QUBE - A CubeSat for Quantum Key Distribution Experiments

Roland Haber, Daniel Garbe, Klaus Schilling
Center for Telematics
Magdalene-Schoch-Str. 5, 97074 Wuerzburg, Germany; +49 (931) 615 633 39
rolandh@telematik-zentrum.de

Wenjamin Rosenfeld
LMU Munich
Schellingstr. 4, 80799 Munich, Germany; +49 (089) 2180 2045
wenjamin.rosenfeld@physik.uni-muenchen.de

ABSTRACT

In a world of global satellite communication networks, it is crucial to ensure the security of these data links. QUBE is a project that will develop and launch a CubeSat for the downlink of strongly attenuated light pulses, with encoded quantum information, which can be used for the exchange of encryption keys. This 3U Pico-Satellite will be built using the UNISEC-Europe standard, which has been proven to provide a robust framework for increased reliability for CubeSat missions. In addition to advanced reaction wheels for precision pointing, the satellite will be carrying the DLR-OSIRIS optical downlink system as well as dedicated payloads for testing components required for quantum key distribution. A miniaturized quantum random number generator (QRNG) will create a sequence of numbers, which can be used to set the quantum states of the light. The light pulses will then be downlinked to the optical ground station at DLR in Oberpfaffenhofen, Germany, which is equipped with the corresponding components for receiving the quantum states. Additionally, the random numbers will partially be made available via an RF downlink. This will allow evaluating the link loss as well as the noise and errors in the transmission of quantum signals. In QKD, due to the underlying quantum mechanics, any attempt of reading the quantum states will alter them, which makes interceptions easily detectable. The quantum communication experiments will evaluate whether secure communication links are possible even on a CubeSat scale. A major challenge for building the required CubeSat is the attitude determination and control system that will provide precise pointing. This work will outline detailed mission requirements as well as the chosen subsystems for tackling these challenges in order to deliver a successful mission.

INTRODUCTION

This paper covers the various challenges of building a CubeSat for quantum key distribution (QKD) experiments. In the QUBE project, the CubeSat form factor as major design driver is met by high demands in attitude control and pointing accuracy as well as pointing stability for the optical downlink system. The goal of this first phase of the project is to test the components and the viability of performing QKD between a single CubeSat in low Earth orbit (LEO) and an optical ground station (OGS) in Germany. Two payloads for quantum communication tests are being developed. For this testing phase, the BB84 scheme will be employed as quantum cryptography protocol by the Ludwig Maximilian University (LMU) in Munich using a wavelength of 850 nm. The Max Planck Institute for the Science of Light (MPL) with support by the OHB System AG will be testing the performance of a QRNG and experiment with the detection of weak phase modulated signals in the 1550 nm range. In a potential second phase, the complete QKD systems will be integrated and extended to enable the generation and distribution of actually useable keys. It will possibly be implemented on additional satellites for the distribution of encryption keys to multiple ground stations around the globe.

SPACECRAFT CONCEPT

The QUBE spacecraft will adhere to the CubeSat Design Specification[1] of a 3U satellite. Figure 1 shows the QUBE satellite with its UHF antennas deployed at the top and the optical communication module facing down.

