

CubEniK

Kurzbericht

Dok.-Nr.:	n/a
Ausgabe:	1
Ausgabedatum:	30.09.2024
Erstausgabe am:	30.09.2024

Erstellt:	Daniel Heinig	Datum/ Unterschrift:	Daniel Heinig <small>Digital unterschrieben von Daniel Heinig Datum: 2025.03.13 09:54:52 +01'00'</small>
Freigabe PM:	Dr. Erik Beckert	Datum/ Unterschrift:	Erik Beckert <small>Digital unterschrieben von Erik Beckert Datum: 2025.03.13 10:12:05 +01'00'</small>

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

INHALT	2
1 EINLEITUNG.....	3
2 ANWENDBARE DOKUMENTE	3
3 ABKÜRZUNGEN UND AKRONYME	3
4 URSPRÜNGLICHE AUFGABENSTELLUNG	4
5 TECHNISCHER STAND, AN DEN ANGKNÜPFT WURDE.....	4
6 ABLAUF	5
7 ERGEBNISSE	6
8 ZUSAMMENARBEIT MIT ANDEREN EINRICHTUNGEN.....	7

1 EINLEITUNG

Dieser Bericht umfasst die gesamte bisherige Laufzeit des Projekts CubEniK (CubeSat Demonstration of Entangled Photon Pair Key Distribution) von 02/2022-03/2024. Er gliedert sich in zwei Teile nach NKBF 98:

Teil I: Kurzbericht (dieses Dokument)

Teil II: Eingehende Darstellung (AD-1)

Als dritten Teil wird dem Zuwendungsgeber der Erfolgskontrollbericht als separates Dokument zugänglich gemacht, ist aber nicht Teil dieser Veröffentlichung.

Teil I fasst die ursprüngliche Aufgabenstellung sowie den wissenschaftlichen und technischen Ausgangsstand, den Ablauf des Vorhabens und die wesentlichen Ergebnisse sowie die Zusammenarbeit mit anderen Einrichtungen zusammen.

2 ANWENDBARE DOKUMENTE

Dieses Dokument ist in Verbindung mit den nachfolgend aufgeführten Dokumenten zu lesen, die in dem hier angegebenen Umfang Bestandteil dieses Dokuments sind.

AD	Dokument Nr.	Ausgabe	Ausgabe- datum	Titel
AD-1	n/a	1	30.09.2024	Teil II – Eingehende Darstellung

3 ABKÜRZUNGEN UND AKRONYME

Abkürzung	Bedeutung
AD	Anwendbare Dokumente
CubEniK	CubeSat Demonstration of Entangled Photon Pair Key Distribution
EPS	Entangled Photon Source – verschränkte Photonenquelle
IOF	Fraunhofer-Institut für Angewandte Optik und Feinmechanik
LEO	Low Earth Orbit – niedrige Erdumlaufbahn
n/a	nicht anwendbar
ND	Normatives Dokument
QKD	Quantum Key Distribution - Quantenschlüsselverteilung
RD	Referenzierte Dokumente

4 URSPRÜNGLICHE AUFGABENSTELLUNG

Das Projekt CubEniK hat sich das Ziel gesetzt, Quantenschlüsselverteilung (QKD) mit verschränkten Photonen mit Hilfe eines CubeSats in einem Low Earth Orbit (LEO) zu demonstrieren und einen ersten nationalen QKD-Link zwischen zwei Standorten für den mindestens sechsmonatigen Betriebszeitraum zu realisieren. Im Rahmen der Untersuchungen und Entwicklungsarbeiten erfolgt ebenfalls eine Charakterisierung möglicher Schlüsselraten und die Ableitung entsprechender QKD-Netzwerkarchitekturen. Die gesamte CubEniK-Mission soll damit den ersten Schritt in Richtung Realisierung eines QKD-Netzwerks via CubeSats sicherstellen.

Das Teilvorhaben des Fraunhofer IOF in den ersten beiden Phasen A/B des Gesamtvorhabens umfasste hierfür Zuarbeiten zu den Grundlagen für das Missionsdesign, zum vorläufigen Design der Space- und Ground-Segmente sowie zur Entwicklung von kritischen Komponenten und Sub-Systemen. Dabei wurden verschiedene technologische Fragen identifiziert, deren Klärung für die Fortsetzung des Projekts essentiell ist. Diese umfassen vor allem die Quelle der verschränkten Photonen mit ihrem Pumplaser QKD-Synchronisation und Polarisationskontrolle sowie das Pointing- und Trackingsystem. Im Rahmen einer Aufstockung wurden die technologischen Risiken für diese Schlüsselkomponenten minimiert und konkrete, technische Lösungen erarbeitet.

5 TECHNISCHER STAND, AN DEN ANGKNÜPFT WURDE

Es existieren bisher nur einige wenige QKD-Netzwerke, welche von Forschungsinstituten zu Testzwecken betrieben werden und die großteils auf dem Prepare-and-Measure QKD-Protokoll BB84 basieren. Im Gegensatz dazu fokussiert der technische Inhalt von CubEniK auf die Nutzung von verschränkten Photonenpaaren, basierend auf dem QKD-Protokoll „BBM92“.

Die Reichweite faserbeschränkter Netzwerke ist dabei beschränkt. Größere Entfernungen können mit satellitenbasierter QKD überbrückt werden. Projekte wie der chinesische Satellit MICIUS und Initiativen der ESA wie EAGLE 1 oder die Experimente des NUS in Singapor mit den Satelliten SpooQy-1 and SpooQy-2, sowie Kanadas QUEYSSat haben die Machbarkeit satellitenbasierter QKD untersucht. Alleinstellungsmerkmal von CubEniK wird die Dual-Downlink-Konfiguration sein. Damit passiert die Schlüsselerzeugung auf den Bodenstationen und es müssen keine sensiblen Daten oder Schlüssel auf dem Satelliten gespeichert werden. Der Satellit muss also kein vertrauenswürdiger Knoten im Kommunikationsnetz sein.

Im Rahmen der QuNET-Initiative hat das Fraunhofer IOF mit großes Wissen im Bereich der terrestrischen Freistrahl-QKD generiert. Zudem hat es Komponenten zu Missionen wie James Webb (<https://www.iof.fraunhofer.de/en/pressrelease/2021/james-webb-space-telescope-with-optics-from-jena.html>), JUICE (<https://www.iof.fraunhofer.de/de/presse-medien/pressemitteilungen/2023/juice-weltraummission-startet-mit-teleskop-aus-jena-zum-jupiter.html>) und ExoMars beigesteuert sowie eine spacetaugliche EPS entwickelt (<https://www.iof.fraunhofer.de/de/presse-medien/pressemitteilungen/2021/photronics-plus-2021.html>).

7 ERGEBNISSE

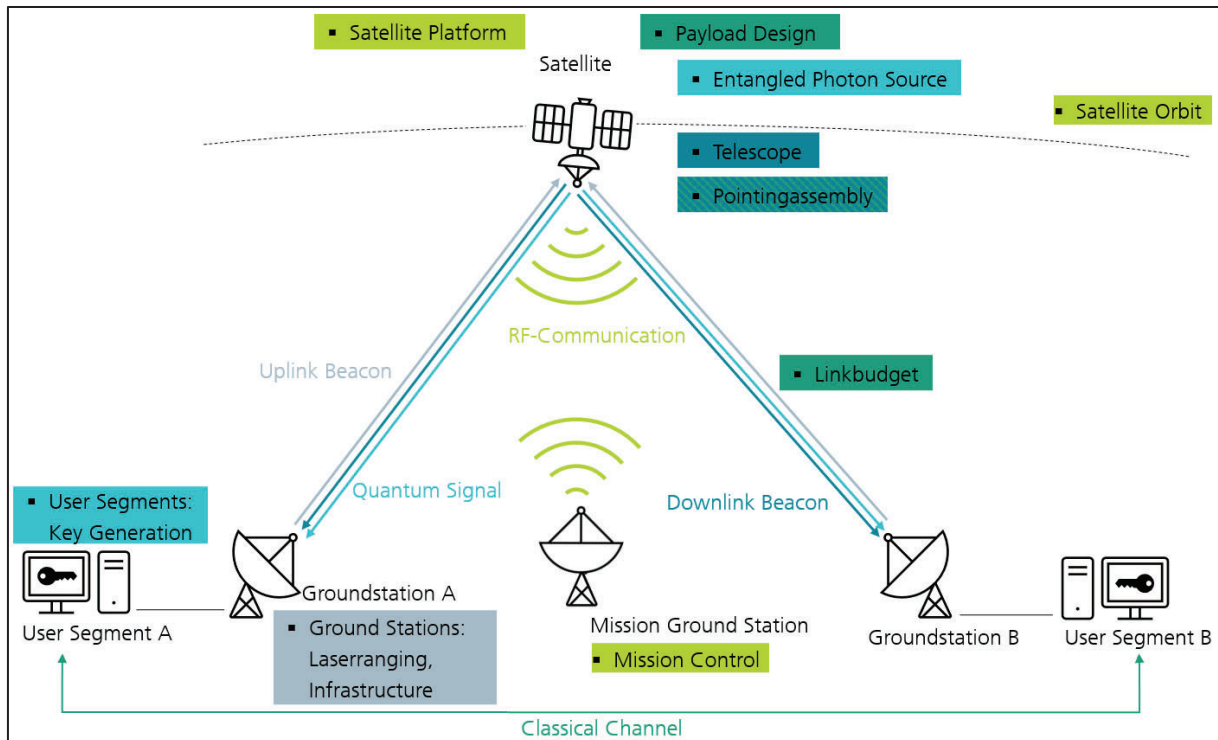


Abbildung 2: Systemübersicht CubEniK: von einem Satelliten werden verschränkte Photonen auf zwei Bodenstationen verteilt, die daraus den geheimen Schlüssel generieren.

