Assessing Vulnerability of Proposed Designs for Interdependent Infrastructure Systems

Earl E. Lee, II
Rensselaer Polytechnic Institute
leee7@rpi.edu

John E. Mitchell
Rensselaer Polytechnic Institute
mitchj@rpi.edu

William A. Wallace
Rensselaer Polytechnic Institute
wallaw@rpi.edu

Abstract

Recent events have heightened our awareness of the vulnerability of civil infrastructure systems. Most of the research on this topic focused on individual systems, while more recent efforts have recognized the interconnectedness of systems. Infrastructure systems have become so highly interconnected that a failure in one system can propagate through many systems and affect large geographic areas. The focus of this research is on reducing vulnerability by adding redundancy while taking into account the interdependencies of infrastructure systems.

The paper will first present background and definitions related to interdependent infrastructure systems. An algorithm is presented that identifies vulnerabilities in the current and proposed design due to interdependencies with other infrastructure systems. An illustrative case, the reliance of telecommunications on power, is then presented to demonstrate the usefulness of the proposed procedure. The paper concludes with a discussion of further research, both theoretical and operational.

1. Introduction

Recent events, in particular the September 11, 2001 attacks, have increased concern over the vulnerability of infrastructure systems, those that provide the basic services of transportation, power, communications, etc. Alternative designs are being proposed to reduce vulnerability, typically by introducing redundancy – often at a substantial cost. However, any reduction in vulnerability may not be forthcoming if the designers do not consider the interdependence of infrastructure systems. For example, a proposed redundant path for a telecommunications network may be connected to the power system at a different point than an equivalent path in the present network – but the source of power maybe the same for both connections. The result is, if the power source is disabled, both paths will fail and telecommunications service will be not be available from these paths. This paper will present a systematic procedure for assessing the vulnerability of proposed designs for interdependent infrastructure systems.

Previous work has defined five types of interdependence: (1) Input – output of one system is an input to another; (2) Mutual dependence – two or more systems where the output of each system is an input to each of the other systems; (3) Co-located – sections are within a prescribed geographical region; (4) Shared – two services which rely on common sections of an infrastructure system; and (5) Exclusive-or – sections of an infrastructure system that can support only one service at a time [1]. In order to ascertain the reduction in vulnerability due to a proposed design, each of the foregoing types of interdependence must be assessed.

The examples and discussion in this paper will focus on infrastructure systems with a hierarchical structure such as power and telecommunications. The paper will first present background and definitions related to interdependent infrastructure systems. An algorithm is

presented that identifies vulnerabilities in the current and proposed design due to interdependencies with other infrastructure systems. An illustrative case, the reliance of telecommunications on power, is then presented to demonstrate the usefulness of the proposed procedure. The paper concludes with a discussion of further research, both theoretical and operational.

2. Background

In Executive Order 13010 of July 15, 1996, President Clinton established a national agenda for protecting the critical infrastructure systems. In the report of the President's Commission on Critical Infrastructure Protection (PCCIP), the following definitions are given:

> **Infrastructure**: a network of independent, mostly privately-owned, manmade systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services[2, p.3].
>
> **Vulnerability:** A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat [2, p. B-3].
>
> **Vulnerability Assessment:** Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation [2, p. B-3, B-4].

Critical infrastructures are those that are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security. The report of the PCCIP defines Transportation; Oil and Gas Production and Storage; Water; Emergency Services; Government Services; Banking and Finance; Electrical Power; and Telecommunications as critical infrastructures [2, p. 3].

The objective of the definitions provided by the PCCIP and by other authors such as Rinaldi, Peerenboom and Kelly [3]is to aid in the discussion of policies for addressing the vulnerability of infrastructures to natural, technological and intentional human-induced hazards [2, 3]. However, these definitions are not precise enough for the mathematical modeling necessary to provide decision support for designees of systems to reduce the vulnerability of infrastructures and the services they provide. Based upon this body of prior work and ongoing research, the following set of definitions has been established [1].

