# Cyber–Physical Vulnerability Assessment of the Colonial Pipeline Using MBRA and Fault Tree Analysis

**Tanishka Kiran Chitnis**
Graduate Student – MS in Cybersecurity
Khoury College of Computer Sciences
Northeastern University
Boston, Massachusetts, USA

Email: chitnis.t@northeastern.edu

**Submitted To**
Secretary of the U.S. Department of Homeland Security (DHS)
Washington, D.C., USA

Course: CY 5250 – Decision Making in Critical Infrastructure
Instructor: Themis A. Papageorge
Date: 2nd December 2025

# Table of Contents:

# Colonial Pipeline Network:

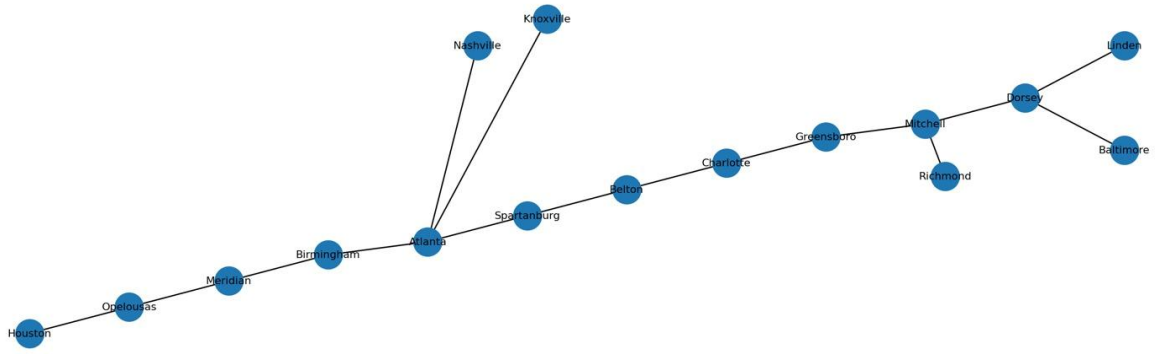



***Figure 1 – Network Graph***

Colonial Pipeline runs from Houston to New York Harbour, which has a total length of 5,500 miles which carries gasoline, diesel, jet fuel, and other products manufactured by petroleum over the eastern cost of the United States through a system of mainlines, junctions, pumping stations, tank farms and terminals (Colonial Pipeline Company, 2024). The pipeline carries approximately one hundred million gallons of fuel daily to meet almost half (45%) of the total fuel needs of the eastern United States (Colonial Pipeline Company, 2024; EIA, 2021). As it accounts for most of the supply because of its extensive reach and importance to the economy, any problems with this pipeline will result in widespread regional shortages, delays in supply, and/or severe impact on operational, economic, and/or national global security throughout the eastern United States. This was practically exhibited in the ransomware attack.

This paper conducts an analysis on the Colonial Pipeline Network in the east coast, with Houston designated as the initial supply point and Linden as the final endpoint. The network is represented with sixteen nodes i.e., Houston, Opelousas, Meridian, Birmingham, Atlanta, Belton, Charlotte, Spartanburg, Greensboro, Mitchell, Richmond, Dorsey, Baltimore, Nashville, Knoxville, and Linden. Richmond is a branch of Mitchell and Baltimore is a branch of Dorsey.

The design of this network is such that there is a dependency between the physical infrastructure, and how it interacts with the various digital systems required to run that infrastructure. In many cases, oil and gas companies are now beginning to use Supervisory Control And Data Acquisition (SCADA) platforms, as well as a growing number of Industrial Internet Of Things (IIoT) devices, to enable their operations to be more efficient than they were with the older style of OT networks, which were previously set up as "air-gapped" systems (ENTELEC, 2021; Fortinet, 2023). By modernizing their environments and connecting OT systems to enterprise IT systems, companies have become vulnerable to threat actors. (Fortinet, 2025). Because of this increase in interconnectedness between OT and IT systems, it has become much easier for a cyber-attack to cause severe disruption to a company's operations using digital controls on a company's physical infrastructure. Thus, there is potential for a cyber-attack on a pipeline company to create much larger impacts throughout the entire pipeline company system (ENTELEC,2021; Fortinet, 2024).

Due to the dual nature of cyber and physical risks to modern infrastructure, cyber risks are analysed separately from physical disruption risks. Cybersecurity risks are represented using a cascade network. This framing is appropriate since once a digital breach occurs; any compromised performance can propagate in both directions through interconnected control systems. Physical threats are represented using a flow-based network representation, which captures how pipe failures can propagate downstream with the flow of fuel. These two network representations allow for a more realistic approach to assessing vulnerability and risk mitigation strategies. The following is going to be the flow of the study; the cyber and physical threats are analysed separately using Cascade and Flow networks. The cascade and flow networks are going to be first represented through an adjacency matrix whose primary intention is to show the connections between the node and the links. Through the adjacency matrix, network parameters will be derived such as node degrees, network degree, link

robustness, and links that can and cannot be removed (critical links), spectral radius, node robustness and nodes than can be removed and blocking nodes that cannot be removed. Node centrality, betweenness centrality (node betweenness centrality and link betweenness centrality most critical metrics for Flow networks), and eigenvector centrality rankings. The above parameters will be calculated for both the networks. From these parameters the fractal dimension and critical vulnerability will be derived these two important parameters will indicate the cascading effect of the networks.
Furthermore, threat probability, vulnerability, consequences, elimination, and response cost will be calculated. These parameters will be simulated in the MBRA tool. This tool will help us understand the critical nodes in both the network and Risk reduction based on allocation of budgets to Prevention and Response controls. Physical and threat vulnerabilities will be identified. Based on the critical nodes derived in the simulation, the physical and threat vulnerabilities will be simulated in the fault tree as a top-down approach to under the budget allocation for a node in case of a threat. The above analysis will provide a strong foundation for computing the budget estimation and prevention controls.

# Cascade Adjacency Matrix (Undirected Cyber Dependency):

The cascade adjacency matrix below shows the network in conditions of being under a cyber-attack where compromise can head in either direction and travel backward or forward through digital control, SCADA, or interdependent operational software. It is for this reason the cascade adjacency matrix is bidirectional. If Houston communicates with Opelousas, the bidirectional matrix will provide "1" for Houston → Opelousas as well as for Opelousas → Houston. Therefore, in this representation, each "1" demonstrates mutual reachability in digital control - a malware, ransomware, or supply-chain based compromise can flow in both directions between the respective connected assets. From the observations of the cascade matrix:

- Houston ↔ Opelousas ↔ Meridian ↔ Birmingham is the main control backbone.
- Atlanta functions as a larger cyber junction with Belton, Nashville, and Knoxville connected.
- Mitchell ↔ Dorsey ↔ Baltimore ↔ Linden creates another dependent digital chain.

Because cyber compromise can propagate regardless of the physical flow direction, the cascade adjacency matrix demonstrates how quickly a cyber-infection or unauthorized cyber-activity can transfer from zone to area to location to zone.

# Matrix for Cascade Network:

| Adjacency matrix | Houston | Opelousas | Meridian | Birmingham | Atlanta | Belton | Charlotte | Spartanburg | Greensboro | Mitchell | Richmond | Dorsey | Baltimore | Nashville | Knoxville | Linden |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Houston | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Opelousas | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Meridian | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Birmingham | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Atlanta | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| Belton | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Charlotte | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Spartanburg | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Greensboro | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| Mitchell | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| Richmond | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| Dorsey | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| Baltimore | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| Nashville | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Knoxville | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Linden | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

# Flow Adjacency Matrix (Directional Physical Dependency):

The below flow adjacency matrix represents the physical flow of refined fuel, which is inherently one-way, only toward Linden over long-distance (Houston being the only point of origin). This is a representation suitable for analysis of physical threats such as sabotage, destruction of valves, ruptured pipelines, or theft/vandalism.

In this representation, a “1” indicates flow is going from upstream → downstream, but not in reverse. In other words:
Houston → Opelousas → Meridian → Birmingham → Atlanta is demonstrating that the mainline trunk is coming from Houston going toward Linden.
After Atlanta, the flow branches off toward Belton (going east) and Nashville/Knoxtown (uplink laterals).
The terminal of the flow chain is Greensboro → Mitchell → Dorsey → Linden.
Important for understanding this physical adjacency matrix is the role it plays in physical vulnerability analysis; the physical threats can only propagate downstream. For example, if the flow chains at Houston ruptures, then flow is stopped. If the flow chains at Mitchell ruptures, then the flow chain stops at Mitchell, thereby impeding supply for its downstream nodes, not the entire system.

| Adjacency matrix | Houston | Opelousas | Meridian | Birmingham | Atlanta | Belton | Charlotte | Spartanburg | Greensboro | Mitchell | Richmond | Dorsey | Baltimore | Nashville | Knoxville | Linden |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Houston** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Opelousas** | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Meridian** | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Birmingham** | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Atlanta** | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| **Belton** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Charlotte** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Spartanburg** | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Greensboro** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Mitchell** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| **Richmond** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Dorsey** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| **Baltimore** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Nashville** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Knoxville** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Linden** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

# Cascade Network Analysis:

The node degrees show the number of direct connections between the different locations. Most of the pipeline nodes have a low degree of 1 or 2, which is a consequence of the pipeline infrastructure being linear. Only a few nodes stand out, such as Atlanta with the highest degree of four as the main junction point of the network, Mitchell, and Dorsey each with a degree of three. These degrees already indicate that the network is sparse, with a few focal hubs and many direct relay points.

The network consists of sixteen nodes and fifteen undirected links and represents a tree structure (meaning if any one of these links fails, there is limited alternative flow routes). The link robustness is indicated by a value of 0.5, or said another way, only half of the links can be removed without breaking large sections of the pipeline into separated pieces. In fact, only seven of the links can be removed, while the remaining links are in fact critical links which if removed would also separate part of pipeline into separate components. For a physical pipeline, the links can also be considered single points of failure where an outage of any of them would cause the fuel flow downstream to stop.

The potential for cascading failures indicated by the spectral radius is 2.20, Even though pipelines are linear networks, and do not have any redundant paths, a failure of a central point can cause failures throughout the entire linkage.

A low spectral radius indicates that the network cannot be percolated, and it would indicate that it is a flat network. The node resilience score of 0.545 suggests the network could support random failures in approximately 50% of the number of total nodes before reaching a threshold for failure or catastrophe. The number of blocking nodes is equal to 8 as there are sixteen nodes in total and eight cannot be removed. The flow at those nodes would result in a loss to flow at any of the blocked node locations.

Degree centrality shows that Atlanta is the most connected node, while the betweenness centrality score shows that Atlanta is ranked first, with Belton, Charlotte, Spartanburg, and Greensboro ranked next, in order. These four nodes are directly part of the flow at the main pathway from west to east or vice-versa, and its management as a bottleneck is critical, because any problem at any of these points may disrupt the entire system.

The eigenvector measure of centrality follows and confirms this pattern, with Atlanta being the core of the network, and Birmingham, Belton, Charlotte, and Nashville as the most important after Atlanta. Overall, the cascade network analysis shows that through the lack of alternate routes, the system will be highly vulnerable, wherein a disruption will very quickly cascade east or west compromising a large portion of the eastern or western supply within the system.

# Flow Network Analysis:

In the flow network model, the Colonial Pipeline operates as a directed system with Houston as the starting point and travels step-by-step toward Linden with multiple other nodes in between. The degree results display this directional arrangement; in most cases, nodes have a single outgoing link indicating one handoff of flow from a location to a node. The exception to this finding is Atlanta, which does report an out-degree of three, which aligns with its important role in the operation as Atlanta is a huge branch point connecting to Belton, Nashville, and Knoxville. Downstream flow continues to Belton, Spartanburg, Charlotte, Greensboro, Mitchell, and Dorsey arriving at Linden at the bottom of the flow.

A network degree of three confirms that Atlanta is the most active junction in the network. There is a total of sixteen nodes in the pipeline along with seven effective undirected links which configure a narrow, tree-like, network backbone shape. The link robustness value of 0.33 along with the fact that there are only two links that can be eliminated before disconnecting, indicates how structurally limited this pipeline system is. Exceptions being side branches such as the Dorsey-Baltimore and Atlanta-Nashville and Atlanta-Knoxville.

The spectral radius of 0.0 is typical of a strictly directed, acyclic flow network. There are no loops or feedback cycles in the pipeline and, therefore any disturbances hinder the supply to downstream nodes. This structural characteristic also contributes to the low resilience of the network in connection to node removal.

Robustness of the nodes was calculated as zero, which means that no node could be removed without impacting some proportion of the system's connectivity. Each of the sixteen nodes functions as a blocking node in the context of the flow. There cannot be redundancy every city is important towards functional completeness.

