

◆ Critical National Infrastructure Reliability Modeling and Analysis

Stephen H. Conrad, Rene J. LeClaire, Gerard P. O'Reilly,
and Huseyin Uzunalioglu

One of the top 10 priorities of the U.S. Department of Homeland Security is protection of our critical national infrastructures including power, communications, transportation, and water. This paper presents models to quantify the interdependencies of critical infrastructures in the U.S. and evaluate plans to compensate for vulnerabilities. Communications is a key infrastructure, central to all others, so that understanding and modeling the risk due to communications disruptions is a high priority in order to enhance public safety and infrastructure resiliency. This paper discusses reliability modeling and analysis at a higher level than usual. Reliability analysis typically deals at the component or sub-system level and talks about "mean time to failure" and "mean time to repair" to derive availability estimates of equipment. Here, we deal with aggregate scales of failures, restoration, and mitigation across national infrastructures. This aggregate scale is useful when examining multiple infrastructures simultaneously with their interdependencies. System dynamics simulation models have been created for both communication networks and for the infrastructure interaction models that quantify these interactions using a risk-informed decision process for the evaluation of alternate protective measures and investment strategies in support of critical infrastructure protection. We will describe an example development of these coupled infrastructure consequence models and their application to the analysis of a power disruption and its cascading effect on the telecommunications infrastructure as well as the emergency services infrastructure. The results show significant impacts across infrastructures that can become increasingly exacerbated if the consumer population moves more and more to telecom services without power lifeline.

© 2006 Lucent Technologies Inc.

Critical Infrastructure Protection Modeling

Disruptions to our critical national infrastructures (e.g., power, telecom, transportation, and emergency services) are an area of increasing

national concern [21]. Each of the infrastructures is highly dependent on telecommunications [6] and each of the infrastructures is subject to

disruptions, examples of which are shown in the list below.

- Telecommunications: Congestion or disruption of key communications nodes by fire, wind, water, or sabotage
- Power: Blackouts caused by insufficient generation to meet demand, transmission bottlenecks, or equipment outages
- Emergency services: Demand greater than response capacity, as during a disaster
- Water: Contamination with toxic substances
- Agriculture and food: Contamination of food supply
- Chemical industry: Explosions, release of toxic gas clouds
- Defense industrial base: Supply line interruptions
- Banking and finance: Disruption of electronic payments systems that cause bank liquidity problems
- Public health: Infectious diseases, anthrax
- Government: Disruptions in operations

The U.S. Department of Homeland Security (DHS) is interested in developing analysis tools that provide insights for making critical infrastructure protection (CIP)-related decisions across all critical infrastructures and their primary interdependencies. The critical infrastructures are a complex “system of systems.” Interdependencies are generally not well understood and disruptions in one infrastructure can propagate into other infrastructures [8]. Infrastructure studies are becoming more prevalent [1, 2, 7, 13, 15].

Risk-informed decisions are needed to help identify investment strategies and other options that best reduce overall risk. **Figure 1** plots the risk profiles for potential disruptions: the likelihood of an event happening versus the consequence of a disruptive event happening. We define risk to be the product of likelihood and consequence.

When the risk is low (lower left corner), the event is unlikely to happen, and if it does, the consequence of the event is relatively low. Therefore, the most appropriate course may be to simply accept the risk, and live with the consequences. However, when risk is high (upper right corner), we should act immediately to mitigate that risk to the extent possible. When risk is in the broad middle area where most potential problems lie, then it is especially important to analyze and

Panel 1. Abbreviations, Acronyms, and Terms

CIP—Critical infrastructure protection
 DHS—Department of Homeland Security
 DSS—Decision support system
 IP—Internet Protocol
 LANL—Los Alamos National Laboratory
 N-SMART—Network simulation modeling and analysis research tool
 NISAC—National Infrastructure Simulation and Analysis Center
 PSTN—Public switched telephone network
 SNL—Sandia National Laboratories
 VoIP—Voice over IP

prioritize before decisions can be made. These types of analysis can help answer questions as follows:

- What are the consequences of a disruptive event?
 - Metrics for consequences include: public health, national security, and economic impacts
- Where are the choke points?
 - Are there specific assets that are essential to infrastructure functioning such that their disruption could have a debilitating impact on an infrastructure’s operations?
- What are the high risk areas that present the greatest opportunities for significant risk reduction?
 - Which investment, mitigation, and research strategies can have the greatest impact in reducing overall risk?

In this paper, we focus on just the first three infrastructures on the previous list: telecommunications,

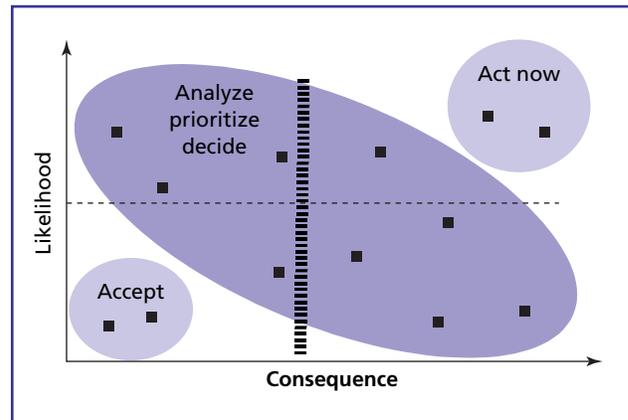


Figure 1. Risk profile for a potential disruption.

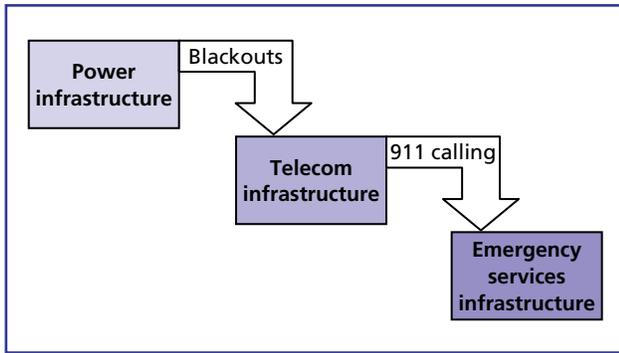


Figure 2.
Example cascading of impacts across industries: power, telecom, and emergency services.

power, and emergency services and the potential cascading effects among them as shown in **Figure 2**. In general, cascading across infrastructures can occur in almost any order, but telecommunications always is a central component surrounding the disruption and is especially important in mitigating the disruptive effects.

For example, the major power blackout on August 14, 2003, affected over 50 million people, and lasted up to 4 days in various parts of the eastern USA. The estimated direct costs were between \$4 billion and \$10 billion [20]. In today’s telecom environment, most people have wireline phones, which continue working during a blackout because phones are powered by telecom central offices, most of which have emergency generators. Therefore, during the August 2003 outage, there was very little cascading of impacts to the telecom infrastructure and to emergency services. As we’ll see later, this may change as people move more and more to wireless-only services and other telecom arrangements without power lifeline back-up.

Models of Telecom

Bell Labs has developed specialized, state-of-the-art simulation models for analysis of networks to study the effects of disruptions, traffic overloads, and user behavior on network performance [6]. The primary suite of simulation models is called N-SMART (network simulation modeling and analysis research tools) and these tools cover both discrete event and/or

flow-based models of telecommunications traffic across networks:

1. N-SMART-Metro for metropolitan area PSTN networks
2. N-SMART National Long Distance for a national long distance network
3. N-SMART-Data for packet data networks,
4. N-SMART Analytic for mathematical foundations which are high-level representations of aggregate network behavior as differential/difference-equations.