The current research identifies five types of interrelationship between infrastructure systems:

- *Input*: the infrastructure requires as input one or more services from another infrastructure in order to provide some other service. An example of this interdependency is the reliance of components in many infrastructure systems on power.
- *Mutual dependence*: at least one of the activities of each infrastructure in a collection of infrastructures is dependent upon each of the other infrastructures. An example of mutual dependence involving two infrastructures occurs when an output of infrastructure A is an input to infrastructure B, and an output of infrastructure B is an input to infrastructure A. This could be a compressor in a natural gas system requiring power to operate and the generating facility that generates the power relies on the natural gas for fuel.
- *Co-located*: any of their physical components are situated within a prescribed geographical region. In this case, the systems have nothing more in common than the physical location they share.
- *Shared (AND)*: some physical components or activities of an infrastructure used in providing two or more services are shared. For example, streets are used by the transit system and by emergency services, two services sharing one infrastructure component.
- *Exclusive-or* (*XOR*): only one of two or more services can be provided by an infrastructure component at a time. Note that a disturbance in an infrastructure that is dependent on another by virtue of its inability to operate if the other infrastructure is operating will effect just its own provision of service. An example of this can be drawn from accounts of the World Trade Center attack when some streets were made available only to emergency vehicles, private and transit vehicles were barred from using these areas [4].

Collectively, these five conditions—input, mutual dependence, co-location, shared and exclusive-or—will be denoted types of *interdependence*, since all imply that an impact on one infrastructure system is also an impact on one or more other infrastructure systems.

The issue of the vulnerability of our civil infrastructures has been addressed in a multitude of forums – the most prominent being the President's Commission on Critical Infrastructure Protection, as previously noted. Numerous researchers have studied the survivability of infrastructure systems by modeling them as networks and analyzing the impact of disruptions on the service provided by the infrastructure. As examples,

Balakrishnan, Magnanti and Mirchandian [5] and Chamberland and Sauso [6] focused on telecommunications networks, and Haimes et. al. [7] studied water systems.

In all cases, the research addressed one infrastructure system and the service it provides and did not consider interdependencies among infrastructure systems. Notable exceptions are work by Rinaldi, Peerenboom and Kelly [3] and Amin [8]that focuses on the issue of interdependent infrastructures and does provide very useful definitions and discussion of the ramifications of disruptions to interdependent infrastructure systems. However, their work stopped short of modeling the vulnerability of networks for analysis of alternative designs – the focus of this paper.

The work by Haimes and his colleagues is also very relevant to the issue of vulnerability of infrastructure systems [9, 10]. In Longstaff and Haimes (2002), hierarchical holographic modeling provides the holistic schema to address the survivability of infrastructure systems, while in Haimes and Jiang (2001), a Lontief-based input-output model is used to understand the interconnectedness among infrastructure systems. This work does provide important insights needed to begin to address the design issues of survivability of infrastructures systems.

In the research reported on in this paper, interdependent infrastructures are viewed as networks, with movement of material (power, electronic signals, etc.) corresponding to flows and with services corresponding to a desired level of these flows. Each network, or infrastructure system, is defined as a collection of nodes and arcs with material flowing from node to node along paths in the network. For each material, each node is either a supply node which is a source for the material; a demand node which is a point that requires some amount of the material; or a transshipment node which is a point that neither produces nor requires the material but serve as a point through which material passes [11]. Arcs may, of course, have limited capacities [12].

Infrastructure systems operate in an environment subject to disruptions, natural, human-caused or willful acts. Interdependent infrastructure systems can be designed to minimize possible service degradation following a disruption – decrease its vulnerability. The following section provides a systematic procedure to support designees tasked with increasing the survivability of interdependent infrastructure systems.