Die Arbeiten wurden in einem Konsortium durchgeführt, in dem eine starke Zusammenarbeit zwischen den Projektpartnern gegeben war. Demzufolge sind viele Ergebnisse als gemeinschaftliche Errungenschaft zu betrachten. Es wird, soweit möglich, der jeweilige Anteil des IOF an den Ergebnissen hervorgehoben.

Zentrales Ergebnis ist das Missionsdesign (Übersicht in Abbildung 2) und ein vorläufiges Design einer optischen Payload für die Quantenschlüsselverteilung (Abbildung 3). Die Rolle des IOF umfasste:

- Koordination und System Engineering der Entwicklung
- Optikdesign
- Mechanikdesign
- Design der Regelung für Coarse- und Finepointing
- Dispersionskorrektur am Risley-Prisma
- QKD-System

Die detaillierten technischen Ergebnisse werden in Teil 2 eingehend dargestellt.



Abbildung 3: links: vorläufiges Design der optischen Payload zur Dual-Downlink-Quantenschlüsselverteilung. Rechts: Optische Payload in 16U-Envelope.

Basierend auf den Ergebnissen wurde die weitere Roadmap wie folgt entschieden:

- Bau von EQM der optischen Payload und EPS und Laser. Folgeantrag gestellt mit Beginn Dezember 2024
- Konkretes Payloaddesign als Basis für weitere Zusammenarbeit mit Plattform-Prime

8 ZUSAMMENARBEIT MIT ANDEREN EINRICHTUNGEN

Das Projekt wurde in Zusammenarbeit mit folgenden Partnern bearbeitet:

- Quantum Optics Jena GmbH
- SPACEOPTIX GmbH
- Zentrum für Telematik e.V.
- DiGOS Potsdam GmbH

Ende des Dokuments

CubEniK

Schlussbericht

Dok.-Nr.:	n/a
Ausgabe:	1
Ausgabedatum:	30.09.2024
Erstausgabe am:	30.09.2024

Erstellt:	Daniel Heinig	Datum/ Unterschrift:	Daniel Heinig Digital unterschrieben von Daniel Heinig Datum: 2025.03.13 09:56:31 +01'00'
Freigabe PM:	Dr. Erik Beckert	Datum/ Unterschrift:	Erik Beckert Digital unterschrieben von Erik Beckert Datum: 2025.03.13 10:12:39 +01'00'

Gefördert durch:



Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

INHALT	2
1 EINLEITUNG.....	3
2 ANWENDBARE DOKUMENTE	3
3 ABKÜRZUNGEN UND AKRONYME	4
4 EINGEHENDE DARSTELLUNG DER GELEISTETEN ARBEIT	5
4.1 MISSIONSANALYSE	6
4.1.1 Link Budget.....	6
4.1.2 Satellitenstruktur	6
4.1.3 Update Missionsziel	7
4.2 PAYLOADDESIGN.....	7
4.2.1 Konzept Payload.....	8
4.2.2 Design Terminal.....	9
4.2.3 Tracking/Pointing.....	9
4.2.4 Achromatisierung Risley-Prismen	12
4.2.5 QKD-System.....	13
4.2.6 Wellenlängenstabiler Pumplaser	20
5 ZUSAMMENFASSUNG UND AUSBLICK	22
6 LITERATURVERZEICHNIS.....	22

1 EINLEITUNG

Dieser Bericht umfasst die gesamte bisherige Laufzeit des Projekts CubEniK (CubeSat Demonstration of Entangled Photon Pair Key Distribution) von 02/2022-03/2024. Er gliedert sich in zwei Teile nach NKBF 98:

Teil I: Kurzbericht (AD-6), gesondertes Dokument

Teil II: Eingehende Darstellung.

Als dritten Teil wird dem Zuwendungsgeber der Erfolgskontrollbericht als separates Dokument zugänglich gemacht, ist aber nicht Teil dieser Veröffentlichung.

2 ANWENDBARE DOKUMENTE

Dieses Dokument ist in Verbindung mit den nachfolgend aufgeführten Dokumenten zu lesen, die in dem hier angegebenen Umfang Bestandteil dieses Dokuments sind.

Es ist zu beachten, dass alle in den Dokumenten aufgeführten Anforderungen anwendbar sind, sofern nicht anders vermerkt oder Ausnahmen festgelegt und vereinbart wurden.

AD	Dokument Nr.	Ausgabe	Ausgabe- datum	Titel
AD-1	CubEniK-AN-001	1	28.06.2022	CubEniK: Missionsanalyse
AD-2	CubEniK-IOF-SPE-0001	1	31.05.2022	CubEniK: Systemspezifikationen
AD-3	CubEniK-IOF-SDD-0001	1	17.10.2022	CubEniK: System Design Document
AD-4	CubEniK-IOF-BAR-0001	1	03.04.2023	CubEniK: Breadboard Activities Report
AD-5	CubEniK-DIG-QKD-OGS-PDD-1.0	1	03.04.2023	QKD OGS Preliminary Design
AD-6				Kurzbericht

3 ABKÜRZUNGEN UND AKRONYME

Abkürzung	Bedeutung
AD	Anwendbare Dokumente
CP	Coarse Pointing
EPS	Entangled Photon source
FP	Fine Pointing
FSM	Fast-Steering-Mirror
HIL	Hardware-In-The-Loop
IOF	Fraunhofer-Institut für Angewandte Optik und Feinmechanik
n/a	nicht anwendbar
μC	Micro-Controller
ND	Normatives Dokument
PSD	Position-Sensitive-Device
RD	Referenzierte Dokumente
RSP	Risley-Prismen-Scanner
SKR	Secure Key Rate

4 EINGEHENDE DARSTELLUNG DER GELEISTETEN ARBEIT

In diesem Kapitel werden die im Rahmen des Vorhabens durchgeführten Arbeiten ausführlicher dargestellt, insbesondere im Vergleich zur ursprünglichen Vorhabenbeschreibung. Für einen Projektüberblick sei hier auf AD-6 (Kurzdarstellung) verwiesen, um Doppelungen zu vermeiden. Die Arbeit des IOF fokussiert sich auf das Missionsdesign und besonders die Payload des Space Segments. Ground Segment und Space Segment Platform wurden im Wesentlichen von den Partnern Digos und Zentrum für Telematik getragen.

In der Anfangsphase wurde primär eine Missionsanalyse durchgeführt, um die Mission zu definieren und die technischen Lösungsräume einzugrenzen. Aufgrund des Neuheitswertes der Mission und der geringen Anzahl vergleichbarer Missionen, kann nur begrenzt auf Erfahrungen und "Best Practices" zurückgegriffen werden. Der Lösungsraum war also zu Beginn sehr weit. Mithilfe von aufgestellten (Link-, Volumen-, Masse-, Energie-) Budgets und Trade-off-Analysen wurden Parameter wie Wellenlänge, Orbit, Teleskopdurchmesser, Plattformgröße und die Payloadarchitektur eingegrenzt. Der Prozess wurde dem DLR kontinuierlich kommuniziert und ist in AD-1 bis AD-5 dokumentiert. Aus diesem Grund wird hier im Wesentlichen eine Ergebniszusammenfassung präsentiert, um den Umfang des Dokumentes in den geforderten Grenzen zu halten. Insbesondere bei Abweichungen von der ursprünglichen Vorhabenbeschreibung wird der Entscheidungsprozess kurz erläutert.

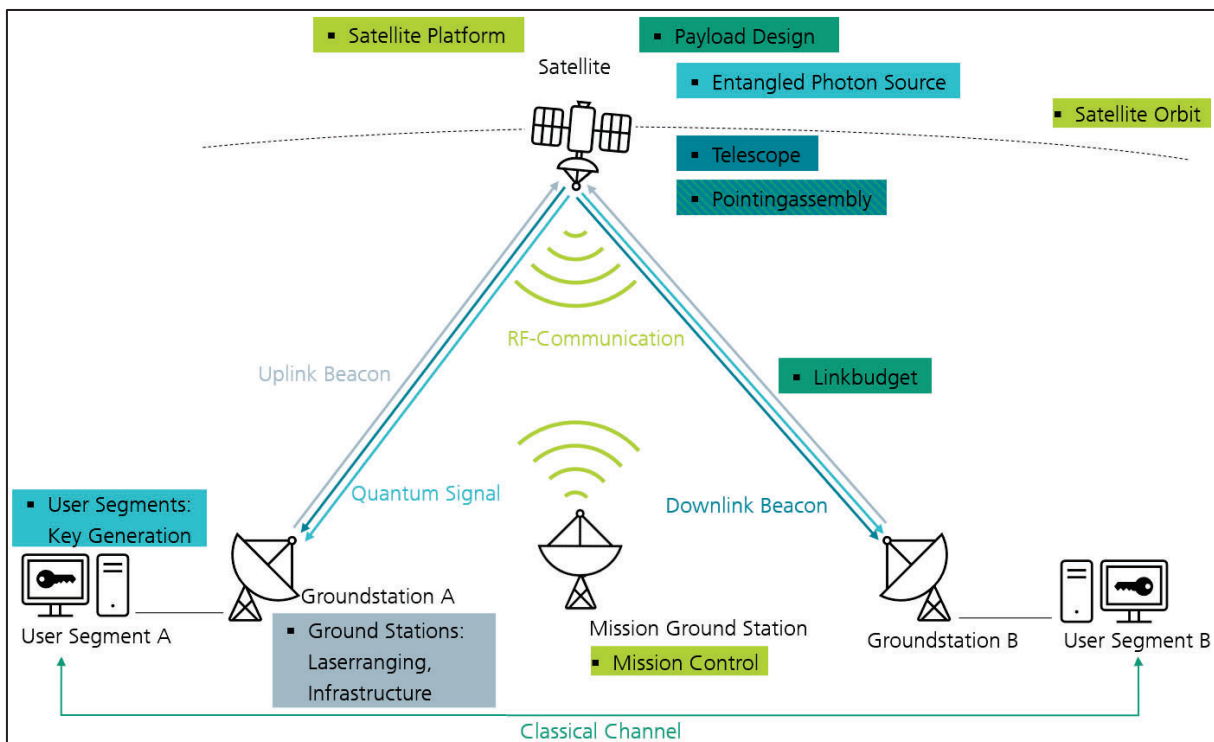


Abbildung 1: Systemübersicht CubEniK: von einem Satelliten werden verschränkte Photonen auf zwei Bodenstationen verteilt, die daraus den geheimen Schlüssel generieren.