These models simulate a broad spectrum of networks at both metropolitan and national levels. The level of detail and run time is graphically displayed in **Figure 3**. The first three are detailed point-to-point geographic-based network simulations that require significant run times for a given analysis for a single sector of telecom infrastructure. For analysis across multiple infrastructures, the “challenge of dimensionality” comes into play, and these detailed event-based simulations take too long to run (many hours). As such, aggregated models of networks have been developed using dynamic simulation [4, 19] methodology. System

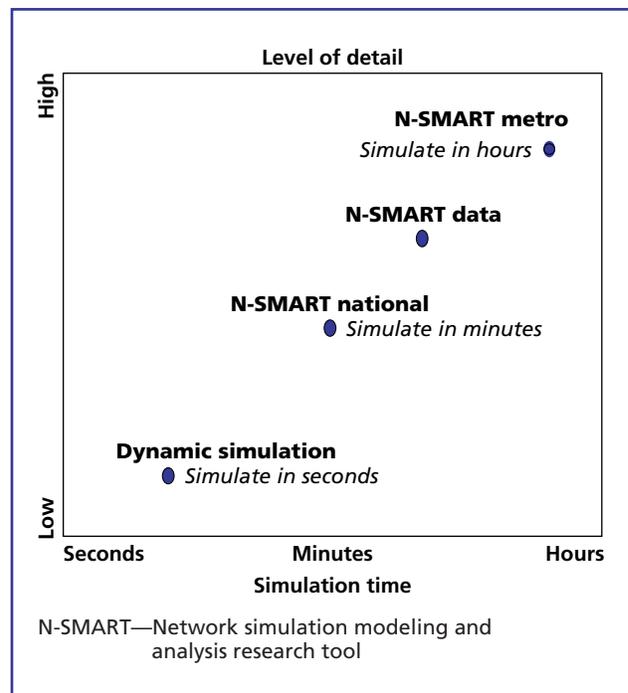


Figure 3.
Broad spectrum of telecom models.

dynamics is a way of thinking about the future that focuses on “stocks” and “flows” within processes and the relationships between them. It uses simulation to solve a system of non-linear differential equations. This modeling approach has been used as a quantitative means to explore overall system performance and evaluate policy options.

Models of Critical Infrastructures

The CIP/DSS (Critical Infrastructure Protection/ Decision Support System) project at Argonne, Los Alamos, and Sandia National Laboratories has developed a risk-informed decision support system that provides insights for making critical infrastructure protection decisions by considering all critical infrastructures and key resources, and their primary interdependencies. Initiated as a proof-of-concept in August 2003, the CIP/DSS project has demonstrated how it will assist decision makers in making informed choices by a) functionally representing all critical infrastructures and key resources with their interdependencies; b) computing human health and safety, economic, public confidence, national security, and environmental impacts; and c) synthesizing a methodology for decision making that is technically sound, defensible, and extendable.

System dynamics consequence models representing the key infrastructures were built using Vensim* [22]. The output of these models is captured in a consequence database from which “decision metrics” tuned to particular decision-maker profiles are computed. Multi-attribute utility functions determined from interviews with decision makers are used to compare alternative infrastructure protection strategies and help build consensus among stakeholders in a decision. The consequence models simulate the dynamics of individual infrastructures and couple separate infrastructures to each other according to their interdependencies. Dynamic processes like these are represented in the CIP/DSS infrastructure sector simulations by differential equations, discrete events, and codified rules of operation.

The initial CIP/DSS prototype used nearly 5000 variables to coarsely simulate the dynamics of the critical infrastructures and key resources at the national and metropolitan scales: many of these variables are

output metrics estimating the human health (e.g., deaths from an event), economic (monetary damage), or environmental effects (air contamination) of disturbances to the infrastructures. **Figure 4** shows some of the models from the 10,000 foot level, i.e., without any detail, just to give an idea of the complexity involved. Each of the boxes represents a different infrastructure. The box in the middle is the telecom and information infrastructure. The lower right box is the power infrastructure.

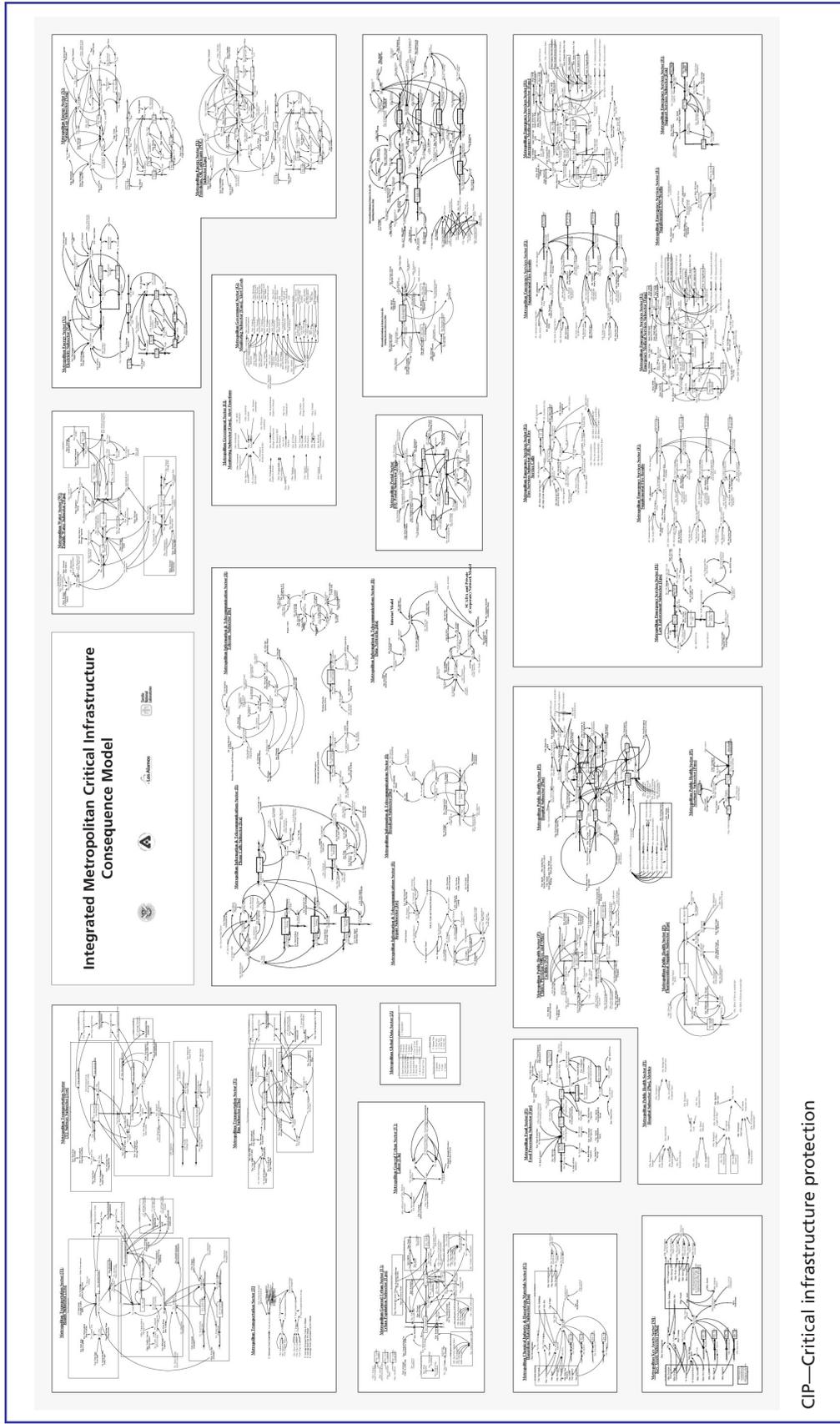
In the next section we make this general discussion more specific. That is, we simulate three infrastructures (power, telecom, and emergency services) together in relation to a specific problem that might be encountered in the future. In particular, power blackouts may cause loss of telephone service for those without power back-up, which then impacts the ability of people to call 911 in emergency service situations. The resulting impact is that regular injuries could become major injuries, and major injuries could become fatal [14].