Centrality metrics provide additional insight into how individual nodes are operationally critical. Degree centrality suggests again that Atlanta is the main structural hub and is followed by Belton, Mitchell, and Dorsey manage either transitions or flow into the downstream segments. Betweenness centrality suggests the same ordering: Atlanta has the highest betweenness followed by Belton, Spartanburg, Charlotte, Greensboro, and Mitchell. All these nodes have a high measure because they are located on most directed paths throughout the system. Each of these nodes effectively acts as a chokepoint for flow across the system.
Eigen vector measures the influence of a node in a network and scores relative is assigned based on other nodes connections to each other. Like the previous analysis, Atlanta is the most prominent node, followed by

Birmingham, Belton, Spartanburg, and even Nashville and Knoxville. Their high values signify that they are part of substructures connected to nodes that carry significant influence, which is Atlanta, thereby increasing their potential to be a system that support overall functioning.

# Cascade Resilience Equation:

The resilience equation is as follows:
Resilience Equation for resilience line = log(q) = b + k * gamma * ro
Here q stands for fractal dimension
Gamma stands for vulnerability
Ro stands for spectral radius
B and k are the constants
Two sample Vulnerability values are considered, for the cascade network vulnerability 90% and 20% is considered. With estimated threat, consequence, elimination, and response cost the values are simulated in the MBRA tool through with fractal dimension is calculated. The fractal dimension of vulnerability 90% is as follows:

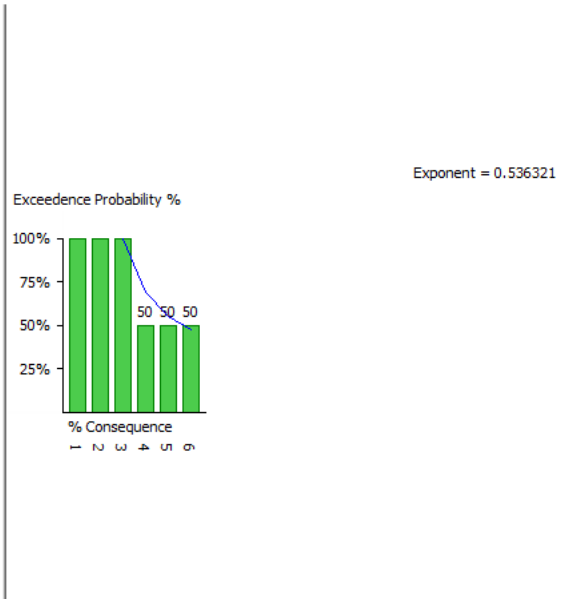



***Figure 2 – Fractal dimension of cascade network at 90% vulnerability***

The fractal dimension of vulnerability 20% is as follows:

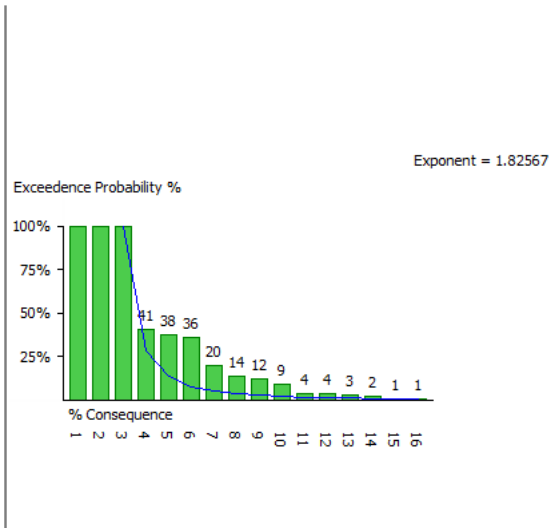



***Figure 3 – Fractal dimension of cascade network at 20% vulnerability***

Two algebraic equations are produced which is substituted to calculate the b and k values.
The spectral radius of the cascade system is 2.2 and a calculated critical vulnerability of 3.20 means the cascade network has limited tolerance of increasing stress. The decline in log(q) as calculated from increasing vulnerability values indicates limited resilience and increased fragility to cascading disturbance.

| Gamma | q | log(q) | gammra*ro |
|---|---|---|---|
| 0.20 | 1.83 | 0.26 | 0.44 |
| 0.90 | 0.54 | -0.27 | 1.98 |

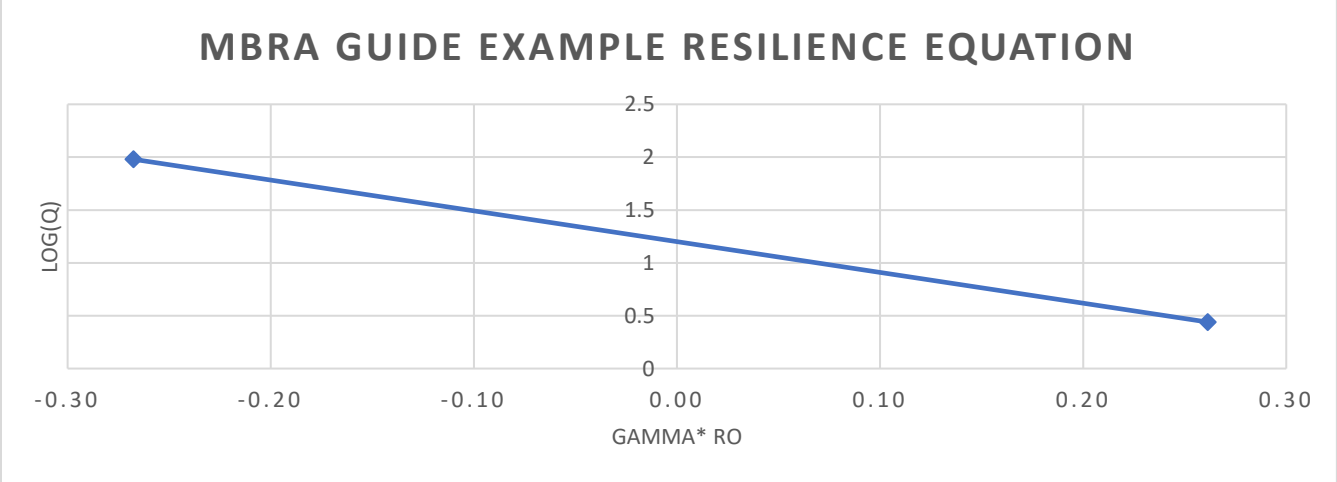



***Figure 4 – Cascade network resilience line***

# Flow Network Resilience Equation:

In the flow network the spectral radius is 0, which reduces the resilience equation to log(q) = b, as spectral * vulnerability value is less than 1 fault spreading dies out. The following fractal dimension q values were observed for flow network:

