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

A Scalable Quantum Cryptography Network for Protected Automation Communications

Qubitekk, Inc.

Dr. Duncan Earl

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: A Scalable Quantum Cryptography Network for Protected Automation Communications

Objective

- The electrical grid needs a long-term authentication/encryption solution with minimal impact on grid operations. Quantum Key Distribution (QKD) can deliver these benefits but performance and cost-effectiveness have yet to be quantified. Toward that goal, we will demonstrate and monitor a cost-effective QKD solution for securing substation communications.

QKD Transceiver modified for use with/as ORNL AQCESS node.

Schedule

- Duration: Oct. 2016 to Sept. 2019
- QKD components designed (met Sept. 2017)
- Prototypes fabricated (met Sept. 2018)
- Technology deployed and characterized (To be completed in 2019)
- Demonstration in 2019 will deliver performance data on QKD components and will provide utilities with a reference implementation for using QKD for long-term substation security.

Total Value of Award:	**$4,602,487**
Funds Expended to Date:	**64.5%**
Performer:	**Qubitekk, Inc.**
Partners:	**Oak Ridge National Lab.** **Electric Power Board** **Schweitzer Engineering Labs**

Advancing the State of the Art (SOA)

- **First large-scale deployment of QKD for securing the electrical grid.**
- We are deploying a QKD network that not only improves security by using entangled photon QKD but also incorporates cost-saving client nodes (called AQCESS nodes)
- Final solution has the potential to deliver long-term, cost effective, secure grid communications.
- Utilities will benefit and adopt this solution because it provides cyber security without introducing operational complexity
- Grid cybersecurity will improve because system provides uncrackable, self-managing cryptographic keys with channel tamper detection.

QKD benefits to utility networks.

Challenges to Success

Challenge 1: Source Development

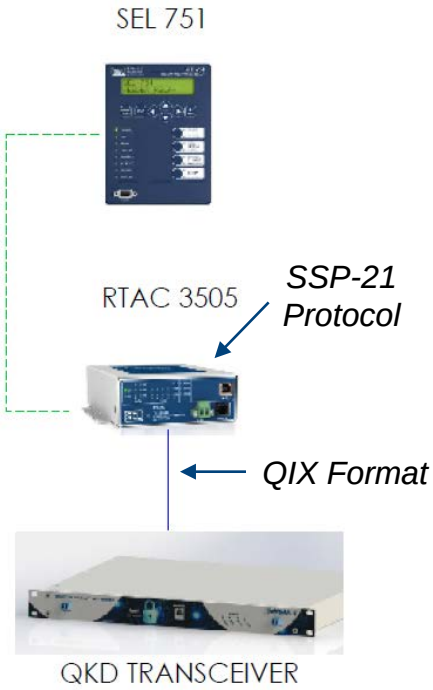
- Compact, stable entangled photon sources are required for this project. Shrinking designs that previously existed on a laboratory bench is a challenge that has been addressed by model-driven designs and prototypes that leverage a common integrated opto-thermal-electrical housing for sources based on bulk-crystal SPDC.

Challenge 2: Third-Party Integration

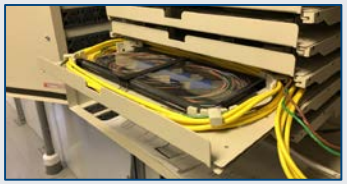
- QKD solutions provide uncrackable keys to clients. However, these keys are only useful if the client has a method for receiving and using the keys. We have worked with 3rd party vendors to incorporate the SSP-21 open-source protocol developed by and for utility ICS networks that is compatible with QKD keys.