Inter-Infrastructure Vulnerability: Power and Telecom

Today, there is very little cascading of impacts due to a power blackout. Most people still have wireline phones that continue to work during a blackout. Why do they work? Central offices have emergency diesel generators to power the telephone lines during a blackout. Hence, people have access to emergency services (police, fire, medical) even during a blackout.

However, this situation may change in the future. It is a fact that more and more people are moving to situations where their phones won't work in the event of a blackout. Examples include:

1. People with only cordless phones, which need power to operate.
2. People with wireless-only service. It is estimated that about 4% of households in 2004 have wireless-only service, i.e., no wireline service. This is expected to grow rapidly because of the economic incentive to do so [18].
3. People with voice over cable telephony service. The cable modems need power to operate.
4. People with other VoIP arrangements where back-up power is not provided.



CIP—Critical infrastructure protection

Figure 4. Interconnected metropolitan CIP sectors.

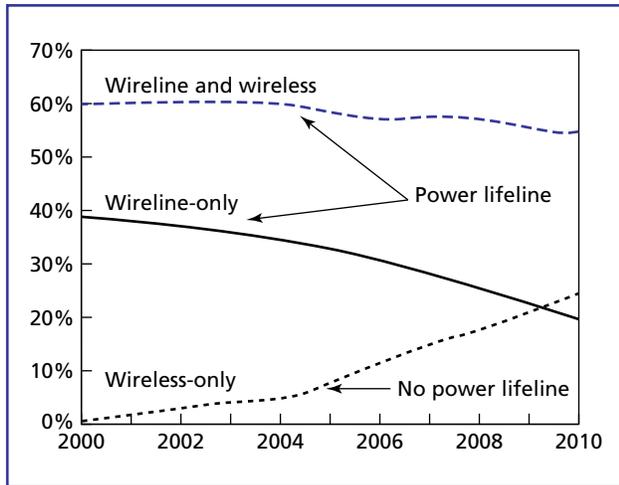


Figure 5.
Forecast of households without power lifeline.

Where a telephone service has back-up power, we use the terminology “power lifeline.” When it does not, we say “no power lifeline.”

As an example, category 2, or wireless-only service, is affected only after several hours of blackout. Cell towers typically depend on battery back-up, capable of lasting approximately 4 hours. Hence, a power disruption (blackout) lasting longer than 4 hours would eliminate telephone service for all those “wireless-only” access arrangements [14]. **Figure 5** shows a breakdown of households in terms of their access method to telecommunications services as wireline-only, wireless-only, and both wireline and wireless access as a function of time [5]. By 2010, 20–25% of households may use services with no power lifeline, and we study extremes where this goes to 100% in a sensitivity analysis. It should be noted that many people have wireless service to increase their safety when they are away from home.

Telecom Model: Example Vensim Model of Aggregate Wireline + Wireless Network

This section describes a simple model, shown in **Figure 6**, and uses it as the basis for our aggregate wireline and wireless network of a metropolitan area of 5 million people.

The telecom model is a time-driven simulation, where time moves in discrete steps, and within each time step, a number of call events such as arrivals and departures occur. The simulation state is updated at the beginning of each time interval for the aggregate

call events occurring within the interval. Although this method improves the simulation scalability at the expense of accuracy, good models can be developed to achieve the desired accuracy in a scalable manner [9]. Call blocking depends on the sequence of arrival, reattempts, and departure events. We approximate the number of arrivals, reattempts, departures, and call blocking at each time step as detailed in [16].

Figure 7 shows the stocks and flows of a flow-based model. At time t , the state of the network is described by one or more variables (stocks). One stock is the number of calls in progress for the network. The flows that change this stock in a time step Δ_t are call departures and calls admitted in Δ_t . Another stock is the reattempt pool for the network, a pool of incomplete calls from earlier time intervals. The flows that change this stock are reattempts drawn from the pool and a fraction of incomplete calls (that were not abandoned). The vertical block arrows could be interpreted as “converters” that set the rates, namely the call arrival rate, the call departure rate, and the call reattempt rate.

We represent the network as a pool of communication resources. A call arrival is admitted into the network if there is available capacity in the pool. If there is no available capacity, the call can be blocked and retried later, or it can be abandoned immediately. The following summarizes the flow of the simulation. At the beginning of each time interval:

1. Compute the number of departures within next time interval, and adjust the network capacity by this number.
2. Compute the number of arrivals within the time interval.
3. Determine the number of calls that can be admitted into the network using $\min(\text{number of arrivals, available capacity})$. The rest of the calls are blocked. Adjust the amount of available capacity.
4. Determine the number of calls that would retry later using the reattempt probability. Place these calls into the reattempt pool. Abandon the rest of the blocked calls.

At the end of each time interval,

1. Determine the number of departures within the current time interval out of calls admitted at the beginning of the time interval as described at Step 3 above.

