Quantum-based Secure Communications for Remote Operations

NEUP Project 21-24354

2023 ARSS Fall Program Review

Stylianos Chatzidakis

Assistant Professor

School of Nuclear Engineering

Purdue University

October 2023

West Lafayette, IN

Team Info

- **Purdue**
  - Stylianos Chatzidakis (Assistant Professor and Associate Reactor Director, SRO)
  - True Miller (Reactor supervisor, SRO)
  - Brian Jowers (Electronics/I&C reactor staff, RO)
  - V. Theos, Z. Dahm, K. Vasili, K. Gkouliaras, W. Richards, R. Ughade (Grad students)

- **Collaborators**
  - Robert Ammon (Curtiss-Wright)
  - Phil Evans (ORNL)
  - Terry Cronin (Toshiba)

- **TPOC:** Katya Le Blanc (INL) and Ben Cipiti (Sandia)

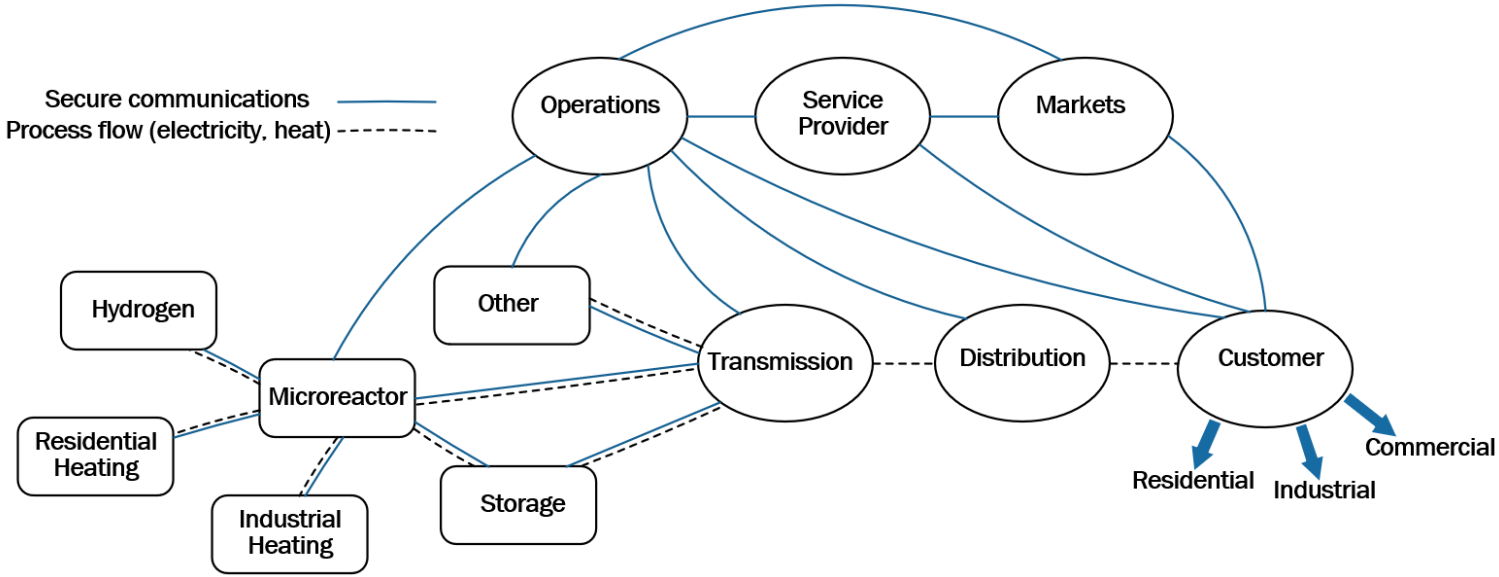
PURDUE UNIVERSITY

OAK RIDGE National Laboratory

CURTISS-WRIGHT

TOSHIBA

New technologies…new challenges



New reactor concepts => Significantly different requirements than existing fuel cycle facilities

Digitalization => New architectures and new vulnerabilities

New technologies => Quantum computing Adversaries now have access to new tools with unprecedent capabilities

What about Cybersecurity?

1st Cyber Age

2nd Cyber Age

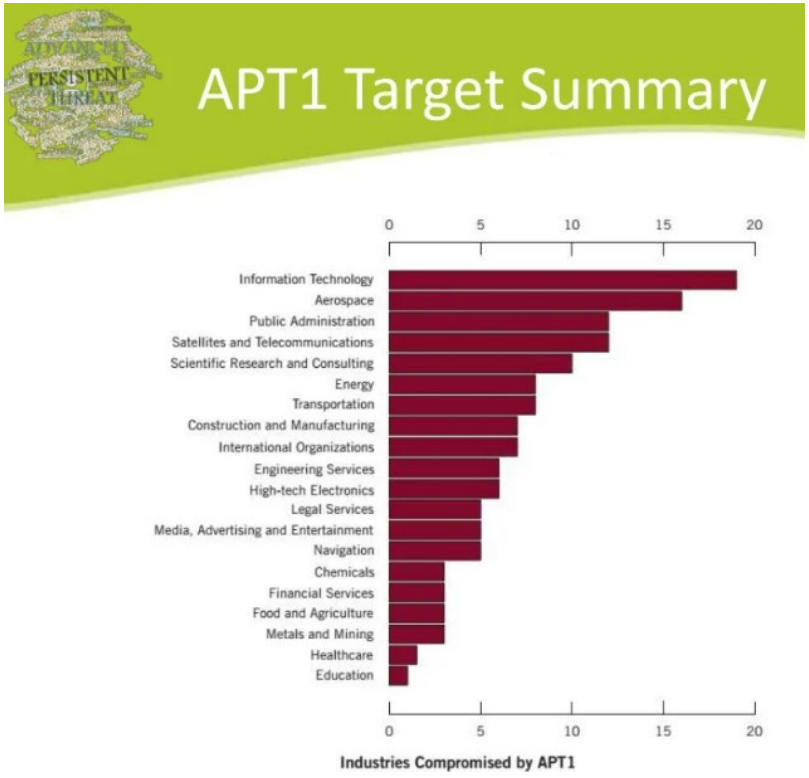
3rd Cyber Age

"I don't care what you do, just keep the plant running!"

- CEO of a large chemical processing plant on security

4th Cyber Age

Energy sector high on target list



NEWS ANALYSIS

Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.

NEWS

Oak Ridge National Lab shuts down Internet, email after cyberattack

DOE laboratory says it was victim of an Advanced Persistent Threat designed to steal

DIVE BRIEF

FBI: US energy sector faces 'reconnaissance, scanning' by Russian hackers; 5 companies targeted

Published March 23, 2022

MIT Technology Review

Featured Topics Newsletters Events Podcasts SIGN IN SUBSCRIBE

COMPUTING

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

PURDUE UNIVERSITY | School of Nuclear Engineering

RADIATION IMAGING AND NUCLEAR SENSING LABORATORY

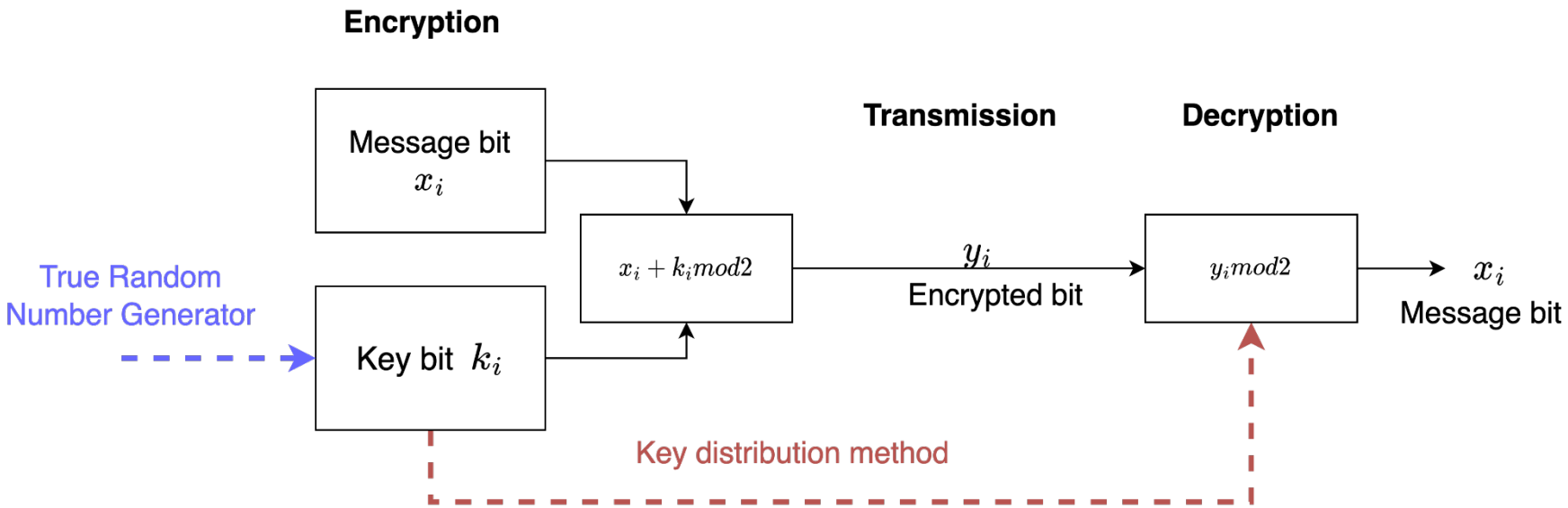
Goals & Objectives

Goal: Experimentally and numerically investigate quantum-based secure communications and demonstrate under prototypic conditions in PUR-1.

