Phil Evans

Oak Ridge
National Laboratory

Timing Authentication Secured by Quantum Correlations - TASQC

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

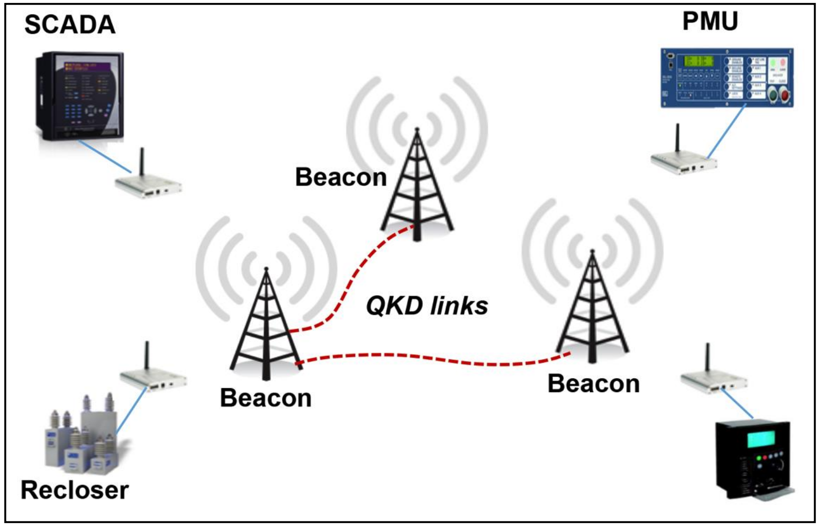
Summary: TASQC

Objective

- Provide an energy-centric secure timing distribution and message broadcast capability that can replace GPS

Schedule

- **Start**: January 2015
  End: May 2017
- IAB Formed: Q3 FY15
- Base system demo: Q4 FY15
- Message passing: Q1 FY16
- 2-way time transfer: Q2 FY16
- Demonstrations: ongoing



Performer:	Oak Ridge National Laboratory
Partners:	Pacific Northwest National Laboratory Sandia National Laboratories University of Texas Austin Qubitekk, Inc.
Federal Cost:	$2.998M
Cost Share:	-none-
Total Value of Award:	$ 2.998M
Funds Expended to Date:	% 78

Project Team & Roles

DOE National Laboratories

- **Oak Ridge - Lead**
  - Quantum, RF, software development. System integration.
- **Pacific Northwest**
  - RF, cyber security, power grid expertise. System integration and field testing
- **Sandia (Albuquerque)**
  - On-chip quantum technology integration with TASQC

Academia

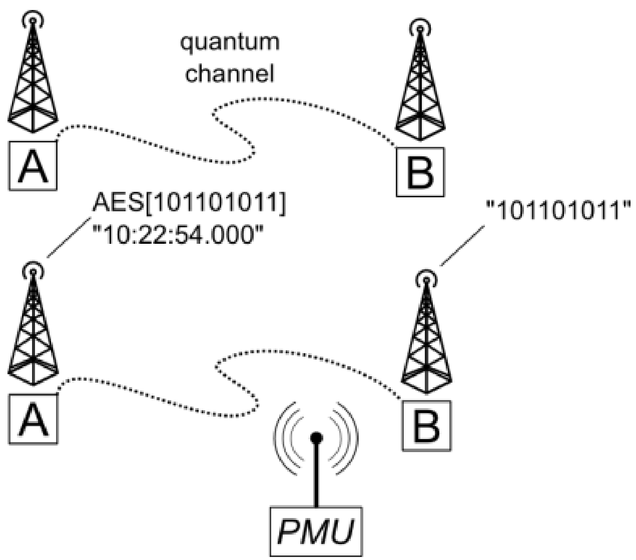
- **University of Texas, Austin**
  - RF and software development. GPS spoofing and time distribution expertise

Industrial Partner

- **Qubitekk**
  - Development of entangled-photon QKD hardware. Industry expertise

Advancing the State of the Art (SOA) (1)

