Quantum-based Secure Communications for Remote Operations

NEUP Project 21-24354

2024 ARSS Spring Program Review

Stylianos Chatzidakis

Assistant Professor and Associate PUR-1 Director

School of Nuclear Engineering

Purdue University

May 2024

West Lafayette, IN

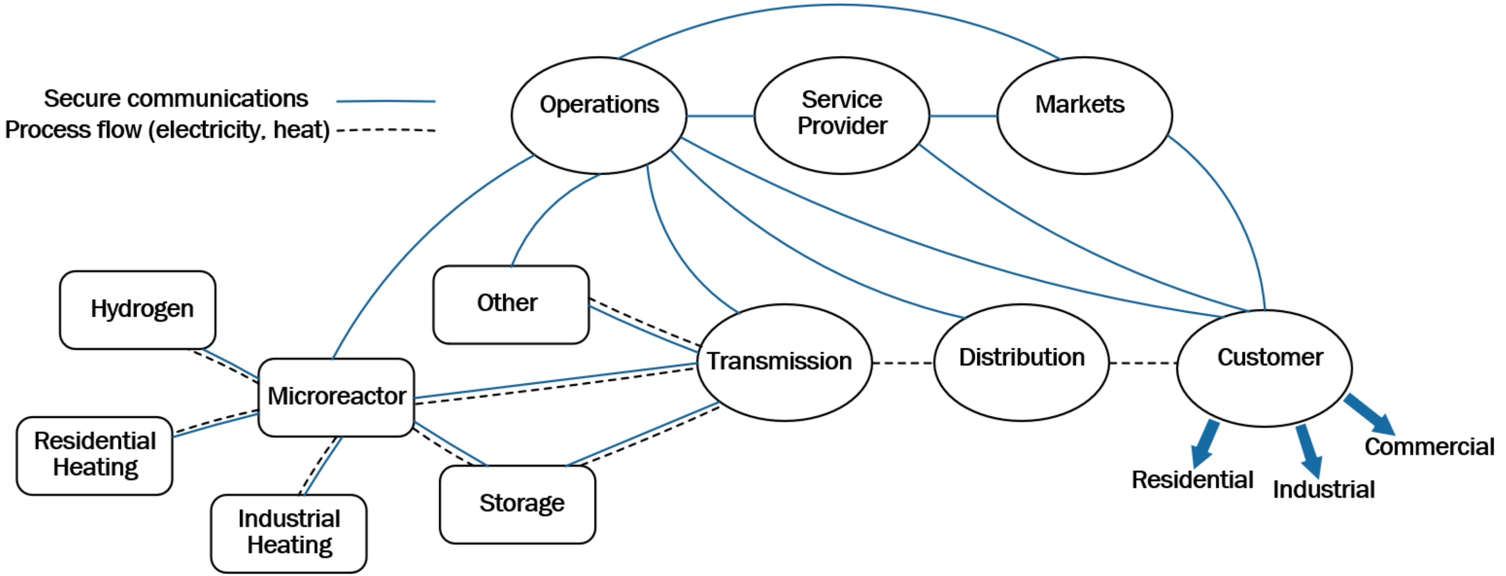
Team Info

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

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

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

New technologies…new challenges



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

Digitalization => New architectures and new vulnerabilities

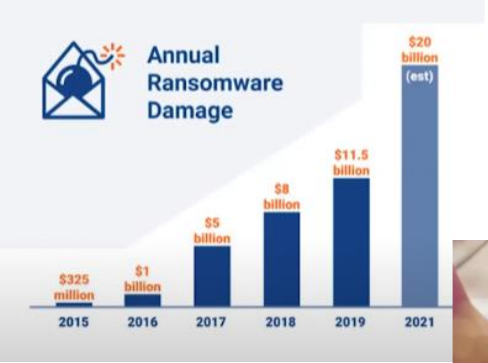
New technologies => Quantum computing Adversaries now have access to new tools with unprecedent capabilities

What about Cybersecurity?

What about Cybersecurity?

1st Cyber Age

2nd Cyber Age



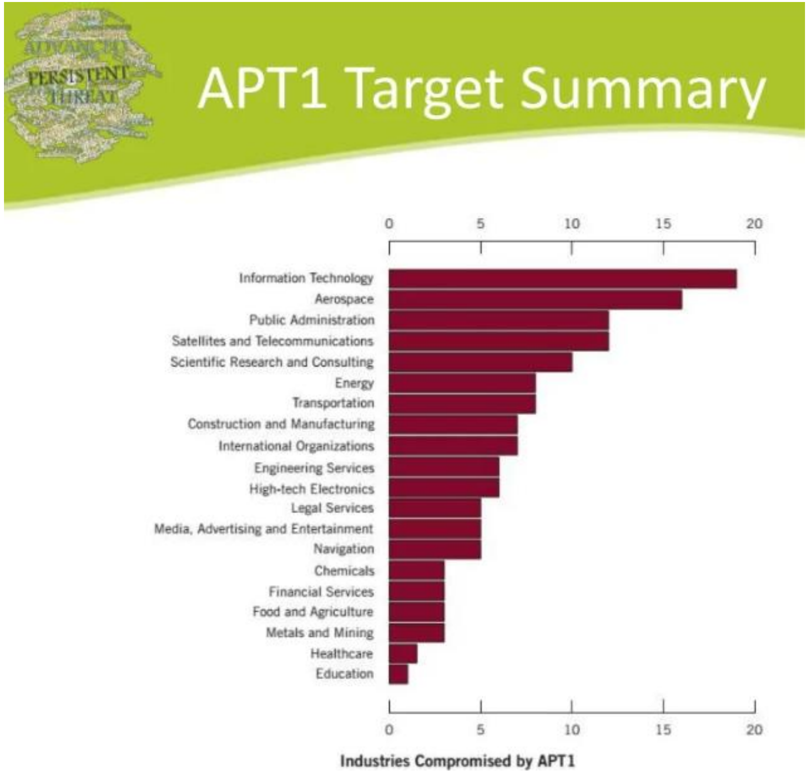
"I don't care what you do,
just keep the plant running!"

- CEO of a large chemical processing plant on security

3rd Cyber Age

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

Problem Statement

Conventional encryption and IT solutions do not guarantee security for nuclear communications

How can we design an unconditional security framework to fulfil cyber requirements?

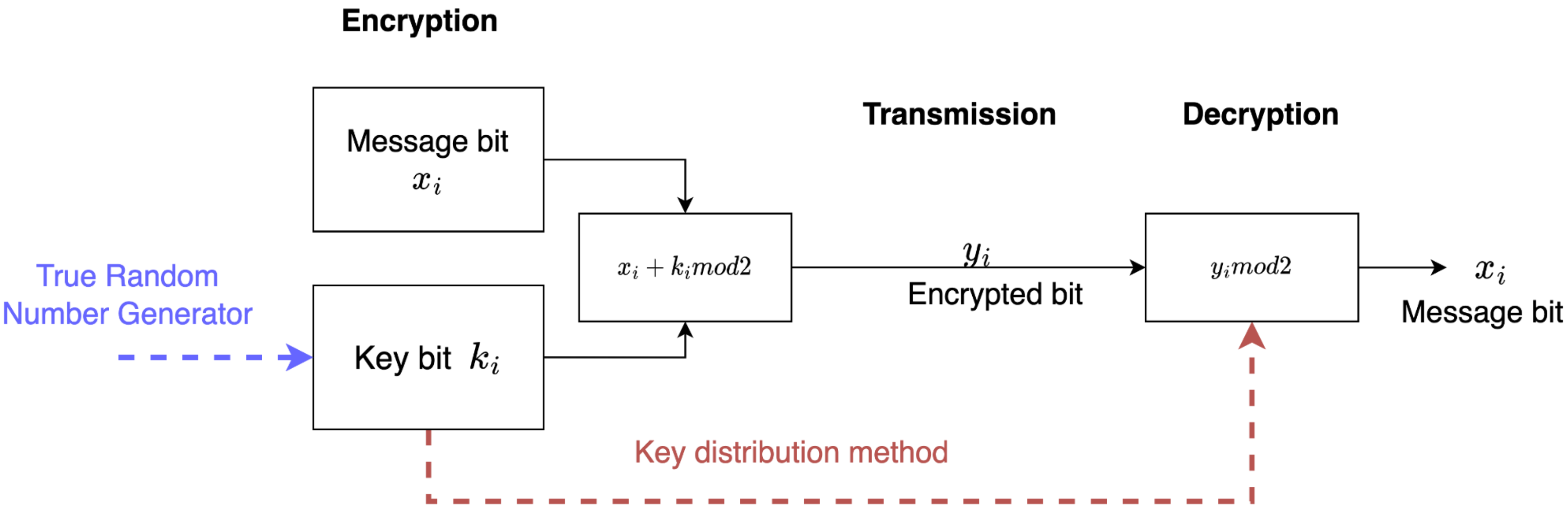
Goals & Objectives

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

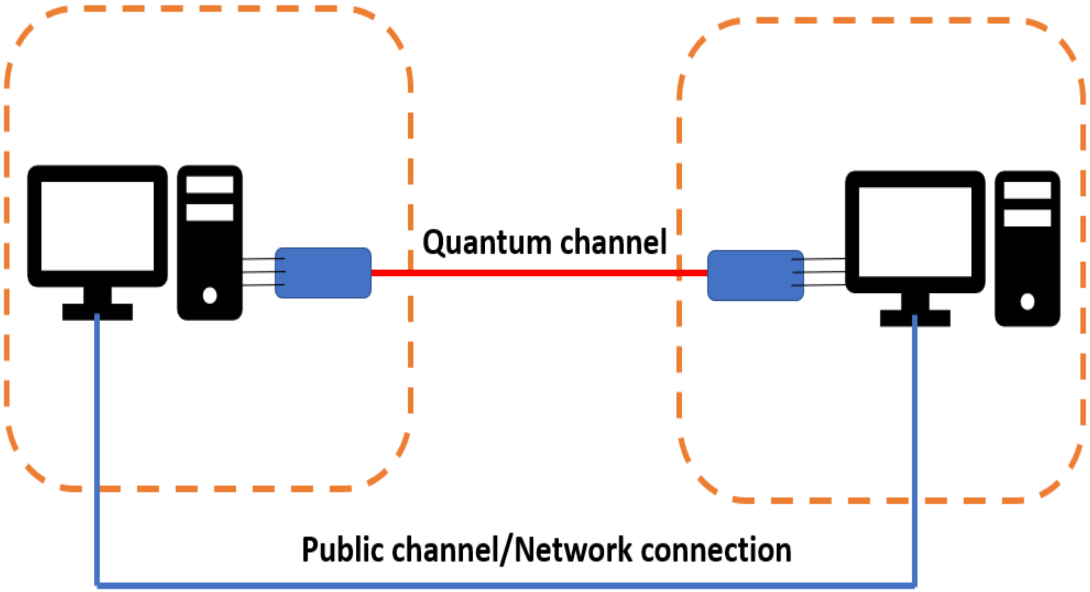
Objectives:

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

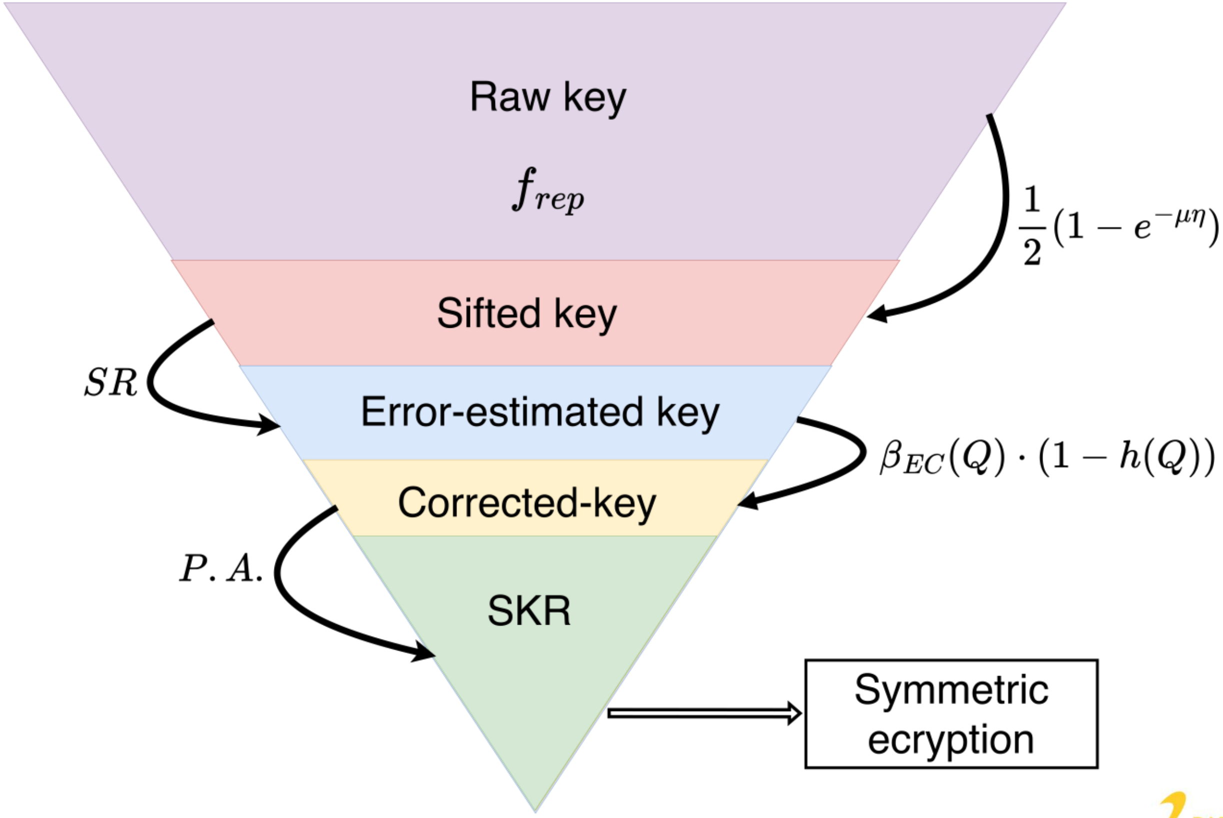
Quantum Key Distribution Guarantees Confidentiality



Quantum Key Distribution Provides Detection of Adversary

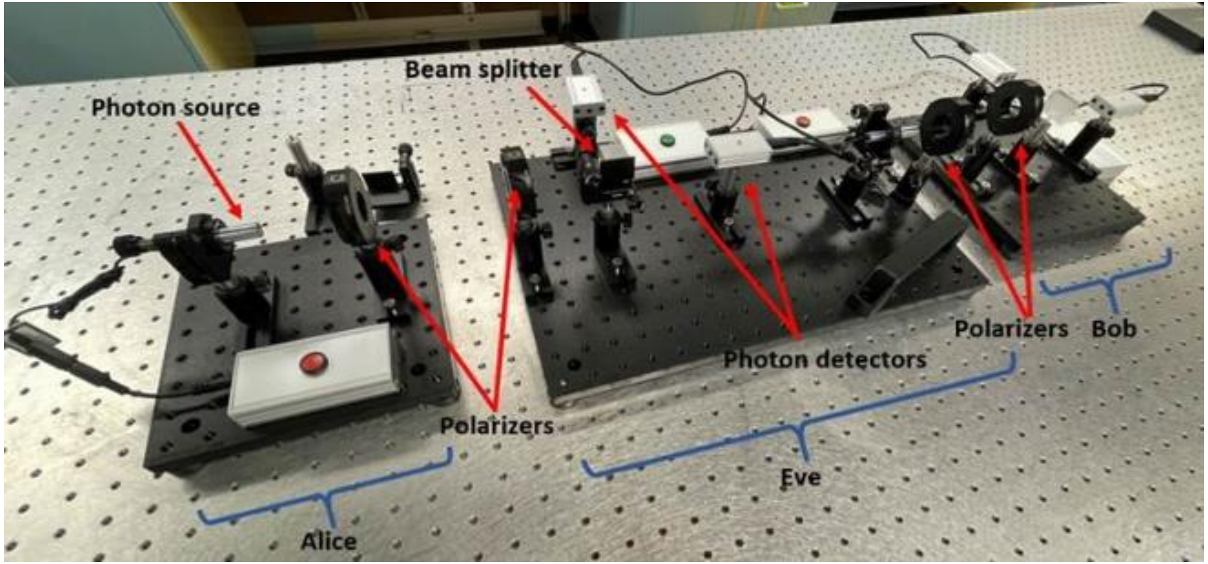


How it works



Raw key
f_{rep}
$\frac{1}{2}(1 - e^{-\mu\eta})$
Sifted key
SR
Error-estimated key
$\beta_{EC}(Q) \cdot (1 - h(Q))$
Corrected-key
$P.\,A.$
SKR
Symmetric ecryption

How it works



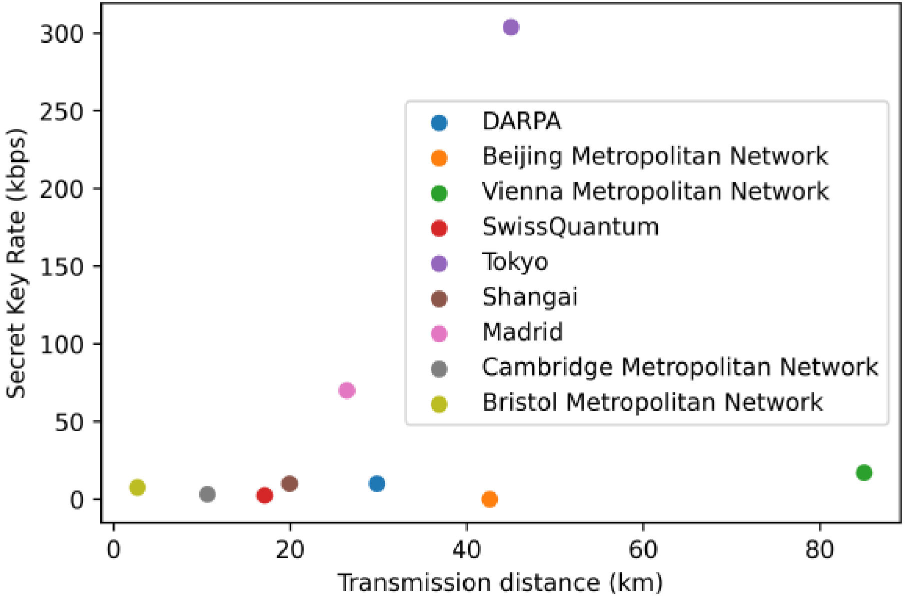
Send photons → Measure QBER → Higher QBER → Lower Security

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

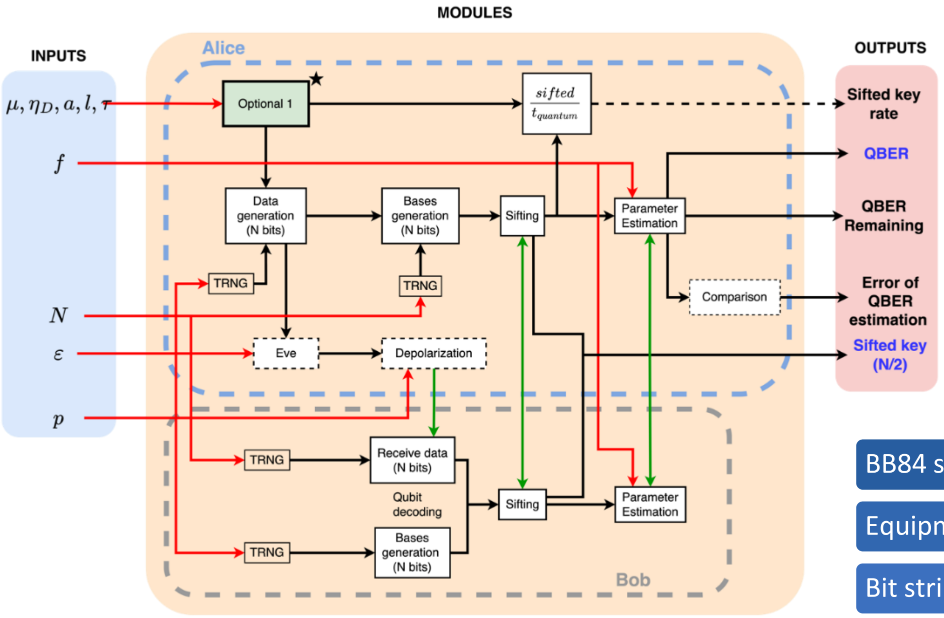
$$QBER = q_e(1 - q_{ch}) + (1 - q_e)q_{ch} = \frac{\varepsilon}{4} + \frac{2q}{3}(2 - \varepsilon)$$

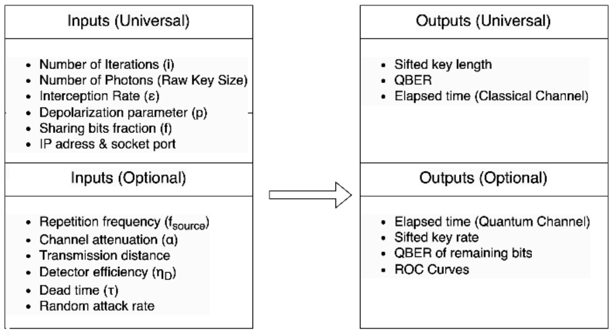
Quantum "Wars"

Network	Year	Longest link	SKR
DARPA [100]	2004	29.8 km	10kbps
Beijing Metropolitan Network [101]	2007	42.6 km	-
Vienna Metropolitan Network [102]	2008	85 km	17kbps
SwissQuantum [103]	2009	17.1 km	2.4kbps
Tokyo [104]	2010	45 km	304kbps
Shangai [105]	2016	19.92 km	10kbps
Madrid [106]	2018	26.4 km	70kbps
Cambridge Metropolitan Network [107]	2019	10.6 km	2.58Mbps
Bristol Metropolitan Network [108]	2019	2.7 km	3.17kbps
Xiran/Guangzhou Metropolitan Link [109]	2019	30.02 km	7.57kbps