3. A Procedure for Assessing the Vulnerability of an Interdependent Infrastructure System Design With a Hierarchical Structure

3.1 An overview

The proposed procedure is to support system designees that have proposed a modification to an infrastructure whose purpose is to reduce the vulnerability of the system and the service it provides. The proposed procedure is to first map the present and proposed infrastructure system with its associated (interdependent) infrastructure systems. Each of the interdependencies defined in Section 2 is then identified (if they exist). Shared interdependency is the use of an infrastructure component for the provision of more than one service, while exclusive-or is the use of an infrastructure component for only one service at a time. In the context of power and telecommunications systems, components of either one can not be used to provide more than one service so one could say that the shared and exclusive-or interdependency are not present. However, one could also argue that the service conduits that power and communications lines are routed through are subject to shared or exclusive-or interdependencies. Voice circuits, known as POTS, can be run in relatively close proximity to power lines (shared), but T-1 or similar data lines can not (exclusive-or). However, this routing does not increase or decrease the vulnerability of the telecommunications system, except with respect to the co-location interdependence, discussed next.

For co-located sections of the proposed design and other infrastructure systems, there would be two cases. The first is that the other systems do not connect to the present system and the vulnerability of the proposed system is unaffected. The second case is where the other infrastructure systems are connected to the present system. For example, a section of a proposed telecommunications path is co-located with a section of the power system that provides power to the present telecommunication system. If there is a disruption at this location, both the proposed and the present systems will fail. Designers can assess the vulnerability of the proposed design due to co-located interdependency by the use of the graphic capabilities of a geographical information system (GIS). However, for input interdependency (and by extension mutually dependent), there is a requirement to identify the components in the two (or more) interdependent infrastructure systems with a hierarchical structure. For this an algorithm is proposed and discussed in the section to follow.

3.2 An Algorithm to Identify Vulnerabilities due to Input Interdependencies

As noted in the overview, the procedure starts with a mapping of the current and proposed infrastructure system and the infrastructure systems that support it

using, for example, a geographical information system (GIS). After identification and resolution, where necessary, of shared, exclusive-or and co-located interdependencies using the GIS capabilities, an algorithm is needed to identify the input interdependencies and assess the vulnerability of the proposed design to disruptions in these interdependent systems.

For example, let us consider a proposed design for a telecommunications system, specifically a telephone network system with a power system supporting it. The designer will first "draw" the proposed redundant path for the telecommunication system, noting the connectors to the power system. The components in this proposed telecommunications path, which are seen as either supply or transshipment nodes in the telecommunications system can also be seen as demand nodes in the power system. The algorithm then starts from these power connections to telecommunications in the power system and traces back through the power system to determine the complete set of transshipment and supply nodes that are necessary for the proposed telecommunications path to be operational.

Next, the connectors in the power system to the current telecommunications network are identified. Again, a search is conducted to determine all the nodes in the power supply that are required for the current telecommunications system to be operational. Any nodes common to these two sets are points where failure of a single node (component) in power results in failure of both the current and proposed telecommunications networks.

In a telephone system, customers function as both supply and demand nodes. Calls originate at a customer and are collected along a distribution cable typically serving dozens of customers. Many distribution cables come together at a Controlled Environmental Vault (CEV). Calls then pass from the CEV through a feeder cable containing thousands of lines and come together in the cable vault of a central office and into a switching system. From the central office, they pass to one of the following: to another central office through an interface trunk; to a tandem[1] via a trunk link; or out through the same set of CEV's that feed the (originating) central office.

The power distribution system shown in Figure 1 has four high voltage power supplies (operating typically in the range of 100,000 to 315,000 volts). This high voltage is input to substations, which transform down the high voltage power received from the transmission system to 13,500 volts (13.5kV). From these substations, power is provided by feeders to 120/208 volt transformers, and then to the customers.

Since this illustration focuses on power and telecommunications, only the power connections to telecommunication components are discussed. The level of detail used would vary based upon the systems being analyzed. Consider the telephone system with supporting power system depicted in Figure 1. To reduce vulnerability, a customer desires an additional communications connection from office A to office B. The existing path passed through CEV A, CO A, and CEV B to connect A to B. The new, proposed path passes through CEV C, CO B, and CEV D.