- **There is no alternative source of secure time distribution for the grid**
  - GPS is widely used. **GPS is vulnerable to spoofing!**
  - eLORAN can provide < 100 ns timing. Currently mothballed. DHS funding limited trials.
- GPS is vulnerable because the signals are well known
  - One-way time distribution will **always** be susceptible to reply attacks
  - Security requires no *a priori* information on signal structure → total randomness
  - Can true randomness be used for secure time distribution with 2-way communication?
- **TASQC** – Timing Authentication Secured by Quantum Correlations
  - Backbone of QKD-connected base stations – *generate and share random keys*
  - Trusted clock source & time synchronization between base stations – *act as verifiers*
  - Base system technology to demonstrate variety of protocols on – *timing, message passing, etc.*



Advancing the State of the Art (SOA) (2)

- **Feasibility:** proof-of-concept has been demonstrated.
  - Requires existing fiber optic and RF/wireless infrastructure
- **Benefits:**
  - Time signals are encrypted with quantum keys and one-time pad crypto: **secure**
  - The stakeholder controls the system: **no reliance on third parties**
  - Flexibility: not just limited to time
    - Secure messaging capability, i.e., notifications of leap seconds
    - Increasingly complex suite of protocols for YOUR needs
- **Operational requirements:**
  - Will meet 1μs timing requirement for PMUs – IEC C37.118-2005
  - Will adopt IEEE-1588 and modify for secure 2-way time distribution
  - IRIG-B timing output for distribution to existing devices
- **Cybersecurity:**
  - Resilience against GPS interference and spoofing; satellite & space weather events

Progress to Date (1)

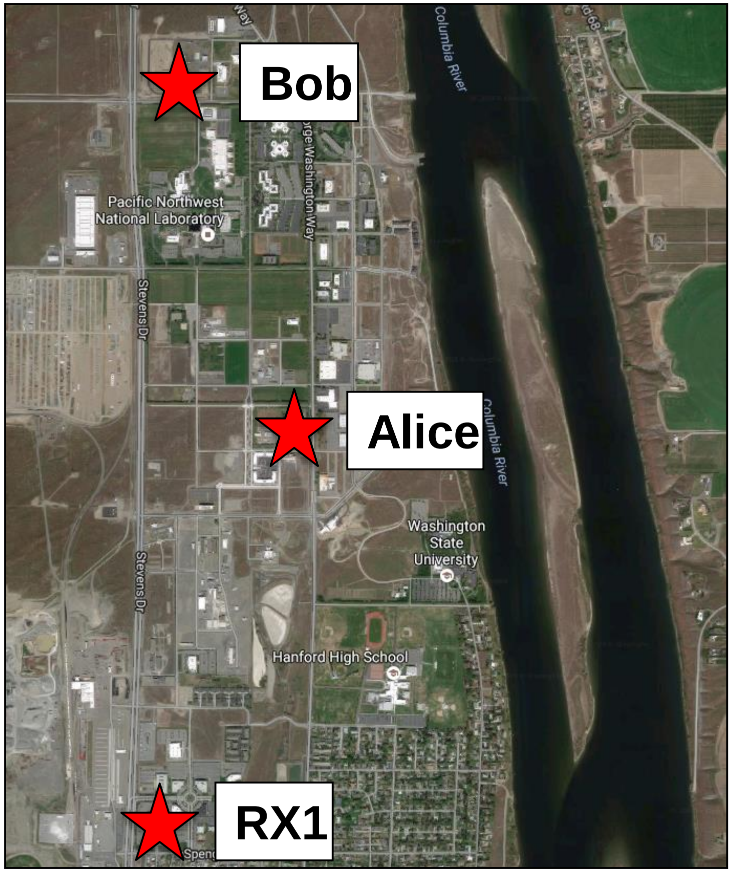
Major Accomplishments

- 3Q FY15: **Industry Advisory Board (IAB) Formation**
  - 11 members from energy & science communities
  - Rich Corrigan (SDG&E) is our Chairman
  - Schedule for webinars & progress reports
- 4Q FY15: **Base System Demonstration**
  - Task 1.8 (**Milestone**) Base Protocol Burn-in Testing @ ORNL ✓
  - Task 1.11 (**Go/**No Go) Prototype Testing @ PNNL ✓
- 1-4Qs FY16: **Protocol Demonstrations & Hardware Modifications**
  - Task 2.1 Encrypted code word ✓
  - Task 2.2 Anti-Replay attack (aka 2-way secure time distribution) ✓
  - Task 2.4 Communications task ✓
- 1Q FY17: **Adoption & modification of IEEE-1588 for TASQC**
  - IAB recommendation