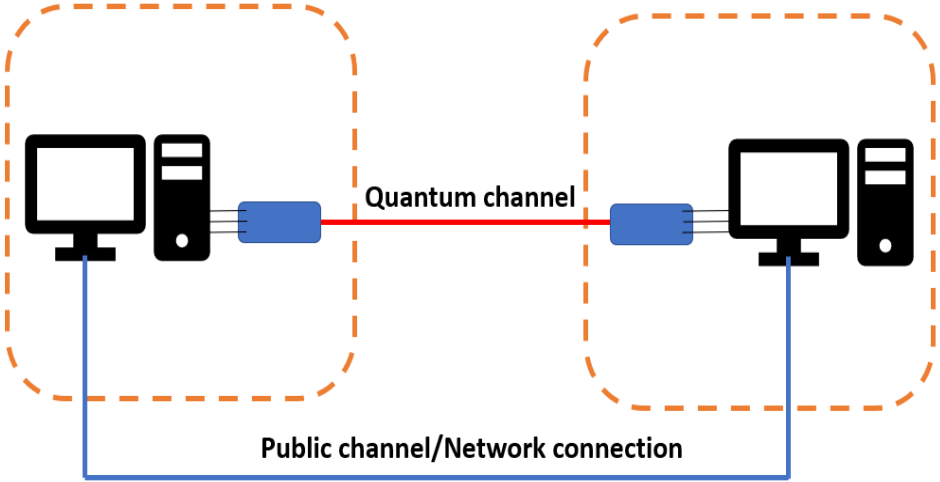
Objectives:

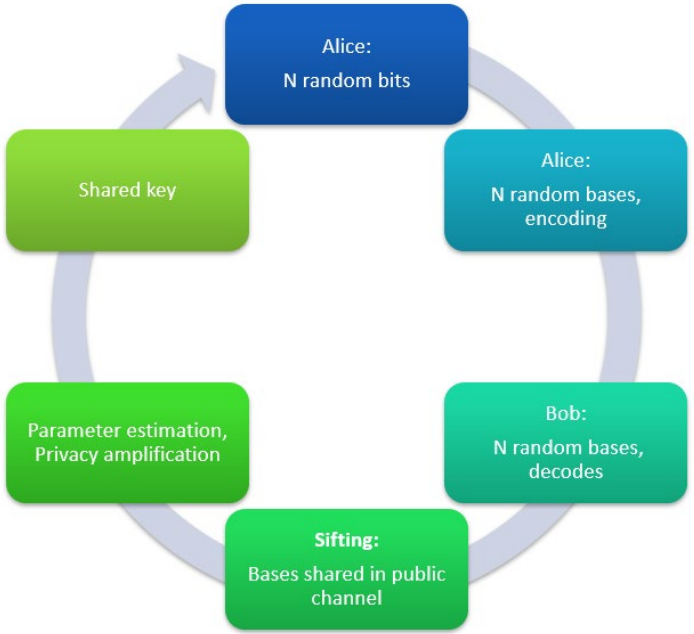
1. Develop a robust quantum communication modeling and simulation framework to support the analysis of QKD systems
2. Develop a cyber physical testbed with remote monitoring and communications in PUR-1
3. Perform testing with prototypic QKD equipment and evaluate performance with and without cyber events

One Time Pad Scheme Guarantees Confidentiality

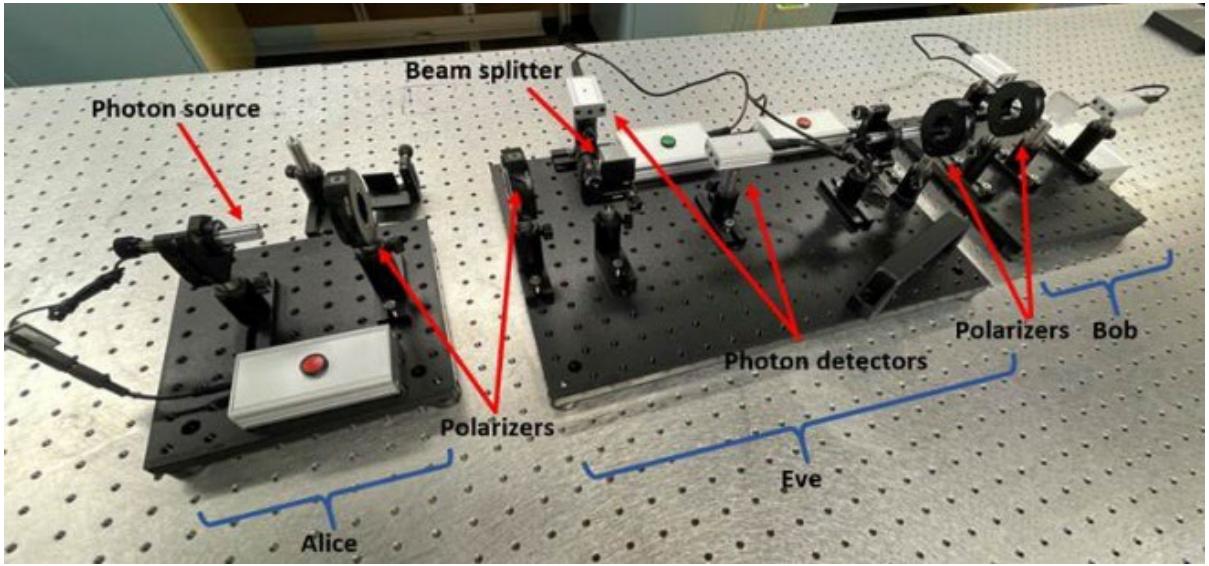


Quantum Key Distribution Provides Detection of Adversary





How it works



Send photons → Measure QBER → Higher QBER → Lower Security

$$SKR = \frac{final\ secret\ key\ length}{sifted\ key\ length}$$

$$QBER = q_e(1 - q_{ch}) + (1 - q_e)q_{ch} = \frac{\varepsilon}{4} + \frac{2q}{3}(2 - \varepsilon)$$

Our work so far…

Development of NuQKD a novel simulation tool for engineering applications.

Formulation of a nuclear reactor communications reference scenario

Analysis of reactor signals and required bandwidth

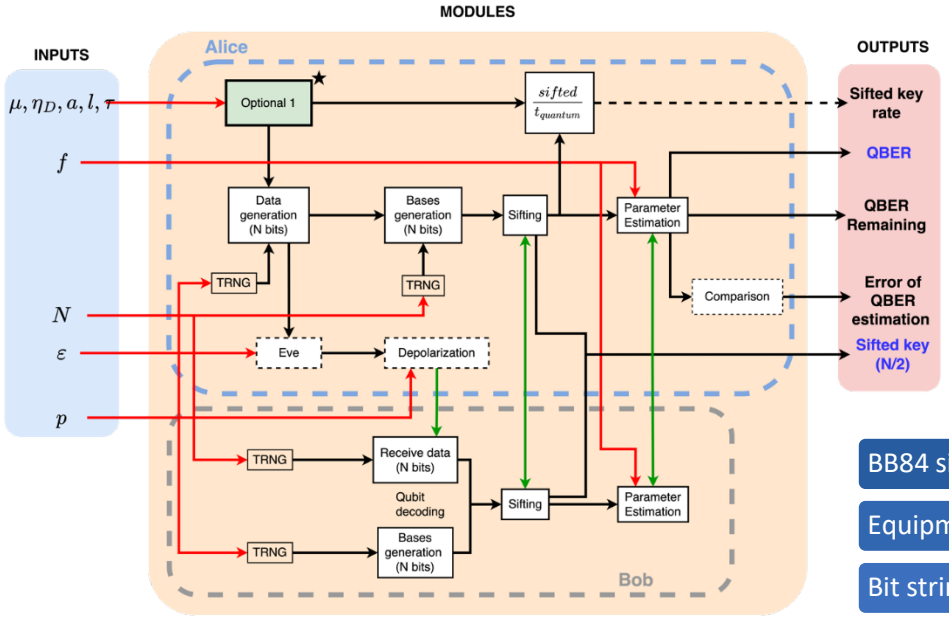
Modelling of channel imperfections and attacker scenarios

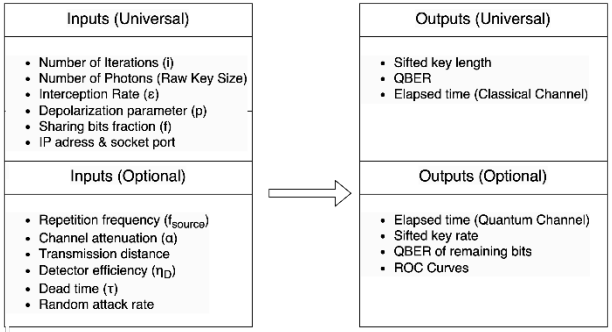
Evaluation of QKD performance for nuclear reactor communications