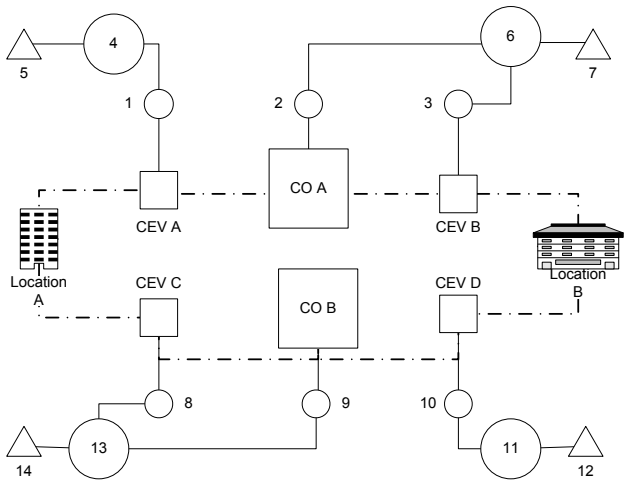

Figure 1. Example of a Redundant Path with No Vulnerabilities due to Interdependency

From the perspective of the provider of the communications, this proposed, new communications line is adequate. Assuming that the designer has ensured or clearly identified areas where the communications lines are in close proximity and therefore vulnerable and has taken steps to the greatest extent possible to minimize this vulnerability. Now consider the reliance on power. Per the earlier discussion, the designer would identify that power connects to the original path at power nodes 1, 2 and 3. Node 1 relies on node 4 which relies on node 5. Nodes 2 and 3 rely on node 6 which relies on node 7. The complete set of power nodes for the original path is 1, 2, 3, 4, 5, 6, and 7. Similarly the new path connects at power nodes 8, 9 and 10. Tracing backward, the procedure indicates the set of nodes for the new path is 8, 9, 10, 11, 12, 13, and 14. Since the two paths have no nodes in common, single component failures in power will not disrupt both paths.

Now consider the example shown in Figure 2.

[1] A tandem has trunk lines to all central offices in its sector and trunks to all other tandems with the same of other companies providing service to the world network.

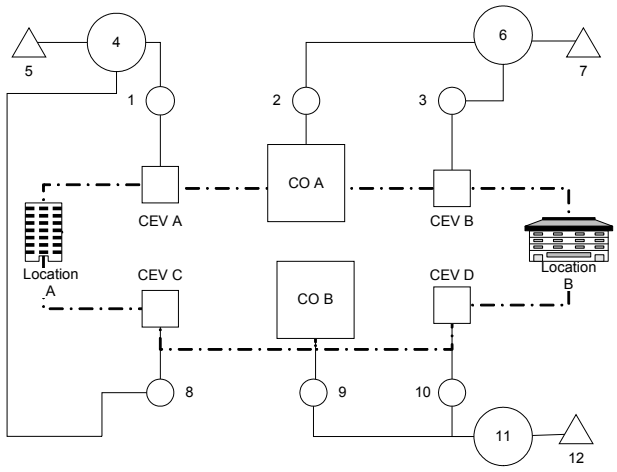

Figure 2. Example of a Redundant Path with Vulnerabilities due to Interdependency

In this case the original path relies on Node 1, 2, 3, 4, 5, 6, and 7. The proposed path relies on 4, 5, 8, 9, 10, 11, and 12. Both paths rely on nodes 4 and 5 so failure at either would result in loss of both communications paths.

In general, the algorithm starts by picking one of the supporting systems and assessing the vulnerability of the proposed system to disruption in the supporting infrastructures. The algorithm has two stages as follows:

- a backward trace through the supporting system to determine the set of transshipment and supply nodes that are needed to make both the proposed design and the current configuration operational, and
- identification of the components in the supporting infrastructure systems that are common to both the proposed and current configuration of the infrastructure system whose vulnerability is being assessed.