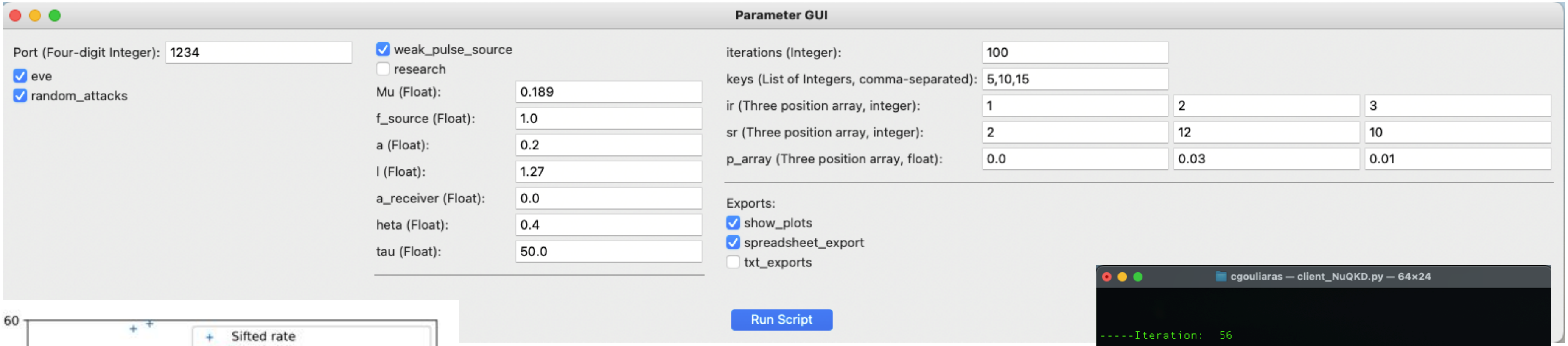
Modeling and Simulation

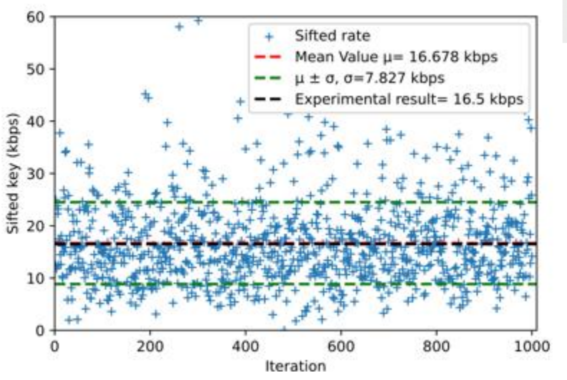


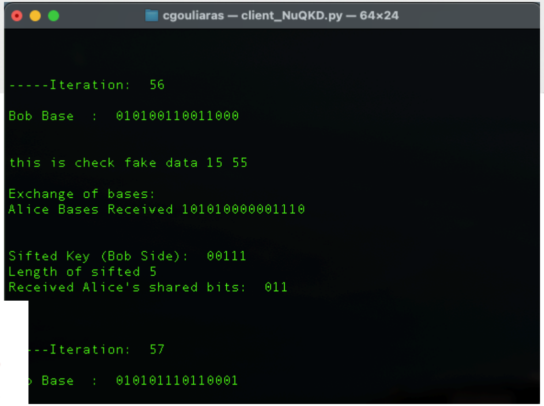


- BB84 simulation (optical fiber and free space)
- Equipment imperfections (source, channel, detector)
- Bit strings from True Random Number Generator (TRNG)
- Two-terminal /Single terminal execution
- Modular design approach
- Advanced customization of multiple input parameters
- Evaluation and export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

NuQKD is now benchmarked and fully operational



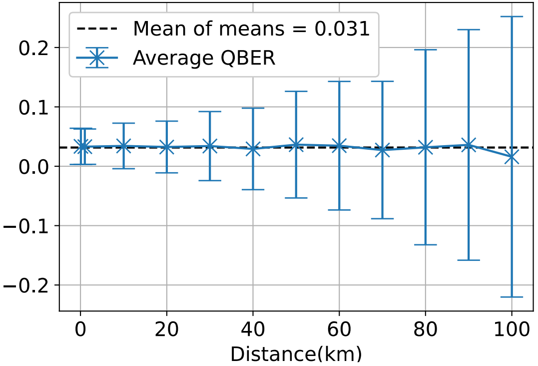


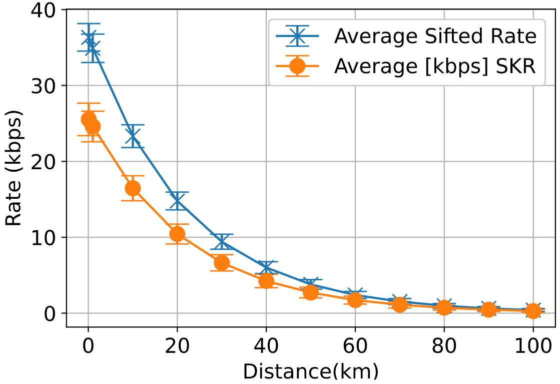


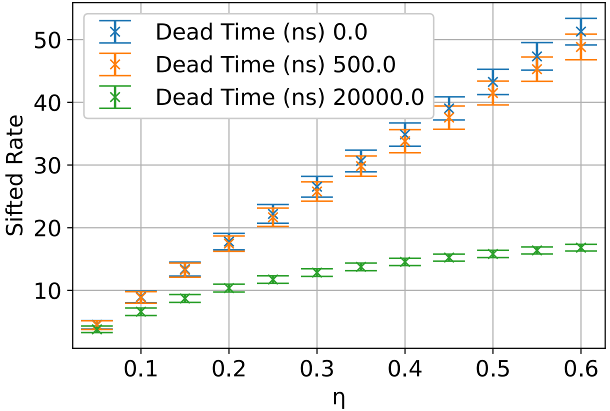
PURDUE UNIVERSITY School of Nuclear Engineering

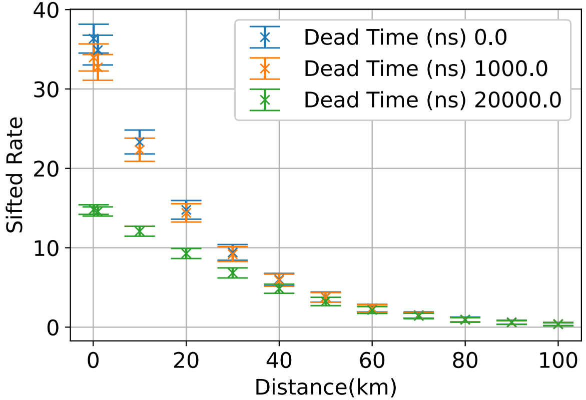
RADIATION IMAGING AND NUCLEAR SENSING LABORATORY

Parametric Analysis

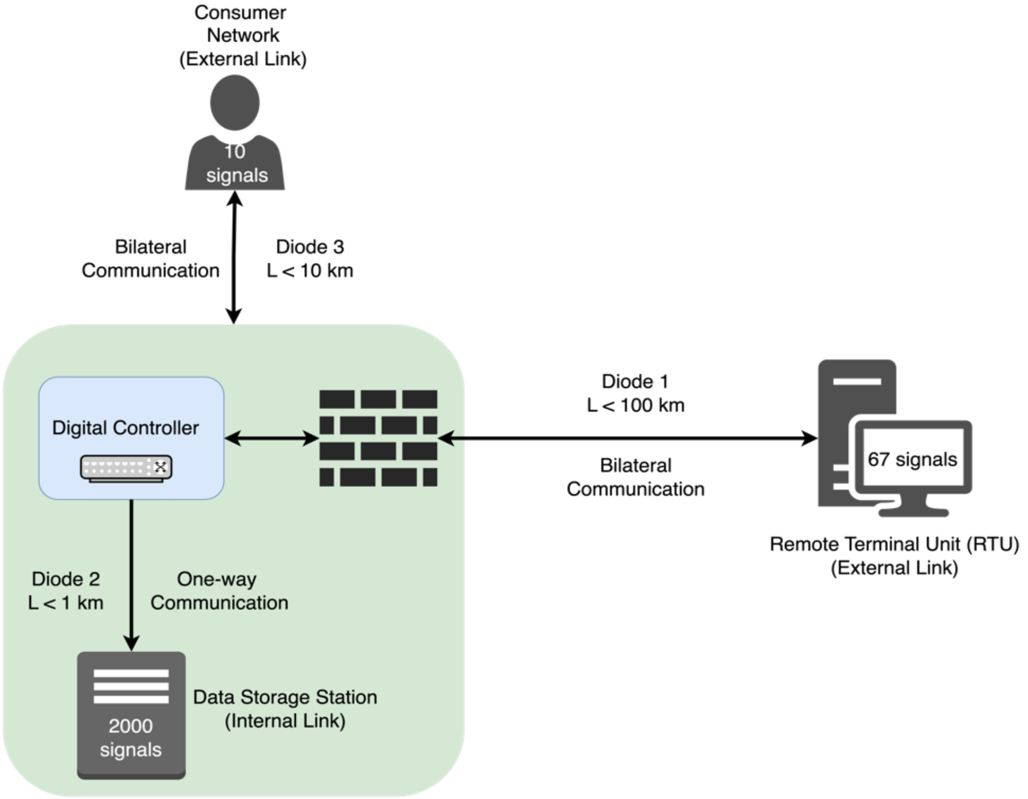








Reactor reference scenario



1. Reactor to Remote Workstation (RTU)

2. Reactor to Data Storage Station

3. Reactor to Energy Grid / Consumer Network

Required Bandwidth

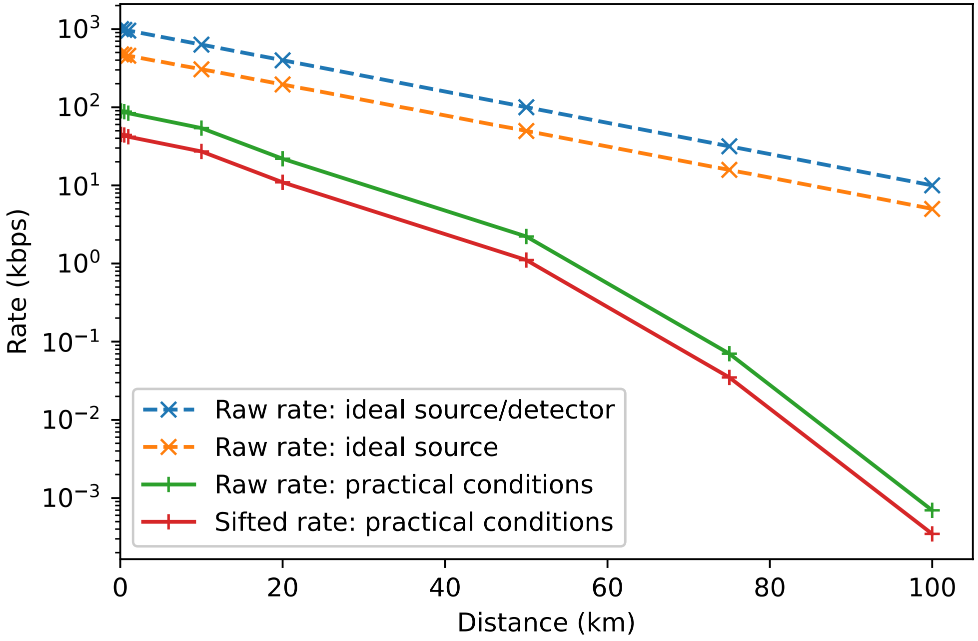
- PUR-1 data used as case study
- OT signals
  - 1 Hz sampling
  - 6-digit accuracy
- Min and max values recorded:
  - Over 24 hours of operation
  - Including transients and outliers

