INCORPORATING PRIORITIZATION IN CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE PROGRAMS

Duane Verner,[1] Kibaek Kim,[2,3] and Frédéric Petit[1,3]

[1] Risk and Infrastructure Science Center (RISC), Global Security Sciences (GSS) Division, Argonne National Laboratory

[2] Mathematics and Computer Science (MCS) Division, Argonne National Laboratory

[3] Computation Institute, University of Chicago

ABSTRACT

Protecting critical infrastructure, especially in a complex urban area or region, should focus on identifying and prioritizing potential failure points that would have the most severe consequences. Such prioritization can inform targeted planning and investment decisions, such as what infrastructure should be hardened or relocated first or what infrastructure should receive priority restoration following a disaster, among other uses. Without a prioritization process, assessment and protection programs are typically guided by intuition or expert judgement, and they often do not consider system-level resilience. While understanding how to prioritize high-consequence failure points for assessments and, ultimately, for protection is essential, the complexity of infrastructure systems can quickly overwhelm. For example, in a notional region with 1,000 electric power assets, almost one million failure scenarios are associated with an N-2 contingency and nearly one billion failure scenarios are associated with an N-3 contingency. As a result, it is simply not feasible both technically and financially for system operators and government agencies to assess and prepare for all possible disruptions. Therefore, a primary goal of critical infrastructure protection and resilience programs should be to identify and prioritize the most critical contingencies affecting infrastructure systems. Achieving this goal will allow decision makers to identify high-impact isolated failures, as well as cascading events, and to prioritize protection investments and restoration planning accordingly. To solve this problem, Argonne National Laboratory developed an optimization framework capable of modeling and prioritizing high-consequence failure points across critical infrastructure systems. The optimization framework can model at the system level or the interdependent "system-of-systems" level and is applicable to any infrastructure.

INTRODUCTION

Argonne National Laboratory (Argonne) has developed an optimization algorithm and modeling framework capable of identifying the highest-consequence failure points within critical infrastructure systems. The optimization algorithm and framework can be applied to any infrastructure at the system level or the interdependent "system-of-systems" level and can be used to model any combination of infrastructure failures. Results from the optimization modeling can be used by analysts to identify priority assets for assessments and to assist infrastructure system owners and operators and government agencies when they are making critical infrastructure protection and mitigation investment decisions.

UNDERSTANDING INFRASTRUCTURE FAILURES

A fundamental component of critical infrastructure security and resilience programs should include understanding how, why, and where systems fail. This understanding should guide decisions on where to conduct in-depth assessments as well as which protection and mitigation measures to pursue. However, a complicating factor is that infrastructure failures vary significantly. Some failures will generate significant consequences at the system or regional level, whereas effects from other failures remain local, while still others have little to no effect on the overall service provided. For illustration purposes, Figure 1 shows a 345-kV electric power transmission system between a generator substation and a remote substation.

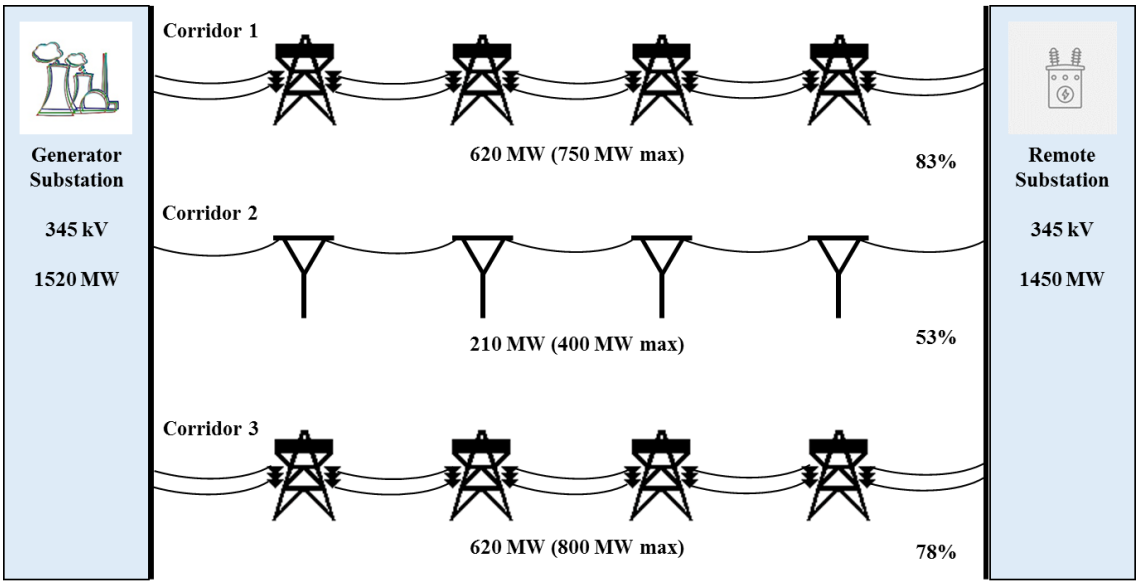

Figure 1 – Electric Transmission Lines[1]

