Metrics and Tools for Measuring Cyber Resiliency of Electric Grids

V. Venkataramanan, Tushar, V. Krishnan, A. Ding, A. Srivastava, A. Hahn, S. Zonouz, and C. Hauser

GOALS

- To develop *metrics for cyber-physical system resiliency* for planning and operation phases that are validated within a cyber physical testbed.
- To provide *tools for resiliency assessment and decision support.*
- To *model transmission, distribution, controllers, cyber attacks* and analyze impact of defensive mechanisms on system resiliency.
- To *measure the resilience at component-level* (e.g. PLCs) considering their control logic source code and at system level.

FUNDAMENTAL QUESTIONS/CHALLENGES

- *Measuring resiliency* is important to activate the best possible defense mechanism by the operator to *maximize operational resiliency.*
- Resiliency metrics are necessary to compare defense mechanisms during planning studies and to improve investment in resilient systems.
- Assessing resiliency of transmission systems is much more complex compared to radial microgrid or distribution systems.
- Validation of such a tool is challenging and requires testbeds to model and simulate transmission and distribution grids, control algorithms, and communication systems, emphasizing device level and system level aspects of resiliency.

RESEARCH PLAN

Our approach is based on the *identification of cyber and physical factors affecting system resilience* and applying a decision making process to integrate all the factors to result in a *single resiliency metric.*

Identify resiliency metrics

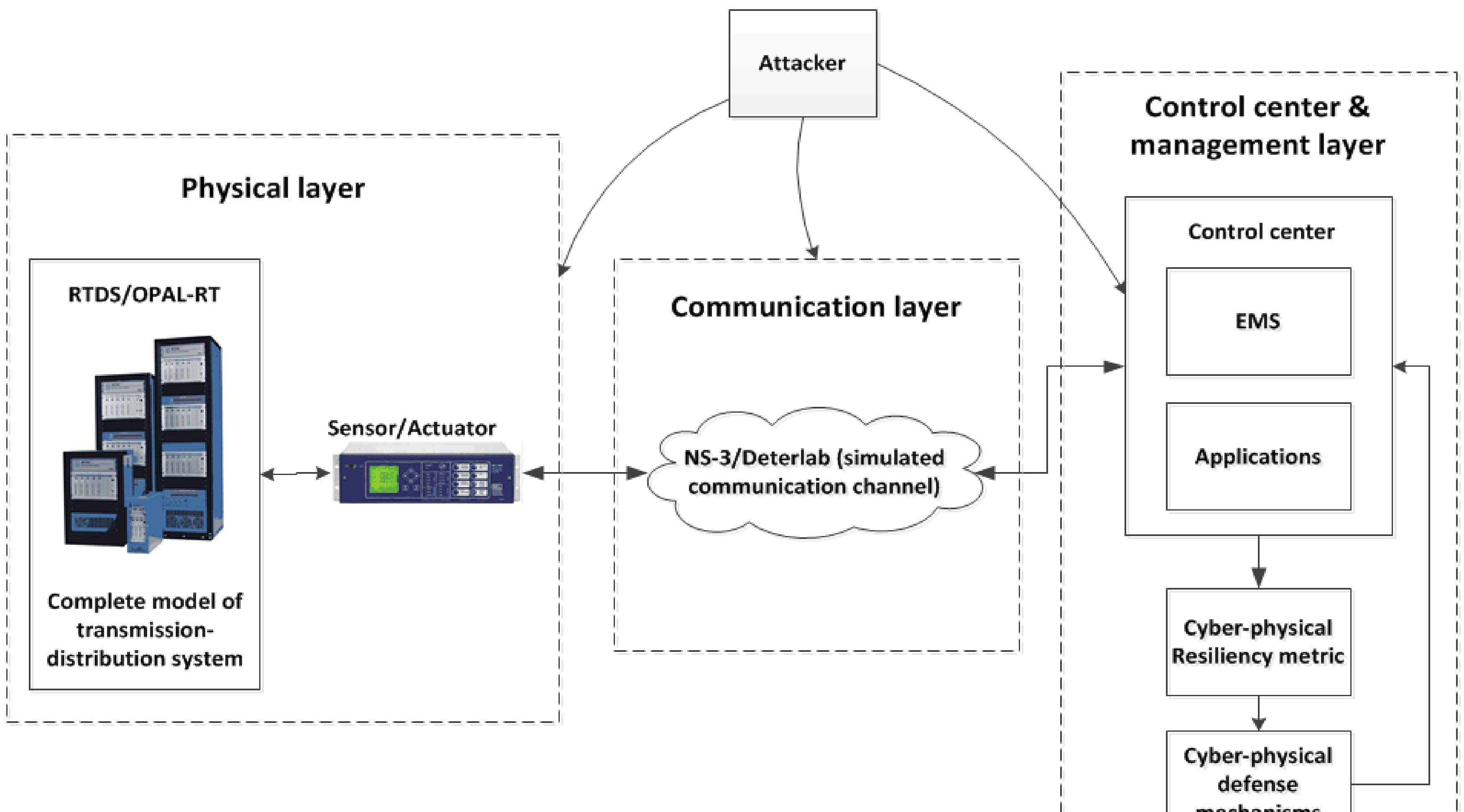
- In developing the metrics we will extend and combine common impact metrics from both the cyber-domain (e.g., Common Vulnerability Scoring System (CVSS), Common Weakness Scoring System (CWSS)) and the power-domain (e.g., topological and system resiliency). We will also develop new metrics for devices (e.g., PLCs).