64 kbps required to transmit all 2,000 signals

Diode	Distance (km)	Type	Signals transmitted	Bandwidth Custom BCD (kbps)	Bandwidth IEEE-754 (kbps)
1	100	Two-way	67	0.533	2.144
2	1	One-way	2,000	16	64
3	10	Two-way	10	0.08	0.32

Key rate vs. distance

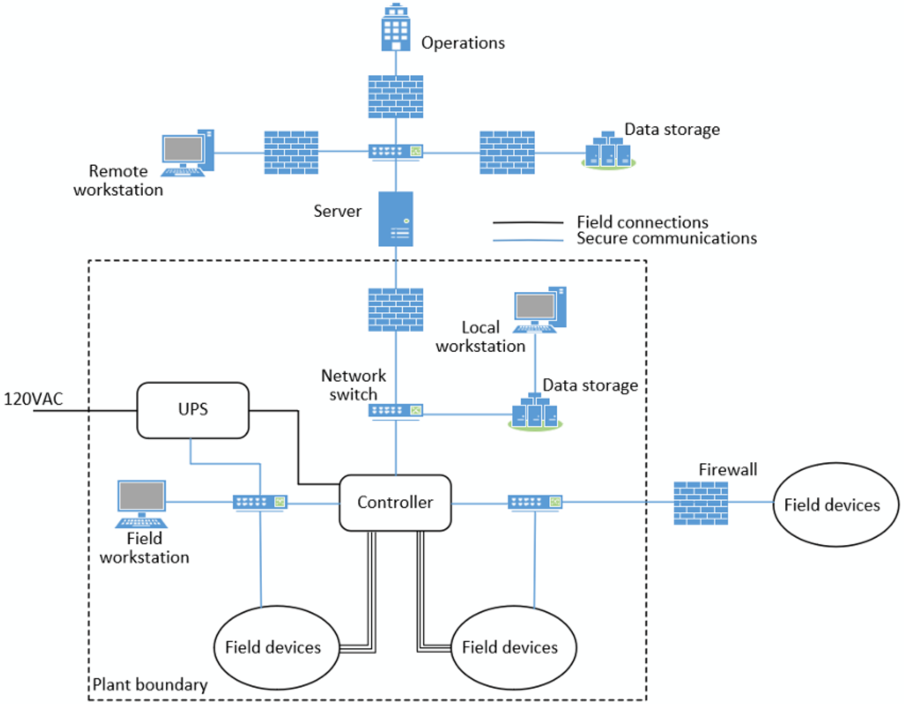
Parameter	Value
Source Repetition rate	1 MHz & 2 MHz
Pulse μ	$\mu = 0.189$
Detector efficiency	0.5
Dead Time	50 ns
Depolarization	5%
Attenuation (channel)	0.2 dB/km
Wavelength	1550 nm SMF



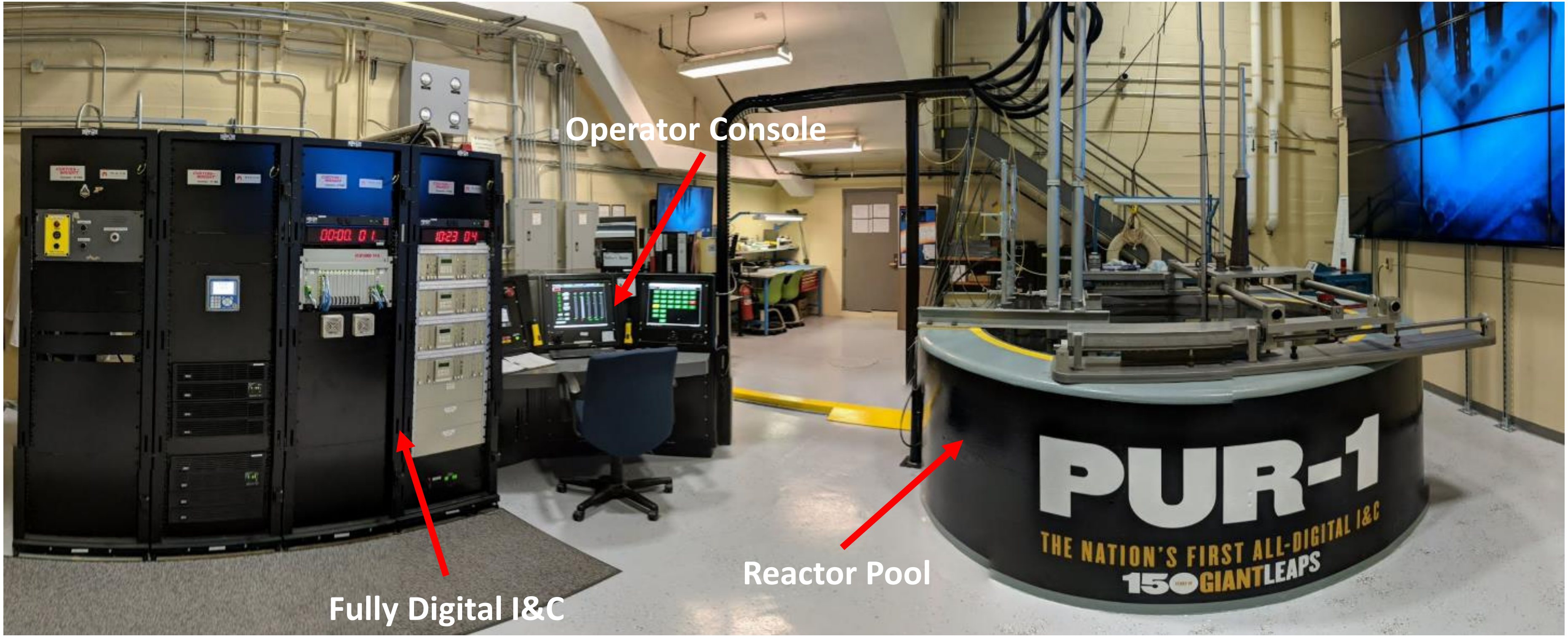
Reliable communication up to 75 km with standard equipment and BB84

Signal Prioritization

Connections	Confidentiality	Integrity	Availability
Field devices to Controller	Low	High	High
Controller to Local Workstation	High	High	High
Controller to Data Storage	High	High	Medium
Local Workstation to Data Storage	High	High	Low
UPS to Controller	Low	High	Low
Field Workstation to Field Devices	Medium	High	Medium
Field Workstation to Controller	Medium	High	Medium
Controller to Server	High	High	Medium
Server to Operations	High	High	High
Server to Remote Workstation	High	High	Low
Server to Data Storage	High	High	Low



