

DE-QOR
Schlussbericht

Design hochperformanter CV-QKD-Module für den flexiblen Einsatz in Quantensicheren Optischen Metro- und Weitverkehrsnetzen Teilvorhaben: Niederratige Fehlerkorrektur für den Schlüsselaustausch in der Quanten- kryptographie

Autoren:

Timo Lehnigk-Emden
Markus Fehrenz

Ansprechpartner:

Markus Fehrenz (Creonic GmbH)
markus.fehrenz@creonic.com



Förderkennzeichen:
16KISQ057

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

© Copyright 2025 by Creonic GmbH.

Inhalt

Abbildungen	3
1 Ziele und Aufgaben	4
1.1 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde	5
1.2 Planung und Ablauf des Vorhabens	5
1.3 Wissenschaftlicher und technischer Stand zu Beginn.....	6
2 Zusammenarbeit.....	7
3 Technische Ergebnisse.....	8
3.1 Konzept & Spezifikation.....	8
3.2 Komponenten und Subsysteme.....	9
3.3 Demonstratorentwicklung.....	11
4 Voraussichtlicher Nutzen.....	13
5 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen	13
6 Veröffentlichungen	13

Abbildungen

Abbildung 1 Architektur	11
Abbildung 2 Encoder und Decoder Hardwareplattform.....	13

1 Ziele und Aufgaben

Ziel des DE-QOR-Projektes ist es, die auf physikalischen Prinzipien basierende Quantenschlüsselverteilung (QKD: Quantum Key Distribution) so weiterzuentwickeln, dass sie als ergänzende Sicherheitsmaßnahme für die fasergebundene Standortvernetzung im Metro- und Weitverkehrsbereich eingesetzt werden kann. Unter Verwendung vertrauenswürdiger kohärenter optischer Übertragungstechnik und digitaler Echtzeit-Signalverarbeitung soll zu diesem Zweck ein hochperformantes und zertifizierbares Continuous-Variable-QKD- (CV-QKD) Modul „Made in Germany“ spezifiziert, bis zu TRL 7 entwickelt, sicherheitstechnisch geprüft und im praktischen Feldeinsatz demonstriert werden.

Heute werden alle Art von Daten weltweit digital über öffentliche Netze zwischen zwei oder mehreren Partnern übertragen. Der Versender hat keine Möglichkeit zu wissen durch welche Netze bzw. welcher Weg für die Daten im konkreten Fall gewählt wird. Aufgrund von Datenschutz und Vertraulichkeit werden die meisten Daten verschlüsselt übertragen und somit ist ein sicherer Weg nicht mehr notwendig und es kann die öffentliche Infrastruktur genutzt werden. Im Allgemeinen werden asymmetrische sogenannte Public-Key Verfahren (verschiedenen Schlüssel zur Ver- und Entschlüsselung) sowie symmetrische Verfahren (gleicher Schlüssel für die Ver- und Entschlüsselung) verwendet.

Während die symmetrische Datenverschlüsselung weiterhin als sicher betrachtet werden kann, können auf Public-Key-Kryptographie basierende Schlüsselaustauschverfahren wie Diffie-Hellman durch hinreichend große Quantencomputer gebrochen werden. Der rasche Fortschritt bei der Entwicklung von Quantencomputern durch Firmen wie IBM, Google und Intel lässt erwarten, dass ein solcher Zustand innerhalb der nächsten 10-15 Jahre erreicht werden kann. Da abgehörte Daten und Schlüsselaustauschinformationen zunächst gespeichert und später entschlüsselt werden können, besteht deshalb für Anwendungen mit langen Geheimhaltungsfristen und hohen Sicherheitsanforderungen bereits heute Handlungsbedarf. Methode der Wahl ist hier die Verwendung eines quantencomputerresistenten Schlüsselaustauschverfahrens, wie z.B. das von NIST und BSI empfohlene McEliece-Verfahren. Die Sicherheit solcher Post-Quanten-Kryptographie (PQC: Post Quantum Cryptography) beruht auf der Tatsache, dass trotz langjähriger Forschung selbst für Quantencomputer keine Algorithmen bekannt sind, um die der PQC zugrunde liegenden mathematischen Probleme mit einer kleineren Komplexität als den verwendeten Grad (math. NP-Schwere) zu lösen. Die Existenz solcher Algorithmen kann jedoch auch nicht komplett ausgeschlossen werden, wobei insbesondere bei hochsensitiven Daten mit langer Speicherzeit (z.B. Gesundheitsdaten, Erhebungen bei Volkszählungen) die Gefahr eines sogenannten store now – decrypt later Angriffs besteht.

