WACHENDORFF
The Encoder Experts

Sachbericht zum Verwendungsnachweis

Teil I: Kurzbericht

Verbundprojekt:	Elektronischer Knowhow-Schutz für innovative Sensorsysteme - VE-ARiS -
Teilprojekt:	Abwehr von Reverse-Engineering auf Board Ebene
Förderprogramm:	Vertrauenswürdige Elektronik
Förderkennzeichen:	16ME0241
Durchgeführt von:	Wachendorff Automation GmbH & Co. KG Industriestr. 7 65366 Geisenheim
Projektlaufzeit:	01.03.2021 – 31.12.2024
Projektleiter:	Mathias Armbruster

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen 16ME0241 gefördert.

Die Verantwortung für den Inhalt der Veröffentlichung trägt der Autor.

Autor(en):

Mathias Armbruster, Wachendorff Automation GmbH & Co. KG

1. Ursprüngliche Aufgabenstellung

Das Gesamtziel des Vorhabens bestand in der Entwicklung einer Abwehr von Reverse Engineering für Mixed-Signal Sensor-ICs, d. h. hochintegrierte Sensorsysteme und SoC-ICs (System-on-Chip).

Der Zuwendungsempfänger Wachendorff hat dabei die Abwehr bzw. den Knowhow-Schutz auf Board-Ebene erforscht. Hierbei wurden Wasserzeichen verwendet, welche als integrierte und personalisierte Schutzfunktionen durch einen zusätzlichen Abwehr-IC zur Aktivierung durch den Sensorsystem-Hersteller verwendet werden.

Das Teilvorhaben bezog sich auf die Bekanntmachung "Vertrauenswürdige Elektronik (ZEUS)" des BMBF vom 16.03.2020. Das Teilvorhaben adressierte mit neuartigen Abwehr-Techniken auf Board-Ebene die folgenden Schwerpunkte der Bekanntmachung:

Design: Im Projekt wurden neuartige Designmethoden (Tarnung) entwickelt, welche eine Fälschung von sicherheitsrelevanten Elektroniksystemen verhindern. Weiter wurden aktive Abwehrtechniken auf Board-Ebene entwickelt, welche die Verifikation der Vertrauenswürdigkeit bzw. der Originalität ermöglichen.

Fertigung: Im Projekt wurden neue Methoden der Systemintegration untersucht: Auf Board-Ebene erlaubt dabei ein eigener Abwehr-IC den Schutz vor Nachbau und Manipulation als wettbewerbsrelevante IPs. Die Lösung durch einen speziellen VE-ARiS IC erlaubt dabei eine breite Nutzung auf Mixed-Signal Sensor-ICs.

Analytik-, Test-, Mess- und Prüfmethoden: Durch die Verifizierung der Echtheit mittels Wasserzeichen können erstmals unerwünschte Funktionen und Manipulationen erkannt werden. Die aktive Abwehr basiert dabei auf hardwarebasierten prozessspezifischen Funktionen und ermöglicht die eindeutige Identifizierung von vertrauenswürdigen Elektronikkomponenten.

2. Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Reverse Engineering[1] von ICs wurde entweder zerstörungsfrei oder zerstörend durchgeführt. Die Röntgentomographie ist eine zerstörungsfreie Reverse Engineering Methode, die schichtweise Bilder von Chips liefert und häufig für die Analyse von internen Durchkontaktierungen, Leiterbahnen, Drahtbonden, Kondensatoren, Kontakten oder Widerständen verwendet wird. Die zerstörende Analyse hingegen besteht darin, das IC

[1] Tehranipoor, Mark Mohammad, Ujjwal Guin, and Domenic Forte. "Counterfeit integrated circuits." *Counterfeit Integrated Circuits*. Springer, Cham, 2015. 15-36.

schichtweise wegzuätzen oder zu schleifen (Delayering). Von jeder Schicht wird dann mittels Raster- oder Transmissionselektronenmikroskopie ein Bild aufgenommen. Mittlerweile wird das Reverse Engineering mittels automatisierter Tools oder sogar kommerzieller Anbieter durchgeführt, so dass die Hürden für Produktpiraterie sinken. In der Vergangenheit wurden bereits verschiedene Abwehr-Mechanismen in der Wissenschaft untersucht[2]:

Board-Ebene: Die Gewährleistung eines vollständigen Schutzes vor Reverse Engineering auf PCB-Ebene ist eine schwierige Aufgabe; die meisten Techniken zielten darauf ab, das Fälschen unwirtschaftlich teuer und zeitaufwendig zu machen. Beispiele sind manipulationssichere Beschläge, kundenspezifische Schraubenformen, geklebte Gehäuse und der vollständige Verguss des Raumes um eine Leiterplatte. Aufwendiger im Board-Design und in der SMT-Prozesstechnik und optischen Kontrolle ist der Einsatz von Ball Grid Arrays, welche keine freiliegenden Pins haben.

3. Ablauf des Vorhabens

Gegenüber der ursprünglichen Ablaufplanung sind im Projektverlauf Abweichungen entstanden, die eine Verlängerung des ursprünglich veranschlagten Durchführungszeitraumes von zwölf Monaten erforderten. Die detaillierte Beschreibung entnehmen Sie bitte dem detaillierten Sachbericht.

4. Wesentliche Ergebnisse

Wesentliche Ergebnisse des Vorhabens sind im Sachbericht detailliert dargestellt.

5. Zusammenarbeit mit anderen Stellen

Die Zusammenarbeit mit anderen Stellen erfolgte größtenteils nach den Darstellungen der Gesamtvorhabensbeschreibung. Das Projekt bildete in seiner Zusammensetzung die gesamte Wertschöpfungskette für Mixed-Signal Sensor-ICs ab. Die Zusammenarbeit richtete sich dabei nach den Kernkompetenzen der Partner: auf ICLevel arbeiteten die Partner iC-Haus und IMMS eng zusammen, auf Board-Ebene primär Wachendorff und IMMS mit Unterstützung durch iC-Haus.

[2] Quadir, Shahed E., et al. "A survey on chip to system Reverse Engineering." ACM journal on emerging technologies in computing systems (JETC) 13.1 (2016): 1-34.

WACHENDORFF
The Encoder Experts

Sachbericht zum Verwendungsnachweis

Teil II: Eingehende Darstellung

Verbundprojekt:	Elektronischer Knowhow-Schutz für innovative Sensorsysteme - VE-ARiS -
Teilprojekt:	Abwehr von Reverse-Engineering auf Board Ebene
Förderprogramm:	Vertrauenswürdige Elektronik
Förderkennzeichen:	16ME0241
Durchgeführt von:	Wachendorff Automation GmbH & Co. KG Industriestr. 7 65366 Geisenheim
Projektlaufzeit:	01.03.2021 – 31.12.2024
Projektleiter:	Mathias Armbruster

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen 16ME0241 gefördert.

Die Verantwortung für den Inhalt der Veröffentlichung trägt der Autor.

Autor(en):

Mathias Armbruster, Wachendorff Automation GmbH & Co. KG

Inhaltsverzeichnis

1. Ergebnisse des Projekts 4

2. Wichtigste Positionen des zahlenmäßigen Nachweises 35

3. Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten 35

4. Voraussichtlicher Nutzen / Verwertbarkeit der Ergebnisse 35

5. Während der Durchführung des Vorhabens bekannt gewordener Fortschritt bei anderen Stellen 35

6. Veröffentlichung der Ergebnisse 35

1. Ergebnisse des Projekts

Zusammenfassung der im Berichtszeitraum 2021 erzielten Ergebnisse:

AP 1: Recherchen und Vorversuche, Gesamtkonzept

Zu Projektbeginn wurden grundlegende Recherchen zu möglichen Kopierschutz-Mechanismen durchgeführt. Hierbei wurde besonders der Fingerabdruck auf Board-Ebene untersucht. Aus der Nachrichtentechnik sind die Verfahren des „Direct Sequence Spread Spectrum“ (DSSS), sowie „Code Division Multiple Access“ (CDMA) bekannt.

Beim DSSS wird durch Spreizung des Nutzdatenstroms mit einem Spreizcode (Chip-Sequenz) höherer Datenrate das Signal auf eine höhere Bandbreite aufgespreizt, um die Energiedichte im Spektrum zu reduzieren und somit eine bessere Störsicherheit zu erreichen. In den ursprünglich militärischen Anwendungen geht das Signal somit sogar im Hintergrundrauschen unter. Nur durch Kenntnis des Vorhandenseins der Übertragung und der passenden Chip-Sequenz kann das ursprüngliche Nutzsignal rekonstruiert werden.

Beim CDMA benutzt man einen ähnlichen Ansatz, um mehrere Nutzdatenströme in einem gemeinsamen Frequenzbereich zeitgleich zu übertragen. Dabei wird jedem Datenstrom eine eigene eindeutige Spreizfolge zugeordnet, wobei diese Spreizfolgen auf Pseudozufall basieren und zueinander Orthogonalität aufweisen, d. h. eine möglichst minimale Kreuzkorrelation aufweisen. Die Rekonstruktion erfolgt mittels Kreuzkorrelationsfunktion (KKF) mit der passenden Spreizfolge.

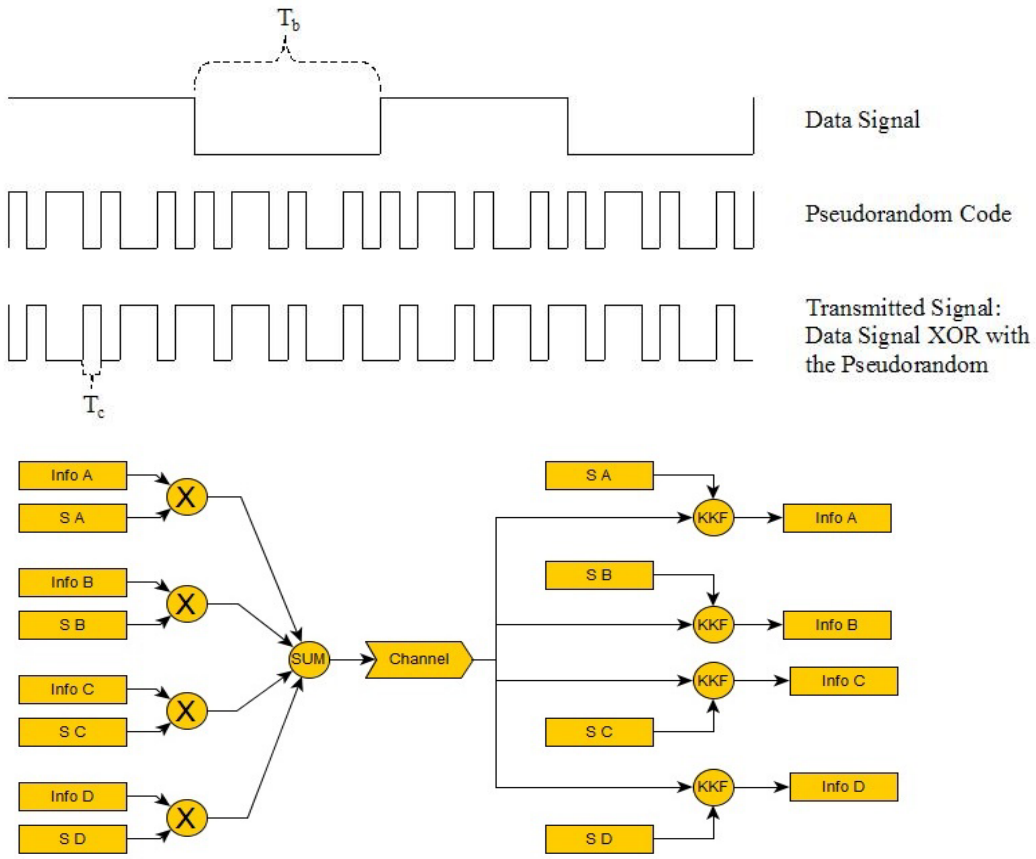


Abbildung 1: Schematische Darstellung des grundlegenden CDMA-Verfahrens (oben) sowie des Verfahrens zur Generierung bzw. Dekodierung des Signals (unten).

Ein Beispiel für die ursprünglich rein militärische Anwendung ist das Global Positioning System (GPS). Die sogenannten C/A-Codes sind für die zivile Nutzung freigegebenen, für die militärische Nutzung wird der sogenannte P(Y)-Code verwendet. Als geeignete orthogonale Pseudo-Random-Folgen gelten die sogenannten „Gold-Folgen“, welche relativ einfach mittels rückgekoppelter Schieberegister erzeugbar sind und welche z. B. bei GPS, UMTS oder WLANs eingesetzt werden.

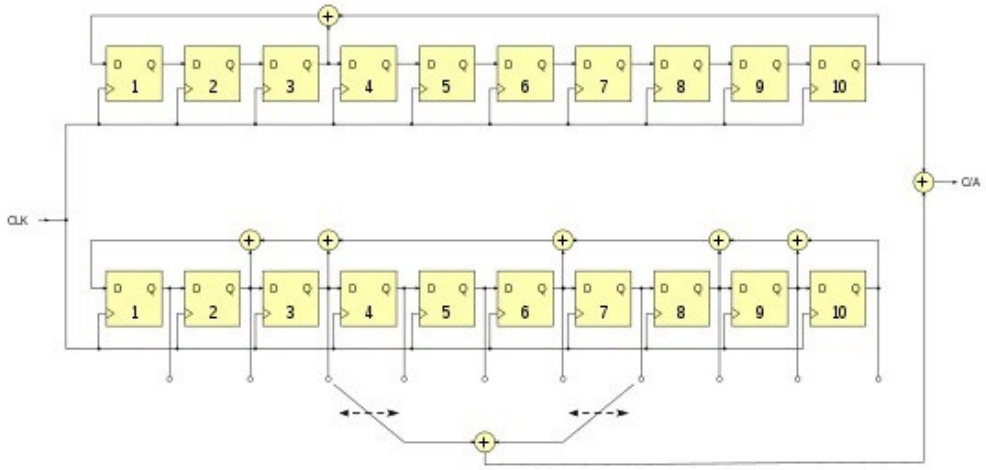


Abbildung 2: Schema eines Generators für Gold-Folgen, der im GPS für den C/A-Code verwendet wird.

Ausgehend von diesen Grundlagen haben sich die Projektpartner entschieden, diesen Spread-Spektrum-Ansatz für die Erzeugung eines Fingerprints auf Board-Ebene zu untersuchen.

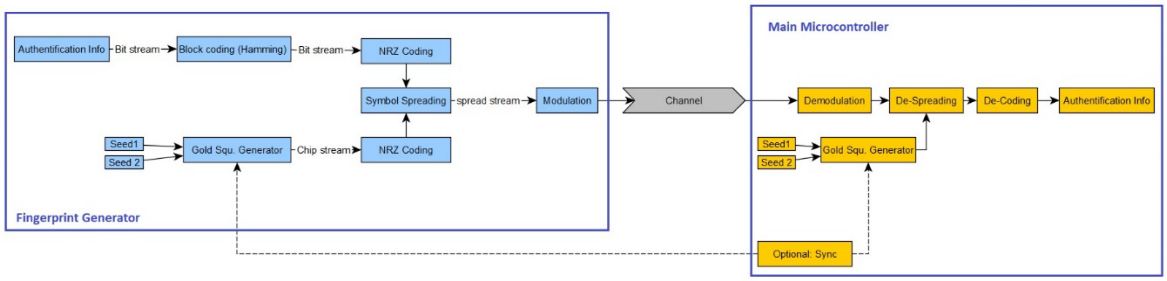


Abbildung 3: Im Projekt entwickeltes Konzept für den Fingerabdruck auf Board-Ebene.

Gemeinsam mit den Projektpartnern wurden die Recherchen und Untersuchungen ausgewertet und ein Gesamtkonzept erstellt.

Dieses Arbeitspaket wurde erfolgreich abgeschlossen.

AP 2: Projektbegleitende Untersuchungen zur Vertrauenswürdigkeit

Die Arbeitspunkte wurden aufgegriffen und begleiten das Projekt fortlaufend. Dabei arbeiten wir eng mit den Projektpartnern zusammen.