Challenge 3: Fiber Loss Management

- Optical losses associated with wavelength division mutliplexers and Lithium Niobate phase modulators limit the total number of AQCESS nodes on a network. This drives the cost-effectiveness of the final solution. To mitigate, decreasing the optical losses on the quantum channel (which cannot be amplified), at the expense of higher losses on the classical channel (which can be amplified), is being pursued



Major Project Accomplishments (to date)

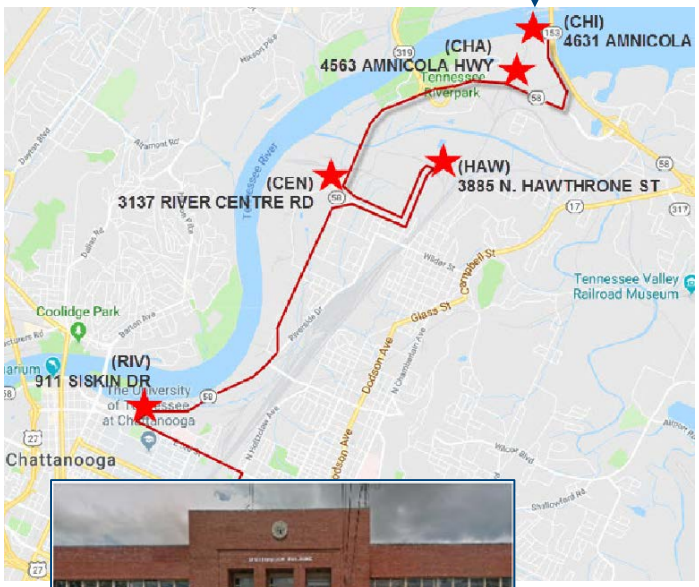
Accomplishment	Completed	Image
Development of PCB-mounted quantum sources and detectors	✓	
Finalized modified QKD transceivers and AQCESS node designs	✓	
Integration of SSP-21 protocol into SEL RTAC 3505	✓	
Identification, measurement, and leasing of fiber channels at EPB utility for QKD testbed	✓	
Development of field test plan to validate performance and benefits	✓	

Next Steps in 2019

Deployment of QKD Network at EPB

- Six QKD devices creating secure network between:
  - Five operational substations
  - One Control Center
- Over 20km of optical fiber
- QKD system will secure communications between:
  - Six SEL RTAC 3505 communication devices monitoring five SEL 751 protection relay controllers.
- All equipment to be monitored remotely
- Will include a remotely controlled eavesdropping device (to test security)
- Equipment deployment to begin in January 2019
- Performance testing though Sept. 2019