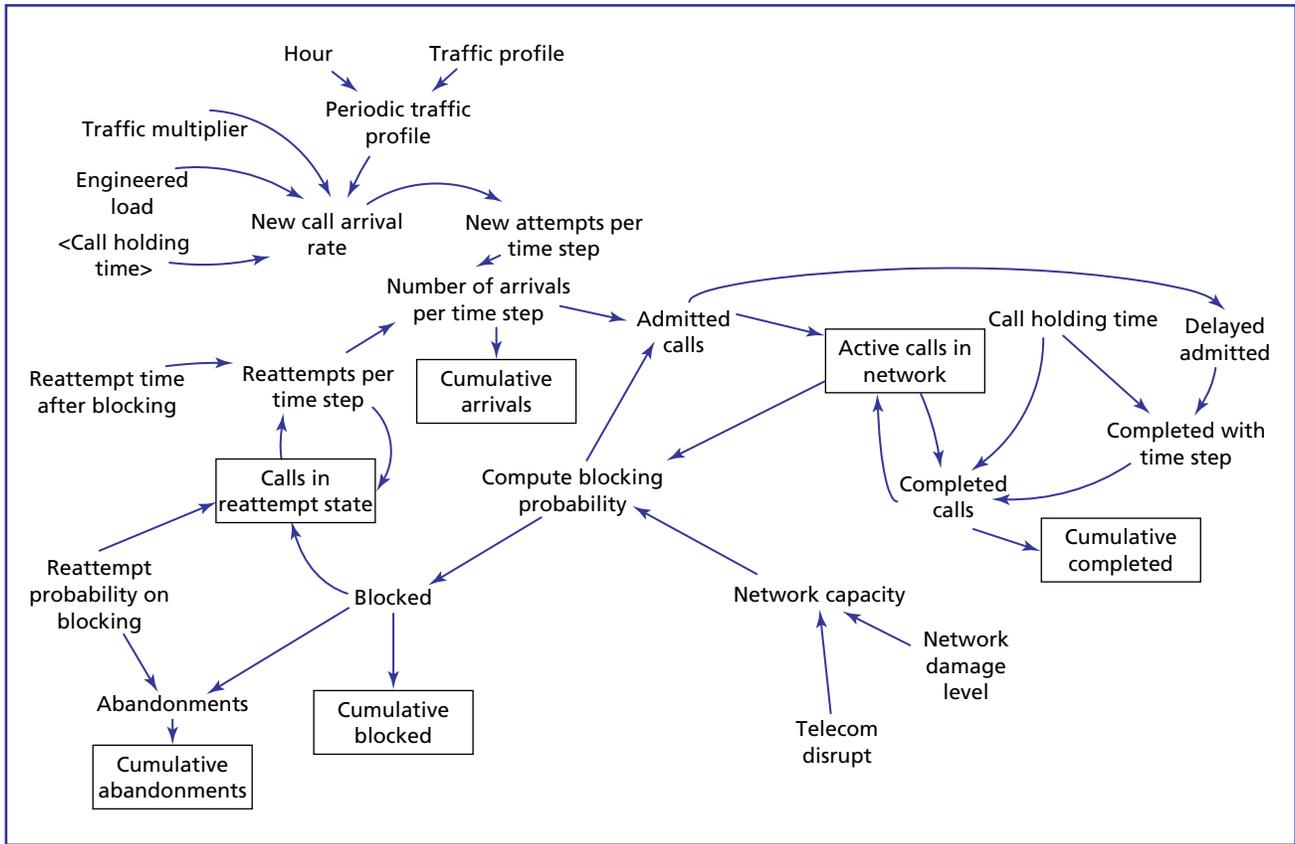


Figure 6.
Aggregate network model.

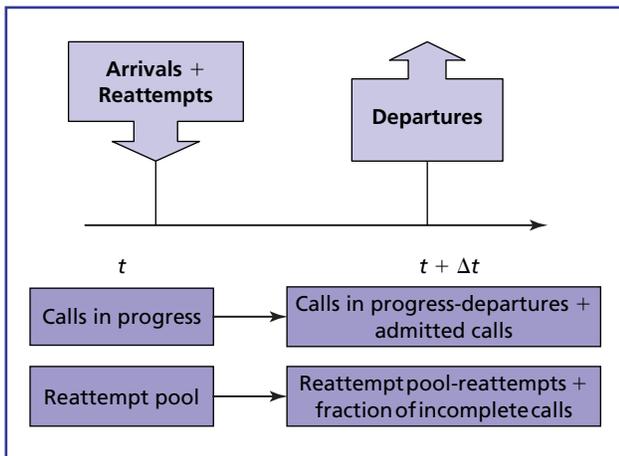


Figure 7.
Flow-based model.

2. Adjust the available capacity for these departures.

The details of this algorithm can be found in [16].

In the lower right of Figure 6, we show a function called network damage and a binary variable, telecom

disrupt, which turns it on or off. The network damage level models telecom disruptions and gives the fraction of the network that is damaged for a given time epoch [14].

Power Blackout Model

A simple power blackout model is represented in Figure 8, using three parameters:

- *Start time of blackout* (e.g., at hour 4 as in Figure 8).
- *Length of blackout* (e.g., 34 hours). In our example, this implies recovery starts at hour 38.
- *Recovery time*, i.e., length of time after recovery starts that the blackout ends.

In our example, recovery takes 4 hours. Hence, the end of the blackout occurs at hour 42. Recovery time is modeled as a linear recovery from the damaged state (no power) to complete recovery. This is a reasonable representation of the manner in which real power distribution systems recover. Typically, hospitals, police stations, and fire stations are restored first. Next, power is restored to television and radio stations.

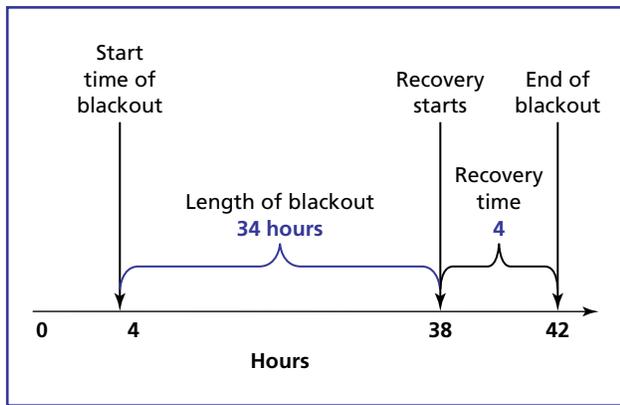


Figure 8.
Timeline model of power blackout.

Following that, service is restored to street lights; then commercial districts; then schools. Finally, power is restored to residential neighborhoods. The restoration of residential power occurs piecewise. Demand is

increased incrementally—one substation at a time—to promote the stability of the recovering system.

Note that a blackout might stimulate some mass calling throughout the metropolitan area, but for simplicity, we don't model that here.

The Vensim model of the blackout model described, along with the number of wireline and wireless subscribers impacted by the blackout, is shown in **Figure 9**. The left side takes a metropolitan area of approximately 5 million people, breaks it down into households with wireline and wireless services, and eventually ends up with five categories of customers,

1. Wireline-only service with power lifeline,
2. Wireline-only service with no power lifeline,
3. Wireline + wireless services with power lifeline,
4. Wireline + wireless services with no power lifeline, and
5. Wireless-only service with no power lifeline.