AP 3: Tarnung

Dieses Arbeitspaket wurde zurückgestellt und Arbeitspaket 5 vorgezogen. Somit können die Projektpartner früher an den Arbeiten mit dem ARiS-IC beginnen.

AP 5: Aktive Abwehr Board-Ebene / VE-ARiS-Chip

Im Projektverlauf wurde dieses Arbeitspaket vorgezogen, um den Projektpartnern frühzeitig Feedback zum Aris-IC zu geben. Der in der Projektskizze erwähnte Abwehr-IC („ARiS-IC“) enthält eine individuelle Authentifizierungs-Information, welche z. B. im Produktionsprozess mit dem individuellen Drehgeber verknüpft wird. Diese Authentifizierungs-Information wird mit einer Goldfolge gespreizt. Dabei können die beiden Seed-Werte des Goldfolgen-Generators als zusätzliche Authentifizierungsmerkmale ebenfalls im Produktionsprozess individualisiert werden. Der Fingerabdruck-Generator moduliert den so gespreizten Authentifizierungs-Datenstrom so, dass dieser im Rauschen des Übertragungskanals an den Haupt-Microcontroller untergeht. Idealerweise wird der Fingerabdruck so im Rauschen der DC-

Versorgungsspannung auf Board-Ebene oder in der Stromaufnahme des Fingerprintgenerators oder in einer vermeintlichen statischen Steuerleitung (Enable-Signal) versteckt. Der Fingerabdruck wird dann vom Microcontroller mittels internem ADC überwacht, demoduliert und entspreizt. Es ist ebenfalls denkbar, dass eine serielle Dummie-Kommunikation zur Ablenkung zwischen Fingerprint-Generator und Microcontroller erfolgt. Das CLK-Signal einer solchen Übertragung könnte die Synchronisation der beiden Goldfolgen im Fingerprint-Generator und Microcontroller erleichtern.

Der Microcontroller verifiziert den Fingerabdruck im Rahmen des Hochfahrens des Geräts. Es ist noch zu klären, wie sich der Microcontroller bei Fehlschlag verhalten soll (Abbruch des Bootens mit oder ohne Fehlermeldung, sporadisches oder dauerhaftes Ausgeben falscher Prozessdaten zur Maximierung der Störung der Anwendung etc.).

Als ersten Schritt zur Verifizierung des beschriebenen Ansatzes wurden in mehreren Iterationen mittels Labview entsprechende Simulationsprogramme entwickelt, um die Erzeugung von geeigneten Gold-Folgen, die Spreizung und Entspreizung, sowie die Modulation nachzubilden. Mittels dieser Programme lassen sich Einflussparameter einfach variieren. Labview hat dabei den Vorteil, dass sich relativ einfach mittels entsprechend ansteuerbarer Laborhardware die korrespondierenden physischen Signale zur Einspeisung in reale PCBs erzeugen lassen.

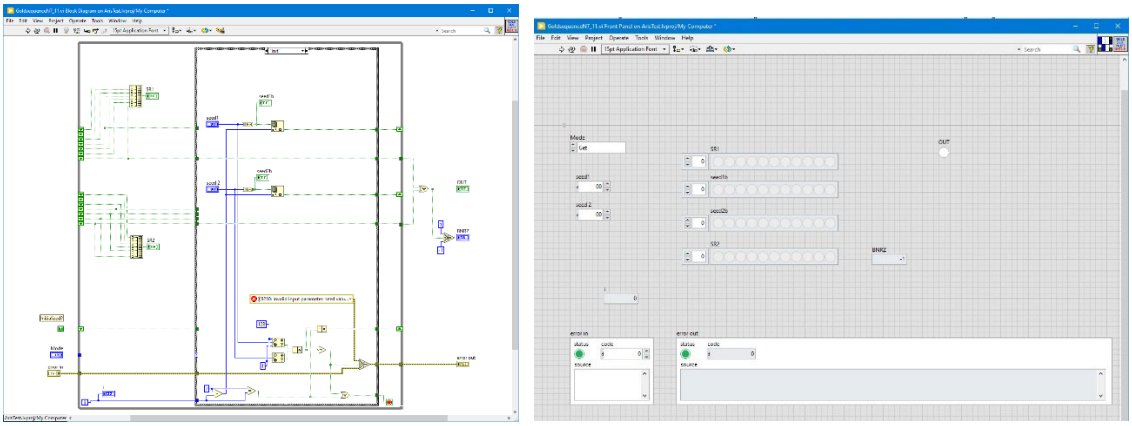


Abbildung 4: Im Projekt entwickeltes Simulationsprogramm zur Erzeugung der Goldfolgen.

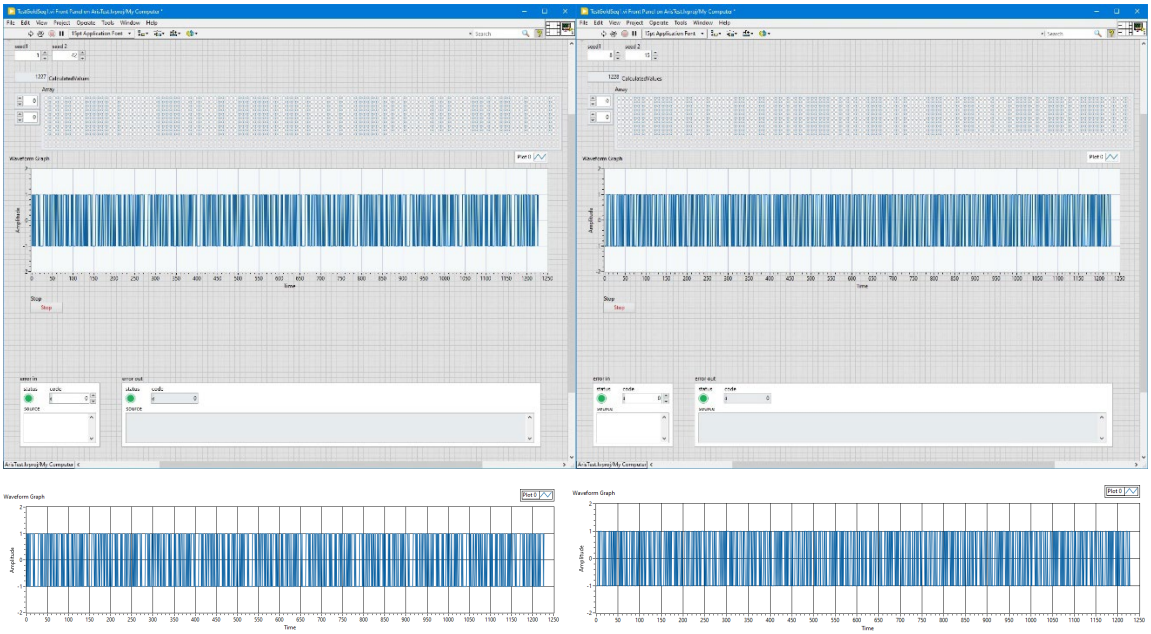
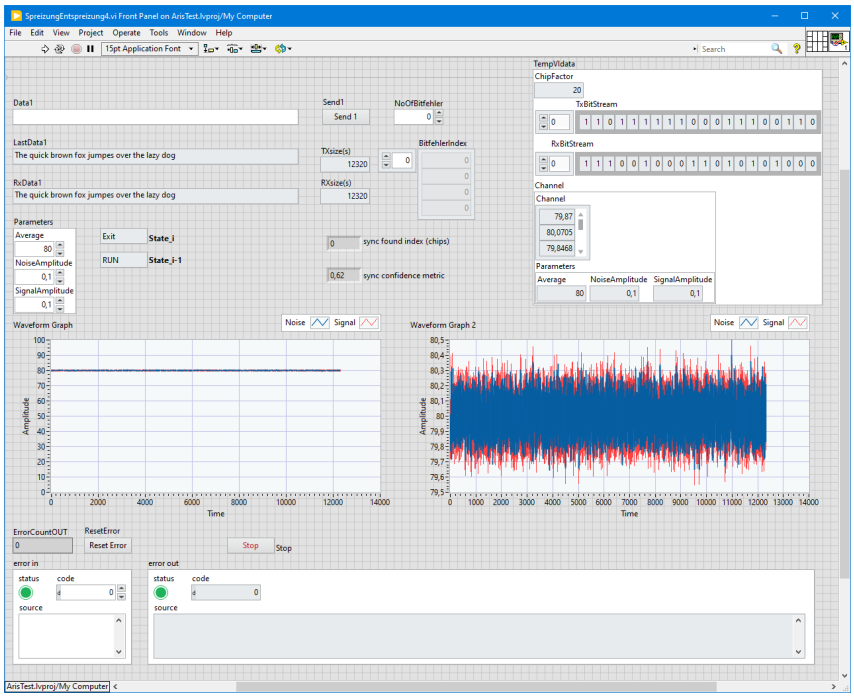


Abbildung 5: Exemplarisch die Sequenzen für die Seed-Paar-Werte (1;42) und (8;15).

Abbildung 6 zeigt die 4. Iterationsstufe der Labview-Simulation. Hier wurde die zu übertragende Information als Erkenntnis zu vorhergegangenen Simulationen vor der Spreizung zusätzlich Hamming-Codiert, um bis zu 3 Bitfehlern pro Symbol ausgleichen zu können (Simulation über Feld „NoOfBitfehler“).



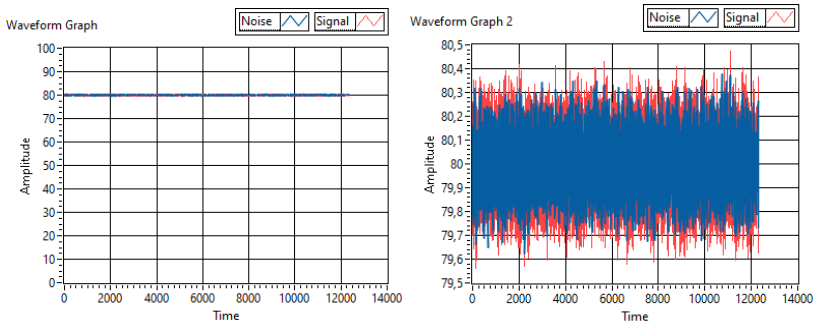


Abbildung 6: Integration einer Hamming-Codierung für höhe Robustheit.

Als Authentifikations-Info wurde hier der Satz „The quick brown fox jumpes over the lazy dog“ mit einer Goldfolge der Länge N=127 (2x 7bit Schieberegister) mit Seed (8;15) gespreizt und auf ein Trägersignal mit Durchschnittswert =80 (angenommene Stromaufnahme in mA) und überlagertem Rauschen der Amplitude 0,1 aufmoduliert. Dabei war die Signalamplitude mit 0,1 identisch zum Rauschen. „Empfangsseitig“ kann das Signal erfolgreich rekonstruiert werden.

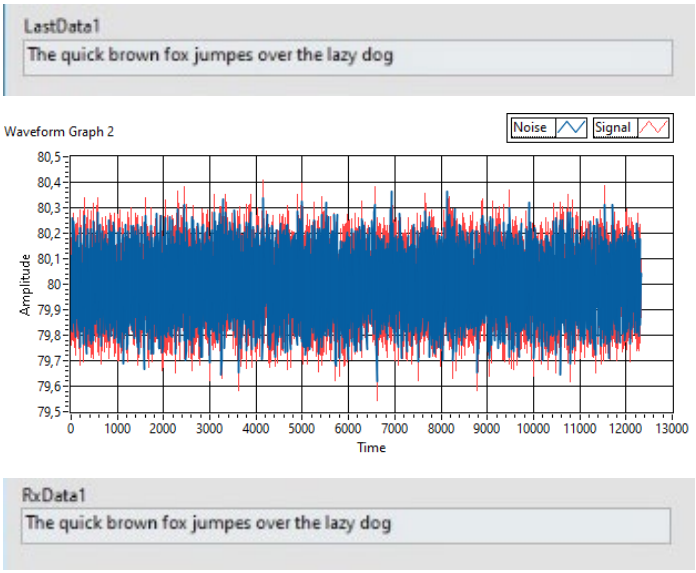


Abbildung 7: Authentifikations-Info (oben), Signal (mitte) und decodiertes Signal (unten).

In weiteren Versuchen wurde die Authentifikations-Info sogar erfolgreich mit einer Signalamplitude von 0,07 übertragen, kleiner als die Rausch-Amplitude. Darunter konnte das Signal nicht rekonstruiert werden.

Die nächsten Schritte für den nächsten Berichtszeitraum sind nun eine Einspeisung der Simulationssignale in ein reales PCB sowie die Realisierung in Hardware (Diskret oder mittels CPLD/FPGA).

Zusammenfassung der im Berichtszeitraum 2022 erzielten Ergebnisse:

AP 1: Recherchen und Vorversuche, Gesamtkonzept

Dieses Arbeitspaket wurde bereits im letzten Berichtszeitraum erfolgreich abgeschlossen.

AP 2: Projektbegleitende Untersuchungen zur Vertrauenswürdigkeit

Die Arbeitspunkte wurden aufgegriffen und begleiten das Projekt fortlaufend. Dabei arbeiten wir eng mit den Projektpartnern zusammen.

AP 3: Tarnung

Dieses Arbeitspaket wurde zurückgestellt und Arbeitspaket 5 vorgezogen. Somit können die Projektpartner früher an den Arbeiten mit dem ARiS-IC beginnen.

AP 5: Aktive Abwehr Board-Ebene / VE-ARiS-Chip

Im Projektverlauf wurde dieses Arbeitspaket vorgezogen, um den Projektpartnern frühzeitig Feedback zum Aris-IC zu geben. Der in der Projektskizze erwähnte Abwehr-IC („ARiS-IC“) enthält eine individuelle Authentifizierungs-Information, welche z. B. im Produktionsprozess mit dem individuellen Drehgeber verknüpft wird. Diese Authentifizierungs-Information wird mit einer Goldfolge gespreizt. Dabei können die beiden Seed-Werte des Goldfolgen-Generators als zusätzliche Authentifizierungsmerkmale ebenfalls im Produktionsprozess individualisiert werden. Der Fingerabdruck-Generator moduliert den so gespreizten Authentifizierungs-Datenstrom so, dass dieser im Rauschen des Übertragungskanals an den Haupt-Microcontroller untergeht. Idealerweise wird der Fingerabdruck so im Rauschen der DC-Versorgungsspannung auf Board-Ebene oder in der Stromaufnahme des Fingerprintgenerators oder in einer vermeintlichen statischen Steuerleitung (Enable-Signal) versteckt. Der Fingerabdruck wird dann vom Microcontroller mittels internem ADC überwacht, demoduliert und entspreizt. Es ist ebenfalls denkbar, dass eine serielle Dummie-Kommunikation zur Ablenkung zwischen Fingerprint-Generator und Microcontroller erfolgt. Das CLK-Signal einer solchen Übertragung könnte die Synchronisation der beiden Goldfolgen im Fingerprint-Generator und Microcontroller erleichtern.

Der Microcontroller verifiziert den Fingerabdruck im Rahmen des Hochfahrens des Geräts. Als ersten Schritt zur Verifizierung des beschriebenen Ansatzes wurden in mehreren Iterationen mittels Labview entsprechende Simulationsprogramme entwickelt, um die Erzeugung von geeigneten Gold-Folgen, die Spreizung und Entspreizung, sowie die Modulation nachzubilden. Mittels dieser Programme lassen sich Einflussparameter einfach variieren. Labview hat dabei

den Vorteil, dass sich relativ einfach mittels entsprechend ansteuerbarer Laborhardware die korrespondierenden physischen Signale zur Einspeisung in reale PCBs erzeugen lassen.