Vulnerability 10%

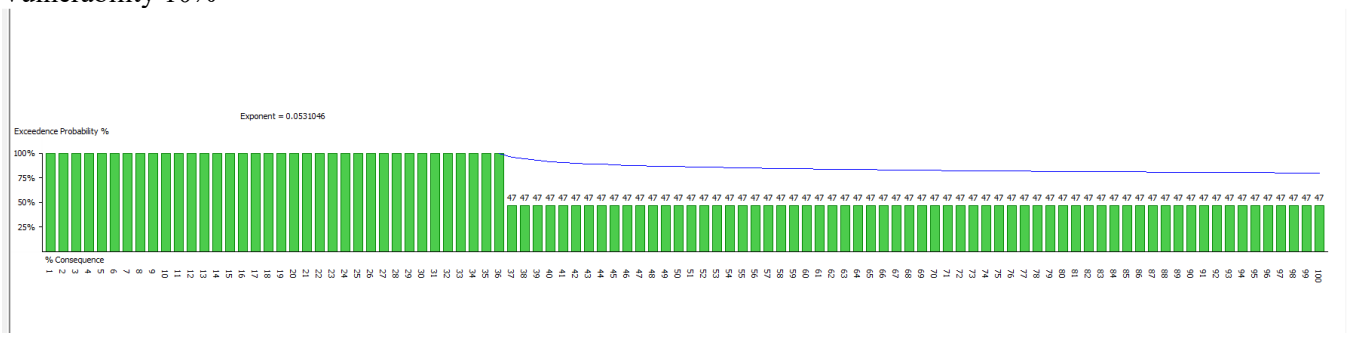



***Figure 5 – Fractal dimension of flow network at 10% vulnerability***

Vulnerability 20%

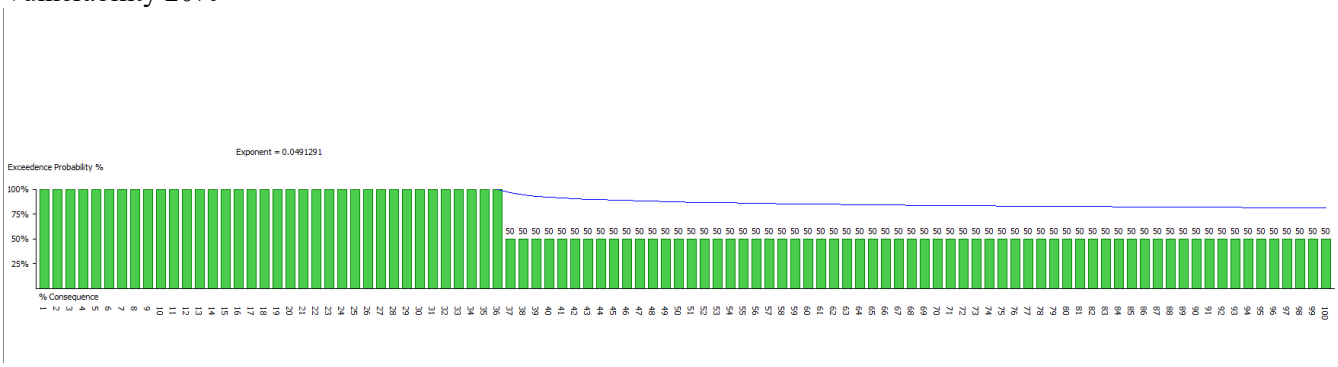



***Figure 6 – Fractal dimension of flow network at 20% vulnerability***

Vulnerability 52%

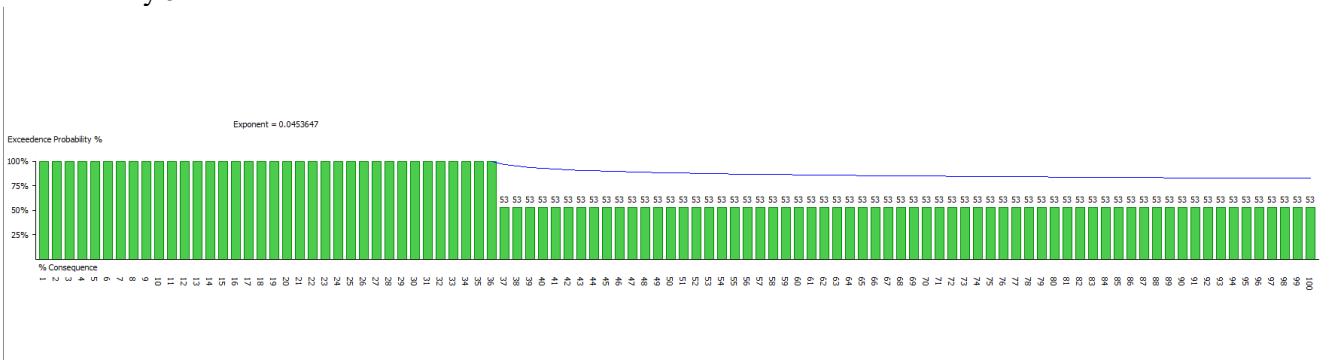



***Figure 7 – Fractal dimension of flow network at 52% vulnerability***

Vulnerability 61%

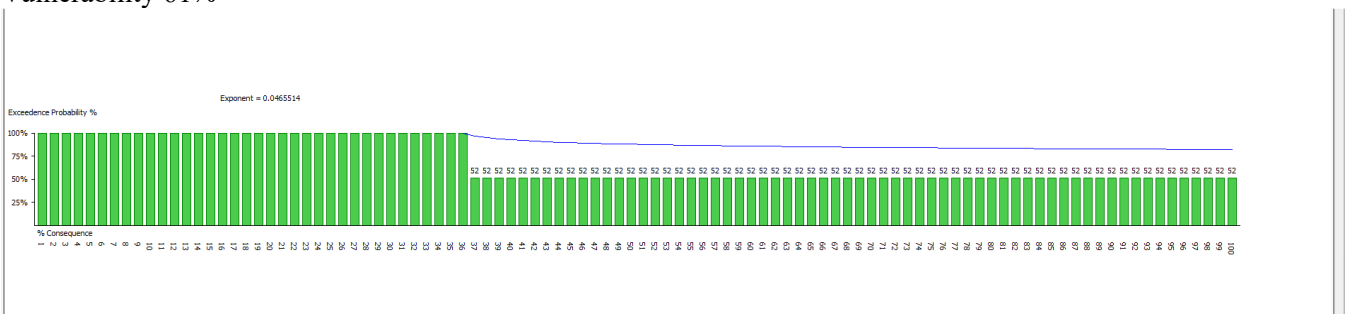



***Figure 8 – Fractal dimension of flow network at 61% vulnerability***

Vulnerability 73%

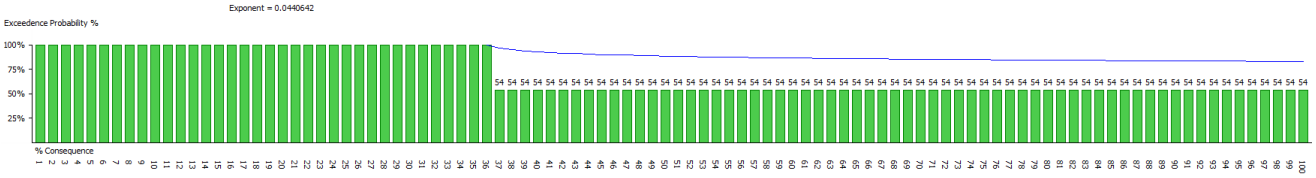



***Figure 9 – Fractal dimension of flow network at 73% vulnerability***

Vulnerability 80%

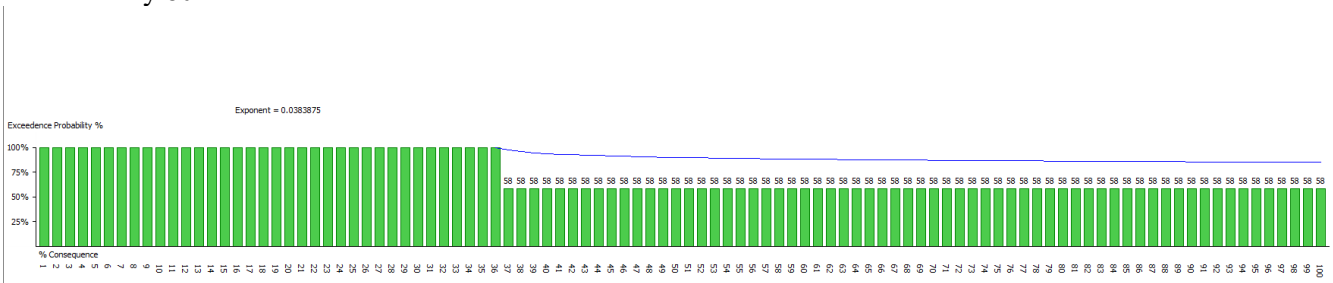



***Figure 10 – Fractal dimension of flow network at 80% vulnerability***

The above values of vulnerability and fractal dimension which was derived after simulating the MBRA were substituted in the log(q) = b

| Gamma | q | log(q) |
|---|---|---|
| 0.10 | 0.053 | -1.28 |
| 0.20 | 0.049 | -1.31 |
| 0.52 | 0.047 | -1.33 |
| 0.61 | 0.045 | -1.35 |
| 0.73 | 0.044 | -1.36 |
| 0.80 | 0.380 | -0.42 |

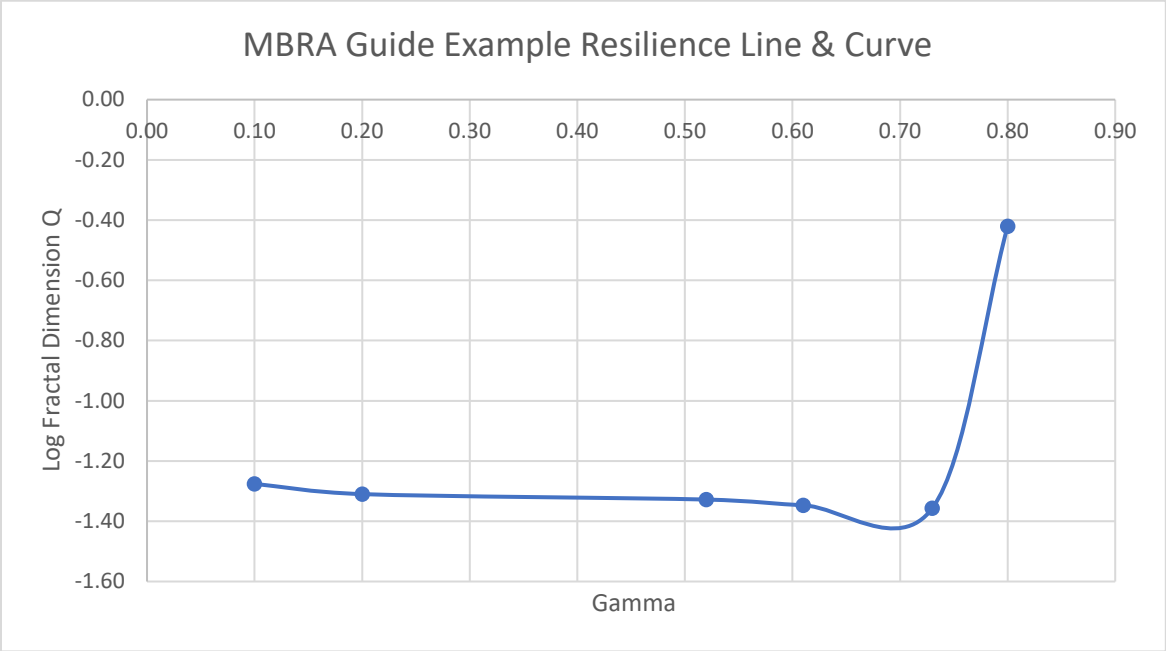



***Figure 11 – Flow network resilience curve***

The resilience curve for the flow network indicates that log(q) is typically small as a function of γ, which indicates weak robustness and structure that is more sensitive to vulnerabilities. The gradual decline in q by γ indicates continuous degradation of flow capacity, while the sharp improvement at vulnerability γ = 0.80 suggests a threshold effect where a small subset of nodes remains functional despite upstream disruption. The resilience suddenly rises at γ = 0.80 and indicates a threshold effect as very few nodes are able still functioning despite upstream disruption. Overall, the flow network does not have much resilience and redundancy.

# Cyber Threat, Vulnerability, Consequences, Prevention Costs ($), and Response Costs ($) for Cascade Network:

Cyber threat probabilities were rated 100% for all network links and nodes, because modern pipeline OT/IT environments are consistently being probed externally, subjected to ransomware campaigns, and having credentials spoofed. As these threats are not limited by geographic area, every node in the communications network is under the same threat level. Each node (Houston, Atlanta, Birmingham, etc.) was assigned the same cyber vulnerability level of 30%, and vulnerability level is common for a centralized industrial control environment as there are system-wide configurations, shared authentication, and legacy OT assets that create similar levels of vulnerability conditions across all nodes and system components.

Cyber vulnerability for links was treated differently due to the topology role represented by the link being backbone and trunk links carry greater traffic and are coordinating larger segments of the system, there are higher dependency of flows, and ultimately threat vectors are typically seeking segments that can create the largest operational, or economic impact in the event of a cyber-attack. Disrupting certain links could isolate the entire sub-networks from one another, or sever the main flow, source to destination, whereas affecting certain links might only affect a peripheral branch only. Example, the colonial pipeline ransomware attack majorly affected the North-East region.

The result from the cyber-attack was approximately $11.15 million in consequence, created by summation of costs associated with cyber-induced disruption. This included an estimated downtime value of approximately $3.6

million (for 24 hours of disruption at $150k/hour) (Ransomware.org, 2022; NE Digital, 2023), a ransom amount of approximately $4.5 million (ABS Group, 2021), IT/OT recovery estimates of $2.8 million (Cybersecurity Magazine, 2022), and approximately $0.25 million in regulatory fines and fees (PHMSA, 2025; Industrial Cyber, 2023). Consequences then at the node and link node levels were assumed based on flow criticality and downstream dependency (example of node type - hub, trunk, junction, peripheral branch choice). This establishes the rationale why Houston and Atlanta for example realized impacts on the order of over $10M, backbone links (links contributing to flow) around $7-$8 million each and peripheral links around $6 million each. Cybersecurity budget for Colonial Pipeline was approximately 40 million dollars pre-attack (Ransomware.org), 2022. Given that as constraints, trunk links with a greater vulnerability (ex. cyber-attack) could be appropriated reasonably at a cost of around 1 million dollars (related to the ratios above), peripheral links could be roughly appropriated of around 0.8M-0.9M consistent with the typical OT security cost models. That is based upon the rationale that if in a typical year even in the range of 20-30 assets each warranted $0.8M-(annually) - $1.2 million dollar expenditures for prevention, it was all then positioned comfortably under the overall expenditures of the enterprise security budget of $40m. The prevention cost for response, which changed to account for whether the node or link for incident response was critical or non-critical.

## Physical Threat, Vulnerability, Consequences, Prevention Costs ($), and Response Costs ($) for Flow Network:

For the random physical attack / accident scenario, the threat probability was assumed to be100% for all nodes and links. Considering that any node or link could be hit in a random event. Physical vulnerability values for links were assigned based on their structural and flow importance within the pipeline. Backbone and source-to-junction connections received higher vulnerability (80–85%) due to greater throughput and disruption potential (Colonial Pipeline, 2024; Virginia Places, n.d.), mid-network and junction links were assigned moderate values (75–78%), and peripheral branches received lower vulnerability (≈70%) because incidents there impact only localized flow.

The Colonial Pipeline accident which resulted in about 1,200,000 gallons spilled and costing approximately $3.3M (source: EIA 2021 and Reuters 2021), environmental cleanup - $0.5M), infrastructure repair-$1.0M), and regulatory fines-$0.25M (source: PHMSA 2025a) and Industrial Cyber 2023) would overall be estimated at $4.75M. Then, the base cost is adjusted by node/link criticality. Major source/backbone is rounded up to $5.0M (Houston, Atlanta). Junction / mid-network connectivity is kept close to the range of $4.5–4.75M. Branch / peripheral connectivity is adjusted to $4.0M, given a spill is lower throughput therefore also less cleanup, and disruption (PHMSA, 2025b).

The consequence of a spill on a flow network can be expressed as the amount of gallons as well that would be lost (spilled and unrecovered) from that spill, which is expected based on what is known about the physical impact of a spill on the flow network and derived by converting the $4.75 million 'moderate spill' (baseline) into gallons using PHMSA planning value of approximately $200/gallon for crude oil releases. Therefore, the physical impact on the flow network from a typical mid-network event is approximately 24,000 gallons (PHMSA, 2023).

The cost for both prevention and response does not change because they reflect fixed engineering costs associated with each spill—i.e., valve installation, monitoring equipment, excavation, containment, and repair—and are not calculated based upon the gallons of liquid spilled, but rather on the dollars spent. Hence, while physical consequences are stated in gallonage for easy comparison, the MBRA optimization model will still record the costs for both prevention and response in dollars to maintain cost comparability among all mitigation strategies.

The prevention cost ($M) indicates expenditures on valves, monitoring, inspection, hardening of right-of-way, and engineering controls (TSA, 2021; CISA, 2025). Which were again adjusted based on the position of the nodes and

flow impact. Source/backbone was assumed at $1.50M (highest spend per node/link). Junction / mid-network was assumed at $1.25M. Peripheral was assumed at $0.75M.

Response cost ($M) encompasses emergency repair, temporary containment, additional cleanup, and crisis logistics after an incident. Scaling it at 40–50% of the associated prevention cost with $1.50M prevention cost will have $0.75M response cost. Similarly, $1.25M prevention cost has $0.63M response cost and $0.75M prevention cost has $0.38M response cost. This reflects typical proportions between prevention and post-incident response seen in pipeline incident history (PHMSA, 2025b) and maintains the same ordering—source/backbone components are the most expensive to respond to, peripheral branches the least.

# Physical and Cyber Threats:

Colonial Pipeline had a ransomware breach. Reports suggest that before the ransomware the threat actors compromised the corporate IT network and exfiltrated almost 100 GB of data (Reuters, 2021a; Cyber Law International & CCDCOE, 2022). The OT fuel-delivery systems were not directly compromised; however, moments later ceased pipeline operations as a precaution against lateral movement into Industrial Control Systems thus demonstrating that IT-only attacks can start a national energy crisis. (ABS Group, 2021; Claroty, 2021; Tenable, 2022) The shutdown affected 45 percent of the East Coast's fuel supply; it caused panic buying, spikes in the price of fuel, and a multi-state emergency declaration. (EIA, 2021; International Energy Agency [IEA], 2021; KU News, 2021; Reuters, 2021b).

