

Hardware-Aware Bayesian Quantum Architecture Search for NISQ Machine Learning, with Applications to Power-Grid Security

Muhammad Mahad Khaliq | Faculty mentor: Dr. Ali Shiri Sichani

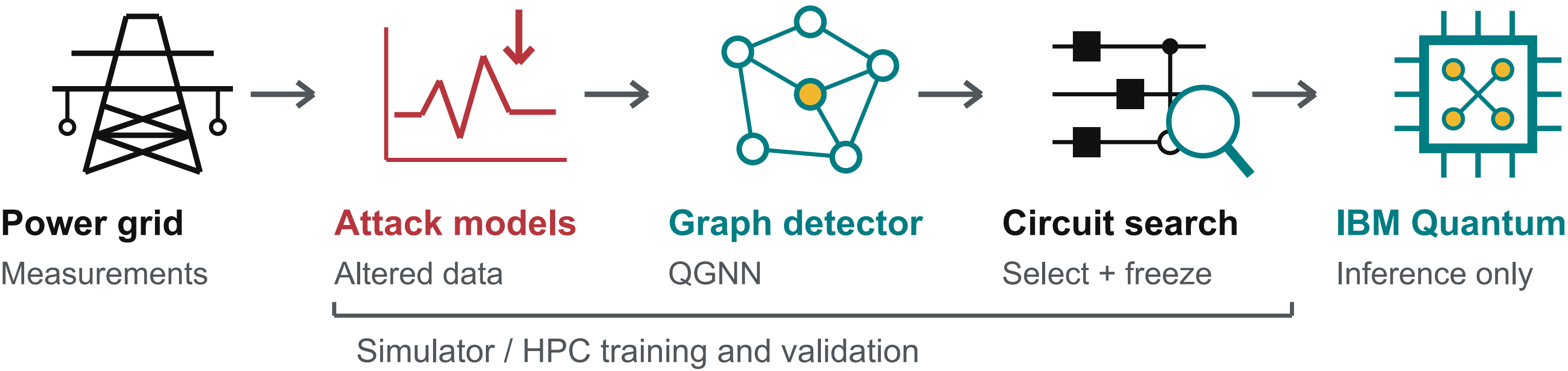
QIC-IBM Quantum Road to Practitioner (R2P) Internship | EECS, University of Missouri, Columbia | Summer 2026

621,000	balanced examples	30 / 57 / 118	IEEE bus systems	3	IBM Quantum backends	2 + 4	accepted papers + active drafts
---------	-------------------	---------------	------------------	---	----------------------	-------	---------------------------------

1 Problem and research approach

Can compact quantum models support power-grid security under realistic physics, data and hardware constraints?

False-data injection (FDIA) alters grid measurements to evade bad-data detection. We study attacks, detectors and their hardware cost.



2 Methods and quantum resources

Q-NPG / RB-QNPG

Quantum Natural Policy Gradient / Robust Belief-Conditioned Q-NPG. The robust variant adds physical beliefs and model-shift handling.

Compact attacker cores

IEEE 30 / 57 / 118: 4 / 6 / 8 qubits and 36 / 72 / 96 trainable quantum parameters.

Complementary methods

Q-PCQPO: Quantum Physics-Constrained Policy Optimization. Q-ASP: Quantum Adversarial Self-Play.

Learning and verification

Policy training used simulators and Hellbender HPC. IBM devices executed frozen circuits; training was not performed end-to-end on QPUs.

