Cyber Resilience Metrics for Bulk Power Systems

Sachin Shetty, Gael Kamdem De Teyou, Bheshaj Krishnappa and David Nicol

RESEARCH GOALS

- Need to understand and quantify the cyber resilience of bulk power system (BPS)
- Quantify graceful degradation for bulk power system in presence of cyber threats
- Availability of resilience metrics will support risk management decision making in bulk power system sectors.
- Facilitate operators to prioritize corrective actions.
- Motivate operators to continually assess their response to risks to cyber threats.

RESEARCH CHALLENGES

- Resilience of a system depends critically on defining acceptable system performance
- Space of possible changes across systems large due to the large number of system states, operating conditions and attack paths
- Existing models for power grid structural resilience focus on graceful degradation due to local and cascading failures which are caused due to physical faults or natural disasters
- Model complex BPS layers corresponding to security domains characterized with different security policies and protocols.
- Define metrics which take into account both impact and exploitability of attack

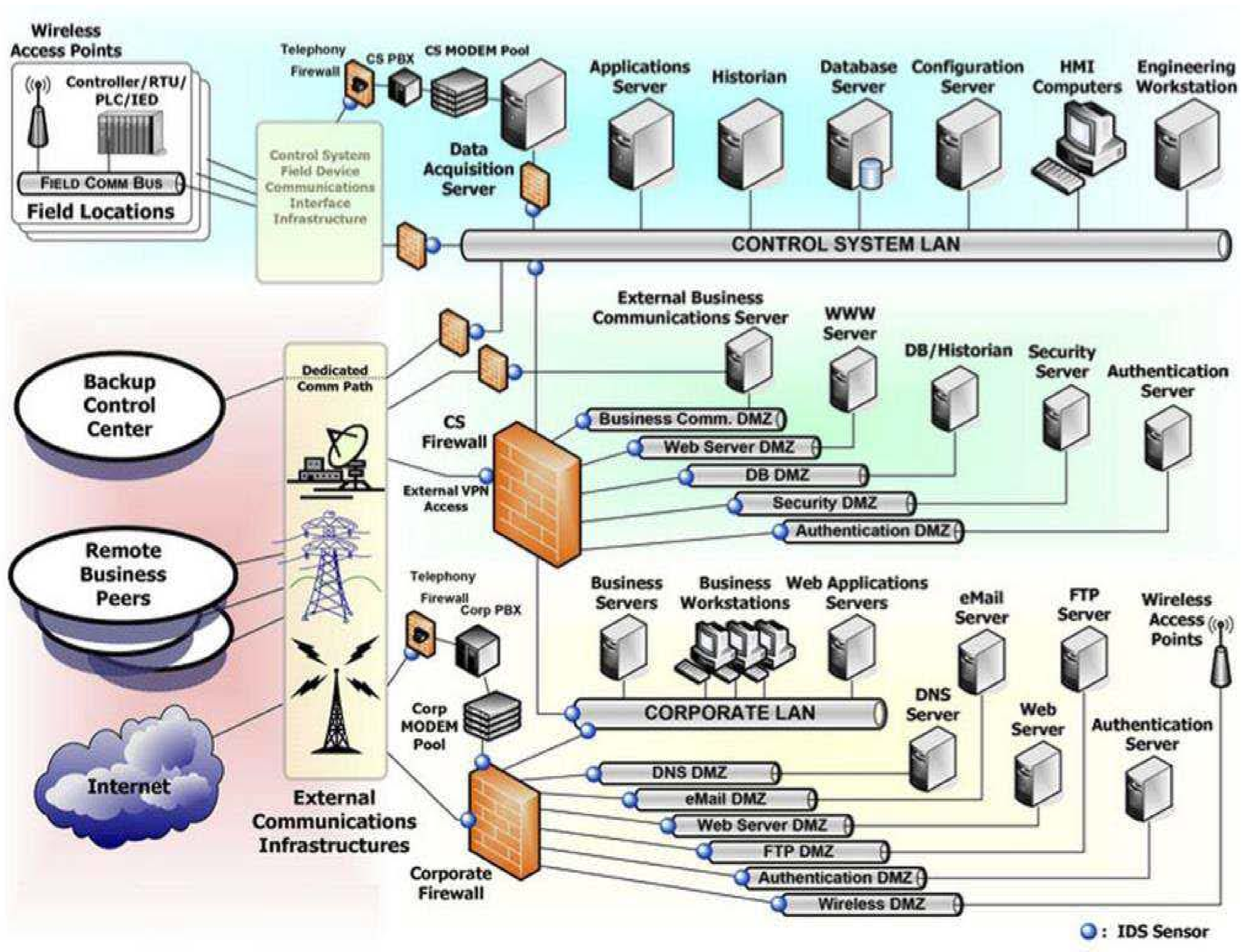
CREDC/INDUSTRY RESEARCH PARTNERSHIP

- Collaborative project between Old Dominion University and Reliability First (RF) to develop cyber resilience metrics for BPS
- RF is a Federal Energy Regulatory Commission (Commission)-approved Regional Entity responsible for ensuring the reliability of the North American Bulk-Power System within the Eastern Interconnection.
- Derive metrics to evaluate cyber resilience of BPS operators
- Advance RF's mission of promoting grid reliability and resiliency.
- Provide industry relevance for CREDC research collaborating with RF to leverage industry expertise

