Applications of Quantum Protocols and Post-Quantum Cryptography in Aviation and Space

H. Bartz, G. Liva, N. Mäurer, F. Moll, S. Scalise, T. Strang

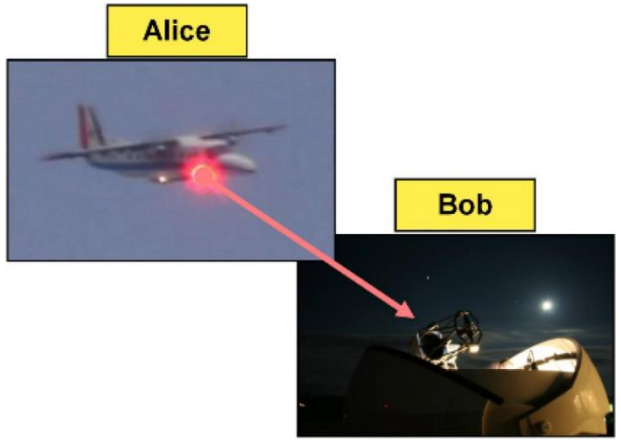
CODE 2020 - Workshop 7, 11th November 2020

thomas.strang@dlr.de

Outline

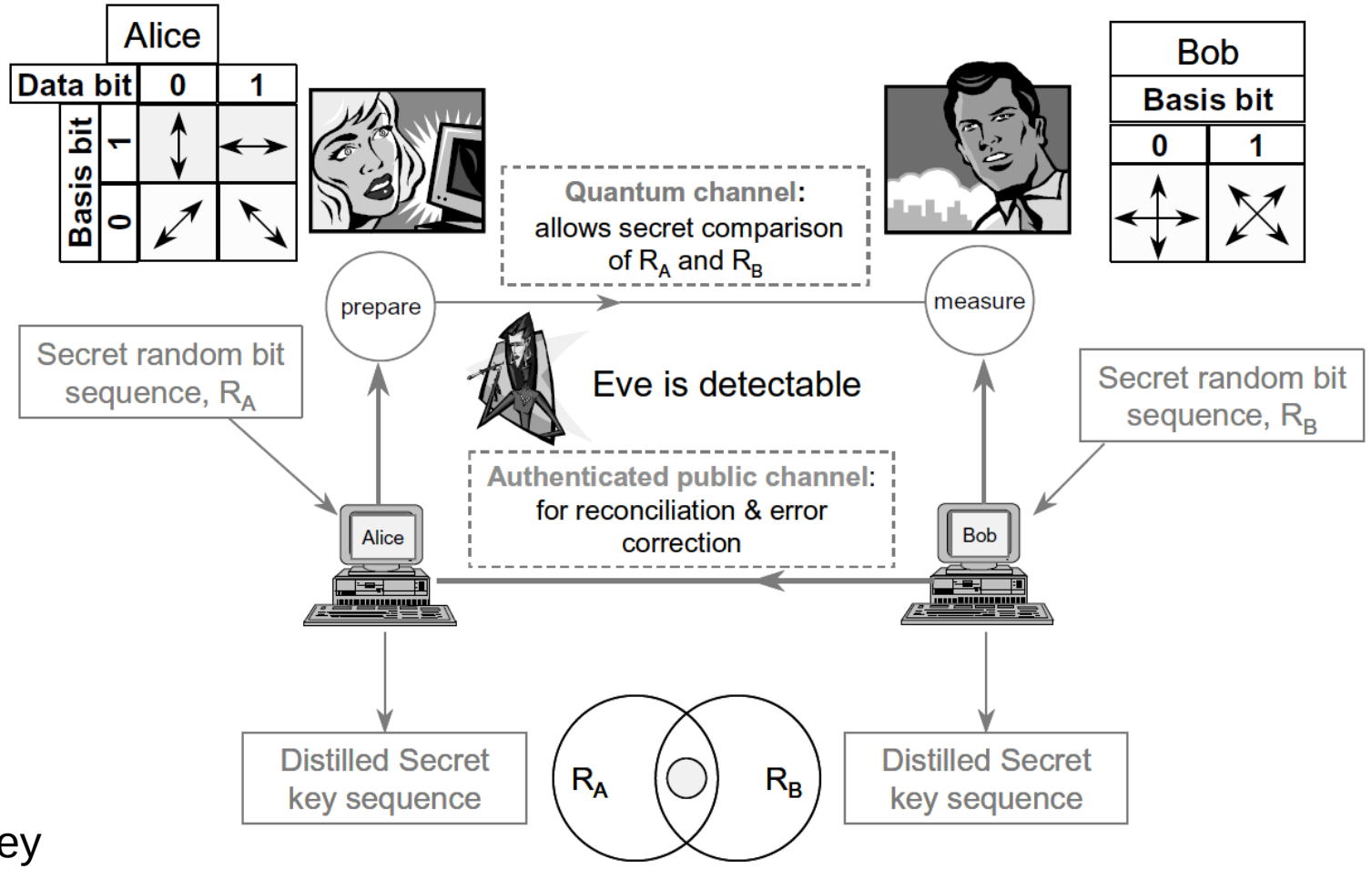
- Satellite based Quantum Key Distribution (QKD)
- Principles of Post Quantum Cryptography (PQC)
- PQC in aviation: Flying PQC demonstrator

Quantum Key Distribution



- Use of polarization states in optical free-space communication
  - Alice prepares polarization states
  - Bob measures polarization states
  - Random choice of preparation and measurement basis
  - Postprocessing → Shared Secret Key