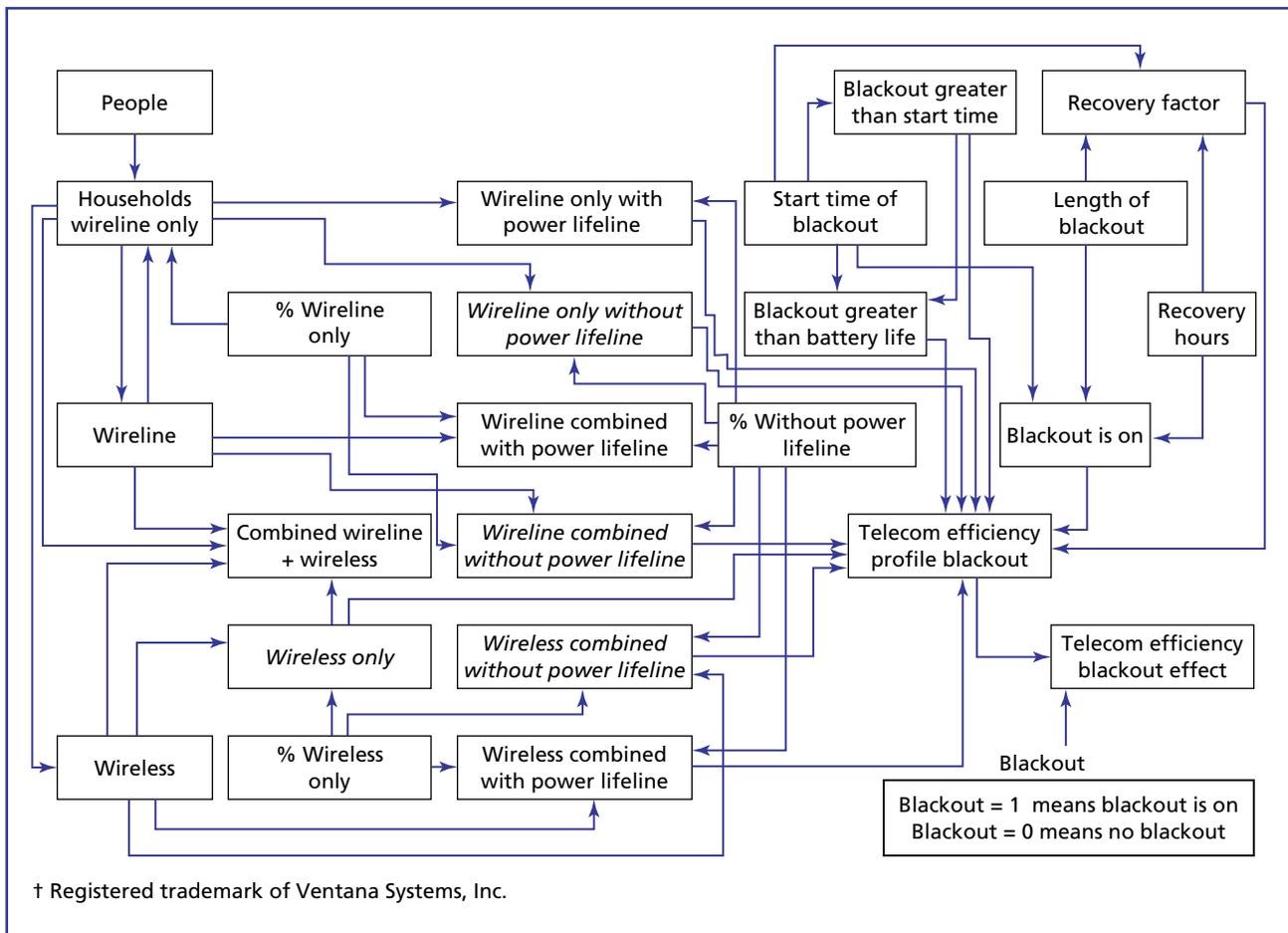


Figure 9.
Vensim[†] model of power blackout.

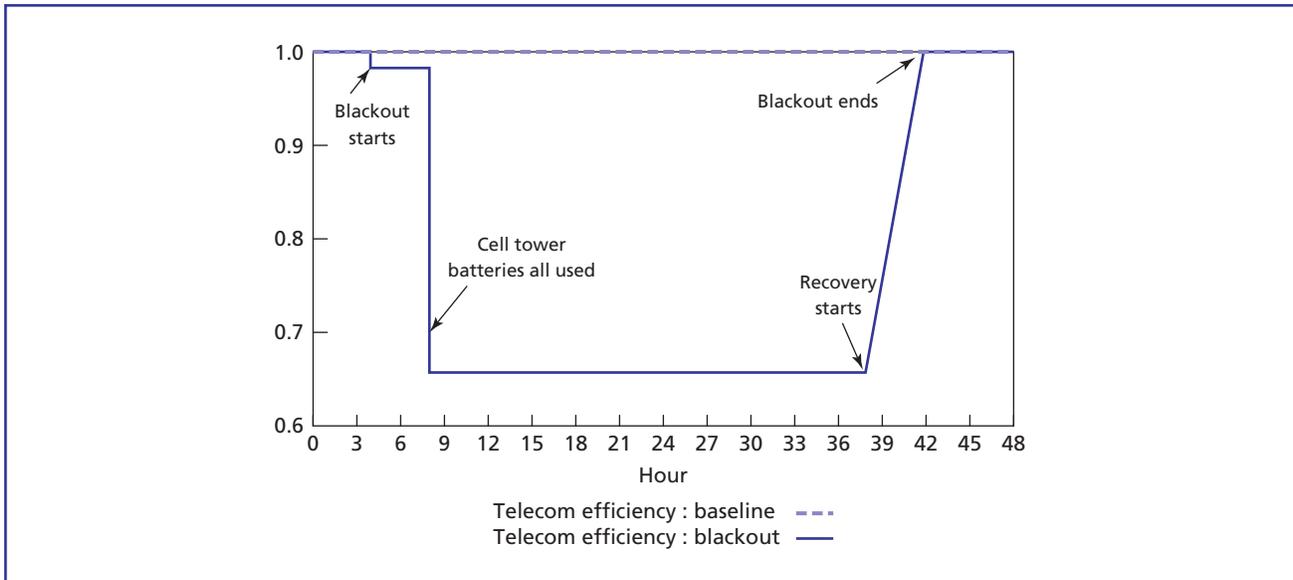


Figure 10.
Network telecom efficiency.

The result of all this is a telecom efficiency function for a given scenario on the right side of Figure 9, explained next.

Network Telecom Efficiency Under Blackout Scenario

Combining the simple blackout model with the forecast of lines throughout the area that are impacted by a power blackout, we get a network telecom efficiency function, which is really a service availability index of customers able to make telephone calls. The dashed line on **Figure 10** is the baseline at 100%, that is, telecom efficiency = 100% for the whole period. Everyone is able to make telephone calls in general, and 911 calls in particular.

The solid line on Figure 10 is the blackout scenario starting at hour 4 and lasting until hour 42 in this example. The blackout starts at hour 4 with a slight dip in telecom efficiency for those wireline-only customers with no power lifeline. Then it dips significantly at hour 8 after all the cell towers run out of back-up power. We modeled this as an instantaneous drop. In reality, it would be spread out over a few hours as different cell towers black out because their battery reserves run down. Note that batteries run down as a function of the amount of calling load. So, if there is a spike in demand for cell usage, the cell towers may last significantly less than 4 hours on their

battery reserve. This telecom efficiency function over time is input into the emergency services model discussed next.

Emergency Services Model

Emergency services consist of police, fire, and medical emergency services. While we could break these down into three categories and deal with each separately, here we simply bundle them together since they are all accessed by calling 911 in an emergency [3]. Approximately 200 million calls are made to 911 each year and one-third are wireless [10]. Some telecom 911 city level calling volumes are included in **Table I**. Notice that the number of 911 calls varies widely between areas.

For our generic metropolitan area of 5 million people, we will assume an average 2.5 calls per person per year. This leads to an average of approximately

Table I. 911 calling by city.

City	Calls per year	Population	Calls/person
Washington	1.8 million	563,000	3.2
Los Angeles	5 million	3,694,000	1.4
Baltimore	1.7 million	651,000	2.6

Table II. Economic cost per injury.

Injury		Illness	
Cost per regular injury:	\$14,250	Cost per regular illness	\$3,562
Cost per major injury:	\$55,500	Cost per major illness	\$13,875
Cost per fatal injury: (death)	\$1,120,000	Cost per fatal illness (death)	\$280,000

34,000 calls per day assuming that the calls are uniformly distributed over the 365 days of the year. We also assume that there is no abnormal increase in emergency calls during the blackout. Nationally, two-thirds of 911 calls are non-emergencies. A non-emergency is one in which there is no dispatch of police, fire, or medical services. So, in the end, with our blackout, many of these non-emergency calls won't get through but they have little impact since there was no emergency in the first place.

Injury Facts and Costs

In 2003, over 20 million people (about 55,000 per day) suffered disabling injuries at home, work, in their community, or while using transportation [11, 12]. In addition, about 2.4 million people (about 6,000 per day) die each year. These statistics represent our baseline conditions when the telecom efficiency index is at 100%.

There are two methods commonly used to measure costs due to injuries and death [12]. One is the economic cost framework and the other is the comprehensive cost framework. Economic costs are a measure of the productivity lost and expenses incurred because of injuries. There are five economic cost components: 1) wage and productivity losses, which include wages, fringe benefits, household production, and travel delay; 2) medical expenses, including emergency service costs; 3) administrative expenses, which include the administrative cost of private and public insurance plus police and legal costs; 4) motor-vehicle damage, including the value of damage to property; and 5) uninsured employer costs for crashes involving workers. The total cost of unintentional injuries in 2003 in the USA was \$607 billion [12]. The comprehensive cost framework includes not only the economic cost components, but also a measure of the value of lost quality of life associated

with the deaths and injuries. Comprehensive costs [12] are generally three times as large as economic costs but we use economic costs only to be conservative in our estimates (**Table II**) [14].