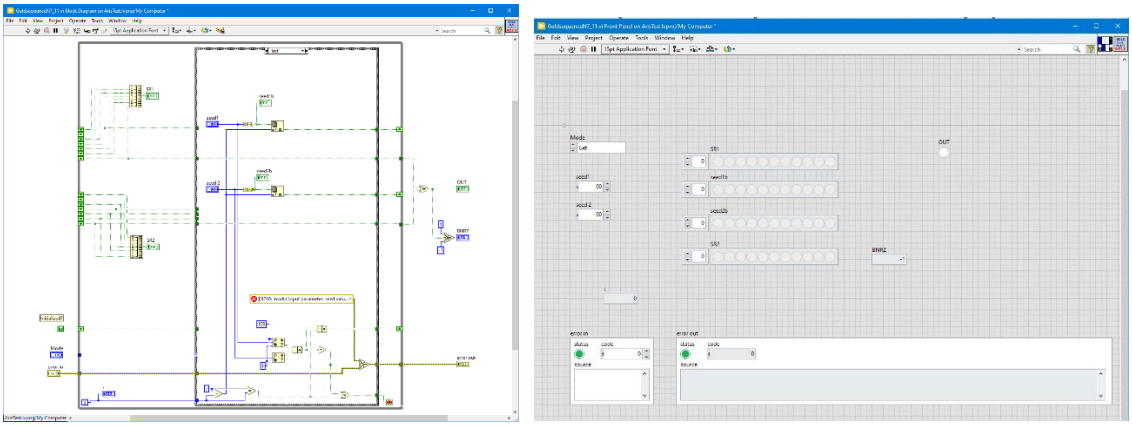


Abbildung 8: Im Projekt entwickeltes Simulationsprogramm zur Erzeugung der Goldfolgen.

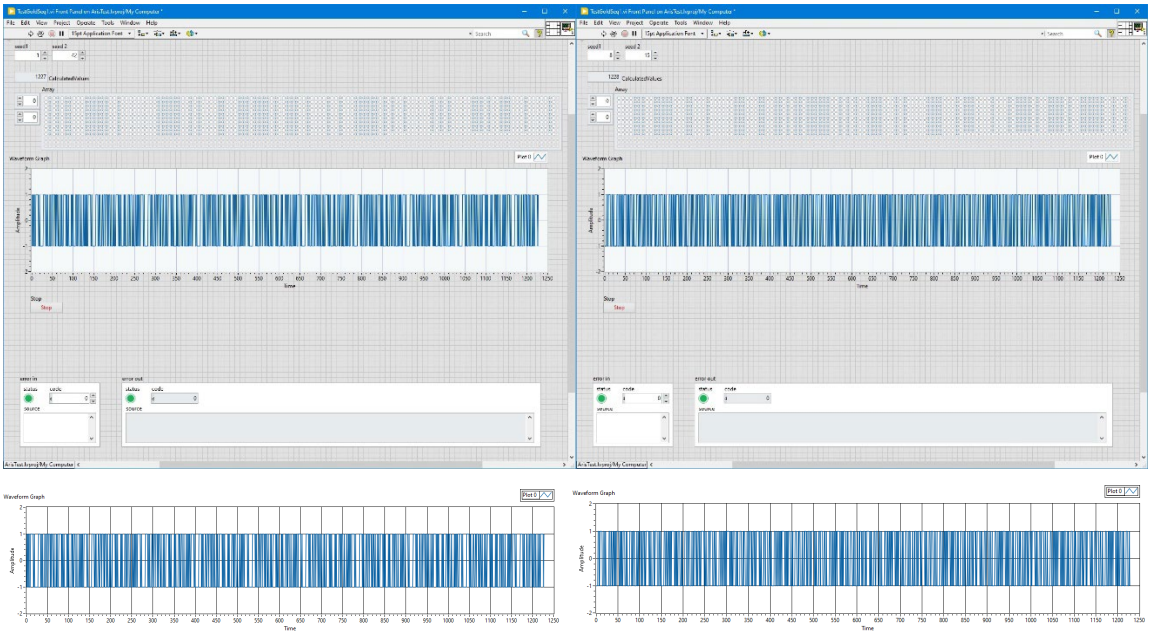


Abbildung 9: Exemplarisch die Sequenzen für die Seed-Paar-Werte (1;42) und (8;15).

Abbildung 6 zeigt die 4. Iterationsstufe der Labview-Simulation. Hier wurde die zu übertragenden Information als Erkenntnis zu vorhergegangenen Simulationen vor der Spreizung zusätzlich Hamming-Codiert, um bis zu 3 Bitfehlern pro Symbol ausgleichen zu können (Simulation über Feld „NoOfBitfehler“).

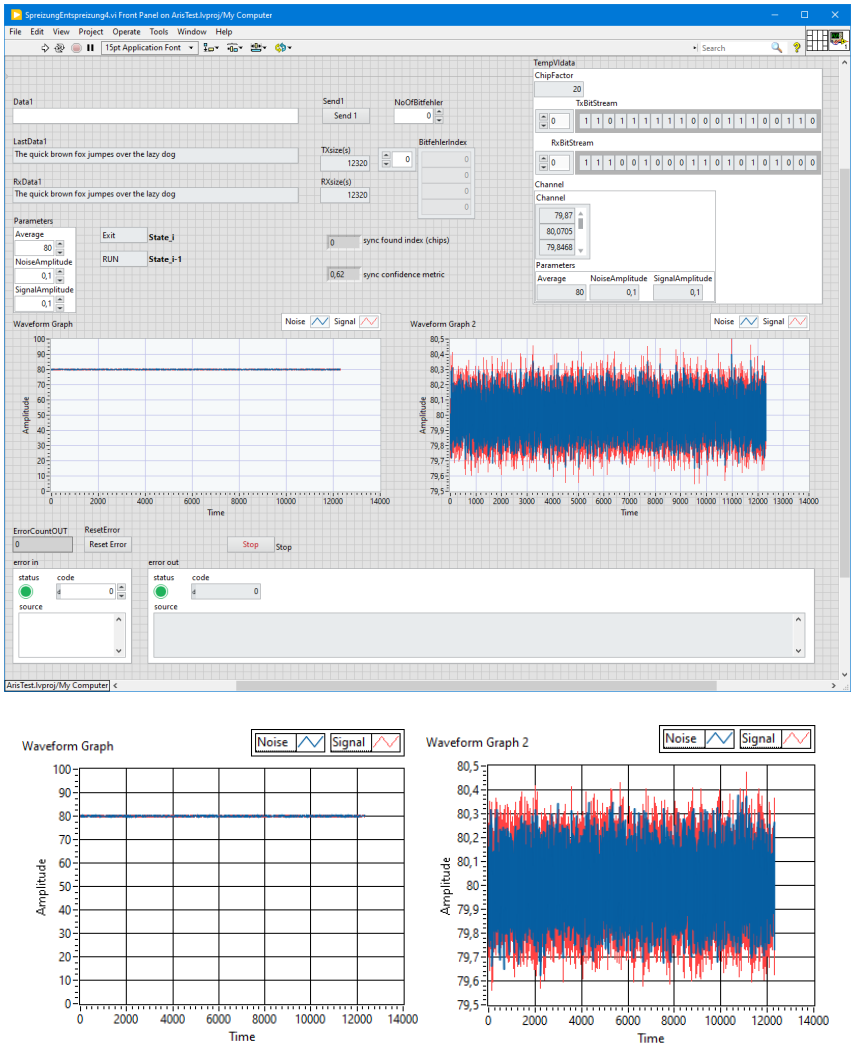


Abbildung 10: Integration einer Hamming-Codierung für höhe Robustheit.

Als Authentifikations-Info wurde hier der Satz „The quick brown fox jumpes over the lazy dog“ mit einer Goldfolge der Länge N=127 (2x 7bit Schieberegister) mit Seed (8;15) gespreizt und auf ein Trägersignal mit Durchschnittswert =80 (angenommene Stromaufnahme in mA) und überlagertem Rauschen der Amplitude 0,1 aufmoduliert. Dabei war die Signalamplitude mit 0,1 identisch zum Rauschen. „Empfangsseitig“ kann das Signal erfolgreich rekonstruiert werden.

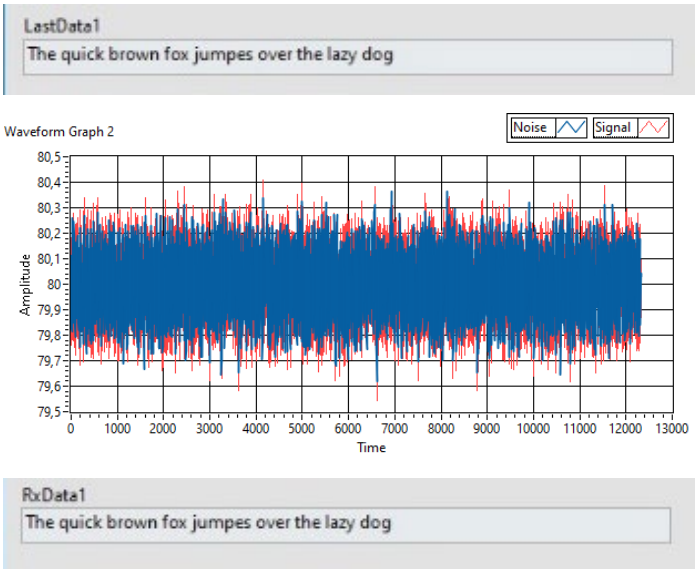


Abbildung 11: Authentifikations-Info (oben), Signal (mitte) und decodiertes Signal (unten).

In weiteren Versuchen wurde die Authentifikations-Info sogar erfolgreich mit einer Signalamplitude von 0,07 übertragen, kleiner als die Rausch-Amplitude. Darunter konnte das Signal nicht rekonstruiert werden.

Im aktuellen Berichtszeitraum wurde zur Verifizierung des beschriebenen und simulierten Verfahrens und zur Untersuchung der Wechselwirkungen zwischen Wasserzeichen und der Primärfunktion des Drehgebers, ein physischer Demonstrator auf Basis eines bestehenden Drehgebers erstellt. Dazu bot sich aus folgenden Gründen zunächst die Verwendung eines Industrial-Ethernet-Drehgebers von Wachendorff an. Die Vorteile sind:

- Trennung von Sensorik und Schnittstellenelektronik auf separaten Leiterplatten/Platinenbaugruppen (ALPs)
- Günstiger Bauraum für Modifikationen durch 58 mm-Gehäuse
- Sensor-Baugruppe wird bei iC-Haus bestückt
- Einfacher Zugriff auf Drehgeberdaten mittels Webserver/Rest-Protokoll

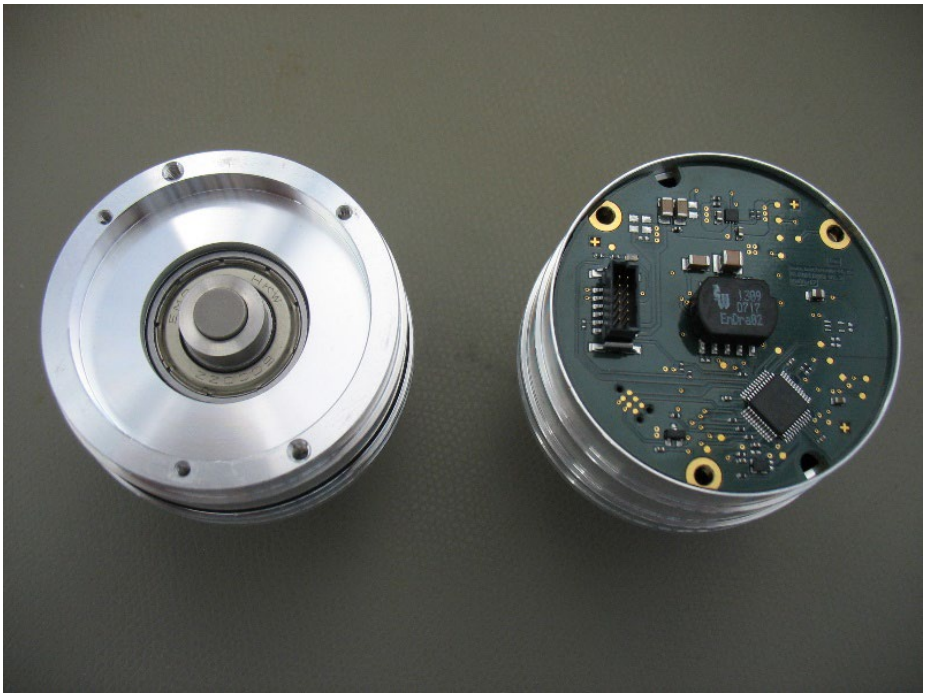


Abbildung 12: Sensor-Leiterplatte vor Modifikation.

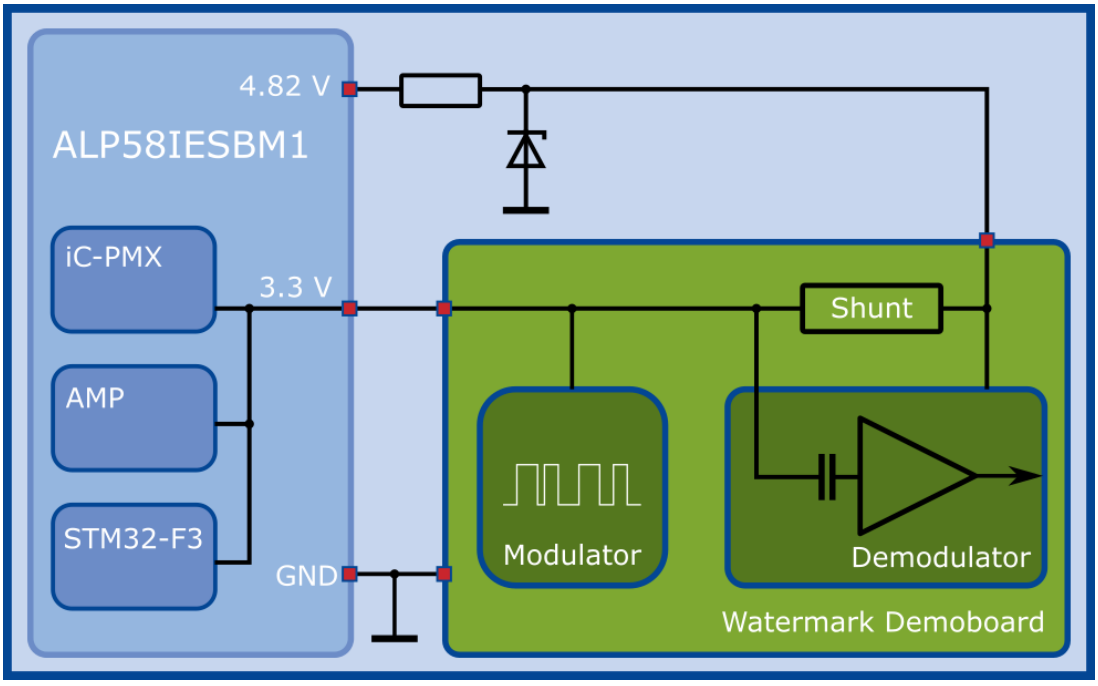


Abbildung 13: Blockschaltbild des Drehgeber-Demonstrators. Der modifizierte Drehgeber (Wachendorff) ist Blau dargestellt und Grün der Wasserzeichendemonstrator (IMMS).

Der Demonstrator ermöglicht das Ein- und Auskoppeln des Wasserzeichens in 2 mögliche physische Kanäle, welche in gemeinschaftlichen Sitzungen der 3 Projektpartner identifiziert wurden:

1. Modifikation 1: In die Versorgungsspannung der Analogstufe des Sensor-ICs (IC-PMX von iC-Haus). Dies verursacht eine Pseudozufällige minimale Verschiebung des Gleichanteils der differenziellen Sensorsignale HOP und HON, welche theoretisch auf

Seite des Microcontrollers bzw. dessen ADC wieder separiert und ausgewertet werden kann, und das zur Tarnung möglichst intern ohne oder nur mit minimalem Einsatz zusätzlicher externer Beschaltung.