BB84 Quantum Key Distribution (QKD) Protocol



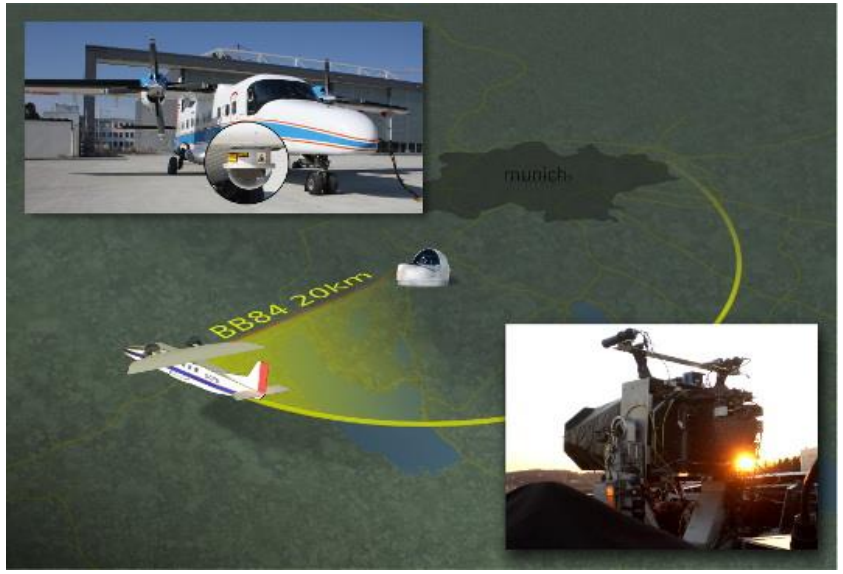
J. E. Nordholt et al., Present and Future Free-Space Quantum Key Distribution, Proceedings of SPIE Vol. 4635, 2002

Quantum Key Distribution
Work performed at DLR KN

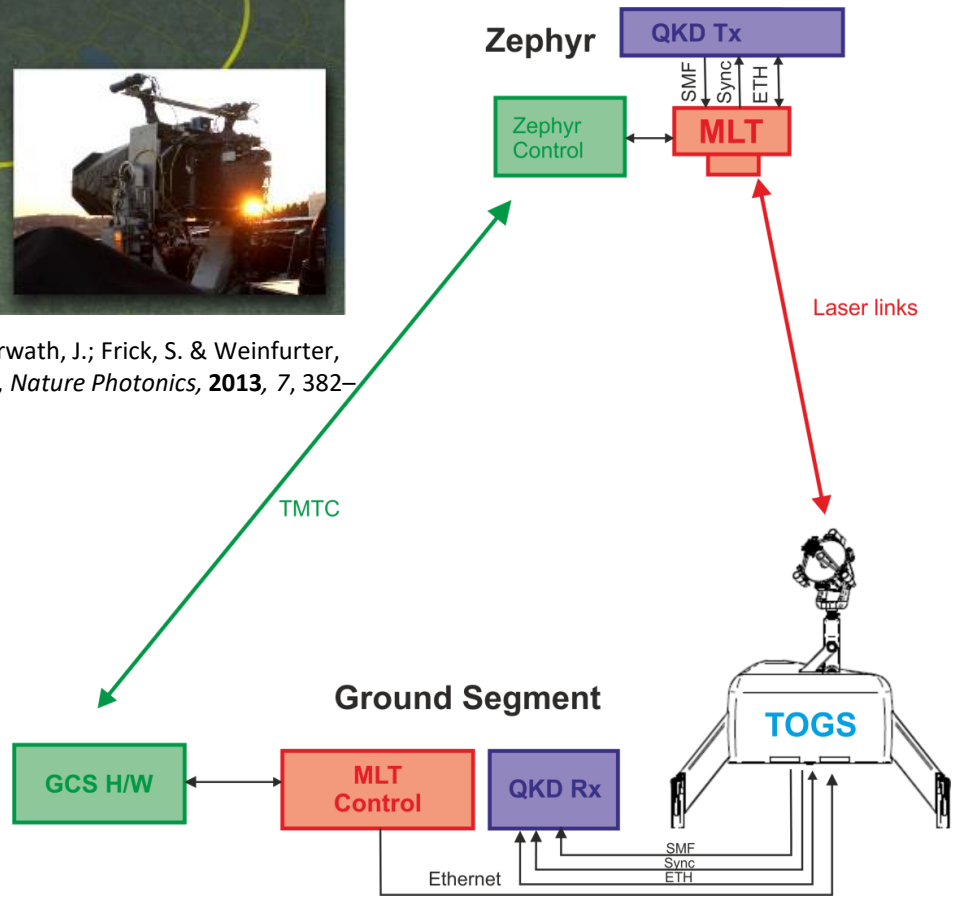
- Flight Experiment for Demonstration of polarization encoded BB84 in 2013
- Partner: LMU
- Erwin-Schrödinger Prize 2015 (The Stifterverband Science Award)

- Study on secure key distribution on continental scale using high altitude pseudo satellites (HAPS)
- Partners: Airbus, LMU, MPL, Mynaric

- Study on Investigation of gravitationally induced decoherence (consultant for OGS interface)
- Partners: OHB, UniW



Nauerth, S.; Moll, F.; Rau, M.; Fuchs, C.; Horwath, J.; Frick, S. & Weinfurter, H., Air-to-ground quantum communication, *Nature Photonics,* **2013***, 7*, 382–386