Stage 1 is accomplished using a reverse search algorithm. In the book *Network Flows* [12, pp. 73-77], the following discussion is given.

> To illustrate the basic ideas of search algorithms, suppose that we wish to find all the nodes in a network $G=(N,A)$ that are reachable along directed paths from a distinguished node s, called the *source*. A search algorithm *fans out* from the source and identifies an increasing number of nodes that are reachable from the source. At every intermediate point in its execution, the search algorithm designates all the nodes in the network as being in one of the two states: *marked* or *unmarked*. The marked nodes are known to be reachable from the source, and the status of unmarked nodes has yet to be determined. Note that if node i is marked, node j is unmarked and the network contains the arc (i, j) we can mark node j; it is reachable from source via a directed path to node i plus are (i, j). Let us refer to arc (i, j) as *admissible* if node i is marked and node j is unmarked, and refer to it as *inadmissible* otherwise. Initially, we mark only the source node. Subsequently, by examining admissible arcs, the search algorithm will mark additional nodes. Whenever the procedure marks a new node j by examining an admissible arc, (i, j), we say that node i is a predecessor of node j [i.e., *pred (j) = i*]. The algorithm terminates when the network contains no admissible arcs.

```
algorithm   search;
begin
      unmark all nodes in N;
      mark node s;
      pred(s):  = 0;
      next:   = 1;
      order(s): = s;
      List: ={s}
      while LIST ≠Ø do
      begin
          select a node i in LIST;
          if node i is incident to an admissible arc (i,
   j) then
          begin
              mark node j;
              pred (j): = i;
              next: = next +1;
              order (j): = next;
              add node j to LIST;
          end
          else delete node i from LIST;
      end;
  end;
```

Figure 3.4 Search algorithm.

…Figure 3.4 gives a formal description of the search algorithm. In the algorithmic description, *LIST* represents the set of marked nodes that the algorithm has yet to examine in the sense that some admissible arcs might emanate from them. When the algorithm terminates, it has marked all the nodes in G that are reachable from s via a directed path. The predecessor indices define a tree consisting of marked nodes.

…The search algorithm described in Figure 3.4 allows us to identify all the nodes in a network that are reachable from a given node s by directed paths. Suppose that we wish to identify all the nodes in a network from which we can reach a given node t along directed paths. We can solve this problem by using the

> algorithm we have just described with three slight changes: (1) we initialize LIST as LIST = {*t*}; (2) while examining a node, we scan the incoming arcs of the node…; and (3) we designate an arc (*i, j*) as admissible if *i* is unmarked and *j* is marked. We …refer to this algorithm as a *reverse search algorithm*.

Stage 2 will be accomplished by the pairwise comparison of the sets of nodes generated in Stage 1 for the current and proposed path(s) for common elements. These common elements represent points in the supporting system that make both the redundant and the original paths in the system under study vulnerable. Assuming a single supporting system and letting L_i denote a set of nodes in the supporting system for proposed path *i*, where $i = 1, \ldots n\text{-}1$ and letting the *n*th path be the current configuration of the system that the designer is proposed to reduce its vulnerability, then the procedure finds the nodes in the set $L_i \cap L_n$ for each L_i , the pair-wise intersections of the sets of nodes. The elements of this intersected set, are the nodes in the supporting system, i.e., power systems for telecommunications, that if one or more of them failed, both the current and proposed system would fail, i.e., the telecommunications systems. Designers can identify these nodes on a GIS presentation, and evaluate the effects of node failure, individually or in combination, on the proposed design, i.e. assess its vulnerability.

The following section presents a case based upon past research following the World Trade Center attack [1].