The incident highlighted a number of systematic problems in Colonial Pipeline’s infrastructure, including the lack of separation of network segmentation, enforcement of multi-factor-authentication (MFA), and issues with their remote access VPN (CRN, 2021; Claroty, 2021).Ransomware actors are increasingly targeting OT-adjacent networks because pipeline operators routinely connect business and operational systems in pursuit of efficiency and reliability. (ISA, 2020; Fortress Information Security, 2022; Securitas Technology, 2022). This linkage dramatically increases the chances that a cyber breach creates a physical shutdown of operations without any supervision of equipment. (ABS Group, 2021; Claroty, 2021).

The physical attacks are less publicized than the Colonial cyber incident, physical attacks are a category of threat for pipelines that has existed for a long time and continues to be high impact (PHMSA, 2025; Securitas Technology, 2022). The landscape of physical security includes both opportunistic attacks and acts of premeditated sabotage: (TSA, 2021; CISA, 2025).

1. Perimeter Breaches

Some valve sites, pump stations, and pipelines are found in isolated areas with little to no monitoring (TSA, 2021; DP Center of Texas, n.d.). If an unwanted person were to access an unattended station, damage a fence, disable the communications system, or open a valve. Environmental contamination of pipeline products, an unplanned process shutdown, or a risk to personnel safety could result from a violation of this kind.

2. Theft and Vandalism

There are frequent thefts involving copper wiring, fuel, sensors, and equipment in and around pipeline sites (Securitas Technology, 2022; DP Center of Texas, n.d.). In some counties, for example, criminal groups will even tap into pipelines and siphon fuel, resulting in explosions or comprehensive spills (DP Center of Texas, n.d.; PHMSA, 2025). While these sorts of disruptive crimes are less common in the U.S., the Colonial Pipeline experience in 2020, where a failed detection system led to a spill after someone had tampered with the system, demonstrates that this issue may have a troubling financial and environmental set of consequences. (Industrial Cyber, 2023; Virginia Places, n.d.). Another form of vandalism can involve firearm, cut, or recreational disturbance. (TSA, 2021)

3. Sabotage
An individual may want to undermine the pipeline due to political, religious, or criminal reasons. For Example, individuals associated with extremist groups, former employees who have been wronged by their employer, or individuals/organizations supported by a government may be attempting to inflict economic damage, create an ecological disaster, or incite fear into the public. (CISA, 2025; Securitas Technology, 2022). Political extremists, disgruntled insider, and/or state actors may seek to damaging to create a havoc on an economic, environmental, or even psychological basis (CISA, 2025). Sabotage is particularly impactful because it is primarily executing against critical nodes in the system, such as, but not limited to compressor stations and trunk-line junctions. (Colonial Pipeline, 2024; Virginia Places, n.d.; TSA, 2021).

# Cascade Network MBRA results:

The maximum response budget in the MBRA tool was $27 M, and colonial pipeline's cybersecurity annual budget was
$40 M so the prevention budget was computed at $13M dollar which corresponds to allocating about $20M of effective prevention spending to this segment of the network, while leaving the rest of the corporate budget for other systems. The objective function risk and weight by degrees parameters were set. The following results were obtained.

**Identification of Critical Nodes**:
Houston was ranked one as Houston is the origin of the Colonial Pipeline system and the largest entry point for refined fuel entering the network. All downstream nodes depend on Houston for supply. If Houston fails, the entire pipeline effectively loses input volume
There is no alternative path to bypass Houston. MBRA sees this as a total network throughput loss.

Atlanta comes out as Rank 2, which is exactly expected from a central trunk node. Atlanta's characteristics justify this ranking: It is a major mid-pipeline junction. It feeds Nashville, Knoxville, Charlotte, Belton, and the eastern branch. Losing Atlanta cuts the pipeline in half. Multiple downstream cities become disconnected. It creates both supply loss and rerouting inefficiencies

Meridian and Opelousas form the Western Backbone Midpoint. These nodes sit between Houston, Birmingham, and Atlanta. Removing one breaks the supply chain early in the pipeline. They do not have alternate routes. They feed into larger hubs (Birmingham → Atlanta). That makes them significantly important but not as irreplaceable as Houston or Atlanta. Similarly, Mitchell and Dorsey (Eastern Split Junctions). These nodes control the eastern branch of the pipeline. Dorsey connects to Baltimore and Linden. Mitchell connects Greensboro, Richmond, and Dorsey. Loss of either node isolates a large part of the right-side distribution network. There are no parallel paths, so failures propagate quickly

**Risk Reduction:**
Houston observed the highest risk reduction. Even though Atlanta is a major hub in the network, the model shows a smaller risk-reduction compared to other critical nodes. The model reduces risk first at the highest-impact chain: Houston → Opelousas → Meridian → Birmingham. These nodes sit on the main trunk of the network and have the largest consequence values, so any reduction in their vulnerability produces a big drop in total system risk. Once these upstream backbone nodes are hardened, most of the major cascade paths feeding into Atlanta are already secured.

# Flow Network MBRA results:

The maximum response budget in the MBRA tool was $38M, the prevention budget was computed at $19M dollar.
The objective function risk and weight by height parameters were set. The following results were obtained.

**Identification of Critical Nodes:**
Houston is the primary source of flow. Opelousas, Meridian, Birmingham are the first major backbone transition points Any physical failure here affects the flow towards the entire network. Criticality of the nodes in the flow network demonstrating the physical threat is with respect to the actual physical flow. i.e., the first major nodes are ranked critical, and Atlanta is ranked seven compared to the cascade network demonstrating cyber threat.

**Risk Reduction:**
Houston, Meridian, and Birmingham with the strongest risk reduction of 95 -94%. Houston is the primary source of flow Meridian and Birmingham are key interior junctions: they do not originate flow, but failure at either still interrupts a large portion of the network. Any failure here stops flow for every downstream node. Because flow is strictly directional, risk appears in chokepoints that control upstream-to-downstream movement, rather than cyber-centrality patterns. When Prevention and Response budgets are allocated across the flow network, a consistent pattern is observed. Risk reduces most strongly at major upstream flow sources and backbone links, while mid-chain and peripheral nodes experience proportionally smaller reductions. Improving resilience in the upstream backbone gives the highest payoff because every downstream node depends on this segment, so small improvements amplify across the entire chain.

# Analysing impact of a targeted cyber-attack on Atlanta in Cascade Network:

Analyse the effects of targeting specific nodes or "hubs" within the colonial cascade network, node with the highest number of connections is considered which is Atlanta (the most connected hub. Same contagion probability of 30% chosen for random attack calculations, the estimated effect on 1-2 of Atlanta's nearest neighbour nodes in the context of the cascade network would be determined. Atlanta's nearest neighbour nodes in the colonial cascade network include the following nodes: Birmingham, Belton, Nashville, and Knoxville. Thus, using a contagion risk of 30%, the model suggests that if a targeted attack were launched against Atlanta,

CAtlanta=0.30(Atlanta)+0.30(Birmingham)+0.30(Belton)+0.30(Nashville)+0.30(Knoxville)
C(Atlanta)=5×0.30=1.50≈ 2 nodes
C(Birmingham) = 0.30(Atlanta)+0.30(Birmingham)+ 0.3(Meridian) = 0.9 = 1 node
C(Belton) = 0.30(Atlanta)+0.30(Belton)+ 0.3(Spartanburg) = 0.9 = 1 node
C(Nashville) = 0.30(Atlanta)+ 0.30(Nashville) = 0.6 = 1 node
C(Knoxville) = 0.30(Atlanta)+ 0.30(Knoxville) = 0.6 = 1 node

# Analysing impact of a targeted physical-attack on Atlanta in Flow Network:

Considering flow network a targeted attack on Houston will impact all the thirteen downstream sites (the largest consequence of supply loss) and including Houston be a 14-node consequence. However, we are considering only Atlanta for this paper, considering a unidirectional pipeline, flow of supply will go from Birmingham to Atlanta to Belton, Atlanta to Nashville and Atlanta to Knoxville. Therefore, Birmingham would be above the point of failure, thus, the failure of Atlanta would only cause Flow loss to those below it in the flow chain.

So, for the Flow Network, we only count the downstream neighbours from the Attack node, for example:

C (Atlanta) = 0.75 (Belton) + 0.70 (Nashville) + 0.70 (Knoxville) + 0.85 (Atlanta) = 3
C(Belton) = 0.75(Belton)+ 0.3(Spartanburg) = 1.05 = 1 node
C(Nashville) = 0.70 (Nashville)
C(Knoxville) =0.70 (Knoxville)

The Flow Consequence for Atlanta is 3 which is three nodes losing their physical service due to disruption at Atlanta; Failures at upstream bottlenecks may cause Flow losses to a significant portion of the network.

A low contagion coefficient, represented here by $\gamma = 0.30$, provides a reasonable estimate for how little a cyber compromise would impact, as it does not necessarily jump over every logical connection and many of these potential paths are already blocked with defence mechanisms, thus resulting in very few additional cyber nodes expected to be compromised. On the other hand, a physical supply chain network has a direct connection to the flow of products/services from one location to another, therefore if there is a disruption in the upstream supply chain, it will disrupt the upstream supply chain to all downstream supply chains immediately. Therefore, the physical consequences from the same Atlanta failure will be far greater than the cyber cascade consequences.

# Fault Tree Analysis of the Cascade Network:

In the cascade network, two critical nodes Houston and Atlanta were, and the cybersecurity threat Ransomware and Supply Chain attack were considered for computation of fault tree. Ransomware consequence was $4.4M and for supply chain attack $4.35 M (Fortress Information Security, 2023; ABS Group, 2021). Threat probability for all four basic events was set to 100%, and vulnerability probability was fixed at 30% inconsistent with the previous logic.

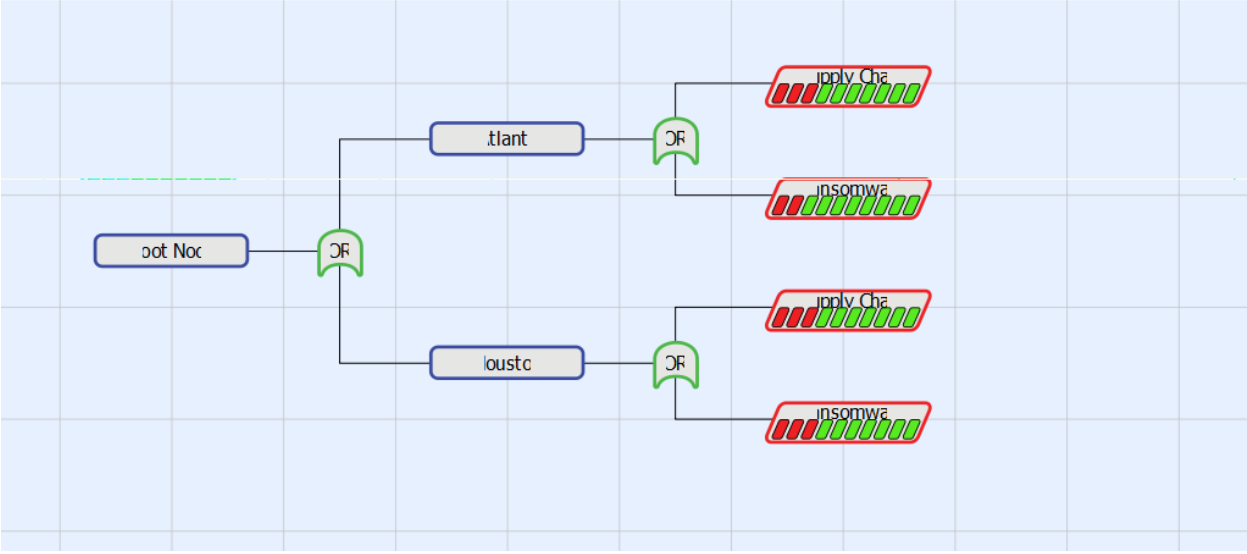



***Figure 12 – Cascade network fault tree***

**Consequence estimation**

Node-level consequences were anchored in the cyber cost breakdown used earlier
$C_{\text{cyber}}$ = shutdown hours × $/hr + ransom + IT/OT recovery + business/legal loss ≈ $11.15 M.
(Ransomware.org, 2022; NE Digital, 2023; Claroty, 2021; Industrial Cyber, 2023).
Prevent duplicate counting of the prevention budgets allocated to each basic event type, only part of the overall amount was assigned to each basic event type. Using realistic incident studies, ransomware and supply-chain compromises were both set to base costs of about $4.4M and $4.35M, respectively. (ABS Group, 2021; Fortress Information Security, 2023) Because Houston is the origin of flow and more central than Atlanta, these base costs were scaled by ±10%:

Houston
Ransomware consequence: $4.4\text{M} \times 1.10 \approx \$4.84\text{M}$
Supply-chain consequence: $4.35\text{M} \times 1.10 \approx \$4.79\text{M}$
Atlan
Ransomware consequence: $4.4\text{M} \times 0.90 \approx \$3.96\text{M}$
Supply-chain consequence: $4.35\text{M} \times 0.90 \approx \$3.92\text{M}$
This preserves realistic orders of magnitude while recognising that failure at Houston has slightly higher system-wide impact than the same failure at Atlanta.