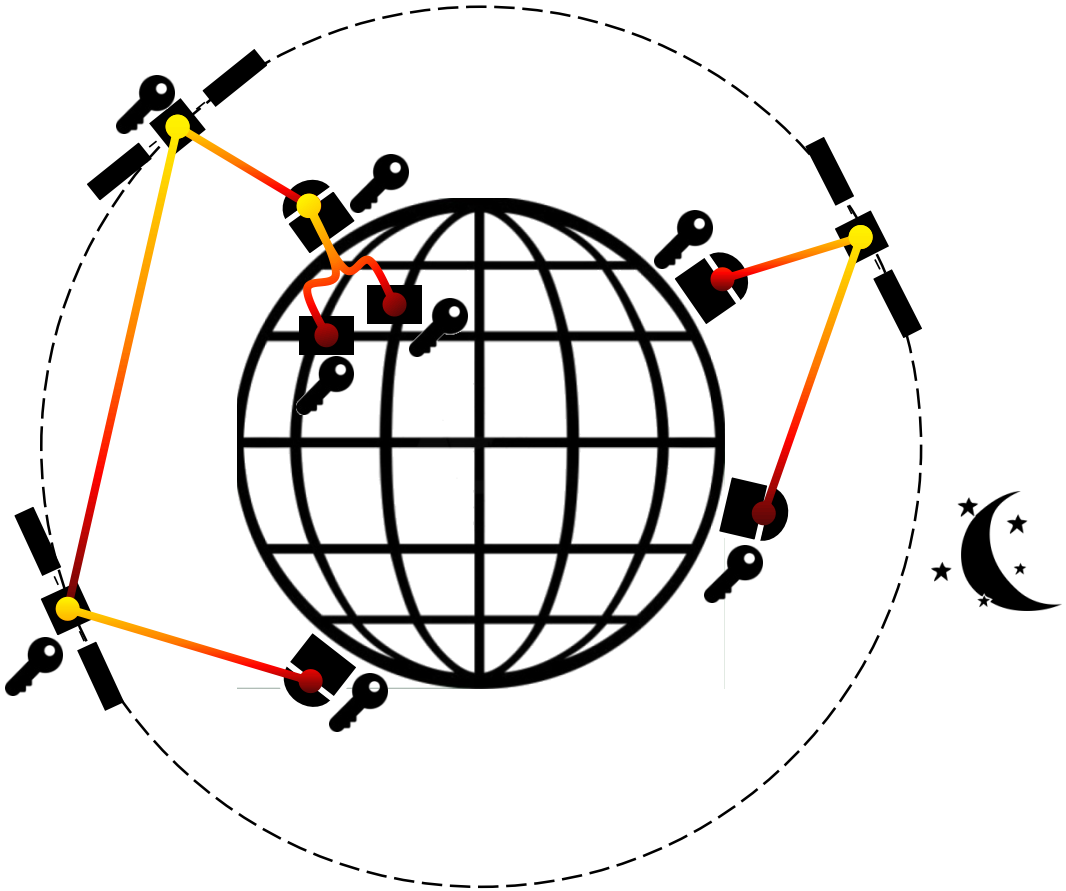


Moll, F. et al. ; Botter, T.; Marquardt, C.; Pusey, D.; Shrestha, A.; Reeves, A.; Jaksch, K.; Guenthner, K.; Bayraktar, O.; Mueller-Hirschkorn, C.; Gallardo, A.; Gonzalez, D.; Rosenfeld, W.; Freiwang, P.; Leuchs, G. & Weinfurter, H., Stratospheric QKD: feasibility analysis and free-space system concept, Proc. Of *SPIE 11167,* **2019**

Going Space: Satellite based global Quantum Key Distribution

Selected research subtopics

- High pointing accuracy
- Channel Modelling
- Day and night QKD
- Space implementations (quantum /classical comms)
- Single satellite schemes/ network schemes
- Trusted node concepts with prepare and measure protocols (BB84)



Quantum-Resistant Cryptography

Threats: Quantum Computing Algorithms

- Grover's search algorithm
- Shor's factoring algorithm

that are a threat for today's cryptosystems.

Symmetric Cryptosystems:
Only Grover's search algorithm is a threat

- can be fixed by doubling the key size

Asymmetric Crypto[illegible]ems:
Most systems are bas[illegible]n the hard problem of factoring large integers or the di[illegible]e logarithm problem

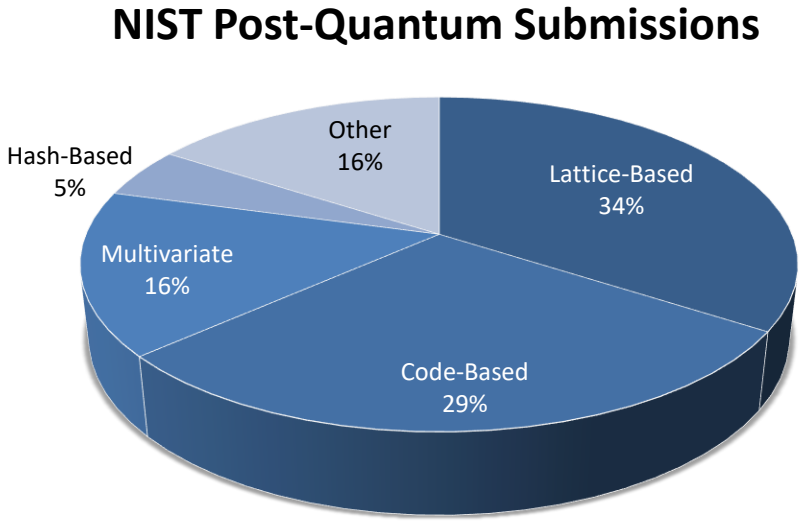
- solved by Shor's algorit[illegible] in **polynomial time**
- cannot be fixed by tuning [illegible]e parameters

- Prototypes of "small" quantum computers (up to 72 qubits) exist already
- Communication encrypted today can be stored and decrypted tomorrow

