



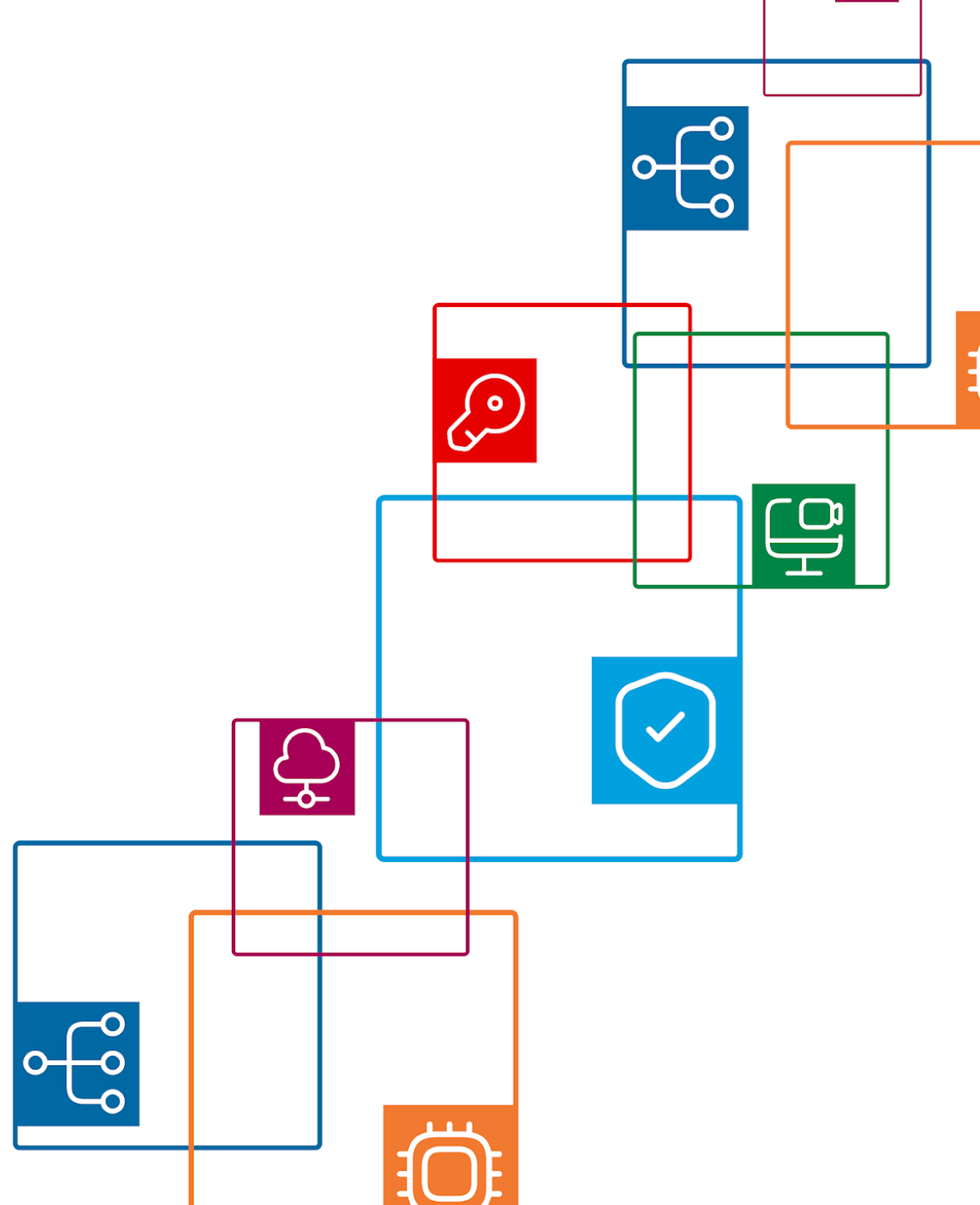
Bezpečnost na nejnižší vrstvě

Josef Vojtěch

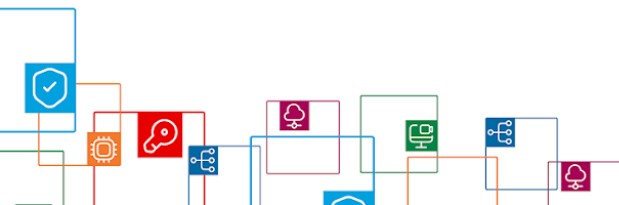
Oddělení Optických sítí

CESNET z.s.p.o.

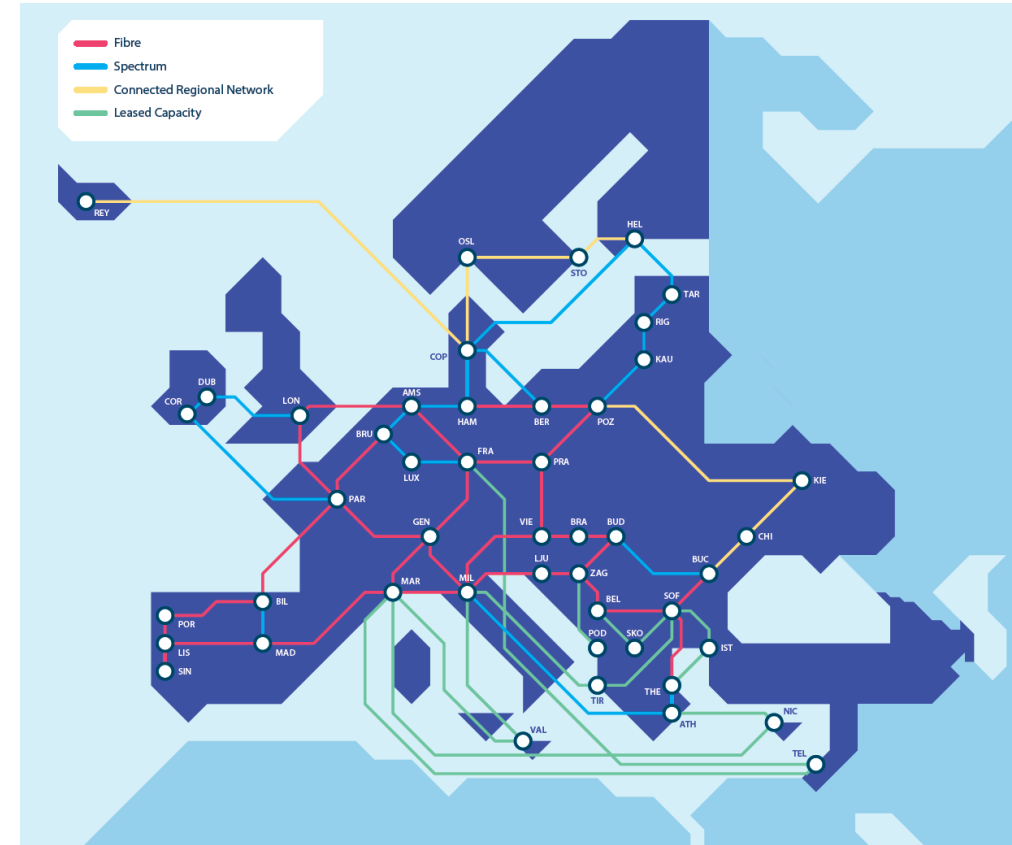
Konference CESNET, 30. 9. 2026



- TF sítě
 - GÉANT a Core-TFN
 - FOREST
 - Optická frekvence – propojení optických hodin
- Vlákenné snímání
- QKD - Kvantová distribuce klíče
- Závěr