Progress to Date (2)

Major Accomplishments

- Stand-up of PNNL Cyber-RF test range
  - Network & dedicated fiber links
  - 900 MHz antenna arrays
- Publications, conference & workshop presentations:
  - C. Lim *et al.* "Loss-tolerant quantum secure positioning with weak laser sources", *Phys. Rev. A* **94** 032315; [arXiv.org link]
  - L. Narula & T. Humphreys "Requirements for Secure Wireless Time Transfer" – *IEEE/ION PLANS Conference* 2016, Savannah GA; [link]
  - P. G. Evans "Quantum Technologies for Secure Wide-Area Time Distribution", *IEEE/NIST Timing Challenges in the Smart Grid Workshop* 2016, Gaithersburg MD



TASQC stations on the PNNL Cyber-RF test range. Bob → RX1: 2 miles

Challenges to Success

Mutual Understanding – Needs & Technologies

- Aligning needs and requirements with technology in development
  - Physics PhDs learn the power grid; power grid engineers learn quantum!
- Multi-faceted team with broad knowledge base
- Outreach, webinars, meetings at NASPI & Distributech

Absolute trust in GPS

- Educating the community: GPS is vulnerable and you need alternatives!

Availability of Suitable Optical Fiber Infrastructure

- Quantum requires low-loss, dark/unlit fiber runs. No optoelectronics.

Use of 'open' RF bands, e.g., 900 MHz ISM, is noisy

- Focus on RF development: work on error correction, spread-spectrum techniques to recover signal

Collaboration/Technology Transfer

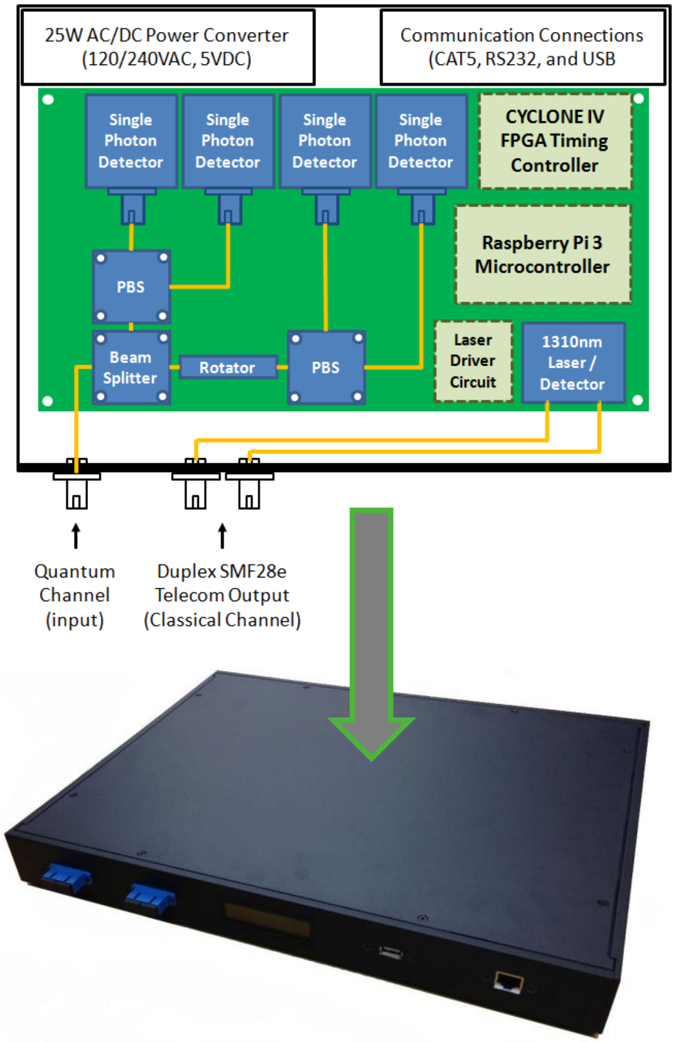
Plans to transfer technology/knowledge to end user

