


Trusted Relay Node Networking



*Extending
quantum
communications
over long
distances using
trusted relay
nodes*

Existing quantum data transmissions between secure links are limited in range to about 100 miles. This project demonstrates that a succession of these links, joined by relay nodes located in physically secured locations, can overcome this distance limitation. Nationwide deployment of quantum technologies requires interoperable systems from multiple vendors. An operator must be able to plug-and-play a quantum device without regard for the underlying physics or placing a burden on operators to reconcile disparate technologies. This effort develops and demonstrates a three-node network, extending quantum communications by building and deploying trusted relay nodes. The project addresses two existing impediments to widespread implementation of quantum communications technology: limitations on the maximum link range and non-interoperable implementations. By developing and implementing a systems-level approach to interoperable trusted relay nodes, this project brings the security assurances of quantum communication systems to long-haul distances.

KEY TAKEAWAYS

- Secures supervisory control and data acquisition and industrial control system networking over long distances
 - Develops and demonstrates a three-node network extending quantum communications by building and deploying trusted relay nodes
- 

OUTCOME

While an all-quantum end-to-end network may one day be possible using quantum relays, these devices have not been demonstrated even in a laboratory setting and are decades away from being deployable at scale. This project researches, designs, and implements a secure relay node that allows for unattended, reliable, and secure operations without the need for supervision of the relay device outside of the laboratory to increase the distance over what a single system can achieve.

PARTICIPANTS

ROLE



Design, develop, and deploy interoperable quantum communication systems with low facility support requirements, suitable for use in electric power substations.



Field demonstration partner; participates in joint demonstrations of quantum communication systems in order to show seamless interoperability of heterogeneous systems.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Raymond Newell
Principal Investigator
Los Alamos National Laboratory
505-695-4370
raymond@lanl.gov

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: October 2017 – February 2020

Total Award Value: \$400,000
DOE Share: \$400,000
Cost Share: \$0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: <https://www.energy.gov/ceser>

Date Written: June 2021