Daher ist die sichere und zuverlässige Schlüsselübertragung essential um quantensicher, symmetrische Verschlüsselung zu verwenden. Die abhörsichere Übertragung der Schlüssel erfordert aufgrund der Quanteneigenschaften eine Übertragung mit möglichst wenig Energie bzw. wenigen Quanten z.B. Photonen.

Die konkreten Arbeitsziele von DE-QOR beginnen mit der Untersuchung und Definition der Systemarchitektur eines praktisch realisierbaren CV-QKD Moduls. Daraus abgeleitet werden Anforderungsprofile an Komponenten und Subsysteme, von denen in DE-QOR etliche Techniken entwickelt und demonstriert werden.

Die Übertragungsstrecke wie z.B. eine Glasfaser ist kein störungsfreies Medium, die Signal werden durch Rauschen gestört. Die Kombination einer langen Übertragungsstrecke typischer Weise > 80km und einer niedrigen Sendeenergie führen zu einem sehr niedrigen Signal-Rausch Verhältnis typischer Weise < -15dB. Daher ist eine Fehlerkorrektur (FEC: Forward-Error Correction) essentiell um das System funktionstüchtig zu betreiben. Creonic entwickelt mit dem Partner KIT FEC Codes und deren Implementierungen um diese besonderen Anforderungen abzudecken. Creonic konzentriert sich dabei auf die Entwicklung von Chipdesign der Encoder und Decoder sowie um die Entwicklung eines FPGA basierten Demonstrators für den FEC Teil. Der Creonic Teildemonstrator wird in den Gesamtdemonstrator des Partners ADVA integriert.

1.1 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Creonic hat Expertise im Bereich mikroelektronischer Schaltungsentwürfe aufgebaut und eine Methodik entwickelt, die komplexe Algorithmen effizient und schnell auf FPGAs implementiert. Mit dieser Methodik werden energiesparende Schaltungen für drahtgebundene und drahtlose Kommunikation entwickelt. Diverse Nachrichtentechnik-Standards werden damit abgedeckt, z.B. DVB (digitales Fernsehen). Die Creonic-Methodik ermöglicht schnelle Entwicklung und umfangreiche Verifikation der entwickelten Produkte. her sich nur rudimentär mit neuronalen Netzen und herkömmlichen KI-Algorithmen beschäftigt.

Das Kerngeschäftsfeld ist die drahtlose und drahtgebundene Kommunikation über sehr große Entfernungen, wie beispielsweise in der Raumfahrt, als auch sehr kurzen Distanzen innerhalb eines einzelnen Raumes wie in Rechenzentren. Derzeit befinden sich mehr als 30 Satelliten mit Creonic Chipdesigns im Orbit. Weiterhin ist Creonic aktiv an der Entwicklung neuartiger Kommunikationstechnologien mit einem Fokus auf Sicherheit, hoher Geschwindigkeit und geringe Verzögerung, in internationalen Forschungsprojekten beteiligt. Creonic verfügt über große Kompetenzen im Bereich Hardwaredesign und anwendungsspezifischer Mikrochipentwicklung. In der Forschung beschäftigt sich die Creonic GmbH mit Hardwarearchitekturen für Decoder mit Zuverlässigkeitsinformation mit hohen Datenraten und kleiner Ausführungszeit (Latenz).