In this example, the generation plant produces 1,520 MW[2] of power that is transported to the remote substation via three transmission corridors. Corridor 1 combines two circuits (lines) that allow transport of a maximum of 750 MW. Corridor 2 is a single circuit that allows transport of a maximum of 400 MW. Corridor 3 combines two circuits that allow transport of a maximum of 800 MW. By design, the three corridors operate below their maximum capacity levels, which allows for the relocation of power among the remaining circuits in the event of a disruption in one of them. For example, if the Corridor 2 circuit fails, the system's overall vulnerability will increase but it will not experience cascading system failure because the two other corridors can compensate for the loss (Figure 2).

[1] The percentages represent the line transfer capabilities.

[2] About 5% of power is lost during transmission because of energy dissipated in the conductors and the equipment used for transmission. Thus, from a starting generation capability of 1,520 MW, a maximum of about 1,450 MW of power arrives at the substation. For the purpose of illustration, the example assumes that electric power is divided equally among the transmission circuits that remain operable.

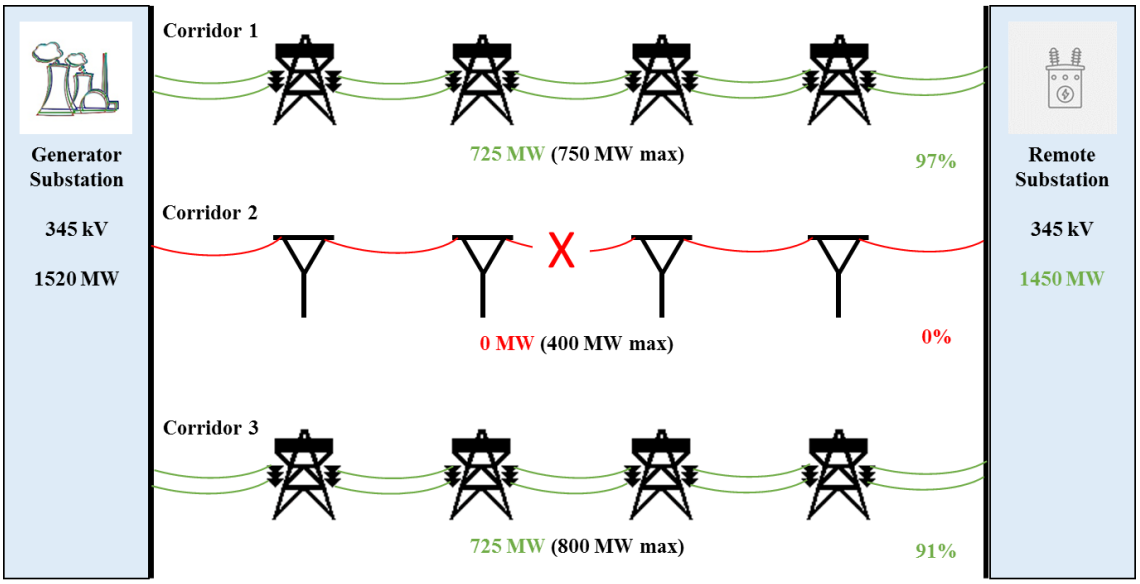

Figure 2 – Loss of Corridor 2 Circuit

Corridor 1 circuits would operate at 97% of their capability and Corridor 3 circuits would operate at 91% of their capability. Similarly, the loss of one circuit from Corridor 1 would not trigger a cascading system failure because of the ability of the remaining circuits to compensate (Figure 3).

