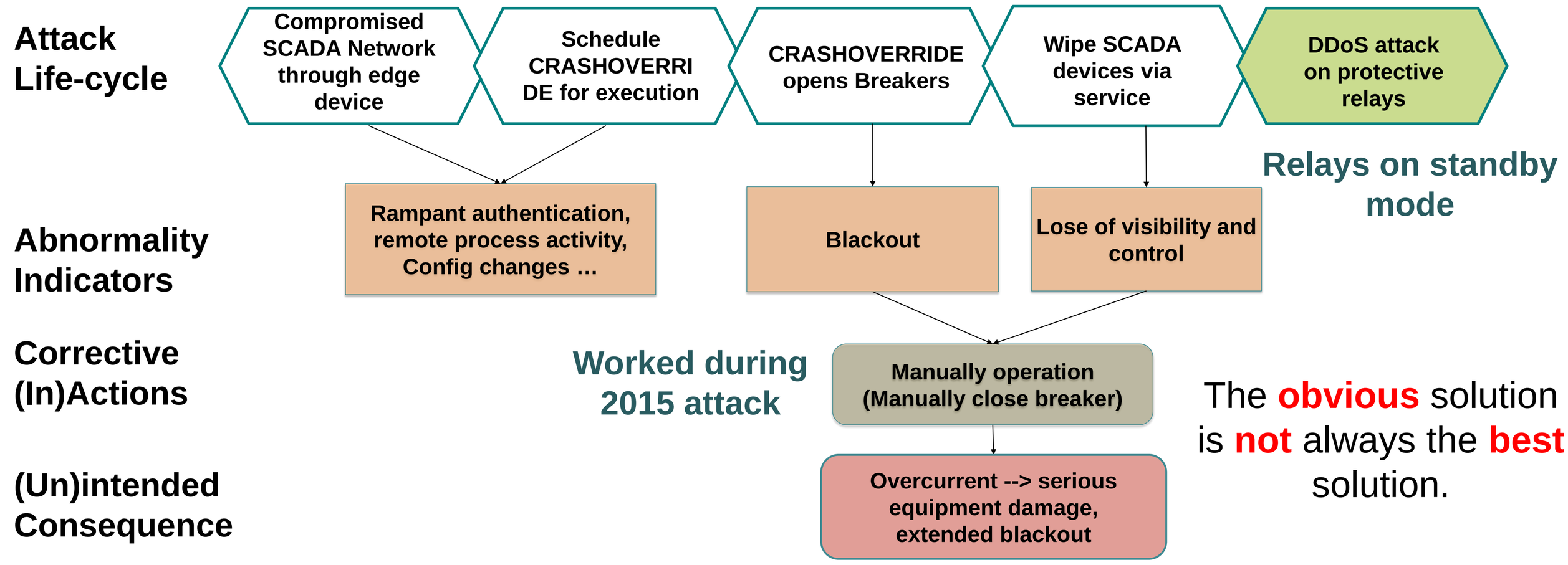
Scenario-Based Simulator for Operational Resilience During a Cyber Attack