Im Bereich der verschlüsselten Datenübertragung bestehen bei Creonic bisher wenige Vorarbeiten. Es wurden Konzepte auf Papier ausgearbeitet, um das Potenzial und mögliche Anwendungen innerhalb der bestehenden Produkte im Bereich der optischen Übertragung, zu erforschen.

1.2 Planung und Ablauf des Vorhabens

Das Projekt begann mit der Definition der Gesamtrahmenparameter durch die Projektpartner, wobei insbesondere die Anforderungen an Durchsatz, Latenz und Ressourcenverbrauch für die FEC-Hardwareentwicklung spezifiziert wurden. Diese Parameter bildeten die Entwicklungsbasis für alle nachfolgenden Aktivitäten. In enger Abstimmung mit ADVA wurden die Schnittstellen zur Signalverarbeitung des Gesamtdemonstrators festgelegt, wobei die Integration eines Zufallszahlengenerators und der optischen Signalvorverarbeitung besondere Berücksichtigung fanden. Auf dieser Grundlage erfolgte die Auswahl einer geeigneten Hardwareplattform, die sowohl die Interaktion im Gesamtsystem als auch die speziellen Anforderungen der neuartigen, speicherintensiven Decoderarchitektur mit

sehr großen Blocklängen erfüllte. Dies mündete in der Auswahl der Zielhardwareplattform und der Einleitung ihrer Beschaffung.

Im nächsten Schritt wurden gemeinsam mit dem KIT die spezifischen Codeparameter für die benötigten niedrigen Coderaten und großen Blocklängen festgelegt. Diese Parameter grenzten die verfügbaren Fehlerkorrekturverfahren ein. Gemeinsam mit dem KIT wurden verschiedene Kandidaten für Hardwarearchitekturen identifiziert, einer theoretischen Analyse unterzogen und eine Teilmenge für vertiefende simulationsbasierte Untersuchungen ausgewählt. Für diese ausgewählten Kandidaten wurden bitgenaue Softwaremodelle von Encoder und Decoder entwickelt, die mit einer Zufallszahlenquelle und einem Kanalmodell verbunden wurden. Umfangreiche Langzeitsimulationen dienten dazu, die Codeperformance und die Architekturkorrektheit zu bewerten. Die gewonnenen Erkenntnisse bildeten die Entscheidungsgrundlage für die finale Auswahl der Hardwarearchitektur.

Aufbauend auf den Simulationsergebnissen erfolgte die Implementierung der IP-Cores auf der ausgewählten FPGA-Hardwareplattform. Auf der Senderseite wurde ein Encoder implementiert, der die Zufallszahlen vor der Übertragung encodiert. Die besondere Herausforderung auf der Empfängerseite lag in der Implementierung des Decoders, der aufgrund der niedrigen Coderaten eine speicherorientierte Architektur erfordert, die von gängigen, durchsatzoptimierten Ansätzen abweicht. Die entwickelten Softwaremodelle dienten als Referenz für die Verifikation der Hardware-IP-Cores mittels geeigneter Simulationstools, um die funktionale Äquivalenz sicherzustellen.

Parallel zur Modellentwicklung und Implementierung wurde ein eigenständiger Demonstrator aufgebaut, um die Funktionalität von Encoder und Decoder eigenständig und unter Echtzeitbedingungen prüfen zu können. Den abschließenden Höhepunkt des Projekts bildete der Aufbau des finalen Gesamtdemonstrators gemeinsam mit allen Projektpartnern. Unter Verwendung der definierten Schnittstellen wurden die Einzelkomponenten – einschließlich der implementierten FEC-IP-Cores – miteinander verbunden und einer erfolgreichen Erprobung unterzogen. Die Echtzeitfähige Umsetzung des Gesamtsystems demonstrierte das Potenzial der Projektergebnisse und schafft eine Basis für die weitere Verwertung.

