

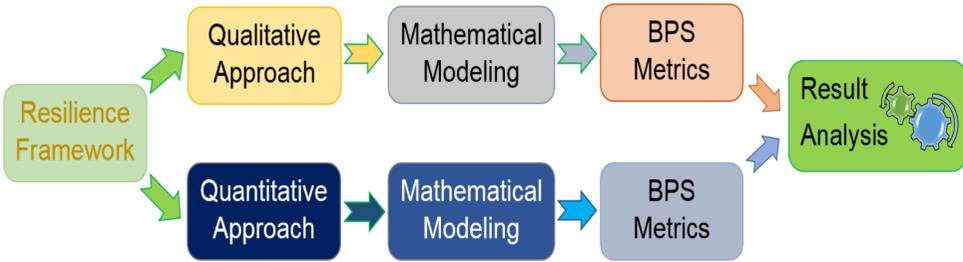
RESEARCH MOTIVATION

- Availability of Bulk Power Systems (BPS) **cyber resilience metrics** will support **risk management** and mitigation decisions
- Provide **quantitative insights** to ensure operational resilience and assist in development of cost-effective mitigation plan
- Motivate BPS operators to continually assess their resilience capabilities and **benchmark** their **performance**

RESEARCH VISION

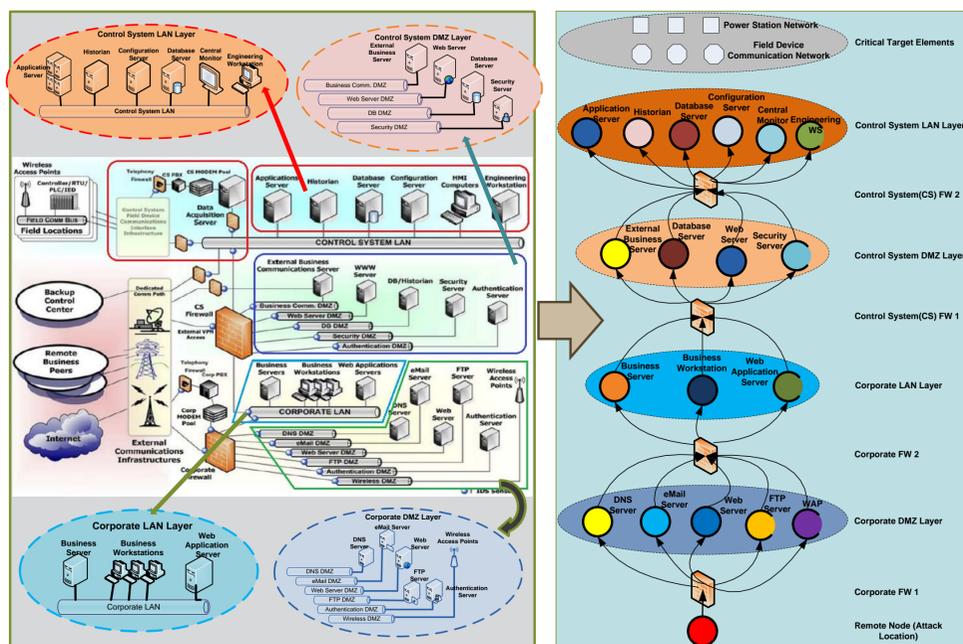
We aim to develop quantifiable cyber **resilience metrics** for BPS vulnerable to cyber attacks

RESEARCH ROADMAP



- Development of **mathematical models** to derive cyber resilience metrics such as **robustness**, **redundancy**, **rapidity**, and **resourcefulness** properties of the BPS network considering the interconnected substations and control centers in presence of cyber threats
- Development of a **qualitative tool** to provide users with a **qualitative approach** to assess the **security posture** of cyber systems and networks in the bulk power systems
- Development of a **quantitative tool** to provide **quantitative cyber resilience assessment** for the **utility companies** based on network/hardware/software configurations

BPS NETWORK MODELING USING NIST ARCHITECTURE



QUALITATIVE TOOL PRELIMINARY RESULTS



Table: Resilience Score

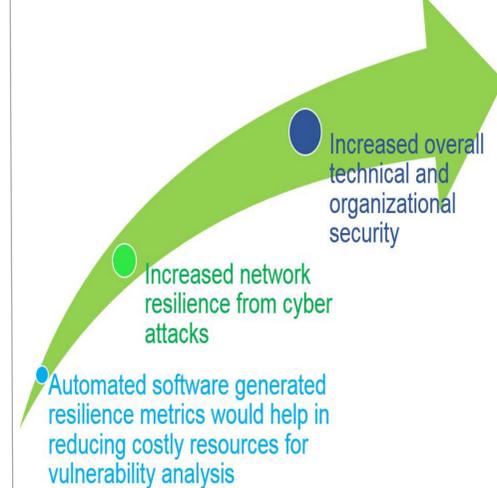
Dimension/Criteria	Robustness	Redundancy	Resourcefulness	Rapidity
Physical	4.2	4.1	3.9	4.4
Organizational	3.5	3.3	3.5	3.7
Technical	4.5	3.5	2.9	4
All Dimension Average	4.1	3.6	3.4	4
Resilience	3.8			

RESEARCH IMPACT ON BPS SECURITY

BPS System Security Impact



Organizational Impact



COLLABORATION OPPORTUNITIES

Seeking collaborative opportunities from industry partners:

- Evaluation of qualitative tool
 - Reference architectures to aid in development of quantitative tool
- ✓ Contact: sshetty@odu.edu
- ✓ Activity webpage: <https://cred-c.org/researchactivity/cyber-resilience-metrics-bulk-power-systems>