Substation

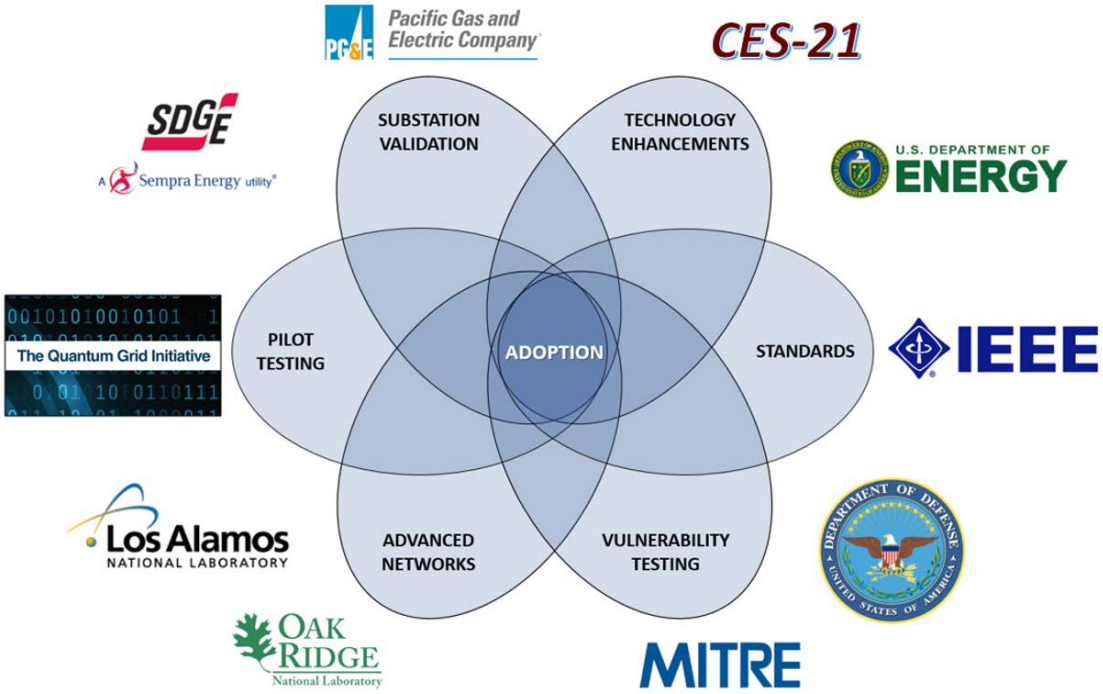


Control Center

Collaboration/Technology Transfer

Technology transfer to end users

- This project involves end users (utilities - EPB), equipment providers to the end users (automation component vendors - SEL), and quantum equipment providers (Qubitekk).
- The demonstration at EPB will serve as a “reference implementation” for other utilities interested in a quantum solution
- Industry adoption is a process involving several partners



More Details on Technology

Quantum Key Distribution (QKD)

QKD systems use quantum physics to generate truly random keys that cannot be cracked by any computer and provide instantaneous detection of eavesdropping. QKD transceivers are secure, but expensive.

AQCESS Nodes

New technology developed by Oak Ridge National Laboratory with the potential to reduce the number of QKD transceivers required on a multi-client quantum network. Could result in significant cost savings if security and performance of device can be successfully demonstrated.

QKD Transceivers & AQCESS Nodes

INTEGRATION

USB Serial output can be used by 3rd party devices that implement SSP-21 protocol

PCB MOUNTED QUANTUM COMPONENTS

QKD and AQCESS Node devices use entangled photon sources, single photon counting detectors, and Lithium Niobate polarization modulators.