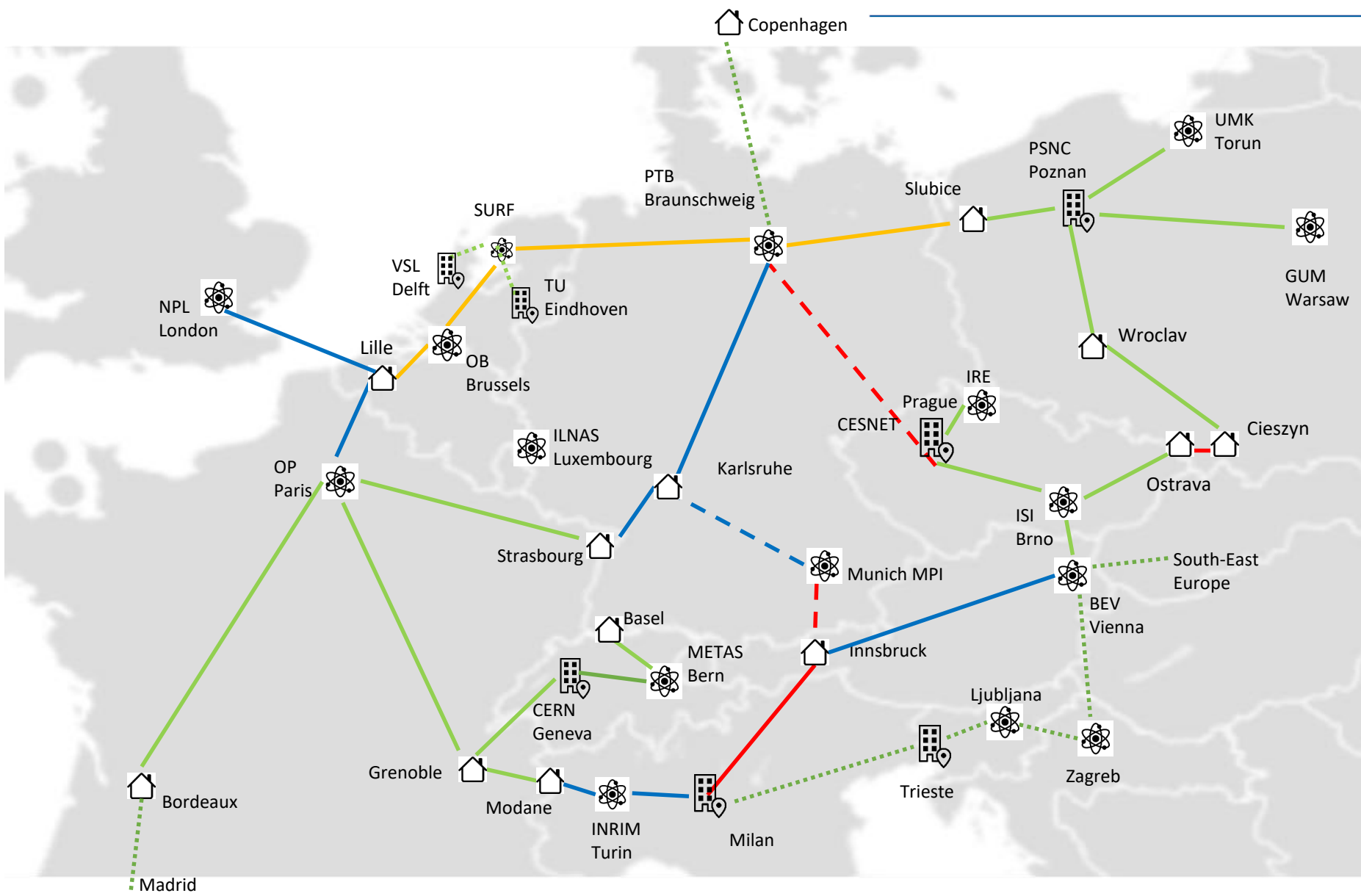


- GÉANT - série projektů vývoje sítě (cca 30 let), dnes 38 partnerů
- Dlouhodobá spolupráce v oblasti času a frekvence, snímání a QKD
- Special Interest Group for the Time and Frequency Network (SIG-TFN) od roku 2024, CESNET v řídící komisi
- Podpora PTB, REFIMEVE, GUM, INRIM, NPL, METAS, Observatoire de Paris, Observatoire de Bruxelles, VSL, UFE, FAMO, CERN.
- Dvě pracovní skupiny SIG-TFN:
 - T/F Sustainability (led by Richard Lui)
 - C-TFN technical specification (Led by Guy Roberts)



March 2025





Included:

- 10-year IRU for fibre on red routes
- Bidirectional amplifiers as needed to light the fibre on the red routes

Excluded:

- Green lines – fibre built by NRENs
- Blue lines – fibre built by NMIs
- Dashed green – proposed future links
- flywheels, counters frequency combs needed are to be funded by the national time/frequency providers
- Time/Frequency overlay services



NMI Frequency reference



Research institute



Hut for housing RLS

Adopted from Guy Roberts

Fiber-based Optical network for European Science and Technology (FOREST)

2026 zařazen na cestovní mapu ESFRI

<https://www.cesnet.cz/pro-media/ceska-stopa-v-evropske-infrastrukture-budoucnosti-cesnet-pomaha-budovat-sit-pro-prenos-extremne-presneho-casu-86>

- Hlavní směry:

Mezinárodní metrologie a experimenty s extrémní přesností v základní a aplikované fyzice

Kvantové komunikace (QKD)

Vláknové snímání pro geovědy a dohled infrastruktur

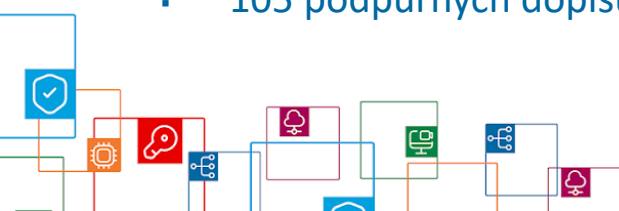
- Konsorcium 60 institucí ze 17 států EU, 13 NMI a 13 NREN

- Podpora:

- 13 odpovědných ministerstev z 10 států
- Ostatní výzkumné infrastruktury a další organizace: EPOS, JIVE, LOFAR, ESRF, GEANT, JRC, BIPM, EURAMET, CERN
- 105 podpůrných dopisů od dalších institucí, včetně >20 průmyslových partnerů



forest-ri.eu



- Jednotka času má přednost před definicemi hodnot ostatních jednotek SI, protože ji umíme určit s nejvyšší přesností/nejmenší nejistotou, tedy $<10^{-18}$
- V roce 2022 na 27. konferenci o vahách a mírách (CGPM) byla schválena rezoluce pro redefinici sekundy po roce 2030 s využitím optických hodin
- “Member States to support the development of national and international infrastructures mandatory for optical frequency standard comparisons”
- “As of today, **only** comparisons mediated by **optical fibre** links provide the required instability and accuracy for comparing optical clocks”