PURDUE UNIVERSITY

RADIATION IMAGING AND NUCLEAR SENSING LABORATORY

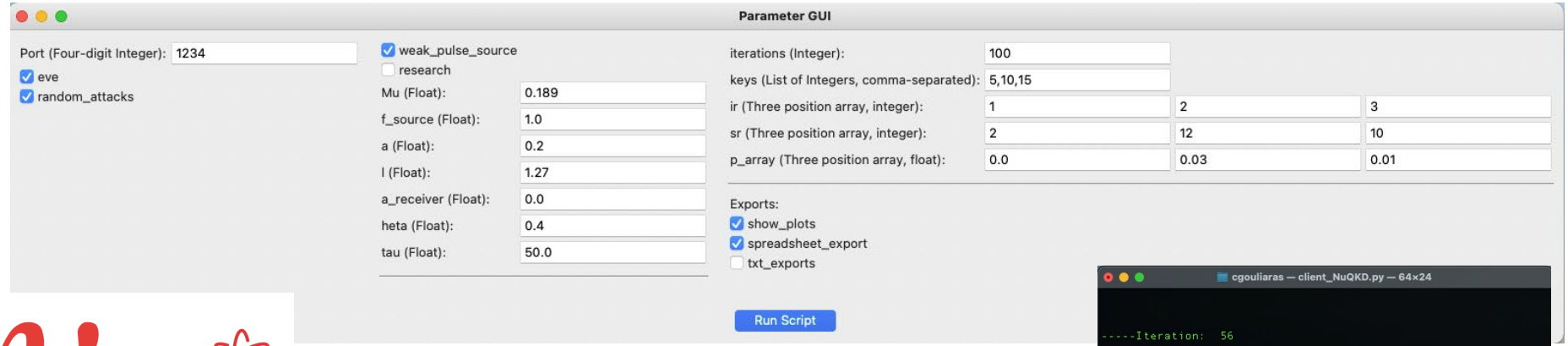
NuQKD simulation algorithm

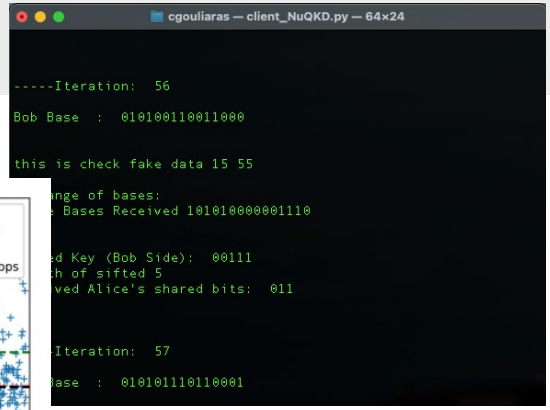


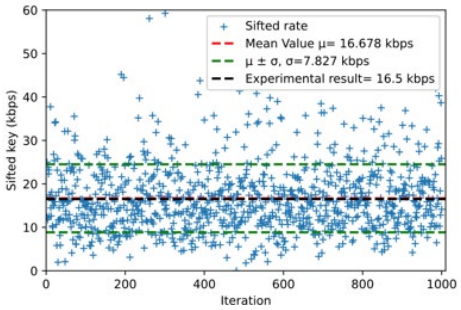


- BB84 simulation (optical fiber and free space)
- Equipment imperfections (source, channel, detector)
- Bit strings from True Random Number Generator (TRNG)
- Two-terminal /Single terminal execution
- Modular design approach
- Advanced customization of multiple input parameters
- Evaluation and export of various performance metrics

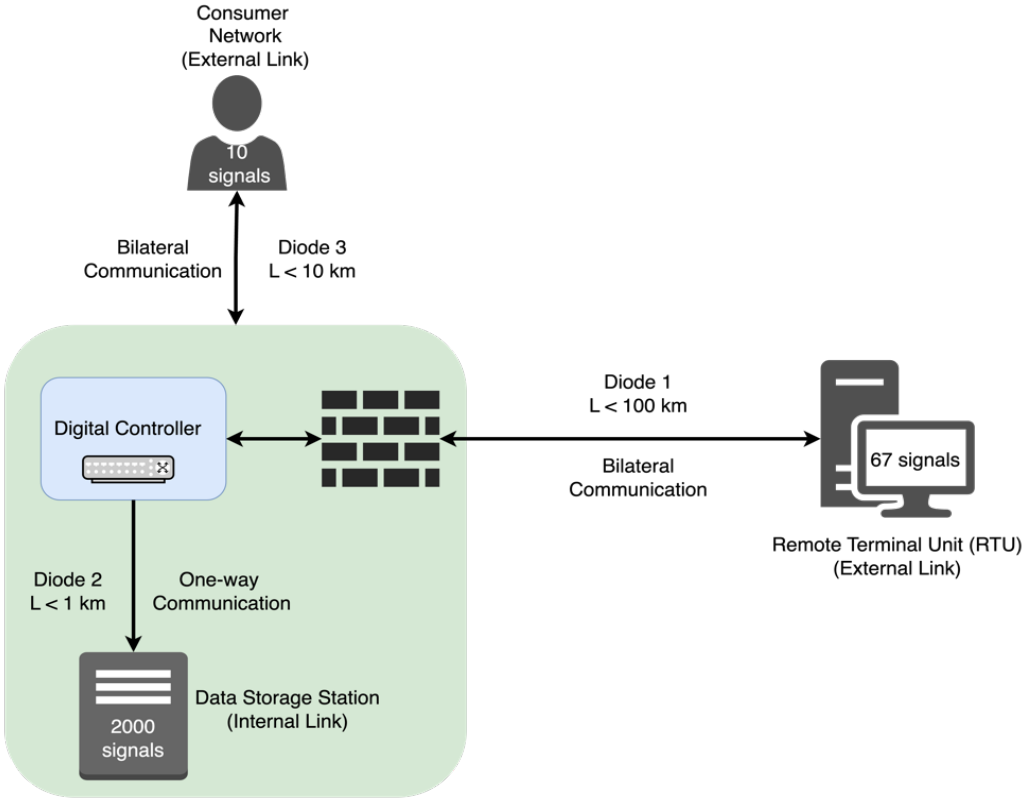
NuQKD is now benchmarked and fully operational







Reactor reference scenario



1. Reactor to Remote Workstation (RTU)

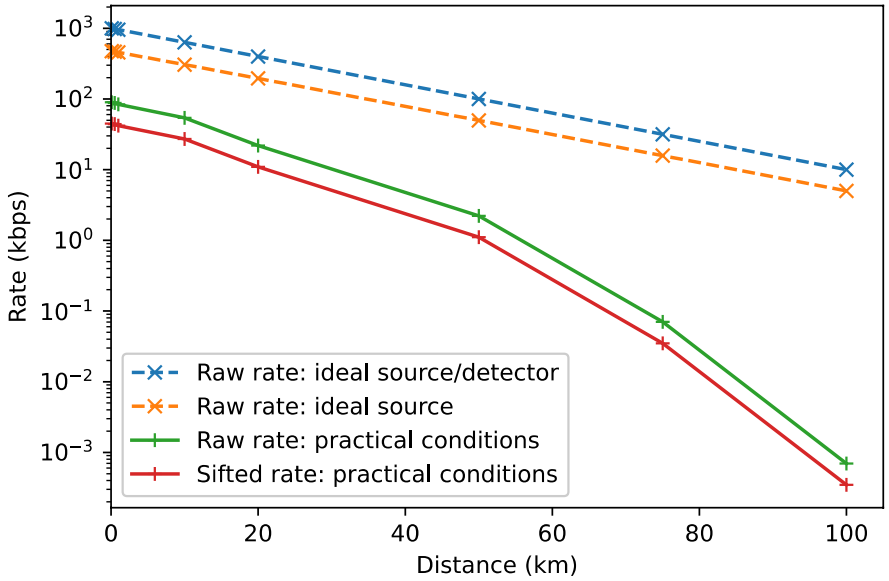
2. Reactor to Data Storage Station

3. Reactor to Energy Grid / Consumer Network

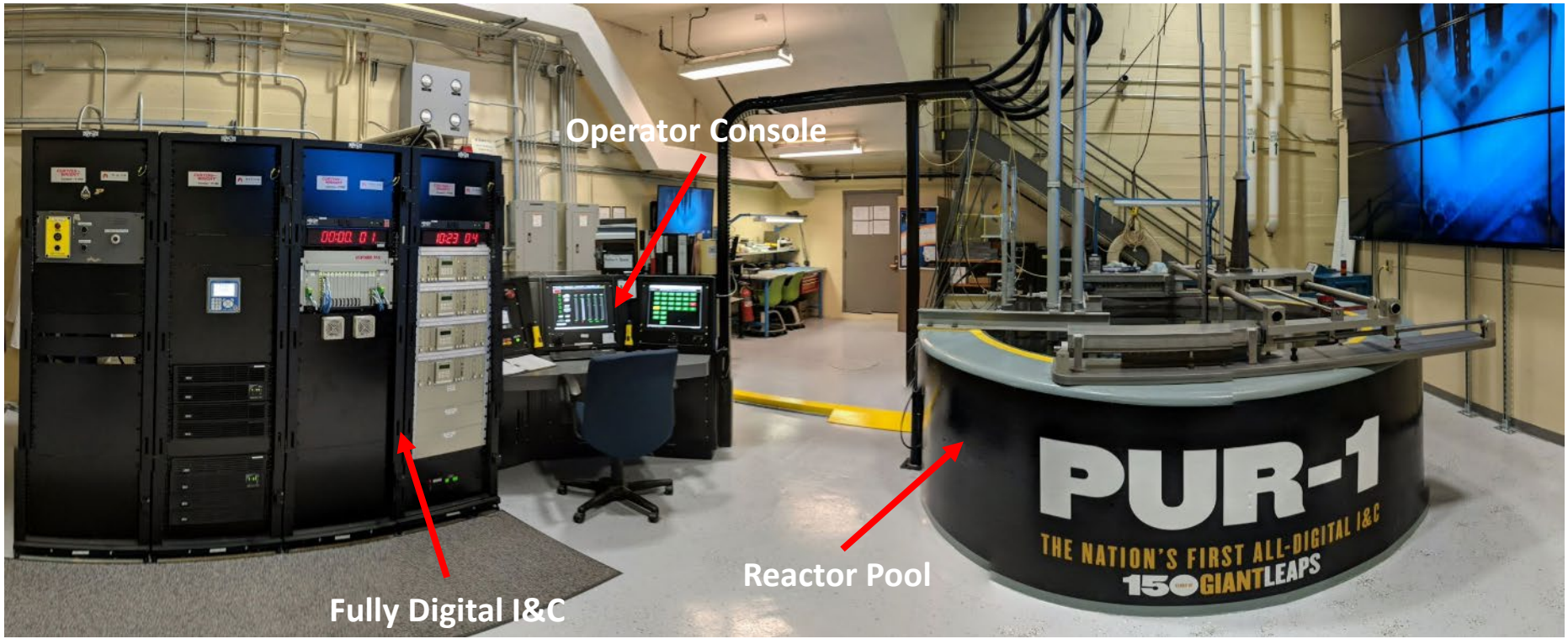
Reactor data & Bandwidth

- PUR-1 data used as case study
- 67 core signals
  - 1 Hz sampling
  - 6-digit accuracy
- Min and max values recorded:
  - Over 24 hours of operation
  - Including transients and outliers