2. Modifikation 2: Die Sensorik des iC-PMX verfügt über 16 verschiedene Messsignale, welche nicht parallel, sondern sequenziell über ein einzelnes Signalpaar (HOP/HON) an den Microcontroller übertragen wird. Die Umschaltung der Messsignale erfolgt durch den Microcontroller über das Umschaltsignal „SH“. Mit dem Ready-Signal (RDY) vom iC-PMX zurück zum Microcontroller besteht ein potentieller Rückkanal auf den das Wasserzeichen als pseudozufälliger zeitlicher Jitter aufmoduliert werden könnte. Auch hier sollte die Detektierung seitens Microcontroller zur Tarnung möglichst mit Bordmitteln möglich sein. Vorteil dieser Variante könnte sein, dass über das „SH“ Signal eine zeitliche Synchronisierung zwischen Microcontroller/Demodulator und Aris-Chip/Modulator möglich sein könnte.

In beiden Fällen erfolgt die Wasserzeichengenerierung mittels entsprechender Schieberegister, die Individualisierung des Wasserzeichens kann z. B. durch setzen eines entsprechenden Seed-Wertes mittels SPI- oder I2C-Schnittstelle erfolgen. Die Aufmodulierung auf den physischen Kanal erfolgt entweder durch Schalten eines zusätzlichen Verbrauchers an der Analogversorgung bzw. mittels Schaltens von Verzögerungsgliedern zur Erzeugung des beschriebenen zeitlichen Jitters. Diese Schaltungen werden von iC-Haus in den „Aris“-Chip integriert (siehe Zwischenbericht von iC-Haus).

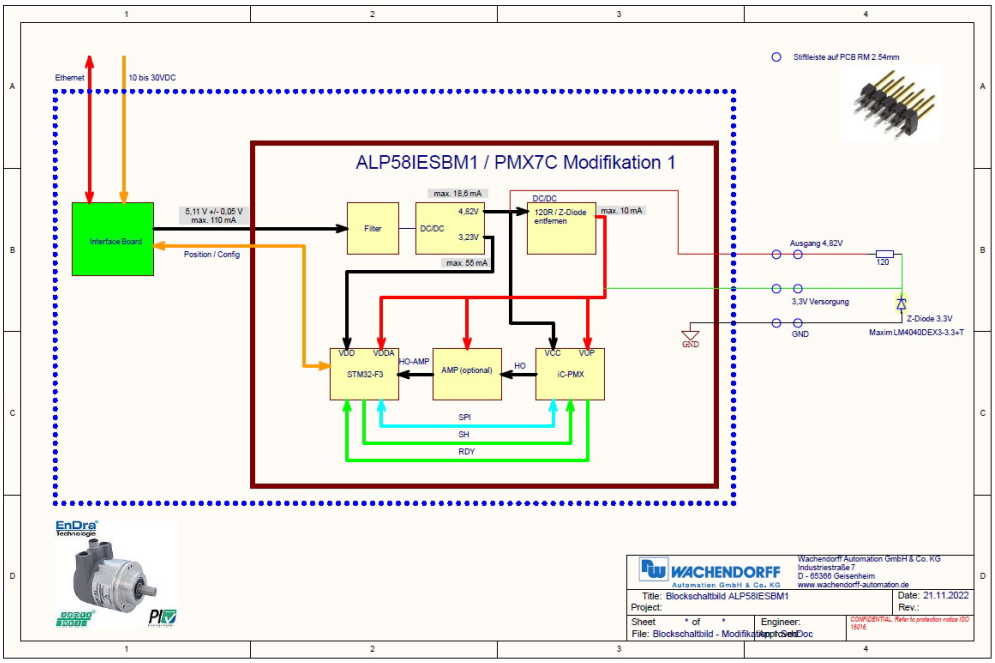


Abbildung 14: Blockschaltbild Modifikation1: Wasserzeichen in der Analog-Versorgung.

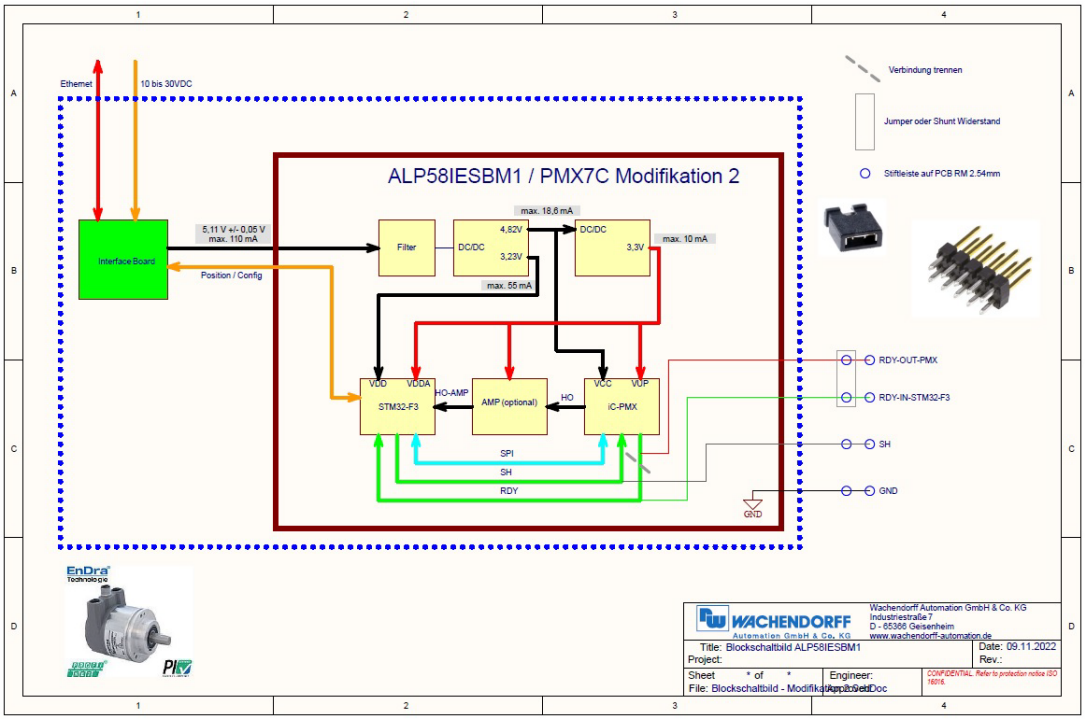


Abbildung 15: Modifikation2: Wasserzeichen über SH und RDY.

Es wurde also ein Demonstrator auf Basis der erwähnten 58 mm Industrial Ethernet-Gebers erstellt, bzw. 3 Einheiten, jeweils für IMMS, iC-Haus und Wachendorff. Dazu wurden die Sensor-Leiterplatten sowie das Gehäuse modifiziert und die notwendigen Signale nach außen geführt. Notwendige mechanische Hilfskomponenten wurden im 3D-Druck-Verfahren erstellt.

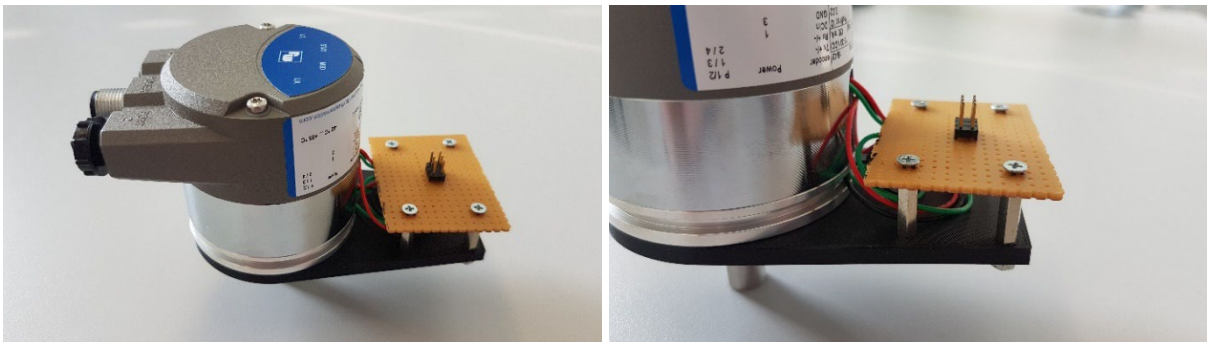


Abbildung 16: Photos des Demonstrators (v1).

Mit dem Demonstrator (v1) wurden erste Genauigkeitsmessungen durchgeführt, um sicherzustellen, dass diese Modifikation an sich, also noch ohne eingekoppeltes Wasserzeichen, keine negativen Auswirkungen auf die Genauigkeit des Sensorsystems und somit den Drehgeber hat.

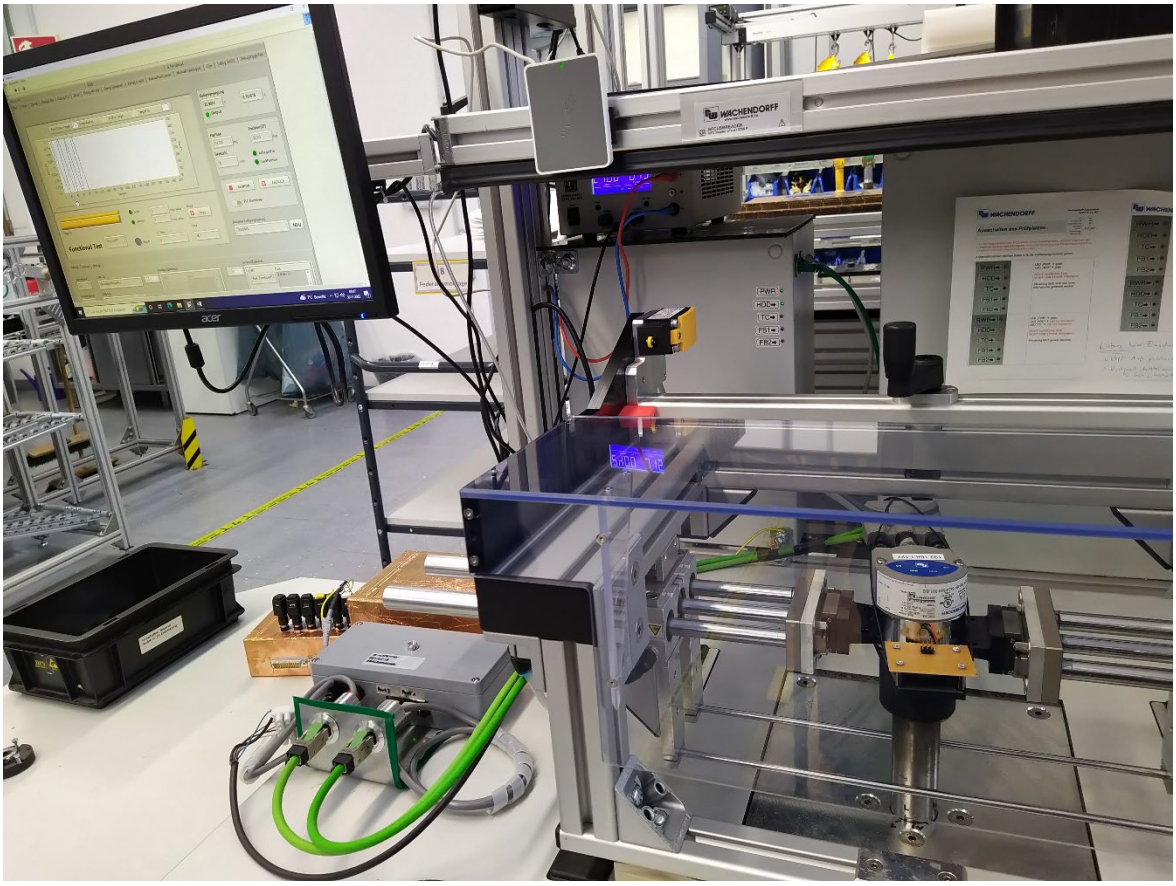


Abbildung 17: Genauigkeitsvermessung des Demonstrators (v1) auf dem Wachendorff Prüfplatz.

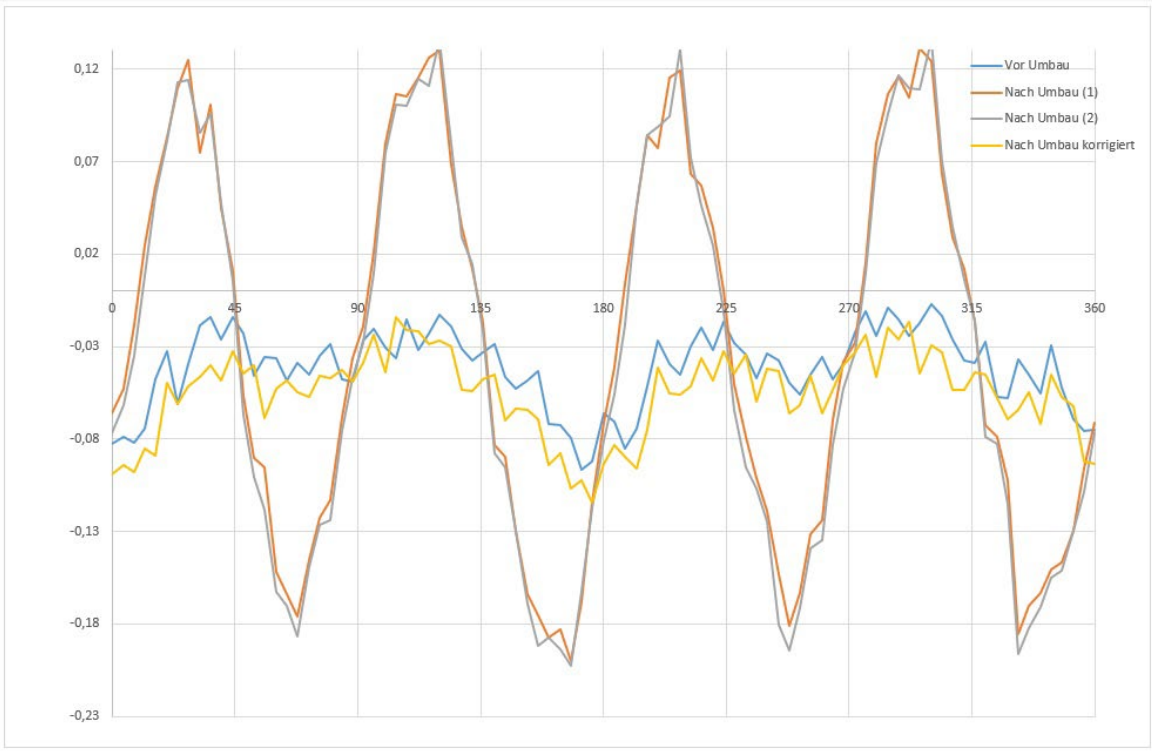


Abbildung 18: Ergebnisse der Genauigkeitsvermessung des Demonstrators nach Modifikation, aber noch ohne Wasserzeichen.

Wie man Abbildung 18 entnehmen kann, wurde zunächst der unmodifizierte Geber vermessen (blau). Die Linien Braun, Grau und Gelb zeigen dann Messungen nach Modifikation. Wie man sieht, mussten dabei mehrere Iterationen durchgeführt werden. Die Abweichung zischen der finalen Modifikation (gelb) und der Ausgangskurve (blau) liegt im Bereich der Messungenauigkeit.

Auf ein Einkoppeln des simulierten Wasserzeichens wurde verzichtet, da das IMMS bereits einen FPGA-basierten Wasserzeichendemonstrator aufgebaut hat. Dies beiden Teildemonstratoren wurden beim IMMS bereits kombiniert und ersten Versuchen und Messungen unterzogen.

