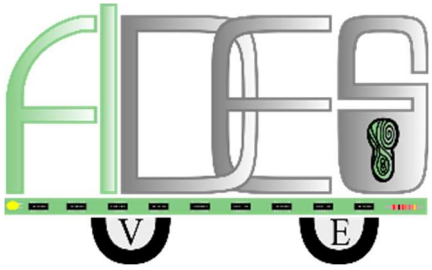
Schlussbericht

BMBF-Verbundprojekt VE-FIDES:
Verbundprojekt: Knowhow-Schutz und Identifizierbarkeit
von Elektronikkomponenten für vertrauenswürdige Produktionsketten



Zuwendungsempfänger	**Continental Automotive Technologies GmbH**
Vorhabenbezeichnung	Verbundprojekt: Knowhow-Schutz und Identifizierbarkeit von Elektronikkomponenten für vetrauenswürdige Produktionsketten – VE-FIDES –
Förderkennzeichen	16ME0259
Projektlaufzeit	01.03.2021 – 31.12.2024
Berichtszeitraum	01.03.2021 – 31.12.2024
Fälligkeit	30.06.2025
Erstelldatum	06.06.2025
[redacted]	

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

[redacted]

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

Inhaltsverzeichnis

Abkürzungen/Erläuterungen 4
1 Teil 1 Kurzbericht 5
1.1 Ursprüngliche Aufgabenstellung sowie den wissenschaftlichen und technischen Stand, an den angeknüpft wurde 5
1.2 Ablauf des Vorhabens 5
1.3 Die wesentlichen Ergebnisse sowie ggf. die Zusammenarbeit mit anderen Forschungseinrichtungen 5
1.3.1 AP1.2a: 5
1.3.2 AP1.2b: 5
1.3.3 AP1.2C: 5
1.4 Auszug aus Abschlusspräsentation 6
2 Teil 2 Eingehende Darstellung 7
2.1 AP1 Wissenschaftlich-technische Ergebnisse 7
2.1.1 Berichtszeitraum 01.03.2021 – 31.12.2021 AP1.a 7
2.1.2 Berichtszeitraum 01.03.2022 – 31.12.2022 AP1.2b 7
2.1.3 Berichtszeitraum 01.03.2024 – 31.12.2024 AP1.2c 8
2.2 Mitarbeit an den Arbeitspaketten AP2, AP3, AP4 9
2.3 Andere wesentliche Ereignisse 9
2.4 Wichtigsten Positionen des zahlenmäßigen Nachweises 9

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

[redacted]

Abkürzungen/Erläuterungen

Abkürzung	Erläuterung
ASIC	**a**pplication-**s**pecific **i**ntegrated **c**ircuit, anwendungsspezifische integrierte Schaltung
API	application programming interface
CES	Continental Engineering Service GmbH
HSM	Hardware Security Module
POK	Physical Obfuscated Keys (Cornell University) Physical Obfuscated Keys (POKs) ermöglichen die manipulationssichere Speicherung von zufälligen Schlüsseln, die auf physischer Unordnung basieren. Die Ausgangsbits aktueller POK-Designs müssen zuerst aufgrund von Messrauschen korrigiert und dann dekorreliert werden, da die ursprünglichen Ausgangsbits möglicherweise nicht i.i.d. (unabhängig und identisch verteilt) sind und auch öffentliche Hilfsinformationen zur Fehlerkorrektur notwendigerweise die korrigierte Ausgabe dieser http-URL korrelieren, aus diesem Grund enthalten aktuelle Designs eine Schnittstelle zur Fehlerkorrektur und/oder Ausgabeverstärkung, und Privacy Amplification zur Komprimierung der korrigierten Ausgabe in eine einheitliche zufällige Bitzeichenfolge.
PUF	Physical unclonable Function **(Wikipedia)** **Physical unclonable functions** (auch Physically unclonable functions) oder kurz PUF sind Hardwarestrukturen in einem Halbleiter, die dazu dienen, eine eindeutige Identifikation des Halbleiters zu ermöglichen oder Schlüssel für kryptografische Verfahren zu sichern. Halbleiter können komplette elektronische Chipkarten oder Mikroprozessoren sein, insbesondere solche mit Hardware Security Module für kryptografische Aufgaben. Wie ein Fingerabdruck ist die PUF ein individuelles Merkmal, welches an ein physikalisches Objekt gebunden ist. Die PUF basieren darauf, dass durch kleinste Schwankungen im Produktionsprozess bestimmte Baugruppen ein individuelles Verhalten zeigen, obwohl durch das Produktionsverfahren absolut gleiche Teile entstehen sollten. Systeme mit einer PUF-Einheit werden daher alle im absolut gleichen Produktionsprozess hergestellt und erfahren – zumindest im Hinblick auf die PUF – keinerlei individuelle Bearbeitung.
SIP	System in Package, Beispiel zwei ICs in einem Gehäuse und Mold Compound
Tachographen-System	Ein System zur Erfassung der Lenk-und Ruhezeiten von Fahrern von Nutzfahrzeugen bestehend aus dem digitalen Tachograph, den Tachographen Karten und dem Geschwindigkeitsgeber. Weitere Erläuterungen im LRZ Sharepoint: Tachograph_Präsentation_VE-FIDES Meeting_20210622 und Tachograph – Wikipedia
Geschwindigkeits-geber	Teil des Tachographen-System zur Erfassung der Geschwindigkeitssignale des Nutzfahrzeuges.