533 bps required to transmit all 67 signals



Introducing PUR-1

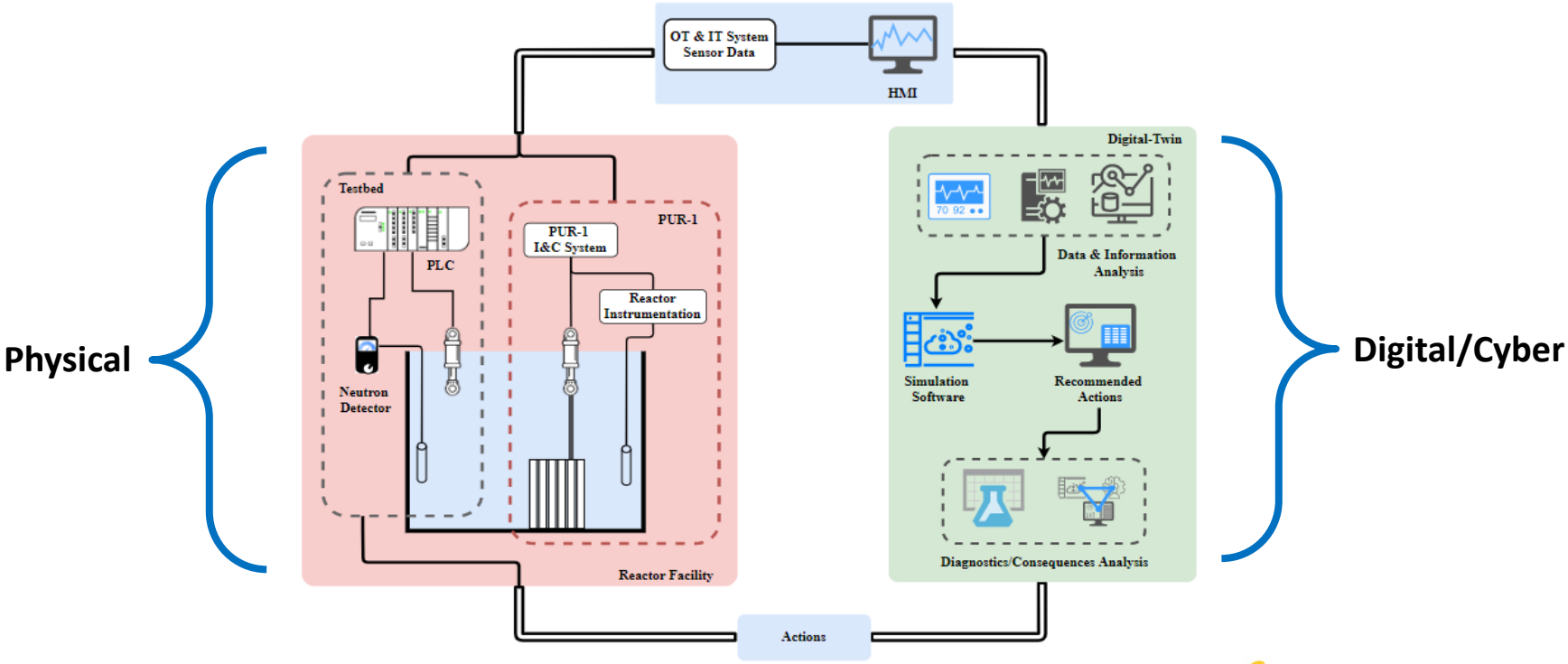


Before and after…

1960 - 2017

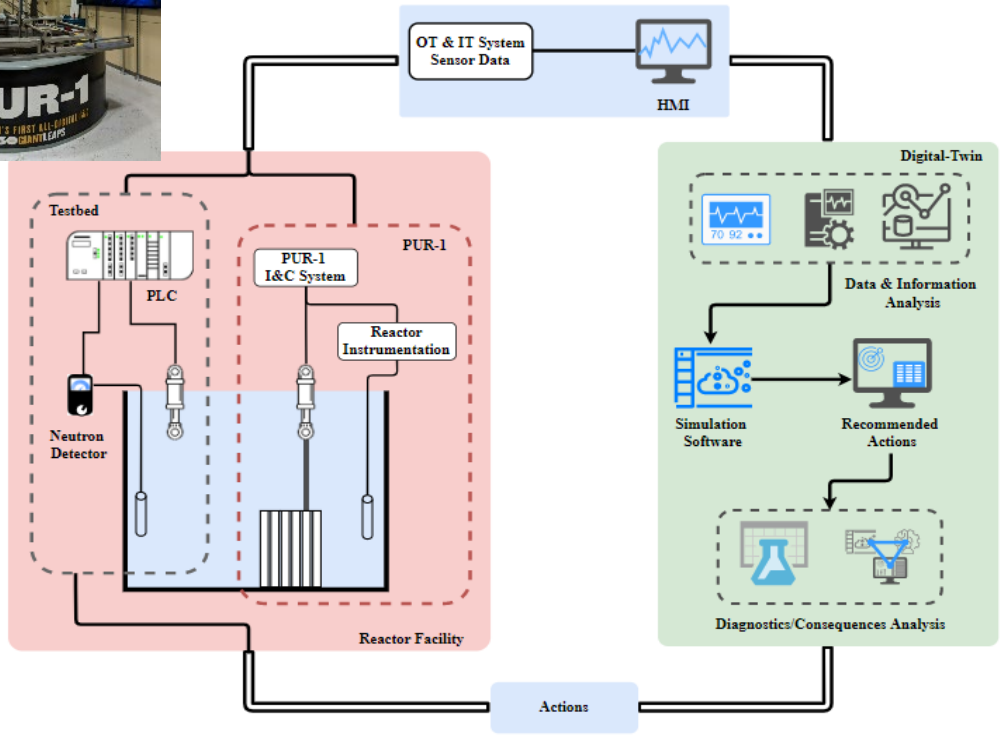
2019 - present

Towards a Real-Time Cyber-Physical Digital Twin



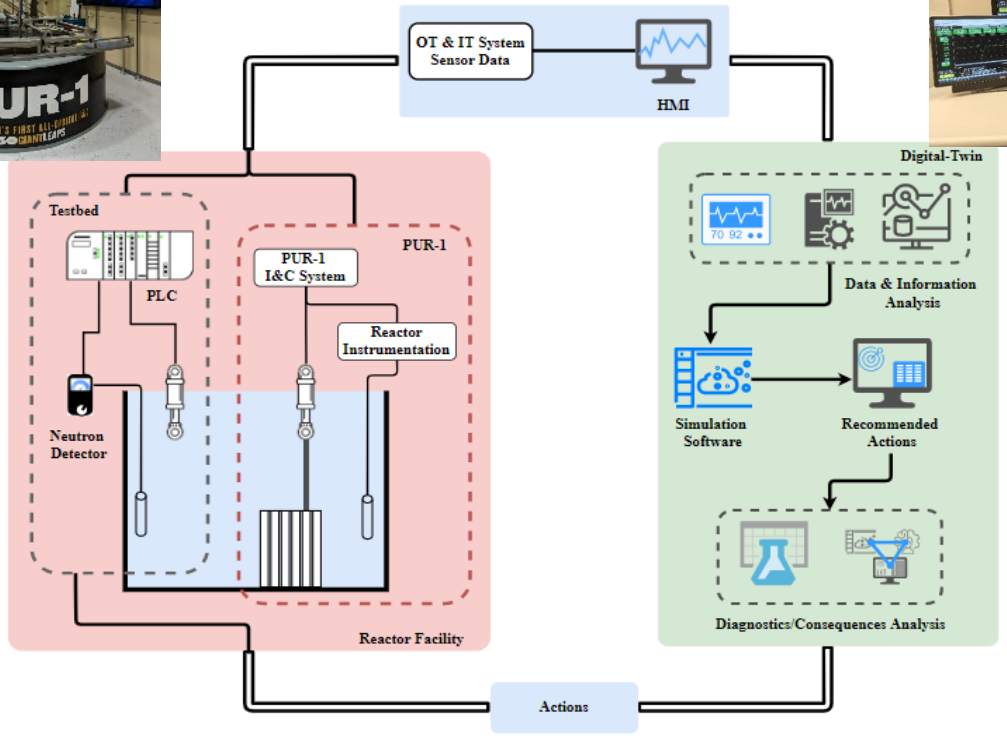
Towards a Real-Time Cyber-Physical Digital Twin