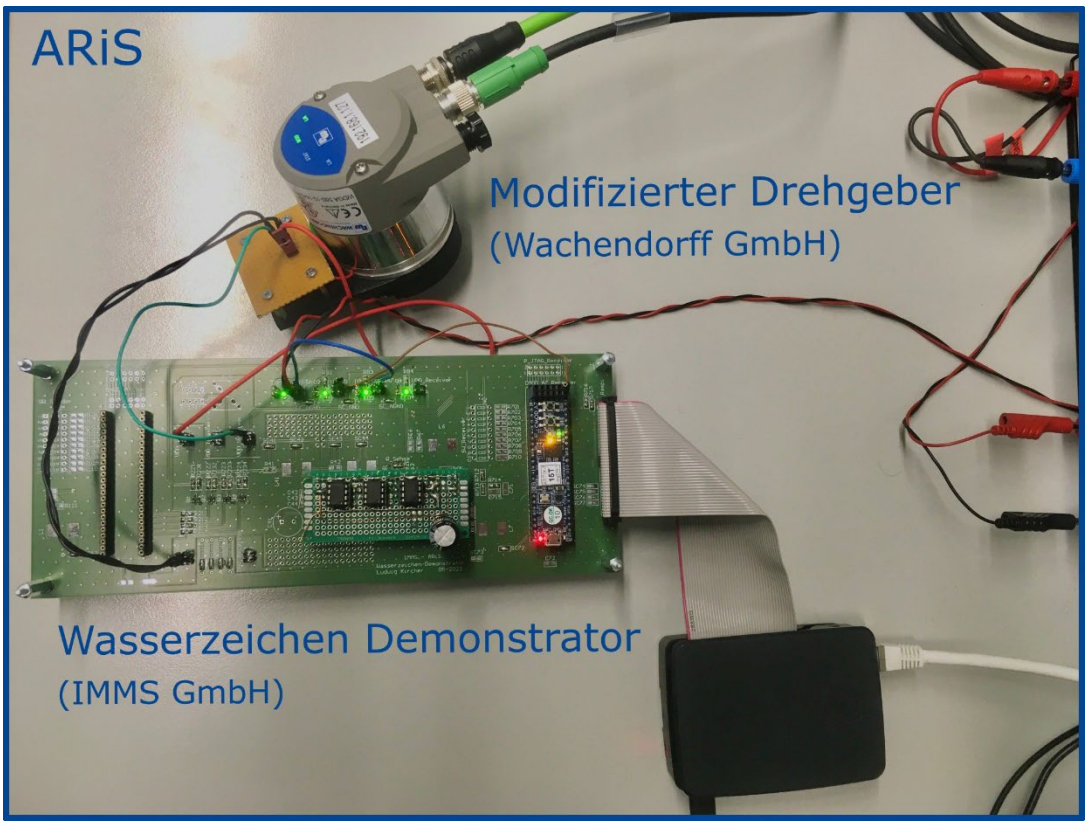


Abbildung 19: IMMS-Wasserzeichen-Demonstrator mit modifiziertem Drehgeber (v1).

Ausblick/Nächste Schritte:

- Wiederholung der Genauigkeitsmessungen des Demonstrators mit eingekoppeltem Wasserzeichen (Besuch IMMS bei Wachendorff)
- Übertragung/Implementierung des FPGA-Demodulators ins Drehgeber-Zielsystem (Microcontroller, Firmware, etc.)
- Übertragung/Implementierung des FPGA-Wasserzeichen-Generator in den Aris-Chip (→iC-Haus) und Implementierung dieses Chips in das Zielsystem
- Finale Verifizierung/Validierung

Zusammenfassung der im Berichtszeitraum 2023 erzielten Ergebnisse:

AP 1: Recherchen und Vorversuche, Gesamtkonzept

Dieses Arbeitspaket wurde bereits im Berichtszeitraum 2021 erfolgreich abgeschlossen.

AP 2: Projektbegleitende Untersuchungen zur Vertrauenswürdigkeit

Die Arbeitspunkte wurden aufgegriffen und begleiten das Projekt fortlaufend. Dabei arbeiten wir eng mit den Projektpartnern zusammen.

AP 3: Tarnung

Die Bearbeitung von AP 3 wurde aufgrund fehlender Ressourcen im Bereich Embedded Software zurückgestellt und stattdessen die Entwicklung der Wasserzeichen fokussiert. Ende 2023 Jahr wurde ein weiterer Entwickler in diesem Bereich eingestellt sowie ein Unternehmen identifiziert, dass Aufgaben ggf. im Unterauftrag übernehmen kann, um die entstandenen Rückstände zumindest teilweise zu kompensieren.

AP 5: Aktive Abwehr Board-Ebene / VE-ARiS-Chip

Im Projektverlauf wurde dieses Arbeitspaket vorgezogen, um den Projektpartnern frühzeitig Feedback zum Aris-IC zu geben. Der in der Projektskizze erwähnte Abwehr-IC („ARiS-IC“) enthält eine individuelle Authentifizierungs-Information, welche z. B. im Produktionsprozess mit dem individuellen Drehgeber verknüpft wird. Diese Authentifizierungs-Information wird mit einer Goldfolge gespreizt. Dabei können die beiden Seed-Werte des Goldfolgen-Generators als zusätzliche Authentifizierungsmerkmale ebenfalls im Produktionsprozess individualisiert werden. Der Fingerabdruck-Generator moduliert den gespreizten Authentifizierungs-Datenstrom so, dass dieser im Rauschen des Übertragungskanals an den Haupt-Microcontroller untergeht. Idealerweise wird der Fingerabdruck so im Rauschen der DC-Versorgungsspannung auf Board-Ebene oder in der Stromaufnahme des Fingerprintgenerators oder in einer vermeintlichen statischen Steuerleitung (Enable-Signal) versteckt. Der Fingerabdruck wird dann vom Microcontroller mittels internem ADC überwacht, demoduliert und entspreizt. Es ist ebenfalls denkbar, dass eine serielle Dummie-Kommunikation zur Ablenkung zwischen Fingerprint-Generator und Microcontroller erfolgt. Das CLK-Signal einer solchen Übertragung könnte die Synchronisation der beiden Goldfolgen im Fingerprint-Generator und Microcontroller erleichtern.

Der Microcontroller verifiziert den Fingerabdruck im Rahmen des Hochfahrens des Geräts. Als ersten Schritt zur Verifizierung des beschriebenen Ansatzes wurden in mehreren Iterationen

mittels Labview entsprechende Simulationsprogramme entwickelt, um die Erzeugung von geeigneten Gold-Folgen, die Spreizung und Entspreizung, sowie die Modulation nachzubilden. Mittels dieser Programme lassen sich Einflussparameter einfach variieren. Labview hat dabei den Vorteil, dass sich relativ einfach mittels entsprechend ansteuerbarer Laborhardware die korrespondierenden physischen Signale zur Einspeisung in reale PCBs erzeugen lassen.

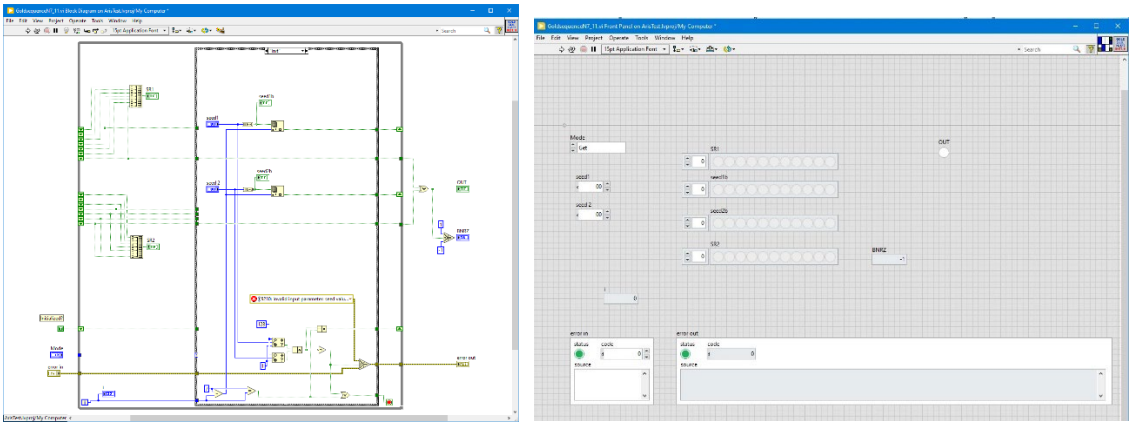


Abbildung 20: Im Projekt entwickeltes Simulationsprogramm zur Erzeugung der Goldfolgen.

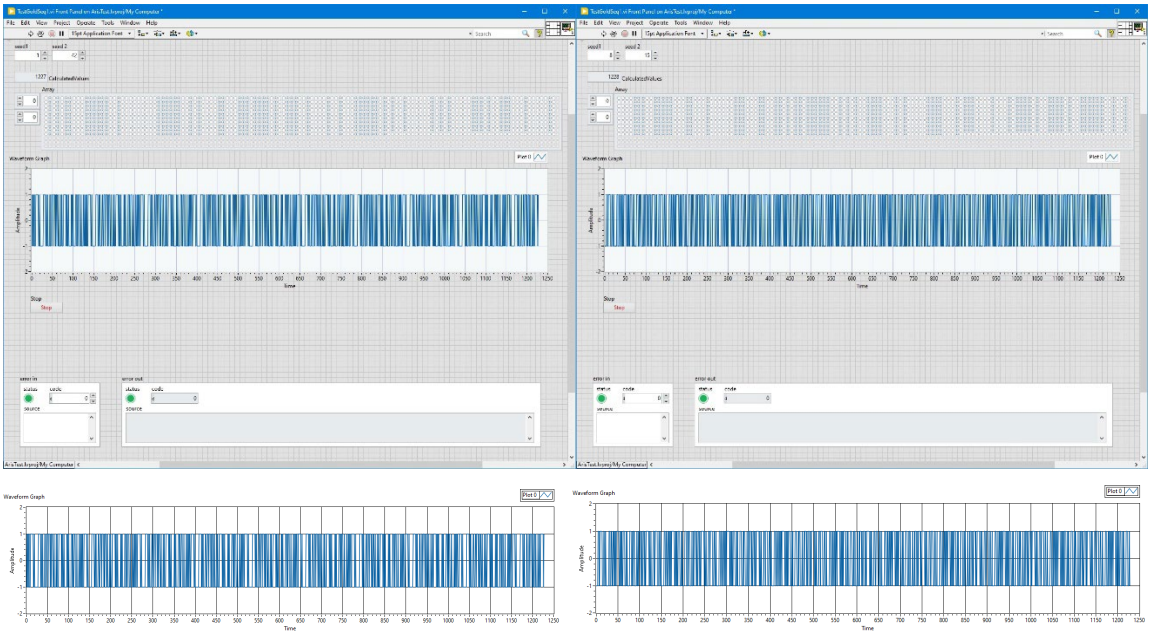


Abbildung 21: Exemplarisch die Sequenzen für die Seed-Paar-Werte (1;42) und (8;15).

Abbildung 6 zeigt die 4. Iterationsstufe der Labview-Simulation. Hier wurde die zu übertragende Information als Erkenntnis zu vorhergegangenen Simulationen vor der Spreizung zusätzlich Hamming-Codiert, um bis zu 3 Bitfehlern pro Symbol ausgleichen zu können (Simulation über Feld „NoOfBitfehler“).

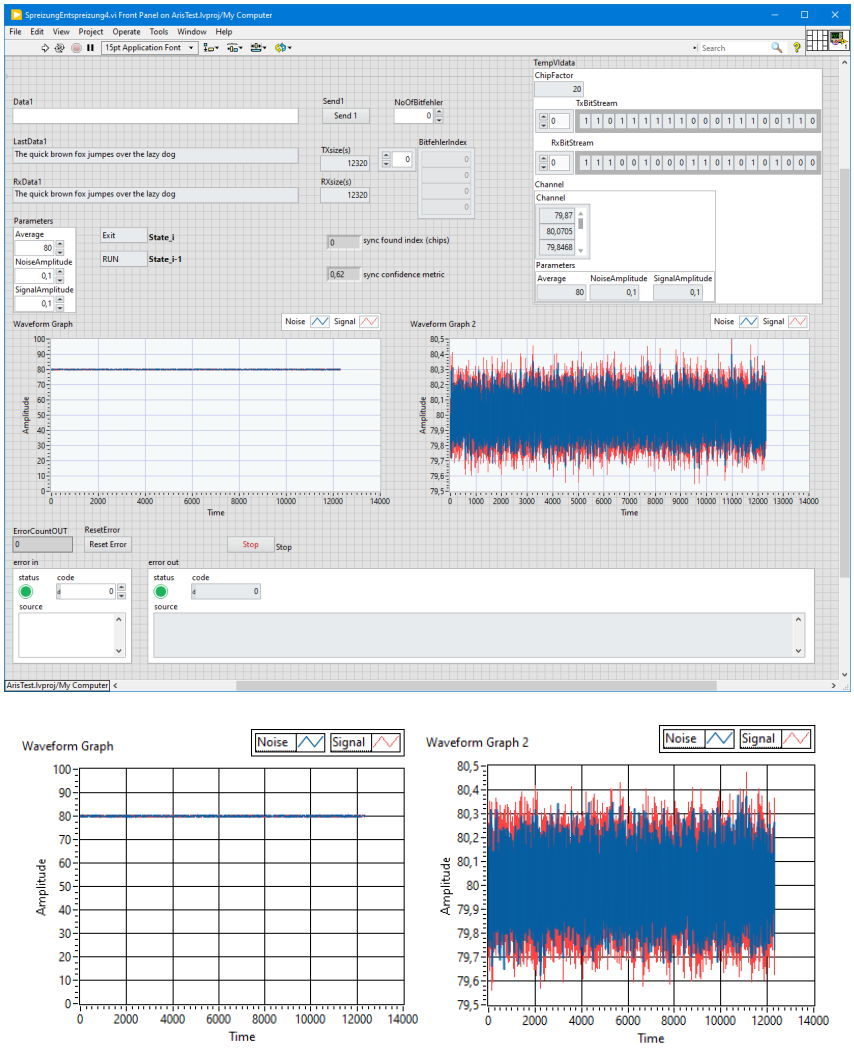


Abbildung 22: Integration einer Hamming-Codierung für höhe Robustheit.

Als Authentifikations-Info wurde hier der Satz „The quick brown fox jumpes over the lazy dog“ mit einer Goldfolge der Länge N=127 (2x 7bit Schieberegister) mit Seed (8;15) gespreizt und auf ein Trägersignal mit Durchschnittswert =80 (angenommene Stromaufnahme in mA) und überlagertem Rauschen der Amplitude 0,1 aufmoduliert. Dabei war die Signalamplitude mit 0,1 identisch zum Rauschen. „Empfangsseitig“ kann das Signal erfolgreich rekonstruiert werden.

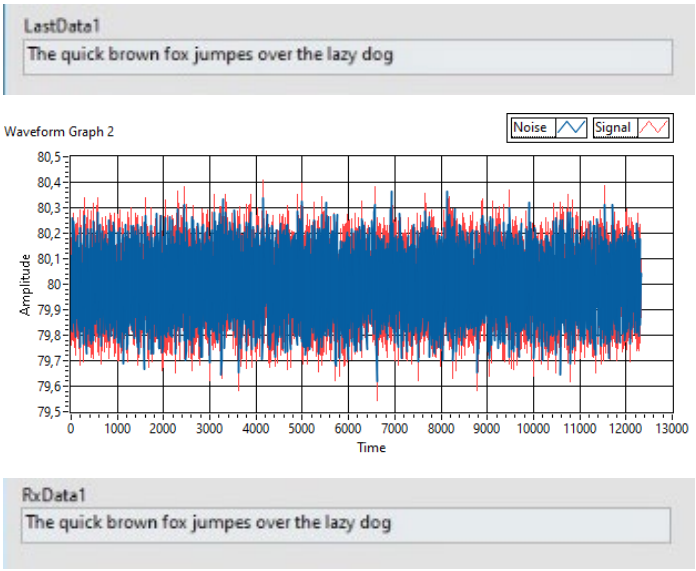


Abbildung 23: Authentifikations-Info (oben), Signal (mitte) und decodiertes Signal (unten).

In weiteren Versuchen wurde die Authentifikations-Info sogar erfolgreich mit einer Signalamplitude von 0,07 übertragen, kleiner als die Rausch-Amplitude. Darunter konnte das Signal nicht rekonstruiert werden.