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

1 Teil 1 Kurzbericht

1.1 Ursprüngliche Aufgabenstellung sowie den wissenschaftlichen und technischen Stand, an den angeknüpft wurde

Generierung von Fingerabdrücken aufgrund eindeutiger Eigenschaften von Leiterplatten und darauf verbauter Komponenten am Beispiel des Conti Tachographen-Systems.

1.2 Ablauf des Vorhabens

- AP1.2.a: Erstellung der Sicherheitsanforderungen am Beispiel des Tachographen-Systems in Bezug auf Produktsicherheit und Produktion
- AP1.2.b: Bewertung der Lösungskonzepte aus AP1.1 über die Absicherung der Lieferkette zur Erfüllung der Sicherheitsanforderungen des Tachographen-System
- AP1.2 c: Technische und ökonomische Evaluation der technischen Lösungen aus AP2-AP4 zur Erfüllung der Anforderungen des Tachographen-Systems sowie Abgleich der Anforderungen aus AP1.1-AP1.2 und der Lösungen aus AP2-AP4 mit verfügbaren Standards und Identifikation von Ergänzungsmöglichkeiten der Standards OnBoard Messung von Leiterplatten- und Komponenten Fingerprints.

1.3 Die wesentlichen Ergebnisse sowie ggf. die Zusammenarbeit mit anderen Forschungseinrichtungen

1.3.1 AP1.2a:

FIDES_AP1_2a_Erstellung_Sicherheitsanforderungen_05_endgültig_20211017.pdf:
Sicherheitszertifizierung nach Common Criteria mit dem Assurance Level EAL 4+
Umwelttests_Getriebesensoren.pdf: Anforderungen zur Erfüllung der gesetzlich und kundenseitigen Umweltanforderungen

1.3.2 AP1.2b:

FIDES_AP1_2b_Bewertung_AP1_1_02.pdf:
Continental hat die Ergebnisse des AP1.1 von Siemens überprüft: Der Aufwand ein PUF zu implementieren ist zu hoch, zur Absicherung der Lieferkette sind in unserem Anwendungsfall organisatorische Maßnahmen aktuell ausreichend.

1.3.3 AP1.2C:

FIDES_AP1.2C_Bewertung_02.pdf:
Eine Identifizierung von HALL ICs, Komponenten, Leiterplatten im Tachographen-System ist aus unterschiedlichsten Gründen in naher Zukunft (2 - 4 Jahre) noch nicht umsetzbar. Die Verwendung der GTA API (application programming interface) ist für zukünftigen Tachographen Release zur Vereinfachung der SW Reuseability eine sehr gute Verbesserungsmöglichkeit.

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

1.4 Auszug aus Abschlusspräsentation

Ziel
Generierung von Fingerabdrücken aufgrund eindeutiger Eigenschaften von Leiterplatten und darauf verbauter Komponenten am Beispiel des Conti Tachographen-Systems