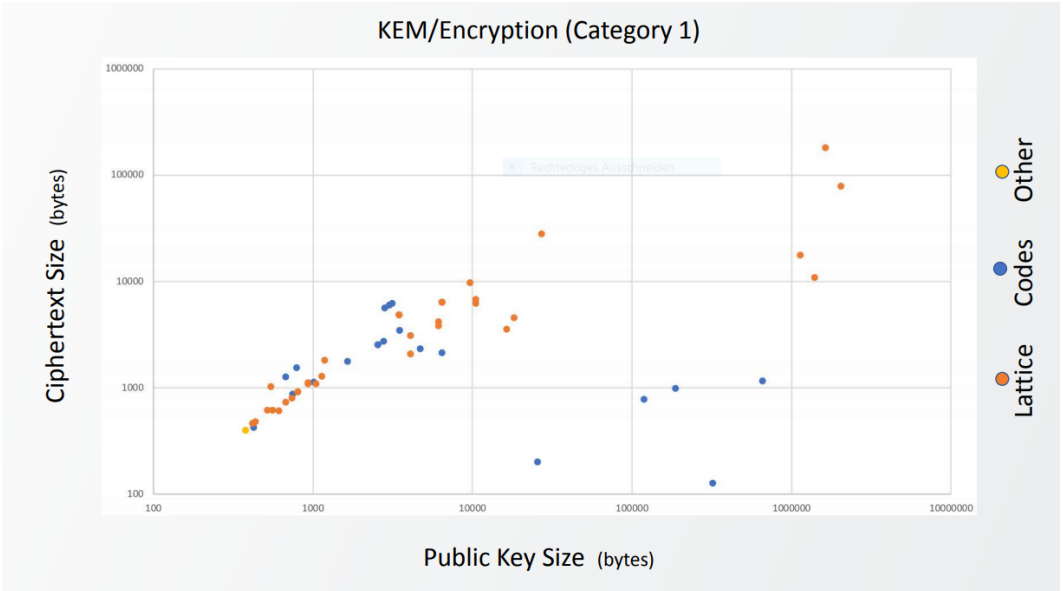
> **Is there a risk we'll be caught unprepared?**
>
> Yes. There was an enormous amount of effort put into fixing the Year 2000 bug. You'll need an enormous amount of effort to switch to post-quantum. If we wait around too long, it will be too late.
>
> Interview with P. Shor, Nature, Oct 2020

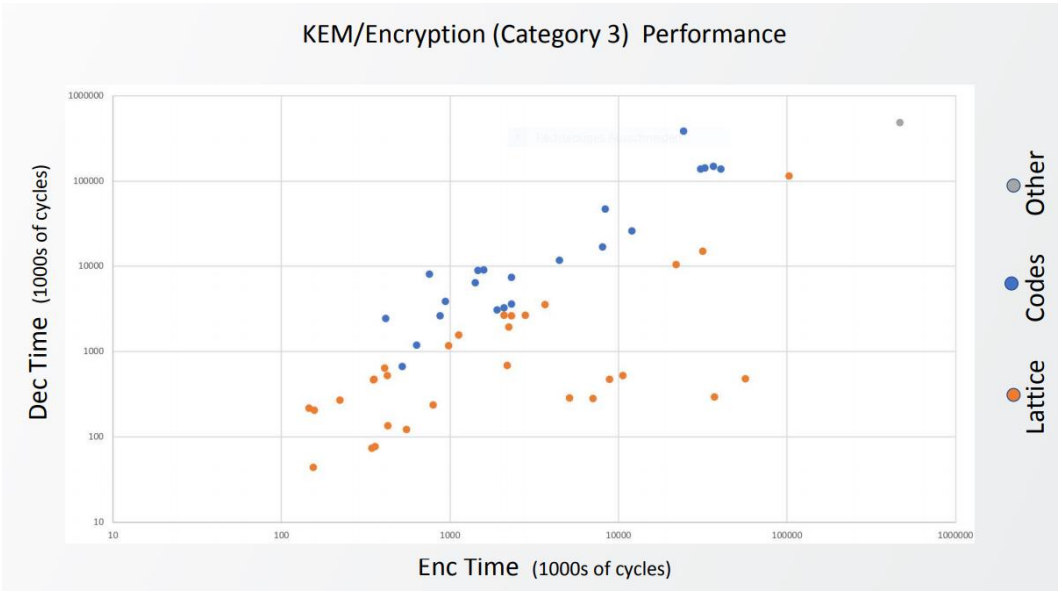
Demand for quantum-resistant public-key cryptosystems!

Quantum-Resistant Cryptography
Different Approaches



- All quantum-resistant approaches come at a cost of (significantly) **increased key sizes** compared to RSA
- **But:** there are other figures-of-merit:
  - computational complexity for encryption/decryption of code-based PQC is **often significantly lower** (e.g. RSA vs. McEliece)
  - **ciphertext-size** often very short (McEliece)
  - **computational complexity of key generation**
  - **Throughput**/rate-loss





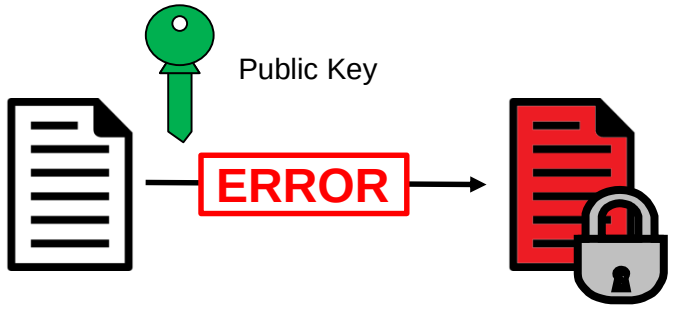
https://csrc.nist.gov/projects/post-quantum-cryptography

Quantum-Resistant Cryptography
Code-Based McEliece Cryptosystem

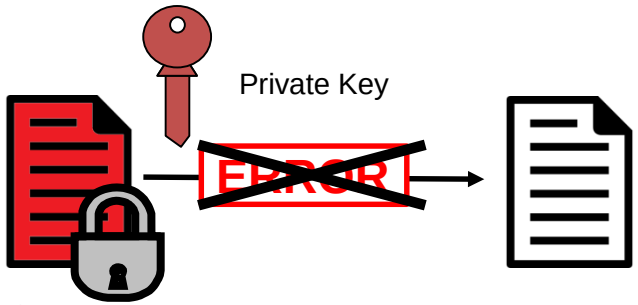
Strong confidence since the McEliece cryptosystem is as old as RSA