Develop resiliency analysis tools

- Develop tools to *quantify resiliency improvements* through techniques such as reconfiguration, redundancy, partitioning, non-persistence, special protection schemes, PLC security defense, automated response, intentional islanding, and wide-area load shedding.

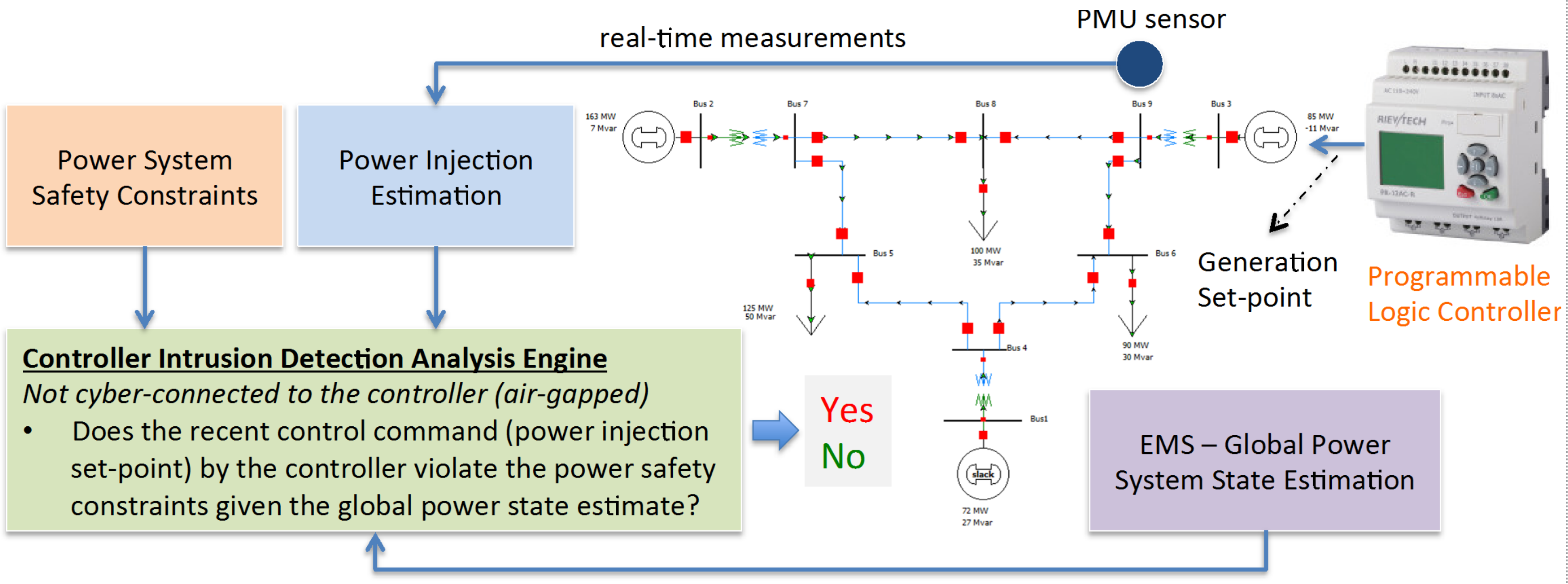
Verification and validation

- Test and validate the developed metrics and tools utilizing the comprehensive cyber-physical test bed consisting of real time simulators, communication network simulators, Energy Management Systems (EMS), PLCs, PMUs, PDCs, and relays.



