen und optimierte Ansteuer- und Auswerteschaltungen für on-chip Monitore bei gleichzeitig wenig Hardware-Aufwand und niedriger Test-Zeit adressiert. Nach Projektende gilt es, dies in unterschiedlichen Gesichtspunkten auszubauen, um damit zukünftige komplexere System für ADAS-Anwendungen zu unterstützen, die mehr Sicherheit anfordern. Der erste Zielmarkt für die Anwendung der Ergebnisse dieses Projekts ist das Power Management für Automobilanwendungen mit einem Umsatz von rund zwei Milliarden USD im Jahr 2024 und einer jährlichen Wachstumsrate von 4,3% [5].

Im Zuge des Projektes entwickeln sich bei BOSCH diverse verwandte Aktivitäten, so werden parallel die Kompetenzen bzgl. Design-for-Test (DfT) erweitert und Plattformkonzepte für andere Effizienzthemen erarbeitet. Hierzu finden kontinuierlich Abstimmungen statt um die Anschlussfähigkeit in mehreren Dimensionen sicherzustellen. Im Rahmen von VE-VIDES wurden weiterhin mögliche wissenschaftlichen Anschluss Themen diskutiert, beispielsweise die Verknüpfung von künstlicher Intelligenz mit Daten aus den hier erstellten Monitorstrukturen.

### I.3 Literaturverzeichnis

- [1] R. Reis, M. Lubaszewski, J. Jess, "Design of Systems on a Chip: Design and Test," Book, Springer, 2007
- [2] M. Beckert, et. al., "Delta-Sigma-Datenkonverter-Anordnung und Verfahren zum Überprüfen eines Delta-Sigma-Datenkonverters", Patent, Robert Bosch GmbH, 2006
- [3] M. Agarwal; B. C. Paul; M. Zhang; S. Mitra, "Circuit Failure Prediction and Its Application to Transistor Aging," 25th IEEE VLSI Test Symposium (VTS'07), 2007
- [4] F. Firouzi; F. Ye; A. Vijayan; A. Koneru; K. Chakrabarty; M. B. Tahoori "Re-using BIST for Circuit Aging Monitoring," 20th IEEE European Test Symposium (ETS), 2015
- [5] Yole Market and Technology Report 2019
- [6] International Organization for Standardization. ISO 26262 & ISO 21434 (Draft). <https://www.iso.org>
- [7] S. Bhunia, M. Tehranipoor. "The Hardware Trojan War: Attacks, Myths, and Defenses." Springer Verlag, 2018.
- [8] K. Xiao et. al., "Hardware Trojans: Lessons Learned after one Decade of Research." TODAES 2016. <https://doi.org/10.1145/2906147>
- [9] IEEE 1149.1-2013 - IEEE Standard for Test Access Port and Boundary-Scan Architecture; [https://standards.ieee.org/standard/1149\\_1-2013.html](https://standards.ieee.org/standard/1149_1-2013.html)
- [10] BQ79606A-Q1, Datasheet: <https://www.ti.com/product/BQ79606A-Q1>
- [11] MC33771A, Datasheet: [https://www.nxp.com/docs/en/data-sheet/MC33771B\\_SDS.pdf](https://www.nxp.com/docs/en/data-sheet/MC33771B_SDS.pdf)
- [12] R. F. H. Fischer and S. Müelich, "A New Helper Data Scheme for Soft-Decision Decoding of Binary Physical Unclonable Functions," in IEEE Access, vol. 10, pp. 12644-12653, doi: 10.1109/ACCESS.2022.3146989.sss, 2022

### I.4 Veröffentlichungen

- [13] G. Bracher et al, "On-Chip ESD Monitors," ESD Forum 2024 Conference Proceeding, 2024 [In Review process]
- [14] N. Klefe et al., "Overcoming Impedance-Mismatch Induced Offsets in Background Bond Wire Defect Detection," IEEE International Symposium on Circuits and Systems (ISCAS), 2024