Private Key: secret input for decoder for an error-correcting code
Public Key: compact description of the error-correcting code

Encryption



Decryption



- ✓ Security level depends on
  - error-correction performance of the code
  - structure of the code

Our Goals:

- ✓ Design an analysis of new code-based post-quantum cryptosystems with *small key-size and high security level*
- ✓ Reducing the key-size by designing appropriate codes:
  - Rank-Metric codes (Gabidulin codes, LRPC codes)
  - Low / Moderate Density Parity-Check (LDPC/MDPC) Codes

Code-Based Quantum-Resistant Cryptography
Work performed at DLR-KN

Work related to code-based McEliece cryptosystems based on

- Low- / Moderate-Density Parity-Check (L/MDPC) codes
  - Protograph-based MDPC code design
  - Improved decoding algorithms
- Rank Metric codes
  - Low-Rank Parity-Check (LRPC) codes
  - Variants of Gabidulin codes

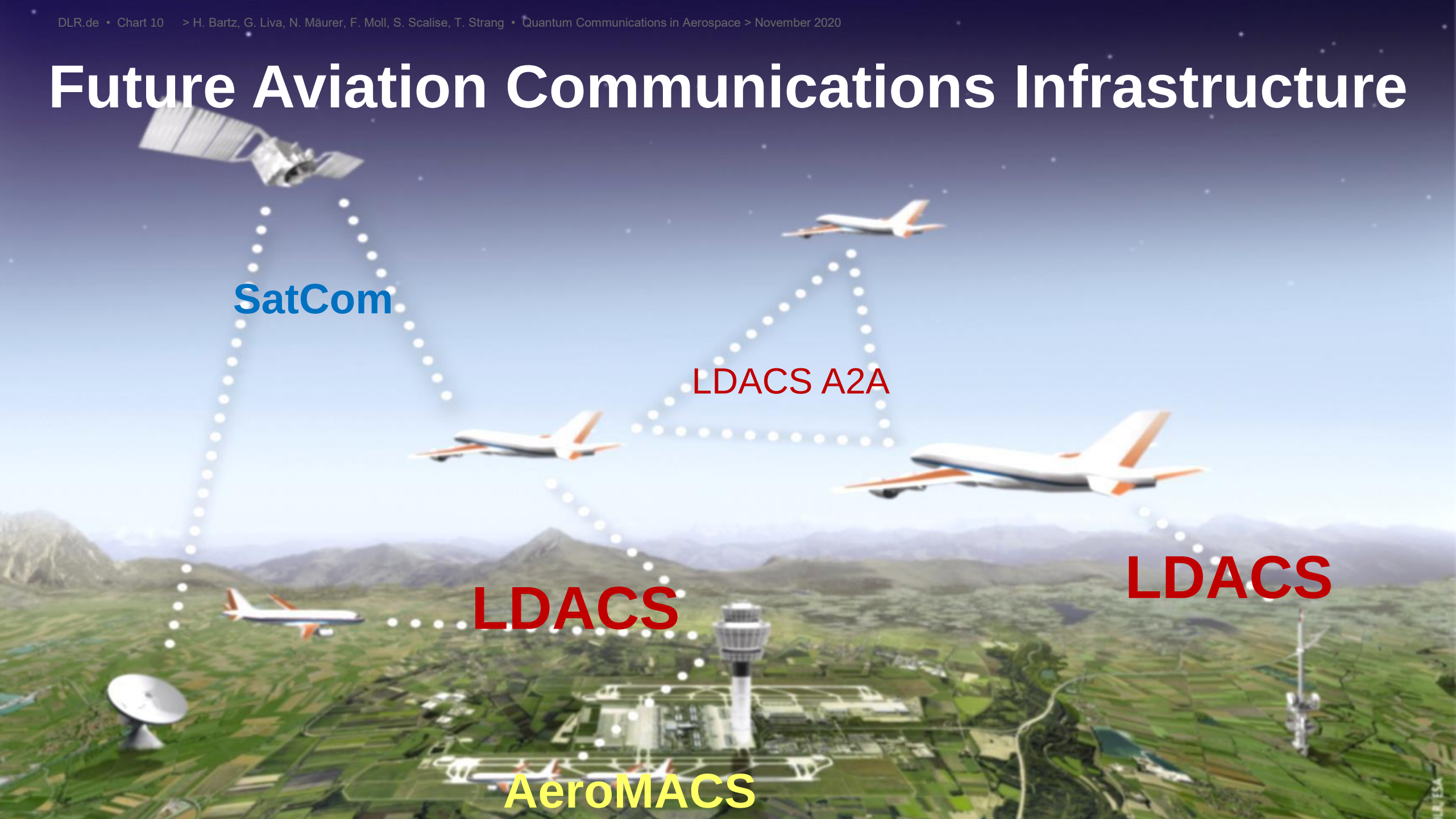
=> *The results above allow for smaller key-sizes at a fixed security level*

Work about the cryptanalysis of code-based cryptosytstem

- Identification of weak keys in the Faure-Loidreau cryptosystem
- Generic decoding algorithm for rank-metric codes (accepted at PQCrypt 2020)