Attacker
Physical layer
RTDS/OPAL-RT
Complete model of transmission-distribution system
Sensor/Actuator
Communication layer
NS-3/Deterlab (simulated communication channel)
Control center & management layer
Control center
EMS
Applications
Cyber-physical Resiliency metric
Cyber-physical defense mechanisms

Framework for System-Level Resiliency



Controller Intrusion Detection Analysis Engine

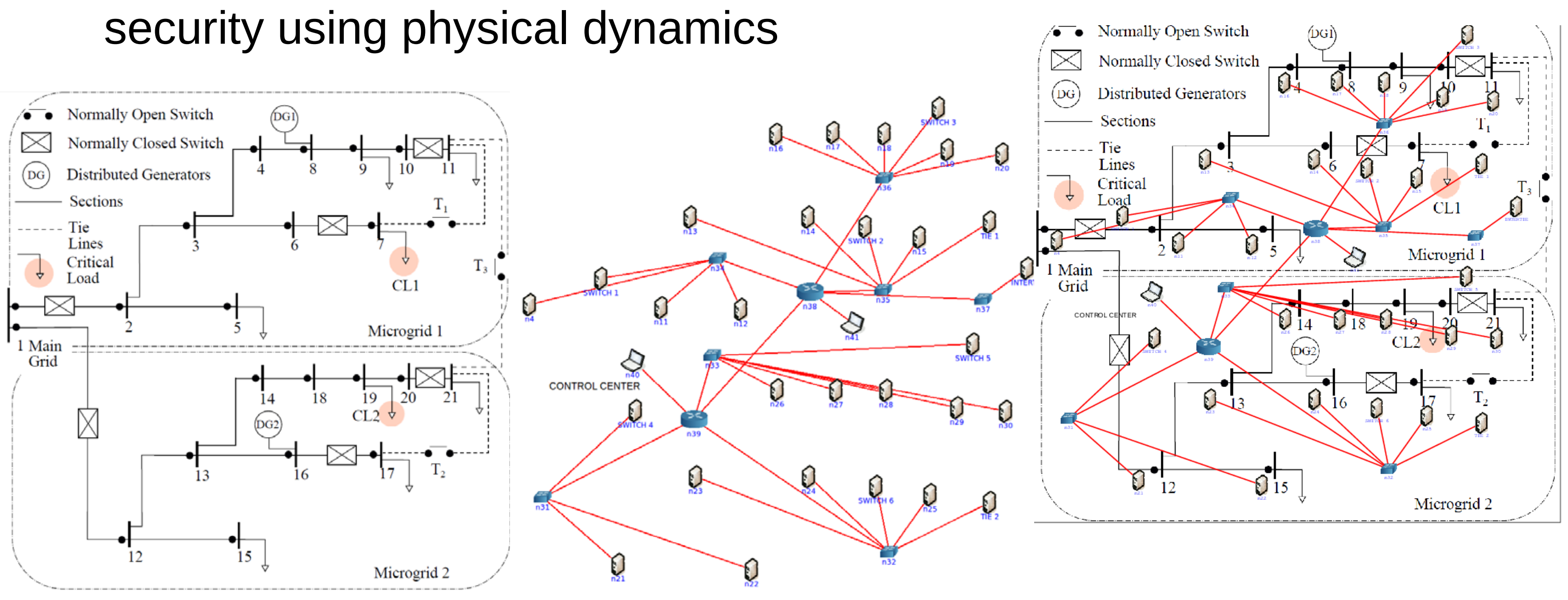
Not cyber-connected to the controller (air-gapped)

- Does the recent control command (power injection set-point) by the controller violate the power safety constraints given the global power state estimate?