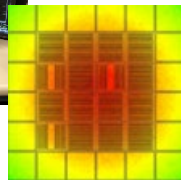
PUR-1



Towards a Real-Time Cyber-Physical Digital Twin

PUR-1

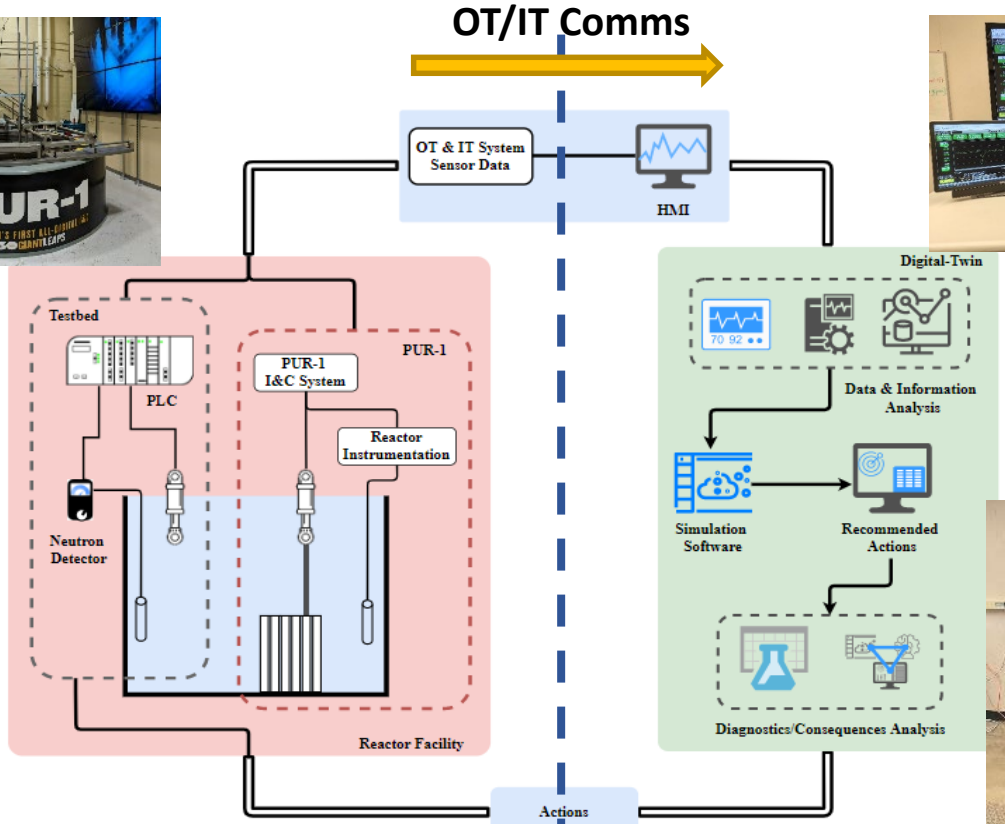




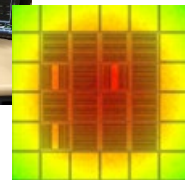
RMSS

Towards a Real-Time Cyber-Physical Digital Twin

PUR-1



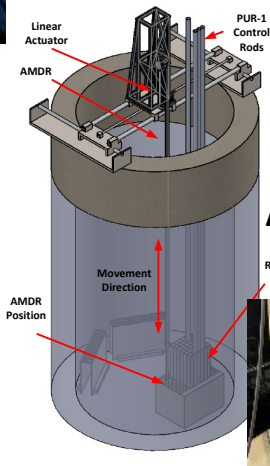
RMSS



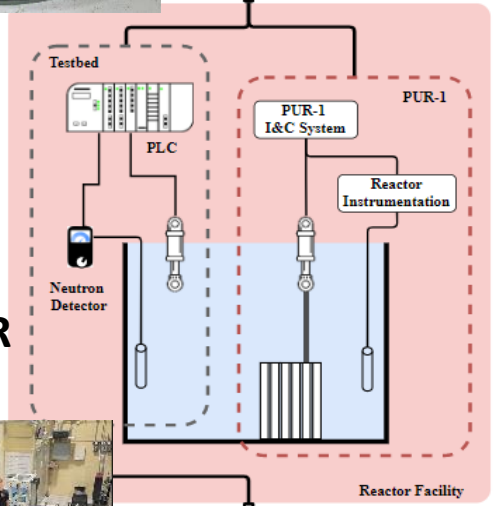
Control rack

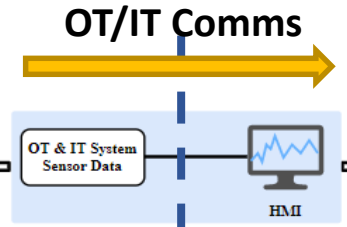
Towards a Real-Time Cyber-Physical Digital Twin