- Software developed is open source
- Qubitekk is our industry partner
  - TASQC is compatible with current and future Qubitekk systems
- Asset owners are most likely end users
- Plan to gain industry acceptance:
  - Utility-hosted field tests and demonstrations
    - (seeking more partners with appropriate test & verification facilities!)
    - See our interactive study here: https://www.surveymonkey.com/r/B9CSY7D
  - Adopting current standards
    - IEEE-1588 for time synchronization
    - Satisfying IEC C37.118-2005 for 1 μs time requirement
    - IRIG-B time output for integration with legacy equipment

Qubitekk - Enhanced Grid Security

Integration with entanglement-based QKD system:

- Polarization-entangled QKD system integrated with TASQC for maximum data security
- QKD system utilizes unique protocol between classical and quantum channel to maximize key bit rate
- Works over traditional telecom fibers
- Employs active polarization-compensation on quantum channel
- Can be used with pre-existing buried and suspended optical fibers
- Leverages existing DWDM technology



Entanglement-based QKD Receiver

Next Steps for this Project

Integration with different quantum technologies

- Different ‘flavors’ of QKD, suited for different infrastructure
- Will demonstrate TASQC with two other quantum systems:
  - Entangled photon QKD – Qubitekk
  - QKD-on-chip – Sandia

Industry-hosted testing & deployment studies

- Running TASQC on utility hosted test beds
- Conducting deployment study for variety of use cases

Publish & Transition

- Present results at conferences, publish in peer-reviewed journals
- Transition TASQC from basic to applied R&D; partner with industry