Im aktuellen Berichtszeitraum wurde zur Verifizierung des beschriebenen und simulierten Verfahrens und zur Untersuchung der Wechselwirkungen zwischen Wasserzeichen und der Primärfunktion des Drehgebers, ein physischer Demonstrator auf Basis eines bestehenden Drehgebers erstellt. Dazu bot sich aus folgenden Gründen zunächst die Verwendung eines Industrial-Ethernet-Drehgebers von Wachendorff an. Die Vorteile sind:

- Trennung von Sensorik und Schnittstellenelektronik auf separaten Leiterplatten/ Platinenbaugruppen (ALPs)
- Günstiger Bauraum für Modifikationen durch 58 mm-Gehäuse
- Sensor-Baugruppe wird bei iC-Haus bestückt
- Einfacher Zugriff auf Drehgeberdaten mittels Webserver/Rest-Protokoll

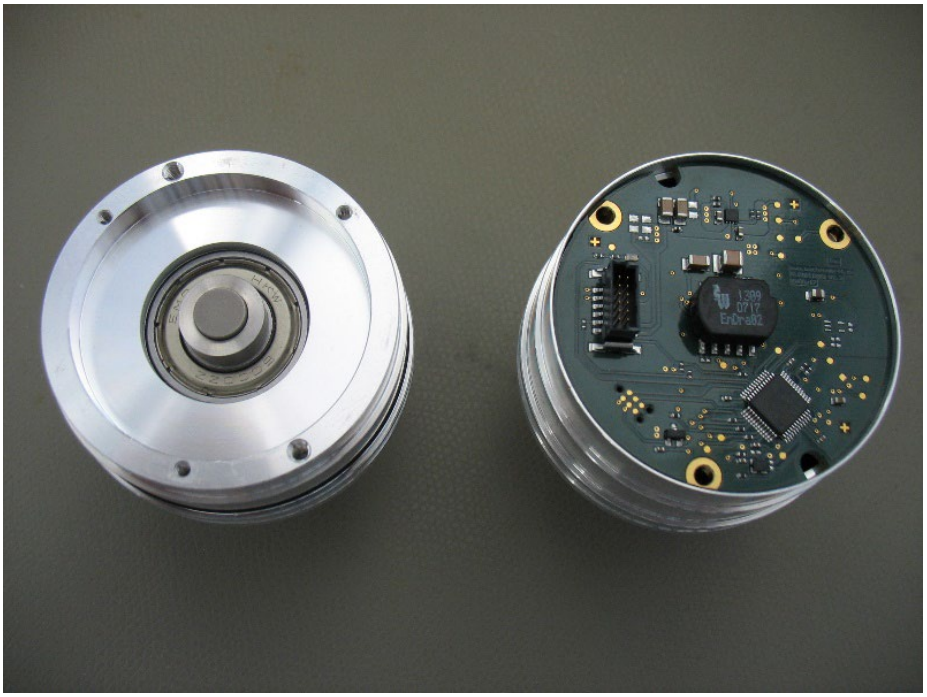


Abbildung 24: Sensor-Leiterplatte vor Modifikation.

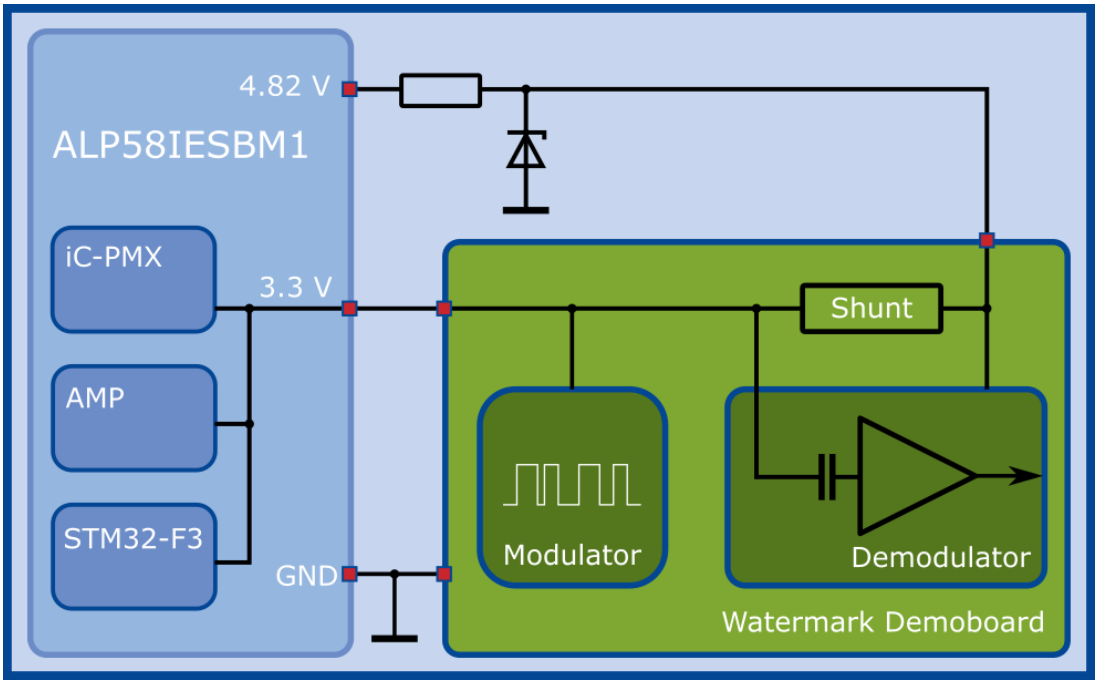


Abbildung 25: Blockschaltbild des Drehgeber-Demonstrators. Der modifizierte Drehgeber (Wachendorff) ist Blau dargestellt und Grün der Wasserzeichendemonstrator (IMMS).

Der Demonstrator ermöglicht das Ein- und Auskoppeln des Wasserzeichens in 2 mögliche physische Kanäle, welche in gemeinschaftlichen Sitzungen der 3 Projektpartner identifiziert wurden:

1. Modifikation 1: In die Versorgungsspannung der Analogstufe des Sensor-ICs (IC-PMX von iC-Haus). Dies verursacht eine Pseudozufällige minimale Verschiebung des Gleichanteils der differenziellen Sensorsignale HOP und HON, welche theoretisch auf

Seite des Microcontrollers bzw. dessen ADC wieder separiert und ausgewertet werden kann, und das zur Tarnung möglichst intern ohne oder nur mit minimalem Einsatz zusätzlicher externer Beschaltung.

2. Modifikation 2: Die Sensorik des iC-PMX verfügt über 16 verschiedene Messsignale, welche nicht parallel, sondern sequenziell über ein einzelnes Signalpaar (HOP/HON) an den Microcontroller übertragen wird. Die Umschaltung der Messsignale erfolgt durch den Microcontroller über das Umschaltsignal „SH“. Mit dem Ready-Signal (RDY) vom iC-PMX zurück zum Microcontroller besteht ein potentieller Rückkanal auf den das Wasserzeichen als pseudozufälliger zeitlicher Jitter aufmoduliert werden könnte. Auch hier sollte die Detektierung seitens Microcontroller zur Tarnung möglichst mit Bordmitteln möglich sein. Vorteil dieser Variante könnte sein, dass über das „SH“ Signal eine zeitliche Synchronisierung zwischen Microcontroller/Demodulator und Aris-Chip/Modulator möglich sein könnte.

In beiden Fällen erfolgt die Wasserzeichengenerierung mittels entsprechender Schieberegister, die Individualisierung des Wasserzeichens kann z. B. durch setzen eines entsprechenden Seed-Wertes mittels SPI- oder I2C-Schnittstelle erfolgen. Die Aufmodulierung auf den physischen Kanal erfolgt entweder durch Schalten eines zusätzlichen Verbrauchers an der Analogversorgung bzw. mittels Schaltens von Verzögerungsgliedern zur Erzeugung des beschriebenen zeitlichen Jitters. Diese Schaltungen werden von iC-Haus in den „Aris“-Chip integriert (siehe Zwischenbericht von iC-Haus).

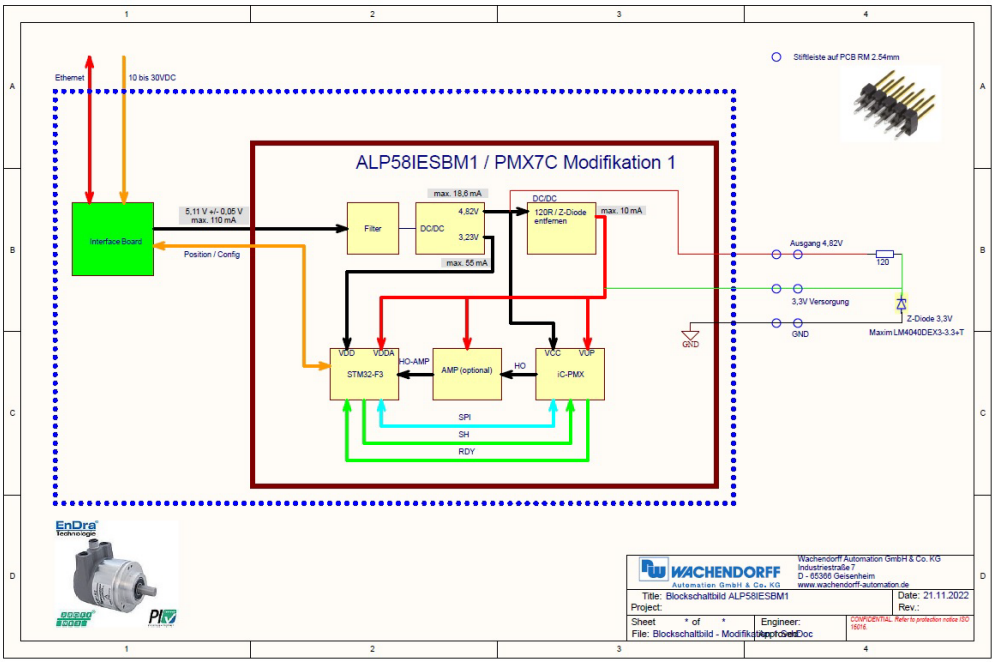


Abbildung 26: Blockschaltbild Modifikation 1: Wasserzeichen in der Analog-Versorgung.

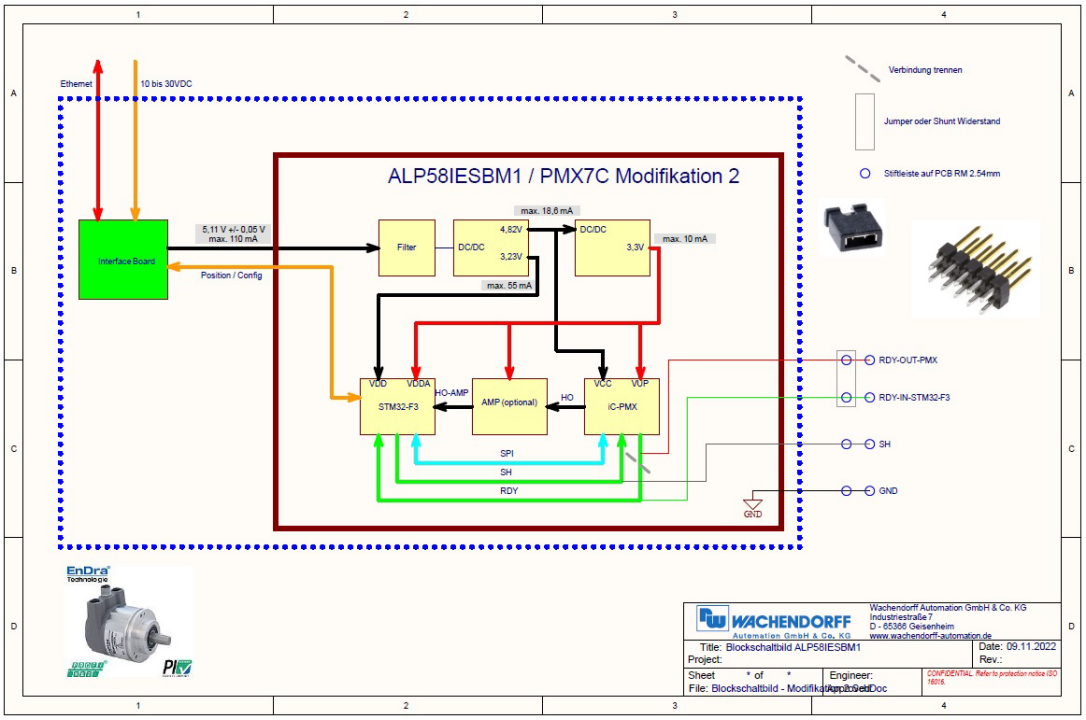


Abbildung 27: Modifikation 2: Wasserzeichen über SH und RDY.

Es wurde also ein Demonstrator auf Basis der erwähnten 58 mm Industrial Ethernet-Gebers erstellt, bzw. 3 Einheiten, jeweils für IMMS, iC-Haus und Wachendorff. Dazu wurden die Sensor-Leiterplatten sowie das Gehäuse modifiziert und die notwendigen Signale nach außen geführt. Notwendige mechanische Hilfskomponenten wurden im 3D-Druck-Verfahren erstellt.

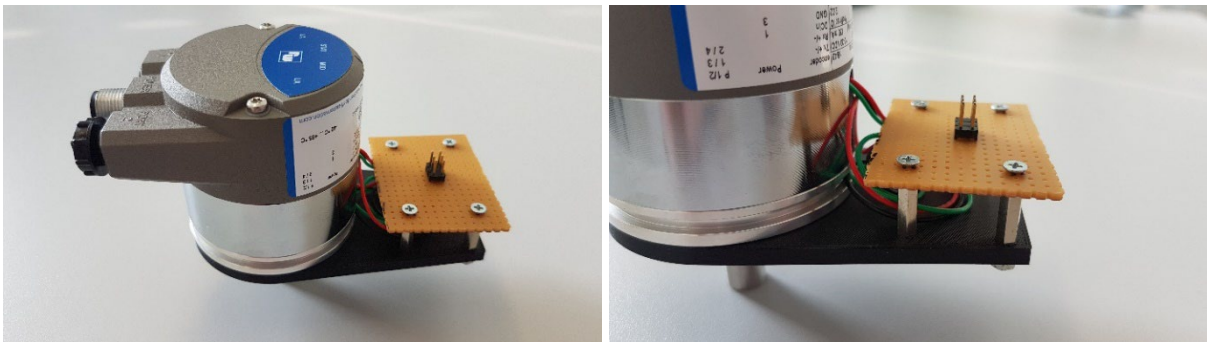


Abbildung 28: Photos des Demonstrators (v1).

Mit dem Demonstrator (v1) wurden erste Genauigkeitsmessungen durchgeführt, um sicherzustellen, dass diese Modifikation an sich, also noch ohne eingekoppeltes Wasserzeichen, keine negativen Auswirkungen auf die Genauigkeit des Sensorsystems und somit den Drehgeber hat.