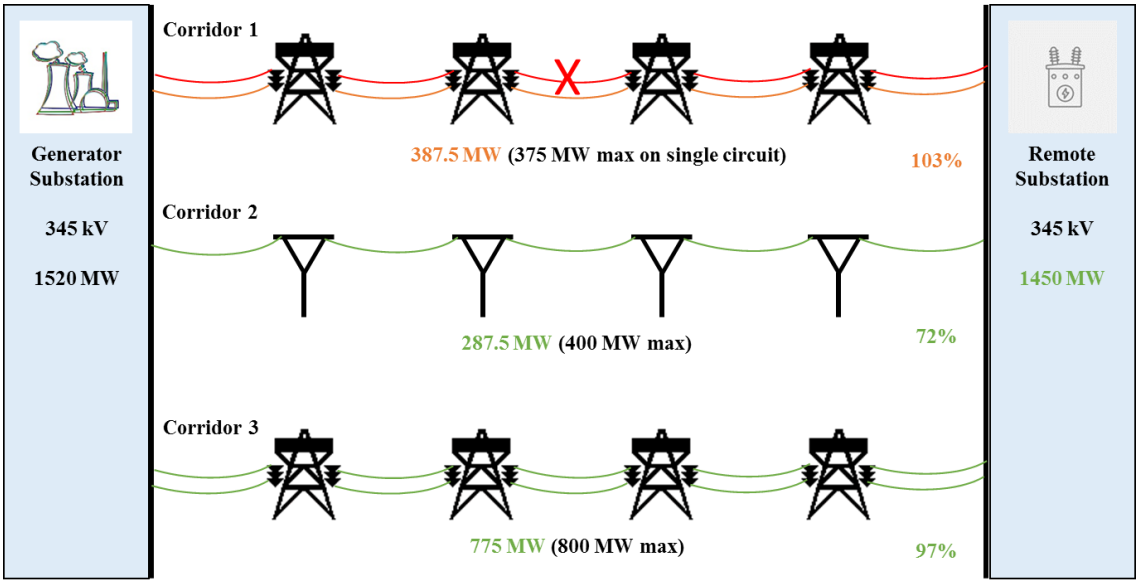

Figure 3 - Loss of One Circuit in Corridor 1[3]

Building on the operating conditions identified in Figure 3, Corridor 3 would operate near full capacity (97%); Corridor 2 would operate at 72%; and the remaining circuit of Corridor 1 would

[3] For the purposes of illustration, the example assumes that electric power is divided equally among the transmission circuits that remain operable. In a real case, it would be expected that Corridor 2 would operate at higher capacity to compensate.

operate at 103%, which, over time, could lead to the loss of the second circuit and therefore a failure of Corridor 1 (Figure 4).

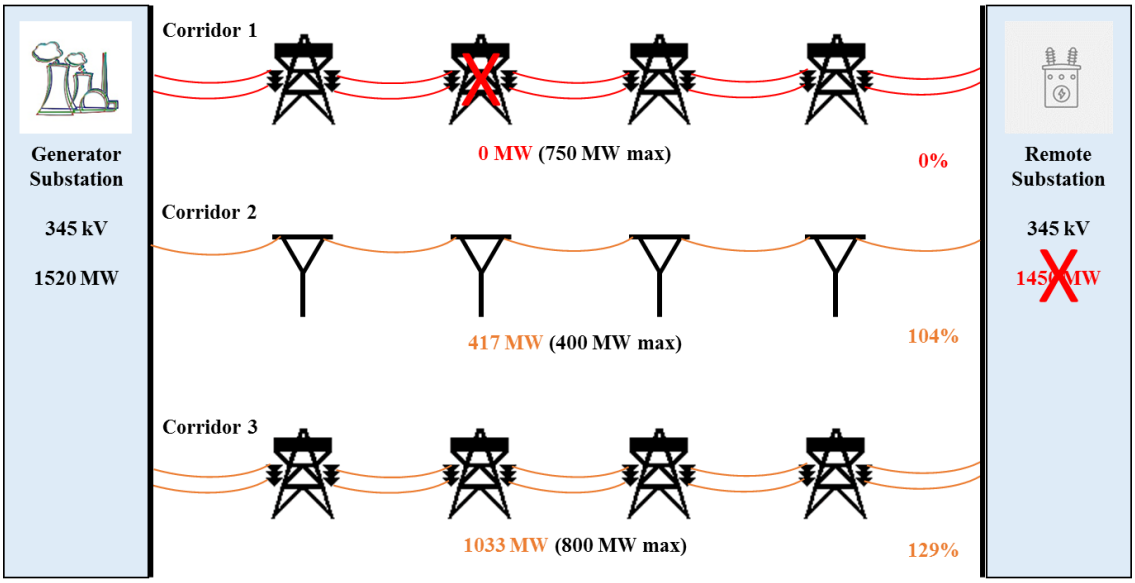

Figure 4 - Loss of Two Circuits in Corridor 1

A loss of Corridor 1 would impede the ability of the two other corridors to operate safely. Corridor 2's circuit would operate at 104% of its capability, and Corridor 3's circuits would operate at 129% of their capability. Under this scenario, the circuits could begin to heat and ultimately trip, triggering a system failure. Assuming all other risk factors are equal, this simplified example shows that the consequence of disruption of Corridor 1 is greater than disruption of Corridor 2, and, as such, Corridor 1 should receive priority when making security and risk management decisions.