Alle Projektpartner wurden entsprechend ihrer Kompetenzen zur Durchführung des Projektvorhabens eingesetzt. Creonic und das KIT verfolgen einen gemeinsamen iterativen Ansatz für die Entwicklung und Untersuchung geeigneter Fehlerkorrekturverfahren. Das KIT bringt die Expertise des Codedesign ein, Creonic das Wissen über die Auswirkungen auf die Hardwareimplementierung. Im Anschluss untersucht Creonic verschiedene Hardwarearchitekturen mittels Entwurfsraumexploration. Dabei werden alle relevanten Parameter aufgelistet und deren Auswirkungen auf das Hardwaredesign betrachtet. Zur Verifikation der Ergebnisse wird eine Architektur auf einer FPGA Hardware implementiert. Diese Plattform wird zu einem vollständige FEC Demonstrator weiterentwickelt, der in den Gesamtdemonstrator integriert wird.

1.3 Wissenschaftlicher und technischer Stand zu Beginn

Im Bereich der Quantenkommunikation ist QKD die Technologie mit dem wohl höchsten Reifegrad. Die Sicherheitsbeweise, Komponentenwahl und Signalverarbeitung sind bei DV-QKD mit (modifizierten) BB84 Protokollen bereits so weit fortgeschritten, dass kommerzielle Geräte verfügbar sind. CV-QKD-Systeme sind zwar noch nicht kommerziell verfügbar, jedoch sind in der Literatur zahlreiche

Vorarbeiten zu finden, die den Ausgangspunkt für die in DE-QOR verfolgte Entwicklung eines CV-QKD Modules bilden werden.

Es gibt in ITU-T SG13 und SG17, ETSI QKD ISG, und ISO/IEC JTC 1/SC27 eine Reihe von Standardisierungsaktivitäten für QKD-Netze, QRNG, Schnittstellen und Sicherheitsaspekten. Im vorliegenden Vorhaben sind insbesondere das ETSI GS QKD 014 Schlüsselinterface und die Arbeiten von ETSI zur Definition eines Sicherheitsprofils für QKD-Implementierungen von Relevanz.

Digital Fehlerkorrekturverfahren sind seit der theoretischen Beschreibung von Shannon 1948 im praktischen Einsatz. Die zunehmender Bedeutung an schneller digitaler Datenübertragung hat die Entwicklung in den letzten 30 Jahren stark vorangetrieben. Die aktuellen Verfahren wie LDPC, Turbo oder Polarcode und deren Implementierungen reichen sehr nahe an das theoretische Limit (Shannon Grenze) heran. Die Datenraten liegen im Bereich von bis zu 400 Gbit/s für einen Kanal. Alle uns bekannten Anwendungsfälle (Mobilfunk, Glasfaser, Satellit) haben Übertragungskanäle die eine Coderate > 0.2 benötigen. Je höher die Coderate desto mehr Informationen lassen sich auf dem Kanal übertragen, daher verwendet man immer die maximal mögliche Coderate. Untersuchungen für kleine Coderaten < 0.1 sind kaum zu finden, da es bisher dafür keine Anwendung gab, da die Effizienz bzw. der Durchsatz pro Bandbreite für viele Anwendungen viel zu gering ist.

Alle klassischen Anwendungen versuchen durch physikalisches Design (z.B Antennen) und durch digitale Signalverarbeitung das Signal-Rausch Verhältnis (Signal-to-Noise Ratio: SNR) zu steigern um mehr Daten pro MHz Bandbreite zuverlässiger zu übertragen. Die typischen Blocklängen sind kleiner als 100 000 Bits um die Verzögerung die bei der Dekodierung entsteht sowie den Speicherverbrauch klein zu halten. Größere Blocklängen bieten kaum noch Vorteil in Bezug auf die Korrektoreigenschaften.

Die QKD Anwendung benötigt eine Übertragung mit möglichst wenig Leistung um die Sicherheit zu gewährleisten. Daher kommen viele dieser Techniken nicht in Frage und es verbleiben Fehlerkorrekturverfahren mit sehr niedrigen Coderaten und großen Blocklängen da die meisten Bits im Codeword Paritätsinformaten sind.

Hardwarearchitekturen nach dem Stand der Technik haben das Ziele den Durchsatz pro Chipfläche zu steigern um schneller und energieeffizientere Systeme zu bauen. Man kann diese Hardwarearchitekturen als rechenzentrisch beschreiben, da die Anzahl der Operationen pro Zeit optimiert werden soll.