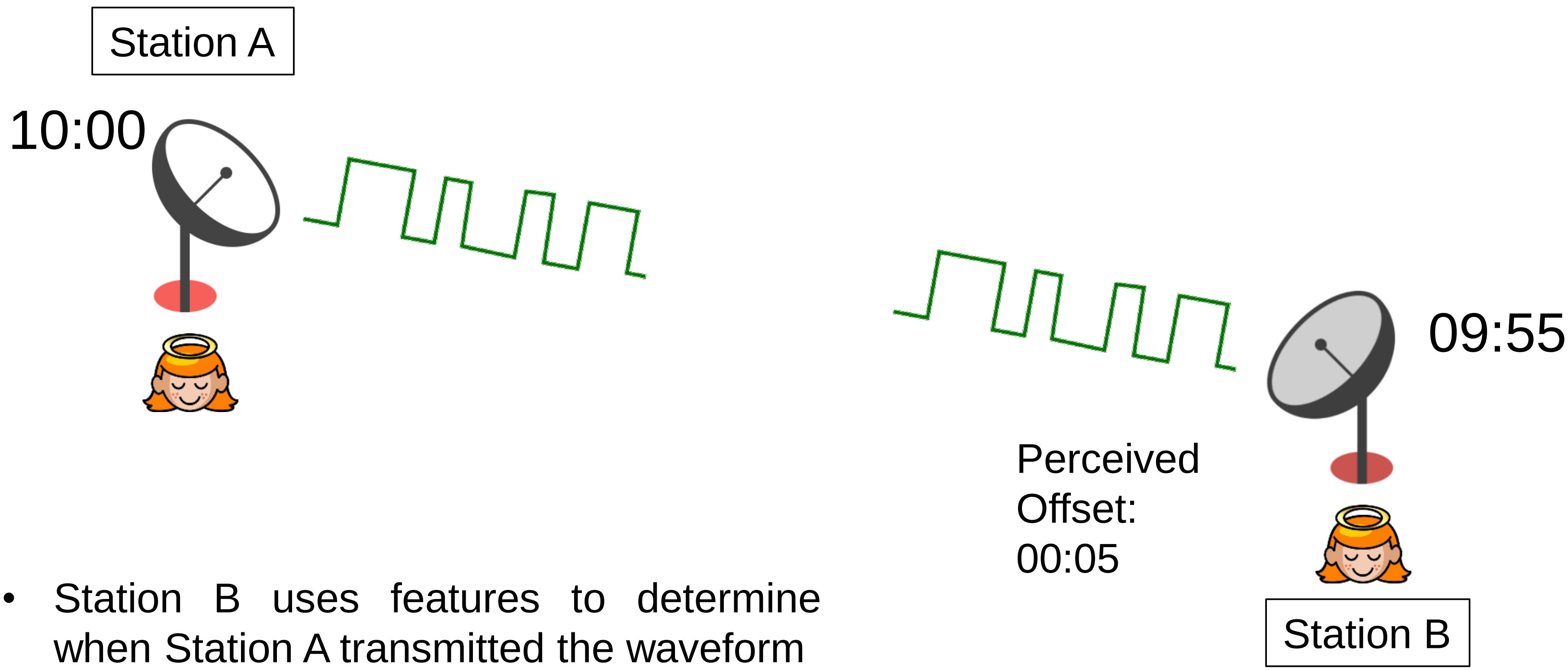
Thank You

Questions?

Additional Slides

1. Why 1-way time distribution is insecure
2. Conditions required for secure time distribution
3. The TASQC 2-way protocol
4. Implementation of the TASQC TX and RX stations

One-Way Time Distribution is Insecure



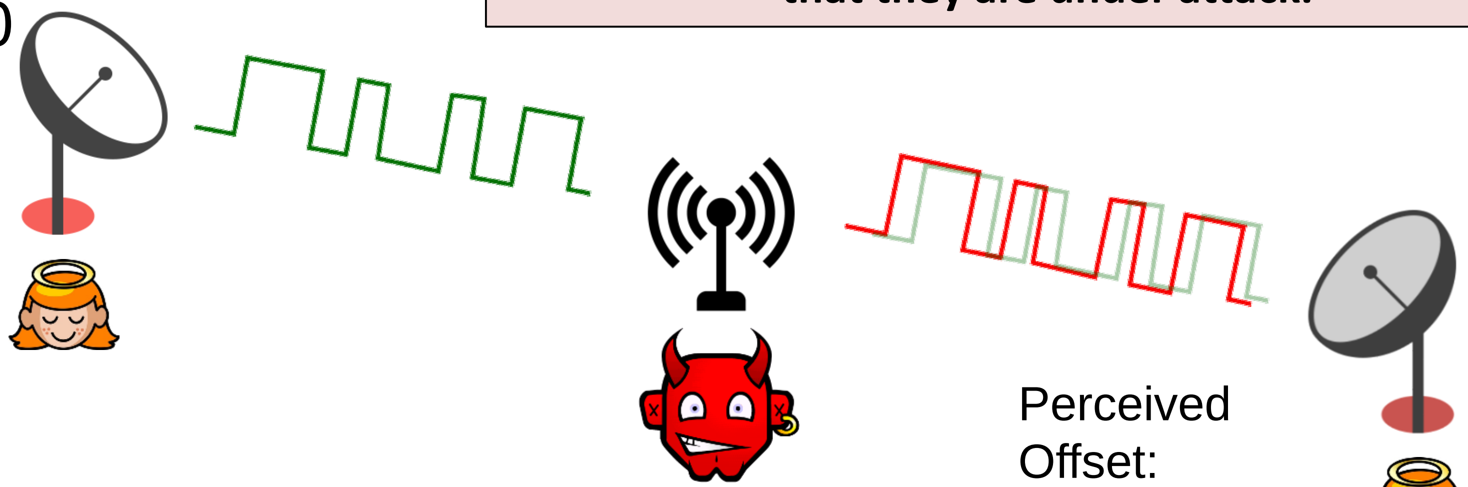
- Station B uses features to determine when Station A transmitted the waveform
- Station B takes the propagation delay into account

One-Way Time Distribution is Insecure 2

Protocol is considered compromised if the perceived offset is incorrect and the stations cannot figure out that they are under attack.