Infrastructure fails in many different ways with varying consequences. This N-1 contingency test shows that this system can sustain the disruption of Corridor 2. However, in our example, the loss of one circuit in Corridor 1 would generate an overuse of the remaining circuit in the corridor and could lead to additional consequences. The N-1 contingency can be mitigated by shedding some of the load to bring the transfer capability in Corridor 1 BACK TO 100%, which could avoid problems leading to the N-2 contingency case. The N-2 contingency test, resulting in the total loss of the two circuits in Corridor 1, would cascade to the two other corridors and lead to an overall system failure.

While this section focused on electric power, there are many similar nuances associated with failures in other infrastructure. For example, within the telecommunications sector, loss of a cellular tower does not necessarily mean that your phone will lose service, the closing of a road does not always mean that you can't get to your destination, and so on. In other words, infrastructure system failures are not all created equal.

THE NEED FOR PRIORITIZATION

Without a prioritization process, infrastructure assessment, protection and mitigation programs are typically guided by intuition or expert judgement, and they often do not consider system-level

reliability, redundancy, and overall resilience. While understanding how to prioritize high-consequence failure points for assessments and, ultimately, for protection is essential, the complexity of infrastructure systems can quickly overwhelm decision-makers. For example, in a region with 1,000 electric power assets, almost one million failure scenarios are associated with an N-2 contingency, and nearly one billion failure scenarios are associated with an N-3 contingency (Figure 1Figure 5). As a result, system operators and government agencies find it simply technically and financially prohibitive to assess and prepare for all possible disruptions.

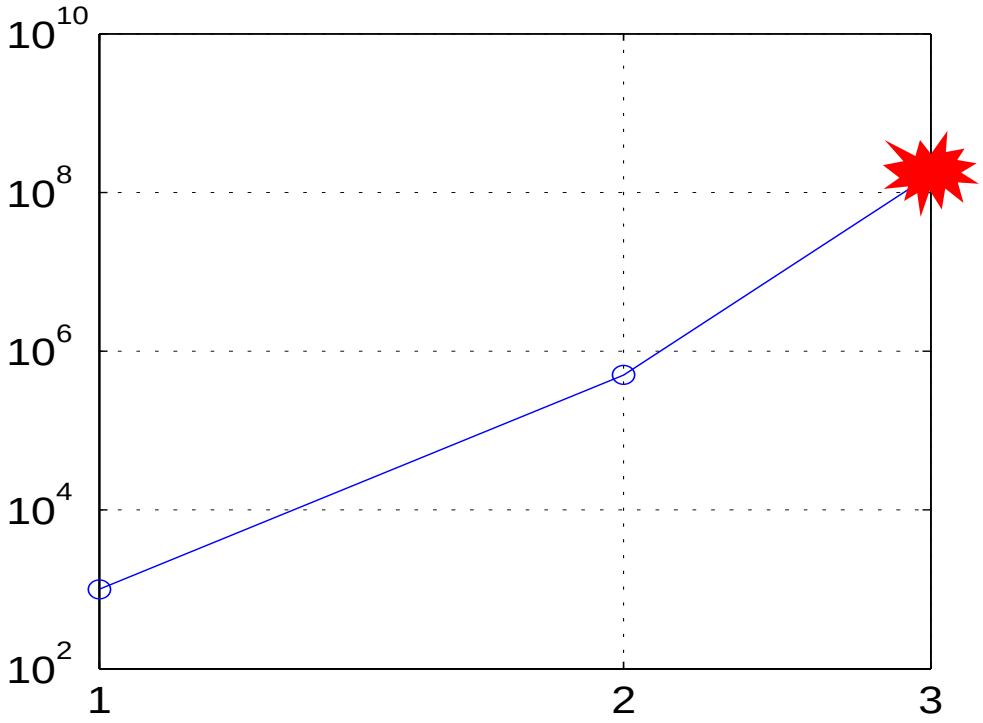

Figure 5 – Possible Failure Scenarios with an N-3 Contingency for 1,000 Electric Power Assets

Therefore, a primary goal of critical infrastructure protection and resilience programs should be to identify and prioritize critical contingencies affecting infrastructure systems. Achieving this goal will allow decision makers to identify high-impact isolated infrastructure failures, as well as cascading events, and to prioritize protection investments and resilience planning accordingly. Such an approach should also consider infrastructure interdependencies.

CONSIDERING INFRASTRUCTURE INTERDEPENDENCIES

Interdependencies among critical infrastructure assets increase risk to individual assets and the overall system. These interconnected infrastructure components constitute a “system of systems” where the failure of one or multiple infrastructure elements can cascade and affect the resilience of the entire system and ultimately the region. Figure 6 illustrates interdependencies among seven different infrastructure sectors and subsectors.