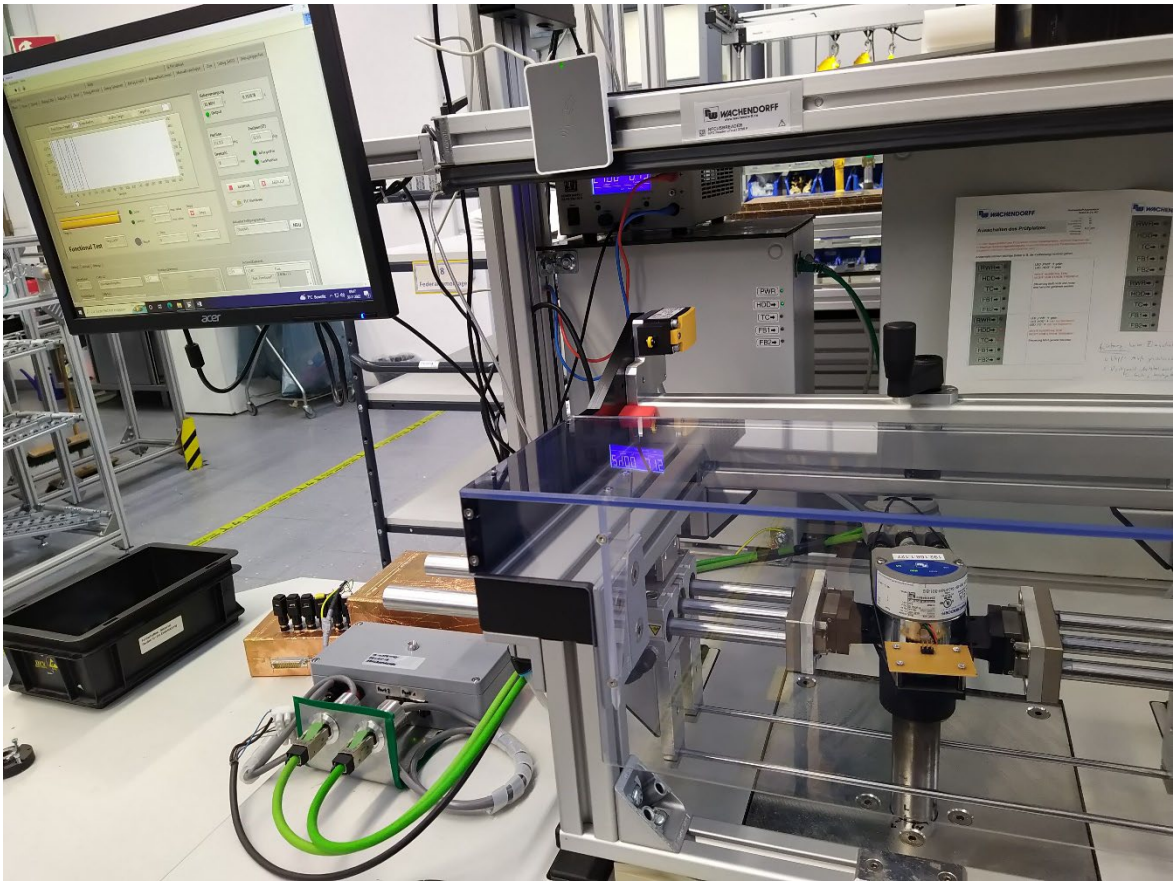


Abbildung 29: Genauigkeitsvermessung des Demonstrators (v1) auf dem Wachendorff Prüfplatz.

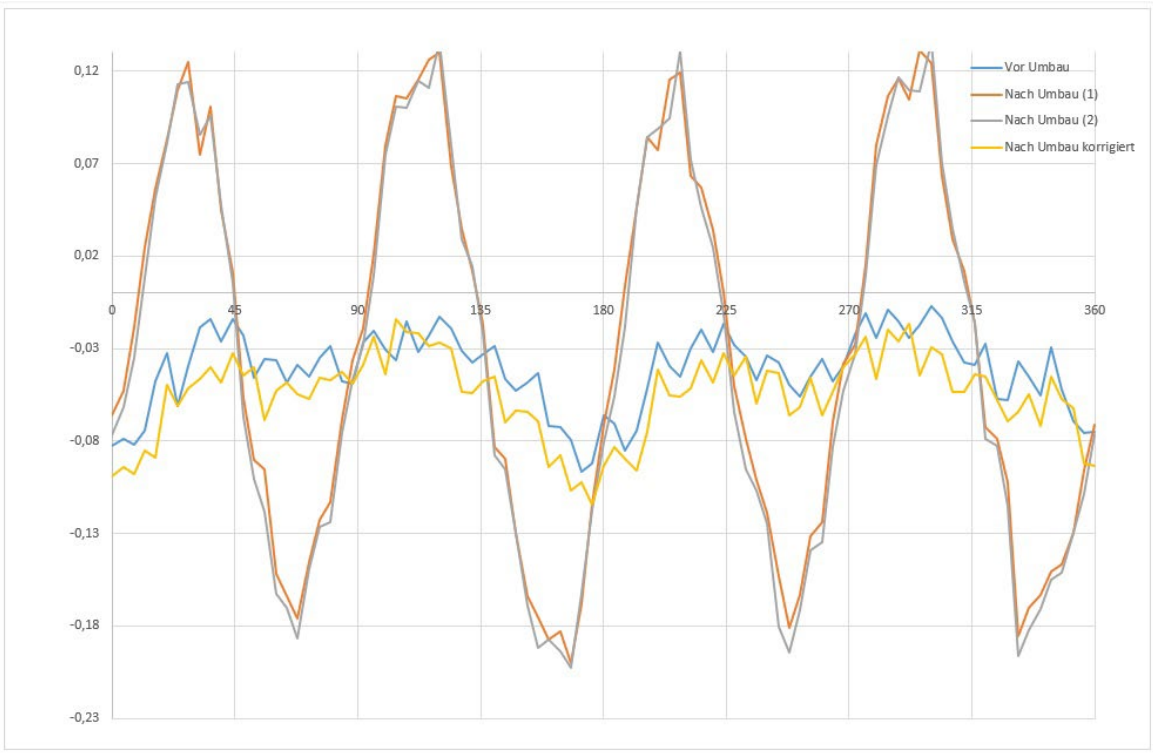


Abbildung 30: Ergebnisse der Genauigkeitsvermessung des Demonstrators nach Modifikation, aber noch ohne Wasserzeichen.

Wie man Abbildung 18 entnehmen kann, wurde zunächst der unmodifizierte Geber vermessen (blau). Die Linien Braun, Grau und Gelb zeigen dann Messungen nach Modifikation. Wie man sieht, mussten dabei mehrere Iterationen durchgeführt werden. Die Abweichung zischen der finalen Modifikation (gelb) und der Ausgangskurve (blau) liegt im Bereich der Messungenauigkeit.

Auf ein Einkoppeln des simulierten Wasserzeichens wurde verzichtet, da das IMMS bereits einen FPGA-basierten Wasserzeichendemonstrator aufgebaut hat. Diese beiden Teildemonstratoren wurden beim IMMS bereits kombiniert und ersten Versuchen und Messungen unterzogen.

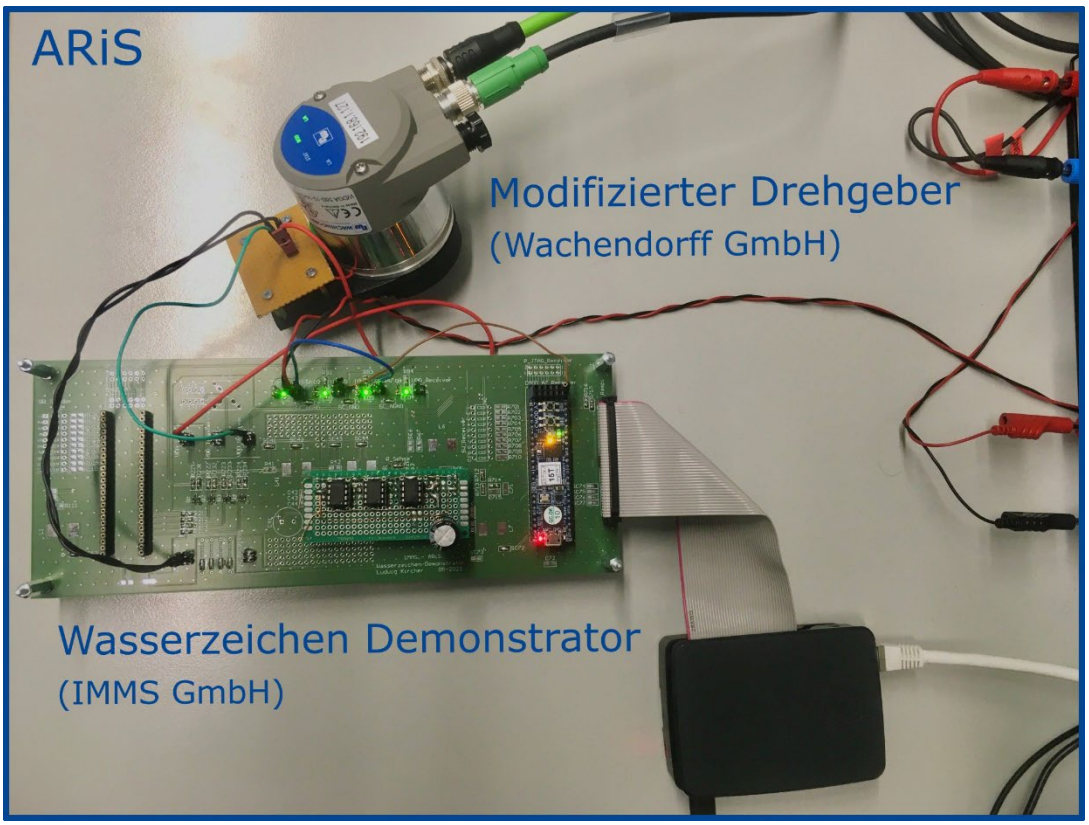


Abbildung 31: IMMS-Wasserzeichen-Demonstrator mit modifiziertem Drehgeber (v1).

Im Berichtszeitraum 2023 wurden vom IMMS statische Messungen mit den Demonstratoren durchgeführt, deren Ergebnisse ausreichend gut waren, um im Projekt fortzufahren (vgl. JB IMMS). Die geplante Durchführung der Messung bei WA wurde zurückgestellt und soll im Rahmen der APs 6h und 6j erfolgen. Gründe für die Rückstellung:

1) Nötiges WA-Fertigungsequipment (Prüfplatz) stand in 2023 aufgrund hoher Auslastung zeitweise nicht zur Verfügung;
2) Personelle Engpässe aufgrund mehrmonatigen Ausfalls (IMMS, Hr. Gläser, WA, Hr. Hanss);

3) Vor allem wurde die Messung in der nächsten Iteration des Demonstrators (mit Aris-Chip statt FPGA mit Freiverdrahtung) als technisch sinnvoller bewertet.

Zur Übertragung/Implementierung des FPGA-Demodulators ins Drehgeber-Zielsystem (Microcontroller, Firmware, etc.) wurden alle notwendigen Vorarbeiten durchgeführt. Die explizite Ausführung liegt gegenüber der ursprünglichen Planung aufgrund von Personalengpässen im Bereich der Embedded Software noch im Rückstand. Ab März 2024 wird sich die aktuell enorme Personalbindung signifikant Entspannung, so dass wir einen erfolgreichen Abschluss innerhalb der Verlängerung erwarten.

Die Übertragung/Implementierung des FPGA-Wasserzeichen-Generator in den Aris-Chip (→iC-Haus) und Implementierung dieses Chips in das Zielsystem wurde zu Beginn 2024 gestartet und soll im Rahmen der Laufzeitverlängerung inkl. finaler Verifizierung abgeschlossen werden.

Das Arbeitspaket wird voraussichtlich im kommenden berichtszeitraum abgeschlossen.

AP 6: Nachweis /Laborversuche

Der Nachweis des VE-ARiS-Systems wird in diesem Arbeitspaket anhand von einem Positionsgeber mit IC von iC-Haus und Board von Wachendorff erbracht, um eine Abwehr auf allen drei Ebenen - Tarnung sowie aktive Abwehr auf IC- und Board-Ebene - nachzuweisen.

In einem ersten Schritt sollten hierzu alle bisher entwickelten Technologien - Tarnung, aktive Abweg auf Board-Ebene und TAN-Verfahren - auf Design-Ebene integriert werden. Die Integration der vom IMMS im FPGA-Bord erarbeiteten Algorithmen zur Detektion, Decodierung und Authentifizierung in den Microcontroller des Drehgebers, werden im Berichtszeitraum 2024 erfolgen. Da die wesentlichen Vorabreiten aber bereits erledigt sind und sich die Personalsituation im Bereich Embeded Software bei Wachendorff ab März signifikant entspannt, sind wir überzeugt die ausstehenden Ziele in der Verlängerung zu erzielen und das Projekt zu einem erfolgreichen Abschluss führen zu können.

Unabhängig von der Software wurden Labormuster der Board-Technologien - Tarnung, aktive Abwehr und TAN-Verfahren - auf Board-Ebene aufgebaut. In diesem Schritt wurden gemeinsam mit iC-Haus auch geeignete ARiS- ICs aufgebaut. Das vorhandene Labormuster (3 physische Exemplare) wurde in mehreren Iterationen so erweitert, dass der ADC im Microcontroller des Drehgebers das vom Wasserzeichengenerator erzeugte und getarnt als fluktuierender Stromverbrauch in der internen Stromversorgung übertragene Wasserzeichen detektiert, um es nach den in den Vorberichten beschriebenen Korrelationsverfahren zu decodieren und zu authentifizieren (Abbildung 32 - Abbildung 34).

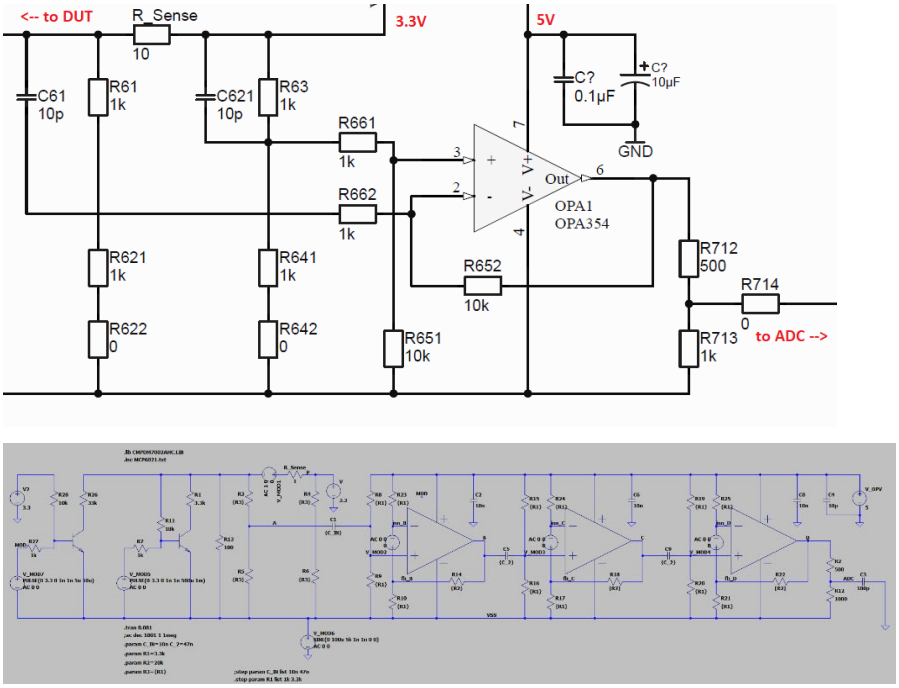


Abbildung 32: Schaltungsvarianten A (oben) und B (unten) zur möglich Strommessung zur Detektion des getarnten Wasserzeichen in der internen Versorgungsspannung.

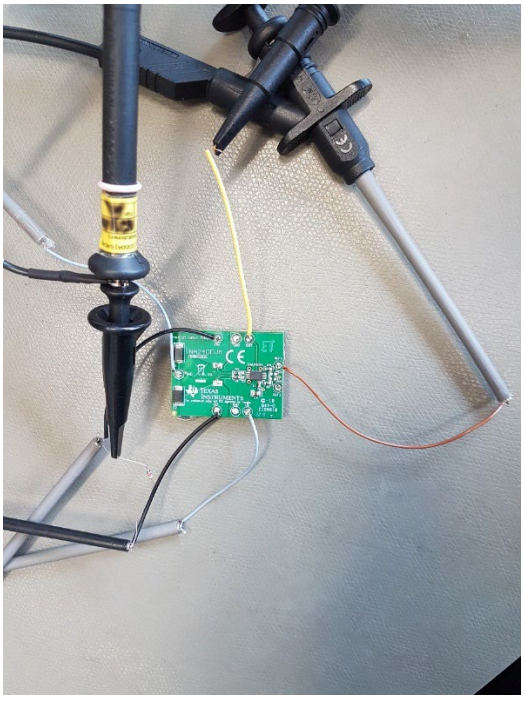


Abbildung 33: Zusätzliches Demoboard zur Strommessung (3.Iteration).