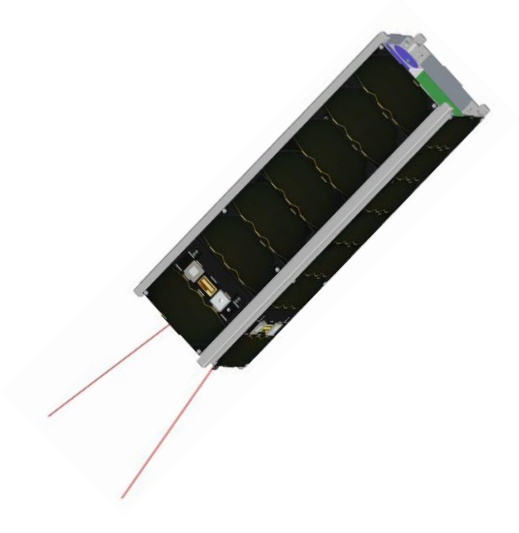

Figure 1: QUBE spacecraft concept

With the exception of two access ports for the optical laser link and the star camera respectively, the whole body is covered with solar cells. For obtaining electrical power, solar cells by Azur Space with an efficiency of 28% are connected pairwise and in series in order to provide the required voltage levels for charging the batteries. Pairs of solar cells are then connected in parallel in order to scale and maintain the same voltage levels with an elevated current[2]. Subsystems and payloads are housed within the satellite and interconnected using the UNISEC-Europe system bus[3]. Bolts and spacers are employed for fixing each printed circuit board (PCB) to the satellite structure, which is essentially only made up of the four aluminum rails, to which the solar panels are screwed.

When considering the satellite as a combination of three individual units, the lower unit, where the UHF antennas are located, contains the main components that are necessary for basic satellite operations. These include the lower backplane, the on-board computer (OBC), two electronic power systems (EPS) and a communications module (COMM) with two redundant modems and the antenna deployment. From the lower backplane another UNISEC bus extends along the z-axis towards the top of the satellite and allows for the same plug & play connectivity as the lower backplane. The middle unit of the satellite houses the attitude determination and control system (ADCS), including the six reaction wheels, as well as the two quantum payloads by LMU[4] and MPL[5] for the generation of quantum signals and of quantum random numbers respectively. Besides the UNISEC bus, the quantum payloads are additionally connected to the DLR optical downlink system in the top unit via individual optical fibres. Also in the top unit is the star camera that will provide precise attitude information. Proximity of the star camera to the optical downlink system is key to ensure validity of the attitude data with regard to the laser module.

QUANTUM KEY DISTRIBUTION

QKD is a concept that allows two parties to communicate securely over potentially insecure channels[6]. In particular, it provides a shared random key, whose knowledge to any adversary can be reduced arbitrarily close to zero. In combination with the classical one-time pad method of encryption, one obtains in principle provable security, which (given a proper physical realization) only relies on very fundamental assumptions – the laws of physics. In contrast to currently used encryption methods, relying on computational hardness of certain mathematical problems, it is thus also safe to any future developments of algorithms and computational technology, such as the quantum computer.

Figure 2 illustrates the basic principle of QKD. Between Alice and Bob, there is a traditionally unsecure communication channel, that is now secured by using the quantum key distributed by the satellite to each partner. A third entity, called Eve, is unable to eavesdrop on both the communication channel between Alice and Bob (due to the lack of the decryption key), and the quantum channel between each partner and the satellite (due to the underlying quantum physics, that leave any interception detectable). If either Alice or Bob discover that Eve has succesfully intercepted the quantum key exchange, then the key can be discarded and a new one can be generated.

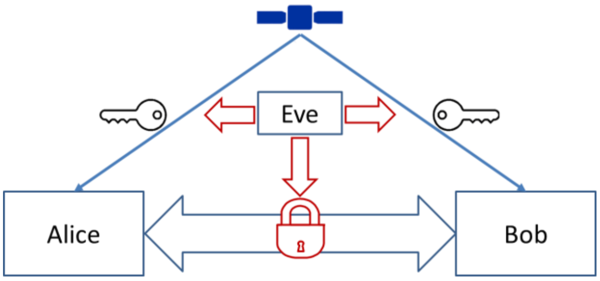

Figure 2: QUBE QKD concept

The basic idea of the QKD method is to employ the principal impossibility of making perfect copies of unknown quantum states, i.e. cloning/amplification, together with the fact that any measurement alters/destroys a quantum state without providing full information on it. By using quantum states for the transmission of information, e.g. polarization states of single photons, one can detect any attempt of tampering/interception by measuring the ratio of occurring errors (so-called quantum bit error rate, QBER).

