Escuela Superior Politécnica del Litoral

PARES & NONES
Un break científico

Manuel S. Alvarez-Alvarado
mansalva@espol.edu.ec
FIEC-ESPOL

Quantum Computing for Reliability Assessment of SCADA with Continuous Penetration Testing and High Penetration of Cyber-Physical Attacks

PROBLEM IDENTIFICATION

Recent studies have demonstrated the effectiveness of Quantum Computing (QC) for accelerating reliability assessments in traditional power systems. However, applying QC to SCADA-regulated systems introduces unique complexities that remain unexplored in the literature. To bridge the gap, it is proposed a novel approach to evaluate the impact of Continuous Penetration Testing (CPT) on power system reliability, particularly in SCADA-regulated generation systems using QC.

GENERAL OBJECTIVE

To develop and validate a quantum-enhanced methodology for assessing the impact of CPT on the reliability of SCADA-regulated power generation systems (see **Figure 1**), aiming to improve the accuracy and computational efficiency of cyber-physical risk evaluation compared to classical approaches.

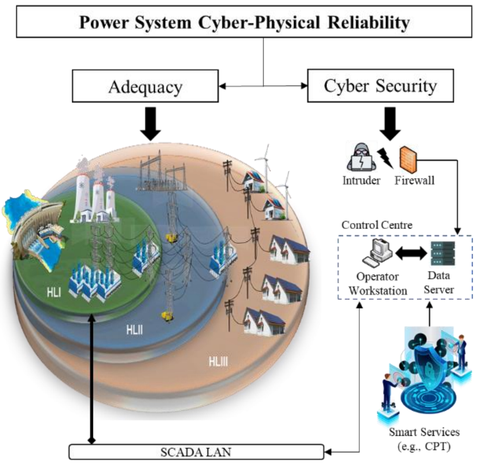

Figure 1
Research scope

PROPOSED APPROACH

- A mathematical framework to capture the attack and defense rates of the cyber-physical system, modeled through a continuous-time Markov chain with time-varying hazard rates, which enables dynamic and cyber-aware reliability assessment (see **Figure 2**).
- The proposed approach incorporates an advanced algorithm based on QC to determine the reliability indices of the power system, specifically through the application of Quantum Amplitude Estimation.

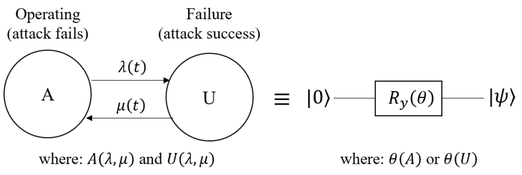

Figure 2
Equivalent Reliability Model in QC

RESULTS

- In **Figure 3 (a)**, it can be observed that when CPT services are employed, the unavailability remains significantly lower compared to scenarios without CPT. This reduction in U directly translates to a smaller angle θ, as shown in **Figure 3 (b)**, reflecting a more stable and resilient system state. This fact leads to an increment in system reliability, which can be measurable through the reliability indices (see **Table 1**).
- To validate the results and show the efficacy of the proposed approach, Monte Carlo (MC), Latin Hypercube (LH) and QC with 4.5 million experiments (or shots for the case of QC) are tested through reliability assessment with CPT for SCADA. The metrics to measure the computational efficiency in terms of accuracy, precision, convergence, and time simulation.
- The normalized results are illustrated in **Figure 4**, providing a clear and comparative visualization of the effectiveness of each employed technique.

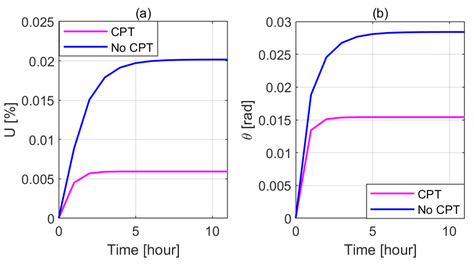

Figure 3
SCADA Reliability model (a) classical input; (b) QC input

Table 1 Reliability Indices

Index	PCAS [%]	ETTA [hr/yr]	ENCA [attack/yr]	EENP [MWh/yr]
No CPT	0.27	371	24.0	164
CPT	0.08	1191	7.00	52.6

PCAS: Probability of Cyber-Physical Attack Success
ETTA: Expected Time to Attack
ENCA: Expected Number of Cyber-Attacks
EENP: Expected Energy Not Provided

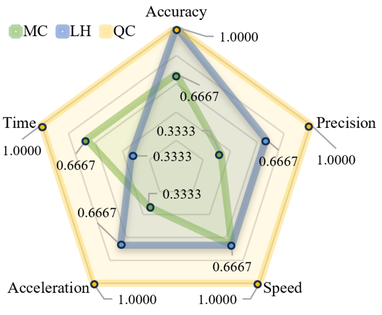

Figure 4
Sampling techniques overall performance

CONCLUSIONS

- The results reveal that with the incorporation of CPT, the system's vulnerability to successful cyber-physical attacks is significantly reduced, as indicated by the lower PCAS and decreased ENCA.
- The proposed QC-based algorithm enhances computational efficiency, achieving higher accuracy, precision, and faster convergence compared to classical MC and LH methods.

ACKNOWLEDGEMENT

- This study was financially supported by the Decanato de Investigación from the Escuela Superior Politécnica del Litoral (ESPOL).

PUBLISHED PAPER

- This research was submitted on the IEEE transactions on Smart Grids. For more details concerning the research do not hesitate to write to the email mansalva@espol.edu.ec