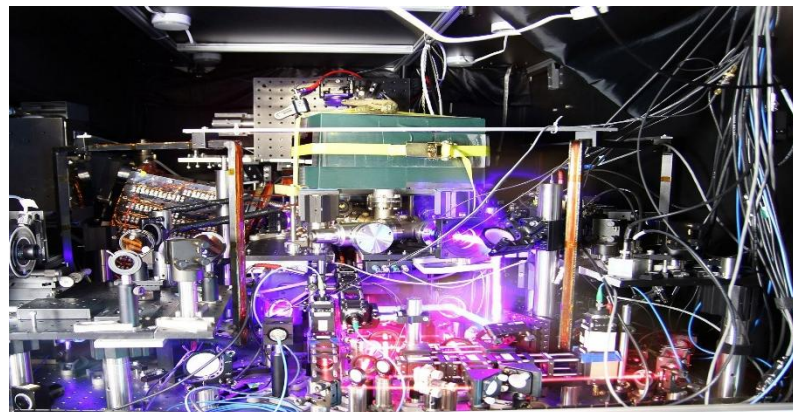


Foto: Ye group and Baxley/JILA

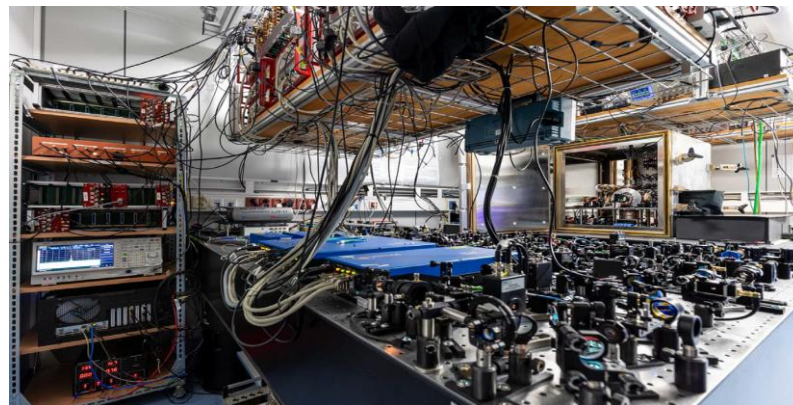
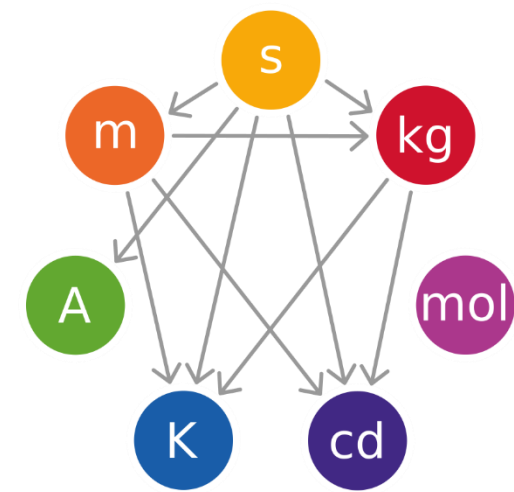
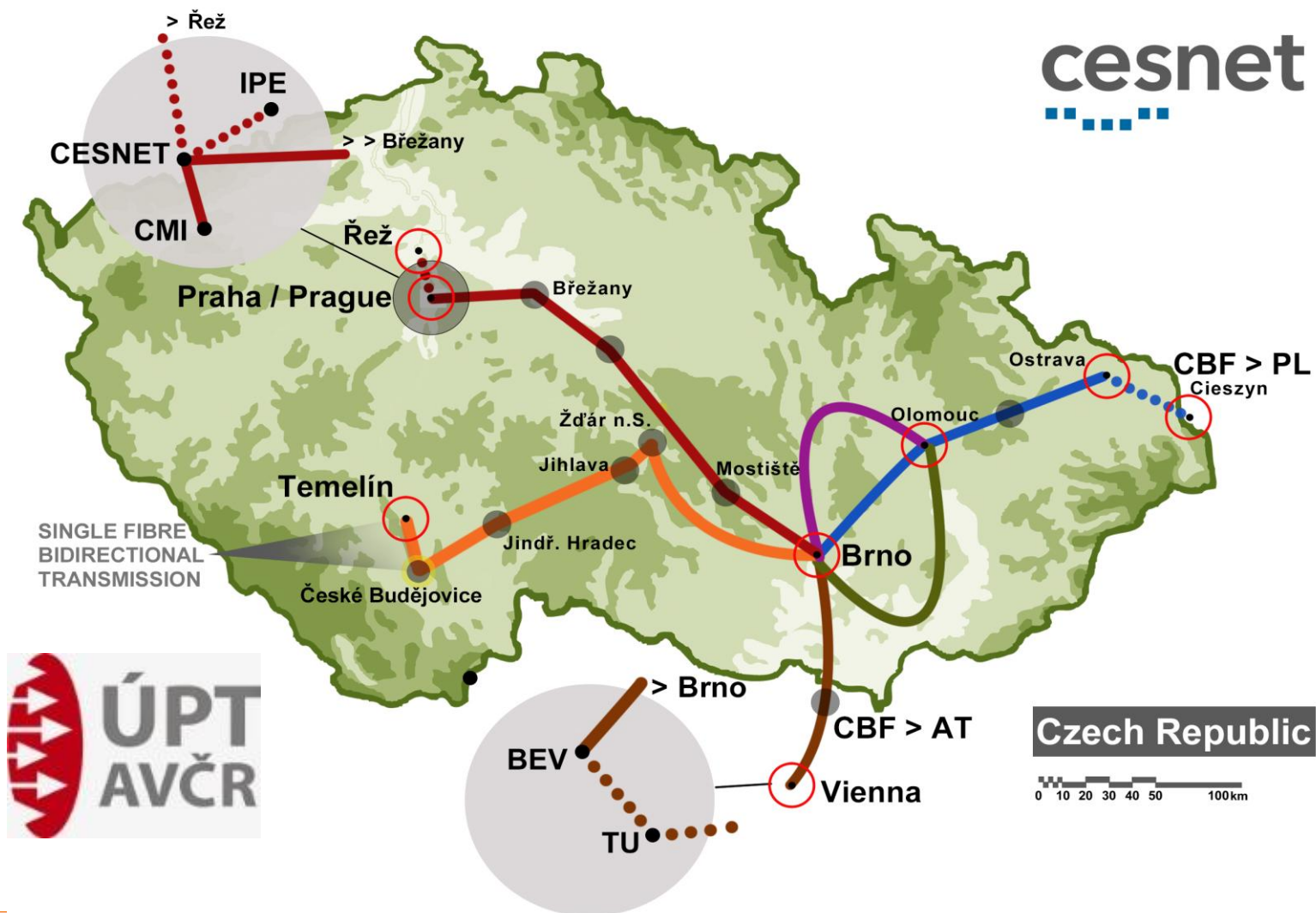


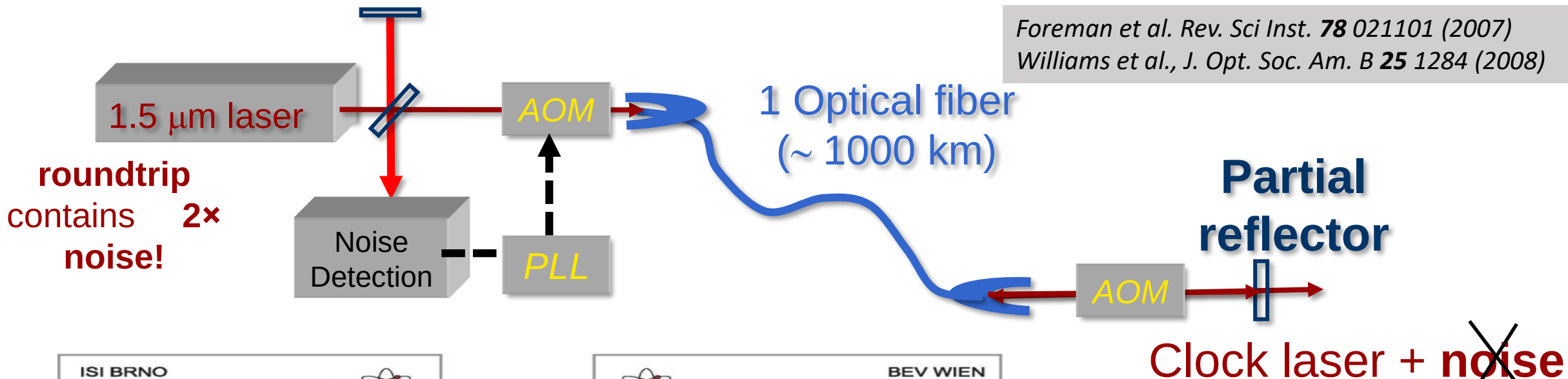
Foto: Laboratoř Ca⁺ iontových hodin ÚPT AV ČR



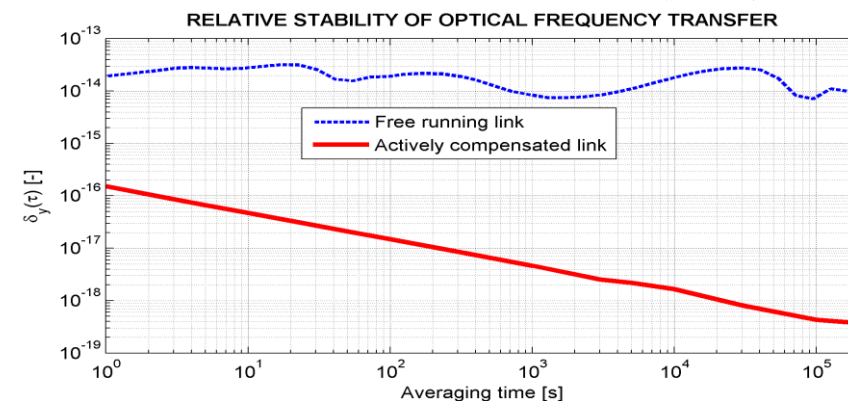
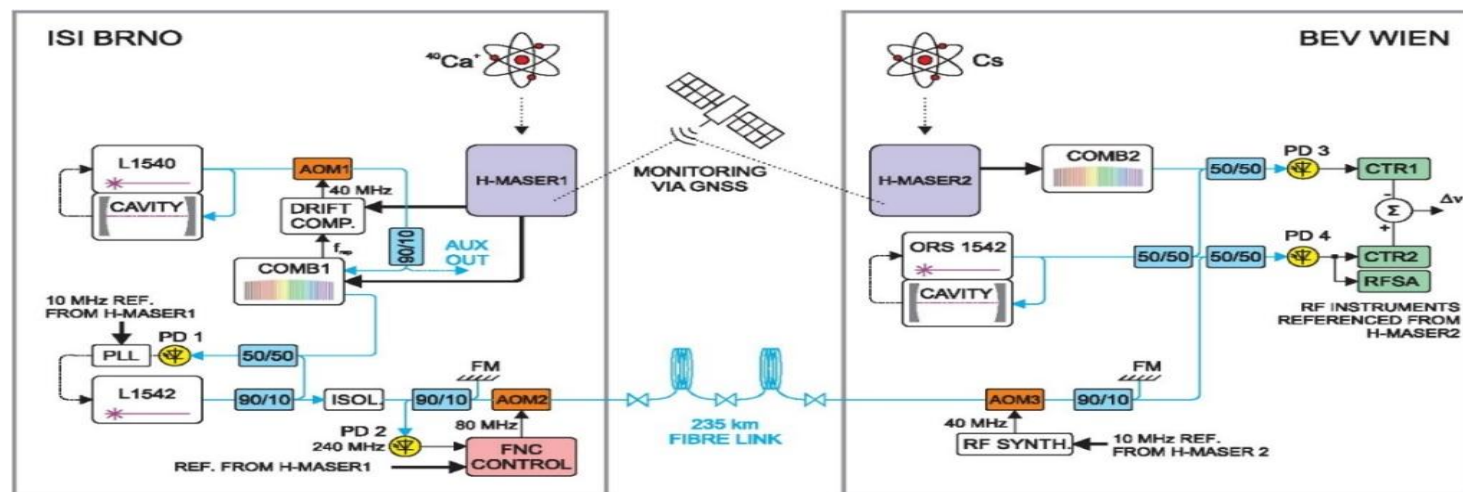
Soustava jednotek SI (2019)