4. Illustrative example

While the example used in Figures 1 and 2 may seem trivial, consider the situation in lower Manhattan. In this geographic area, assume there are 6 high voltage sources for the power system, supplying 15 substations with 6 to 7 feeders each. In telecommunications, there are 17 central offices with four CEVs each. (The number of central offices and power substations, while not exactly matching the systems of Consolidated Edison and Verizon are representative. Since the September 11 attack, information on location and number of components is sensitive.) The procedure to be illustrated by this case would start with a GIS mapping of the proposed and the current telecommunications systems with the supporting power system. However, the case is too complex to portray actual locations in graphical form for this paper.

For this case there are 15 power substations and the neighborhoods they serve. Each substation has 6 or 7 feeders used to distribute power. The 15 substations (numbered 1-15) are served by 6 separate high voltage sources, referred to as A, B, C, D, E, and F. Each source supplies 2 or 3 substations depending on system construction. Each feeder may provide power to 20-40 transformers. Since the focus of this paper is the interdependencies of telecommunications and power, each feeder is shown with its connections to telecommunications components. All other loads from the feeder are aggregated. If additional infrastructure systems were modeled, greater detail would be needed.

In the telecommunication system, 17 central offices are being modeled. Each central office will be served by 4 CEVs. Due to geographic proximity, the central offices are interconnected to facilitate call routing throughout Manhattan. The interconnections are as follows: CO 1 connects to COs 2 and 4; CO 2 connects to COs 1, 3 and 5; CO 3 connects to COs 2 and 6; CO 4 connects to COs 1 and 7; CO 5 connects to CO 2; CO 6 connects to COs 3, 9 and 10; CO 7 connects to COs 4, 8 and 13; CO 8 connects to CO 7; CO 9 connects to COs 6 and 11; CO 10 connects to COs 6 and 12; CO 11 connects to COs 9, 12 and 14; CO 12 connects to COs 10, 11 and 15; CO 13 connects to COs 7, 16 and 17; CO 14 connects to COs 11 and 17; CO 15 connects to CO 12; CO 16 connects to CO 13; CO 17 connects to CO 13 and 14.

Let us consider a business with officers at location 1 and 2. Location 1 is served by CEV 6-3 and location 2 by CEV 13-2; power at locations 1 is from Substation 6 Feeder 6 and locations 2 by Substation 13, Feeder 1. The client has an existing communications connection and wishes to add another for improving survivability. Assuming shortest path routing, the existing line runs from CEV 6-3 to CO 6 to CO 9, CO 11, CO 14, CO 17, CO 13, to CEV 13-2. To meet the clients' requirements, the company would need to connect the location to a CEV not served by CO 6. The closest option would be CEV 5-4 powered by Substation 5, Feeder 6. At location 2, the closest CEV not serving CO 13 is 8-4 powered from Substation 11, Feeder 3. The new path is 5-4 to CO 5, CO 2, CO 1, CO 4, CO 7, CO 8 to CEV 8-4.

The connection and construction of the power is shown in Figure 3.

Starting at the connections of the CEVs and COs to the power grid and utilizing the algorithm to first back trace though power and then find the intersections, the following is the set of nodes in the power system where failure of the component, regardless of cause, will result in failure of both communications paths: Let L_c be the set of power nodes serving the current path and L_p be the set for the proposed path. The intersection consists of High Voltage Supplies C, D or E and Substation 11.

Figure 3. Hierarchical Representation of Power System with Connections to Phone System