4.1 Missionsanalyse

4.1.1 Link Budget

Das Linkbudget stellt eine Berechnung der Verluste und Gewinne im gesamten Pfad zwischen Photonenquelle und Schlüsselerzeugung dar. Es erlaubt eine Abschätzung der erzeugten Menge abhörsicherer Schlüssels. Dafür wurden entsprechende Softwaretools entwickelt.

Das Linkbudget hängt unter anderem ab von:

- Orbit
- Teleskopapertur (Space und Ground)
- Wellenlänge
- Restfehler Lageregelung und Pointing/Tracking

Da die Entfernung zwischen Satellit und Bodenstation sich im Verlauf der Umlaufbahn ändert und die Verluste auf beiden Armen voneinander abhängig sind, wurde das Budget anhand von vom ZfT berechneten realitätsnahen Orbitdaten simuliert. Auf diese Weise konnte die erzeugbare Schlüsselmenge betrachtet werden. Mit dem Ziel, einen Schlüssel von 256 bit Länge pro Überflug zu generieren, wurden folgende Rahmenanforderungen ermittelt:

- Orbit: LEO
- Teleskopapertur Space: 80 mm
- Teleskopapertur Ground: 800 mm
- Wellenlänge: 810 nm
- Gesamt-Restfehler Lageregelung und Pointing/Tracking: 1 urad

Die Anforderungen stellen den in unseren Augen besten Kompromiss zwischen Linkbudget und anderer Einschränkungen wie technischer Machbarkeit und Platzbedarf dar.

4.1.2 Satellitenstruktur

In der GVB wurde ein zweiteiliger Satellit mit motorisiertem Gelenk vorgeschlagen, um dem sich im Orbit verändernden Winkel zwischen den Bodenstationen zu folgen. Es hat sich gezeigt, dass die zu erwartenden Restfehler der Lageregelung nicht allein mit dem Finepointing ausgleichbar sind, wenn gleichzeitig eine hohe Genauigkeit gefordert ist. Ein Coarsepointingsystem ist also unumgänglich, welches auch sich verändernden Winkel abdecken kann. Das motorisierte Gelenk ist damit obsolet.

4.1.3 Update Missionsziel

Projektziel laut GVB war, Quantenschlüsselverteilung (QKD) mit verschränkten Photonen mit Hilfe eines CubeSats in einem Low Earth Orbit (LEO) zu demonstrieren und einen ersten nationalen QKD-Link zwischen zwei Standorten für den mindestens sechsmonatigen Betriebszeitraum zu realisieren. Es wurde von einer üblichen Plattformgröße von etwa 6 U ausgegangen. Die Missionsanalyse hat gezeigt, dass dieses Ziel nicht erreichbar ist. Die gewählte Teleskopapertur von 80 mm stellt den in unseren Augen besten Kompromiss zwischen Linkbudget und anderer Einschränkungen wie technischer Machbarkeit und Platzbedarf dar.

Außerdem wurde ein zweiteiliger Satellit mit motorisiertem Gelenk vorgeschlagen, um dem sich im Orbit verändernden Winkel zwischen den Bodenstationen zu folgen, was sich als technisch nachteilig herausgestellt hat. Das Missionsstatement wird daher angepasst.

Ziel des Projektes CubEniK ist die Entwicklung und Qualifizierung eines Engineering-Qualification-Modells einer kompakten Payload für die Dual-Downlink-QKD. Dazu wird vorerst die Eignung verfügbarer Terminals untersucht. Bei Nichteignung wird auf das vorhandene Doppelteleskopdesign zurückgegriffen.

4.2 Payloaddesign

Folgende Analysen wurden durchgeführt:

- Benötigte Komponenten
- Bauraum
- Volumen
- Energiebedarf

Auch wenn diese Iterationen nur eine vorläufige Analyse darstellen und mit steigender Detaillierung reiteriert werden müssen, geben sie eine Mindestschranke für die Plattformgröße von 16 U vor.

Basierend auf diesen Analysen wurde ein vorläufiges Modell der optischen Payload erstellt, das im Folgenden näher beschrieben wird.

4.2.1 Konzept Payload

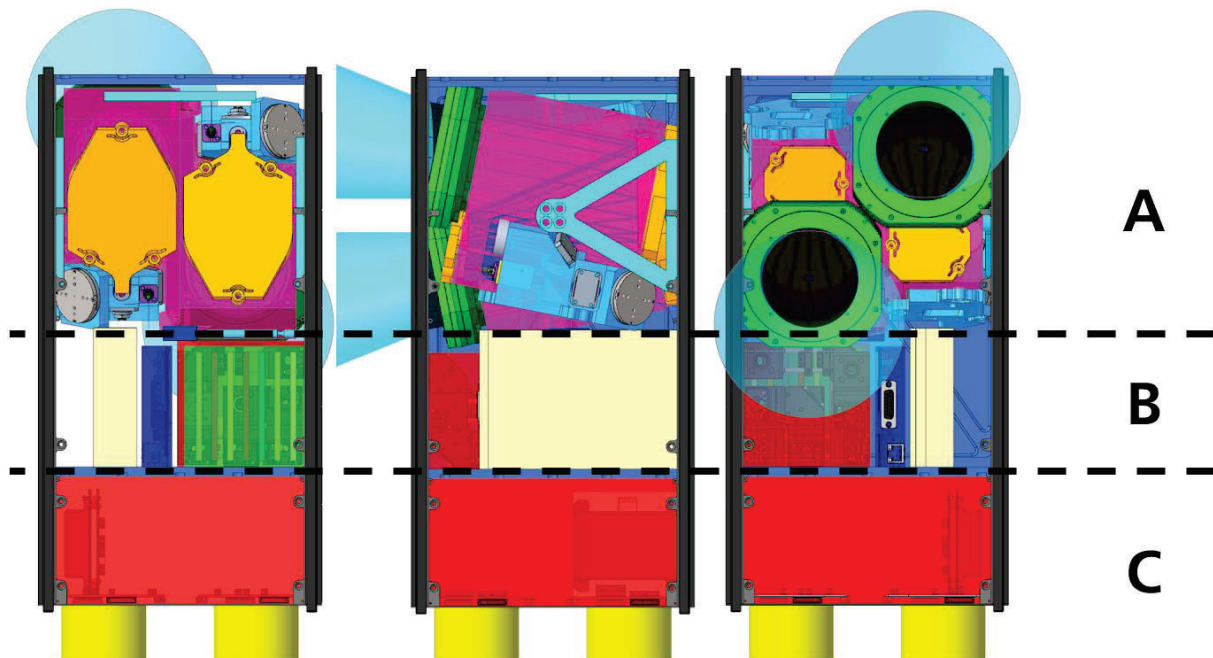


Abbildung 2: Der Entwurf kann in drei Teile unterteilt werden: optische Nutzlast (A), elektronische Nutzlast (B), Plattform (C).

Die Payload gliedert sich in zwei Teile (Abbildung 2):

1. Optische Payload
2. Elektronische Payload

Die Entwicklung fokussierte sich auf die optischen Payloadkomponenten, schematisch dargestellt in Abbildung 3.

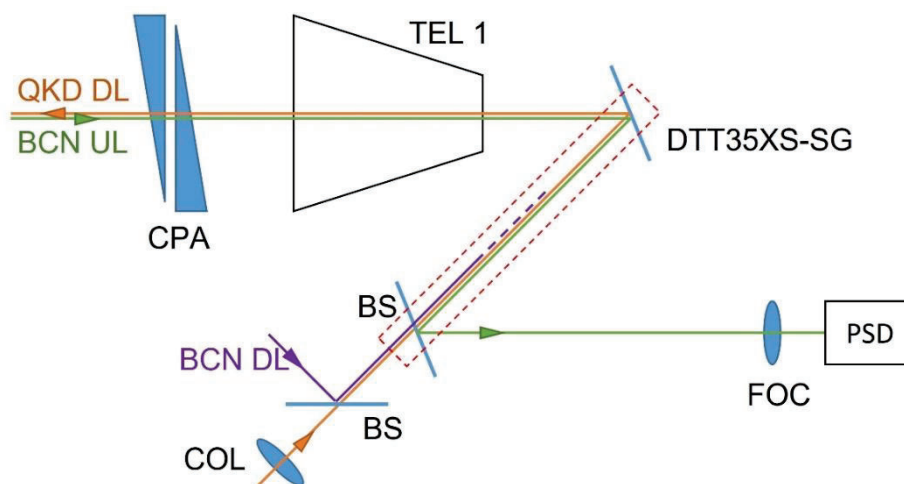


Abbildung 3: optischer Strahlengang der Baugruppe. Das DTT35XS-SG bezieht sich auf den gewählte FSM.