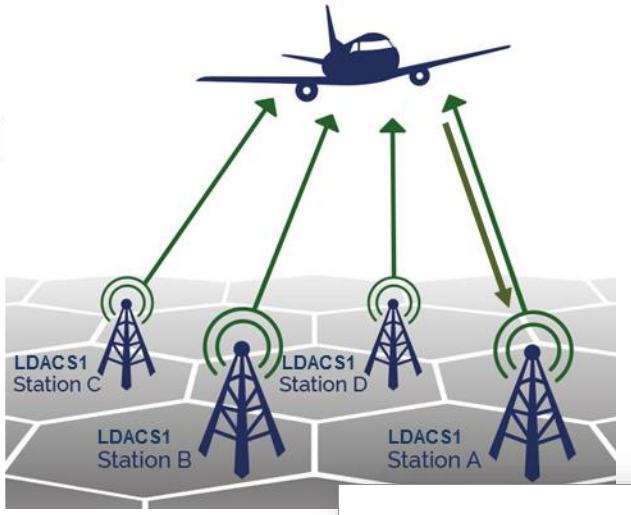
=> *These results are improtant to ensure the resilience and security of code-based cryptosystems*

Future Aviation Communications Infrastructure



Digital Datalinks – LDACS

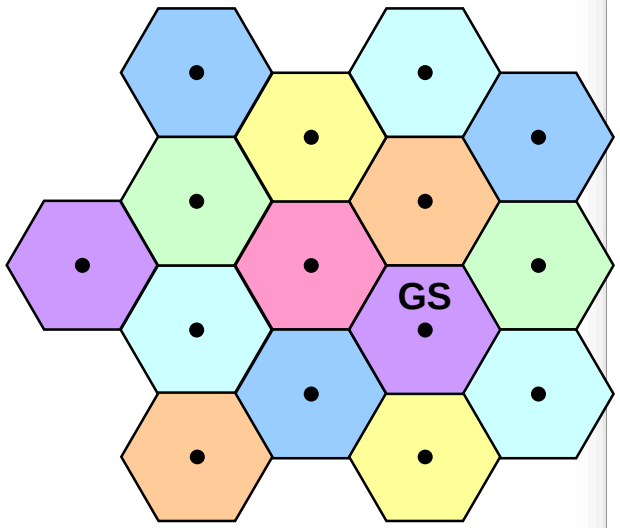
- Terrestrial digital wireless communication system for civil operational aeronautical Safety-of-Life communication

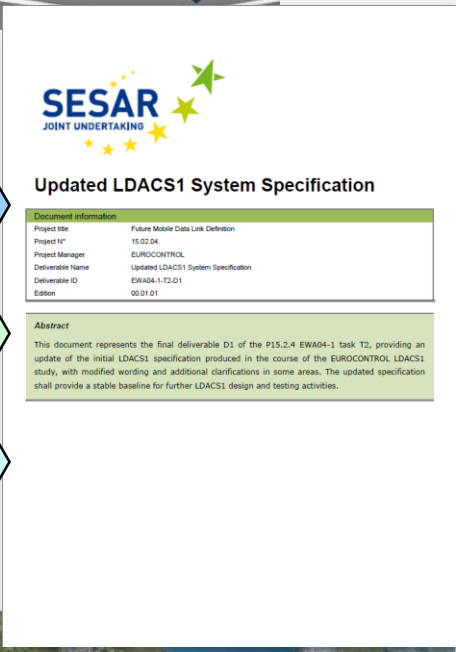


- Based on 3G and 4G technology
  - Cellular communication via ground-stations
  - Supports data and voice communication

  → **Sufficient bandwidth** for **secure communication**

  - LDACS as broadband extension of VDL mode 2




SESAR JOINT UNDERTAKING

Updated LDACS1 System Specification

Document information	
Project title	Future Mobile Data Link Definition
Project N°	15.02.04.
Project Manager	EUROCONTROL
Deliverable Name	Updated LDACS1 System Specification
Deliverable ID	EWA04-1-T2-D1
Edition	00.01.01

Abstract

This document represents the final deliverable D1 of the P15.2.4 EWA04-1 task T2, providing an update of the initial LDACS1 specification produced in the course of the EUROCONTROL LDACS1 study, with modified wording and additional clarifications in some areas. The updated specification shall provide a stable baseline for further LDACS1 design and testing activities.