Introducing PUR-1

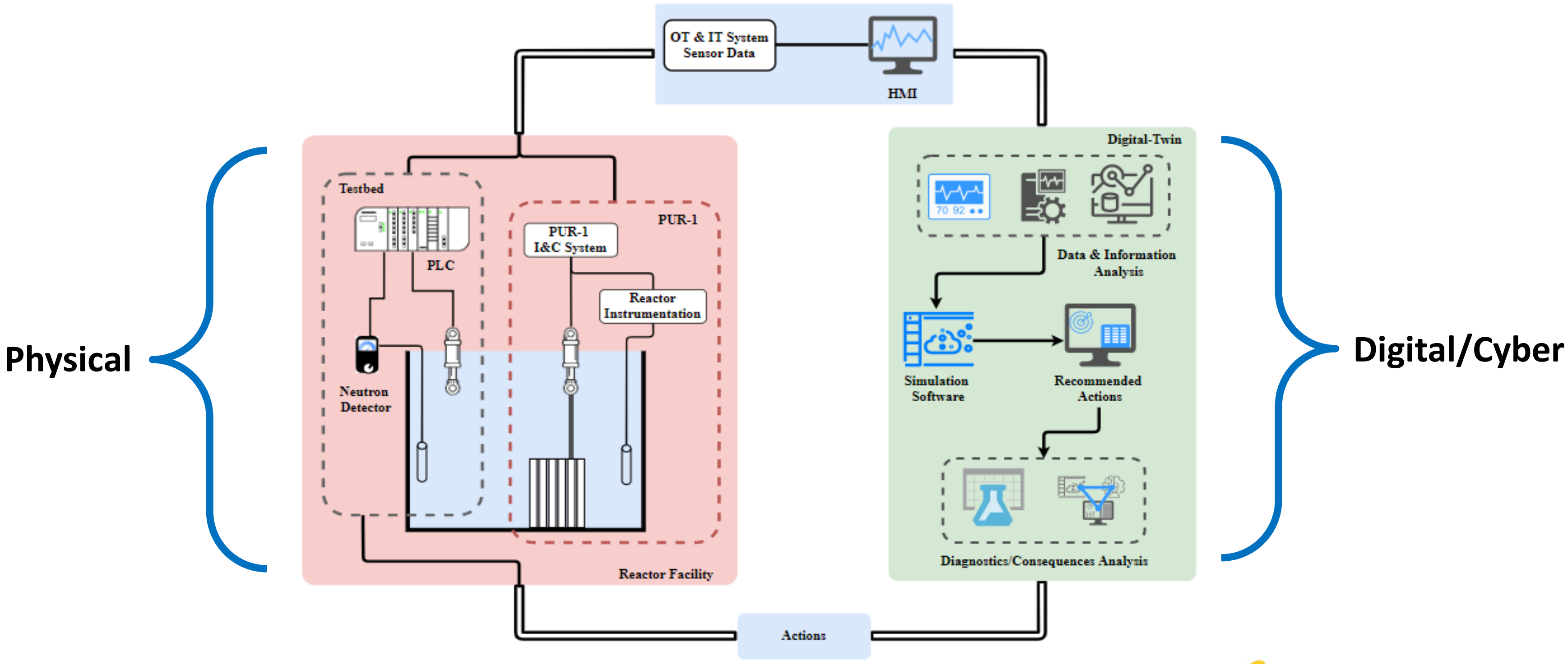


Before and after…

1960 - 2017

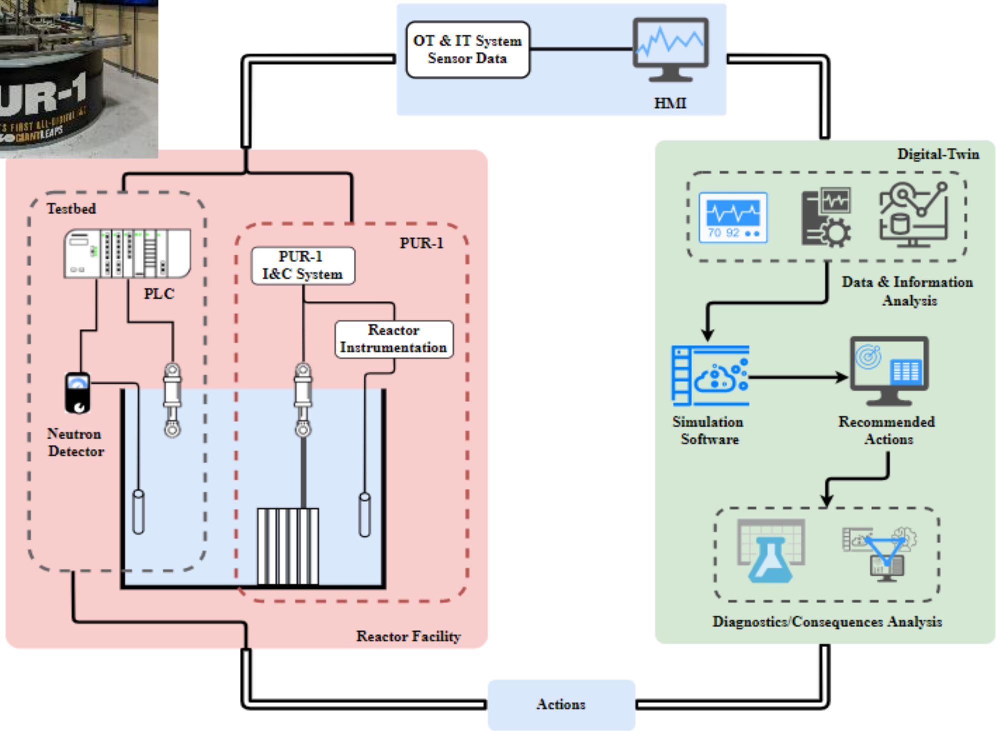
2019 - present

Towards a Real-Time Cyber-Physical Digital Twin

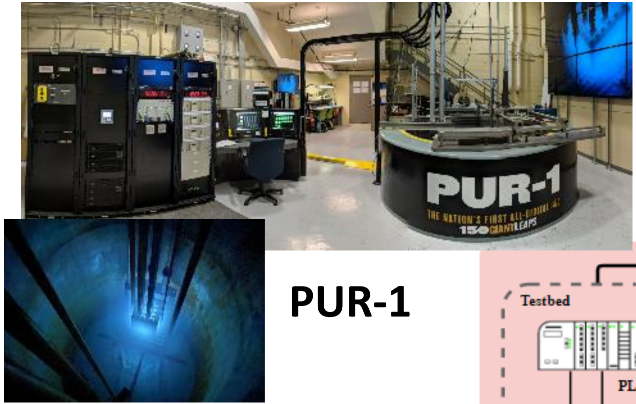


Towards a Real-Time Cyber-Physical Digital Twin

PUR-1

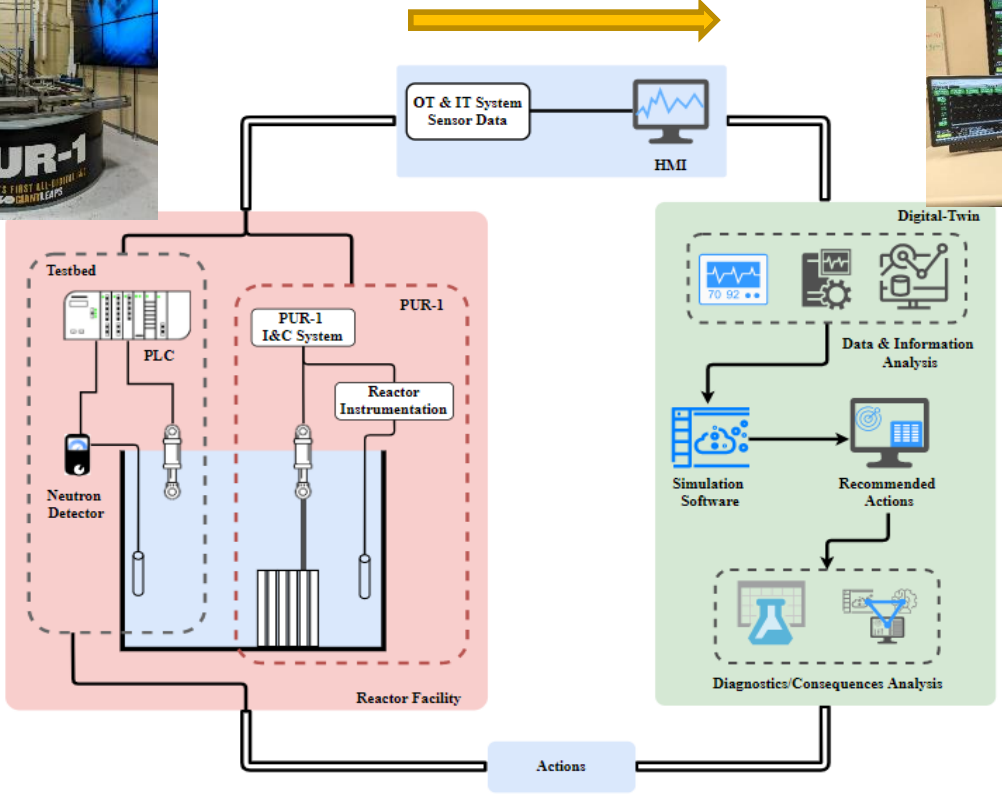


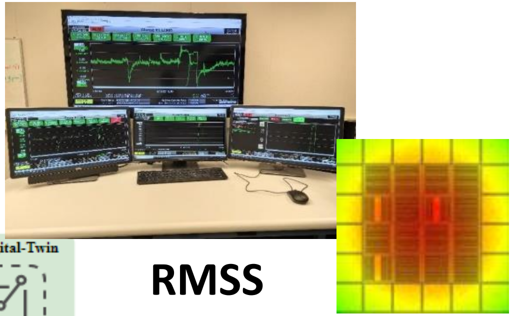
Towards a Real-Time Cyber-Physical Digital Twin



PUR-1

OT/IT Comms

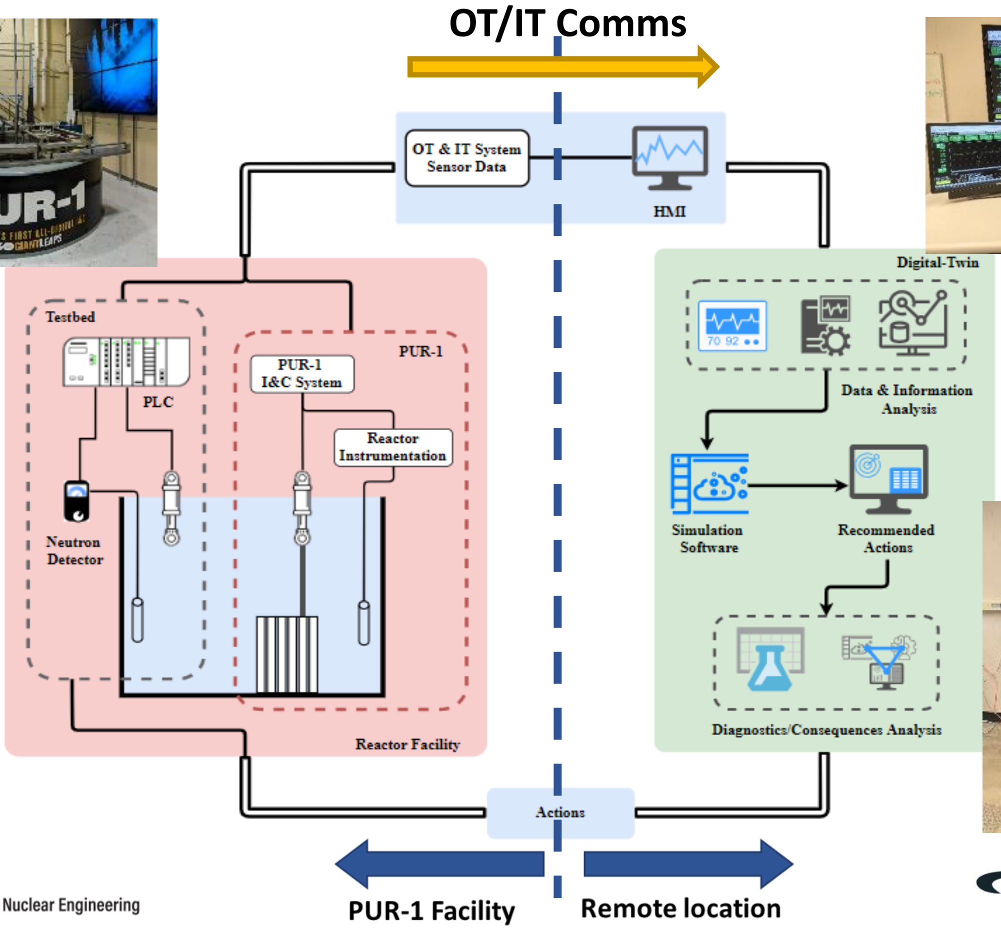


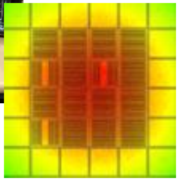


RMSS

Towards a Real-Time Cyber-Physical Digital Twin

PUR-1



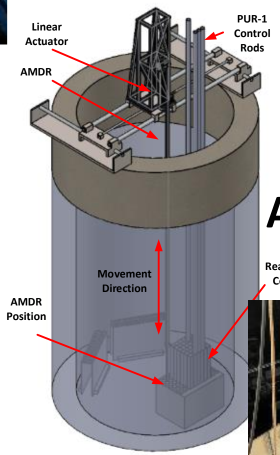


RMSS

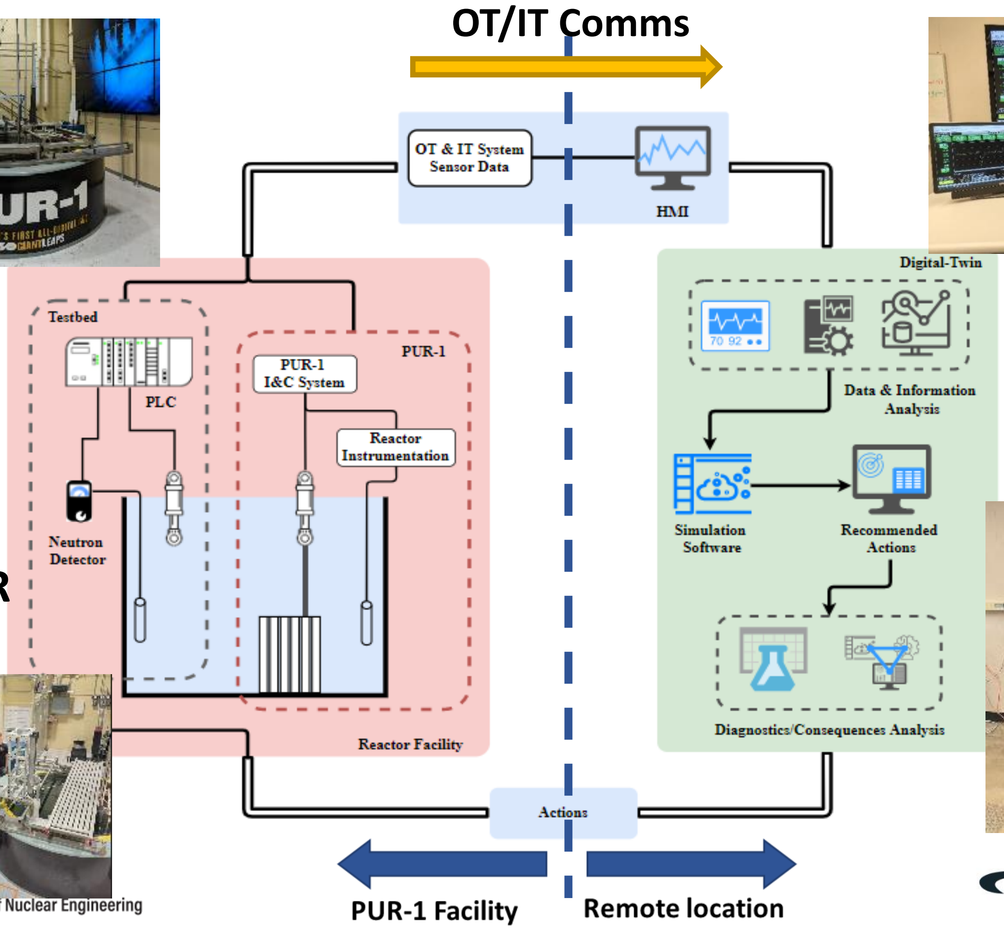
Control rack

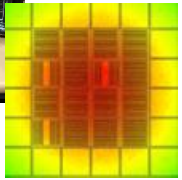
Towards a Real-Time Cyber-Physical Digital Twin