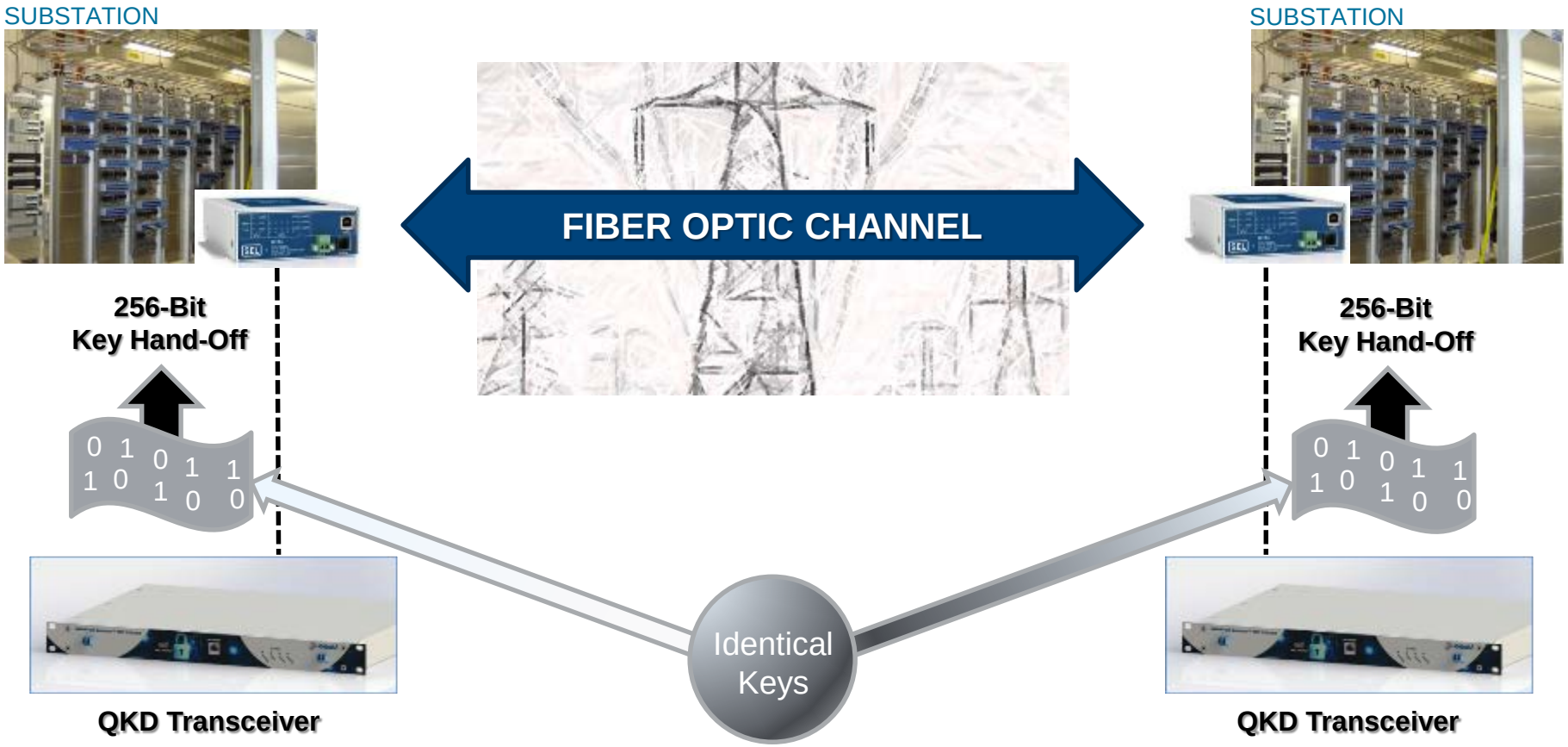
FIBER CONNECTED

Telecom optical fiber used to connect two or more QKD transceivers