- Využívá temné spektrum 1100 km, rozšíření na 1400 km
- Ztráty kompenzovány obousměrnými zesilovači (32 bidi EDFA)

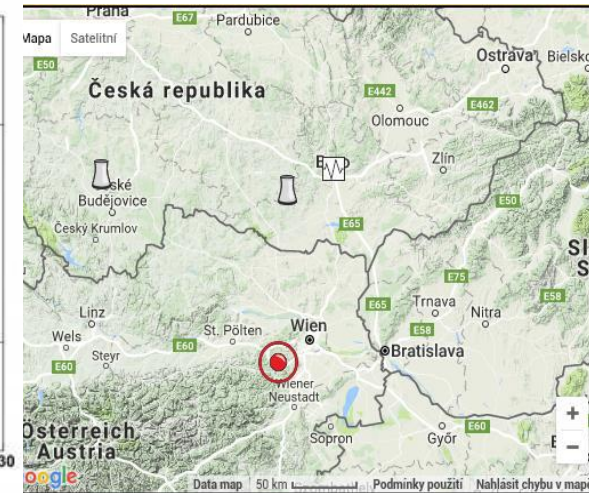
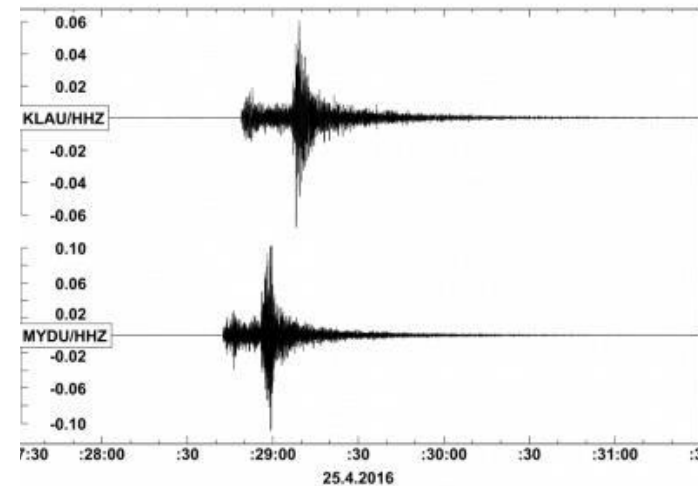
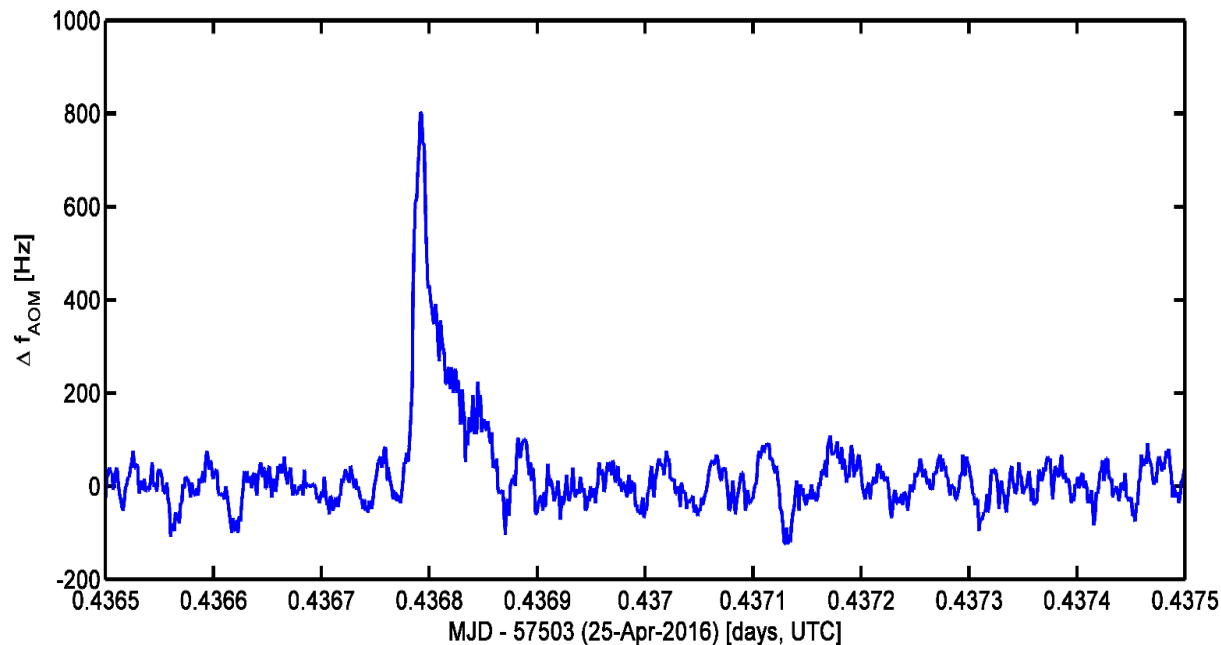


Foreman et al. *Rev. Sci. Instr.* **78** 021101 (2007)
Williams et al., *J. Opt. Soc. Am. B* **25** 1284 (2008)



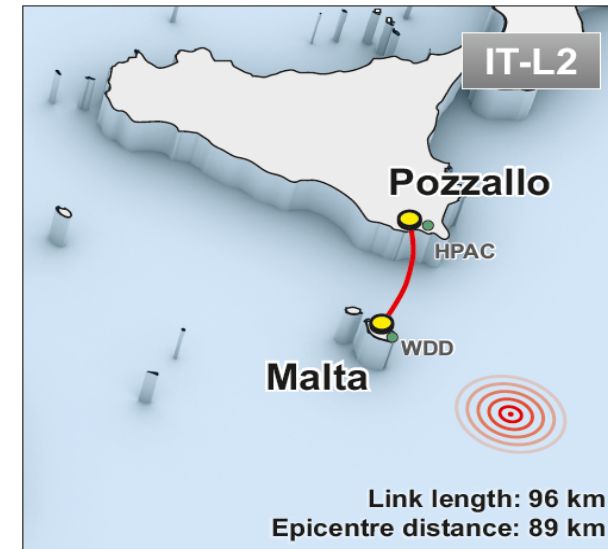
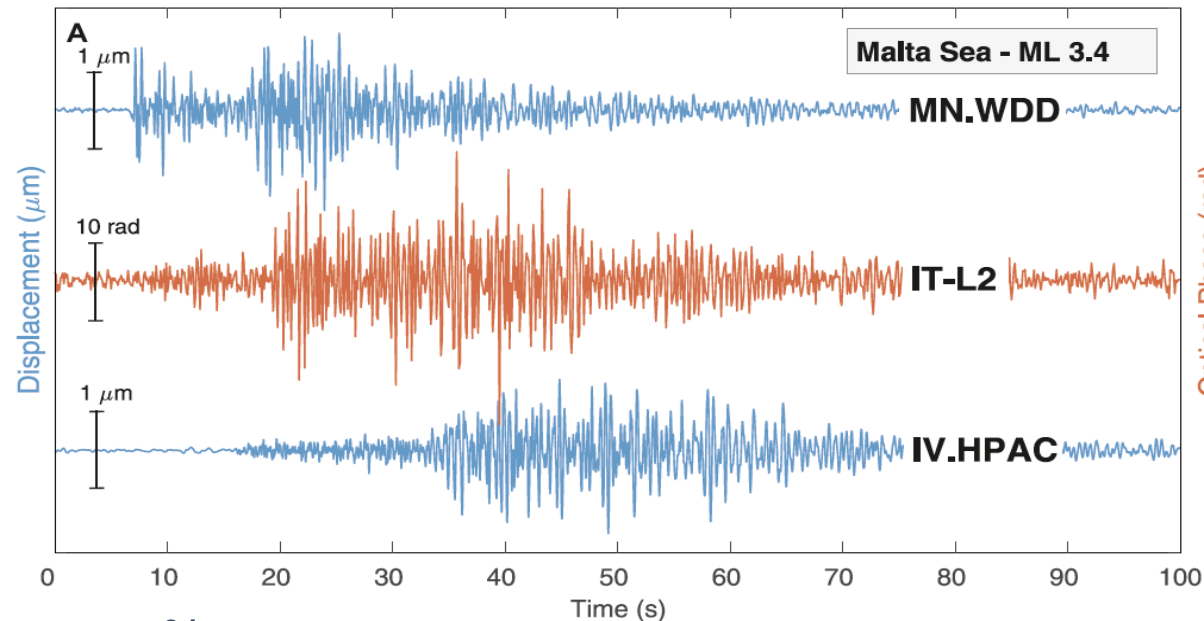
Cizek et al. *Opt. Express.* **30**, 5450 (2022)

- Aktivní stabilizace přímo zachytí zemětřesení
- 25, dubna 2016 – ML 4.1, epicentrum 20 km JV od Vídně