PUR-1



AMDR

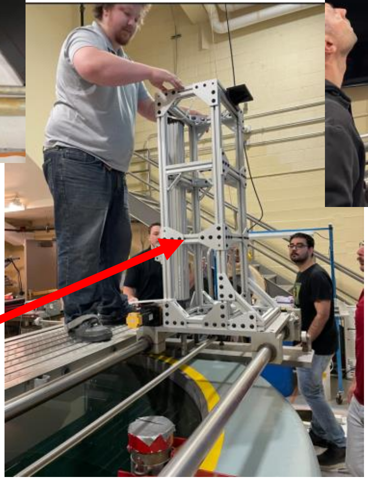


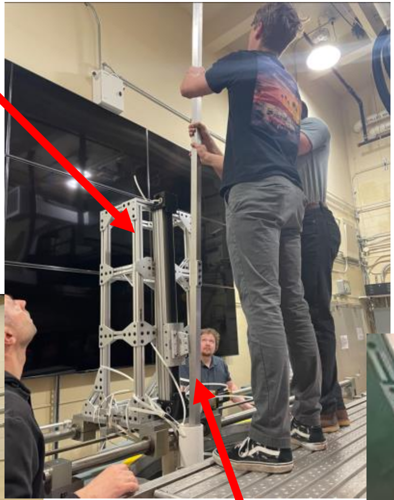


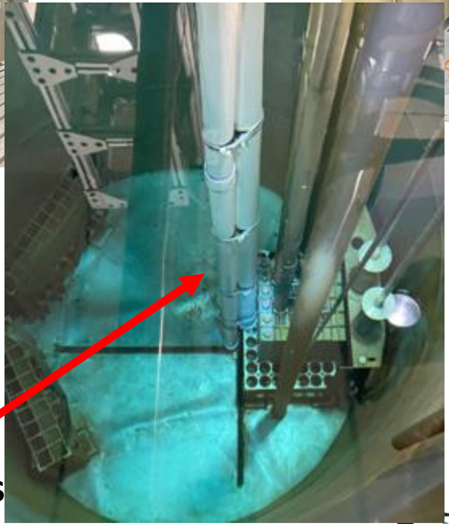
RMSS

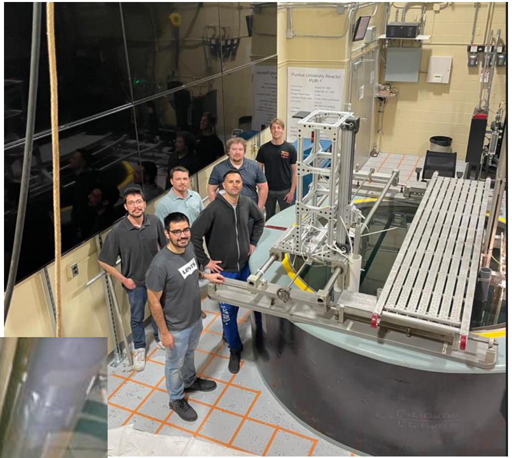
Control rack

Installing and Testing AMDR









Actuator

AMDR

Support structure

Guide tubes

Completed May 2023

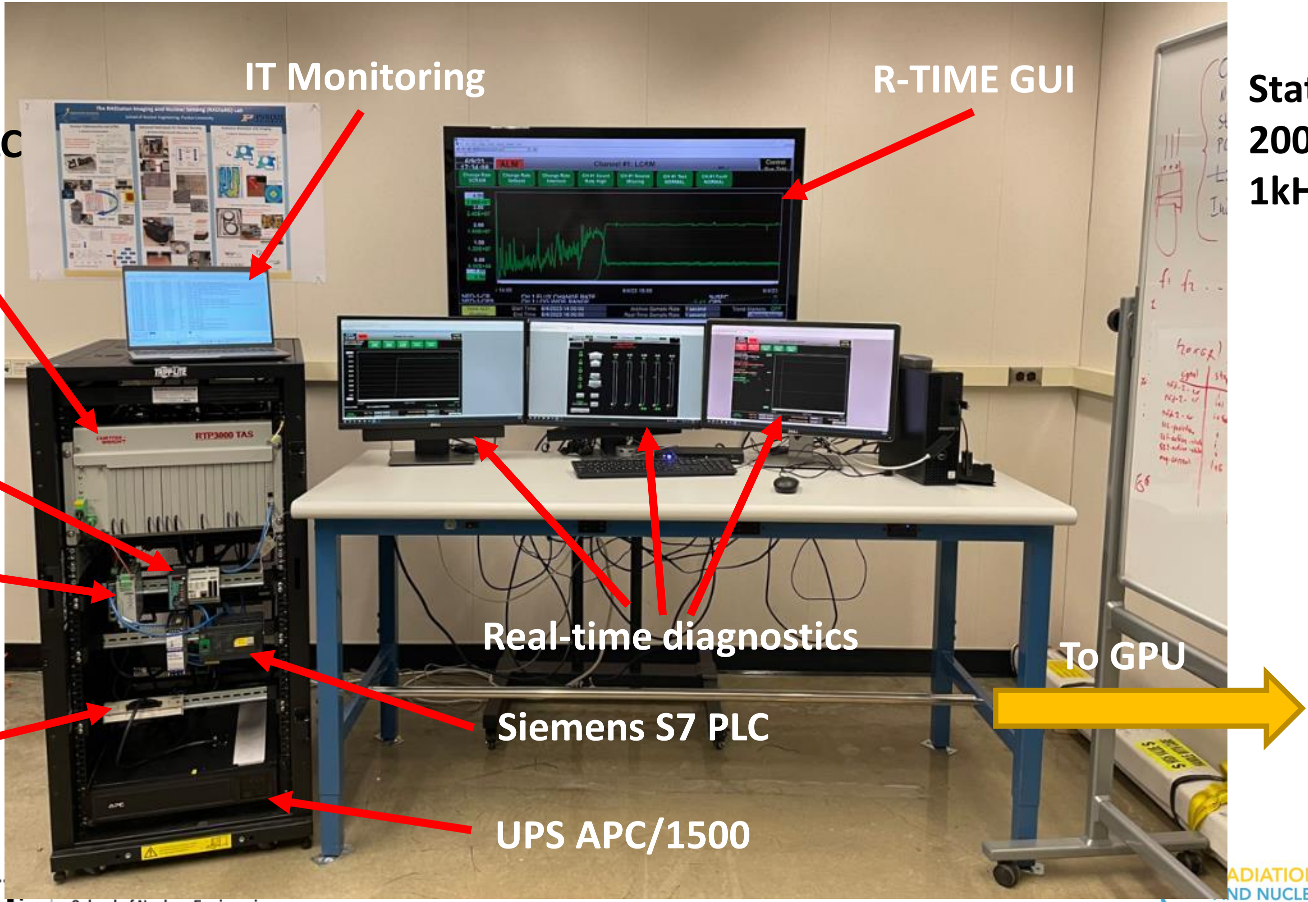
Digital/Cyber Remote Station

RTP 3000 TAS N+
Nuclear grade PLC
16 CH AI/AO
32 CH DI/DO

Field Programmable Gate Array

Power distribution unit

Actuator control



Stats:
2000 parameters
1kHz sampling

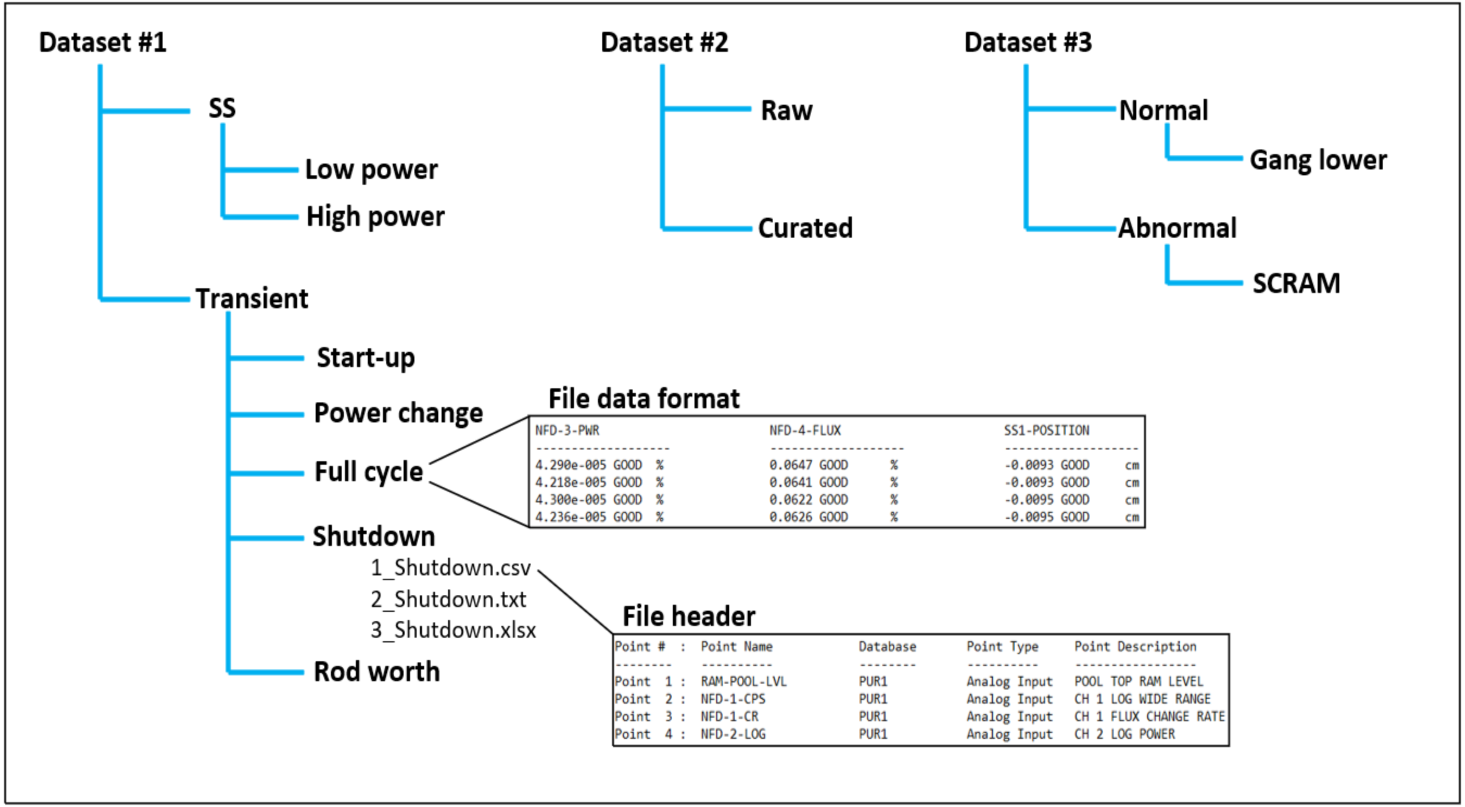
Instrumentation & Control

- **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

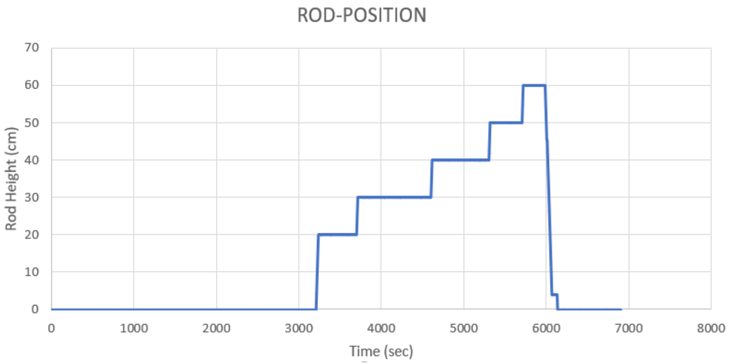


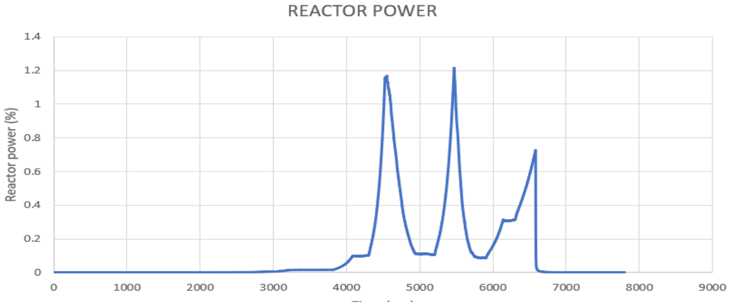
File data format

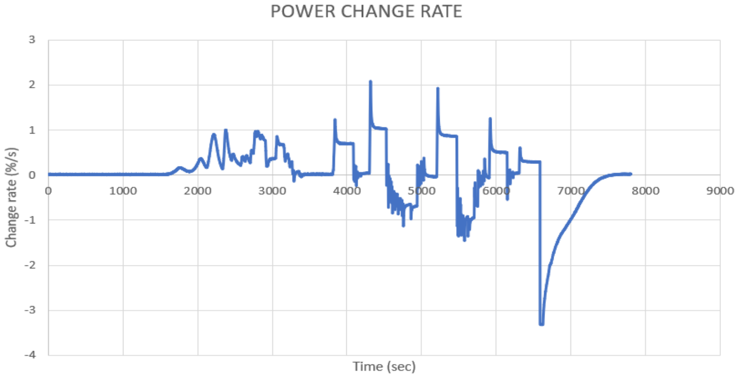
NFD-3-PWR			NFD-4-FLUX			SS1-POSITION		
4.290e-005	GOOD	%	0.0647	GOOD	%	-0.0093	GOOD	cm
4.218e-005	GOOD	%	0.0641	GOOD	%	-0.0093	GOOD	cm
4.300e-005	GOOD	%	0.0622	GOOD	%	-0.0095	GOOD	cm
4.236e-005	GOOD	%	0.0626	GOOD	%	-0.0095	GOOD	cm

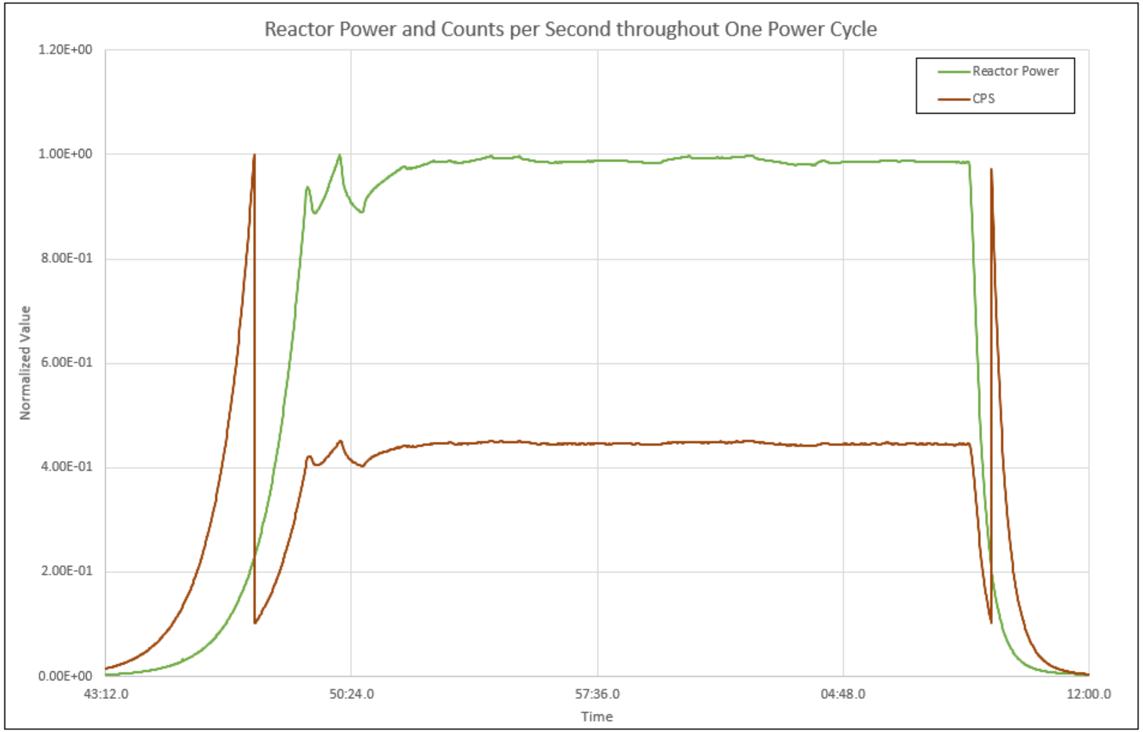
File header

Point # :	Point Name	Database	Point Type	Point Description
Point 1 :	RAM-POOL-LVL	PUR1	Analog Input	POOL TOP RAM LEVEL
Point 2 :	NFD-1-CPS	PUR1	Analog Input	CH 1 LOG WIDE RANGE
Point 3 :	NFD-1-CR	PUR1	Analog Input	CH 1 FLUX CHANGE RATE
Point 4 :	NFD-2-LOG	PUR1	Analog Input	CH 2 LOG POWER



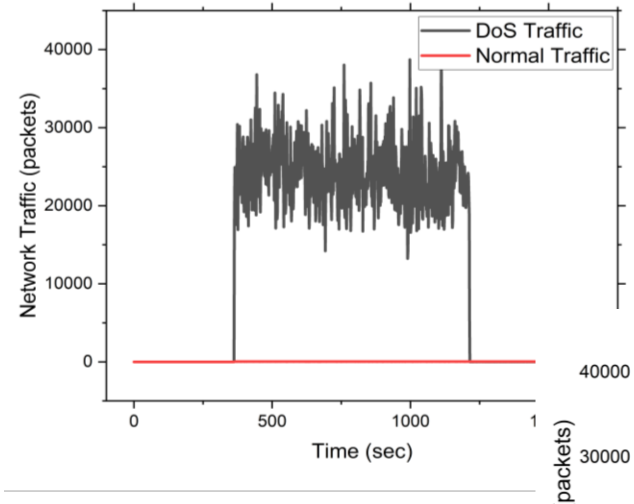


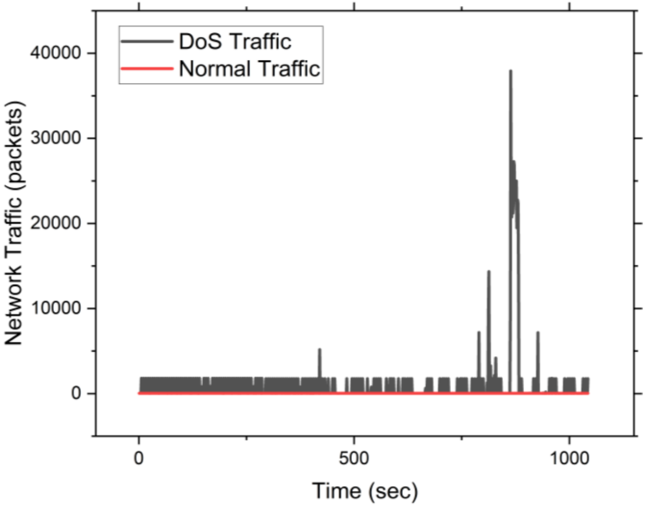


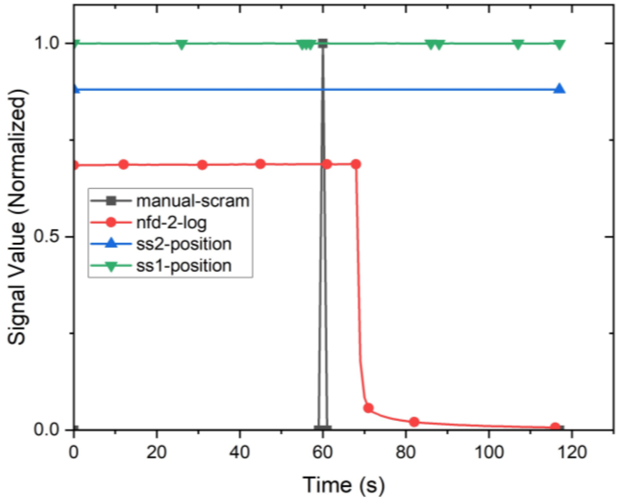


RADIATION IMAGING AND NUCLEAR SENSING LABORATORY

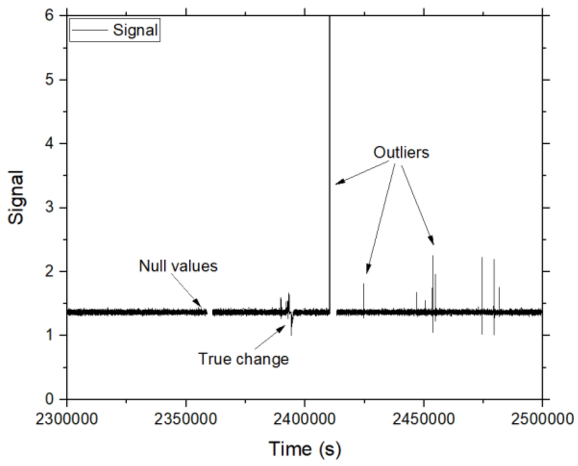
DoS and FDI

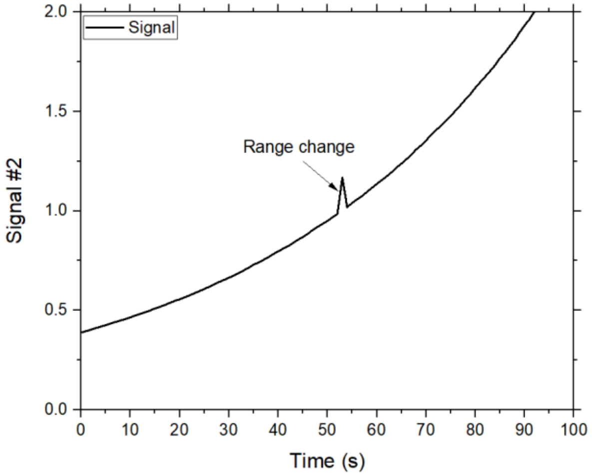

DoS Traffic
Normal Traffic
Network Traffic (packets)
40000
30000
20000
10000
0
0
500
1000
Time (sec)