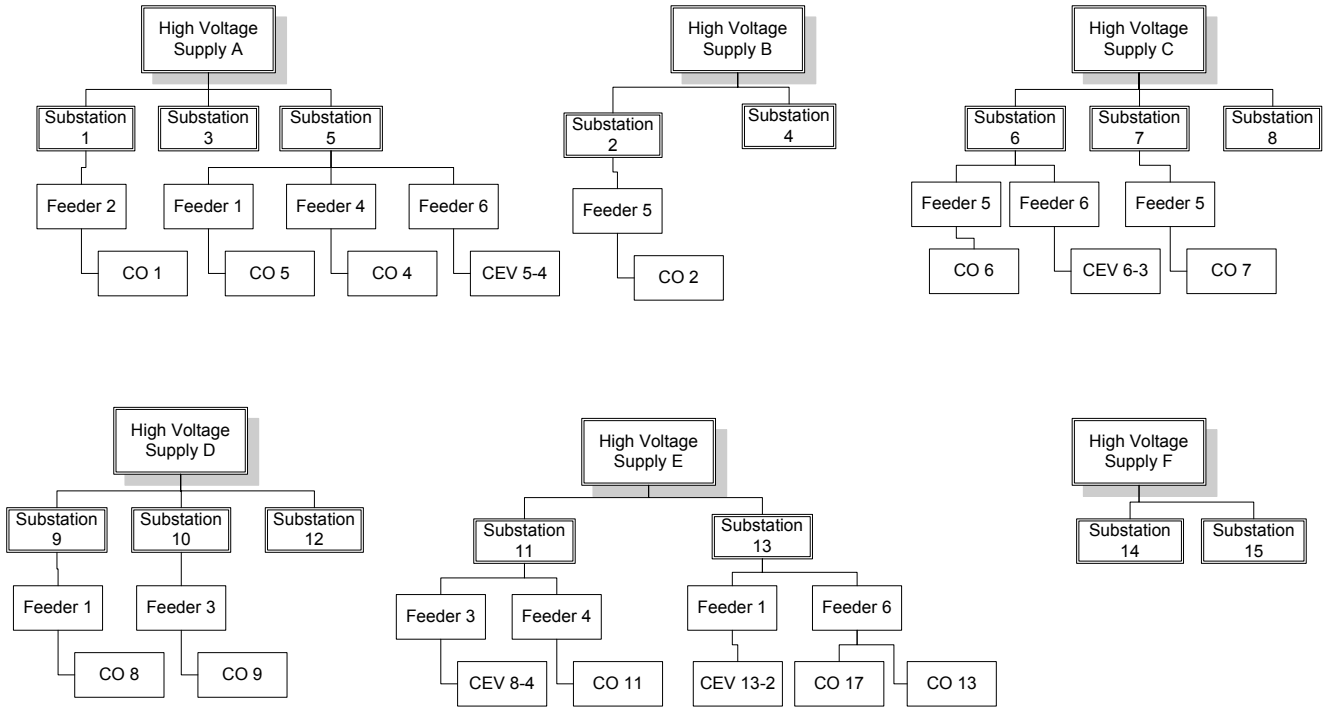

Table 1. List of components in power that if disrupted would cause failure in the original and proposed telecommunications paths.

Failed Power Component	Failed Component in Original Telecommunication Path	Failed Component in Proposed Telecommunication Path
High Voltage Supply C	CEV 6-3 and Central Office 6	Central Office 7
High Voltage Supply D	Central Office 9	Central Office 8
High Voltage Supply E	Central Office 11,13,14, and 17 and CEV 13-2	CEV 8-4
Substation 11	Central Office 11	CEV 8-4

In some cases, it may be useful to consider the possibility of changes to the power network to reduce these vulnerabilities. In the example just shown, one vulnerable point was CEV 8-4. If a new power shunt could be run to this CEV from a power source not affected by the other failures, one vulnerable point would be removed. Since no feasible path was found, it was not necessary for the designers to check for the co-location interdependency as outlined in Section 3.1.

5. Conclusions

The illustrative case identified components in the power system where both existing and proposed paths in telecommunications were vulnerable due to single failures in the power system. This method has the advantage of being scenario independent, i.e. the cause of the failure of the power component is irrelevant. However, this method does require a system engineer to propose an alternative path. The next step in this research is to develop a methodology that, given an existing infrastructure system, its supporting infrastructures, and two locations (nodes), could determine if an alternative, independent path exists with respect to each supporting system and provide this information to the designers.