**Elimination / prevention cost estimation**
Houston received an overall prevention budget of $1.20 million, and Atlanta received an overall prevention budget of $1.08 million. These amounts represent the combined costs of investing in OT segmentation, OT monitoring, and backup hardening, implementing Multifactor Authentication (MFA), and incident readiness. (Tenable, 2021, Claroty, 2021
Each node's cyber budget was then split between the two threat types:
Ransomware controls (backup, EDR, playbook, segmentation) represent 60% of node budget (ABS Group, 2021; Ransomware.org, 2022). The Supply Chain controls (vendor due diligence, SBOM, patching, contract clauses) are 40% of node budget. (Fortress Information Security, 2023; LogicManager, 2021) This yields the elimination costs used in the fault tree:

- **Houston**

Ransomware elimination cost: $0.60 \times 1.20 \approx \$0.90\text{M}$
Supply-chain elimination cost: $0.40 \times 1.20 \approx \$0.75\text{M}$

- **Atlanta**

Ransomware elimination cost: $0.60 \times 1.08 \approx \$0.65\text{M}$
Supply-chain elimination cost: $0.40 \times 1.08 \approx \$0.55\text{M}$
The initial risk in total was 5.25 with Houston Ransomware ranking with $1.45M, followed by Houston supply-chain 1.44. Atlanta's ransomware risk was 1.19 followed by supply chain with 1.18. With $2M budget allocation, the resulting highest budget allocation of $0.57M to Houston's ransomware which resulted reduction to 0.47 and vulnerability reduction to 9.7%. Followed by Houston supply-chain with budget allocation of $0.54M risk reduction of 0.39, and vulnerability reduced to 8.2%. Atlanta's supply-chain had budget allocation of $0.45M with risk reduced to 0.34 and vulnerability reduced to 8.6%. Atlanta ransomware had budget allocation of $0.44M with risk reduced to 0.29 and vulnerability reduced to 7.2%. Overall, the top-event risk decreases from 5.25 to 3.76 (risk reduced ≈ 1.49) and aggregate vulnerability falls from about 76% to 46% (a ~30% reduction). The ranking of critical basic events is therefore seen as:

1. Houston ransomware
2. Houston supply-chain
3. Atlanta supply-chain
4. Atlanta ransomware

This confirms that, under the assumed costs and consequences, marginal cyber-security investments should first target ransomware and supply-chain controls at Houston, then analogous controls at Atlanta.

# Fault Tree Analysis of the Flow Network:

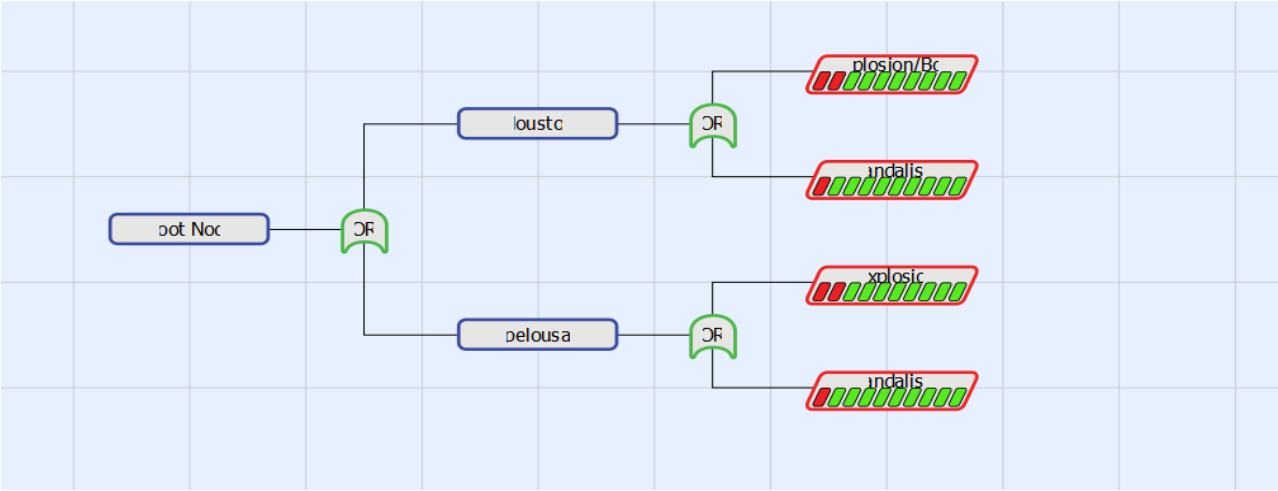



***Figure 13 – Flow network fault tree***

The fault tree of the flow network considers two stations critical to physicality- Houston (where the pipeline starts) and Opelousas (the first junction downstream)- and two types of physical threats at each node (Explosion/Bomb, Vandalism / third-party damage). Both events are linked with the OR-gates which means if one event occurs at either node the failure will have occurred at the system level.

Houston is the most vulnerable facility. Its vulnerability (35–50%) is set higher than Opelousas (30–45%) since the source station is larger, more visible, and often found within a busier metropolitan area where there are potential opportunities for third-party interference. Opelousas remains important, but because it is a less public exposed junction its vulnerability is at a slightly lower percentage.

**Consequence estimation**

Theft and vandalism have been estimated between $3.3 million and $4.5 million, based on the historical trends seen in the physical-damage incidents involving moderate quantities of leaked or spilled product (e.g., approximately 1.2 million gallons), which have also resulted in significant costs associated with clean-up and product loss (PHMSA, 2025; Reuters, 2021; TSA, 2021). Based on the assumption that the costs associated with clean-up efforts for spilled product are approximately equal to the number of gallons spilled multiplied by 1,000 (roughly $3.3 million), these estimates align well with the long-term incident data maintained by the PHMSA, which indicates that excavation damage and third-party interference account for the majority of cases within the mid-range consequence level (PHMSA, n.d.; DPC of Texas, n.d.). It is assumed that explosion or sabotage-related incidents will result in a similar consequence tier as physical-damage incidents (i.e., approximately the same, but possibly a bit more), and these incidents are projected to incur costs from $4.5 million to $5 million (CISA, 2025; TSA, 2021; ABS Group, 2021), reflecting the view of regulatory agencies that most unintended or accidental damages cause a lower level of disruption to structure, environment, and service than do intentional acts of violence.

**Elimination / prevention cost estimation**

Elimination (prevention) costs follow the same physical logic as above. Explosion/sabotage scenarios incur the most elimination costs i.e., $1.0M for Houston and $0.8M for Opelousas (PHMSA, 2025; CISA, 2025; TSA, 2021). Vandalism/third-party damage have lower elimination costs i.e., $0.75M for Houston and $0.70M for Opelousas (PHMSA, 2025; DPC of Texas, n.d.). Houston considered as the source has received higher elimination cost than Opelousas.

**Risk Reduction:**

Taking all this into account, the optimization allocates the physical-security budget across the four basic events, instead of concentrating it.

Houston - Explosion/Bomb was allocated the largest budget (~$0.86M), which reduced risk by ~0.33 units, and reduced vulnerability by ~6.59%.
Houston - Vandalism (by the second largest funding) at (~$0.75M), reduced risk by ~0.23 units of risk and reduced vulnerability by ~5.0%.
Opelousas - Explosion occurred at an estimated funding of ~$0.71M which provided ~0.29 units risk reduction and ~6.13% vulnerability reduction.
Opelousas - Vandalism allocation of ~$0.68M provided risk reduction of ~0.20 and vulnerability reduction of ~5.28%.

In summary, Houston is still the predominant physical-risk driver, especially for high-consequence explosions, and commands the largest single software investment. However, the model does not intend to allocate everything to Houston. Once Houston's explosion and vandalism vulnerabilities are mitigated, the next cost-effective way to reduce system-level risk is to harden Opelousas, because a problem in that location could still segment the entire east-bound flow even if Houston remains hardened.
In effect, the final ranking implies a paired criticality where Houston is the dominant source node, and Opelousas is the critical downstream junction node. The optimal allocation of the budget will strive to balance the investment in both source node and junction node to achieve the greatest reduction overall in physical spill risk, based on the available budget.

# Prevention and response controls for Physical Flow network:

The network analysis of physical cascades system reveals that resilience is primarily contingent on a few structurally critical nodes, especially those with high betweenness centrality, and blocking points, where any disruption stops and segment flows stops downstream (as a large segment downstream) consistently. In a tree-structured pipeline system with little redundancy, physical disruption at those points demonstrates immediate consequences (systemic effects). Accordingly, prevention and response controls must be implemented in a purposefully concentrated manner at the nodes with the highest overall physical risk: Houston (source), Opelousas, Meridian, Birmingham, and Atlanta.
1. Prevention Controls: Reducing the Potential for Physical Disruption
Physical prevention means stopping or detecting intrusion, sabotage, or accidental damage before any flow is disrupted. Since high-betweenness and junction nodes have the greatest share of pipeline throughput, prevention controls in these locations have the greatest potential to reduce system-wide risk. (TSA, 2021; CISA, 2025).

2. Enhanced Perimeter Security:
The high-priority nodes, which include Houston (TX), Opelousas (LA), Birmingham (AL), and Atlanta (GA) should have layer of anti-tamper security fencing in addition to such features as upgraded fencing; intrusion detection devices; thermal imaging and/or low-light cameras; and monitored entry/exitways into the location. It is believed that the application of the measures will minimize the likelihood of the types of breaches or inadvertent trespassers which so often have occurred to all utilities and service providers as precursors to acts of vandalism and/or fuel theft of a significant magnitude.

3. Valve, Pump and Compressor Hardening:
For nodes with blocking functionalities (Meridian, Mitchell, Dorsey, etc.), integral valve housings, blast resistant housing/casings and tamper-proof actuator enclosures are required. Since these nodes directly affect regional or multi-state flow of oil and gas, preventing physical or mechanical interference at these nodes can help mitigate the risk of a cascading hazard event. (CISA, 2025; ABS Group, 2021)

4. ROW Protection Patrols Nodes with high betweenness are situated on mainline ROW junctions where long-distance ROW segments meet. Increasing the frequency of ROW patrols, adding drone monitoring, and identifying anomalies and incident reporting methods quickly will reduce the likelihood of accidental third-party impact, and by far, one of the most frequent causes of pipeline failure (PHMSA, n.d.; DPC of Texas, n.d.). Controls in this area significantly reduce the overall risk of failure that may affect the entire downstream corridor.

# Prevention and response controls for Cyber Cascade network:

Cybersecurity measures for a cyber-physical pipeline system must be implemented across the enterprise, but in a Flow network representation, when cyber events propagate along operational pathways, the intensity of cascade impacts is not evenly distributed across the system. Therefore, while Zero-Trust Architecture (ZTA) must be implemented network-wide, the depth and rigor of implementation oftentimes must be prioritized at high-betweenness, high-centrality, and blocking nodes as chokepoints in the Colonial Pipeline's Cyber Flow network. Nodes in Atlanta, Belton, Spartanburg, and Greensboro support concentrated SCADA command flows A breach of a single high-centrality node would create an imbalanced amount of disruption in the normal operating procedures and processes of the utility operator and a downstream effect across all segments associated with the utility operator. (ABS Group, 2021; Claroty, 2021; Cybersecurity Dive, 2021). ZTA, which includes identity validation, least privilege, encrypted protocols, VPN secured access, network segmentation, micro-segmentation, etc., provides the foundation for assurance. However, the following node-prioritized controls will provide the highest marginal reduction in risk (Tenable, 2021; TSA, 2021, ISA, 2020;).:

1.Modernization of Legacy OT Systems:
Legacy protocols and Windows-based human-machine interface (HMI) servers are used in most of the current pipeline supervisory control and data acquisition (SCADA) systems. The objectives of the efforts to modernise high-centrality nodes are to mitigate the risks posed by insecure systems (e.g., by replacing all legacy systems that do not support encrypted/protected authentication with secure systems capable of providing encrypted/protected authentication). One of the most serious vulnerabilities to SCADA systems today is outdated programmable logic controllers (PLCs) and hard-coded credentials that were not patched, but all have the potential for allowing an attacker the ability to inject false commands or manipulate control logic resulting in varying flow rates. (ISA, 2020; ABS Group, 2021).