M. Cizek et al., "Transfer of stable optical frequency for sensory networks via 306 km optical fiber link," 2016 European Frequency and Time Forum (EFTF), 2016

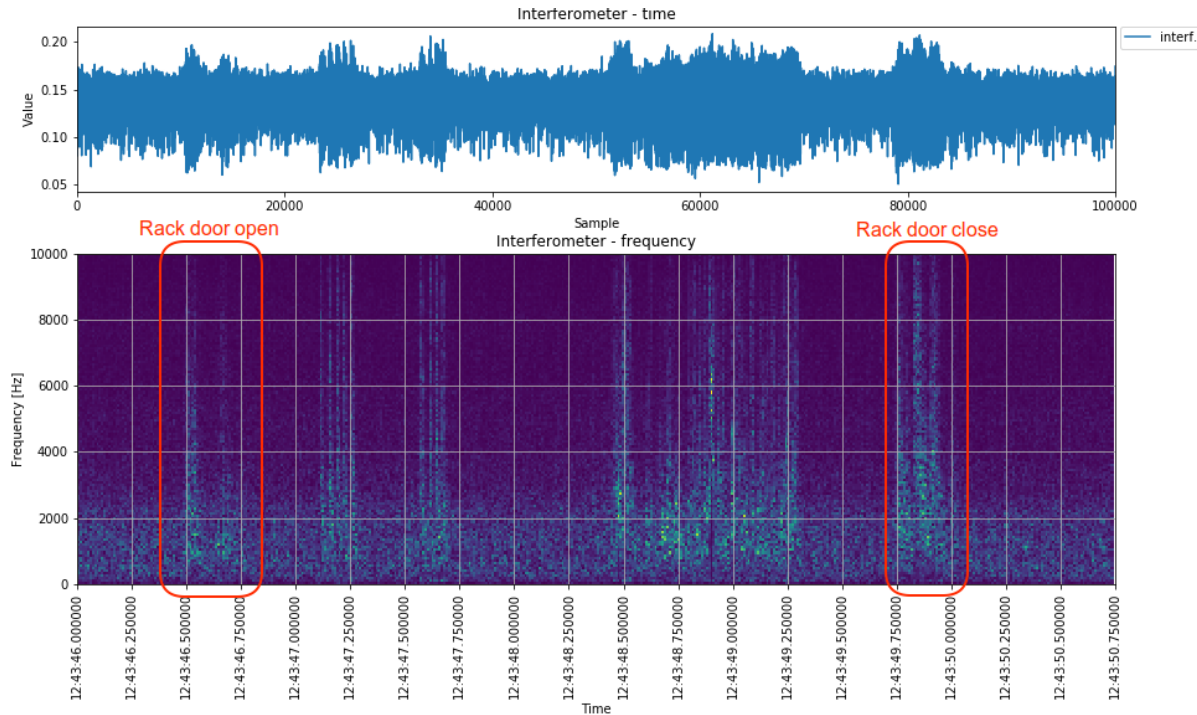
• Submarine optical link: Malta Sea earthquake - Sept 2017



G Marra, C Clivati, R Lockett, A Tampellini, J Kronjäger, L Wright, A Mura, F Levi, S Robinson, A Xuereb, B Baptie, D Calonico „Ultrastable laser interferometry for earthquake detection with terrestrial and submarine cables“, Science, 361, 486-49 (2018)

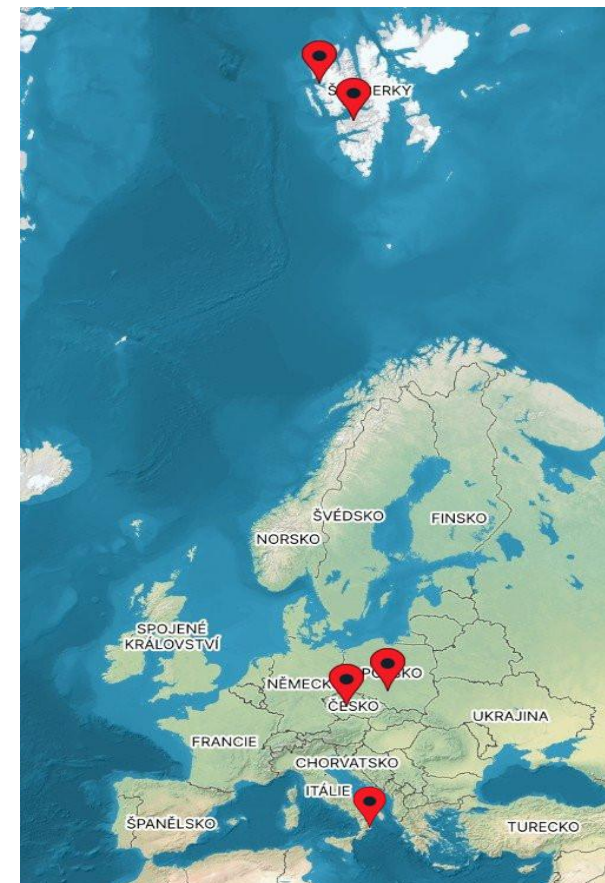
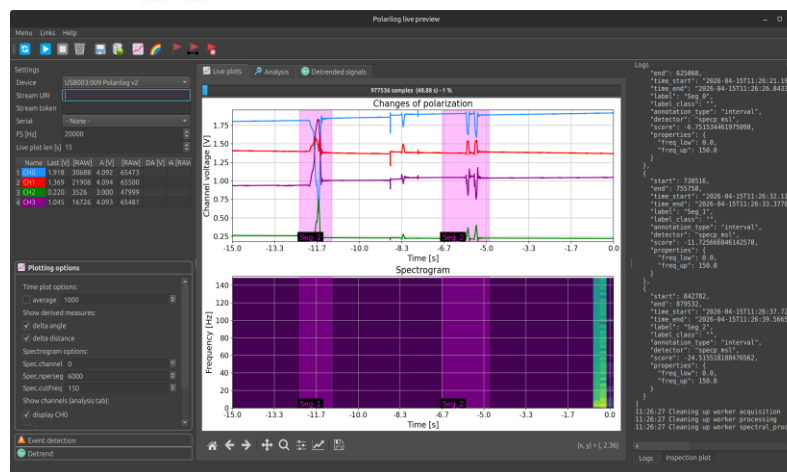
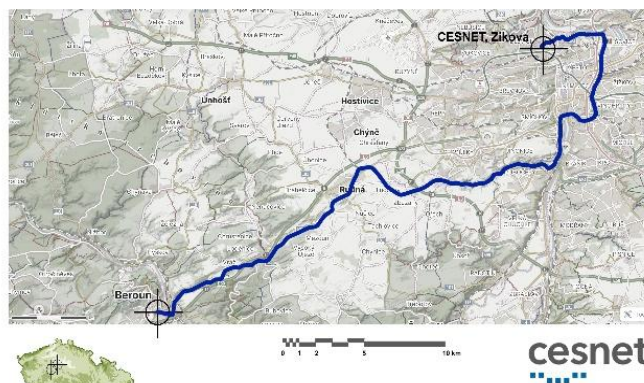
- 70% of the Earth's surface is water; Ocean Bottom
- Seismometers instalation difficult and expensive - Over 1 million km of submarine cable already installed
- Submarine fibre links are far quiet (up to 40 dB) compared terrestrial links
- Potential of important application: By detecting underwater earthquakes close to their epicentre, precious life-saving time could be gained in a tsunami warning