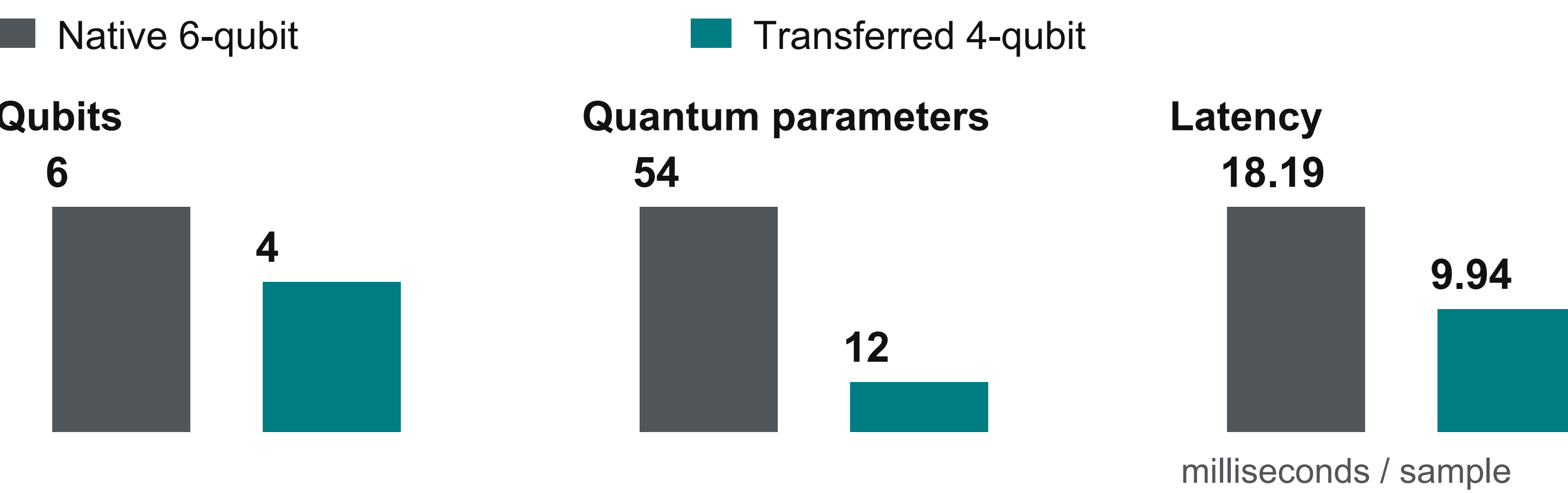
3 Data and reproducibility

501,000 QGrid-Synth examples + 120,000 public-data examples. Common splits, physical evaluators, seed-level records and provenance support controlled comparisons.

4 Bayesian circuit optimization

Search: 4/6 qubits; 1-3 layers; CNOT, CZ or RZZ entanglers; Z or Z+ZZ readout; graph features and data re-uploading.

Four initial designs + six Bayesian proposals. Development seeds 10-12; frozen selection checked on seeds 0-9.



78% fewer parameters | ~45% lower latency

F1: 0.825 +/- 0.061 vs 0.814 +/- 0.053. The predictive difference is unresolved; compactness and measured resource reduction are the supported findings. [3,4]

5 Trustworthy detection

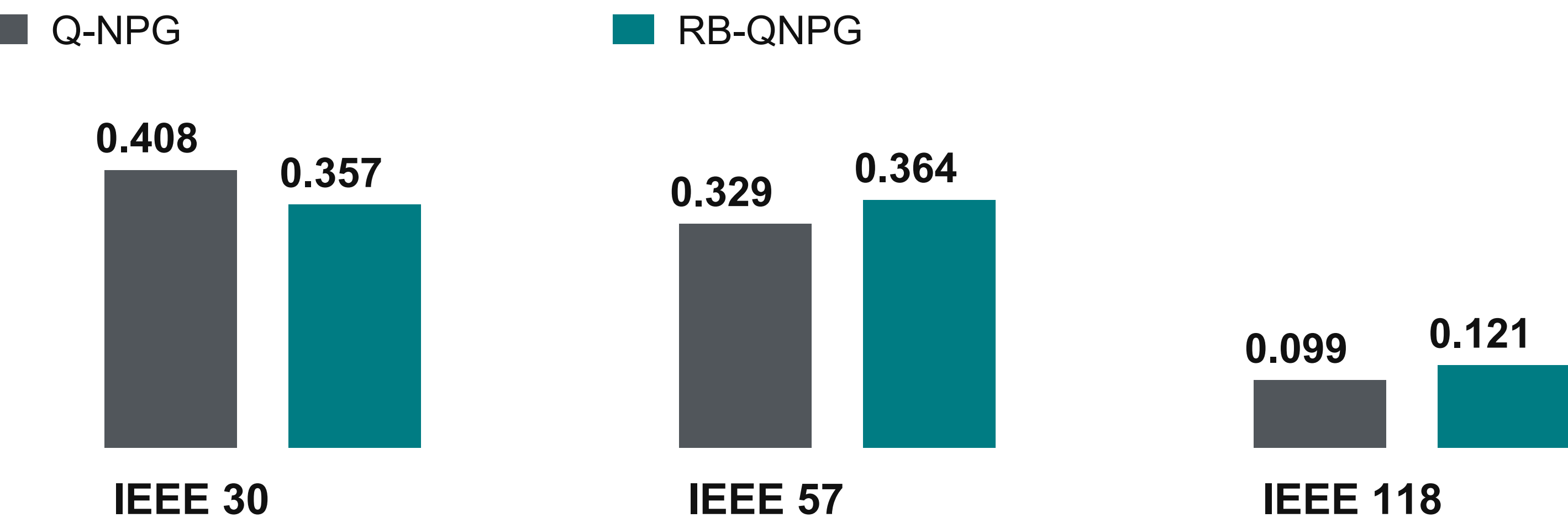
QGNN = Quantum Graph Neural Network. Graph-aware inputs are compressed into a small quantum register. Audits cover calibration, sensor/graph shifts and finite shots.