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

RESEARCH VISION

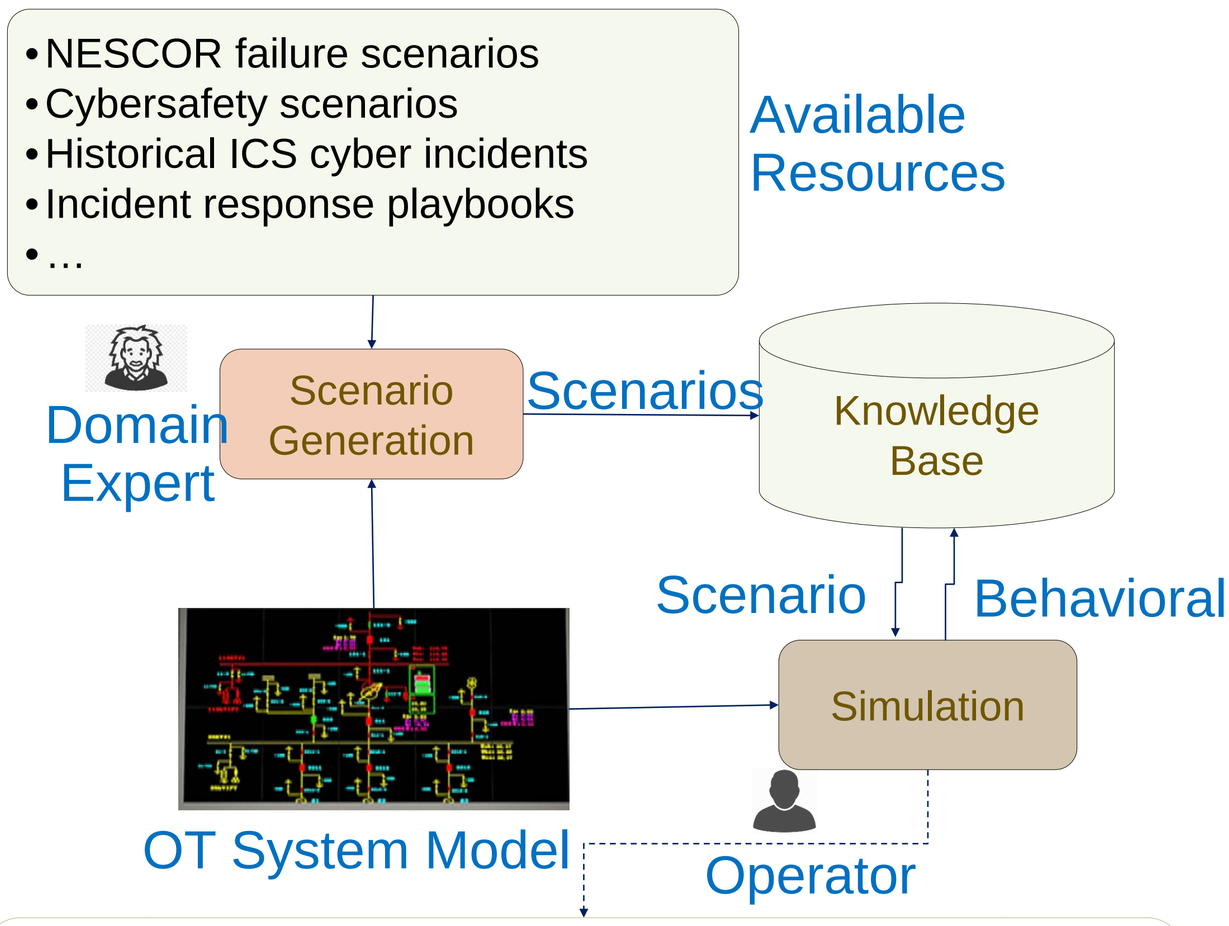
Develop a scenario-based simulator that assists energy delivery system operators during a cyber attack to avert unintended consequences.

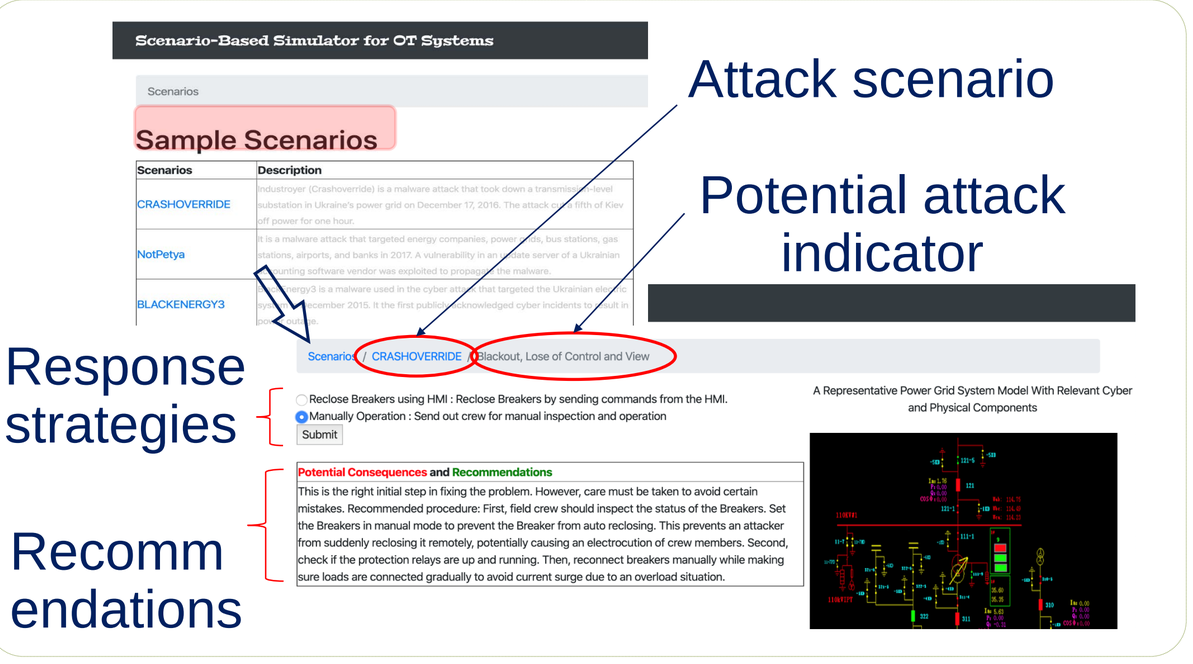
EXAMPLE SCENARIO - CRASHOVERRIDE



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.

SYSTEM ARCHITECTURE





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 Tool demonstrations and testing
- Provide interaction behavior data

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

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