- Kampusové vlákno, interferometrická metoda

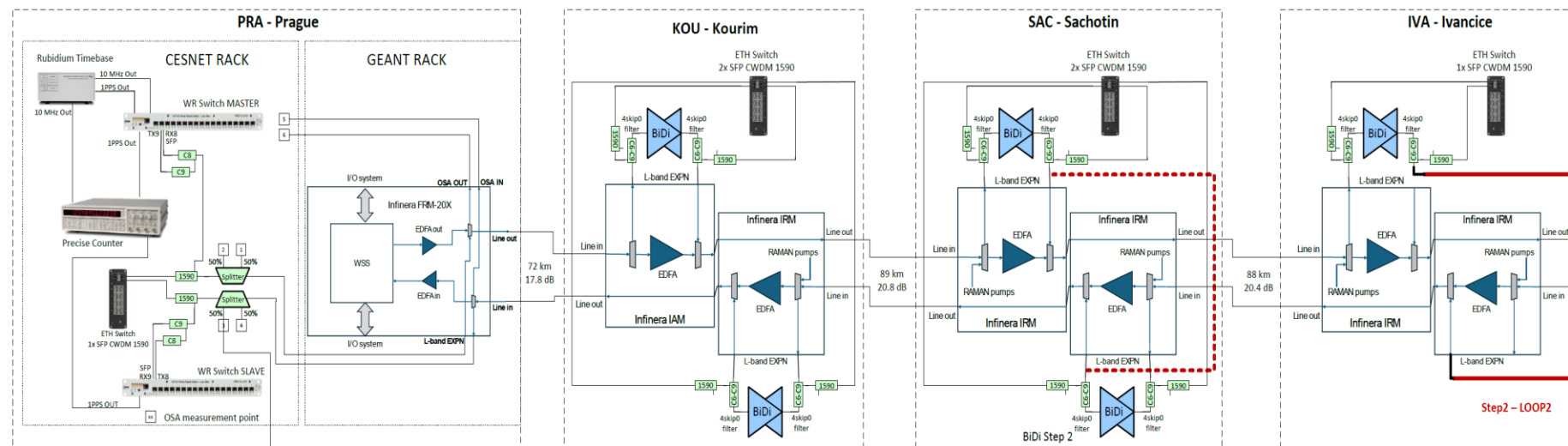
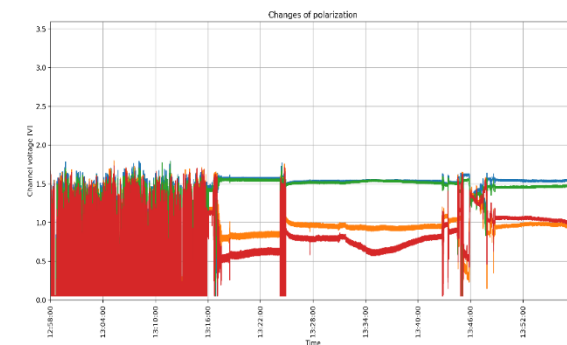
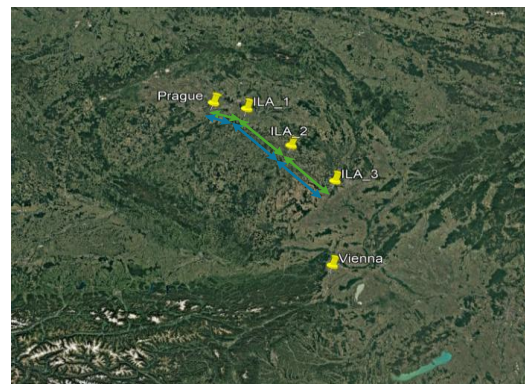


Slapak et al. IEEE Access, vol. 8, 183965 (2020)

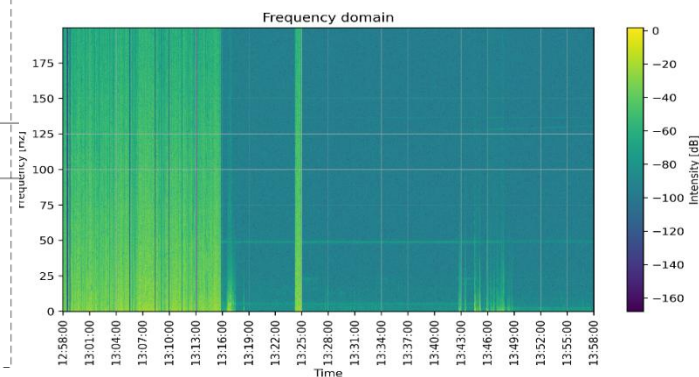
- Nevyžaduje kvalitní zdroj měřicího signálu
- Může měřit odposlechem
- Polbox adaptován pro HE projekt SUBMERSE
- Nasazeno
 - Praha–Řež od 2022/05 Praha-Beroun od 2024
 - Longyearbyen, Svalbard, NO od 2024/04
 - Ny-Alesund, Svalbard NO od 2024/04
 - Crotone-Preveza, IT-GR, od 2026/03 (GEANT)
 - GEANT long haul incubator, 2025



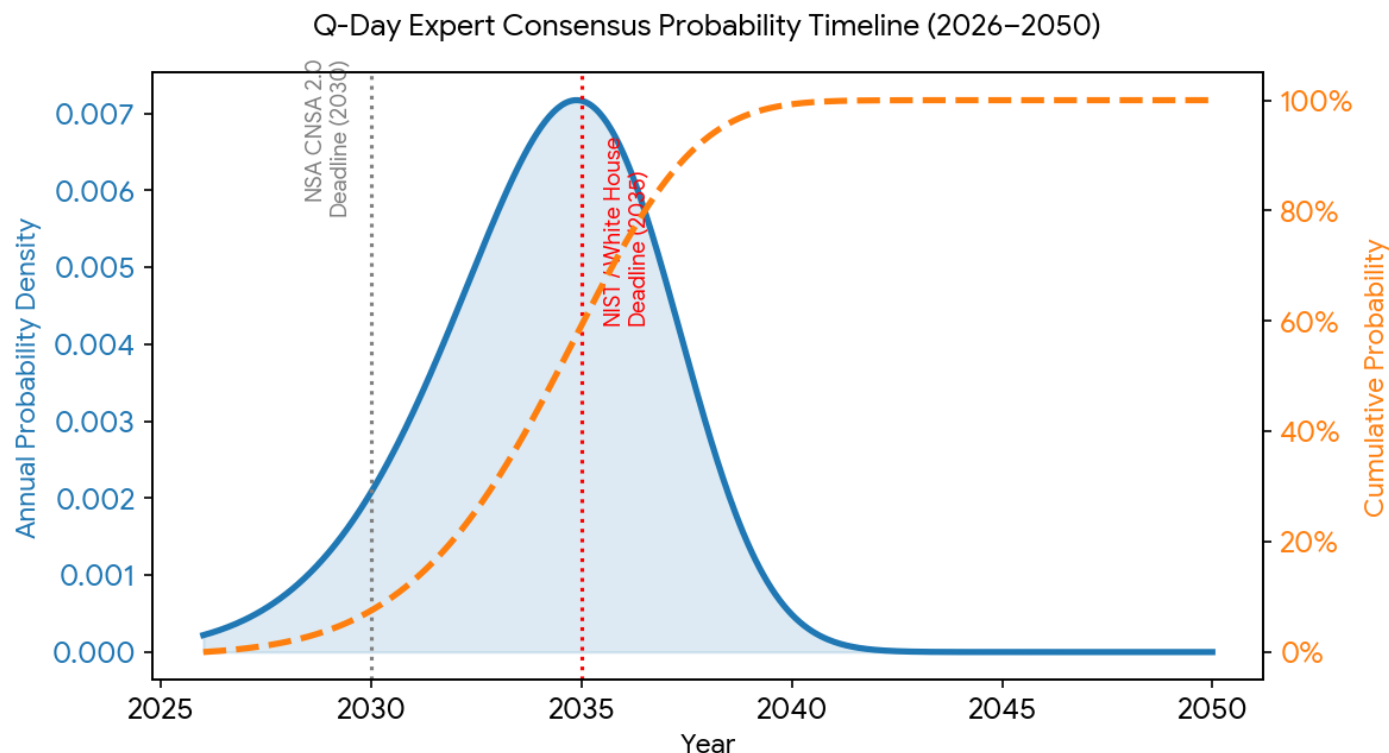
- 500km field trial v rámci Long-haul WR inkubátoru
- Smyčka na lince Praha Vídeň



GEANT - CESNET Trial Test White Rabbit BiDi EDFA Precise Time
 1. step: 3x BiDi, 322 km
 2. step: 5x BiDi, 498 km

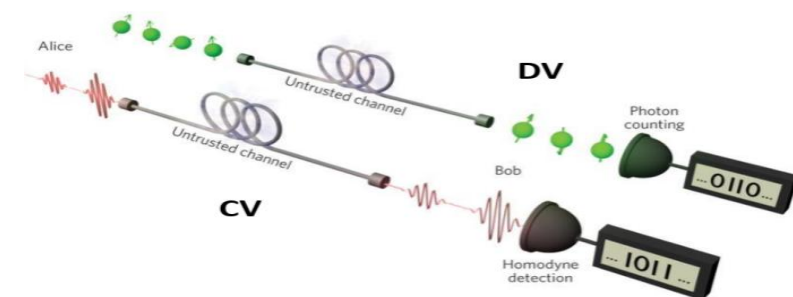


- Q-Day hypotetický bod zvratu kdy „kryptograficky relevantní kvantový počítač“ (CRQC) se stane dostatečně výkonným pro prolomení asymetrických kryptografických algoritmů, například RSA

