**EDS OPERATIONAL RESILIENCE**

- Countermeasures deployed to mitigate cyber attacks in EDS may reduce the cyber risk at the cost of degrading operator resilience.
- Need to maintain EDS QoS when countermeasure are applied to an operational EDS.

**RESEARCH VISION**

- Optimal selection of countermeasure which balances the tradeoff between security risk and quality of service.

**RESEARCH APPROACH**

- SDN-based architecture for autonomous attack containment which dynamically modifies access control rules based on configurable trust levels.
- Playbook which keeps a collection of work flow rules that define an OT organization’s strategy to respond to certain cyber security events.
- Cost model to select the countermeasure which balances the tradeoff between security risk and quality of service.

**SYSTEM MODEL**

- Alert → Playbook → Optimization → Apply Security Settings
- Message Authentication Code (MAC) and Key length represent cryptographic parameters that determine security risk and QoS settings.
- MAC and Key Length increase Security Level (SL) and impact packet delay and throughput in SCADA communication network.

**SOME RESULTS FROM OUR WORK**

- Substation automation control and monitoring and alarm/fault processing (operation-critical services) needs strict time constraint ($\leq 100$ ms) along with desired SL.
- Non-power system equipment monitoring and power quality monitoring, customer metering (Non operation-critical service) demands strict throughput ($\geq 97\%$).

**RESEARCH VISION**

- Countermeasures deployed to mitigate cyber attacks in EDS may reduce the cyber risk at the cost of degrading operator resilience.
- Need to maintain EDS QoS when countermeasure are applied to an operational EDS.

**SYSTEM MODEL**

- Alert → Playbook → Optimization → Apply Security Settings
- Message Authentication Code (MAC) and Key length represent cryptographic parameters that determine security risk and QoS settings.
- MAC and Key Length increase Security Level (SL) and impact packet delay and throughput in SCADA communication network.

**SOME RESULTS FROM OUR WORK**

- Substation automation control and monitoring and alarm/fault processing (operation-critical services) needs strict time constraint ($\leq 100$ ms) along with desired SL.
- Non-power system equipment monitoring and power quality monitoring, customer metering (Non operation-critical service) demands strict throughput ($\geq 97\%$).

**IMPACT ON GRID RESILIENCE**

- Business Impact
  - Reduce spread of impact of attacks
  - Ensures security investment by providing countermeasures that balance security risk and quality of service

**COLLABORATION OPPORTUNITIES**

- Seeking collaborative opportunities from industry partners:
  - Scenarios where SDN can play an effective role in automatically changing the network configuration to limit the impact of cyber attack
  - Identifying required operational quality of service.
  - Identifying parameters for determining operational resilience?