Die elektronische Payloadkomponenten sind als Volumenmodelle dargestellt, da das endgültige Design noch nicht zur Verfügung stand. Sie werden durch vergleichbare Bauteile angenähert, um Schätzungen für Volumen und Energiebedarf zu erhalten.

4.2.2 Design Terminal

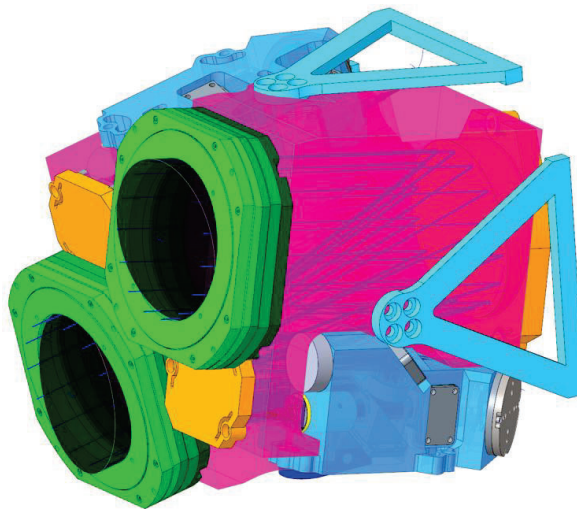


Abbildung 4: vorläufiges Design der optischen Payload. Grün: Rotationsantriebe der Risley-Prismen. Pink: modifizierter Grundkörper der Spaceoptix-Teleskope. Orange: Spiegel der SpaceOptix-Teleskope. Blau: Folgeoptikblock.

Basierend auf den Anforderungen der Missionsanalyse wurde ein vorläufiges Design der optischen Payload erstellt (Abbildung 4). Die Basis bilden zwei obstruktionsfreie Metallspiegelteleskope des Konsortialpartners Spaceoptix mit einer Apertur von 80 mm. An dessen Struktur sind Änderungen nötig, um die anderen Komponenten aufzunehmen. Das sind zum einen die Risleyprismen, zum anderen die er Folgeoptikblock mit Finepointing, Faserkopplung sowie Strahlkombination.

4.2.3 Tracking/Pointing

Für das Pointing der optischen Terminals wurde sich für eine Kombination aus Coarse-Pointing (CP) mittels Risley-Prismen-Scanner (RPS) und Fine-Pointing (FP) mittels Fast-Steering-Mirror (FSM) entschieden. Die Pointing-Regelung soll auf einem Micro-Controller (μC) umgesetzt werden. Dafür ein vereinfachter Regelalgorithmus, für die Steuerung des Scanners umgesetzt und mit einer linearen Regelung des FSM kombiniert. Die Performance wurde in Simulationen und die Code-Ausführungszeiten auf μC -Hardware demonstriert [1]. Weiter wurde untersucht, wie alternative Steuerungskonzepte des RPS hinsichtlich ihrer Rechengenauigkeit und der Rechenzeit-Performance auf der Zielhardware diese Aufgabe bewältigen.

Dass vorher demonstrierte Verfahren wird im Folgenden als „Paraxiale Lösung“ bezeichnet, da es neben vielen Vereinfachungen vor allem auf der paraxialen Approximation der Prismen-Refraktion

beruht. Mit steigender Berechnungskomplexität wurden noch die „Two-Step Lösung“ [2] und ein auf dem „Newton-Verfahren“ beruhende iterative Lösung [3] untersucht.

In numerischen Simulationen wurden die erzielten Genauigkeiten untersucht, in dem eine Zielablenkung vorgegeben wurde. Die drei Verfahren errechneten die benötigten Stellwerte der Prismen und basierend auf diesen Ergebnissen wurde die realisierte Ablenkung errechnet. Der Vergleich zwischen Soll und Ist in Abbildung 5 dargestellt. Wie erwartet unterscheiden sich die Genauigkeiten zwischen den Methoden stark, um ca. einen Faktor 10 jeweils.

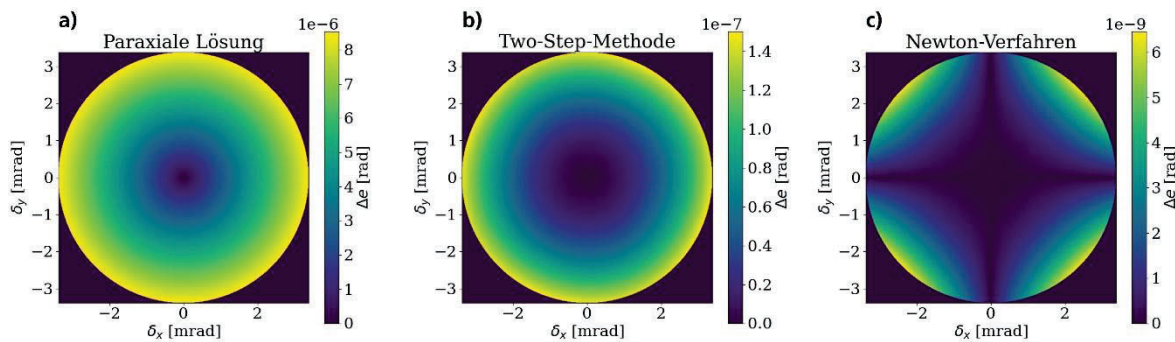


Abbildung 5: Open Loop Genauigkeiten der drei inversen Lösungen. Dargestellt ist die Abweichung zwischen Sollwert Vorgabe und erreichtem Istwert in der Simulation über die gesamten Verstellbereiche.

Für einen Vergleich auf der Zielhardware wurde ein Hardware-in-the-Loop (HIL) Modell umgesetzt. Dabei wurde ein als Controller agierender STM32 μ C mit einem Rechner und einem weiteren μ C verbunden. Der Rechner lieferte eine optische Simulation der Strahlablenkung durch den RPS und den FSM bis zur Detektion mit dem Position-Sensitive-Device (PSD). Der zweite μ C simuliert die zeitliche Impulsantworten der beteiligten Komponenten, um so realistischere Verzögerungen zwischen Steuerung und Umwelt zu implementieren. Der Aufbau ist in Abbildung 6 zu sehen.

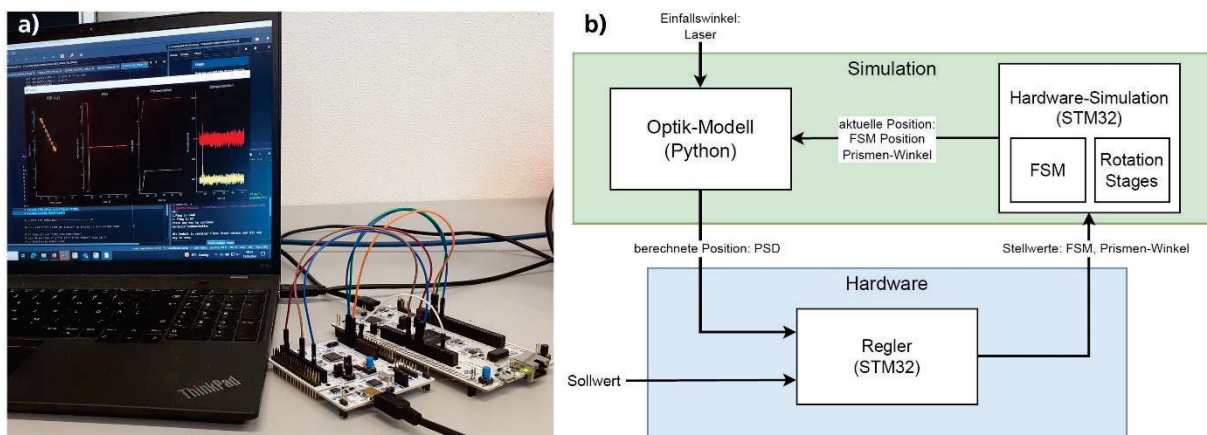


Abbildung 6: Foto des Hardware-In-The-Loop Aufbaus in a). Schematische Darstellung des Signalflusses in b).

Es zeigte sich, dass die erreichten Genauigkeiten in dieser Closed-Loop-Konfiguration nahezu gleich sind, wie die Simulation mehrerer Uplink-Beacon Akquisition-Szenarien in Abbildung 7

zeigt. Der zeitliche Verlauf einer solchen Akquisition ist in Abbildung 8 a) zu sehen. In Abbildung 8 b) ist ein Regelungsszenario zum Ausgleichen einer konstanten Winkel drift simuliert worden.