Implementations of QKD protocols require preparation and measurement of states at the quantum limit, like detection of single photons or small phase variations comparable to vacuum fluctuations. Thanks to the recent advancements of integrated photonics technologies, as well as of detectors, the required components can in principle be miniaturized to fit even into very small satellites, such as CubeSats[7,8]. Still, implementing a QKD link between such a satellite and an optical ground station represents a considerable challenge. On the one hand the low power budget and harsh environmental conditions during launch and operation require extremely efficient, stable and robust QKD components which need to be developed and optimized specifically for this purpose. On the other hand, there are additional requirements on the satellite. These include a sufficiently large optical terminal with efficient tracking to minimize losses. Any losses can be critical in a QKD scenario due to the impossibility to amplify quantum signals.

The ultimate limit for achieving any secure key for a given link is determined by the signal-to-noise ratio of the quantum signal to scattered light and detector noise. As polarization of light is important to most QKD protocols, it has to be preserved within the satellite on the way to the optical terminal, which sets high requirements on the employed optical components. Due to the same reason, the orientation of the satellite has to be well under control and tracked efficiently. Also, for correctly detecting the quantum signals, synchronization between the satellite and the ground station is required at a level which exceeds that of a typical classical communication scenario. Finally, due to extremely low light levels required in QKD, any scattering of light from the satellite has to be minimal.

QKD EXPERIMENTS

As mentioned above, building QKD components for the LEO space environment in a CubeSat represents a considerable technological challenge. On top of the required compactness and energy-efficiency, there are several additional problems to address. As the low power budget does not allow for a full-scale temperature stabilization of the critical components, large temperature drifts of several 10° C have to be taken into account. This involves their mechanical stability as well as possible drifts of the wavelength and of the birefringence influencing the polarization[9]. In order to provide the dry gas atmosphere necessary for operation of certain components, e.g. vertical cavity surface emitting lasers (VCSEL), and to reduce problems with outgassing and contamination of optical surfaces, these components have to be hermetically packaged. Also, there is only insufficient data available on the degradation of specific optical materials and optoelectronic components in a space environment.

The experiments planned for this first phase of the mission include functional tests of all payloads, as well as first tests of the classical and quantum optical links to the ground station. In particular, measurements of the optical channel and performance of the optical terminal will be undertaken. In parallel, the functionality of the QRNG will be assessed. The random bits will be analyzed on board by a payload controller (PCON) and also sent to the ground station using the classical optical or UHF link. After establishing an optical link, signals of the discrete variable (DV)-QKD module working at 850 nm will be sent to the optical ground station and analyzed there. Here, the overall link efficiency, as well as the quality of the transmitted polarization states (which will be analyzed via quantum state tomography) are the most crucial parameters. Similarly, an integrated photonic chip will be tested by analyzing weak sideband modulation of the signal at 1550 nm. Finally, as test for a necessary part of a full QKD protocol, the DV-QKD module will send polarization states according to the random bits generated on board by the QRNG.

The first phase of the project will provide valuable experience on operation and reliability of QKD components in space conditions as well as the feasibility of performing a full QKD protocol under these specific constraints. Based on this knowledge, the hardware will be further developed and extended in order to perform QKD with the satellite and, based on that, key distribution between widely separated ground stations using the satellite as a trusted node.