Teilarbeitspakete

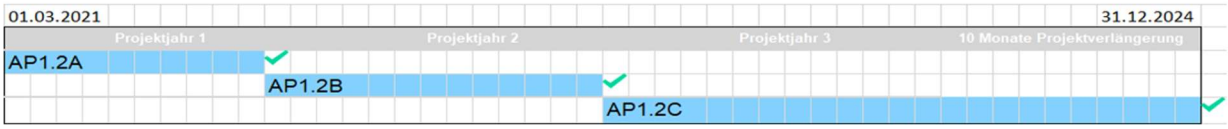
- AP1.2.a: Erstellung der Sicherheitsanforderungen am Beispiel des Tachographen-Systems in Bezug auf Produktsicherheit und Produktion
- AP1.2.b: Bewertung der Lösungskonzepte aus AP1.1 über die Absicherung der Lieferkette zur Erfüllung der Sicherheitsanforderungen des Tachographen-System
- AP1.2 c: Technische und ökonomische Evaluation der technischen Lösungen aus AP2-AP4 zur Erfüllung der Anforderungen des Tachographen-Systems sowie Abgleich der Anforderungen aus AP1.1-AP1.2 und der Lösungen aus AP2-AP4 mit verfügbaren Standards und Identifikation von Ergänzungsmöglichkeiten der Standards OnBoard Messung von Leiterplatten- und Komponenten Fingerprints.

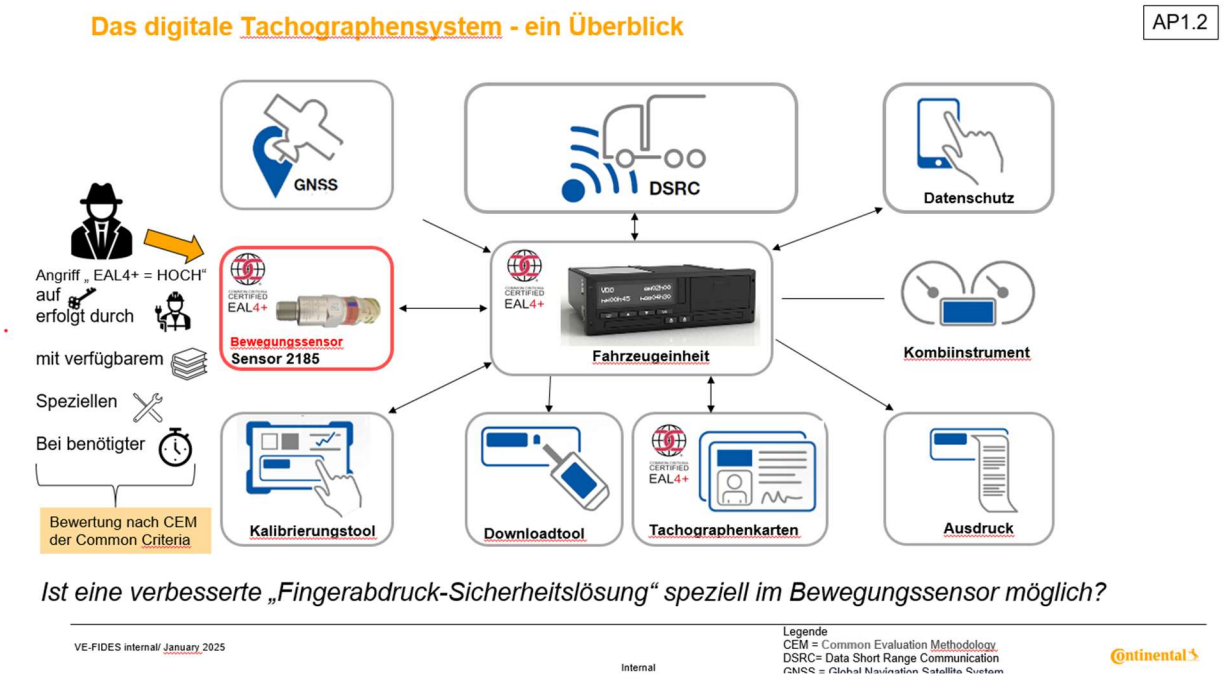
Ergebnisse

AP1.2a: FIDES_AP1_2a_Erstellung_Sicherheitsanforderungen_05_endgültig_20211017.pdf:
Sicherheitszertifizierung nach Common Criteria mit dem Assurance Level EAL 4+
Umwelttests_Getriebesensoren.pdf: Anforderungen zur Erfüllung der gesetzlich und kundenseitigen Umweltanforderungen

AP1.2b: FIDES_AP1_2b_Bewertung_AP1_1_02.pdf:
Continental hat die Ergebnisse des AP1.1 von Siemens überprüft: Der Aufwand ein PUF zu implementieren ist zu hoch, zur Absicherung der Lieferkette sind in unserem Anwendungsfall organisatorische Maßnahmen aktuell ausreichend.