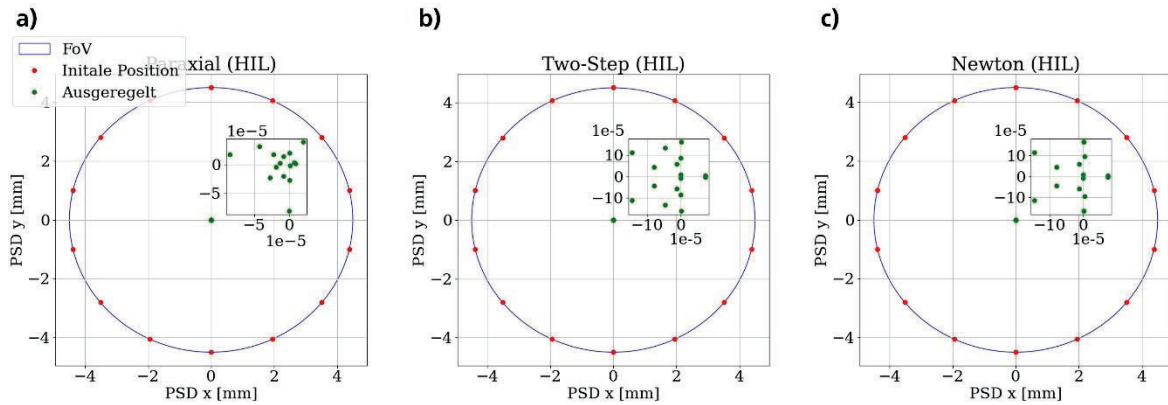


Abbildung 7: Simulierte ausgeregelte Beacon-Acquisitions-Szenarien im HIL-Setup. Die roten Punkte sind die initialen Detektionen in der Fläche des PSDs. Die grünen Punkte in der Zoom-Darstellung zeigen die ausgeregelten Positionen auf den PSDs.

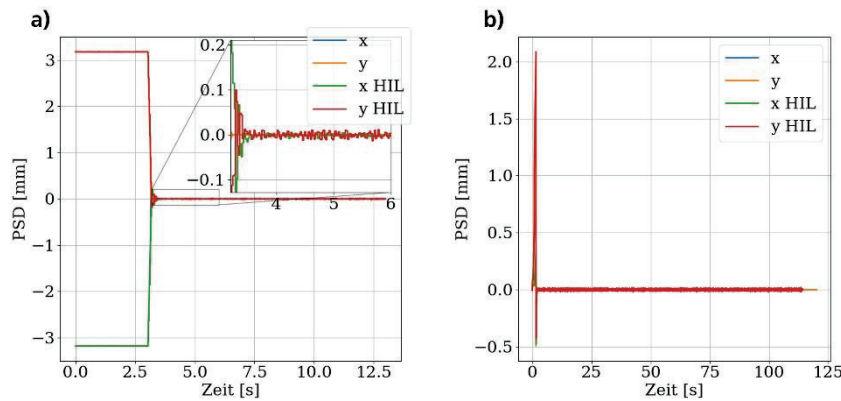


Abbildung 8: HIL-Simulation im Zeitverlauf für eine Beacon-Acquisition (a) und zum Ausgleichen einer gleichmäßigen Winkel drift (b). Die Winkelgeschwindigkeit in b) ist konstant 1,11 mrad/s.

Hardware	Paraxial Näherung	Two-Step-Methode	Newton-Verfahren
PC (Python)	2,81 μ s	20,04 μ s	36,47 μ s
STM32 (C++)	12 μ s	89 μ s	386 μ s

Tabelle 1: Rechenzeiten für eine inverse Lösung der Scannergleichungen.

Schließlich wurden die Verfahren auf dem bestehenden Laboraufbau umgesetzt. Die Regelung des RPS lief diesmal auf einem PC, da eine Ethernet-Verbindung zum Ansteuern der Rotations Stages nötig war. In der Abbildung 9 zeigt, sich das alle drei Verfahren im gleichen Genauigkeitsbereich einen Störung ausgleichen können. Der FSM hat dabei in Rechteckpulsen die Störungen induziert.

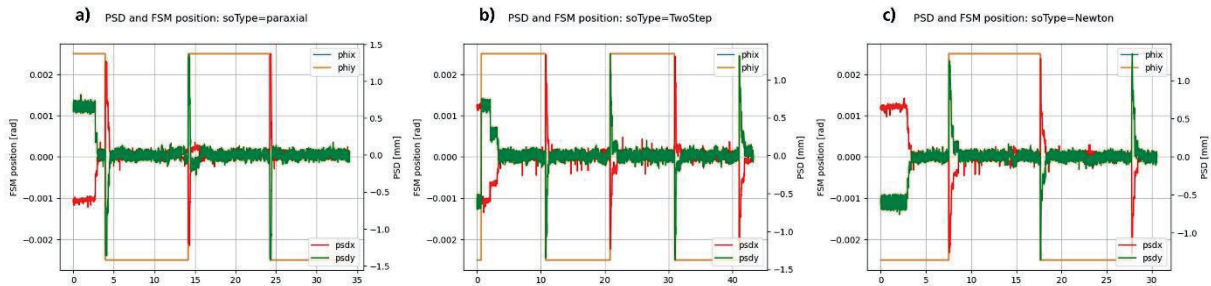


Abbildung 9: Ausregelung von Störimpulsen durch die CPA durch die drei beschriebenen Lösungsverfahren. Die FSM Kippwinkel (rechte Achse) erzeugen einen Störimpuls. Die Reaktion und Ausregelung der Spotposition auf dem PSD ist auf der linken Achse ablesbar.

Aktuelle Hardware-Einschränkungen der verwendeten seriellen Interfaces wie USB und Ethernet bestimmen im aktuellen Aufbau wesentlich die Verzögerungszeiten. Deshalb war eine Auswertung in der zeitlichen Performance auf den Vergleich der Code-Ausführungszeiten beschränkt, die in Tabelle 1 aufgelistet sind. Die erhöhte Genauigkeit der Berechnungen erhöhen die Rechenzeiten. Besonders auf der limitierten μC -Hardware. Im Gegenzug zeigt sich kein Gewinn in der tatsächlichen Regelung. Auch wenn auf eine Code Optimierung verzichtet wurde, zeigt sich ein wesentlich höheres Potential der Skalierbarkeit auf μC -Hardware mit der „Paraxialen Lösung“.

4.2.4 Achromatisierung Risley-Prismen

Im Rahmen des Projekts wurden verschiedene Achromatisierungsstrategien für Risley-Prismen untersucht. Bei den Betrachtungen wurden die sehr ambitionierten Anforderungen für die QKD-Signale zu Grunde gelegt, nämlich eine Winkeldispersion von ungefähr $1\mu\text{rad}$ über eine spektrale Mindestbandbreite von 30nm (Wellenlänge um 800nm) bei einem vollen Scanwinkel von 22° . Um potentiell weitere Signale zu übertragen, wurde nach Möglichkeiten einer Bandbreitenvergrößerung gesucht, wobei ein minimaler Bauraum angestrebt wurde. In der zweiten Spalte der Tabelle 2 sind als Vergleich einige Kenndaten eines Quarzglasprismas ohne Achromatisierung dargestellt. Trotz der sehr geringen Materialdispersion des Quarzglas sind Winkeldivergenzen von $1.3\text{e-}2^\circ$ weit jenseits der Systemanforderungen zu verzeichnen. Theoretische Minimaldicken eines Prismas betragen ca. 17mm (80mm Öffnung). Bei klassischen Achromatisierungen werden Gläser mit verschiedenen Brechzahlen und Materialdispersionen zu Prismendoublets geeignet kombiniert. Die aus dem Optikdesign bekannten Achromatisierungsregeln können nur sehr beschränkt angewendet werden, da bei den sehr harschen Winkeldispersionsanforderungen der Feldchromatismus großen Einfluss hat. Aus diesem Grund wurden nach einer ersten Glasvorauswahl eine Vielzahl von verschiedenen Materialkombinationen numerisch getestet. Die Kombination von Schwerflint- und Schwerekrongläsern zeigte sich als vorteilhaft, wobei das hochbrechende Material eingangsseitig zu verwenden ist. Ein typisches Beispiel mit einer Winkeldispersion von $5\text{e-}5^\circ$ ist in der 4. Spalte der Tabelle zu sehen. Um allerdings solche Winkeldispersionen in der Realität zu erreichen, müssen die Materialdispersionen extrem genau aufeinander abgestimmt sein.

Die Varianten 1, 3 und 4 werden hier aufgrund geplanter Schutzrechtsanmeldungen nicht detailliert beschrieben. Sie erlauben eine z.T. deutliche Reduktion der Prismendicke (Variante 1) oder der Dispersion (Variante 4). Im Folgeprojekt sollen derartige Prismen produziert werden, Veröffentlichungen sind in Folge geplant.

Tabelle 2: Eigenschaften von Risley-Scanner-Konfigurationen mit verschiedenen Achromatisierungsvarianten.

Typ	(0) Prisma	(1) Variante 1	(2) Prismen-doublet	(3) Variante 3	(4) Variante 4
Material-beispiel	Quarzgläser	-	N-PSK57 N-SF66	-	-
Prismen-winkel (max)	11.7°	-	14.2° (max.)	-	-
Min. Dicke	~17mm	~7mm/16mm	~20mm	~21mm	~21mm
Bandbreite	30nm	30nm	30nm	30nm	120nm
Divergenz	1.3 e-2°	3. e-4 / 8.e-5°	5.e-5°	3.e-5°	< 1.8 e-5°

4.2.5 QKD-System

Wir analysieren die Mission im Rahmen des BBM92-Protokolls. Dabei werden die Eigenschaften der Quantenverschränkung genutzt, um eine sichere Kommunikation zu ermöglichen (Abbildung 10). Eine Quelle erzeugt Paare verschränkter Photonen und sendet ein Photon von jedem Paar an zwei getrennte Parteien, die gemeinhin als Alice und Bob bezeichnet werden. Jede Partei wählt dann zufällig eine von zwei Polarisationsbasen aus, um ihre empfangenen Photonen zu messen, entweder geradlinig oder diagonal, ohne die andere Partei über ihre Wahl zu informieren. Nach den Messungen legen Alice und Bob öffentlich offen, welche Basis sie für jedes Photonenpaar verwendet haben. Sie behalten nur die Ergebnisse aus den Fällen, in denen sie zufällig die gleiche Basis gewählt haben, und verwenden diese korrelierten Ergebnisse, um einen gemeinsamen geheimen Schlüssel zu bilden. Die Verschränkung stellt sicher, dass die Messergebnisse korreliert sind, was inhärente Sicherheitsmerkmale bietet; jeder Abhörversuch würde die Verschränkung stören, was sich in erkennbaren Diskrepanzen in der Korrelation der Messergebnisse von Alice und Bob äußert. Diese Eigenschaft ermöglicht es den Parteien, die Sicherheit ihres Schlüssels zu überprüfen und die Anwesenheit eines Abhörers zu erkennen.

