U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

# Timing Authentication Secured by Quantum Correlations (TASQC)

## Oak Ridge National Laboratory (ORNL)

**Phil Evans**

**Cybersecurity for Energy Delivery Systems Peer Review**

November 6-8, 2018

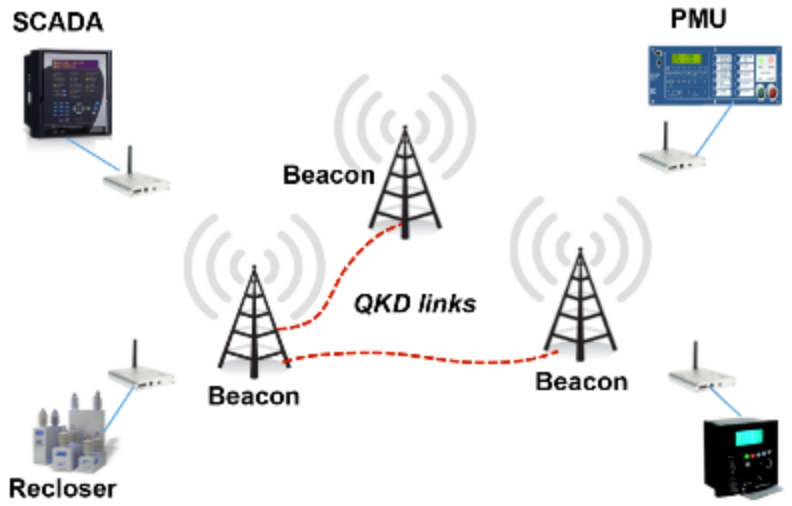
# Summary: TASQC

## Objective

- Provide an energy-centric secure timing distribution and message broadcast capability that complements, and could replace, GPS

## Schedule

- **Start**: January 2015
  **End:** September 2019
- IAB Formed: Q3 FY15
- Base system demo: Q4 FY15
- Message passing: Q1 FY16
- 2-way time transfer: Q2 FY16
- Demonstrations: ongoing
- **Capabilities realized**:
  Secure time distribution and synchronization for time-aware/sensitive grid networking and applications




| | |
|---|---|
| **Total Value of Award:** | **$ 2.998M** |
| **Funds Expended to Date:** | **% 99** |
| **Performer:** | **Oak Ridge National Laboratory** |
| **Partners:** | **Pacific Northwest National Laboratory**<br>**Sandia National Laboratories**<br>**University of Texas Austin**<br>**Qubitekk, Inc.**<br>**Electric Power Board (EPB)** |

# Advancing the State of the Art (SOA)

## There is no alternative source of secure time distribution for the grid

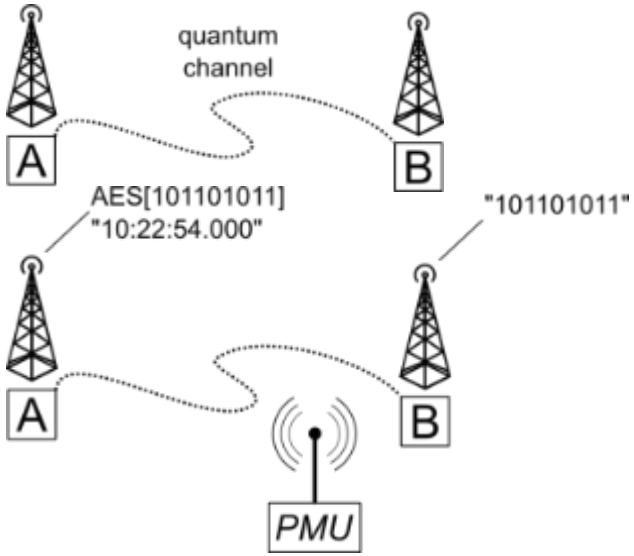
- GPS is widely used. **GPS is vulnerable to spoofing!**
- eLORAN can provide < 100 ns timing. Additional trials scheduled for 2019/2020

## 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 dark fiber optic and RF/wireless infrastructure
- **Benefits:**
  - Time signals are encrypted with quantum keys and one-time pad: **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:**
  - Meets 1μs timing requirement for PMUs – IEC C37.118-2005
  - Has IEEE-1588 and IRIG-B timing output for distribution to existing devices
- **Cybersecurity:**
  - Resilience against GPS interference and spoofing; satellite & space weather events

# Progress to Date

- 3Q FY15: Industry Advisory Board (IAB) Formation
- 4Q FY15: Base System
  - Task 1.8 (Milestone) Base Protocol Burn-in Testing @ ORNL ✓
  - Task 1.11 (Go/No Go) Prototype Testing @ PNNL ✓
- FY16: Protocol Demos & 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: IEEE-1588 & IRIG-B output
  - IAB recommendation
- 3Q FY17: Demo with Chip-scale QKD systems
  - Conducted on-site at SNL
- FY18: Preparations for final utility demonstrations

# Challenges to Success

## Mutual Understanding – Needs & Technologies

- Aligning needs and requirements
- Multi-faceted team with broad knowledge base
- Outreach, webinars, meetings

## Absolute trust in GPS

- “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
- Partnerships with utilities with owned spectrum

# Collaboration/Technology Transfer

- 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
- Plans to gain industry acceptance:
  - Utility-hosted field tests and demonstrations
  - Adopting current standards
  - Enabling technology for other grid applications