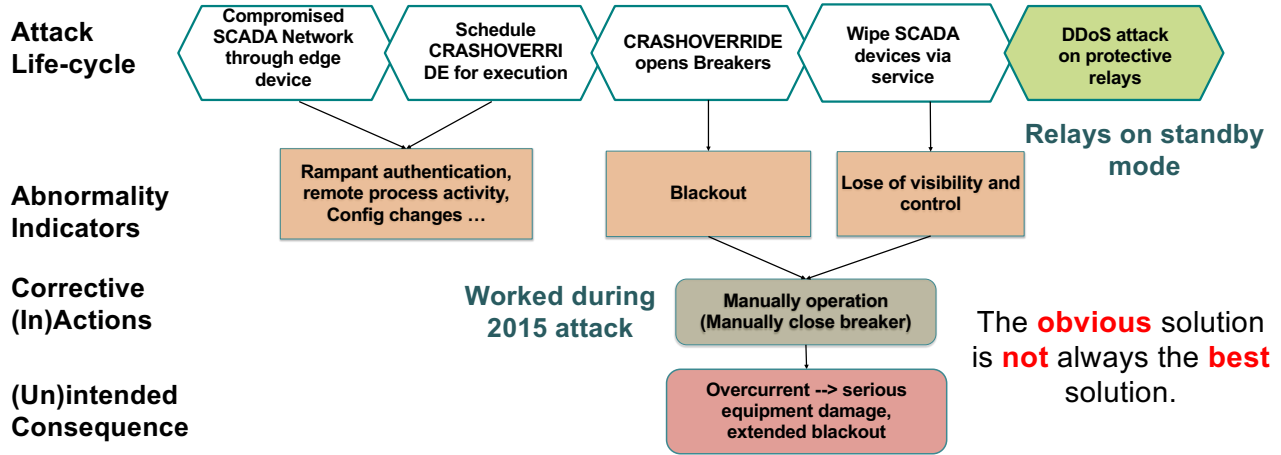


## RESEARCH VISION

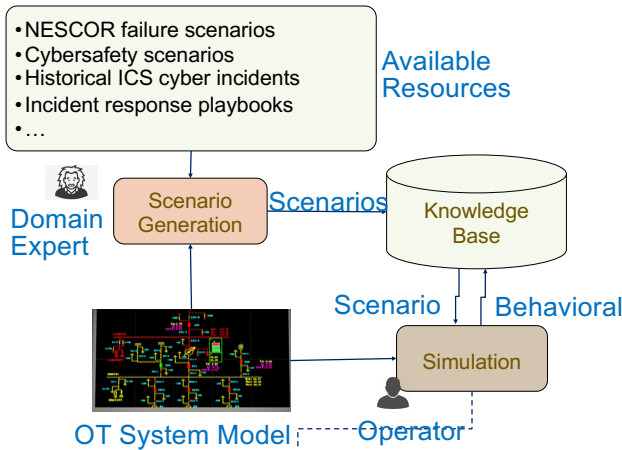
*Develop a scenario-based simulator that assists energy delivery system operators during a cyber attack to avert unintended consequences.*

## 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

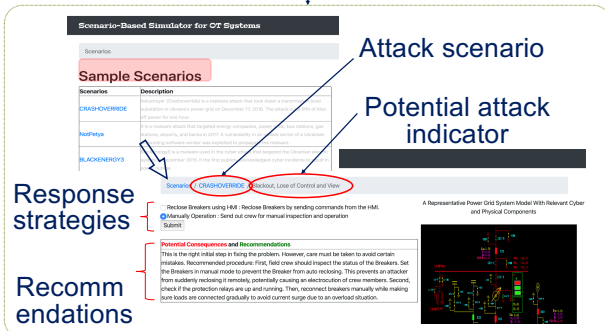


## SIMULATOR FOR BETTER OPERATIONAL RESPONSE

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.



**Attack scenario:** Scenario: CRASHOVERRIDE - Blackout, Loss of Control and View

**Potential attack indicator:** (Highlighted in red in the screenshot)

**Response strategies:** (Listed in the screenshot)

**Recommendations:** (Listed in the screenshot)

## 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](mailto:msiegel@mit.edu), [keman@mit.edu](mailto:keman@mit.edu)