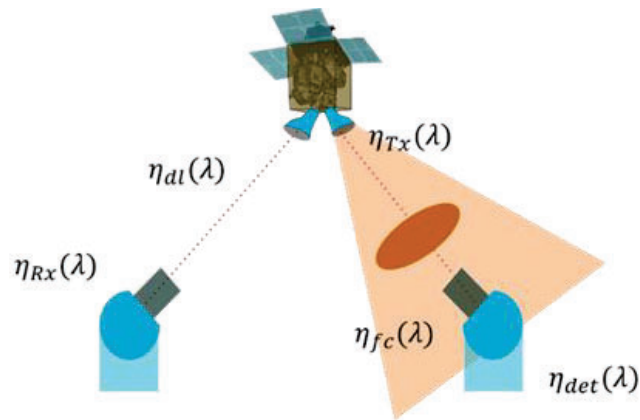


Abbildung 10: Dual-Downlink-QKD: der Wert η steht für den Verlustparameter für jeden Teil des Systems, dl: Downlink, Rx: Empfänger, Tx: Sender, fc: Faserkopplung, det: Detektor.

In Anlehnung an den Ansatz von Kržič et al. [4] wählen wir die Parameter entlang des Kommunikationskanals aus, die die Performance des QKD-Protokolls beeinflussen. Die Kommunikationspipeline ist in drei Hauptteile unterteilt (Tabelle 3):

- A) Satelliten-Parameter: Hier werden hauptsächlich die Verluste der Entangled Photon Source (EPS) bis zu den Emitter-Teleskopen erfasst.
- B) Parameter der Freiraumverbindung: Budget der Freiraumverbindung zwischen dem Satelliten und dem optischen Bodenempfänger.
- C) Interne Parameter der optischen Bodenstation: Dieser Abschnitt berücksichtigt die Verluste, die in der Empfangsoptik und der Detektionselektronik der OGS entstehen.

Tabelle 3: Linkbudget

Main Section	Parameters	Value
A	EPS intrinsic generation rate	Depending on mission requirements
	EPS intrinsic heralding	0,47 (for 1550 nm), 0,80 (for 810 nm)
	QKD baseline error rate	0,02
	Transmitter aperture diameter (m)	0,18
	Transmitter pointing jitter (s)	1,00E-06
	Transmitter optics transmittance	0,75
B	Zenith angle Alice (rad)	0,71612785
	Zenith angle Bob (rad)	0,71612785
	Satellite distance Alice (Km)	Depending on mission requirements
	Satellite distance Bob (Km)	Depending on mission requirements

	OGS altitude Alice	187,0
	OGS altitude Bob	579,0
	Atmospheric transmittance at zenith	0,783
	Background spectral radiance	100 (At night), 1,00E+06 (Day light with moderated intensity)
	Alice link loss	Depending on satellite distance
	Bob link loss	Depending on satellite distance
C	Detection time jitter per site (s)	1,50E-11 (for 1550 nm), 6,00E-11 (for 810)
	Coincidence window	5 * Detector jitter
	Dark count rate per detector	1,00 cps
	Detector efficiency (%)	> 80,00
	Detector dead time (s)	2,00E-10
	Error correction efficiency	1,22
	Coupling	SMF (day light), MMF (night-time)
	MMF core diameter (m)	30,00E-06
	MMF numerical aperture	0,275
	Receiver optics transmittance	0,75 (for 1550 nm), 0,60 (for 810 nm)
	Receiver AO correction level	Tip-tilt (MMF coupling), full (SMF coupling)
	Receiver aperture diameter (m)	0,8
	Receiver obscuration diameter	0,328
	Receiver spectral filter bandwidth (m)	3,00E-09

Die oben genannten Parameter sind das erforderliche Minimum, um die optimalen Werte für die asymptotische Secure Key Rate (SKR) und die Intrinsic Brightness der Entangled Photon Source (EPS) als optimale Schwellenwerte für die Mission zu ermitteln. Die aktuelle Mission ist für eine LEO-Umlaufbahn geplant. Das bedeutet, dass wir eine maximale Höhe von fast 1000 km und eine untere Grenze von ca. 200 km für diese Szenarien bei Nacht mit symmetrischer Position der OGS in Betracht ziehen sollten, und unter Verwendung der MMF-Kopplung können wir Folgendes schätzen (Tabelle 4):

Tabelle 4: Ergebnisse Linkbudget

Satellite distance Alice/Bob (Km)	222 Km		1022 Km	
EPS Wavelength (nm)	810	1550	810	1550
EPS intrinsic generation rate (pairs/s)	2,27167e+08	7,64114e+08	3,10697e+08	1,03655e+09
Alice/BOB link loss (dB)	-11,8	-15,0	-25,0	-28,3
Asymptotic SKR (bps)	1,01738E+05	2,776145E+04	285,95	77,23
QUBER (%)	5,427	5,682	5,780	5,782

Die hier geschätzten Werte stellen das Optimum unter den gegebenen Bedingungen dar. Wir haben einen maximalen Bedarf von 1,03 Gpairs/s für das EPS bis zu einer Entfernung von 1022 km von der OGS berechnet. Diese Berechnungen sind durch den derzeitigen Stand der Technik des OGS und der Detektoren begrenzt und könnten verbessert werden, wenn die technologischen Errungenschaften dies erlauben:

- Empfängerteleskope mit großen Aperturen
- Detektoren mit geringem Jitter und höherer Effizienz
- Verwendung niedrigerer Wellenlängen, um den Effekt der Divergenz zu verringern.
- Verschränkte Photonenquellen mit höherer intrinsischer Verkündigung.

4.2.5.1 Komplementäre Optimierungstechniken

Zusätzlich zur vorherigen Analyse evaluieren wir drei Techniken zur Erhöhung der Stabilität des EPS, die sich auf die passive Polarisationskontrolle und die Zeitsynchronisation in einem Szenario mit hohen Verlusten konzentrieren.

4.2.5.2 Passive Polarisationskompensation

Passive Kompensationsverfahren können eingesetzt werden, um die Polarisationswerte für einen Referenzlaser (der die spektrale Breite einer vorhandenen Quelle verschränkter Photonen nachbildet) beizubehalten, wobei eine Genauigkeit von über 98 % erreicht wird. Um dieses Ergebnis zu erreichen, wird ein Kompensationsprotokoll für die verschränkten Photonen abgeleitet. Dies gewährleistet eine hochgenaue Ausrichtung der Polarisation und Verschränkung,

die für eine effektive Quantenkommunikation entscheidend ist, insbesondere in Systemen mit CubeSats und kleinen Satelliten (Abbildung 11).

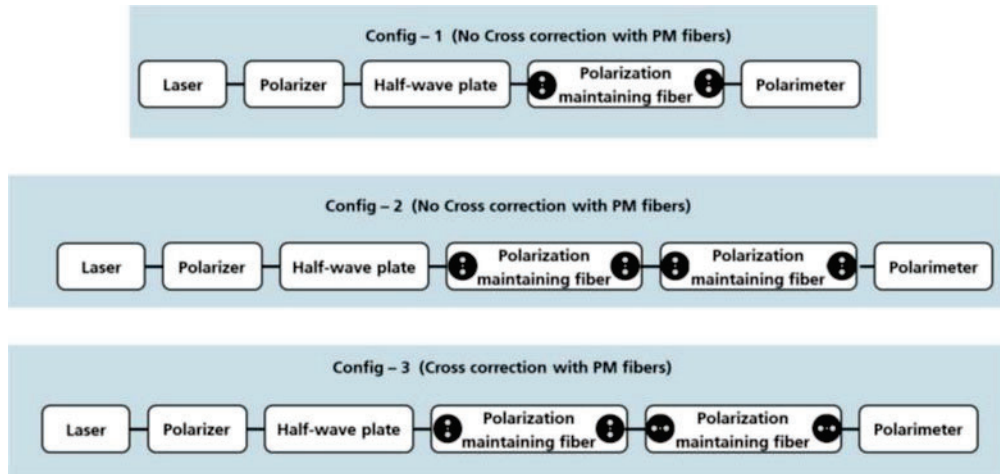


Abbildung 11: passive Polarisationskompensation

Als Referenzlichtquelle wird ein Laser verwendet, der die spektrale Breite der vorhandenen verschränkten Photonenquelle (EPS) nachbildet. Das Laserlicht durchläuft zunächst einen Polarisator, um die Reinheit des Zustands zu erhöhen und sicherzustellen, dass das Licht, das in die nachfolgenden Komponenten gelangt, eine klar definierte Polarisation aufweist. Dann trifft der Laser auf eine Halbwellenplatte, die die Polarisation um einen bestimmten Winkel dreht und eine Feinabstimmung auf die gewünschte Polarisationsbasis (HV oder DA) ermöglicht. Anschließend wird der Laser in eine polarisationserhaltende Faser eingekoppelt, die den Polarisationszustand bewahrt, indem sie die Auswirkungen der Doppelbrechung über lange Strecken für den H/V-Polarisationszustand minimiert. Schließlich wird der Laser durch ein Polarimeter geleitet, das den Polarisationszustand misst, um zu überprüfen, ob die Polarisationsausrichtung während des gesamten Aufbaus beibehalten wurde.