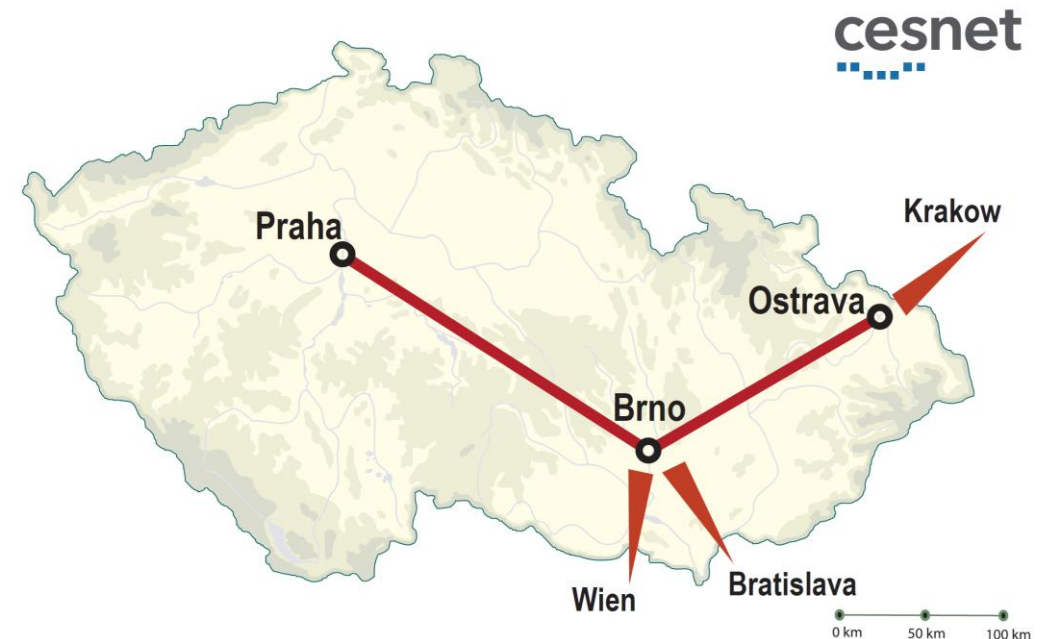


<https://quantumsecuritydefence.com/insights/what-is-q-day/>

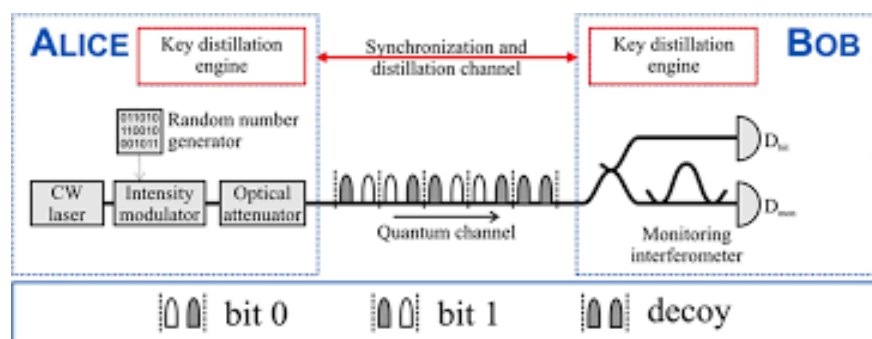
- QKD představuje metodu pro bezpečný přenos kryptografického klíče pro symetrickou kryptografii (např. Vernamova šifra - důkaz a není ohrožena kvantovými počítači).
- Dva základní přístupy – Diskrétní proměnné DV a Spojité proměnné CV
- DV-QKD
 - OpenQKD – 2021 první meziměstské nasazení v ČR
 - NESPOQ – 2021-2025 - QKD a PQC
 - NUCRYPT – 2023-2026 - zvýšení odolnosti QKD proti implementačním útokům
- CV-QKD
 - SEQRET – CV QKD benefituje z integrace, vhodné pro paralelní přenosy s daty

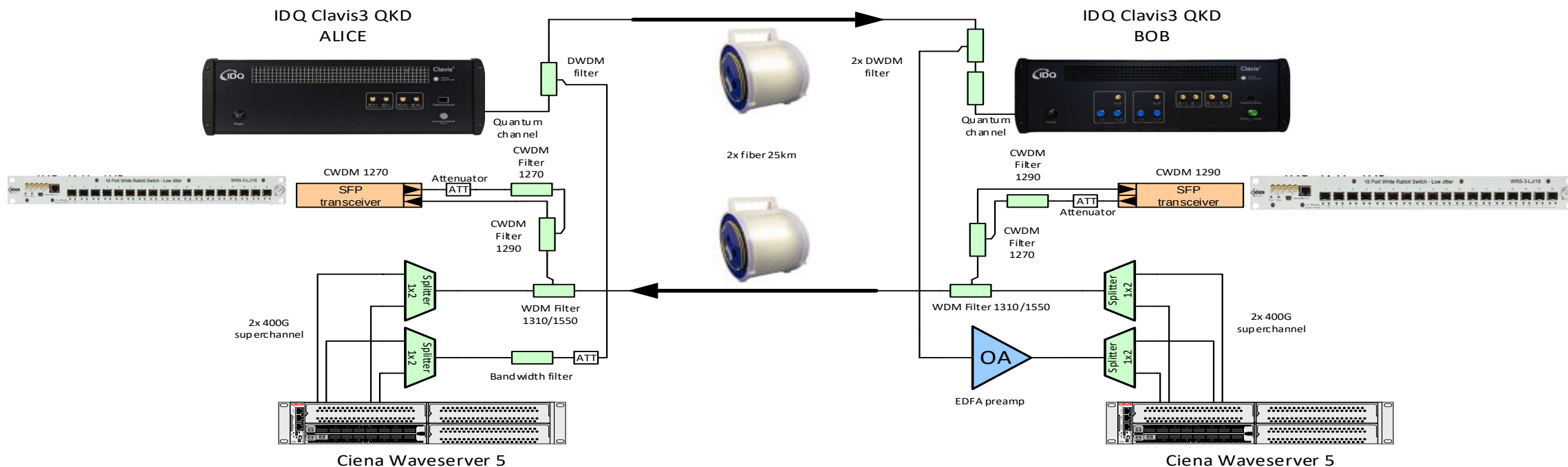


- CZ-QCI (výzva DIGITAL-2021-QCI-01-DEPLOY NATIONAL)
 - Vznikla páteř Praha-Brno-Ostrava (zařízení BB84 s návodnými stavy)
- Euro QCI (výzva CEF-DIG-2024-EUROQCI) 2026-6/2029
 - QCI-AT-CZ-PL
 - QCI-SK-CZ-PL



- Spolupráce s PSNC a TUO
- Ostrava - Cieszyn - 65 km, 16 dB
- Paralelní přenos White Rabbit a dat
- QKD systém COW (Coherent one Way protocol)

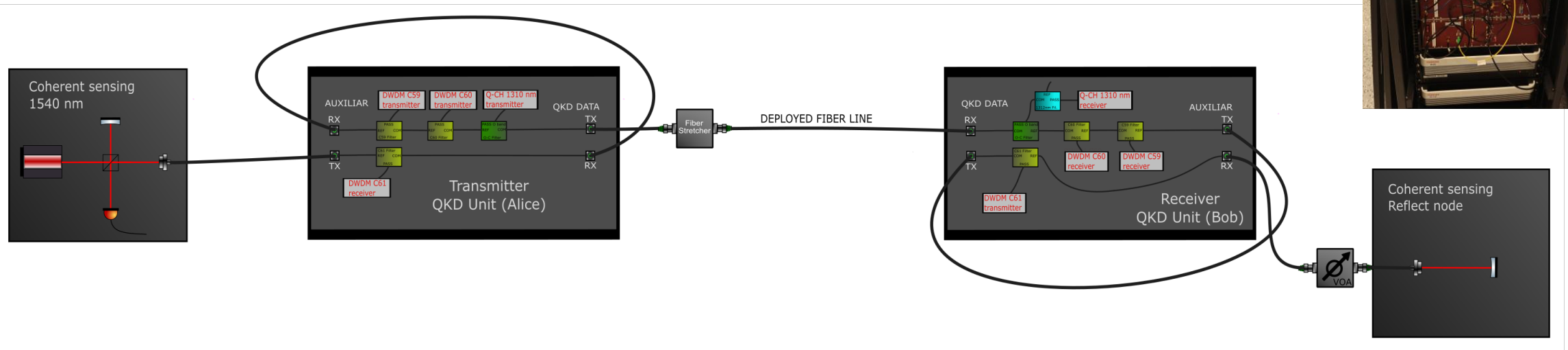
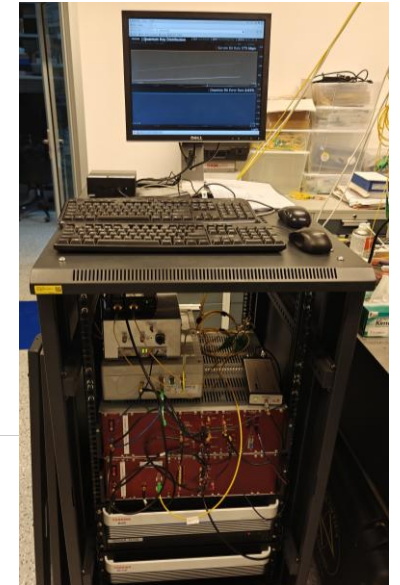




CESNET test - Superchannel 2 x 400Gbit/s plus QKD system

Jan Radil, Martin Šlapák, Rudolf Vohnout, et al "Quantum and Data Signals in a Single Fiber – Multiplexing by Smart Use of High-Grade Filters," in IEEE Communications Letters, doi: 10.1109/LCOMM.2025.3545315