2 Zusammenarbeit

Creonic und das KIT verfolgen einen gemeinsamen iterativen Ansatz für die Entwicklung und Untersuchung geeigneter Fehlerkorrekturverfahren. Das KIT bringt die Expertise des Codedesign ein, Creonic das Wissen über die Auswirkungen auf die Hardwareimplementierung. Im Anschluss untersucht Creonic verschiedene Hardwarearchitekturen mittels Entwurfsraumexploration. Dabei werden alle relevanten Parameter aufgelistet und deren Auswirkungen auf das Hardwaredesign betrachtet. Zur Verifikation der Ergebnisse wird eine Architektur auf einer FPGA Hardware implementiert. Diese Plattform wird zu einem vollständige FEC Demonstrator weiterentwickelt, der in den Gesamtdemonstrator mit ADVA integriert wird.

3 Technische Ergebnisse

Das DE-QOR-Projekt zielt auf die Entwicklung eines funktionsfähigen Demonstrators für Quantenschlüsselverteilung (QKD) mit robusten Fehlerkorrekturverfahren unter extremen Kanalbedingungen. Im Fokus stehen die Hardwareimplementierung von Encoder/Decoder-Systemen, Reverse Reconciliation und die systemübergreifende Zusammenarbeit zwischen den Partnern ADVA, Creonic und KIT. Dieser Bericht fasst die erreichten Arbeiten zusammen und beschreibt die technischen Lösungsansätze, Ergebnisse und künftigen Entwicklungsrichtungen.

3.1 Konzept & Spezifikation

Ziel der Arbeiten war die Auswahl einer Zielhardwareplattform auf Basis der von den Projektpartnern definierten Gesamtrahmenparameter, wie Durchsatz, Latenz und Ressourcenverbrauch. Diese Parameter bildeten die Spezifikation für die FEC-Hardwareentwicklung. Ein besonderer Fokus lag dabei auf der Berücksichtigung der neuartigen, speicherintensiven Decoderarchitektur mit sehr großen Blocklängen. Das konkrete Projektziel war die Auswahl der Zielhardwareplattform und die Einleitung ihrer Beschaffung.

Um die genannten Anforderungen zu erfüllen, wurden zunächst die Grundlagen für eine erfolgreiche Zusammenarbeit im Konsortium geschaffen. Es wurden Systemübersichtsbilder erstellt und Schnittstellen festgelegt, um ein paralleles Arbeiten zu ermöglichen. Insbesondere mit ADVA wurde die Integration eines Zufallszahlengenerators und der optischen Signalvorverarbeitung koordiniert. Zur Sicherstellung der Kompatibilität einigten sich die Partner auf den Einsatz identischer FPGA-Hardwareplattformen, die via SFP+ über Ethernet verbunden werden können. Zusätzlich wurde eine enge Zusammenarbeit mit dem KIT etabliert, bei der die notwendigen Kanalmatrizen via Matlab ausgetauscht wurden, um die Entwicklung abzustimmen und die Vergleichbarkeit von Performancemessungen zu gewährleisten.

Aufbauend auf dieser koordinierten Systemdefinition wurde die Evaluierung der Hardwareplattform durchgeführt. Nach intensiven Diskussionen im Konsortium, bei denen die Bedürfnisse aller Partner berücksichtigt werden mussten, fiel die Wahl auf eine RFSoc der Generation 3 von Xilinx. Diese Plattform erfüllt die spezifischen Anforderungen, da sie sowohl die notwendigen analogen Anschlüsse als auch eine ausreichend große Logikfläche für die speicherintensive Decoderarchitektur bietet. Ein entscheidender Vorteil war die bei Creonic vorhandene Erfahrung mit der Vorgängergeneration, was ein zügiges Aufsetzen eines Testsystems ermöglichte. Dieses System, inklusive eines Linux-Betriebssystems, wurde bereits erfolgreich mit vorhandenen Encodern, Decodern und einer statistischen Analyseeinheit validiert.