Vensim Model of Emergency Services: 911 Calls

Figure 11 represents the emergency services Vensim model starting on the left with the telecom efficiency function developed previously in Figure 9. It starts on the left with the level of 911 calls (i.e., 0.4 calls per second or 120 calls every 5 minutes). This is consistent with the 34,000 calls per day to 911 assumed to be evenly distributed over the 24 hours in a day.

We then divide the calls into those that get through and those that don't, as a function of telecom efficiency. We next separate out the non-emergencies (66.67%) and assume that police and fire calls are also not included, and then divide the calls into the following categories:

- No injuries
- Regular injury and regular illnesses
- Major injury and major illnesses
- Fatal injury and fatal illnesses (death)

The split between injuries and illnesses (e.g., heart attacks, asthma attacks) is represented by the factor "injury related %." This factor is estimated at 35.5% [12] because

- In 2002 in the USA, there were 38.9 emergency room visits per 100 persons
- Of those, 13.8 or 35.5% of those visits were injury related.

Response Time for 911

The response time to 911 calls in the USA is amazingly fast for those emergency calls that require dispatch. Note that the non-emergency calls don't require dispatch. The response time is tracked for every call, and a measure of effectiveness is the

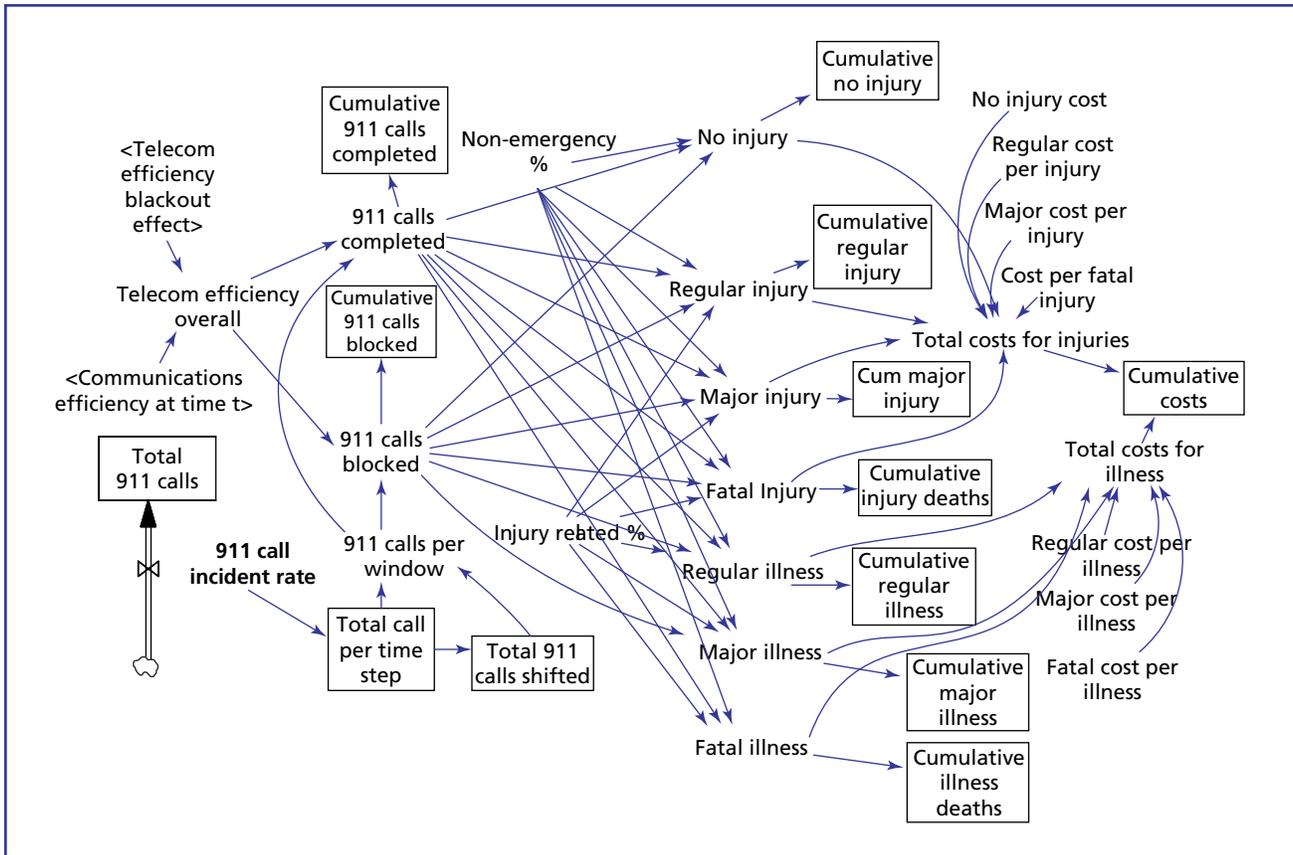


Figure 11.
Emergency services model.

average response time. A typical example is given by Pinellas County, Florida, where response time is approximately 5 minutes from the time of call receipt to dispatch, plus the time to arrive at the scene of the emergency [17]. This is the baseline scenario where all 911 calls are completed through the telecom network. All these calls are ported into one of the following categories: no injury or illness, regular injury or regular illness, major injury or major illness, and fatal injury or fatal illness. The no injury or no illness category is assumed to include all the non-emergency calls (two thirds of all calls). Regular injuries or regular non-injury illness occurs in 70% of the calls, major injuries or major non-injury illness occurs in 29.8% of the calls, and fatal injuries or fatal non-injury illnesses occur in 0.2% of the calls. The major injuries and major illness (29.8%) and the fatal injury and fatal

illness (0.2%) are consistent with national injury and death statistics [12].

The blackout scenario forces us to ask the question: What if the potential 911 callers can't get through because their phone is dead or they have no access to a working phone? Hence, there can be no emergency service response. We postulate changes would occur in the level of injury as follows:

- No injuries category would remain the same.
- Most regular injuries remain regular injuries, but some regular injuries would become major injuries as a function of increased effective response time (or no response in our case). As a result, the fraction of regular injuries relative to total injuries would decrease, while the fraction of major injuries to total injuries would increase.
- Most major injuries remain major injuries but some major injuries would now result in death.

The level of changes to these categories is subject to speculation. In the following, we have assumed that the fraction of overall regular injuries would go down (to 44% from 70% in the baseline), since many regular injuries would become major injuries. The fraction of major injuries would increase to 55.6% from 29.8% in the baseline, and the fraction of fatal injuries would increase as well (to 0.4% from 0.2% in the baseline) since some of those major injuries would result in fatality. These transition levels require further investigation. We further assume that the same process would work for illnesses. They would become more serious or fatal with significant delays in 911 response.

We wish to note that modeling could have been improved if the frequency distribution of response times, as well as emergency response outcome as a function of response time, had been available. In addition, a classification from recognized medical authorities—one that classifies injuries in a way similar to our categories of regular and major injuries, and then lists the most common injuries in those categories, along with some medical opinion/prediction about the impact of non-treatment after 2 hours, 4 hours, 10 hours, or 20 hours—would also assist in modeling future scenarios.