RESEARCH PLAN

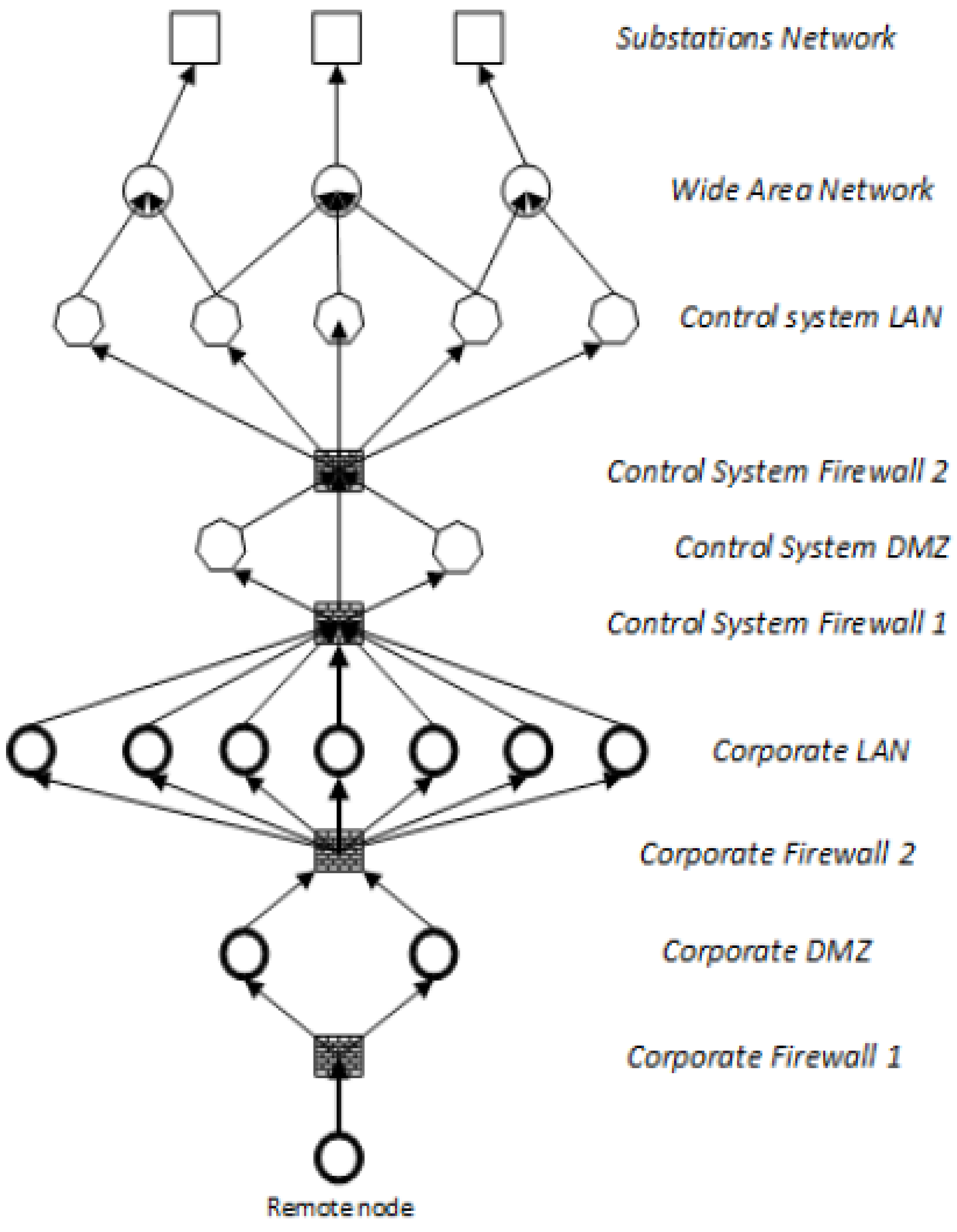
- Develop analytical models for robustness, redundancy, rapidity and resourcefulness properties for networks interconnecting sub stations and control center.
- Formulate the analytic models as multi-level directed acyclic graphs and interdependent coupled networks.
- Identify the design parameters, such as firewall rules, network paths, node recovery time, backup resources available, etc., which achieve the desired resilience
- Multilevel Directed Acyclic Graph (DAG) incorporating substations, communication, control system and corporate network layers.
- Defining metrics to measure the exploitability and the availability impact of each attack path.
- Analyze resilience as function of vendors and products

NIST ICS SECURITY ARCHITECTURE



CSSP Recommended Defense-in-Depth Architecture

GRAPH MODELING OF BULK POWER SYSTEMS



Bulk power systems cyber infrastructure modeled as a multi-level DAG

TECHNOLOGY TRANSITION PLAN

- Develop tool to measure robustness, redundancy, rapidity and resourcefulness properties of the networks interconnecting substation and control center in presence of cyber threats.
- Tool will provide quantitative cyber resilience metrics for utility companies based on network/hardware/software configurations provided to the tool.
- Development of a tool to provide users with a qualitative approach to assess the security posture of cyber systems and networks in bulk power systems

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY