

Scenario-Based Simulator for Operational Resilience During a Cyber Attack

Stuart Madnick, Michael Siegel, Keman Huang, Teklemariam Tesfay, Keri Pearlson

RESEARCH VISION

Develop a scenario-based simulator that assists energy delivery system operators during a cyber attack to avert unintended consequences.

EXAMPLE SCENARIO - CRASHOVERRIDE Compromised Attack Schedule Wipe SCADA DDoS attack SCADA Network CRASHOVERRIDE **CRASHOVERRI** devices via on protective through edge Life-cycle opens Breakers DE for execution device service relavs Relays on standby mode Rampant authentication, Lose of visibility and remote process activity, **Blackout Abnormality** control Config changes ... **Indicators** Corrective Worked during Manually operation (In)Actions (Manually close breaker) The **obvious** solution 2015 attack is not always the best Overcurrent --> serious solution. (Un)intended equipment damage, Consequence extended blackout

Ukraine power grid cyberattack - 2016: attackers took additional steps (DDoS) anticipating operators will respond the way they did to a previous attack. Operators' anticipated response had an unintended consequence.



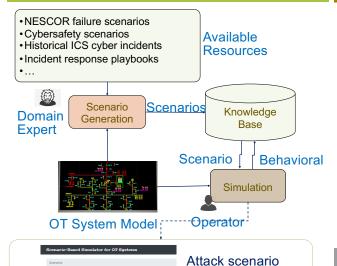
Response

Recomm

endations

strategies 1

SIMULATOR FOR BETTER OPERATIONAL RESPONSE



Our scenario-based simulation enables operators to make informed decisions while dealing with a cyber attack



The Simulator organizes available resources in a format that is customizable and reusable by operators.

COLLABORATION OPPORTUNITIES

Cooperation, support, feedback and involvement from industry partners:

- Attack scenarios, response plans and procedures from industry playbooks to enrich our simulator knowledgebase
- On-site demonstrations and testing of our tool

Contact: msiegel@mit.edu, keman@mit.edu

Potential attack

indicator