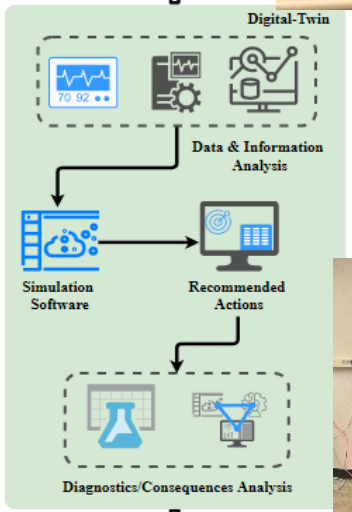
PUR-1



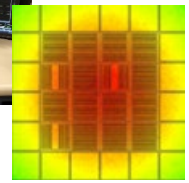
AMDR



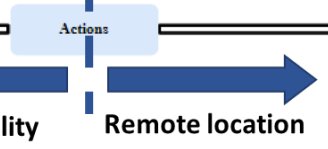




RMSS

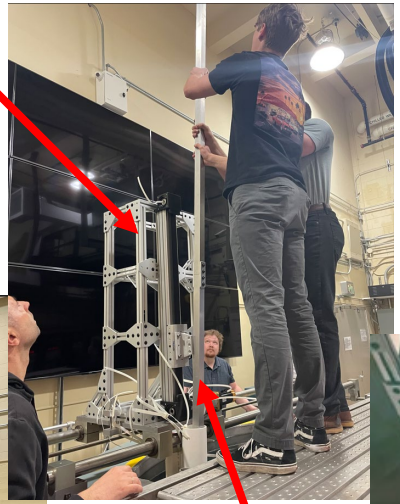


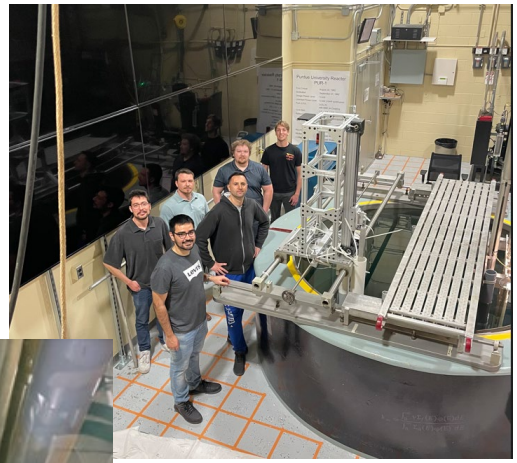
Control rack



Installing and Testing AMDR

Actuator

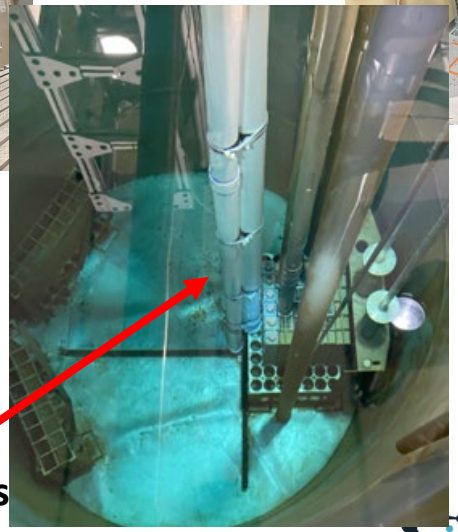




Completed
May 2023

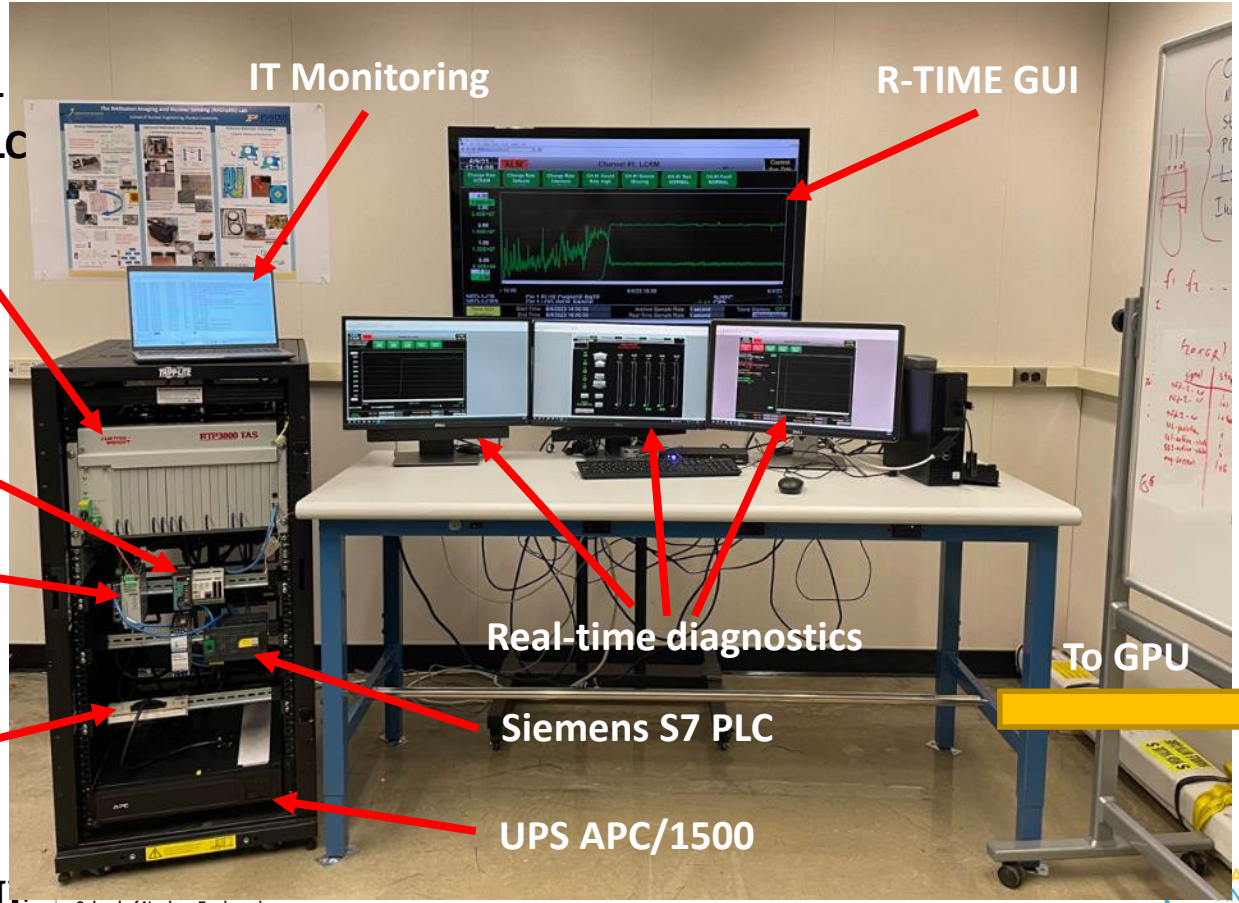
Support
structure

AMDR

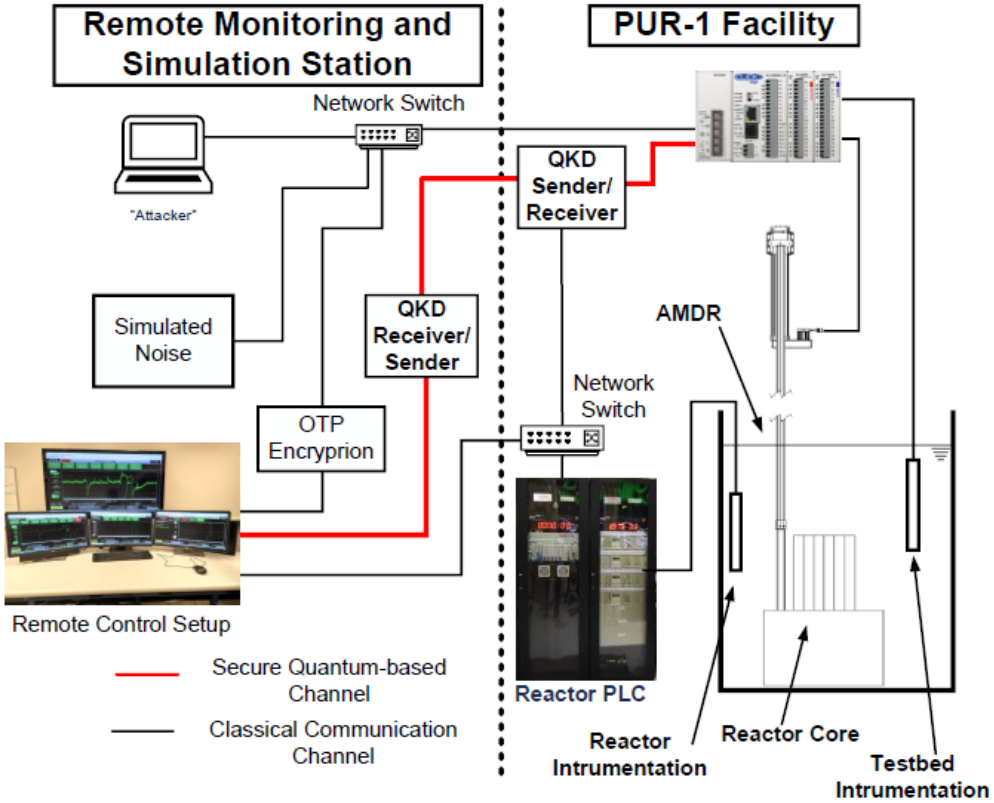


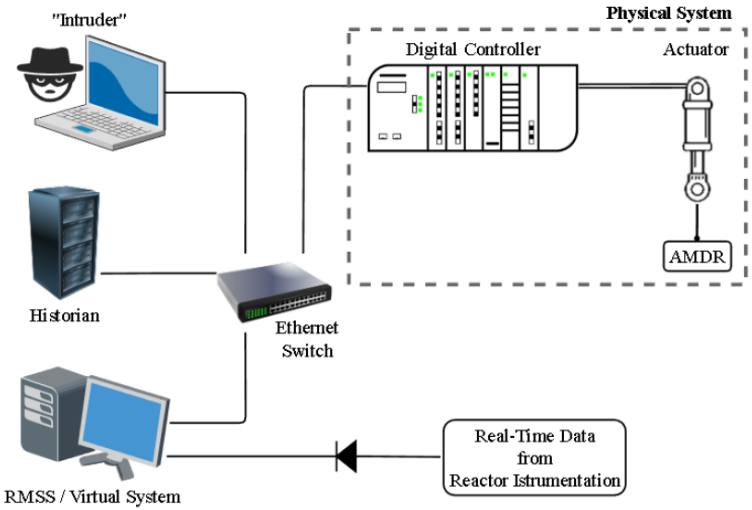
Guide tubes

Digital/Cyber Remote Station



Remote Monitoring System Operational





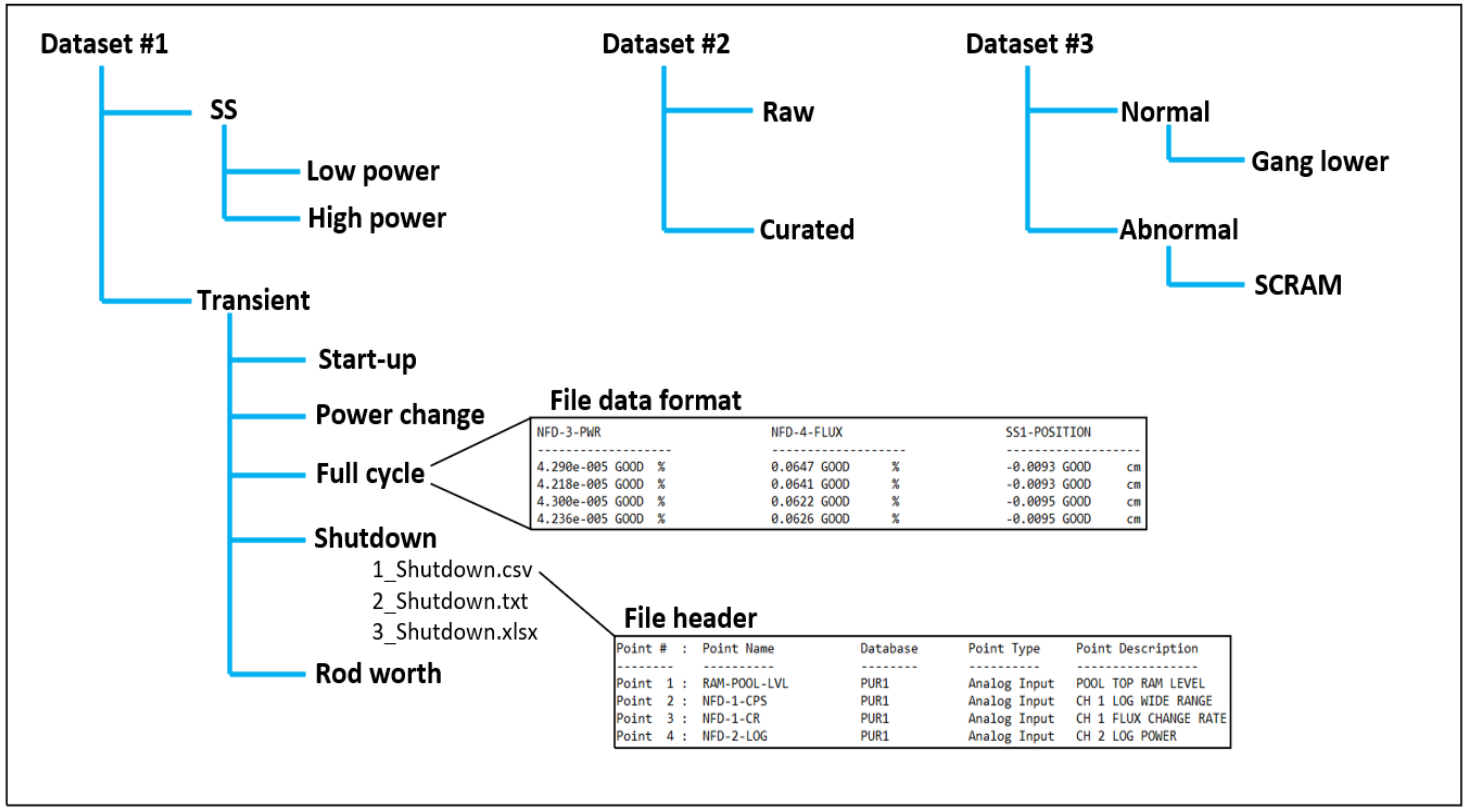
Instrumentation & Control

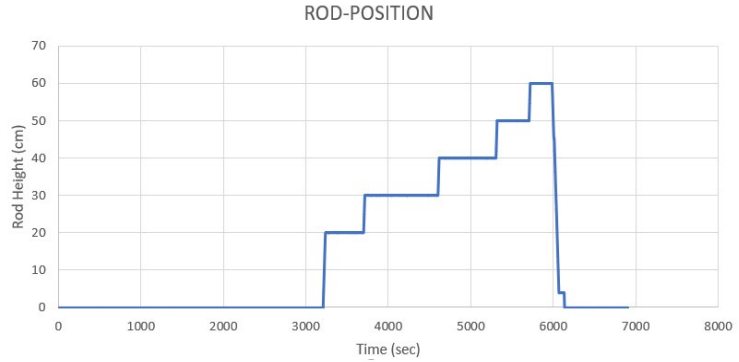
- **Instrumentation**
  - 4 neutron detectors (FC, UIC, CIC) => cps, % power, change rate
  - 3 radiation area monitors (mR/hr)
  - 1 air monitor (Ci/m3)
  - Water chemistry (oC, µS/cm), confinement pressure (kPa)
- **Control**
  - RTP 3000, Ethernet-TCP/IP communications
  - R-Time (sampling rate up to 1 kHz)
- **Archived data (process, network, and host)**
  - All instruments, operator actions, alarms, shim and reg rod positions, source position, HVAC, magnet, pump current/voltage, etc.
  - PLC, UPS (battery status, freq, V, A), and system diagnostics
  - Network traffic (bandwidth, packet analysis, etc.)
  - Engineering workstation host system processes

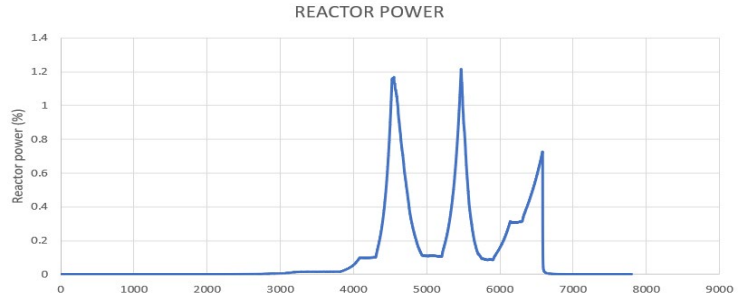
Normal and Abnormal States

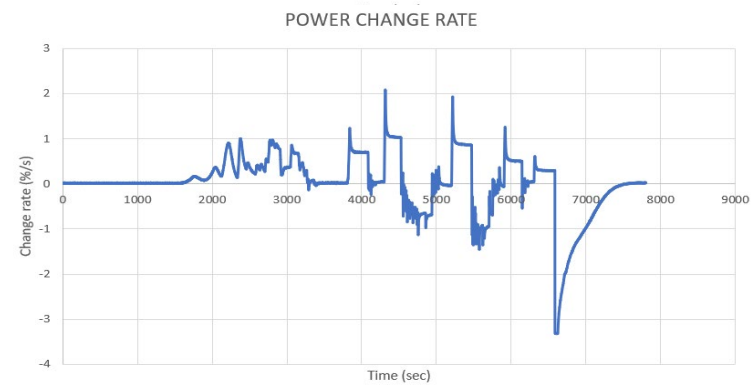
- **Normal operation/state**
  - Startup procedure