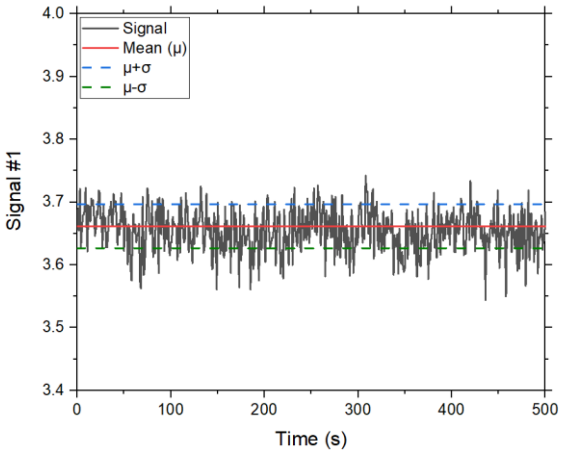

DoS Traffic
Normal Traffic
Network Traffic (packets)
40000
30000
20000
10000
0
0
500
1000
Time (sec)


Signal Value (Normalized)
1.0
0.5
0.0
manual-scram
nfd-2-log
ss2-position
ss1-position
0
20
40
60
80
100
120
Time (s)

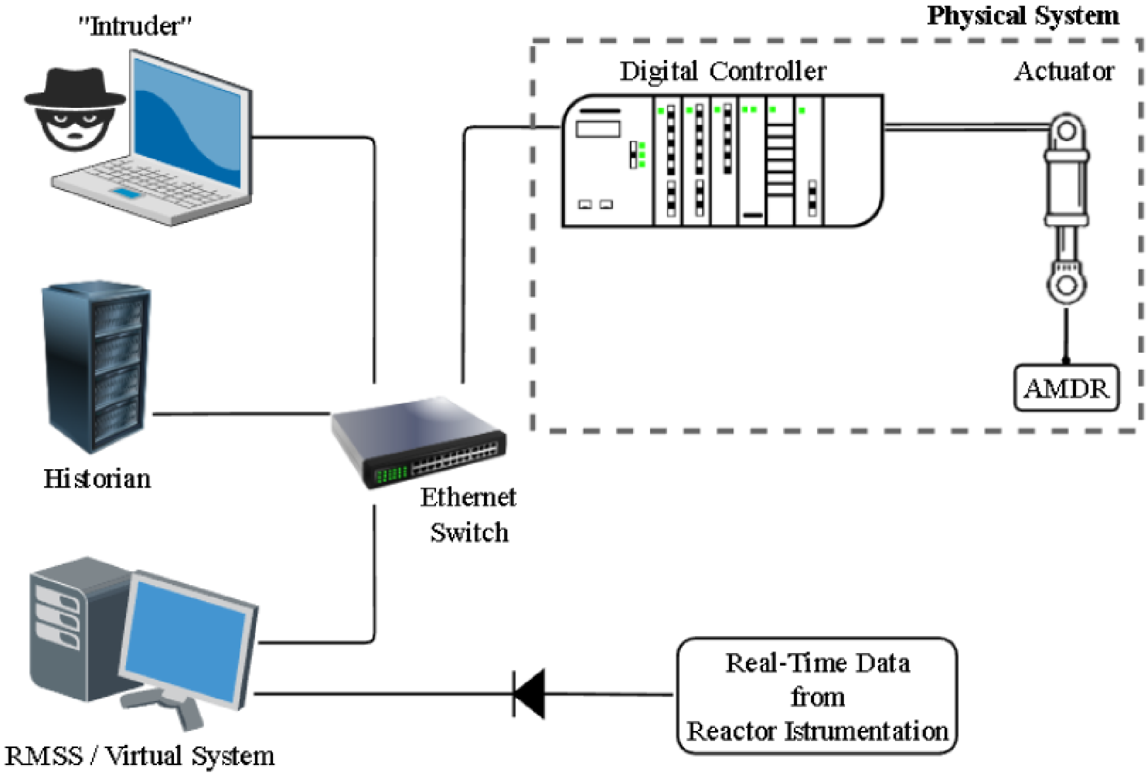
Data Artifacts





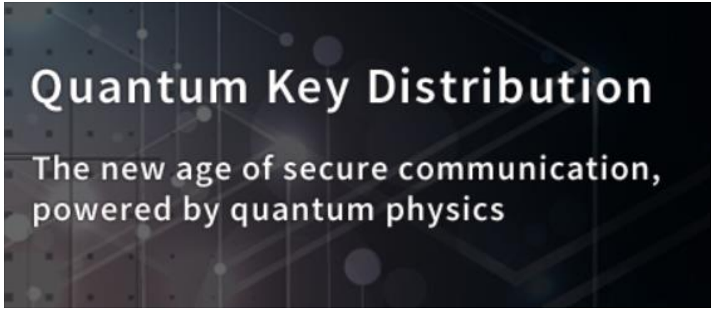


Remote Monitoring System Fully Operational

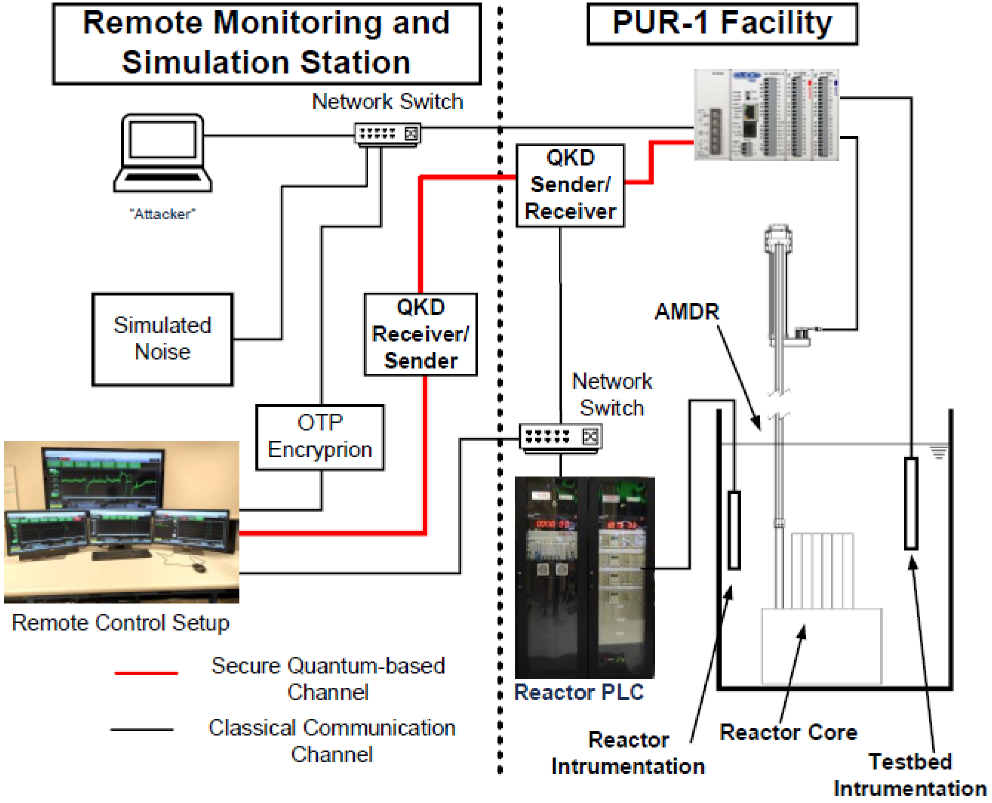


Future Steps

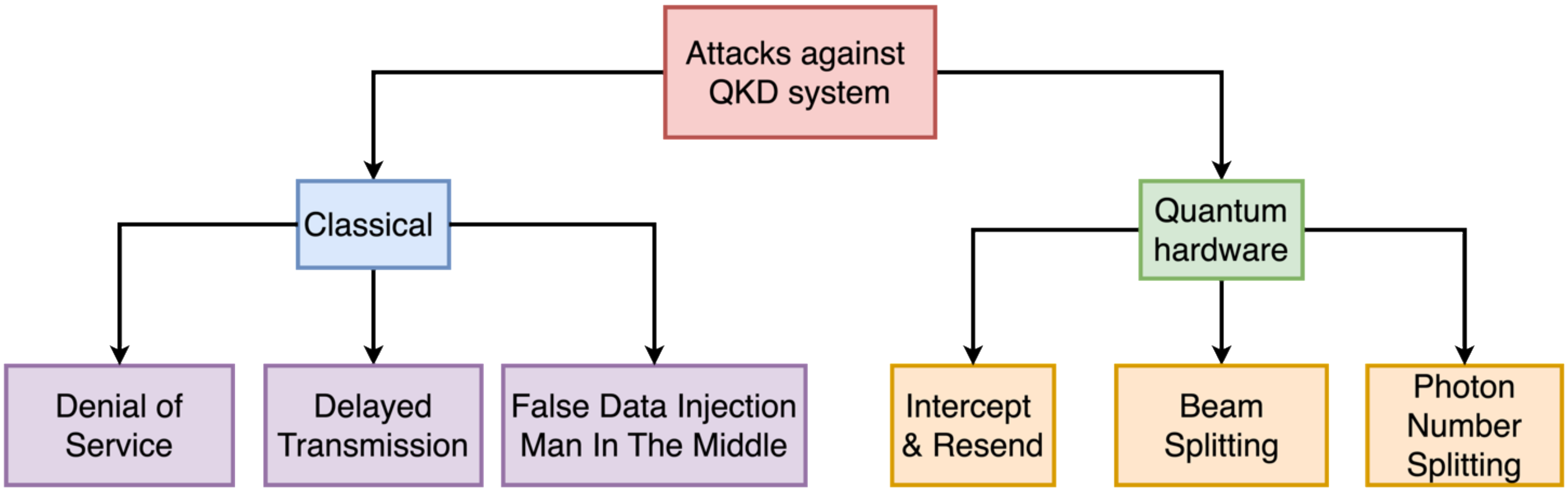
Demo in Prototypic Conditions



https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html#4



Threat Analysis



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.

Quantum ‘keys’ secure nuclear reactor communications

Purdue College of Engineering · Following
Published in Purdue Engineering Review · 5 min read · Sep 13, 2022

9

The nuclear industry is embarking on a transformation that will result in a more reliable and efficient new generation of advanced reactors, the success of which

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 Ben Cipiti at Sandia and Katya Le Blanc at INL for fruitful discussions and expert input.

Questions?