Station A

10:00



09:55

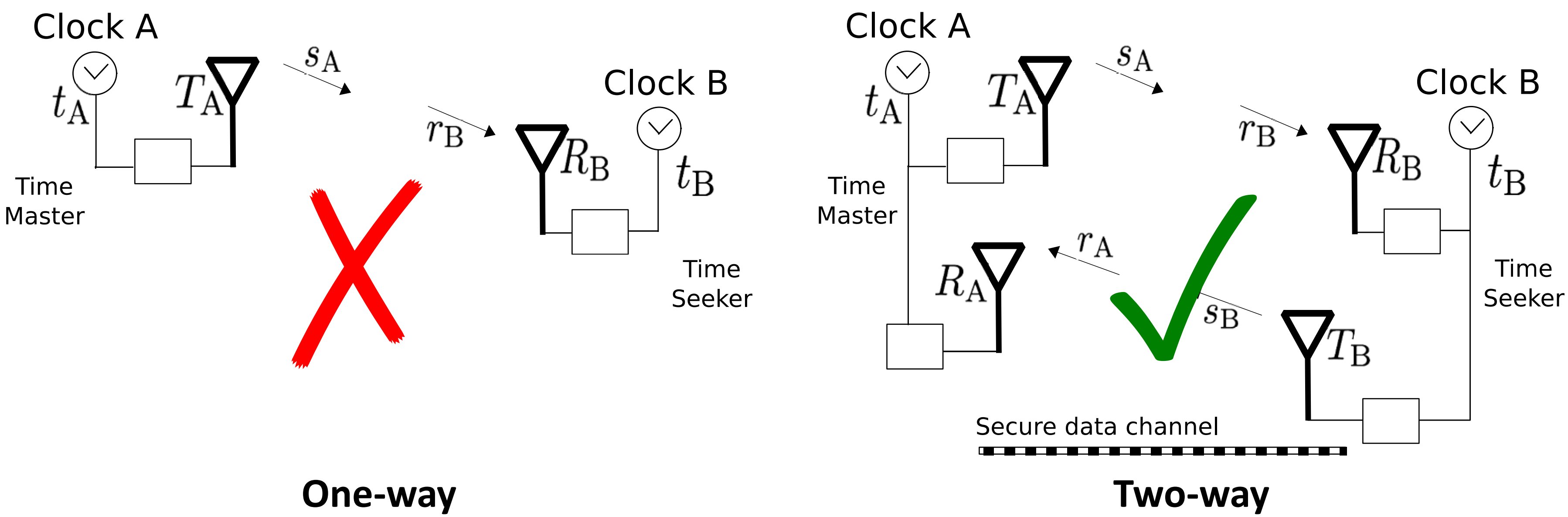
Perceived Offset: 00:04

Station B

- Station B uses features to determine when Station A transmitted the waveform
- Station B takes the propagation delay into account

Conditions for Secure Time Distribution

1. Propagation delay between A and B must be known
2. The path taken by the timing signal must be irreducible.
3. Both A and B must inject **unpredictability** into their transmitted signals.
4. Time delay between B receiving message and replying must be known.



