The objective of this task is to provide tools based on model approximation and relaxation methods in optimization to compute tight bounds on probability of rare events in critical energy infrastructure.

Early detection of risk emergence is key to containing the network structure, the evolution mechanisms, and the decision strategies of the nodes. Techniques from large deviation theory, hidden Markov models, and uncertainty quantification address such an analysis problem for simple models.

Past research has demonstrated that the emergence of fragility in networks occurs in a specific pattern that is due to the topology of the network and the distribution of disturbances.

Analytically, such a computation is extremely hard, as it depends on the network structure, the evolution mechanisms, and the decision strategies of the nodes. Techniques from large deviation theory, hidden Markov models, and uncertainty quantification address such an analysis problem for simple models.

We are interested in expanding such research to represent a wider class of networked systems to embrace cyber-physical systems and, specifically, power systems.

The fundamental analysis question in risk is the computation of the probability that the networked system will enter a forbidden region defined in terms of the states of its nodes. Typically, such an event is a rare event, which presents serious challenges in terms of computation using sampling methods.

Past research has demonstrated that the emergence of fragility in networks occurs in a specific pattern that is due to the topology of the network and the distribution of disturbances.

Analytically, such a computation is extremely hard, as it depends on the network structure, the evolution mechanisms, and the decision strategies of the nodes. Techniques from large deviation theory, hidden Markov models, and uncertainty quantification address such an analysis problem for simple models.

We take a systematic approach for creating computational models that can address the aforementioned challenges.

1. Representation of the different components of a system via finite-state models.
2. Aggregation of the individual finite-state models in a global finite-state model for the entire system.
3. Also incorporating stochastic models for exogenous disturbances, hidden states, and unmodeled dynamics.
5. Distributed computation of risk over finite-state models.
6. Validation with data.

Even with accurate system models, Bayesian inference in a rare observation regime is extremely fragile (sensitive to small noise), and it cannot be used in security applications.

Cyber Layer

Physical Layer

Fig. 2. Cyber-physical system model based on interconnection of finite-state system models.