AP1.2C: FIDES_AP1.2C_Bewertung_02.pdf:
Eine Identifizierung von HALL ICs, Komponenten, Leiterplatten im Tachographen-System ist aus unterschiedlichsten Gründen in naher Zukunft (2..4 Jahre) noch nicht umsetzbar. Die Verwendung der GTA API ist für zukünftigen Tachographen Release zur Vereinfachung der SW Reuseability eine sehr gute Verbesserungsmöglichkeit.





The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

2 Teil 2 Eingehende Darstellung

2.1 AP1 Wissenschaftlich-technische Ergebnisse

Die Aufzählung der Ergebnisse orientiert sich an den Themenbereichen der Vorhabenbeschreibung. Der oben genannte Zuwendungsempfänger führte die folgenden Arbeiten im Berichtszeitraum durch:

Die Arbeiten im Zusammenhang mit IT Security/Sicherheitsanforderungen wurden in Zusammenarbeit mit den Kollegen der Continental Engineering Service GmbH erstellt.

2.1.1 Berichtszeitraum 01.03.2021 – 31.12.2021 AP1.a

AP1.2.a: Erstellung der Sicherheitsanforderungen am Beispiel des Tachographen-Systems in Bezug auf Produktsicherheit und Produktion

Das Dokument mit dem „**FIDES_AP1_2a_Erstellung_Sicherheitsanforderungen_05_endg.pdf**“ Sicherheitsanforderungen wurde seitens Continental erstellt und nach Review im LRZ Sharepoint abgelegt.

https://syncandshare.lrz.de/open/MktZYnJxQlRZQlM1d2tua2lnQnJ4/AP1/AP1.2/AP1.2a/FIDES_AP1_2a_Erstellung_Sicherheitsanforderungen_05_endg%C3%BCltig_20211017.pdf

Zusammenfassung

Ziel dieses Dokumentes ist es, die Sicherheitsanforderungen am Beispiel des Tachographen-Systems in Bezug auf Produktsicherheit und Produktion zu erstellen. Insbesondere am Beispiel des Sensor 2185 (Getriebesensor innerhalb des Tachographensystem) sollen die hardwareseitigen Anforderungen im FIDES Projekt erarbeitet werden, so dass diese sowohl in einer Sicherheitszertifizierung nach Common Criteria mit dem Assurance Level EAL 4+ erfolgreich zertifiziert werden können, als auch den gesetzlich und kundenseitigen Umweltanforderungen entsprechen. Aktuell ist der Gehäuseschutz beim Sensor 2185 der Schwachpunkt in der Sicherheitszertifizierung nach Common Criteria. Und so liegt die Motivation der Continental sich an dem FIDES Projekt zu beteiligen darin, die Ergebnisse aus der Studie für die Verbesserung des Gehäuseschutzes beim Sensor 2185 zu verwenden

Zur Ergänzung des Gesamtbildes wurden die folgenden Dokumente durch die CES und Continental Villingen erstellt und im LRZ Sharepoint abgelegt:

- „**Überblick über Automotive Security Regularien**“ https://syncandshare.lrz.de/open/MktZYnJxQlRZQlM1d2tua2lnQnJ4/AP1/AP1.2/AP1.2a/FIDES_AP1_2a_Automotive_Security_Regularien.pdf

- „**Umwelttests_Getriebesensoren**“ mit den spezifischen Automotive Umweltanforderungen https://syncandshare.lrz.de/open/MktZYnJxQlRZQlM1d2tua2lnQnJ4/AP1/AP1.2/AP1.2a/Umwelttests_Getriebesensoren.pdf

2.1.2 Berichtszeitraum 01.03.2022 – 31.12.2022 AP1.2b

AP1.2.b: Bewertung der Lösungskonzepte aus AP1.1 über die Absicherung der Lieferkette zur Erfüllung der Sicherheitsanforderungen des Tachographen-Systems.