OPTICAL COMMUNICATION

Originally designed for high data rate laser communication on small satellites, the DLR Institute of Communication and Navigation (DLR-IKN) is modifying the Optical Space Infrared Downlink System (OSIRIS) for photon transmissions on QUBE. While first iterations of OSIRIS that flew on the BIROS and Flying Laptop satellites had a much higher power, volume, and mass budget available, DLR has since developed the OSIRIS4CubeSat (O4C) version, which only encompasses about 0.3U and weighs less than 300 g, however still managing up to 100 Mbit/s at a power consumption of 8 W. Since optical signal modulation, and therefore high speed data transmission, will not be the focus of the QUBE project, OSIRIS4QUBE (O4Q) will rely on direct optical fiber feeds originating from the quantum payloads. These feeds will supply the 850 nm and 1550 nm quantum signals to be send to the OGS in Oberpfaffenhofen. Additionally, DLR will be performing multiple in-orbit experiments regarding signal acquisition and tracking, channel measurements, and performance analyses of the OSIRIS payload as well as the optical ground station.

Optical Ground Station

The optical ground station (OGS) used for photon reception is situated at the DLR premises in Oberpfaffenhofen. There, the DLR-IKN[10] operates a fixed rooftop system, which has already been used for airborne QKD experiments in the past[11], as well as a mobile system that can be transported and deployed at remote locations. Either option can theoretically be used with the OSIRIS payload on the QUBE satellite. However, due to the complex nature of the components involved in photon reception, an additional installation of adaptive optics and receivers is being implemented in a coudé room close to the rooftop OGS[12].

Figure 3 shows the rooftop optical ground station in Oberpfaffenhofen.

Figure 3: DLR optical ground station[13]

ATTITUDE DETERMINATION & CONTROL

By far the highest demands on the QUBE satellite platform, originate from the pointing accuracy and stability that is required for the optical downlink system. Since the O4Q payload encompasses a fine pointing system using active beam steering[14], the satellite is tasked with the body pointing operations that will put the optics within an angle of 1° towards the OGS (within 3-sigma). Pointing stability, i.e. a low jitter within the required 1° accuracy, will also play an important role, especially while the satellite continuously adjusts its attitude during a flyover. Unlike other commercially available ADCS modules[15], QUBE will allow for a more distributed approach for its sensors and actuators that has already been applied in a similar manner to the UWE-3 satellite. Figure 4 shows the distributed nature of the ADCS system.

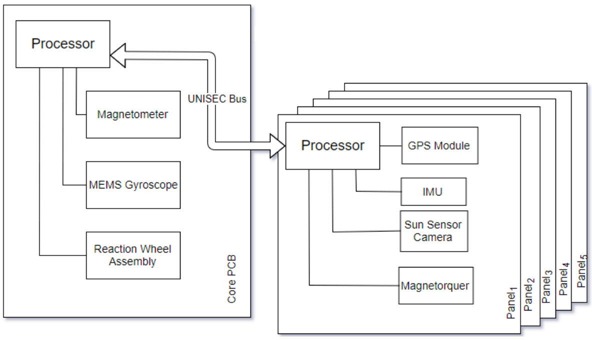

Figure 4: Distributed functionalities of the QUBE ADCS[2]

At the center of the ADCS lies a PCB with a UNISEC interface, a microcontroller, a MEMS gyroscope and three magnetometers. It is complemented by six reaction wheels as well as sensors and actuators that are placed on the solar panels.

Attitude Sensors

Apart from the gyroscope and magnetometers, each solar panel is equipped with a sun sensor and an inertial measurement unit, for redundancy reasons and continuous availability. Miniaturized CMOS cameras are employed for the sun sensors, which are also going to fly on the UWE-4 satellite[16]. Each solar panel also houses a microcontroller that is identical to the one on the ADCS module, therefore providing another layer of redundancy and retaining magnetic attitude control in case of a malfunction of the ADCS.

A star camera will be included in the top part of the satellite and firmly attached to the OSIRIS module. This ensures a minimum deviation between the attitude information coming from the star sensor and the actual position of the OSIRIS optics. The star sensor will likely forward its positional data to the ADCS board via the UNISEC bus.