Zusammenfassend wurde die gestellte Aufgabe somit erfolgreich abgeschlossen. Durch die Koordination mit den Projektpartnern, die Definition klarer Schnittstellen und die technisch fundierte Evaluierung konnte das Projektziel – die Auswahl einer Zielhardwareplattform und die Einleitung ihrer Beschaffung – erreicht werden. Die getroffene Auswahl stellt eine solide Basis für die folgenden Entwicklungsphasen des Projekts dar.

3.2 Komponenten und Subsysteme

Die Aufgabe dieses Arbeitspakets bestand darin, auf Basis der abgeleiteten Systemparameter gemeinsam mit dem KIT spezifische Codeparameter für niedrige Coderaten und große Blocklängen festzulegen. Darauf aufbauend sollten Kandidaten für Hardwarearchitekturen identifiziert, theoretisch analysiert und anschließend simuliert werden. Die Langzeitsimulationen bitgenauer Modelle von Encoder und Decoder dienten dazu, die Codeperformance und Architekturkorrektheit zu bewerten, um eine finale Hardwarearchitektur für die IP-Core-Entwicklung auszuwählen. Das Ziel war die Auswahl einer finalen Hardwarearchitektur.

Zur Bewältigung dieser komplexen Aufgabe wurde ein systematischer Prozess durchlaufen. Zu Projektbeginn wurden gemeinsam mit dem KIT zwei vielversprechende Kanalcode-Kandidaten identifiziert: Polarcodes und LDPC-Codes. Die Bewertung erfolgte vor dem Hintergrund der anspruchsvollen Anforderungen eines Kanals mit einem SNR von bis zu -20 dB, einer Ratenadaption in 5-dB-Schritten und einer Ziel-Datenrate von über 1 Gbit/s. Bei der Untersuchung der Polarcodes zeigte sich, dass zwar eine gute Ratenadaption möglich war, die voraussichtliche Kommunikationsperformance und insbesondere die Implementierbarkeit eines Decoders mit hohem Durchsatz jedoch problematisch waren. Daher wurde diese Codeklasse verworfen.

Die Untersuchung der LDPC-Codes erwies sich hingegen als vielversprechend, sowohl in theoretischer Hinsicht als auch bezüglich der Architektur. Es wurden Codeparameter spezifiziert, darunter ein maximaler Check-Node-Degree von 6, eine minimale Coderate von 1/100, eine Blockgröße von 100.000 Bits und eine LLR-Eingangsbreite von 8 Bit. Auf dieser Grundlage wurden bitgenaue Softwaremodelle von Encoder und Decoder entwickelt, um die Auswirkungen der Quantisierung auf die Performance genau zu bewerten. In enger, iterativer Zusammenarbeit mit dem KIT wurden die Modelle optimiert, wobei Techniken zur Komprimierung interner Werte und eine spezielle Abarbeitungsreihenfolge (Layered Decoding) implementiert wurden. Diese Architektur halbiert die Dekodierlatenz und erhöht so den Durchsatz. Zusätzlich wurde eine Logik zur vorzeitigen Erkennung korrekt decodierter Codewörter integriert, was die Latenz weiter verringert.

Um die geforderte theoretische Analyse der Architekturen quantitativ zu untermauern, wurden die Kandidaten hinsichtlich ihrer erwarteten Ressourcennutzung (Logikzellen, Speicherbandbreite) und ihrer erreichbaren Taktfrequenz bewertet. Für die simulative Untersuchung wurde der entwickelte Software-Encoder mit einer Zufallszahlenquelle als Datenquelle verbunden. Die Daten wurden durch ein Kanalmodell (additives weißes Gaußsches Rauschen, AWGN) geschickt und anschließend vom bitgenauen Decoder verarbeitet. Diese Langzeitsimulationen, durchgeführt mit umfangreichen Zufallsdaten, dienten der Bewertung der Bitfehlerrate (BER) und bestätigten die funktionale Korrektheit der Architekturen.