Summary Results: Injuries and Cost

The results below show a comparison between the baseline model where electric power, telecom, and 911 calling are operating normally, and the blackout scenario where a significant fraction of the population—or approximately 35%—can't call 911, as shown on Figure 10. Here, there is no specific damage to the telecom infrastructure, other than that caused by the lack of power to use their wireless or cordless telephones.

Figure 12 shows injuries and their cost in baseline vs. blackout scenarios. Figure 12a shows changes in injury levels, while Figure 12b shows the overall cost results of injuries. While the costs attributed to regular injury decreased somewhat because there are less regular injuries, the costs for major injury increased since there are many more of them. In addition, the fatal injury (death) category also shows an

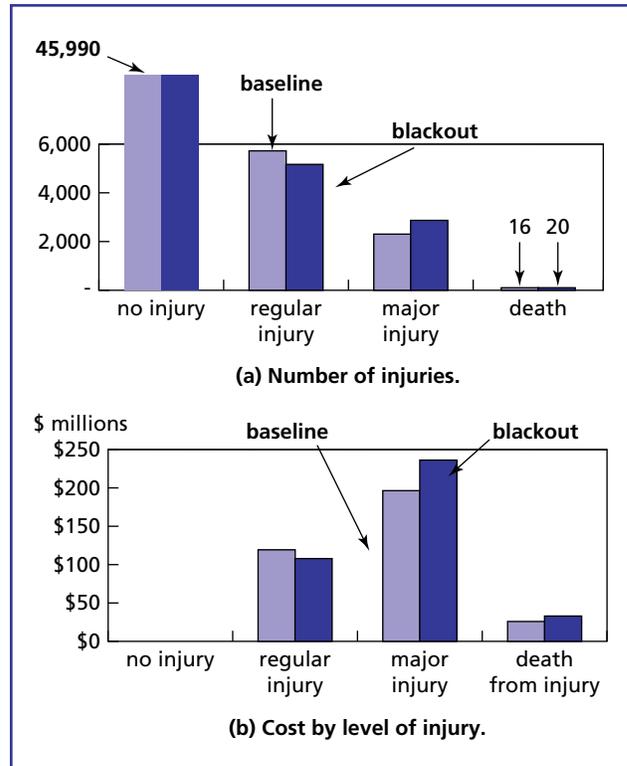


Figure 12. Injuries and their cost in baseline vs. blackout scenarios.

increase. The summary costs for each of the scenarios are shown in **Table III**.

The bottom line is that there is a substantial increase in injuries, non-injuries, and death and increases in those corresponding economic costs. For a blackout lasting approximately 34 hours, for a metropolitan area of 5 million people, the incremental economic cost is estimated at \$36M.

Sensitivity Study: Blackout + Telecom Disruption

So far, we have investigated two scenarios:

1. *Baseline scenario*, or no blackout, and
2. Blackout scenario.

Table III. Summary costs.

Baseline total =	\$342 M
Blackout total =	\$378 M
Incremental cost =	\$ 36 M

Table IV. Summary costs.

Baseline total =	\$342 M
Blackout and telecom disruption total =	\$405 M
Incremental cost =	\$ 63 M

In both of these scenarios, we assumed there was no simultaneous infrastructure damage to the telecom network, except for that caused by lack of power. In this sensitivity study, we add a telecom disruption, perhaps caused by hurricane or earthquake, to the whole network lasting from 8 AM to 10 PM or a 14 hour disruption on day 1 of our two day period, which knocks out 75% of the network capacity. The additional scenario with both blackout and telecom damage reduces the overall telecom efficiency to very low levels during the periods of blackout and telecom disruption. Hence very few 911 calls get through during this period. This results in more major injuries and more fatal injuries. **Table IV** shows the summary costs for this combined infrastructure disruption. The costs are increased to \$63M over baseline, almost double that of the blackout only scenario. As such, the incremental impact of the telecom disruption on top of the blackout would be \$27M.

Sensitivity Study: Length of Blackout and Percentage of Population with No Power Lifeline

Figure 13 shows a sensitivity study where the blackout is extended to multiple days, and where the percentage of the population without power lifeline for telecom services is increased. The results show dramatic increases in the consequences of this disruption in the hundreds of millions of dollars.

Results such as this lead us to ask how to mitigate against such potential outcomes since blackouts of these magnitudes are likely to occur especially when considering long time frames. What mitigation is possible to guarantee access to 911? One customer-initiated mitigation already recommended by telcos is for those wireline customers with cordless phones to also have one wired phone. This mitigation would also apply to wireless-only customers but then they wouldn't be wireless-only in this case.

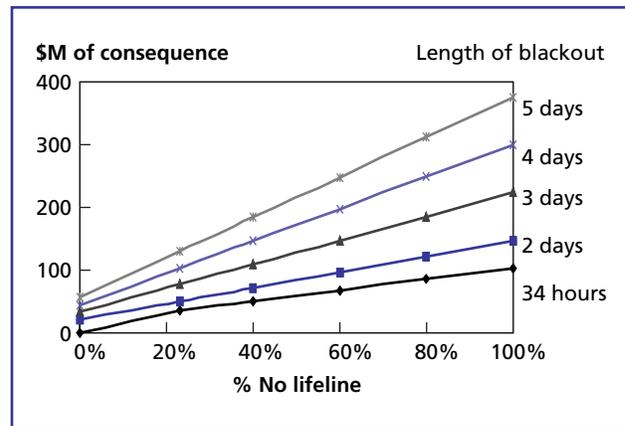


Figure 13. Consequence sensitivity vs. length of blackout and percentage of population with no lifeline.

Another partial solution is battery back-up for multiple days at cell sites at high load, or diesel generators installed at cell sites. The cost of this mitigation is substantial. For example, a small generator might cost \$50,000. Assuming there are 500 cell sites spread throughout our metropolitan area, the mitigation cost would be \$25 million. Going back to Figure 1, if the likelihood of this event was 10% over a long time horizon of decades, and the consequence was \$250 million, then a \$25 million investment in this mitigation might be appropriate.

Conclusions and Future Extensions

This paper presented an example of the work that is currently under way at the National Infrastructure Simulation and Analysis Center. Sandia National Laboratories, Los Alamos National Laboratory, and Bell Laboratories/Lucent Technologies are continuing to develop inter-infrastructure simulation models, extending them with analysis of information and telecommunication networks interactions with other critical infrastructures.

There are a number of important areas to continue this research:

- Investigate the rate of change in injuries as a function of 911 response time due to all sources of emergency: police, fire, and emergency medical services.
- Investigate the general business costs of a power blackout resulting in loss of telecommunications

services. In some industries, for example, airline reservations, this has been estimated at \$1 million per hour. The general business costs should be much larger in our example than for the emergency services infrastructure. For example, the August 14, 2003, blackout affected 50 million people, lasted up to 4 days in various parts of the USA and Canada, and with estimated costs between \$4 billion and \$10 billion. In such a blackout, affecting a metro area of 5 million people, this would translate to an impact of between \$400 million to \$1 billion.

Acknowledgements

We would like to thank our colleagues at Bell Labs, Sandia, Argonne, and Los Alamos National Labs, and especially Theresa Brown and Sharon Deland for providing insight and direction to many of our efforts.

Note

The National Infrastructure Simulation and Analysis Center is a joint program at Sandia National Laboratories and Los Alamos National Laboratory, funded and managed by the U.S. Department of Homeland Security's (DHS) Preparedness Directorate. The views contained in this paper are those of the authors and do not represent the official views of DHS.