Die Bewertung der Lösungskonzepte „**FIDES_AP1_2b_Bewertung_AP1_1_01.docx**“ wurde seitens Continental erstellt und nach Review im LRZ Sharepoint abgelegt.

https://syncandshare.lrz.de/open/MktZYnJxQlRZQlM1d2tua2lnQnJ4/AP1/AP1.2/AP1.2b/FIDES_AP1_2b_Bewertung_AP1_1_01.docx

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

[redacted]

Zusammenfassung

Continental hat die Aufgabenstellung innerhalb dieses Dokumentes mit den folgenden Kapiteln bearbeitet:

- Beschreibung der angewandten Lösungen im Tachographen System
- Betrachtung Zulieferung von Komponenten zur Produktion des Tachographen Systems
- Betrachtung Lieferung Tachographen System an die OEMs
- Zusammenfassung

Continental hat dabei die Ergebnisse des AP1.1 von Siemens „01-20220929-Meilensteintreffen_Enhancing_Trustworthiness_of_an_Industrial_Device-Siemens.pptx“ für die Fälle

- Zulieferung von Komponenten zur Produktion des Tachographen Systems,
- Lieferung des Tachographen System an die OEMs, Getriebehersteller, authorisierte Werkstätten

überprüft und sieht im Moment keine Notwendigkeit diese beiden Fälle durch eine Absicherung mittels PUF zu ergänzen.

2.1.3 Berichtszeitraum 01.03.2024 – 31.12.2024 AP1.2c

Im Arbeitspaket AP1.2c wurden die Rückmeldungen der AP2 - AP4 in Zusammenarbeit mit der CES gesammelt, bewertet und nach Review im Dokument FIDES_AP1.2C_Bewertung_02.pdf dokumentiert und im LRZ Sharepoint abgelegt.

https://syncandshare.lrz.de/open/MktZYnJxQlRZQlM1d2tua2lnQnJ4/AP1/AP1.2/AP1.2C/FIDES_AP1.2C_Bewertung_02.pdf

Fazit

Der ursprüngliche Ansatz von Conti, eine eindeutige Identifikation/Authentisierung eines analogen HALL ICs mittels einem Fingerprint durchzuführen, konnte nicht umgesetzt werden. Der Grund ist die sogenannte Offset Compensation für die Magnetfeldmessung bei dem für unsere Geschwindigkeitsgeber für das Tachographen-System verwendeten HALL IC (wird benötigt aufgrund der Reduktion der Fertigungsstreuung durch den Hersteller).

Bei Verwendung eines digitalen HALL ICs (Steuerbarkeit der Offset Compensation) muss auch das digitale Interface geschützt werden, was im Augenblick von den im Markt befindlichen HALL ICs nicht angeboten wird und auch nicht als zukünftige Funktion von den HALL IC Suppliern angedacht wird.

Aus unserer Sicht wäre die Verwendung eines PUFs bei gleichzeitiger Verwendung eines gesicherten digitalen Interfaces nicht mehr notwendig.

Eine mögliche Alternative wäre die Entwicklung eines HALL IC mit integrierter Sicherheitsfunktionen auch unter der Betrachtung der Anwendung der PUF Möglichkeiten oder der Detektion von Gehäuseverspannungen zur Öffungserkennung des Hall-IC Gehäuses.

Mögliche langfristige Anwendungen der in VE-FIDES gestarteten Entwicklungen für unser Tachographen-System:

- Mess ASIC: Eine zukünftige Anwendung in unserem Tachographen-System kann erst nach Verfügbarkeit des Messverfahrens / Algorithmus überprüft werden.

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

- RISC-V (Secure Element, Open Titan): Abhängig vom Nachweis der Vertraulichkeit durch entsprechende Zertifizierung und der Erfüllung der automotive Anforderungen wäre eine Anwendung in zukünftigen Tachographen-Systemen denkbar.
- GTA API: In zukünftigen Tachographen Release zur Vereinfachung der SW Reuseability angedacht.
- Die Integration eines PUFs in einem Standard Applikation Prozessor (in einem integrierten HSM) wäre aus unserer Sicht technisch machbar aber nicht sinnvoll solange die Software im Standard Applikation Prozessor nicht gegen Manipulationen/Veränderungen geschützt werden kann

Wichtig für Conti ist der notwendige formale Nachweis der Wirksamkeit der Implementierung für die Sicherheitsevaluierung unserer Produkte.

Aufgrund der 2 jährlichen Re-Zertifizierung und damit mit dem ständigen Druck zur Verbesserung der Product Cybersecurity in unseren Produkten, beschäftigen wir uns ständig mit möglichen Lösungen / Verbesserungen der Product Cybersecurity für unser Tachographen-System.

2.2 Mitarbeit an den Arbeitspaketten AP2, AP3, AP4

Die Aufzählung der Ergebnisse orientiert sich an den Themenbereichen der Vorhabenbeschreibung. Der oben genannte Zuwendungsempfänger war an folgenden Themenbereichen beteiligt:

Innerhalb des AP2 waren seitens Continental keine Aktivitäten geplant.