Die darauf folgende Hardwareimplementierung des LDPC-Decoders auf der RFSoc-Plattform zeigte, dass das System grundsätzlich funktionsfähig ist, jedoch der angestrebte Durchsatz von 1 Gbit/s mit einer einzelnen Instanz nicht erreicht wird. Eine Analyse alternativer Plattformen ergab, dass durch die parallele Instanziierung von vier Decodern auf einer Xilinx Versal-Plattform der Ziel-Durchsatz erreicht werden könnte. Da die ursprünglichen Simulationsergebnisse noch nicht zufriedenstellend waren und die Implementierung auf der RFSoc-Plattform die Leistungsanforderungen nicht vollständig erfüllte, wurden im weiteren Projektverlauf gemeinsam mit dem KIT angepasste Codes entwickelt

und simuliert. Dies führte zur Erstellung von drei neuen Hardwarearchitekturen für die Fehlerkorrektur, von denen im nachfolgenden Kapitel diskutiert werden

Zusammenfassend lässt sich festhalten, dass die gestellte Aufgabe – die Evaluierung von Codeverfahren und die Auswahl einer finalen Hardwarearchitektur – durch einen gründlichen Analyse- und Simulationsprozess erfolgreich abgeschlossen wurde. Als Ergebnis wurde die Klasse der LDPC-Codes als geeignet identifiziert, und es wurde eine optimierte Decoder-Architektur (Layered Decoder mit Early Termination) definiert. Die finale Auswahl fiel auf die LDPC-basierte Architektur, da sie sich in der Simulation als robust erwiesen hat und die beste Balance aus Performance, Implementierbarkeit und Komplexität bietet. Die daraus resultierenden Architekturen bilden eine solide Grundlage für die weitere Implementierung, wobei die Diskussion über die optimale Zielplattform zur Erreichung des Enddurchsatzes im Konsortium fortgeführt wurde.

über die definierten Schnittstellen vorgesehen. Die Ziele waren die Implementierung der FEC-IP-Cores und deren Integration in das Gesamtsystem.

Zur Erreichung dieser Ziele wurden die Arbeiten in mehreren Schritten durchgeführt. Zunächst wurde ein alleinstehender Demonstrator aufgebaut, der die Komponenten für Fehlerkorrektur (FEC) und Reverse Reconciliation (RR) vereint. Für die Reverse Reconciliation wurden, basierend auf einem Entwurf von ADVA, mehrere optimierte Implementierungsgenerationen entwickelt, die insbesondere den kritischen Speicherverbrauch adressierten. Die vollständige RR-Logik wurde erfolgreich auf einem FPGA implementiert und getestet, wie die Flächendaten (Alice) und (Bob) zeigen. Diese Implementierung bildete die Grundlage für die spätere Systemintegration.

Im Zentrum der Arbeiten stand die Implementierung der FEC-IP-Cores. Basierend auf den Ergebnissen der vorangegangenen Arbeiten wurden zwei Decoder-Architekturen (Variante 1 und Variante 2) in Hardware umgesetzt und in den Demonstrator integriert. Die Verifikation der IP-Cores gegen die bitgenauen Softwaremodelle erfolgte durch umfangreiche Co-Simulationen, bei denen die Eingangs- und Ausgangsdaten von Hardware- und Softwaremodell verglichen wurden, um die funktionale Korrektheit der Implementierung sicherzustellen. Die Implementierungsdaten zeigten, dass Decoder-Variante 1 für die angestrebte Zielhardware zu ressourcenintensiv war und daher nur auf einer leistungsfähigeren, bei Creonic vorhandenen Plattform evaluiert werden konnte. Aus diesem Grund wurde die Entscheidung getroffen, Variante 2 für die finale Integration zu verwenden, da sie trotz geringerer Komplexität eine höhere interne Auflösung bot und mehr Iterationen zuließ, was aus kommunikationstechnischer Sicht vorteilhafter ist.