*Trademarks

Vensim is a registered trademark of Ventana Systems, Inc.

References

- [1] W. E. Beyeler, S. H. Conrad, T. F. Corbet, G. P. O'Reilly, and D. D. Picklesimer, "Inter-Infrastructure Modeling—Ports and Telecommunications," *Bell Labs Tech. J.*, 9:2 (2004), 91–105.
- [2] S. H. Conrad, W. Beyeler, R. Thomas, T. F. Corbet, T. Brown, G. B. Hirsch, and C. Hatzi, "How Do We Increase Port Security Without Imperiling Maritime Commerce? Using Flight Simulators and Workshops to Begin the Discussion," *Proc. 21st Internat. System Dynamics Conf.* (New York, 2003).
- [3] *Dispatch Monthly Magazine*, <<http://www.911dispatch.com/index.html>>.
- [4] J. W. Forrester, *Urban Dynamics*, Productivity Press, Portland, OR, 1969.
- [5] F. J. Governali, J. Armstrong, D. Zimmerman, Goldman Sachs, *Global Investment Research Report, Telecom Services, Wireline and Broadband*, Apr. 16, 2004.
- [6] D. J. Houck, E. Kim, G. P. O'Reilly, D. D. Picklesimer, and H. Uzunalioglu, "A Network Survivability Model for Critical National Infrastructures," *Bell Labs Tech. J.*, 8:4 (2004), 153–172.
- [7] A. Jrad, H. Uzunalioglu, D. J. Houck, G. O'Reilly, S. Conrad, and W. Beyeler, "Wireless and Wireline Network Interactions in Disaster Scenarios," *Military Commun. Conf. (MILCOM '05)* (Atlantic City, NJ, 2005), pp. 1–7.
- [8] R. J. LeClaire, B. W. Bush, L. Dauelsberg, J. Fair, D. Powell, S. M. Deland, W. E. Beyeler, H. Min, R. Raynor, M. E. Samsa, R. Whitfield, and G. Hirsch, "Critical Infrastructure Protection Decision Support System Evaluation of a Biological Scenario," *Working Together: R&D Partnerships in Homeland Security Conf.* (Boston, MA, 2005).
- [9] R. J. LeClaire and G. O'Reilly, "Leveraging a High Fidelity Switched Network Model to Inform System Dynamics Model of the Telecommunications Infrastructure," *Proc. 23rd Internat. System Dynamics Conf.* (Boston, MA, 2005).
- [10] National Emergency Number Association, <<http://www.nena.org/pages/ContentList.asp?CTID=23>>.
- [11] National Safety Council (NSC), "American National Standard—Manual on Classification of Motor Vehicle Traffic Accidents," American National Standards Institute (ANSI) D16.1-1996, 6th ed., 1996, <http://www.nsc.org/public/mem/ansid16_1.pdf>.
- [12] National Safety Council (NSC), *Injury Facts*, NSC, Itasca, IL, 2004.
- [13] G. O'Reilly, D. Houck, F. Bastry, A. Jrad, H. Uzunalioglu, W. Beyeler, T. Brown, and S. Conrad, "Modeling Interdependencies Between Communications and Critical Infrastructures," *Working Together: R&D Partnerships in Homeland Security Conf.* (Boston, MA, 2005).
- [14] G. O'Reilly, H. Uzunalioglu, S. Conrad, and W. Beyeler, "Inter-Infrastructure Simulations Across Telecom, Power, and Emergency Services," *Proc. 5th Internat. Workshop on Design of Reliable Commun. Networks (DRCN '05)* (Ischia, It., 2005).

- [15] G. P. O'Reilly, D. J. Houck, E. Kim, T. B. Morawski, D. D. Picklesimer, and H. Uzunalioglu, "Infrastructure Simulations of Disaster Scenarios," Proc. 11th Internat. Telecommun. Network Strategy and Planning Symposium (Networks '04) (Vienna, Aus., 2004), pp. 205–210.
- [16] G. P. O'Reilly, H. Uzunalioglu, D. J. Houck, and T. B. Morawski, "A Dynamic Simulation Approach to Business Continuity of Wireline and Wireless Networks with Cross-Industry Infrastructures," Proc. IEEE Internat. Conf. on Commun. (ICC '05) (Seoul, Korea, 2005), vol. 1, pp. 328–332.
- [17] Pinellas County, FL, <<http://www.ci.tarpon-springs.fl.us/911.htm>>.
- [18] M. Richtel, "Dangling Broadband from the Phone Stick," New York Times, Mar. 19, 2005, C1.
- [19] J. D. Sterman, Business Dynamics: Systems Thinking and Modeling for a Complex World, Irwin/McGraw-Hill, Boston, MA, 2000.
- [20] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, Apr. 2004, <<https://reports.energy.gov/BlackoutFinal-Web.pdf>>.
- [21] United States, The White House, National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Washington, DC, Feb. 2003, pp. 6, 47–79, <<http://www.whitehouse.gov/pcipb/physical.html>>.
- [22] Vensim, <<http://www.vensim.com>>.

(Manuscript approved May 2006)

STEPHEN H. CONRAD is a principal member of the technical staff in the Critical Infrastructure Surety Department at Sandia National Laboratories in Albuquerque, New Mexico. He holds a B.A. from West Virginia University and an M.S. and Ph.D. from the New Mexico Institute of Mining and Technology. Dr. Conrad works as an analyst for the National Infrastructure Simulation and Analysis Center (NISAC) where he is developing modeling tools for evaluating infrastructure interdependencies and system vulnerabilities. Prior to joining NISAC, he worked on various problems in the areas of hydrology, probabilistic performance assessments for radioactive waste disposal, and systems analysis.



RENE J. LECLAIRE is a staff member in the CIP/DSS project in the Decision Analysis division at Los Alamos National Laboratory. His work has focused particularly on the telecommunications and banking and finance infrastructures and, most recently, on infectious disease modeling using system dynamics. He holds B.S. and M.S. degrees from the University of Lowell and an Sc.D. from the Massachusetts Institute of Technology. Dr. LeClaire started his career at Los Alamos National Laboratory (LANL) performing system analyses in a variety of technologies. In 1989 he left Los Alamos to work at several start up companies including the Center for Adaptive Systems Applications (CASA), specializing in applying advanced datamining techniques and simulations for large financial institutions. He returned to LANL in 2000.



GERARD P. O'REILLY is a distinguished member of technical staff in the High Reliability Network Architecture and Services Group at Bell Labs in Holmdel, New Jersey, where he is focusing on network reliability modeling and best practices, business continuity, and disaster recovery. He holds a B.S. in mathematics from Manhattan College, New York, and an M.S. and Eng.Sc.D. in operations research, both from Columbia University in New York. He is currently an Adjunct Professor at Stevens Institute of Technology, teaching Switching and Signaling. Dr. O'Reilly served for 12 years as Associate Editor of Switching for the IEEE Transactions on Communications. He has published numerous papers and holds two patents, with several in process. Dr. O'Reilly's research interests include reliability and performance of networks and switching technology evolution.



HUSEYIN UZUNALIOGLU is a member of technical staff in the QoS Management and Assessment Group at Lucent Technologies in Holmdel, New Jersey. He holds B.S. and M.S. degrees from the Middle East Technical University in Ankara, Turkey, and a Ph.D. degree from the Georgia Institute of Technology in Atlanta, all in electrical and computer engineering. A member of the IEEE, Dr. Uzunalioglu includes performance modeling of IP and ATM networks, QoS, voice over IP, and wireless networking among his current research interests. ♦