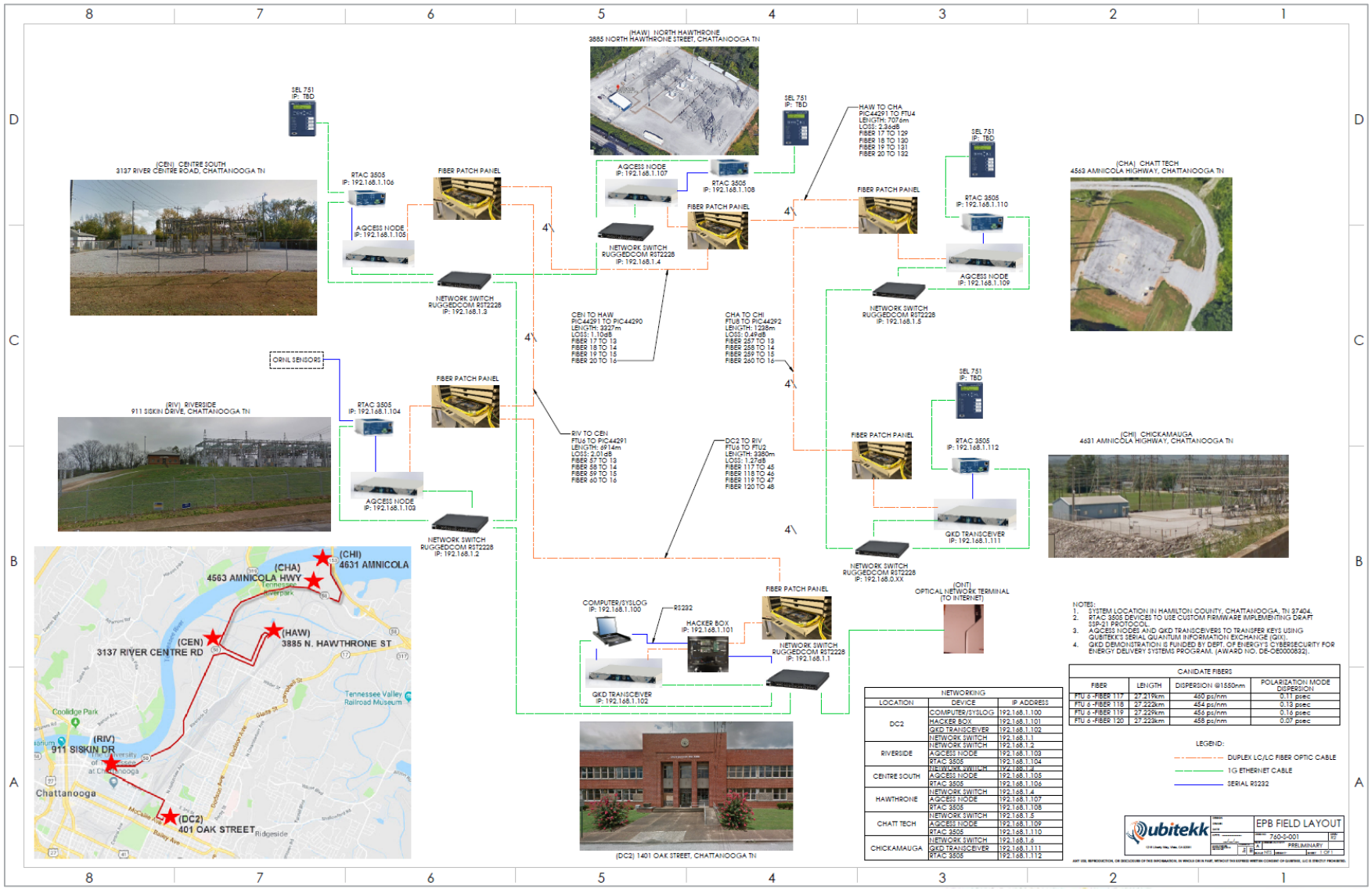
NETWORK CONTROL

Syslog events provide diagnostic and alarm information to SPLUNK and other network management tools