Attitude Actuators

When it comes to reaction wheels, most CubeSat solutions suffer from high torque ripple and discontinuities, because of their low rotational speeds. Others are usually too heavy or have a too high power demand for a 3U system. Together with WITTENSTEIN cyber motor GmbH[17], a low inertia and high speed reaction wheel has been developed, which provides less torque ripple as well as a much lower power consumption. With the cubic form factor of 20x20x20 mm including the electronic circuitry and a weight of about 20 g, multiple wheels can be placed very close together on a UNISEC PCB. In QUBE, six wheels will be placed on the ADCS board to achieve full redundancy in all axes. Commanding is supported via SPI, I^{2}C, and UART. A scalar sinusoidal control scheme has proven to yield the lowest torque ripple compared to conventional trapezoidal control, field-oriented control (FOC), and direct-torque control (DTC)[18]. Figure 5 shows the QUBE actuators and the ADCS PCB side by side.

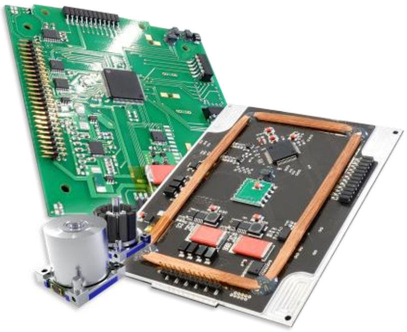

Figure 5: QUBE actuators and ADCS PCB showing an uncovered reaction wheel and a magnetorquer, which is placed on the back of a solar panel

In addition to the reaction wheels, magnetic air coils are used on the back of the solar panels for detumbling after deployment as well as for desaturation of the reaction wheels.

ON-GROUND TESTING

Besides conventional testing and simulations for thermal and structural aspects, the specific challenge of precision pointing requires additional testing efforts with regard to attitude determination and control. A FlatSat for electrical and interconnectivity testing of all subsystems will also be developed.

ADCS Testing

For attitude simulation, hardware-in-the-loop testing, material stress tests, and sensor characterization and calibration, the Dynamic Bench Test Facility (DBTF) at the Zentrum für Telematik (ZfT) is utilized[19]. The Dynamic Bench Test Facility is based on the combined operation of two high precision three-axis motion simulators, a six degree of freedom robotic arm, sensor stimulators and a simulation computer system. Arranging the motion simulators and sensor stimulators into proper geometrical configurations allows for precision pointing tests of the optical payload on the QUBE satellite. In other missions, such as NetSat[20] and TOM[21], this facility is used for testing of multi-satellite systems with focus on formation control, relative navigation, inter-satellite communication links, and cooperative target observation.

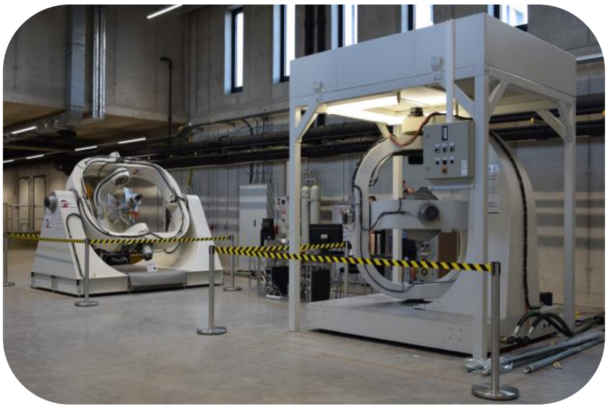

Figure 6: Dynamic Bench Test Facility at ZfT premises for three-axis satellite motion simulation

Figure 6 shows the DBTF, which provides the possibility of testing mission scenarios with actual hardware and real sensory inputs.

FlatSat Testing

Thanks to the implementation of the UNISEC bus system, integration and testing of the satellite in a FlatSat configuration as well as the simple maintenance, extension, and replacement of subsystems in any configuration during development is easily achievable.