L. Narula & T. Humphreys, DOI: 10.1109/PLANS.2016.7479783

The TASQC 2-Way Protocol

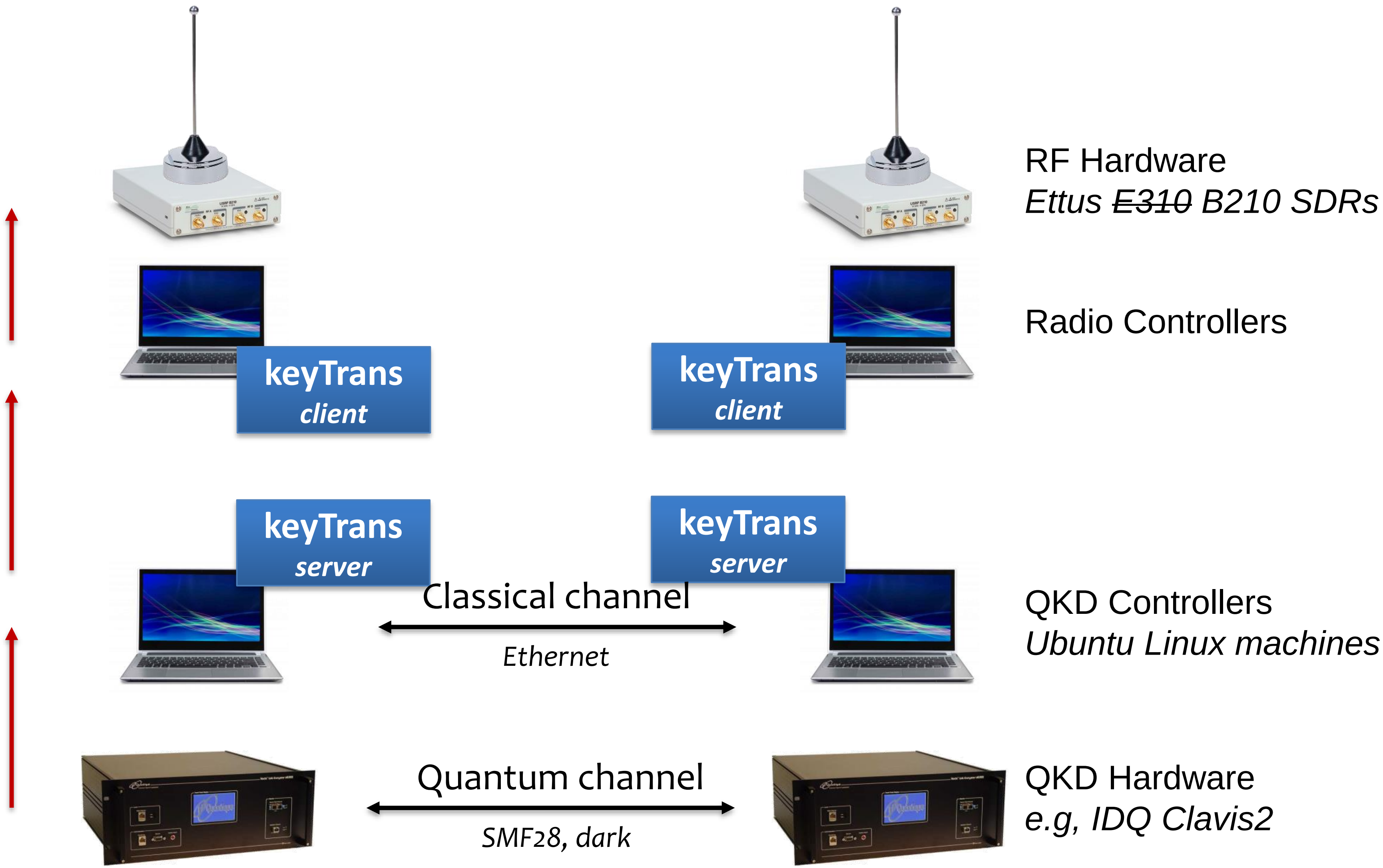
Protocol:

- Alice (master) encrypts and broadcasts time
- Bob (verifier) receives & verifies Alice, broadcasts key
- PMU (slave):
  - Encrypted time received at local clock t_1
  - Decryption key received at local clock t_2
  - Time message decryption, correction for TOF, local clock correction
  - PMU responds with quantum-seeded message
- Alice & Bob receive acknowledgement and confirm

Benefits:

- **Full 2-way secure time distribution**
- Utility / operator owns the system
- Flexibility in QKD flavor, RF bands

TASQC Implementation - TX



TASQC Implementation - RX

RF Hardware (RX1): Receives encrypted message from (A) – tags arrival time and stores. Receives key from (B) at Δt, decrypts message. **Transmits acknowledgement following successful time update**

Additional computation: Time stamp parsing and corrections, generation of IRIG-B signal, IEEE-1588?

Power systems application: PMUs