2. Stricter Access Controls and PAM Enforcement:
Threat vectors typically leverage credential theft or privilege escalation simply at critical nodes to alter parameters for operation. Role Based Access control should be implemented wherever possible. Additionally Privileged Access Management (PAM) with just-in-time access, monitoring of sessions, and strict role separation to reduce the likelihood. a compromise via credentialed components is significantly reduced. There are other important nodes that could potentially be compromised, such as those that control the starting of pumps, alignment of valves, or isolation of segments of the pipeline. **(**HackerNews, 2021; Tenable, 2021; Cybersecurity Dive, 2021).

3. Enforce Multifactor Authentication (MFA):
Many SCADA devices currently do not use MFA due to administrative overhead. However, multifactor authentication should be implemented for the access, especially for access in remote connections, also connections used by field technicians, contractors, and third-party vendors. MFA protects against replay attacks, credential stuffing, and unauthorised access to SCADA without putting passwords at risk.

4. Network Surveillance and Anomaly Detection:
SCAD system should be monitored. The deployment of behavioural detection systems at SCADA aggregation points allows for the earliest potential notification of malicious activity. This includes monitoring for unauthorized Modbus function calls, master pressure-set commands, polling frequencies, or east-west traffic flows suggesting reconnaissance into a lateral movement. An Operational Technology-based (OT) Anomaly Detection Tool

provides in-depth visibility into OT protocols by alerting organizations to out-of-band (OOB) protocols before they are integrated into downstream pumping stations. (Claroty, 2021; ISA, 2020; ABS Group, 2021).

5. Ongoing Monitoring of Corporate IT Systems That Link to OT:
The 2021 Colonial Pipeline incident highlighted that attackers often breach corporate IT networks first and then use shared authentication infrastructure or VPN to pivot to OT systems. For this reason, SIEM monitoring, endpoint detection, and identity monitoring in the corporate IT environments are quite necessary for proper OT protection.IT compromise remains the most common precursor to SCADA disruption. (HackerNews, 2021; Cybersecurity Dive, 2021; Claroty, 2021).

6. Conduct Tabletop Exercises; Red/Blue Teaming:
Enterprise level tabletop and red/blue teaming exercises should be conducted. As the ability of the enterprise to respond in the event of an incident is important as it effects how quickly cascades can be contained, are a significant factor in the scope of impacts. Regular tabletop exercises, SCADA attack simulating drills, incident response practice, and requested red team/blue team engagements improve preparedness. Most of these exercises can occur in sequestered environments that do not interrupt production timelines. For Service Agreements for disaster recovery expectations with appropriate definitions and details within the Service Agreements in Operating and/or Maintenance of SCADA Components should be defined, maintained, and updated with the vendor (ABS Group, 2021; Congress, 2021; Tenable, 2021).

7. Awareness and Operation Training for Cybersecurity:
Human factors are still a key weakness in any SCADA environment. If operations staff, IT staff and field engineer staff are trained on identification and avoidance of phishing, credential hygiene, securing devices, and escalation of incursion events, the risk of a successful initial compromise will be reduced. It is necessary for the employees to understand that cyber anomalies also present themselves into the physical world (e.g., abnormal pressure readings or pump oscillations) when training to recognize early signs of a compromise. (Securitas Technology, n.d.; ABS Group, 2021; ISA, 2020).

When adding awareness and operation training preventative and response controls at high-betweenness, block and centre (node) levels in the SCADA environment, you are achieving the maximum impact (risk reduction and resilience improvement) per dollar with these controls.

8. Cyber-Physical Safety Controls and Failsafe Logic: Independent safety instrumented systems (SIS), rate-limiters on valve actuation, and even hardware interlocks guarantee that even in the event of a cyber-attack on the SCADA command and control functionality, actual physical actions will fail to a safe state. This casts uncertainty over flow reliability but ensures physical operation does not fail and controls will shut down the pipeline from becoming over-pressurized. (PHMSA, 2025; ABS Group, 2021).

9. Redundant Telemetry and Backup Communication Paths: High-betweenness nodes should not be the single point of cyber-induced operational failure. Redundant communications, backup SCADA servers, replicated historian environments and so forth reduce the risk of this failure by maintaining visibility and command should primary systems be compromised. (ABS Group, 2021; Claroty, 2021; Tenable, 2021).

# Budget Requirements for Risk Mitigation and Resilience Improvement:

Cybersecurity investment is based on the fully modelled risk calculations (30% for node-level cyber vulnerability). But unlike node-level vulnerabilities, the operational impact of a cyber compromise is not uniform. Atlanta, Belton, Spartanburg, and Greensboro, SCADA nodes have access to greater levels of SCADA relay, telemetry, and control based on their relatively high-levels of betweenness-centrality; therefore, a cyber outage to these SCADA nodes could propagate consequences and risks rapidly to impact the entire corridor. (ABS Group, 2021; EIA, 2021).

Zero-Trust Architecture (ZTA) and SCADA hardening budget expectancy will be around $0.7M – $1.2M per critical and moderate risk node, as presented in prior discussions about prevention budgets:

High betweenness SCADA hubs (Atlanta; Houston):

~ $1.0M - $1.2M need for segmentation, PAM, MFA, encrypted protocols, and monitoring. (Tenable, 2021; Cybersecurity Dive, 2021).

Mid-network OT nodes (Belton; Charlotte; Birmingham) (Tenable, 2021; LogicManager, 2021).:

~ $0.8M - $1.0M need for configuration hardening, anomaly detection, and access control hardware/software.

Peripheral SCADA nodes (Knoxville; Nashville; Linden):

~ $0.6M - $0.75M as a lower boundary of investment. (ABS Group, 2021)

Cyber response capability (threat hunting, forensics, incident response retainers/ forensics, and SCADA restoration) typically requires 50 - 60% of the prevention budget due to the resource intensive containment and restoration of Cyber security for OT networks. (Cybersecurity Magazine, 2020; ransomware.org, 2021; ABS Group, 2021).

Physical prevention controls will cost $0.75M – $1.50M per node, depending on node type:

Source nodes (Houston): require the most investment (~$1.5M), due to throughput and vast upstream exposure.

Backbone and junction nodes (Opelousas, Meridian, Birmingham): require ~$1.25M - $1.50M for perimeter hardening, valve protection, and patrol enhancement.

High-betweenness hubs (Atlanta): require ~$1.25M for surveillance, ROW protection, and mechanical tampering resistance.

The costs to respond to a physical event typically are 40% - 50% of the prevention budget to cover costs such as emergency isolation, handling incident spills, and repair crews.

Because the presence of physical nodes acts on a single line with direct effects, investing in prevention at incidents nodes will provide the greatest reduction in overall system risk. These principles are consistent with federal guidance that emphasizes protection from the perimeter, automated shutoff systems, and monitoring of key junctions over the equitable allocation of resources throughout the network.

For both a physical and cyber network, the budget plan will again focus on risk reduced per dollar rather than risk distribution. The MBRA-based assessment of both networks showed:

High-betweenness nodes provide the maximum marginal risk reduction per unit of investment.

Blocking nodes will maintain high priority due to their inability to be removed.

Source nodes (Houston) will need to have significantly higher investment in prevention considering their extreme consequence values range.

In sum, the budget needs to be directed primarily at the backbone of the system and the junction nodes to reflect the asymmetric risks of both networks. This way, when an operator times prevention and response investment to network criticality, they can facilitate the highest possible risk reduction for the least cost.

# Cyber Workforce Preparation & the Role of NICC / NCICC: Lessons from Colonial Pipeline:

When Colonial Pipeline experienced a ransomware attack in 2021, it was a reminder of how an attack aimed at Information Technology can affect the Operational Technology (OT) and create national disruption in a vital energy corridor. In order to breach the Colonial Pipeline network and spread ransomware across its network of IT systems, the threat actor took advantage of a compromised username and password combination from a remote access Virtual Private Network (VPN) without Multi-Factor Authentication (MFA) (Colonial Pipeline Ransomware Attack, 2024; IAMagazine, 2021; GAO, 2021).The shutdown on May 7, 2021, of Colonial Pipeline's entire 5,500-mile network of pipeline infrastructure (servicing 45% of the East Coast's fuel supply), resulted in hours-long outages, culminating in long lines at gas stations throughout the East Coast (Kerner, 2022; CRN, 2021)

Analysts describe this attack as a significant disruption of availability and gasoline deliveries and highlighted the vulnerability of critical infrastructure in the U.S. to cyberextortion (GAO, 2021; Science Publishing Group, 2024).

The Colonial Pipeline attack points to significant deficiencies in readiness and risk management for pipeline operations between federal entities and the private sector, according to reports from federal and oversight agencies. This attack resulted in the temporary interruption of fuel supply to many areas of the southeastern United States, leading to increased demands on the government and the private sector for enhanced cyber readiness (GAO, 2021). This attack is one of the most significant points in the history of cyber-attacks, as initial findings from this attack highlighted considerable weaknesses about cybersecurity for our critical infrastructure, which in turn served as the catalyst for several new federal initiatives. (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

Colonial halted the operation of its pipelines after the ransomware attack targeting their IT reach due to uncertainty regarding the attack's area of potential impact on operations as well as the security of Operational Technology (OT)/IT combined security (Kerner, 2022; CISA 2023). Following the attack, CISA and the FBI issued a joint advisory related to DarkSide Ransomware, recommending Multi-Factor Authentication (MFA) for all Remote Access to OT/IT networks, enhanced Patch Management, Hardening Remote Services, and an increase in the number and frequency of Backup and Recovery efforts based on the Colonial pipeline incident (CISA & FBI, 2021). Implicitly these recommendations suggest that the workforce has the expertise to implement and manage these types of controls within an IT/OT Hybrid Environment.

Since pipeline operations are part of the wider US critical infrastructure eco-system, Federal Coordination Centers provide principal support in the preparation for Colonial-type incidents. The NICC (National Infrastructure Coordinating Centre) and the NCCIC (National Cybersecurity and Communications Integration Centre) are designated under the NIPP (National Infrastructure Protection Plan) as the National Hubs for both Physical Security Risks and Cybersecurity risk, respectively. (CISA, 2020).

As part of the NIPP, a supplemental tool is provided to assist stakeholders in establishing a connection with the NICC and NCCIC. As outlined in the Supplemental Tool, both the NICC and NCCIC are available 24/7 and serve as central points of contact for State, Local and Private Sector Stakeholders to exchange information regarding threats, vulnerabilities, incidents, and protective measures which are associated with all Critical Infrastructure sectors. (CISA, 2020).

GAO's review of NCCIC's performance further clarifies its statutory functions. NCCIC is required by the National Cybersecurity Protection Act of 2014 to serve as the federal civilian interface for "multi-directional and cross-sector sharing" of cyber threat indicators, defensive measures, risks, and incidents for both federal and non-federal entities (GAO, 2017).Government Accountability Office GAO notes that NCCIC's mission includes providing situational awareness, issuing analysis and warnings, and coordinating responses to significant cyber incidents across multiple critical-infrastructure sectors (GAO, 2017).Government Accountability Office

Subsequent oversight reports reiterate that NCCIC (now part of CISA's broader mission) is intended to support both government and private operators in managing cyber risks to critical systems (GAO, 2018; Department of Homeland Security, 2020

The purpose of this statutory role (NICC) matches the needs that Colonial has identified. After the attack on Colonial, CISA and the FBI, through the NCCIC-style alerting framework, issued technical guidance on the DarkSide ransomware and recommended ways to mitigate the threat to key infrastructure owners/operators and also provided Indicators of Compromise (CISA & FBI, 2021; CISA, 2021).

Furthermore, CISA's retrospective on Colonial from 2023 directly connects all these efforts as part of a larger initiative to enhance resiliency in pipelines and other sectors of Critical Infrastructure (CISA, 2023).

Finally, this informs the establishment of the NICC and NCCIC Network as both information-sharing centres and conveners of coordinated training, exercises, and workforce development aimed at IT–OT threats.