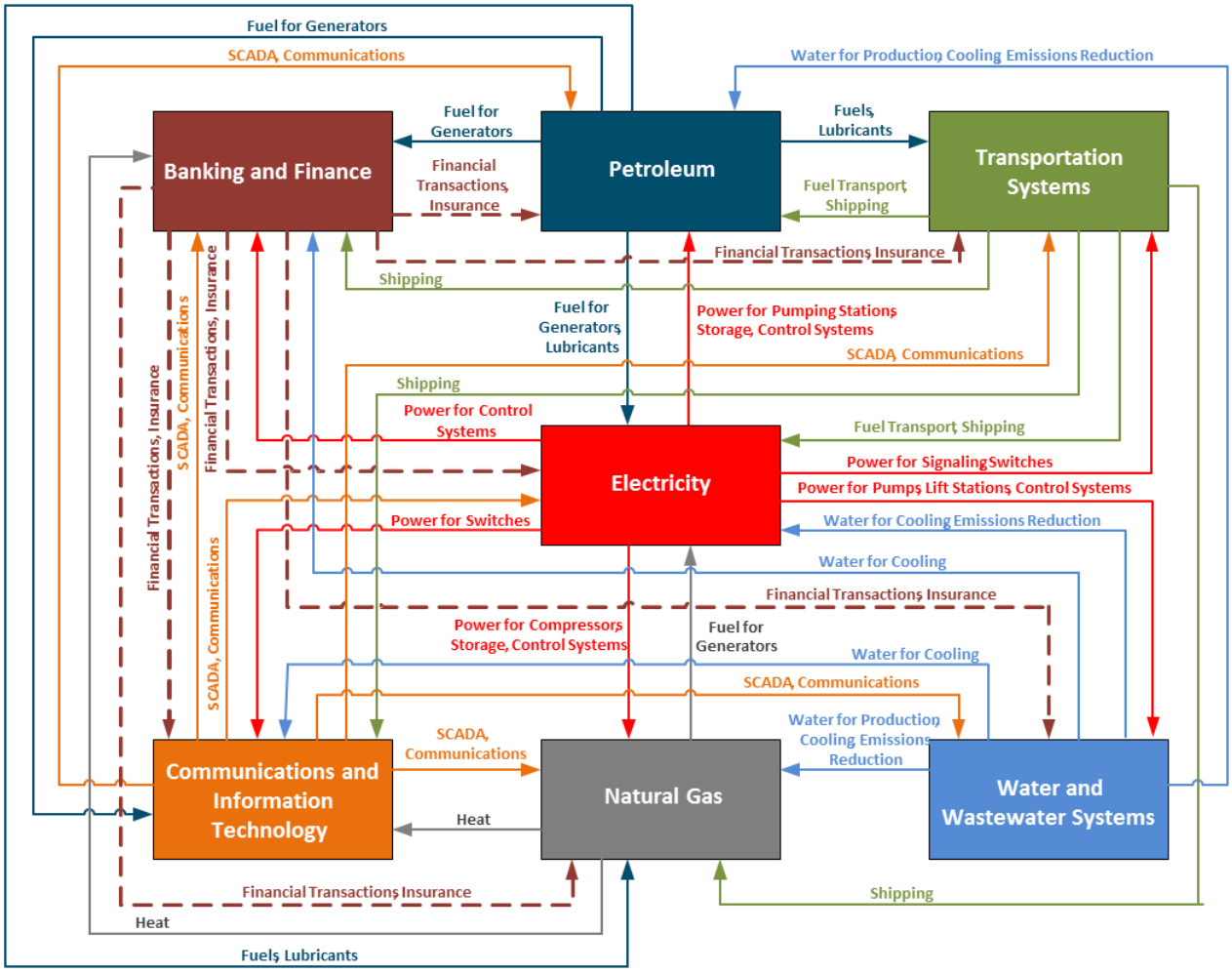

Figure 6 – Critical Infrastructure Interdependencies[4]

However, as highlighted in the earlier electricity example, simply identifying connections between infrastructure does not provide a sufficient understanding of why or whether a connection is critical to the operational integrity of the system. The following case study of electric power and natural gas interdependencies in Florida further illustrates this point. Because Florida is a terminal State, this case study represents one of the simplest examples of interactions between electric power and natural gas because there is no complex downstream system to consider that could further propagate the disruption. Furthermore, the natural gas system is relatively simple with only two major high-pressure transmission pipelines serving the State (i.e., Florida Gas Transmission Co, and Gulfstream Natural Gas System). Figure 7 shows the results of the cascading failure simulation between natural gas and electric distribution systems in Florida.

[4] Adapted from Phillips, J., M. Finster, J. Pillon, F. Petit, and J. Trail, 2016, *State Energy Resilience Framework*, Argonne National Laboratory, Global Security Sciences Division, ANL/GSS-16/4, Argonne, Ill, USA, available at https://www.energy.gov/sites/prod/files/2017/01/f34/State%20Energy%20Resilience%20Framework.pdf, accessed February 14, 2017.