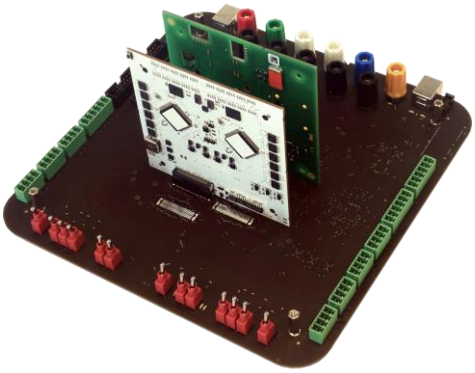

Figure 7: FlatSat & UNISEC board for subsystem and electrical testing

Figure 7 shows the UNISEC development board that is used for subsystem testing, either individually or in combination. Thanks to the added network access and the COMPASS software protocol[22], location independent developments can be undertaken with multiple of these setups in distant facilities.

ORBITAL CONSIDERATIONS

QUBE experiments concerning QKD will have to be taking place while the satellite is in Earth's shadow in order to avoid interference of diffused light as well as reflectivity errors caused by the satellite body (Figure 8).

Figure 8: QUBE orbit simulation with optical laser link during eclipse

Therefore, the desired orbit for this mission will include recurring night time flyovers past Oberpfaffenhofen. In order to achieve recurring experiment times, a sun-synchronous orbit (SSO) would be ideal. An SSO has the advantage of a point on Earth passing the orbital plane at the same local time each day. It is created by choosing the right inclination for the corresponding altitude (Figure 9), so that the change of the longitude of the ascending node rotates around Earth in exactly one year.

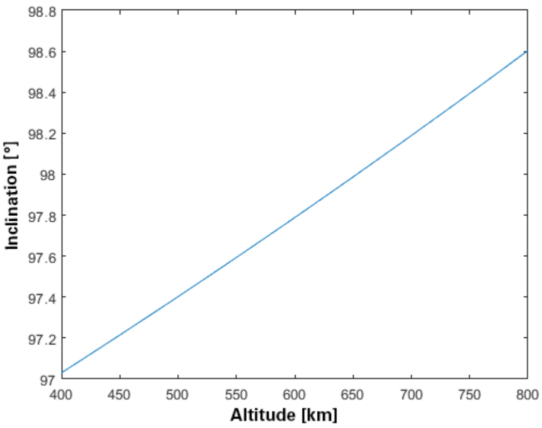

Figure 9: SSO inclinations for different altitudes

By selecting a suitable launch window for this SSO, the required Local Time of Ascending Node (LTAN) can be chosen in order to achieve an orbit, where flyovers at the optical ground station repeat at the same time of night. A suitable launch provider is yet to be selected, however since many earth observation satellites prefer non-eclipsed flyovers, getting in the perfect orbit might be difficult. Additionally, due to the lack of orbit control thrusters, the satellite will be subjected to enough drag to alter the LTAN over the course of a few months. The flyover times will thereby continuously change instead of remaining constant. Due to the reduced life time, ISS deployments will also not be considered for this mission.

In order to meet the high power demands of the payloads and attitude control system, enough energy has to be stored prior to the operational phases. With the six solar cells that will likely be facing the sun at any time in orbit while the satellite is not in Earth's shadow, up to 5.5 W of the power can be delivered to the batteries. The efficiency of the energy conversion between solar cells and batteries lies above 80 %. Taking an SSO at an altitude of about 500-700 km, 60 minutes of each orbit period is sun lit. This yields 5.5 Wh of electrical energy delivered to the batteries. With a total of four batteries available, the amount of electrical energy that can be stored on the satellites comes to 37.6 Wh. Thus, it will take several orbits for a complete energy restoration. Since the total sum of electrical energy consumed by active systems during an operational flyover is higher than the amount of energy recouped in one orbit, the operational phases can only take place every other obit or less.