# ROI Analysis for Prevention and Response Investments at Critical Cascade Nodes (Houston & Atlanta):

A thorough analysis of ROI is needed to determine the effectiveness of Cybersecurity Investments. The two selected nodes of Houston and Atlanta displayed a high structural influence on SCADA/Cybersecurity command propagation. These two nodes provide potential with high vulnerability and can initiate a significant operational cascade through Cyber disruption, and the significance of targeted investment in those locations.
Pre and Post Security Controls

Initial and Residual Risk
Houston has an overall risk of $3.35 million and compared to Houston, Atlanta has a risk of $3.01 million. Post running the MBRA simulation Houston experienced a reduction in resident risk to $2.64 million after the implementation of preventative and responsive control measures ($0.71 million reduction). On the other hand, the residual risk for the city of Atlanta was reduced to $0.59 million after the same measures were put in place, which resulted in an overall reduction of $2.42 million.

The large decrease in residual risk for Atlanta is indicative of the fact that Atlanta is a significant chokepoint in the cyber and physical construction of the pipeline. As a result of the security measures put in place at that location, the residual risks that are presented will be confined to the local area, and therefore have a reduced capacity for cascading negative impacts throughout the downstream pipeline route through Belton, Spartanburg, Greensboro, and Richmond Branch; whereas the security upgrades in Houston's area did not significantly affect the overall system-wide cascading dynamic of the resources.

ROI of Prevention and Response Investments
To quantify the ROI results, monetary value of anticipated losses avoided is considered and divided by the monetary value of the mitigation actions associated with each node in all our network locations.
Houston Total Prevention Cost was at $1.20 million, and Response Action Cost was $0.60 million. This makes the total Prevention + Response Cost to $1.80 million. The ROI associated with mitigation actions taken at Houston was limited to 0.59 for mitigation costs and 1.18 for response costs; the aggregate of both action types results in a 0.39 ROI, indicating that Houston's mitigation actions provided a reasonable return but had a more localized impact while still providing a return on investment.

Atlanta had total Prevention Cost was $1.08M and total response cost was $0.54M. This makes the total cost at $1.62 million. Atlanta has shown a substantial financial performance vs other locations; demonstrated by Mitigation Costs producing a 2.24 ROI (meaning, $1 invested will yield $2.24 of avoided losses); Response Costs

produce an ROI of 4.48; and aggregating both action types, this equates to an overall 1.49 ROI, making it one of the maximum-return nodes in the network.

Alignment with the Objective Graph

Our analysis has shown strong congruence with the curve of Prevention across the Network as predicted by the Matrix-Based Risk Analysis (MBRA) Method. The graph demonstrates that risk is reduced exponentially as funds invested into Prevention are increased. That is, from 100% (at no investment) to approximately 30% (at $13M in total prevention funding). This curve reaches its inflection point at this level where the curve begins to flatten out, indicating that investing mor at Atlanta will produce diminishing returns in terms of risk reduction. As such, placing most resources into nodes that have maximum leverage like in Atlanta will yield the greatest benefit for Future Resilience.

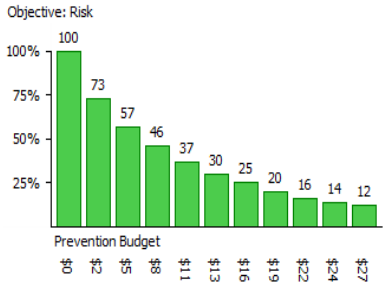



***Figure 14 – Cascade network objective graph***

As shown in the previous analyses on Cybersecurity Investments across the Nodes, while all Nodes benefit from investments in Cybersecurity, Node Atlanta provides a significantly better investment in reduction of risk (78%), along with the highest Return on Investment in the Segment. Houston does provide benefit by reducing risk but to a much smaller degree. Consequently, directing most investments in Atlanta will have the best long-term benefit for enhancing Pipeline Cyber-Physical Resilience.

Given Atlanta's pivotal position as a high-betweenness, high-centrality chokepoint in the SCADA Flow Network, the preventive and response controls proposed for the Colonial Pipeline system generate their highest marginal impact when implemented at this location. Cyber events do not propagate evenly across the pipeline; instead, disruptions originating at Atlanta, Belton, Spartanburg, or Greensboro have the greatest potential to spread into downstream operational segments. While Zero-Trust Architecture (ZTA) must be deployed uniformly across the enterprise, deeper enforcement—paired with modernization of OT systems, stricter access controls, anomaly detection, and enhanced telemetry redundancy—provides outsized benefits at these structurally influential nodes. Strengthening Atlanta with these targeted measures aligns both with the ROI findings and with the physical operational dependencies inherent in the pipeline network. Accordingly, the following node-prioritized prevention and response controls represent the highest-value interventions for mitigating cyber-physical cascade risk in the system.

# ROI Analysis for Prevention and Response Investments at Critical Flow Nodes (Houston & Opelousas):

## Initial and Residual Risk

Houston and Opelousas demonstrated significantly lower expected loss once Prevention and Response Controls were applied to them. Houston's initial expected loss was originally $4.50 Million and was reduced to $0.23 Million after allocating the Physical Security measures, thereby resulting in a total reduction in risk of $4.27 Million or approximately 94.9%. Opelousas had a similar effect with an initial risk of $3.60 Million and residual risk of $0.23 Million and therefore a risk reduction of $3.37 Million (or 93.6%). Of the two Cities, Houston exhibited the largest absolute loss reduction. This is due to its function as the starting point of the entire system and the fact that if there is any damage to it, it will have immediate impacts on the throughput for the entire network. Opelousas is not the starting point of the supply chain but rather is a critical blocking node that prevents product flow downstream when it is damaged. As such, the amount of risk that has been reduced is consistent with the critical nature of the protection of Multi-State Supply Continuity that is identified.

## ROI of Prevention and Response Investments

The Analysis of Returns on Investment (ROI) gives an indication of the financial return on investment for investing in physical-security measures. For Houston, investing in prevention measures costs $1.50M but yields a return of 2.85; investing $0.75M in response measures yields a return of 5.69, creating combined ROI of 1.90. For Opelousas, the ROI values are slightly lower: prevention yield 2.25, response yield 4.49 and total is 1.50. The combined ROI values show that each dollar allocated toward the full prevention-and-response package yields $1.90 in overall risk reduction at Houston and $1.50 at Opelousas. The Flow Network ROI is still relatively high for both nodes, unlike the cascade environment where the ROI is largely determined by a node's impact on digitally propagating, because in contrast, disruptions to the physical world have direct and calculable losses, therefore, the investments in physical barriers, products in tamper-proof enclosures, and improved detection greatly decreased the chance of an outage, thus resulting in high cost/benefit rates.

## Alignment with the Objective Graph

The Objective graph demonstrates Prevention Budget against Risk, and it can be inferred that when initial funding becomes available through the Flow Network, the Risk decreases quickly. Specifically, as $3 million is spend, the risk reduces from 100% to 27%. When the funding increases beyond $3 Million the risk steadily decreases to 11% at $15M funding. Post this it demonstrates a stable plateau even with increased funding the risk does not decrease much it is constant at 8% This indicates that, after the four highest-consequences nodes, (Houston, Opelousas, Meridian, and Birmingham) have been secured, diminishing marginal returns are likely to occur as additional funding is provided. The early steep drop on this graph indicates that the best risk-reduction efficiencies occur by directing funding toward structural-critical nodes, which corroborates the financial results reported in section 2, which clearly show that both Houston and Opelousas produce the greatest financial returns.

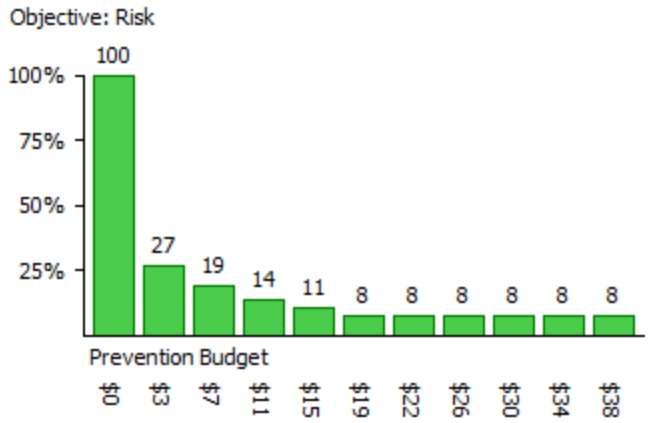



***Figure 15 – Flow network objective graph***

In conclusion, the analysis shows that by investing in security at Houston and Opelousas, businesses will improve their profitability and effectiveness and reduce their risk. Investing in security at Houston and Opelousas will increase ROI dramatically for both prevention and response controls, while it also decreases the impact of residual risk. Specifically, because the Houston and Opelousas nodes in the flow of the Flow Network have a tree-like structure with little redundancy, and the flow is predictable from node to node, any disruption of the flow at those nodes will affect the entire system immediately. Thus, both the prevention and response controls proposed including enhanced perimeter security, tamper-resistant valve housings, compressor and pump hardening, and expanded ROW patrols will not only have a significant impact on the reliability of the flow through Houston and Opelousas but are also the best way to place security resources where they will have the most effect. Concentrating security resources on the most critical nodes of the flow of the Flow Network will result in the greatest competitive advantage and financial return.

# Possible Funding Sources for Cascade and Flow Network Investments

Federal funding sources can provide funding opportunities for both the Cascade Network (cyber/SCADA security) and the Flow Network (physical pipeline protection). For the Flow Network, funding pathways that are most relevant are through the Pipeline and Hazardous Materials Safety Administration (PHMSA). PHMSA provides State Damage Prevention Grants to fund initiatives aimed at decreasing excavation-related accidents and increasing physical protection along the right-of-way. This is an important part of preventing disruptions to the transport of hazardous liquids at high-risk nodes such as Houston and Opelousas (PHMSA, 2025a). Another source of funding is through Pipeline Safety Base Grants administered by PHMSA to provide funding support to state pipeline safety programs for the inspection, enforcement, and improvement of Pipeline System Integrity Programs. At this time, operators may wish to use funds from these grants to support the upgrade of their pipeline infrastructure to meet Physical Control Measures including Valve Housing Hardening and Right-of-Way Surveillance (PHMSA, 2025b). Additionally, if the operator works with municipal or public utility entities, they may also be able to take advantage of the funds available through the Natural Gas Distribution Infrastructure Safety & Modernization Grant Program. The NGDISM Grant Program was authorized under the Bipartisan

Infrastructure Law to provide funding support for the replacement or strengthening of Physical Pipeline Assets including infrastructure relevant to flow resilience (PHMSA, 2025c).
The Cascade Network has a variety of funding mechanisms associated with it that will enable operators to develop and implement the required cybersecurity measures to secure the network in the form of the State and Local Cybersecurity Grant Program (SLCGP). As it is administered by CISA, the SLCGP has the most public information available for access and when pipeline operators partner with government agencies and industrial organizations to achieve mutual transportation goals through security, pipeline operators can access SLCGP funded initiatives and projects to achieve that goal through SCADA system oversight that intersects with government agency oversight through DHS. (CISA, 2025). The Government Accountability Office's (GAO, 2025) recently reported findings related to DHS's use of SLCGP funding sources to aid in mitigating the risk of cyber-attacks to the nation's energy and pipeline sectors, reinforces this assertion.

Therefore, the combined effects of these funding sources provide a unique two-pronged approach for enhancing both physical-infrastructure hardening for the Flow Network through PHMSA grants and Cybersecurity hardening through CISA cybersecurity grants to complement the development of SCADA and cyber defence enhancements and capabilities utilized within the Cascade Network in terms of threat mitigation and enhancement of cyber-physical resiliency for the operators at those high-risk pipeline nodes.