- Standardization in ICAO with DLR in the lead

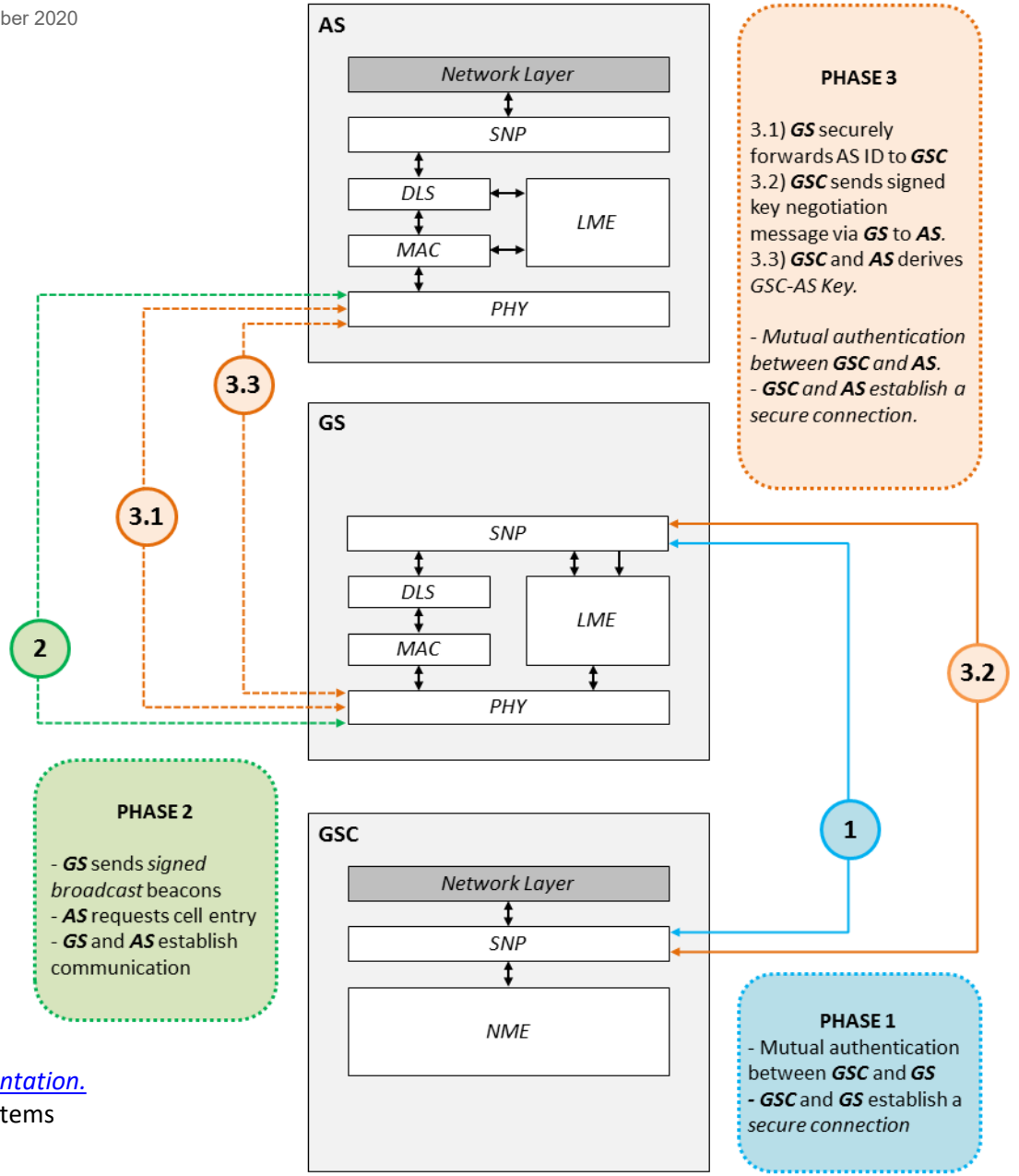
- LDACS prototype with flight trials in march 2019

Cybersecurity for LDACS

LDACS follows a **Security by Design** approach addressing all typical aspects including…

- Protecting **availability** and **continuity** of service
- Protecting the **integrity of messages in transit**
- Ensure the **authenticity of messages in transit**
- Ensure **nonrepudiation of origin for messages in transit**
- Protecting **confidentiality of messages in transit**
- Provide **mutual entity authentication schemes**

…in every component and every protocol step of the entire ground and airborne architecture



Mäurer, Nils und Gräupl, Thomas und Schmitt, Corinna (2019) *Evaluation of the LDACS Cybersecurity Implementation.* In: 2019 AIAA/IEEE 38th Digital Avionics Systems Conference (DASC). 2019 AIAA/IEEE 38th Digital Avionics Systems Conference (DASC), 08.-12. Sep. 2019, San Diego, USA.

LDACS on Air – Towards LDACS Validation

The World's First LDACS In-flight Demonstration in 2019

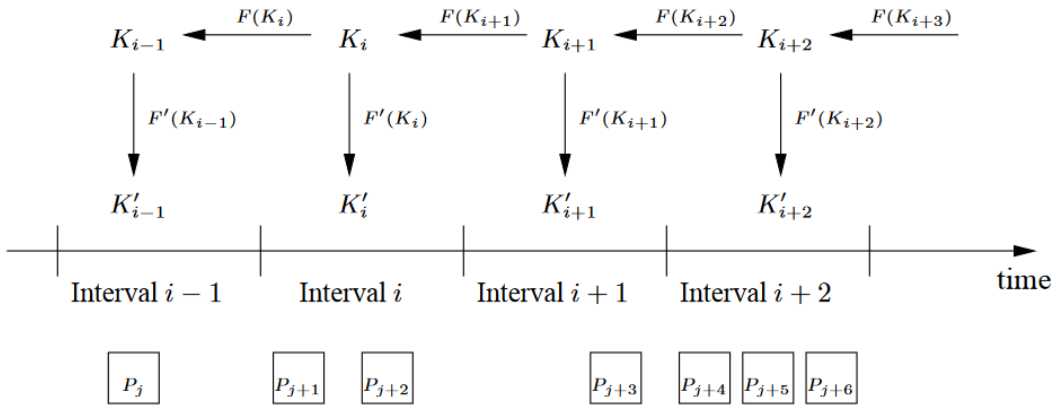
Demonstration of Secured Aeronautical Applications

- Secure transmission of standard services/applications

- Cyber-secure LDACS communications
  - Secure CPDLC and ADS-C applying next generation post-quantum cryptography (McEliece)
    - Secure msg application ("free text") and audio transmission
    - Post-quantum key exchange
  - Secure GBAS via LDACS applying modern broadcast authentication (TESLA)