  - Any power level up to 100% (up to 2% change rate per supervisor guidance)
  - Irradiations
  - Shutdown by gang lower or SCRAM
  - Multiple operators
- **Simulated abnormal states (tentative)**
  - Power excursion (ramp up > 2%, alarm @6%), modify critical rod positions, etc.
  - Oscillations (e.g., equipment degradation), unusual power levels
  - Equipment on/off (pump, HVAC, temperature increase)
  - Cyber
    - Eavesdropping (e.g., process and operation data)
    - Data exfiltration (e.g., Monju type attack, steal host system data)
    - DoS (e.g., Davis-Besse, Browns-Ferry)
    - False data injection (e.g., Stuxnet type replay attack, data tampering)
  - Multiple scenarios (e.g., DoS for distraction+replay attack+oscillations)

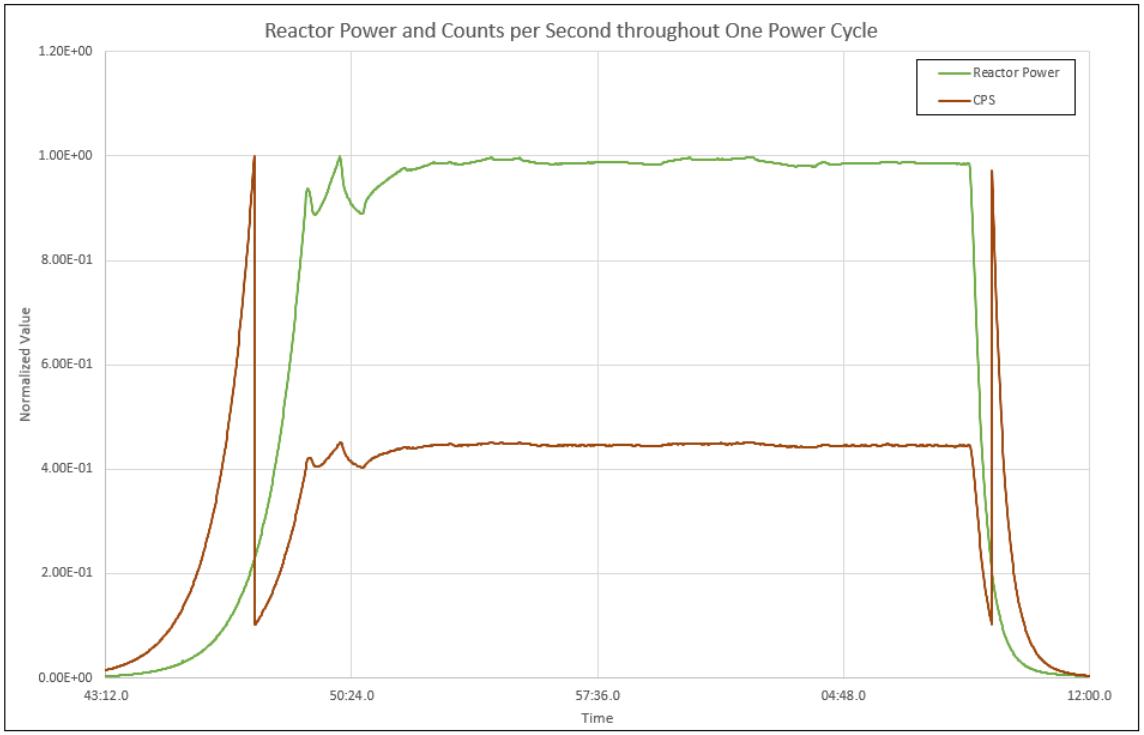
Datasets for Benchmarking





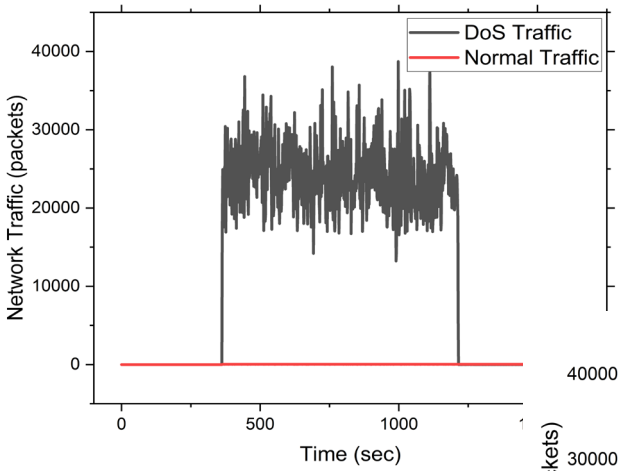


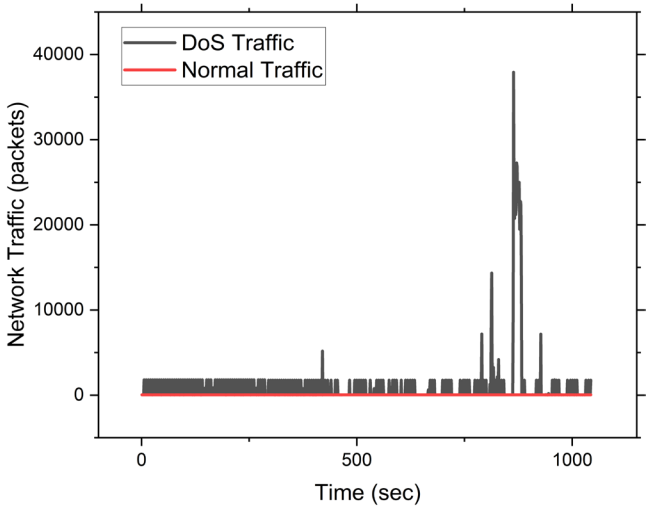


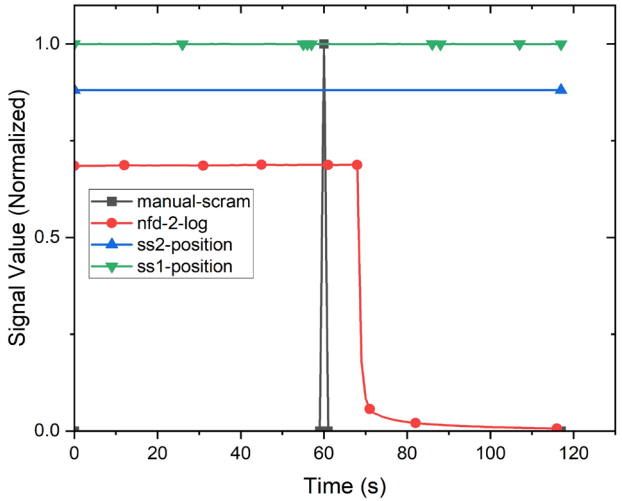


RADIATION IMAGING AND NUCLEAR SENSING LABORATORY

DoS and FDI







PURDUE UNIVERSITY | School of Nuclear Eng

RADIATION IMAGING AND NUCLEAR SENSING LABORATORY

Conclusions

- Explored potential of addressing nuclear I&C confidentiality requirements with QKD
- Developed novel simulation tool (NuQKD) offering unique features
- Constructed reference reactor scenario inspired from modern designs
- Cyber-physical testbed installed and operational
- More than 2000 OT and IT signals including real-time cyber events
- Preliminary results are promising, justify further real-world experimentation