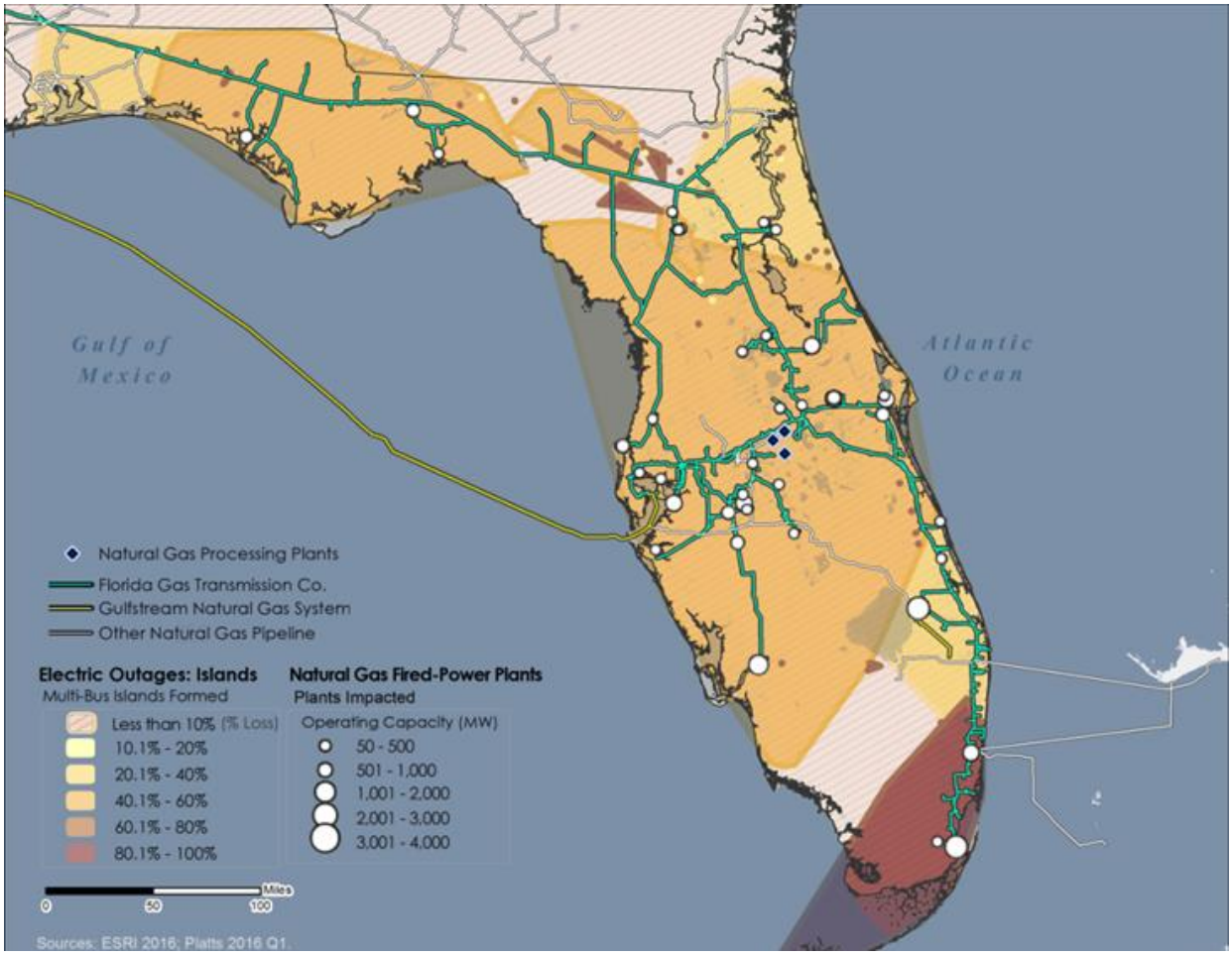

Figure 7 – Cascading Failure Simulation in Florida

The scenario postulates the occurrence of a guillotine (i.e., complete) break on a major interstate transmission pipeline supplying natural gas to the State, resulting in a 100% reduction in the flow of gas through the pipeline. The pipeline break also disrupts fuel delivery to a large number of gas-fired power plants in the State. These power plants would cease operation, leading to a statewide electricity outage with varying load curtailment intensity ranging from 10% to 100%.[5]

In addition, the scenario assumed that Florida has three small natural gas processing plants located in an area that would experience a 40% percent load curtailment, requiring them to curtail operations temporarily. However, because the combined output from these facilities is small relative to the total load, the associated gas curtailment would have no notable impact on gas customers in Florida.[6]

As discussed in the previous section, infrastructure failures are not all created equal. When interdependencies are involved, a failure in one infrastructure can cascade to other systems

[5] Portante, E., B. Craig, J. Kavicky, L. Talaber, and S. Folga, 2016, "Modeling Electric Power and Natural Gas Systems Interdependencies," *The CIP Report*, Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, Washington, D.C., USA, May–June, available at http://cip.gmu.edu/2016/06/03/modeling-electric-power-natural-gas-systems-interdependencies/, accessed February 14, 2017.