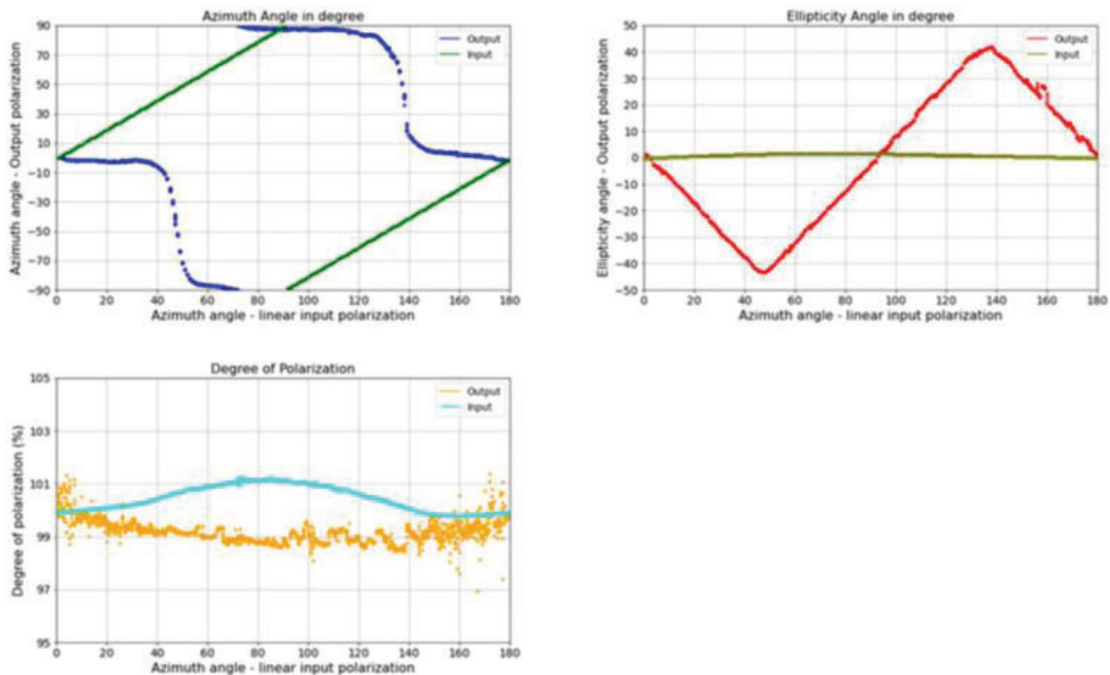


Abbildung 12: Ergebnisse Config-3: x-Achse - Azimutwinkel; (a) Eingangszimut; (b) Elliptizität; (c) Grad der Polarisation.

Insgesamt zeigte die Konfiguration 3 (Abbildung 12) im Vergleich zu den Konfigurationen 1 und 2 eine verbesserte Stabilität der Ausgangsmessungen, insbesondere in Bezug auf den azimutalen Winkel, die Elliptizität und den Grad der Polarisation. Die Kompensation durch die zweite Faser in Konfiguration 3 gleicht die Effekte einer falschen Polarisationsausrichtung effektiv aus, was zu einer größeren Messstabilität und Wiederherstellung der Kohärenz führt. Trotz der Beibehaltung der H/V-Polarisation in der Faser erfährt die D/A-Polarisation zusätzliche Phasenkomponenten, die eine zusätzliche Polarisationskompensation erforderlich machen, vor allem zur Phasenanpassung. Bei polarisationserhaltenden Fasern kann jedoch der Bedarf an einem komplexen Polarisationskorrekturmodul auf eine einfache Wellenplatte zur Phasenanpassung reduziert werden. Diese Reduzierung der Komplexität ist besonders für CubeSat-Anforderungen von Vorteil, bei denen Platz- und Gewichtsbeschränkungen kritische Faktoren sind. Alternativ kann die Korrektur auch auf der Bodenstation auf einfachere Weise durchgeführt werden.

4.2.5.3 Zeitsynchronisierung in einem Szenario mit hohen Verlusten

Wir implementieren einen Zeitstempel eines Pulsasers mit einer RR von 100 Hz über die Korrelationen einer verschränkten Photonenquelle (EPS) unter Verwendung des in Abbildung 13 dargestellten Aufbaus.

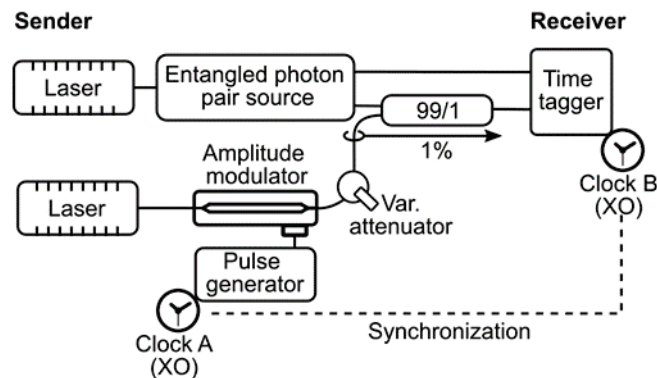


Abbildung 13: Aufbau zur Bewertung der Wirkung eines Pulsasers als Zeitstopper über die Korrelation auf EPS.

In diesem Schema verwenden wir zwei Lasersysteme, das erste zum Pumpen des EPS und ein weiteres zur Erzeugung des Zeitsynchronisationssignals. Das Timing-Signal wird in einem 99:1 Strahlteiler mit einem der Ausgänge des EPS kombiniert. Die Erzeugung eines der Einzelausgänge enthält die Zeitinformation, die eine Synchronisation über größere Entfernungen ermöglicht. Die Abbildung 14 A zeigt den Zeitstempel deutlich auf den einzelnen Zähldaten. Bei den Koinzidenzzählungen hat der Impuls jedoch bei einem Koinzidenzfenster von 1x RMS Timing Jitter keinen Einfluss auf das Muster.

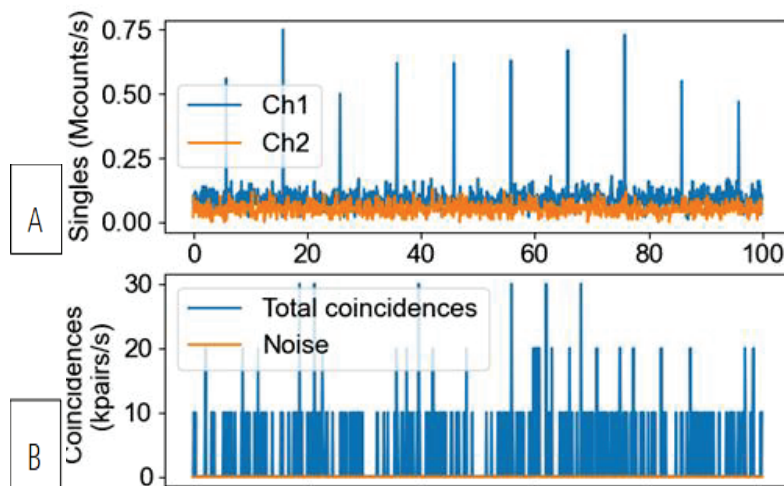


Abbildung 14: A) zeigt die klare Zeitmarkierung auf den Einzelzählungen des EPS, B) die Koinzidenzzählungen zeigen kein Auftreten des Pulsasers innerhalb eines Koinzidenzfensters von 1xRMS Timing Jitter des Detektionssystems.

Wir erhalten einige Hinweise auf das Muster nach 20000 Iterationen, wie die Abbildung 15 zeigt.

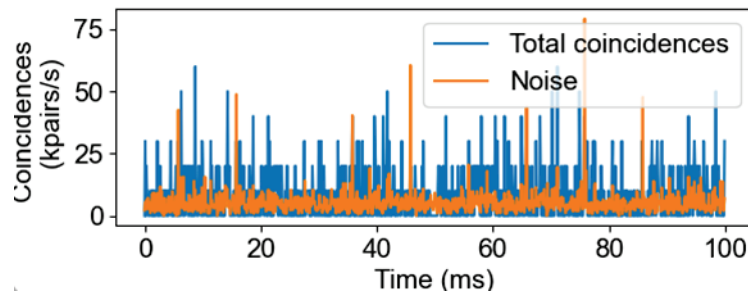


Abbildung 15: Die Erhöhung des Koinzidenzfensters bis zum 20000-fachen der Koinzidenzzählung stellt die Inzidenz durch den Synchronisationsimpuls dar.

Da das Sync-Muster aus einzelnen Photonendetektionen und nicht aus den Koinzidenzen wiederhergestellt werden kann, wird die Zufallszahl nicht erhöht, und die Synchronisation kann für längere Distanzen unter einem QKD-Protokoll garantiert werden.