Publications (1/2)

Journal papers

i. Konstantinos Gkouliaras, Vasileios Theos, William Richards, Zachery Dahm, and Stylianos Chatzidakis (2023). “Exploring the Feasibility of Quantum-based Secure Communications for Nuclear Applications.” Submitted for publication to IEEE Quantum Science and Engineering journal.

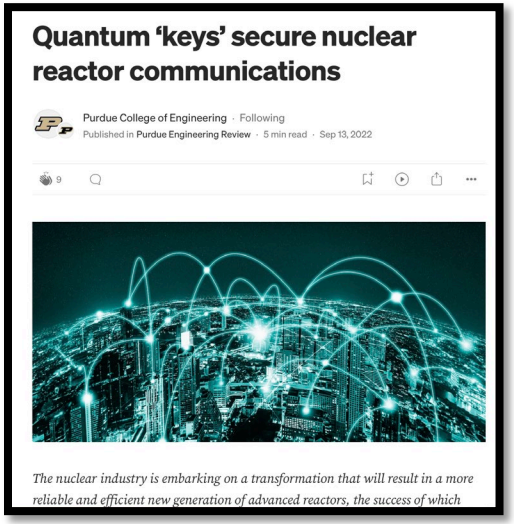
ii. Konstantinos Gkouliaras, Vasileios Theos, William Richards, Zachery Dahm, and Stylianos Chatzidakis (2023). “NuQKD: A Modular Quantum Key Distribution Simulation Framework for Engineering Applications.” Submitted for publication to Advanced Quantum Science and Technology journal.

Theses

i. Vasileios Theos (2023). “Design and Development of a Real-time Cyber-physical Testbed for Cybersecurity Research.” MS Thesis, School of Nuclear Engineering, Purdue University.

ii. William Richards (2023). “Developing Universal AI/ML Benchmarks for Nuclear Applications.” MS Thesis, School of Nuclear Engineering, Purdue University.

iii. Konstantinos Gkouliaras (2023). “Investigating the Feasibility of Quantum Key Distribution for Nuclear Reactor Communications.” MS Thesis, School of Nuclear Engineering, Purdue University.



Publications (2/2)

Conference papers

i. Konstantinos Gkouliaras, Vasileios Theos, Philip G. Evans, Stylianos Chatzidakis (2023). “Simulating Quantum Key Distribution for Nuclear Reactor Communications with NuQKD.” Transactions of the American Nuclear Society, November 12–15, 2023, Volume 129, accepted.

ii. Vasileios Theos, Konstantinos Gkouliaras, True Miller, Brian Jowers, Stylianos Chatzidakis (2023). “Towards a Cyber-Physical Testbed for Cybersecurity Research in Nuclear Environments.” Transactions of the American Nuclear Society, November 12–15, 2023, Volume 129, accepted.

iii. Konstantinos Gkouliaras, Vasileios Theos, Reshma Ughade and Stylianos Chatzidakis (2022). “NuQKD: Development of a QKD simulation tool for nuclear reactor communications.” Transactions of the American Nuclear Society, November 13–17, 2022, Volume 129, accepted.

iv. Vasileios Theos, Konstantinos Gkouliaras, Zachery Dahm, True Miller, Brian Jowers, Stylianos Chatzidakis (2023). “A Physical Testbed for Nuclear Cybersecurity Research.” Transactions of the American Nuclear Society, June 11–14, 2023, Volume 128, pp. 175–178.

v. Vasileios Theos, Konstantinos Gkouliaras, True Miller, Brian Jowers, Ryan Smith and Stylianos Chatzidakis (2022). “Development of A Quantum-Based Cyber-Physical Testbed For Secure Communications In Nuclear Reactor Environments.” Transactions of the American Nuclear Society, November 13–17, 2022, Volume 127, accepted.

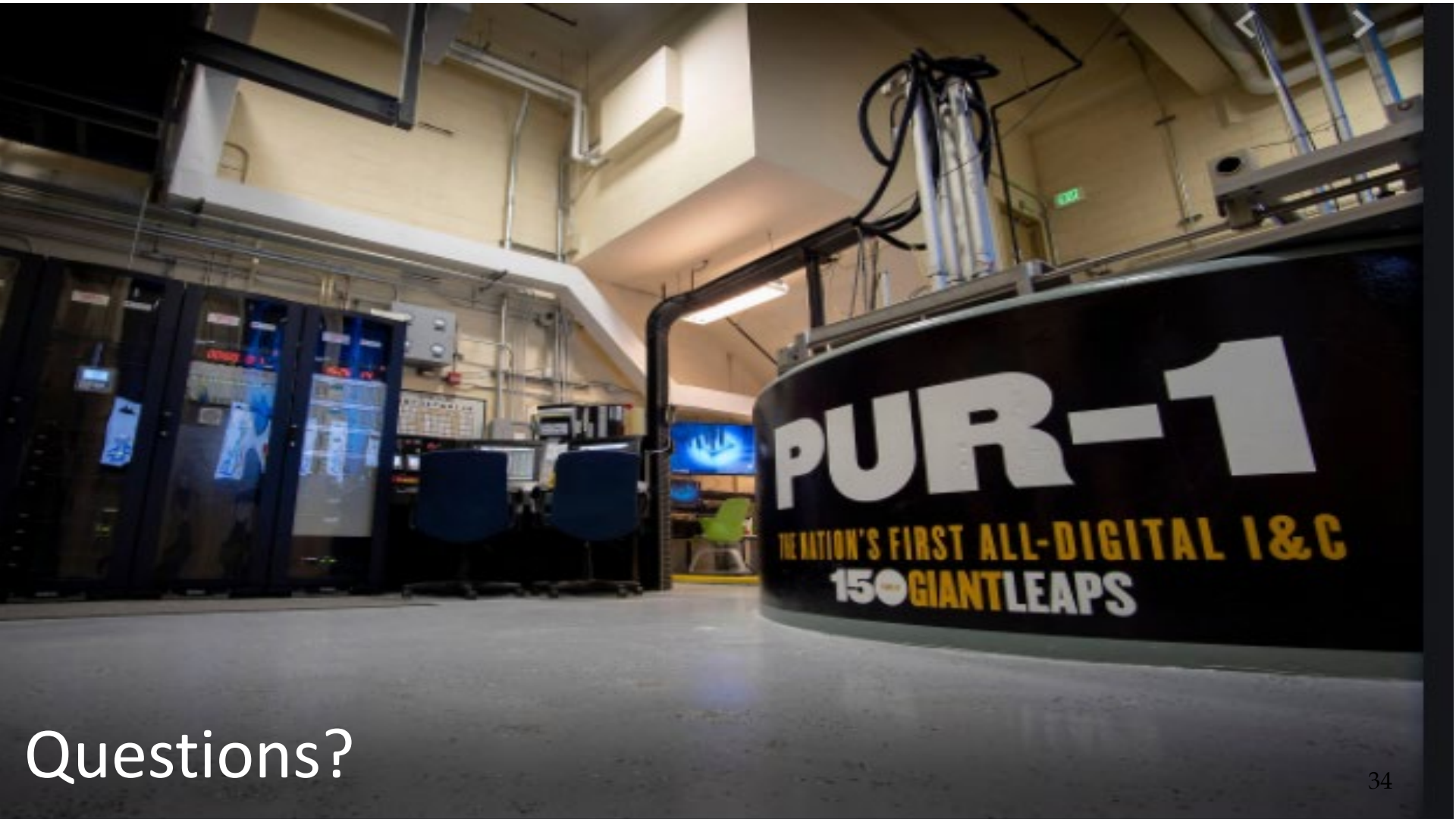
vi. Konstantinos Gkouliaras and Stylianos Chatzidakis (2022). “Evaluation of a QKD Network Structure Suitable for Secure Communications for Advanced Nuclear Reactors.” Transactions of the American Nuclear Society, June 12–16, 2022, Volume 126, pp. 188–191.

vii. Stylianos Chatzidakis and Robert Ammon (2021). “Using the PUR-1 Research Reactor to Explore Quantum Key Distribution for Nuclear I&C Cybersecurity.” Abstract in Meeting Archives of the 2021 Test, Research and Training Reactors (TRTR) Annual Conference, October 18-21, 2021.

Acknowledgements

This research is being performed using funding received from the DOE Office of Nuclear Energy's Nuclear Energy University Programs under contract DE-NE00009174.

We also thank Lon Dawson and Ben Cipiti at Sandia and Katya Le Blanc at INL for fruitful discussions and expert input.



Questions?