[6] Ibid.

increasing the overall consequences. Therefore, considering interdependencies should be an integral part of critical infrastructure security and resilience programs.

APPLYING AN OPTIMIZATION ALGORITHM TO PRIORITIZE INFRASTRUCTURE

Managing risk associated with infrastructure interdependencies requires an understanding of infrastructure failures and, especially in complex urban environments, an ability to prioritize protection and mitigation efforts. Argonne has developed an optimization algorithm for selection and prioritization of infrastructure that runs at the system-level or the interdependent "system of systems-level". The algorithm can apply to the assessment of any infrastructure system.

The optimization algorithm assumes that the physical behavior of a system (e.g., a power network, gas pipeline, or coupled system) is described by the following optimization problem:

$$F(d) \coloneqq min_{u \in U(d)} f(u)$$

where:

- d is the 0-1 vector representing the failures at infrastructure assets,
- u is the control(s) that can be manipulated to mitigate disturbances, and
- $f(u)$ is a system output metric of interest such as cost, delivered load, or deviations from a target operation.

This problem can be solved by the generalized Benders decomposition method proposed by Salmeron *et al.* (2009).[7] This method solves the master problem $max_{d \in D} F(d)$ by iteratively approximating the function $F(d)$ with a set of linear inequalities. Set D contains a set of failure scenarios denoted by d. An element of the set D is denoted by $d = (d_1, d_2, \dots, d_n)$, where an element d_i of the vector is either 0 or 1 for $i = 1, \dots, n$ to create a combination of the asset states. For example, $d = (0,0,1,0)$ can model an event in which, out of $n = 4$ assets, the third asset is disrupted whereas the other assets are not.

The dependence of the control set $U(d)$ on d captures the fact that the control actions available to counteract the disruption might be affected by the disruption d. The control set implicitly captures the network topology and physical laws of an infrastructure system.

Worst-case contingency analysis aims to find a contingency d that causes the maximum damage to the system. The worst-case event (denoted by $d^{(1)}$) can be found by solving the optimization problem:

$$d^{(1)} = argmax_{d \in D} min_{u \in U(d)} f(u)$$

The second most damaging event (denoted by $d^{(2)}$) can be identified by restricting the event set as $D \backslash \{d^{(1)}\}$ and by solving the problem $d^{(2)} = argmax_{d \in D \backslash \{d^{(1)}\}} min_{u \in U(d)} f(u)$. This procedure can be applied recursively to identify the k-th most damaging disturbance. This step is performed by restricting the disturbance set as $D \backslash \{d^{(1)}, d^{(2)}, \dots, d^{(k-1)}\}$. Our optimization algorithm systematically restricts the disturbance set by iteratively adding the linear inequalities to the worst-

[7] Salmeron, J., K. Wood, and R. Baldick, 2009, "Worst-case interdiction analysis of large-scale electric power grids," IEEE Transactions on Power Systems 24.1: 96–104.

case interdiction problem. This approach significantly saves the computational times, as compared with an exhaustive search.

The algorithmic steps are then summarized for identifying the K most damaging disturbances as follows:

1. Create the initial set of disturbances D and the control set $U(d)$ that is dependent on disturbance $d \in D$. Set $k = 1$.
2. Solve the worst-case interdiction problem to find $d^{(k)} = argmax_{d \in D} min_{u \in U(d)} f(u)$.
3. If $k = K$, then **STOP**.
4. Update the disturbance set in order to exclude the k-th most damaging disturbance $d^{(k)}$.
5. Update $k = k + 1$, and go to step 2.

In step 2 of this algorithm, updating the disturbance set D (step 4) is also equivalent to adding a linear constraint to the Benders master problem. The optimization algorithm has been implemented in Julia script language, and CPLEX is used to solve the master and subproblems in the generalized Benders decomposition.