- Využívá pro snímání jak fázi (přenos optické frekvence) tak polarizaci
- QKD (BB84 s návnadovými stavy)
- Koordinátor ÚPT AVČR

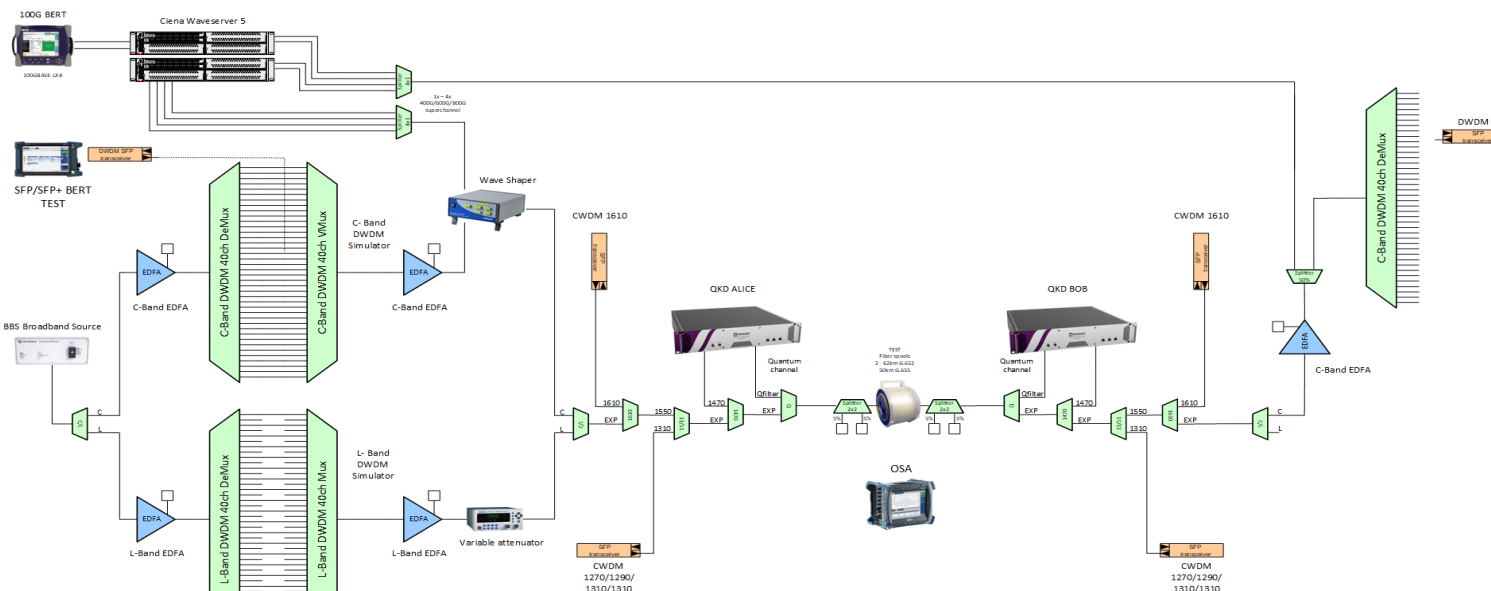


- **QCI 01- INDUSTRIAL – SEQRET, koordinuje KEEQuant**
- Paralelní přenos CV-QKD se zašifrovanými 400Gbps daty
- Zdá se že bylo dosaženo nejvyššího výkonu klasických kanálů přenášených s QKD

CESNET and KEEQuant showcase scalable Quantum Key Distribution (QKD) technology in real-world testbed

Kvantová bezpečnost na dosah: CESNET otestoval novou generaci šifrování dat

10. prosince 2025



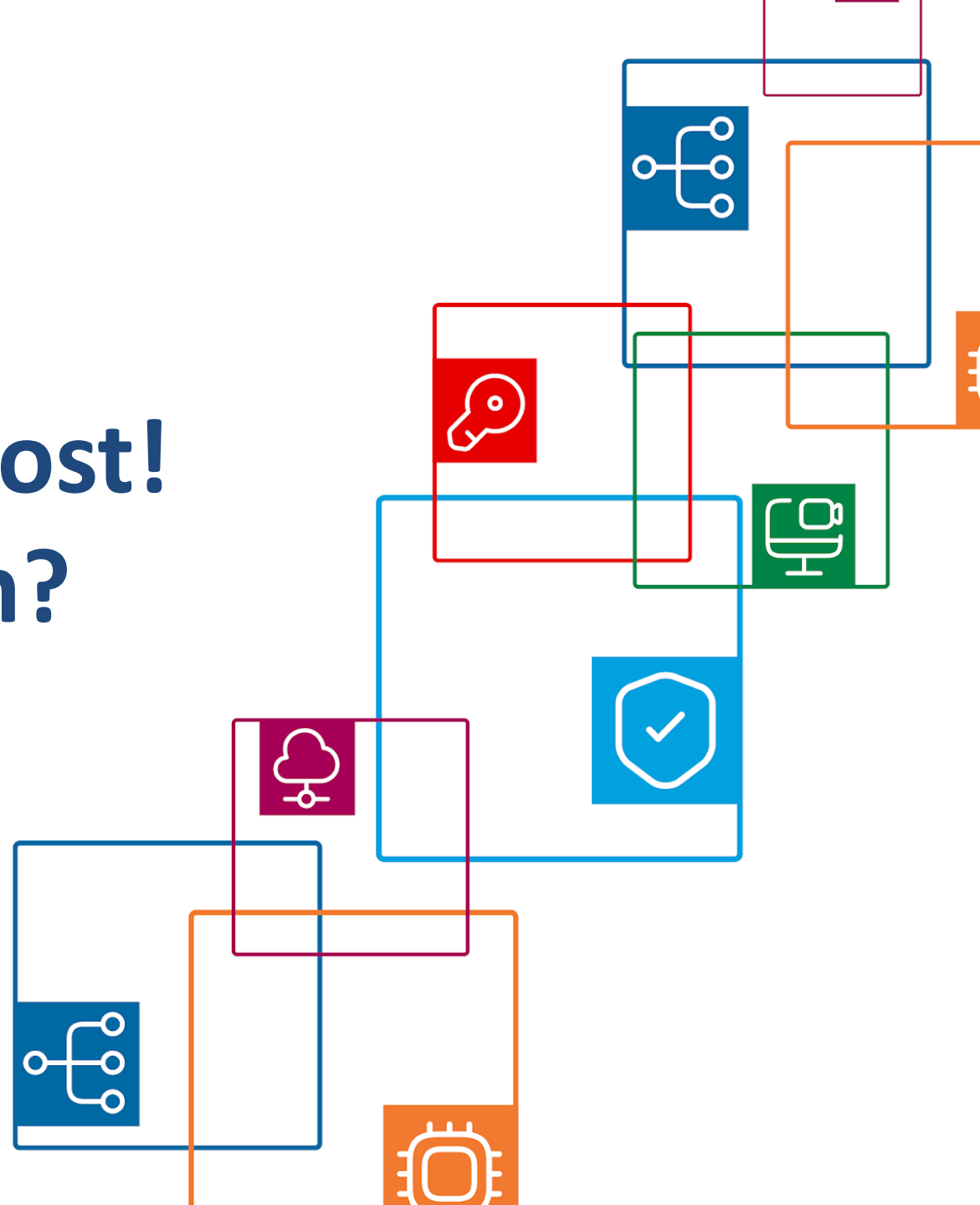
- White Rabbit a optická frekvence jsou důležité nedatové aplikace sítě CESNET3
- SDN přenosový systém CzechLight – dlouhodobě prověřené řešení pro dlouhodobé přenosy jak přesného času tak optické frekvence (nasazeno také např. ve Švýcarsku)
- CESNET je intenzivně zapojen do evropských aktivit GÉANT, SIG-TFN, WR collaboration a FOREST
- Optická síť může mít i sensorické funkce (bezpečnost a včasné varování, atd.)
- QKD představuje matematicky nepodmíněnou odolnost proti útokům typu ulož teď a rozšifruj později
- Integrace TF do QKD v rámci EuroQCI
- Více QKD a sensingu zítra v sále Krakov





Děkuji za vaší pozornost!
Vaše otázky prosím?

josef.vojtech@cesnet.cz



Vývoj hodin



2012

Ion Clock

High-accuracy optical clocks with trapped ions

2016

OC18

Optical clocks with 1E-18 uncertainty

2019

ROCIT

Robust optical clocks for international timescales

Linkové technologie



NEAT-FT

New tools for optical frequency transfer

OFTEN

European network for optical clock comparisons

TiFOON

Optical time and frequency transfer

Návrh sítě



CLONETS

Strategy for a pan-European T/F network

CLONETS-DS

Design study for a pan-European T/F network

- Polarisation method in the field, dedicated CW source and passive listening along railway lines