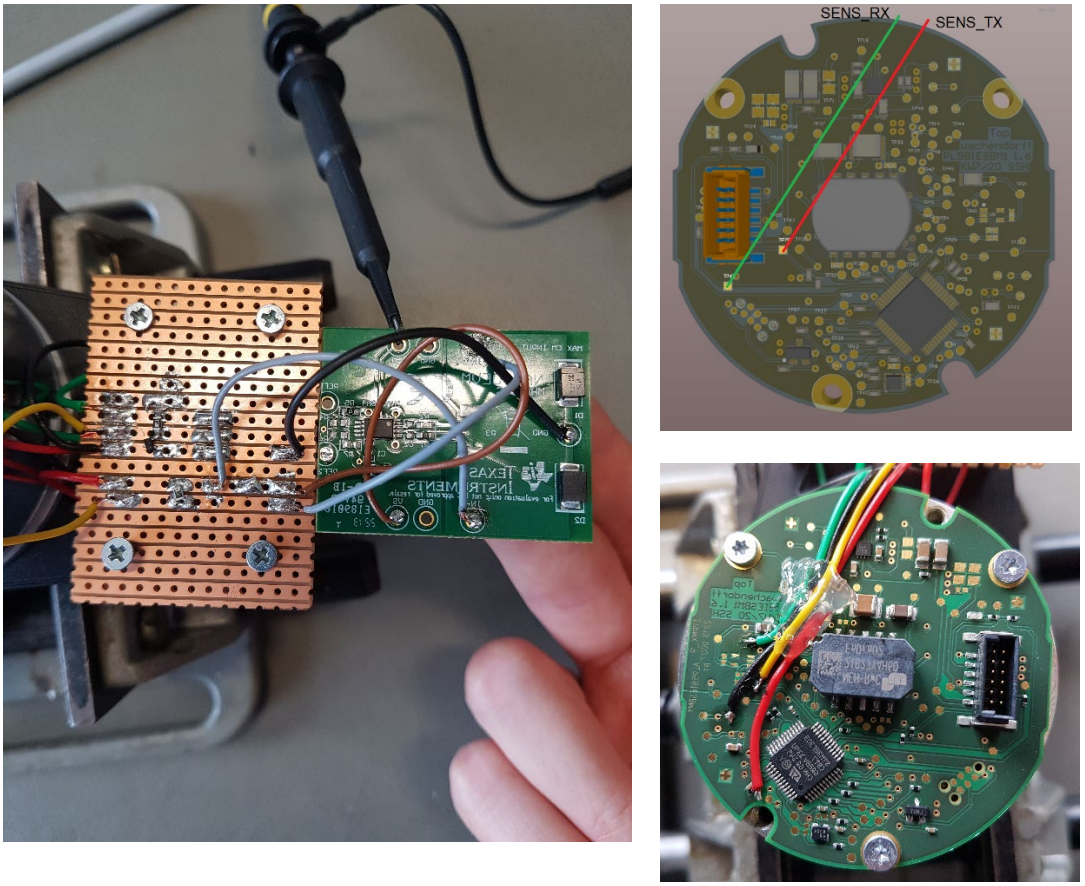


Abbildung 34: Integration der Strommessung in den bestehenden Demonstrator.

Zusammenfassung der im bis zum Projektende erzielten Ergebnisse:

Nach erfolgter Übergabe der Aris.IC (IC-TE341) von IC-Haus an Wachendorff im ersten Quartal 2024, wurden folgende Arbeiten im Berichtszeitraum 2024 durchgeführt:

- Integration ARiS-IC in das Labormuster
- Gemeinsame Laborversuche auf Chip-Ebene
- Gemeinsame Laborversuche auf Board-Ebene
- Aufbau Demonstrator auf Board-Ebene
- Aufbau Demonstrator auf Board-Ebene

Abbildung 35 zeigt den finalen Wasserzeichen Demonstrator, der einen Drehgeber mit Sensorik, Microcontroller und Ethernet-Schnittstelle, IC-TE341 Wasserzeichen-Chip, Modifikation zur Strommessung und Externer USB-SPI-Adapter zur Konfiguration des IC-TE341 enthält.

Die Beschreibung des Wasserzeichen-Detektions-/Dekodier-Algorithmus erfolgt im Abschlussbericht des IMMS.

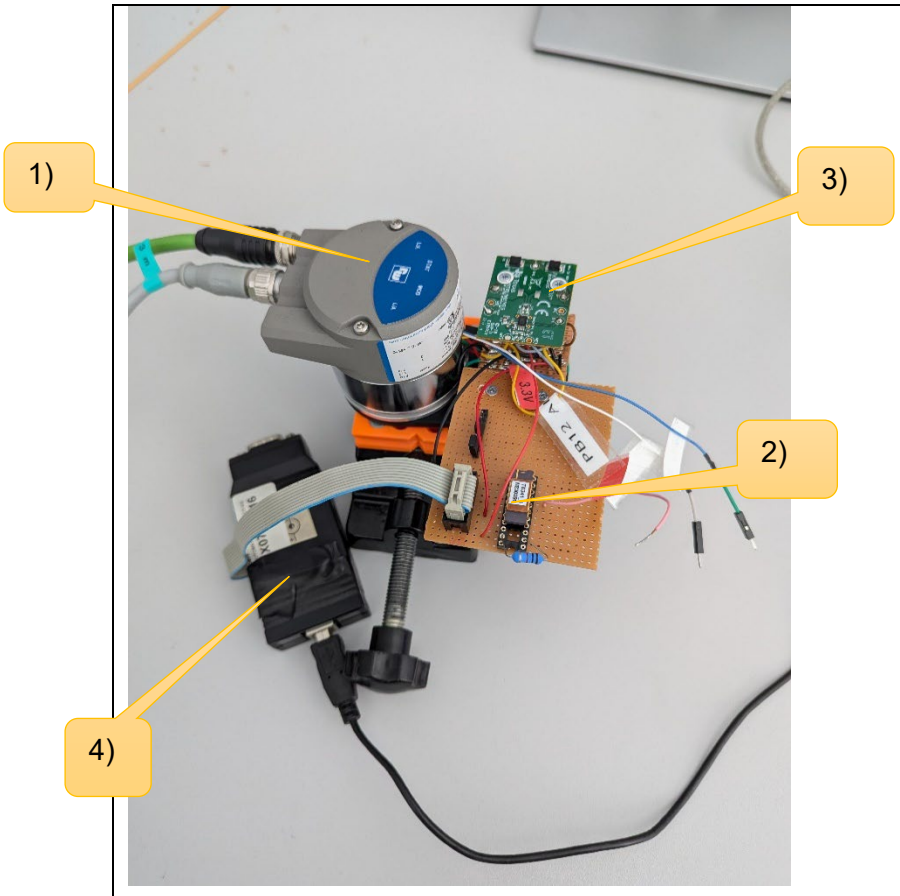


Abbildung 35: Finaler Wasserzeichen-Demonstrator (FinalerDemonstrator.jpg).

1) Drehgeber mit Sensorik, Microcontroller und Ethernet-Schnittstelle
2) IC-TE341 Wasserzeichen-Chip
3) Modifikation zur Strommessung
4) Externer USB-SPI-Adapter zur Konfiguration des IC-TE341

Um das Wasserzeichen mittels Korrelation decodieren zu können, muss der Microcontroller des Drehgebers die im Rauschen der Stromaufnahme versteckte M-Sequenz des Wasserzeichen-Generators kennen. Ein solches Pairing kann z. B. beim Inbetriebnahme-Prozess während der Produktion erfolgen.

Aus Performance-Gründen ist es sinnvoll, die nötige M-Sequenz nicht live im Microcontroller, sondern extern zu berechnen. Die Sequenz kann folgend in einem entsprechenden Look-up-Table im Drehgeber hinterlegt werden.

Der interne Positionswert-Sampling-Zyklus des Drehgebers ist aktuell 50 us. D. h alle 50 us liegen die 16 Samples der Hall-Sensoren vor und werden an die interne Positionswertberechnung übergeben. Um diesen für die Drehgeber-Funktion wesentlichen Zyklus nicht zu stören, wurde entschieden, das Sampeln des Stromwertes für das Wasserzeichen mit diesem Zyklus zu synchronisieren. Das heißt, alle 50 us liegt ein einsprechendes Sample vor. Zur Detektion des für die Demonstration und Funktionsnachweis ausgewählten Wasserzeichen/M-Sequenz werden 405 Samples benötigt. Somit dauert es 20,25 ms, um die ausreichende Menge von Wasserzeichen-Daten zu erfassen. Hierzu zeigt die IMMS Korrelation in **Abbildung 36** im oberen Grafen mehrere Perioden der M-Sequenz. In unteren Grafen erfolgt Korrelation einer Periode der M-Sequenz. Man sieht das ausgeprägte Maximum bei Übereinstimmung, welches sich natürlich mit der Periode der M-Sequenz als Nebenmaxima wiederholt. Zur Optimierung der knappen Systemressourcen ist grundsätzlich eine Periode ausreichend und anzustreben.

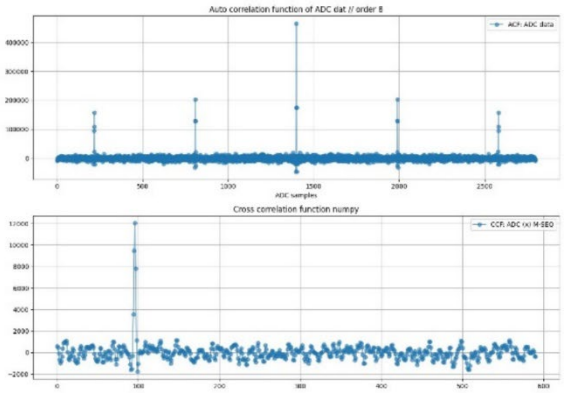


Abbildung 36: IMMScorrelation.jpg.

Abbildung 37 zeigt die auf dem Microcontroller umgesetzte Kreuzkorrelation des Drehgebers. Abweichend zur Abbildung 36 resultiert aus der Kreuzkorrelation ein zweites Maximum im negativen Bereich. Durch das negative Vorzeichen lässt sich diese aber eindeutig vom eigentlichen Maximum abgrenzen. Durch das eindeutige positive Maximum kann die erwartete M-Sequenz eindeutig detektiert werden.

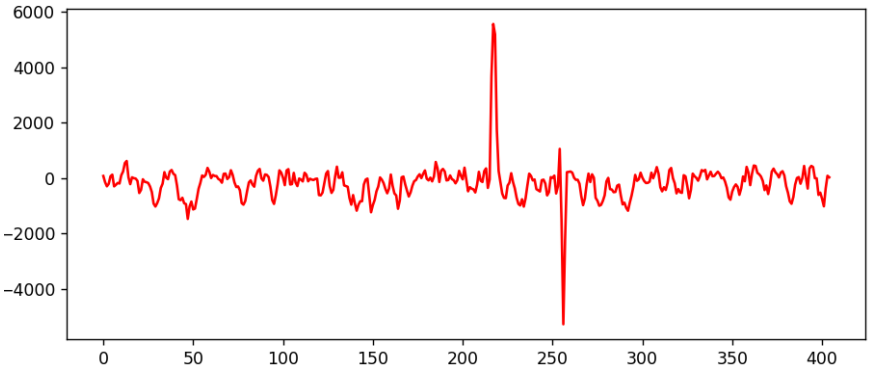


Abbildung 37: Kreuzkorrelation, umgesetzt auf dem Microcontroller des Drehgebers.

Abbildung 38 zeigt die Untersuchungsergebnisse aus der Kreuzkorrelation mit einer falschen M-Sequenz. Es ist erwartungsgemäß kein Maximum detektierbar. Das Ergebnis unterscheidet sich nicht erkennbar von einem zufälligen Rauschen, was in logischer Konsequenz einem komplett fehlenden Wasserzeichen entspricht.

Der dargestellte Detektiervorgang mittels Kreuzkorrelation dauert für die zur Demonstrationszwecken gewählte M-Sequenz bei Ausführung mit Top-Priorität ca. 0,5 s. Eine solche Top-Priorität ist jedoch nicht nötig. Während das Samplen der Raten synchron sowohl mit der Generierung im Wasserzeichengenerator und dem Positionswert-Sampling erfolgen muss, kann die eigentliche Korrelationsberechnung auch mit minimaler Priorität über einen längeren Zeitraum gestreckt werden, um die Drehgeberperformance nicht negativ zu belasten. Festzuhalten ist, dass die im Demonstrator-Versuch angegebenen Zeitwerte nur für die gewählte Länge der M-Sequenz gelten.

Abschließend kann festgestellt werden, dass wir einen **Funktionsnachweis des Wasserzeichen-Verfahrens auf dem Drehgeber** ohne signifikante Einschränkung dessen Funktionalität erbringen konnten, wodurch das zentrale Projektziel erfolgreich nachgewiesen wurde (Abbildung 39).

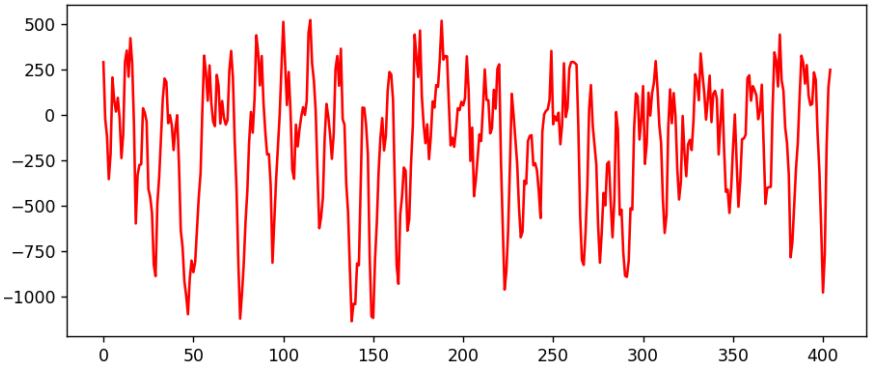


Abbildung 38: Kreuzkorrelation mit einer falschen M-Sequenz.

```
POLY_x = 0x171 (according to the order you choose, see python script)
PRESET_x = 0x1 (could be anything, but must be > 0)
OSC = 0x4f
FREQ_x = 0x0FFF (should result to a MSEQ generator clock of about 6.1kHz

config bits register 0x10:
EXT_PWR = 1 (enable external power dissipation)
EXT_CLK = 1 (enable external power dissipation clock)

START -> mseq generation runs continuously until STOP
```

Abbildung 39: M-Sequenz-Konfiguration via te351_gui.exe tool für den Funktionsnachweis.

2. Wichtigste Positionen des zahlenmäßigen Nachweises

Es wurden weniger Materialien benötigt, als ursprünglich veranschlagt. Die geplanten Fremdleistungen wurden nahezu in vollem Umfang beansprucht. Die Personalkosten wurden unterschritten. Reise- und sonstige Kosten sowie Abschreibungen wurden ebenfalls unterschritten.

3. Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die im Vorhaben durchgeführte Entwicklung bot großes Potenzial, war aber auch mit erheblichen Kosten und Risiken verbunden. Das Projekt erforderte Ressourcen, die über die Kapazitäten von Wachendorff hinausgingen. Daher konnte das Projekt nicht ohne externe finanzielle Unterstützung durchgeführt werden.

4. Voraussichtlicher Nutzen / Verwertbarkeit der Ergebnisse

Der voraussichtliche Nutzen bzw. die Verwertbarkeit der Ergebnisse ist detailliert im Erfolgskontrollbericht dargestellt.

Grob zusammengefasst wird Wachendorff nach Projektende geeignete Sensor-Systeme mit integrierter Abwehr auf dem internationalen Markt anbieten. Durch die erhöhte Sicherheit wird hierbei ein Alleinstellungsmerkmal für besonders kritische Anwendungen (Aufzüge, Industrieroboter, Luftfahrt, etc.) erreicht. Es ist daher davon auszugehen, dass diese Märkte verstärkt auf Wachendorff Produkte setzen.

5. Während der Durchführung des Vorhabens bekannt gewordener Fortschritt bei anderen Stellen

Während der Durchführung des Vorhabens ist kein Fortschritt bei anderen Stellen bekannt geworden, die die Verwertung der erzielten Ergebnisse tangieren.

6. Veröffentlichung der Ergebnisse

Die Fa. Wachendorff bisher keine Ergebnisse veröffentlicht.