Argonne has applied this optimization algorithm to a test system of the California Independent System Operator (CAISO) interconnected with the Western Electricity Coordinating Council (WECC). The test system is obtained from Kim *et al.* (2017).[8] This test system consists of 225 buses, 375 transmission lines, 135 generation units, and 40 loads.[9] The algorithm ran to detect the 100 most critical substations in the system. The criticality of substations is measured based on the amount of load lost resulting from the event that a substation is disabled. In this computational test, the objective function f(u) is defined as the amount of load lost. The control set U(d) is defined by a set of constraints for the security-constrained economic dispatch problem as in Kim et al. (2017).[10] Note, however, that our algorithmic approach is generic to have a user-defined objective function and additional constraints (e.g., generation cost, repair time of the failure components). Figure 8 shows the results based on the test system.

[8] Kim, Kibaek, et al. "Data Centers as Dispatchable Loads to Harness Stranded Power." *IEEE Transactions on Sustainable Energy* 8.1 (2017): 208-218.
[9] Ibid.
[10] Ibid.

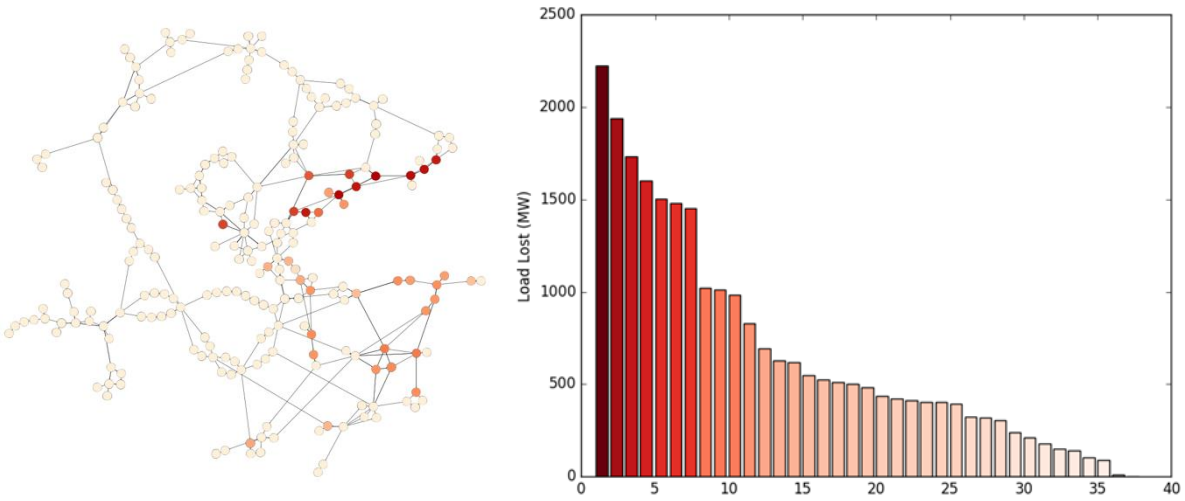

Figure 8 – Result of the Optimization Algorithm for the Test System of CAISO Interconnected with the WECC

In this example, a total of 36 substations resulted in significant load loss and failures; the other substations did not cause any load loss. The optimization algorithm terminated after the detection of zero-load substation failure. Government analysts and infrastructure owners and operators can use this type of information to protect the highest consequence failure points within infrastructure systems.

CONCLUSION

Protecting critical infrastructure, especially in complex urban areas, should focus on identifying and prioritizing potential failure points that would have the most severe consequences. Applying a technique like this optimization algorithm can inform this prioritization process. For example, the algorithm can identify the highest-consequence failures resulting from a cyber-attack against a specific critical infrastructure system, or identify the most consequential failures affecting complex interdependent infrastructure systems supporting a large urban area, regardless of the cause of disruption. Infrastructure system owners and operators, and government agencies can use results from optimization modeling to identify priority assets for in-depth security and resilience assessments, and to inform investment decisions related to critical infrastructure protection and mitigation.

Argonne is currently refining the optimization algorithm framework described within this paper through the Resilient Infrastructure Initiative, which is funded through Laboratory Directed Research and Development (LDRD) resources.[11] The list of critical assets resulting from the optimization algorithm can be analyzed further by infrastructure impact models such as EPfast[12] for electric power. Because of the computational complexity of assessing high numbers of

[11] Argonne Energy and Global Security, undated, *Resilient Infrastructure*, available at https://www.anl.gov/egs/group/resilient-infrastructure, accessed February 14, 2017.

[12] Portante, E.C., et al., 2011, "EPfast: A Model for Simulating Uncontrolled Islanding in Large Power Systems," *Proceedings of the Winter Simulation Conference*, Winter Simulation Conference.

infrastructure connections and associated failure scenarios, these studies are performed on Blues, a 350-node, high-performance computing cluster at Argonne.

ACKNOWLEDGMENT

The work presented in this paper was partially supported by Argonne National Laboratory under U.S. Department of Energy contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

If you would like more information regarding this paper, please contact Duane Verner at dverner@anl.gov.