Das Synchronisationsmuster kann in der Nachbearbeitung für 100 ps Pulsbreite und bis zu 1 MHz Wiederholrate wiederhergestellt werden. Die Koinzidenzen werden nicht beeinträchtigt. Allerdings verbreitert sich die Pulsbreite innerhalb einer Periode von 1 Mikrosekunde auf etwa 40 ns. Dies ist auf die schwankende Taktfrequenz des Arbitrary Waveform Generator in diesem Zeitraum zurückzuführen. Nächste Schritte: Test der Leistung dieses Synchronisationsschemas mit zwei Zeitmessgeräten im Labor (mit Verlusten).

4.2.6 Wellenlängenstabiler Pumplaser

Im Rahmen des Arbeitspakets „Vereinfachte Closed-Loop Regelung für einen mode-hop-freien Pumplaser“ wurde ein Breadboardaufbau realisiert, bei dem eine kommerzielle 405 nm Laserdiode von Ondax mit integrierter Wellenlängenstabilisierung über ein Volume Bragg Grating (VBG) und Kollimation verwendet wurde. Zum Einsatz kamen darüber hinaus die für diese Laserdiode kommerziell erhältlichen Treiber für Laserstrom und Temperaturregelung. Als Referenz für die Wellenlängenstabilität wurde ein hochaufgelöstes Spektrometer genutzt, als Messsystem für eine zunächst vereinfachte Kaskadenregelung von Laserstrom und Temperatur über einen PID-Regler kam ein KISA-Sensor der Firma Coher Sense GmbH zum Einsatz. Dieser Sensor liefert gleichzeitig Informationen über Wellenlänge, Amplitude und Bandbreite einer kohärenten Quelle.

Zunächst wurden das Referenzspektrometer und der KISA-Sensor miteinander verglichen. Nach Anpassungen im Offset und bei Vorzeichen der Driftparameter konnte eine gute Übereinstimmung gefunden werden (Abbildung 16), wobei der KISA-Sensor ein deutlich geringeres Rauschen aufwies. Die im Signal sichtbaren Oszillationen werden nach gegenwärtigem Stand auf eine regelmäßige Schwankung der Wellenlänge des Lasersignals im pm-Bereich zurückgeführt. Die abgeschätzte Auflösung des KISA-Sensors beträgt ca. 1 pm.

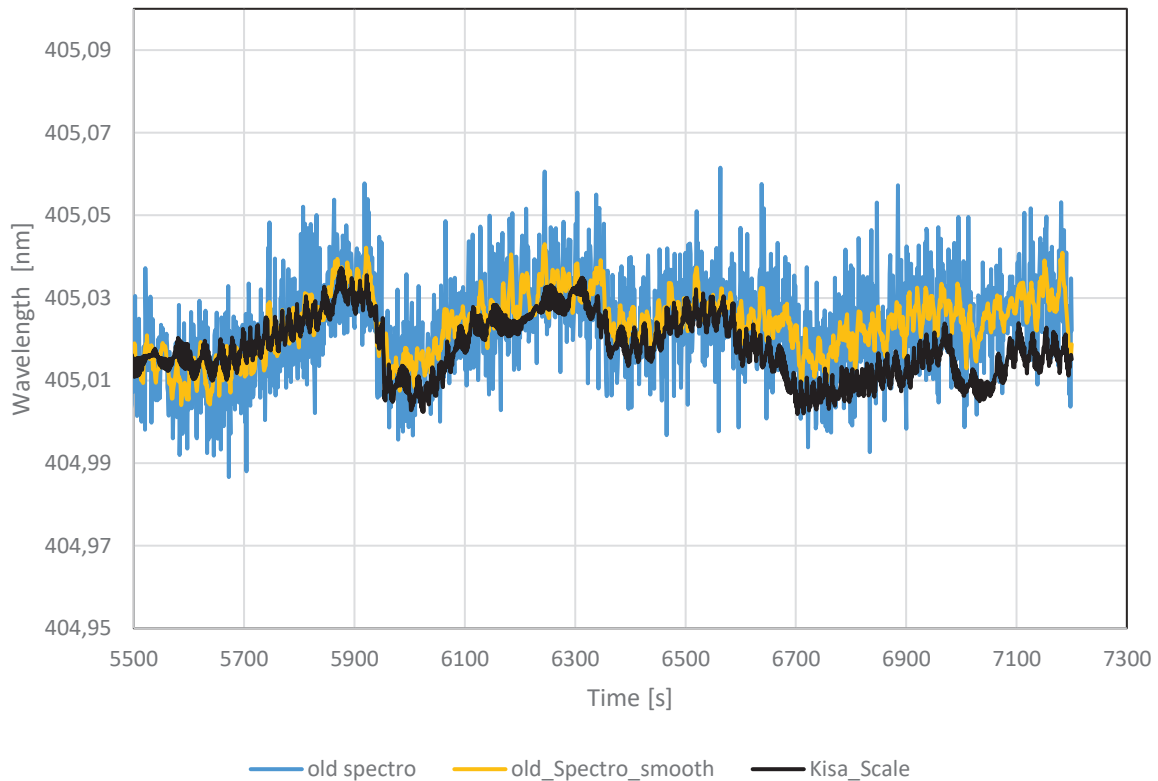


Abbildung 16: Verlauf der Wellenlänge während einer ca. 25-minütigen Messung im Vergleich zwischen Referenzspektrometer („old spectro“) und dem KISA-Sensor

In einem weiteren Versuch wurde die Sprungantwort eines einfachen, kaskadierten PID-Reglers für Laser-strom und -temperatur aufgenommen (Abbildung 17), die Zeitkonstante der Regelung befand sich dabei innerhalb der Sampling-Frequenz beider Messsysteme und konnte nicht besser aufgelöst werden.

Mit ersten optimierten Parametern des PID-Reglers konnte eine Regelgenauigkeit der Wellenlänge ca. <50 pm erreicht werden, die im Rahmen einer ca. 25-minütigen Messung nachgewiesen wurde. Allerdings traten während dieser Messung nach erstem Eindruck auch keine typischen Modensprünge der Laserdiode auf, die sonst typisch für diese Bauart sind.

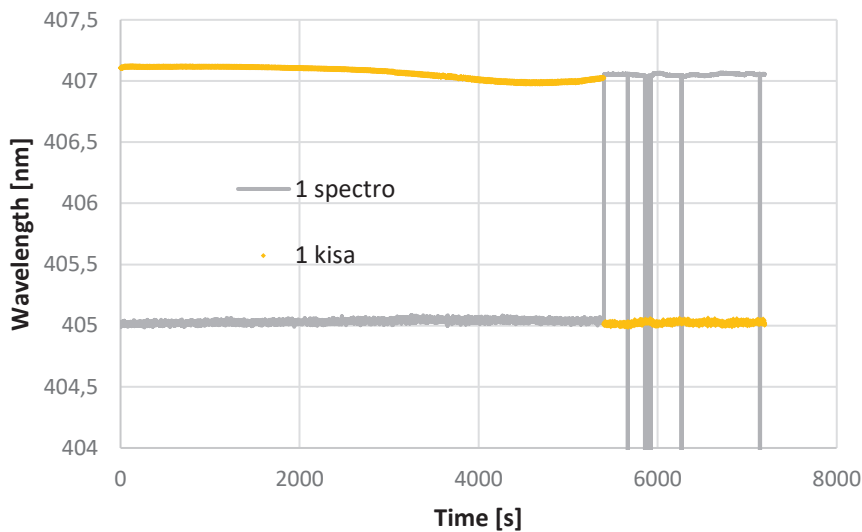


Abbildung 17: Sprungantwort der Wellenlänge auf eine Vorgabe von $\Delta\lambda = 2$ nm

Daraus leiten sich potentielle weitere Arbeiten nach Projektende ab:

- Optimierung des Driftverhaltens des KISA-Sensors unter Temperatureinfluss, in Kooperation mit dem Hersteller Coher Sense GmbH,
- Optimierung der kaskadierten Regelung, ggfls. unter Einsatz verbesserter Regelalgorithmen und in Kooperation z.B. mit dem FG Regelungstechnik der TU Ilmenau,
- Langzeituntersuchungen der Stabilität der Regelung in einem Engineering Qualification Model (EQM).

5 ZUSAMMENFASSUNG UND AUSBLICK

Im bisherigen Verlauf konnte die Machbarkeit einer Dual-Downlink-Mission zur Quantenschlüsselverteilung gezeigt werden. Dabei hat sich das Missionsziel verschoben, da sich die Implementierung auf der ursprüngliche Plattformgröße als nicht umsetzbar herausgestellt hat. Es wurde ein vorläufiges Design einer entsprechenden optischen Payload erstellt.

Nächster Schritt ist der Bau eines Engineering Qualification Models einer entsprechenden optischen Payload.

6 LITERATURVERZEICHNIS

- [1] D. H. M. G. M. B. a. M. H. Peter Krause, „A compact pointing assembly for a CubeSat to ground station free-space optical communication based on a Risley prism scanner coarse and

a tip/tilt mirror fine pointing," in *Environmental Effects on Light Propagation and Adaptive Systems VI of Proc. of SPIE*, Amsterdam, 2023.

- [2] Y. Z. M. H. a. D. F. Yafei Lu, „Theoretical and experimental determination of steering,“ *Applied Optics Vol.52, No.7*, pp. 1389-1398, March 2013.
- [3] S. Alajlouni, „Solution to the Control Problem of Laser,“ *IEEE/ASME TRANSACTIONS ON MECHATRONICS Vol. 21, No.4*, pp. 1892-1899, August 2016.
- [4] A. Krzic, D. Heinig, M. Goy und F. Steinlechner, Dual-downlink quantum key distribution with entangled photons: prospects for daylight operation, ICSO, 2022.

Ende des Dokuments