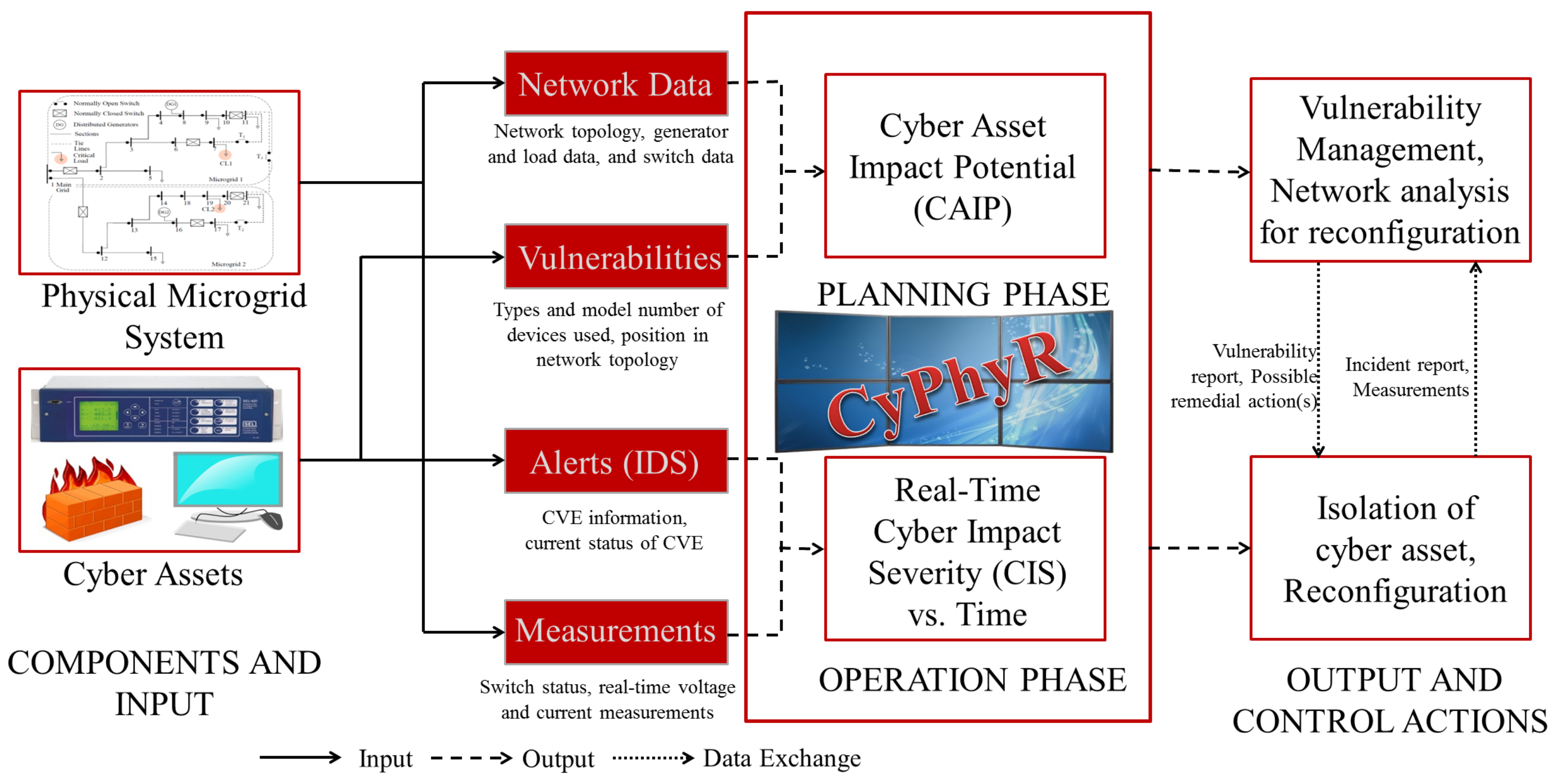
Device-level Resilience using Physical Dynamics

RESEARCH RESULTS

- *Resiliency metrics* have been developed for a small microgrid with a radial topology, which will be extended for distribution systems and transmission systems
- Two metrics are developed – *cyber asset impact potential (CAIP)* for the planning phase, and *cyber impact severity (CIS)* for the operation phase in the real time
- *Developed the CyPhyR* tool to integrate topological aspects from the power system, constraints including power flow, and cyber system vulnerabilities
- *Developed the PLC security assessment toolset* to analyze device security using physical dynamics