SATELLITE SYSTEM BUS

QUBE will heavily benefit from the UWE-3 satellite, which encompasses a modular system architecture using the UNISEC-Europe standard. UWE-3 has been operational in orbit since November 2013 and has mastered LEO challenges with mostly commercial off-the-shelf (COTS) components in a robust and redundant configuration[23]. The system bus design has been optimized with respect to mass, volume, and energy efficiency, while also maintaining a modular and flexible architecture.

The UNISEC architecture has since been advanced for the use in UWE-4, including smaller, unkeyed connectors and a high speed MLVDS data bus. While UWE-4, which is to be launched near the end of 2018, is still a 1U pico-satellite, QUBE represents the first 3U CubeSat to which this system bus will be extended to. Figure 10 shows the extended QUBE bus in comparison to the UWE-4 bus. Essentially, what served as the fron-access board for UWE-4 is being enlarged and equipped with additional UNISEC connectors.

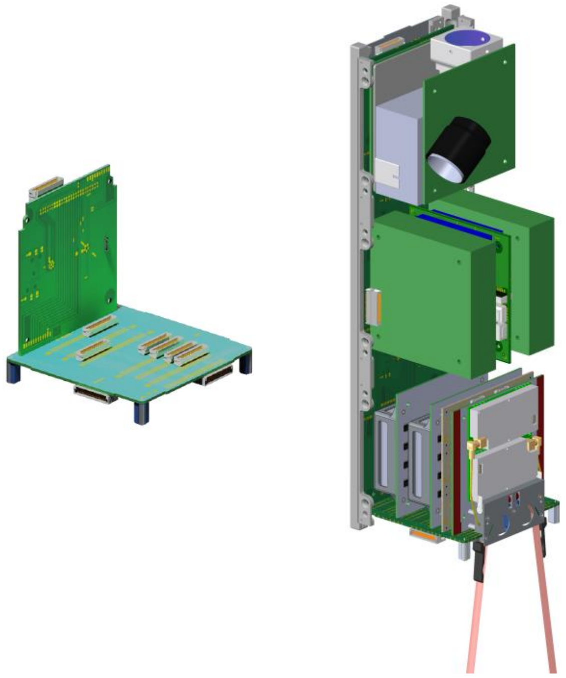

Figure 10: Left: UWE-4 UNISEC system bus[23]
Right: QUBE extended UNISEC system bus

Also a derivative of the successful UWE-3 satellite, in the center of the OBC, is a fully-redundant, low power microprocessor. It acts as the bus master of the UNISEC system bus and represents the heart of the entire satellite and its housekeeping operations. Additional microcontrollers are used on the ADCS module as well as on each of the side panels. The lower backplane includes a redundant set of deployment switches, while the longer backplane provides an umbilical line connector and remove-before-flight switches. During and after integration of the satellite, the umbilical line can be used as a digital interface for debugging and software updates of every subsystem as well as for battery maintenance[24].

On-Board Software

Communication between all subsystems and payloads is handled by the COMPASS protocol, which provides a multi-level structure for turning every component into a globally accessible node, while also offering a wide range of common services to share the available functionalities throughout the satellite[25]. COMPASS includes various functions to effectively tackle typical challenges faced with in subsystem communications, such as delay, real-time requirements, and dynamic and manual routing options inside a network[26]. In-orbit software updates for each subsystem will also be tremendously smoother with the combination of the UNISEC bus and the COMPASS protocol.

CONCLUSION & FUTURE OUTLOOK

The aim of the QUBE mission is to take a step towards broadly available data protection via QKD. In this first phase, the most essential systems for quantum key generation, optical downlink, and attitude control are tested on a 3U satellite in LEO. With a launch planned for the end of 2019, a lot of obstacles still have to be overcome. Once operational in orbit, many new conclusions can be drawn from the QUBE experiments, and follow-up missions will improve and broaden the idea of quantum key distribution toward multi-satellite systems and a global availability of data encryption through quantum communication.

