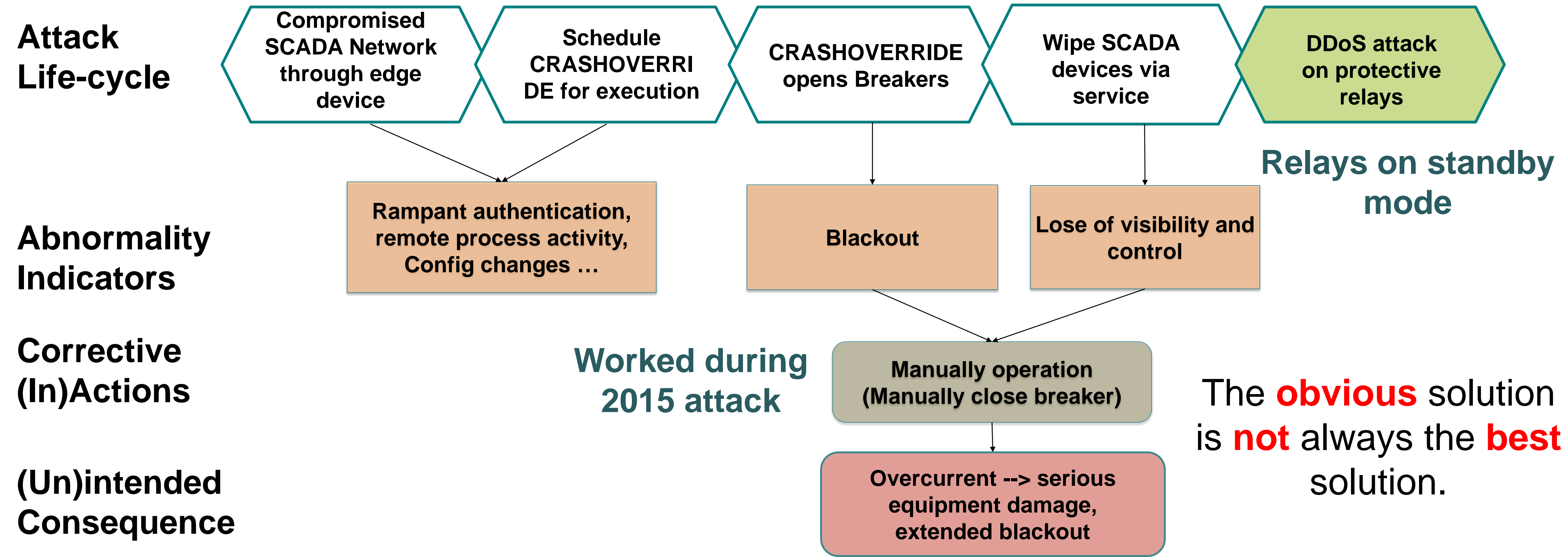


## RESEARCH VISION

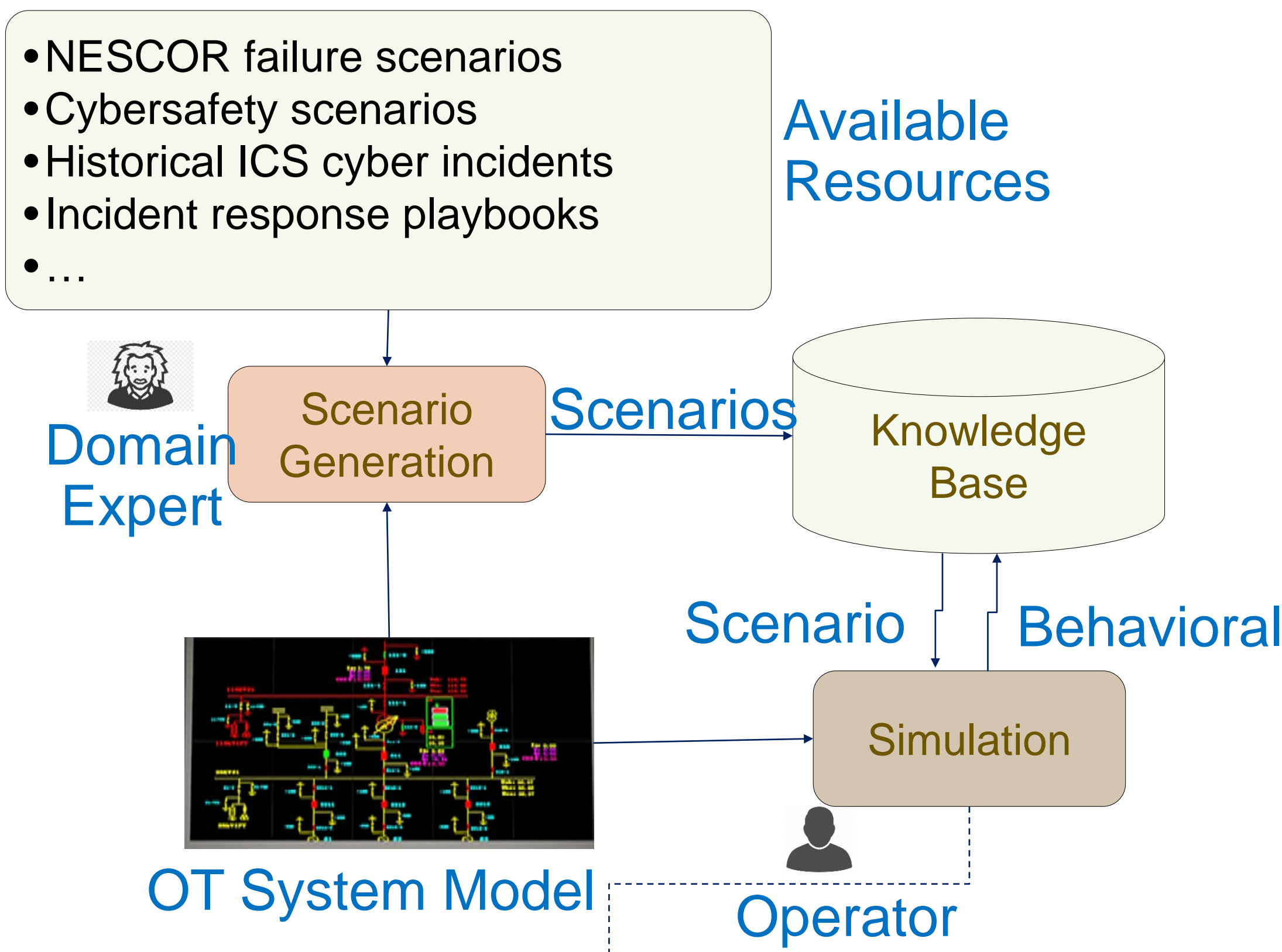
*Develop a scenario-based simulator that assists energy delivery system operators during a cyber attack to avert unintended consequences.*

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

**Attack scenario:** CRASHOVERRIDE

**Potential attack indicator:** Blackout, Loss of Control and View

**Response strategies:** Reclose Breakers using HMI, Manually Operation

**Recommendations:** This is the right initial step in fixing the problem. However, care must be taken to avoid certain mistakes. Recommended procedure: First, field crew should inspect the status of the Breakers. Set the Breakers in manual mode to prevent the Breaker from auto reclosing. This prevents an attacker from suddenly reclosing it remotely, potentially causing an electrocution of crew members. Second, check if the protection relays are up and running. Then, reconnect breakers manually while making sure loads are connected gradually to avoid current surge due to an overload situation.