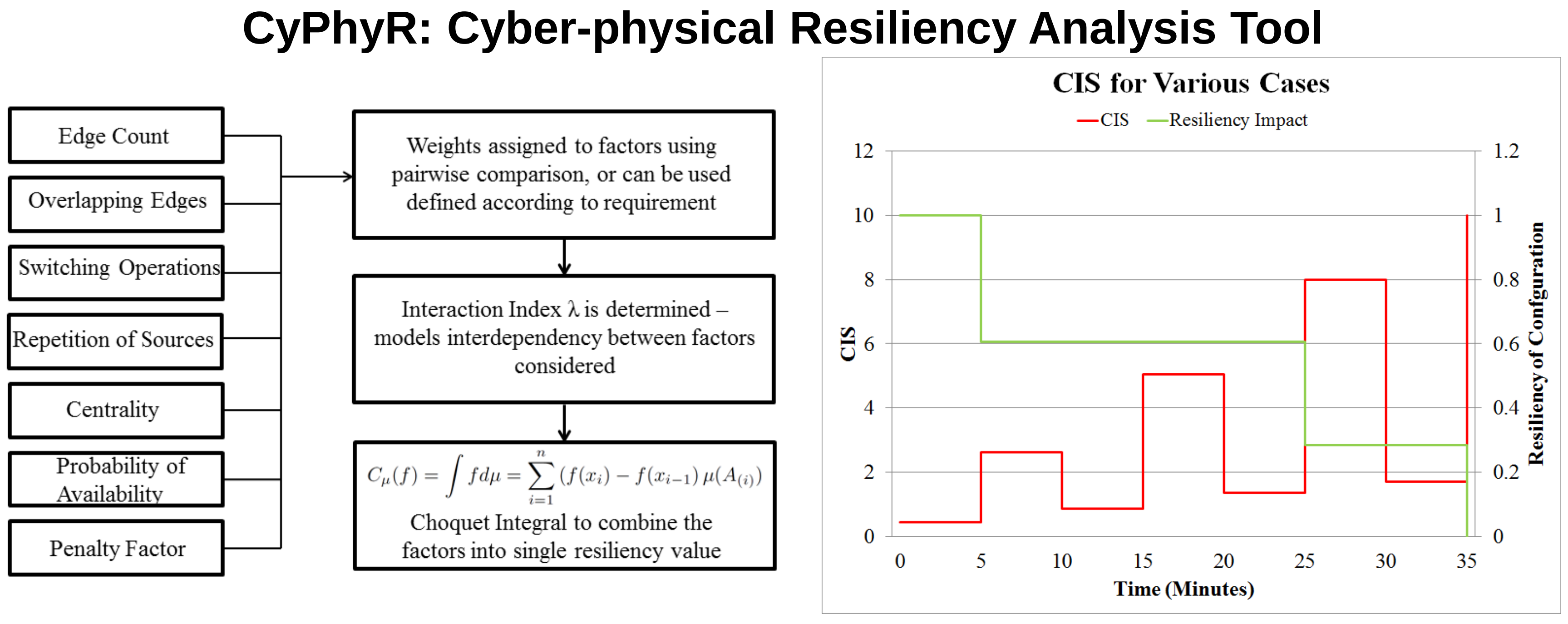


Test System for Microgrid Resiliency



Physical Microgrid System
Cyber Assets
COMPONENTS AND INPUT
Network Data
Network topology, generator and load data, and switch data
Vulnerabilities
Types and model number of devices used, position in network topology
Alerts (IDS)
CVE information, current status of CVE
Measurements
Switch status, real-time voltage and current measurements
Cyber Asset Impact Potential (CAIP)
PLANNING PHASE
CyPhyR
Real-Time Cyber Impact Severity (CIS) vs. Time
OPERATION PHASE
Vulnerability Management, Network analysis for reconfiguration
Vulnerability report, Possible remedial action(s)
Incident report, Measurements
Isolation of cyber asset, Reconfiguration
OUTPUT AND CONTROL ACTIONS
Input
Output
Data Exchange

CyPhyR: Cyber-physical Resiliency Analysis Tool



$$C_\mu(f) = \int f d\mu = \sum_{i=1}^{n} (f(x_i) - f(x_{i-1}) \mu(A_{(i)})$$

Attack Sophistication vs. Resiliency

BROADER IMPACT

- Developed *tools and metrics* that can be used to evaluate impact of cyber vulnerabilities and defense mechanisms for industry partners.
- The *resiliency assessment tool* will enable operators and security admins to obtain the resiliency of their systems in real time and make intelligent decisions to protect/improve the resiliency of their system.
- The *cyber–physical testbed* developed will be used to analyze the effects of cyber attacks and to analyze various defense mechanisms.

INTERACTION WITH OTHER PROJECTS

- We're interested in collaboration with industry and vendors to get feedback on our models, techniques, and tools to determine the real time resiliency of a system.
- We anticipate analyzing the impact of cyber attack defense model developed in other ongoing projects.

FUTURE EFFORTS

- We are working on integrating component level metrics with system-level resilience metrics for microgrid systems.
- We will extend metrics developed from a radial system to a meshed transmission system.
- We will validate developed tools and metrics using cyber physical co-simulation.

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