Acknowledgments

This work is funded by the German Federal Ministry of Education and Research (BMBF) within the IKT 2020 program. The project partners involved in QUBE are LMU Munich (coordination), MPL Erlangen, DLR-IKN, OHB System AG, and ZfT.

References

1. CubeSat Design Specifications Rev.13, The CubeSat Program, Cal Poly SLO, Retrieved from http://www.cubesat.org/resources, June, 2018.
2. Schilling K. et al., “TOM - A Pico-Satellite Formation for 3D Earth Observation,” 4S Symposium, Sorrento, Italy, 2018.
3. http://unisec-europe.eu, June, 2018
4. https://www.uni-muenchen.de, June, 2018.
5. https://www.mpl.mpg.de, June, 2018.
6. Bennett, C. H. et al., "Quantum Cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175-179, 1984.
7. Khan, I. et al., "Satellite-Based QKD," Optics and Photonics News, February 2018.
8. Oi, D. et al., “Nanosatellites for quantum science and technology,” Contemporary Physics, 58:1, 25-52, 2017.
9. Xavier, G. B. et al., "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation," New Journal of Physics, Volume 11, April 2009.
10. www.dlr.de/kn, June, 2018.

11. Schmidt, C. et al., "OSIRIS Payload for DLR's BiROS Satellite," International Conference on Space Optical Systems and Applications (ICSOS), Kobe, Japan, May 2014.

12. Moll, F. et al., "Aerospace laser communications technology as enabler for worldwide quantum key distribution," SPIE Photonics Europe, Brussels, Belgium, 2016.

13. Retrieved from http://www.dlr.de/kn/, June, 2018.

14. Fuchs, C. et al., "Optical satellite downlinks at DLR - OSIRIS," Retrieved from https://artes.esa.int, July, 2017.

15. Mason J.P. et al., "MinXSS-1 CubeSat On-Orbit Pointing and Power Performance," Journal of Small Satellites, Vol. 6, 651 – 662, 2017.

16. Bangert P. et al., "UWE-4: Integration State of the First Electrically Propelled 1U CubeSat," Proceedings of the AIAA/USU Conference on Small Satellites, Logan, Utah, 2017.

17. https://cyber-motor.wittenstein.de, June, 2018.

18. Brosch P.F. et al., "Antriebspraxis. Energieeffiziente Antriebssystem mit fester oder variabler Drehzahl," 1st ed., Vogel Business Media, 2017.

19. Ruf, O. et al., "Challenges and Novel Approaches for Testing Large Numbers of Small Satellites," 68th International Astronautical Congress, Adelaide, Australia, 2017.

20. Schilling, K. et al., "NetSat: A Four Pico/Nano-Satellite Mission for Demonstration of Autonomous Formation Flying," 66th International Astronautical Congress, Jerusalem, Israel, 2015.

21. Schilling K. et al., "TOM: A Formation for Photogrammetric Earth Observation by Three Cubesats," 4th IAA Conference on University Satellite Missions and CubeSat Workshop, Rome, Italy, 2017.

22. Dombrovski S. et al., "Control of Multi-Picosatellite Systems: Tiny Scripting Language and Multi-Layer Compass Protocol," SpaceOps, Marseille, France, 2018.

23. Busch S. et al., "UWE-3, In-Orbit Performance and Lessons Learned of a Modular and Flexible Satellite Bus for Future Picosatellite Formations," 65th International Astronautical Congress, Toronto, Canada, 2014.

24. Busch S. et al., "CubeSat Subsystem Interface Definition," Version 1.0, Retrieved from http://unisec-europe.eu, June, 2018.

25. Dombrovski S. et al., "Uniform, Multi-Level protocol for Ground and Space Segment Operations and Testing," 4S Symposium, Sorrento, Italy, 2018.

26. Dombrovski S. et al., "Tiny 2 Interpreter - In-Orbit Database and Distributed Computing based on Tinytus Language," 68th International Astronautical Congress, Adelaide, Australia, 2017.