Utilizing the reverse search algorithm previously presented and models of interdependent infrastructures developed in prior research [1, 13] , a procedure could be developed which does not require a designer to propose a path. This procedure should be able to provide at least one alternative path between two specified locations (nodes) that is completely independent from both the perspective of the infrastructure system whose vulnerability is being determined and with respect to all of its supporting systems. To accomplish this, the following procedure is proposed.

Using the algorithm presented in this paper, select one supporting infrastructure system and conduct a reverse search on the original, existing infrastructure system path to collect the set of nodes from the supporting system that it relies on. (Note the existing search algorithm has only been proven to work on systems with a hierarchal structure. New search algorithms would have to be developed for systems having other basic structures.) Then, utilizing the integer programming model of interdependent infrastructure systems previously developed [1], simulate failures at all of these supporting system nodes which would lead to disruption in the system being studied and show those components that would still be operational with a failure of any and all of

the supporting systems components. Utilizing the principles of network flow, the model will be able to determine if a feasible path (or paths) exists and the set of nodes that constitute this path (or set of paths). This information will then be provided to the designer.

6. Acknowledgements

This research has been supported by NSF grants CMS 0139306, Impact of the World Trade Center Attack on Critical Infrastructure Interdependencies and DMII 0228402, Disruptions in Interdependent Infrastructures, A Network Flows Approach.

7. References

[1] W. A. Wallace, D. M. Mendonca, E. E. Lee, J. E. Mitchell, and J. H. Chow, "Managing Disruptions to Critical Interdependent Infrastructures in the Context of the 2001 World Trade Center Attack," in *Impacts of and Human Response to the September 11, 2001 Disasters: What Research Tells Us*, M. F. Myers, Ed. Boulder, CO: Natural Hazards Research and Applications Information Center, University of Colorado, forthcoming.

[2] President's Commission on Critical Infrastructure Protection, *Critical Foundations - Protecting America's Infrastructures*. Washington, DC: Report of the President's Commission on Critical Infrastructure Protection, October, 1997.

[3] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, vol. 21, pp. 11-25, December, 2001.

[4] A. Berenson, "A Full Reopening of Stock Trading Is Set for Monday," *New York Times*. September 14, 2001, p. C1.

[5] A. Balakrishnan, T. L. Magnanti, and P. Mirchandani, "Designing Hierarchical Survivable Networks," *Operations Research*, vol. 46, pp. 116-136, January-February, 1998.

[6] S. Chamberland and B. Sanso, "On the Design of Multitechnology Networks," *INFORMS Journal on Computing*, vol. 13, pp. 245-256, Summer, 2001.

[7] Y. Y. Haimes, N. C. Matalas, J. H. Lambert, B. A. Jackson, and J. F. R. Fellows, "Reducing Vulnerability of Water Supply Systems to Attack," *Journal of Infrastructure Systems*, vol. 4, pp. 164-177, December, 1998.

[8] M. Amin, "Toward Self-healing Energy Infrastructure Systems," *IEEE Computer Applications in Power*, vol. 14, pp. 20-28, January, 2001.

[9] T. A. Longstaff and Y. Haimes, "A Holistic Roadmap for Survivable Infrastructure Systems," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 32, pp. 260-268, March, 2002.

[10] Y. Haimes and P. Jiang, "Lontief-based Model of Risk in Complex Interconnected Infrastructures," *Journal of Infrastructure Systems*, vol. 7, pp. 1-12, March, 2001.

[11] J. G. Ecker and M. Kupferschmid, *Introduction to Operations Research*. Malabar, FL: Krieger Publishing Company, 1991.

[12] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin, *Network Flows*. Englewood Cliffs, NJ: Prentice Hall., 1993.

[13] E. E. Lee, D. Mendonca, J. E. Mitchell, and W. A. Wallace, "Restoration of Services in Interdependent Infrastructure Systems: A Network Flows Approach," *Technical Report 38-03-507, Decision Sciences and Engineering Systems*, Rensselaer Polytechnic Institute, Troy, NY, 2003.