- **We have shown the security design to work reliably**

TESLA – key chain

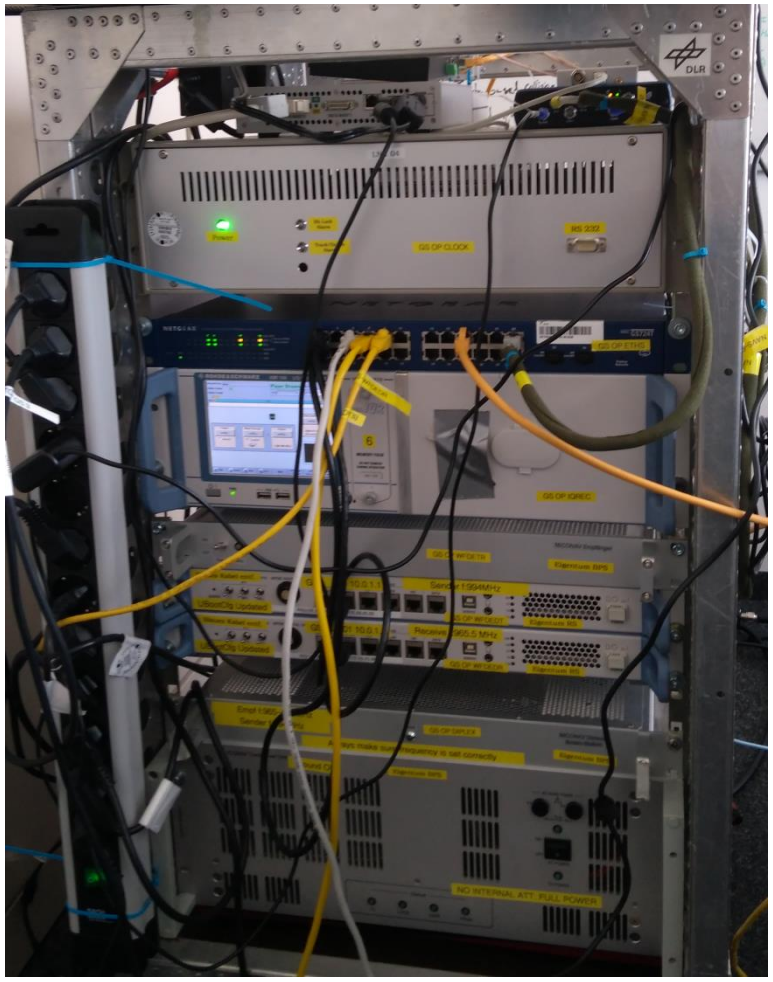


This flight campaign constitutes a major step towards LDACS validation

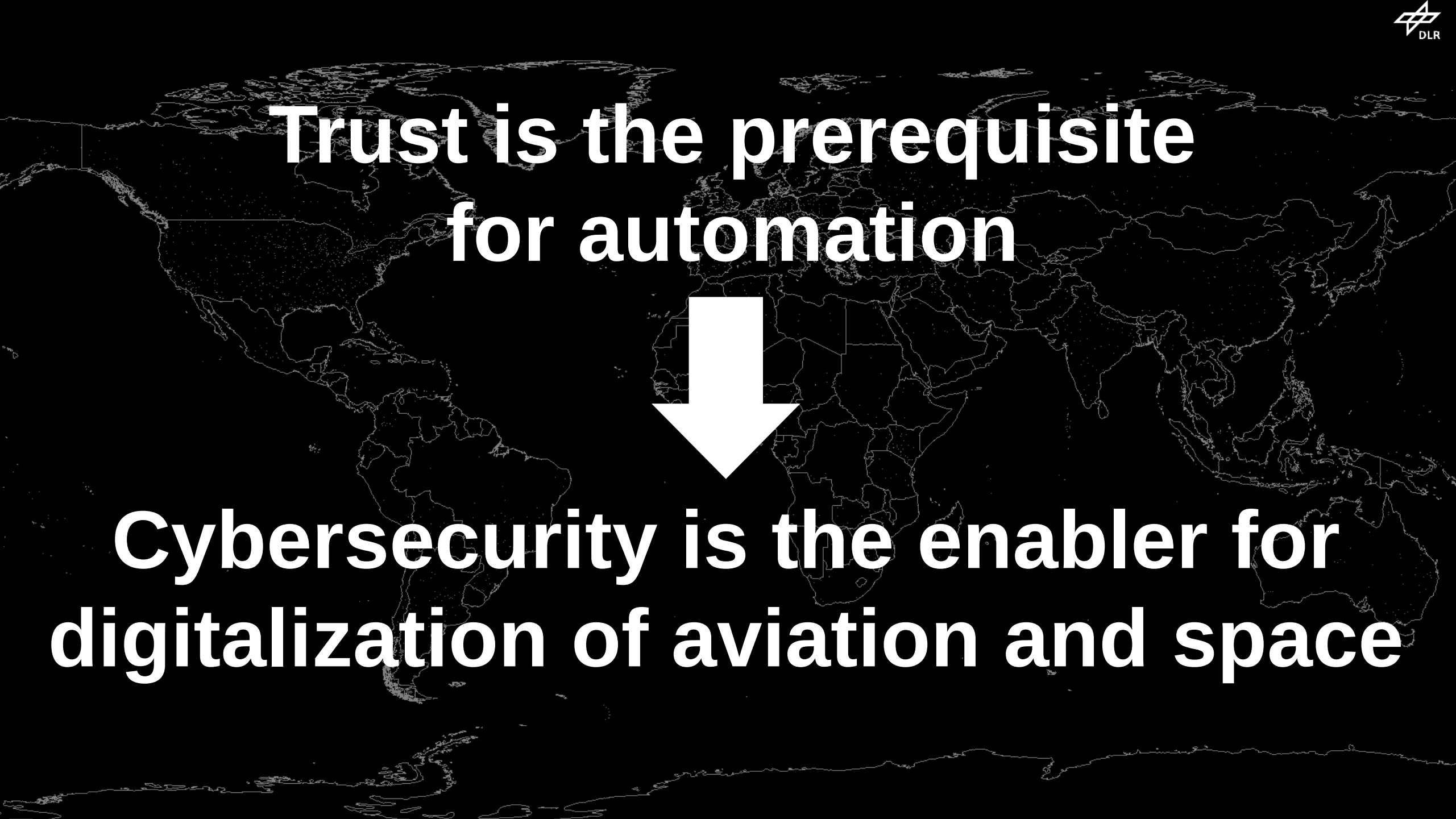
LDACS in Reality – Flight Trials in 2019

Airborne Station

Dassault Falcon 20



Groundstation


Trust is the prerequisite
for automation
Cybersecurity is the enabler for
digitalization of aviation and space