Um die Voraussetzungen für die kollaborative Arbeit im Konsortium zu schaffen, wurde eine erste Datenschnittstelle auf Basis des gRPC-Protokolls implementiert. Obwohl deren Durchsatz für den finalen Demonstrator limitiert ist, ermöglichte sie eine effektive parallele Entwicklung und Tests mit den Projektpartnern.

Abschließend wurde der finale Gesamtdemonstrator in Zusammenarbeit mit allen Projektpartnern aufgebaut. Dabei wurden die entwickelten Komponenten – der LDPC-Encoder, der LDPC-Decoder und die Reverse-Reconciliation-Logik – erfolgreich mit den Partnerkomponenten von ADVA und KIT integriert. Die definierten Schnittstellen erwiesen sich als funktional und robust. In mehreren Testkampagnen wurde der Demonstrator unter Echtzeitbedingungen erfolgreich erprobt. Dabei konnte die korrekte Funktionsweise des Gesamtsystems nachgewiesen werden, insbesondere die zuverlässige Fehlerkorrektur auch bei den geforderten extrem niedrigen Signal-Rausch-Verhältnissen (SNR) von bis zu -20 dB.

Zusammenfassend lässt sich festhalten, dass die wesentlichen Aufgaben dieses Arbeitspakets erfolgreich abgeschlossen wurden. Die IP-Cores für Encoder und Decoder wurden implementiert, verifiziert und in einen funktionsfähigen, alleinstehenden Demonstrator integriert. Die Krönung der Arbeiten war der erfolgreiche Aufbau und Test des finalen Gesamtdemonstrators, der das Potential der Projektergebnisse in einer Echtzeitumgebung unter Beweis stellte. Somit sind die Ziele – die Implementierung der IP-Cores und deren Integration in das Gesamtsystem – vollständig erreicht worden. Die Entscheidung für die ressourcenschonendere Decoder-Variante 2 trug maßgeblich zum Erfolg bei und ermöglichte einen stabilen Betrieb innerhalb der Systemanforderungen.

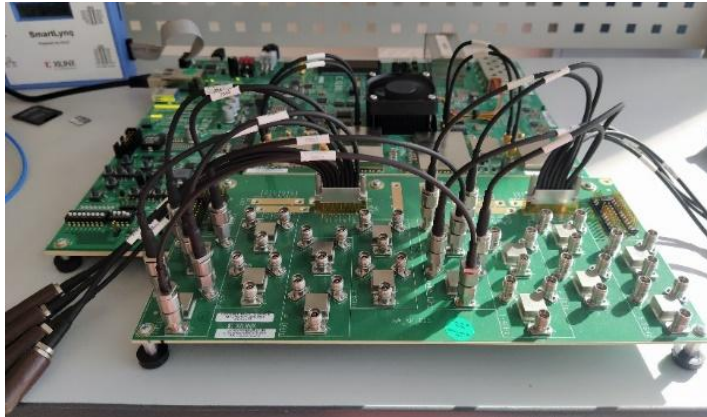


Abbildung 2 Encoder und Decoder Hardwareplattform

4 Voraussichtlicher Nutzen

Die Demonstration des Übertragungssystems wird als vertrauensbildende Maßnahme potentiellen Kunden präsentiert. Der fertiggestellte Demonstrator zur drahtlosen Übertragung stellt eine gute Möglichkeit dar, potentiellen Kunden die Leistungsfähigkeit der Produkte von Creonic zu zeigen.

Die Demonstration des Übertragungssystems wird als vertrauensbildende Maßnahme potentiellen Kunden präsentiert. Erste Kunden wären 2027 mit einem Produkt denkbar. Weitere Testaufbauten sind notwendig um kundenspezifische Anforderungen zu erproben.

5 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Ähnliche Aufbauten wurden im Rahmen anderer Forschungsprojekte auf-gebaut, welche insbesondere bei drahtloser Kommunikation über Satelliten erprobt werden. Dies liegt im Kerngeschäftsfeld von Creonic und wird hier weiter verfolgt.

6 Veröffentlichungen

Im Rahmen des Projektes wurden von Creonic keine Veröffentlichung gemacht.