Full-data classical models retain about 0.15-0.21 higher F1. Under matched 4,000-sample Fourier controls, QGNN gains resolve in 3 of 7 comparisons; 4 remain unresolved after correction. [3]

Resource-aware evidence, not quantum advantage

6 Attack generation and auditing

Historical ten-seed Q-NPG vs RB-QNPG: mean state-deviation score (SDS). Higher is more estimator displacement, not necessarily greater operational harm. [2,4]



Means shown; these are historical nominal-protocol results.

Updated TSG audit: 360 policies, 30 paired seeds per grid. Fixed feasible controls outperform learned arms on the primary impact-stealth endpoint. Longer classical training improves impact; convergence is not established. [5]

Separate idealized-meter audit: 61,440 attacks on IEEE 30/57; zero upper-bound violations; maximum certified efficiency 0.262. Certification does not transfer to the primary sparse-budget protocol. [5,6]

7 IBM Quantum: execution evidence

ibm_miami | Q-NPG

4/6/8 qubits, 1,024 shots; 7 test points. Recorded job elapsed: 24 min 46 s.

ibm_kingston | Q-ASP

4 logical qubits, 1,000 circuits, 1,024 shots. Documented session: 23 min; depth 20 -> 65.

ibm_pittsburgh | QGNN

4 qubits, 4,096 shots, 48 stress inputs. Probability MAE 0.01090; agreement 35/48 (72.9%). Runtime wall 111.7 s; reported quantum time 53 s.

Timing fields differ and must not be summed as QPU time. Stress-selected agreement is not population accuracy.

PUBLICATION PORTFOLIO

[1] NAPS 58 | ACCEPTED, Paper 201

Quantum Machine Learning for Localizing Stealthy False Data Injection Attacks in Power Grids

[4] IEEE / TQE | DRAFT

Robust Belief-Conditioned Quantum and Graph Learning for False Data Injection Attacks in Power Grids

2 accepted papers + 4 active manuscript tracks; umbrella draft not counted again

[2] IEEE QCE / QCRL26 | ACCEPTED, Paper 1594

Offensive Quantum Reinforcement Learning for Stealthy False Data Injection Attack Generation in Power Grids

[5] IEEE TSG | DRAFT

QGrid-Synth: An Impact-Stealth Benchmark for Learned False-Data Injection Against Power-System State Estimation

[3] NeurIPS SaTQuML | MANUSCRIPT

Trustworthy Quantum Graph Detection of False-Data Injection: A Reproducible Cross-Dataset Benchmark

[6] npj / Nature-style | DRAFT

Known-optimum auditing reveals evaluator and representation effects in constrained policies

TEAM Muhammad Mahad Khaliq; Ali Shiri Sichani; Srikar Alla; Varshith Kumar P. Pulluri; Mert Korkali; Hadi Akbarpour; Chi-Ren Shyu

THANKS Mizzou Quantum Innovation Center; IBM Quantum R2P; University of Missouri EECS / College of Engineering; Saint Louis University collaborators; Hellbender HPC.

Next: prepare remaining manuscripts for submission and present the accepted QCRL26 workshop paper in Toronto.

Updated 11 Sep 2026