Innerhalb des AP3 insbesondere im AP3.3 „Vermessung von Sensor- Mikrocontroller Kombinationen“ fand ein intensiver Austausch über die Projektlaufzeit zwischen Continental Villingen zusammen mit CES und der TUM, die dieses AP umsetzt.

Innerhalb des AP4 verfolgte Continental die Diskusion über Inhalt und Aufbau des Demonstrators.

2.3 Andere wesentliche Ereignisse

Innerhalb des AP1 wurden Abstimmungsrunden durch Continental durchgeführt.

Die Protokolle sind im LRZ Sharepoint abgelegt.

An den regelmässigen Abstimmungsrunden für die weiteren APs hat das Team von Continental teilgenommen.

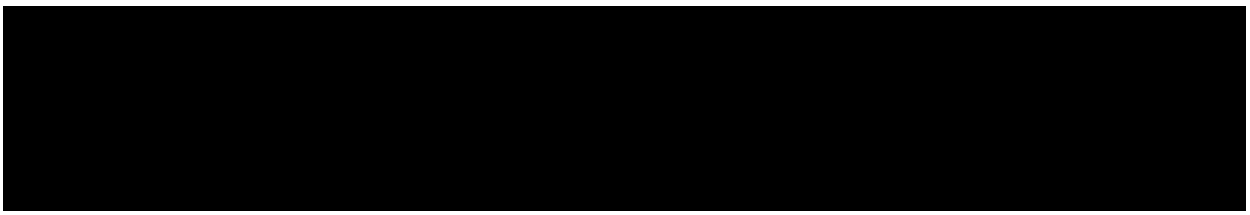
Highlights waren die Teilnahme an den FIDES Meilensteintreffen mit dem damit verbundenen persönlichen Austausch, Networking.

2.4 Wichtigsten Positionen des zahlenmäßigen Nachweises

Die Kosten- und Zeitplanung wurde durch die vielen Veränderungen und angepassten Anforderungen während der Projektlaufzeit nicht eingehalten und es sind deutlich weniger Kosten angefallen und Fördermittel abgerufen worden als in der Antragskalkulation geplant. Insgesamt sind nur 41,26% der geplanten Gesamtkosten angefallen.

Die größte Abweichung ist bei der Kostenposition 0813 Material, wo 3,29% der geplanten Kosten angefallen sind. Wie im Kapitel 2.1.3 Fazit beschrieben, konnte der für Continental interessante Ansatz zur Identifikation von analogen HALL ICs aufgrund der Offset Compensation von der TUM nicht weiterverfolgt werden. Damit war es nicht sinnvoll angedachte Musteraufbauten (Erstellung Musterlayout, Produktion Leiterplatten, Bestückung der Leiterplatten) zu erstellen.

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.



In der Kostenposition 0837 Reisekosten sind Kosten in Höhe von [redacted] angefallen, was eine Ausschöpfung der geplanten Kosten von 8,87% bedeutet. Hier sind die Auswirkungen der Corona-Pandemie auf die Arbeitswelt spürbar, da das Projekt größtenteils während dieser Zeit lief. Dadurch waren nur wenige Dienstreisen und Vor-Ort-Treffen innerhalb des Konsortiums möglich.

Die beiden größten Kostenpositionen im Projekt waren die Position 0823 FE-Fremdleistungen und die Position 0837 Personalkosten. In der Kostenposition 0823 FE-Fremdleistungen sind während der Projektlaufzeit Kosten in Höhe von [redacted] angefallen, was eine Ausschöpfung der beantragten Kosten in Höhe von 50,69% entspricht. Die Fremdleistungen waren zur Unterstützung der Entwicklung für allgemeine IT Security Themen und im speziellen für die Entwicklung von Security Algorithmen (in Zusammenarbeit mit TUM) für die Identifikation der analogen Hall ICs in der Applikationsschaltung vorgesehen. Die Entwicklung von speziellen Security Algorithmen konnten, siehe oben, nicht durchgeführt werden konnte.

In der Kostenposition 0837 Personalkosten sind Kosten in Höhe von [redacted] angefallen und damit eine Beanspruchung der geplanten Kosten von 35,62%. Die geringe Ausschöpfung der Personalkosten beruht ebenfalls auf der im Kapitel 2.1.3 im Fazit beschriebenen nicht Durchführbarkeit der Identifikation von analogen HALL ICs.

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

[redacted]