Key Handoff in QKD/AQCESS Network

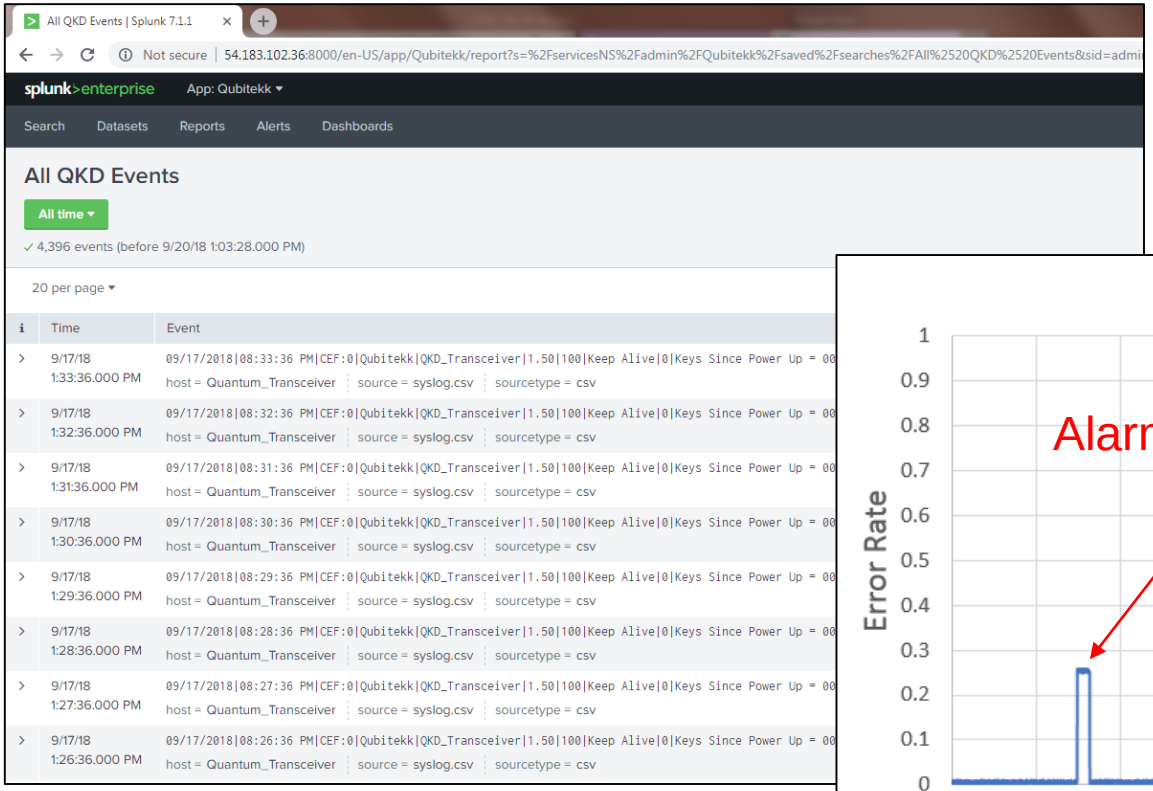


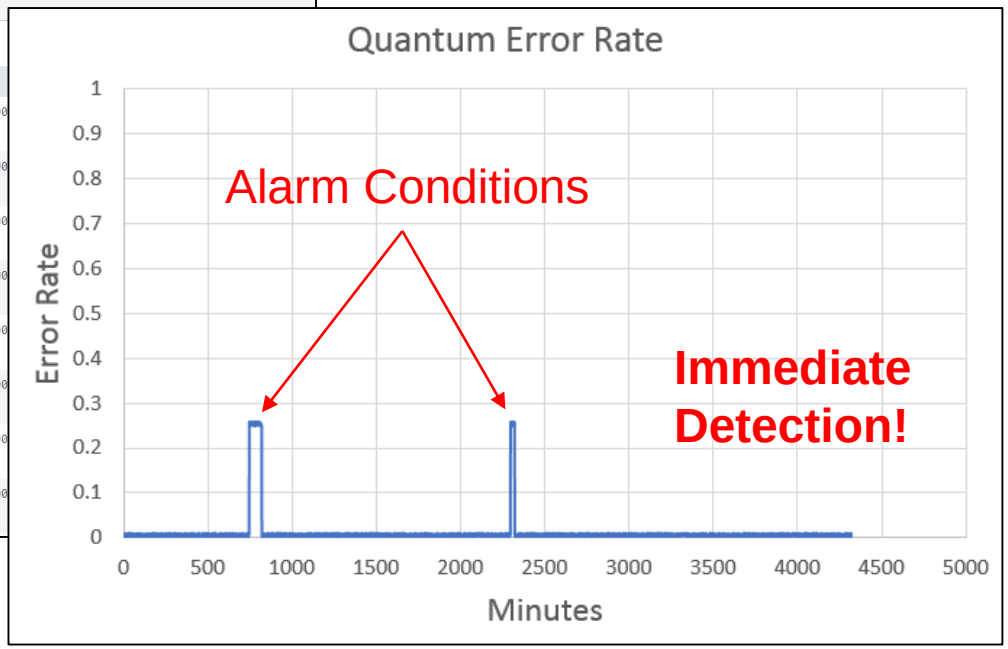
EPB QKD Field Test Network Architecture



Remote Monitoring and Integration with Utility Tools

SPLUNK Report





SPLUNK Dashboards and App coming in the future.

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

For More Information, Contact:

Dr. Duncan Earl

Qubitekk, Inc.

E-mail: dearl@qubitekk.com

Cell: 865-599-5233