# References:

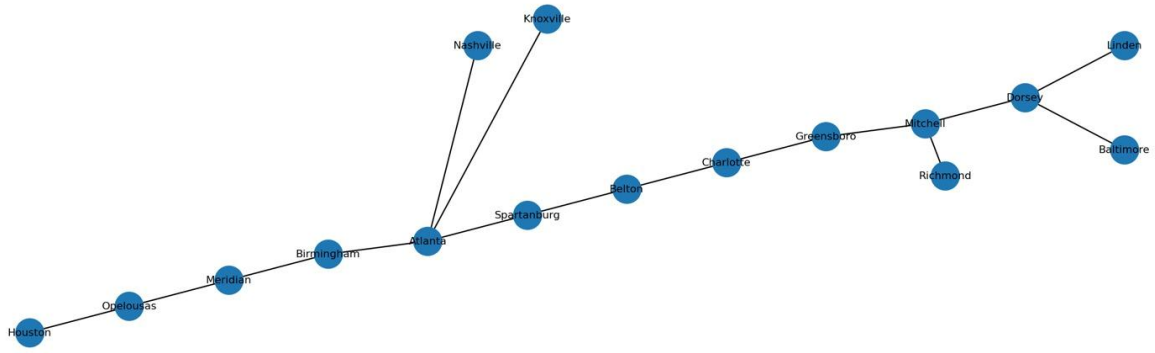

1. Colonial Pipeline Company. (2024). Asset map: https://www.colpipe.com/about-us/asset-map/
2. Colonial Pipeline Company. (2024). Operations: https://www.colpipe.com/our-operations/#:~:text=Colonial%20Pipeline%20was%20founded%20in,visible%20aspects%20of%20our%20operations.
3. EIA. (2021). Colonial Pipeline provides critical fuel supply to the East Coast. U.S. Energy Information Administration: https://www.eia.gov/todayinenergy/detail.php?id=47917
4. ENTELEC. (2022). Oil & gas cybersecurity whitepaper: https://www.entelec.org/wp-content/uploads/2022/02/fortinet-wp-oil-gas-solution.pdf
5. Fortinet. (2024). Cybersecurity in the oil and gas industry: Securing the OT environment: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-cybersecurity-oil-and-gas.pdf?
6. Fortinet. (2025). Key findings from the Fortinet 2025 Operational Technology Security Report: https://www.fortinet.com/blog/business-and-technology/key-findings-from-the-fortinet-2025-operational-technology-security-report?
7. ABS Group. (2021). Cyber risk management advisory: Analysis and recommendations following the Colonial Pipeline shutdown. https://www.abs-group.com/News-and-Events/News/Cyber-Risk-Management-Advisory-Analysis-and-Recommendations-Following-the-Colonial-Pipeline-Shutdown/
8. CISA. (2025). Physical security considerations for temporary facilities.: https://www.cisa.gov/sites/default/files/2025-09/Physical_Security_Considerations_for_Temporary_Facilities_20250915_508.pdf
9. Industrial Cyber. (2023). US PHMSA penalizes Colonial Pipeline $1 million for control room management failures. https://industrialcyber.co/analysis/us-phmsa-penalizes-colonial-pipeline-nearly-1-million-for-control-room-management-failures/
10. PHMSA. (2025a). Civil penalty summary. https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2025-02/Civil-Penalty-Summary-01-21-2025.pdf
11. PHMSA. (2025b). Pipeline incident 20-year trends. https://www.phmsa.dot.gov/data-and-statistics/pipeline/pipeline-incident-20-year-trends
12. TSA. (2021). Pipeline security guidelines. https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf
13. Virginia Places. (n.d.). Colonial Pipeline overview. http://www.virginiaplaces.org/transportation/line25.html
14. Cybersecurity Magazine. (2022): The real cost of OT cyber: Why process-level security is a financial decision. https://cybersecurity-magazine.com/the-real-cost-of-ot-cyber-why-process-level-security-is-a-financial-decision/
15. NE Digital. (2023): Calculating the true cost of a cyber attack: https://www.nedigital.com/en/blog/calculating-the-true-cost-of-a-cyber-attack
16. Ransomware.org. (2022): How downtime drives up the cost of a ransomware attack. https://ransomware.org/blog/how-downtime-drives-up-the-cost-of-a-ransomware-attack/
17. PHMSA. (2023). Valuation of crude oil spills in transportation incidents. U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration. https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2023-10/PHMSA-OilSpillCosts-Report-Final.pdf
18. Claroty. (2021). Lessons from the Colonial Pipeline attack. https://claroty.com/blog/lessons-from-the-colonial-pipeline-attack
19. Cyber Law International & CCDCOE. (2022). Colonial Pipeline ransomware attack (2021). NATO Cooperative Cyber Defence Centre of Excellence. https://cyberlaw.ccdcoe.org/wiki/Colonial_Pipeline_ransomware_attack_%282021%29

20. Cybersecurity Dive. (2022). Post-Colonial Pipeline attack: Lessons for critical infrastructure operators. https://www.cybersecuritydive.com/news/post-colonial-pipeline-attack/623859/
21. DP Center of Texas. (n.d.). Understanding the pipeline right-of-way. https://dpcoftexas.org/understanding-the-pipeline-right-of-way/
22. Fortress Information Security. (2022). The cost of cyberattacks on supply chains. https://www.fortressinfosec.com/blog/cost-of-cyber-attacks-on-supply-chains
23. Reuters. (2021a, May 9). U.S. government working to aid top fuel pipeline operator after cyberattacking. Reuters. https://www.reuters.com/business/energy/top-us-fuel-pipeline-operator-pushes-recover-cyberattack-2021-05-09/
24. Reuters. (2021b, May 12). Top U.S. fuel pipeline edges toward reopening, gasoline shortages worsen. Reuters. https://www.reuters.com/business/energy/top-us-fuel-pipeline-edges-toward-reopening-gasoline-shortages-worsen-2021-05-12/
25. Securitas Technology. (2022). Security threats in the oil and gas industry: Top risks and insights. https://www.securitastechnology.com/blog/security-threats-oil-gas-industry-top-risks-insights
26. ISA. (2020). 9 SCADA system vulnerabilities and how to secure them. International Society of Automation. https://gca.isa.org/blog/9-scada-system-vulnerabilities-and-how-to-secure-them
27. KU News. (2021, December 16). Cyberattack on Colonial Pipeline affected gas prices far less than initially reported, study finds. University of Kansas. https://news.ku.edu/news/article/2021/12/16/cyberattack-colonial-pipeline-affected-gas-prices-far-less-initially-reported-study-finds
28. LogicManager. (2021). Colonial Pipeline hack: What happened and what it means for risk management. https://www.logicmanager.com/resources/news/colonial-pipeline-hack/
29. Tenable. (2021, May 8). Colonial Pipeline ransomware attack: How to reduce risk in OT environments: https://www.tenable.com/blog/colonial-pipeline-ransomware-attack-how-to-reduce-risk-in-ot-environments
30. Tenable. (2022, July 14). Securing critical infrastructure: What we've learned from recent incidents. Tenable. https://www.tenable.com/blog/securing-critical-infrastructure-what-weve-learned-from-recent-incidents
31. UpGuard. (2023). TSA pipeline security guidelines explained: https://www.upguard.com/blog/tsa-pipeline-security-guidelines
32. IAMagazine. (2021). Colonial Pipeline hacked with single password: https://www.iamagazine.com/news/colonial-pipeline-hacked-with-single-password/?
33. Wikipedia (2025). Colonial Pipeline ransomware attack: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack?
34. CRN. (2021). "Colonial Pipeline hacked via inactive account without MFA": https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know?
35. GAO. (2021). Colonial Pipeline cyberattack highlights need for better federal and private-sector preparedness: https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic?
36. CISA. (2023). The attack on Colonial Pipeline: What we've learned and what we've done over the past two year https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
37. Science Publishing Group. (2024). Colonial Pipeline ransomware attack: Bitter lessons for critical energy infrastructure https://www.sciencepublishinggroup.com/article/10.11648/j.ogce.20241205.11?
38. CISA. (2020). Connecting to the NICC and the NCCIC (NIPP Supplemental Tool https://www.cisa.gov/resources-tools/resources/connecting-nicc-and-nccic
39. CISA & FBI. (2021) Joint cybersecurity advisory on DarkSide ransomware: https://nsarchive.gwu.edu/sites/default/files/documents/20706746/06-20210211-aa21-131a_darkside_ransomware.pdf?

40. GAO. (2017). Cybersecurity: DHS's National Integration Center performs required functions but needs to evaluate its activities more completely (GAO-17-163): https://www.gao.gov/assets/gao-17-163.pdf?
41. CISA. (2025). State and Local Cybersecurity Grant Program (SLCGP) fact sheet. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/cybergrants/slcgp
42. GAO. (2025). DHS grant program addresses cybersecurity risks for state, local, tribal, and territorial governments. U.S. Government Accountability Office. https://www.gao.gov/products/gao-25-107313
43. PHMSA. (2025c). Natural Gas Distribution Infrastructure Safety and Modernization (NGDISM) Grant Program. Pipeline and Hazardous Materials Safety Administration. https://www.phmsa.dot.gov/about-phmsa/working-phmsa/grants/pipeline/natural-gas-distribution-infrastructure-safety-and-modernization-grants

# Appendix:

**Colonial Pipeline Network:**




**Matrix for Cascade Network**:

| Adjacency matrix | Houston | Opelousas | Meridian | Birmingham | Atlanta | Belton | Charlotte | Spartanburg | Greensboro | Mitchell | Richmond | Dorsey | Baltimore | Nashville | Knoxville | Linden |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Houston** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Opelousas** | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Meridian** | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Birmingham** | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Atlanta** | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| **Belton** | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Charlotte** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Spartanburg** | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Greensboro** | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Mitchell** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| **Richmond** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Dorsey** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| **Baltimore** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| **Nashville** | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Knoxville** | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Linden** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

Matrix for Flow Network:

| **Adjacency matrix** | **Houston** | **Opelousas** | **Meridian** | **Birmingham** | **Atlanta** | **Belton** | **Charlotte** | **Spartanburg** | **Greensboro** | **Mitchell** | **Richmond** | **Dorsey** | **Baltimore** | **Nashville** | **Knoxville** | **Linden** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Houston** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Opelousas** | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Meridian** | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Birmingham** | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Atlanta** | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| **Belton** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Charlotte** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Spartanburg** | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Greensboro** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Mitchell** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| **Richmond** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Dorsey** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| **Baltimore** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Nashville** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Knoxville** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Linden** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

## Cascade Network characterization:

Figure 9.3 - Cascade Network Analysis

```
Adjacency Matrix C:
[[0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 1 0 1 0 0 0 0 0 0 0 1 1 0]
 [0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0]
 [0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 1 0 1 1 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 1]
 [0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0]
 [0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0]]
```

```
Degree of Node 0 = 1
Degree of Node 1 = 2
Degree of Node 2 = 2
Degree of Node 3 = 2
Degree of Node 4 = 4
Degree of Node 5 = 2
Degree of Node 6 = 2
Degree of Node 7 = 2
Degree of Node 8 = 2
Degree of Node 9 = 3
Degree of Node 10 = 1
Degree of Node 11 = 3
Degree of Node 12 = 1
Degree of Node 13 = 1
Degree of Node 14 = 1
Degree of Node 15 = 1

Network Degree = 4
Number of Nodes = 16
Number of Links (undirected) = 15
```

```
Link Robustness = 0.5
Links that can be removed = 7

Eigenvalues of connection matrix C:
[ 2.20018749e+00  2.06389270e+00  1.59521294e+00  1.41421356e+00
 -2.20018749e+00 -2.06389270e+00  9.56001118e-01 -1.59521294e+00
 -1.41421356e+00  5.50854906e-01  3.70726733e-01 -9.56001118e-01
 -5.50854906e-01 -3.70726733e-01 -8.72061348e-18 -4.57623322e-35]

Spectral Radius = 2.2001874911416746

Node Robustness = 0.5454932799926513
Nodes that can be removed = 8
Blocking Nodes = 8

Degree Centrality:
{0: 0.06666666666666667, 1: 0.13333333333333333, 2: 0.13333333333333333, 3: 0.13333333333333333, 4: 0.26666666666666666, 5: 0.1333333333333

Betweenness Centrality:
{0: 0.0, 1: 0.13333333333333336, 2: 0.24761904761904763, 3: 0.34285714285714286, 4: 0.6000000000000001, 5: 0.5333333333333334, 6: 0.5142857

Eigenvector Centrality (numpy):
```

```
, 5: 0.13333333333333333, 6: 0.13333333333333333, 7: 0.13333333333333333, 8: 0.13333333333333333, 9: 0.2, 10: 0.06666666666666667, 11: 0.2,
```

```
333334, 6: 0.5142857142857143, 7: 0.5333333333333334, 8: 0.4761904761904762, 9: 0.44761904761904764, 10: 0.0, 11: 0.2571428571428572, 12: 0.
```

```
 5: 0.37891478142710017, 6: 0.19320892822628527, 7: 0.26003407071299733, 8: 0.16506179634736468, 9: 0.16995797136255958, 10: 0.0772470401031
```

```
3, 9: 0.2, 10: 0.06666666666666667, 11: 0.2, 12: 0.06666666666666667, 13: 0.06666666666666667, 14: 0.06666666666666667, 15: 0.0666666666666
```

```
4764, 10: 0.0, 11: 0.2571428571428572, 12: 0.0, 13: 0.0, 14: 0.0, 15: 0.0}
```

```
, 9: 0.16995797136255958, 10: 0.07724704010310036, 11: 0.1316305661612524, 12: 0.059826976878661335, 13: 0.26072754885717686, 14: 0.260727548
```

```
11: 0.2, 12: 0.06666666666666667, 13: 0.06666666666666667, 14: 0.06666666666666667, 15: 0.06666666666666667}
```

```
2, 12: 0.0, 13: 0.0, 14: 0.0, 15: 0.0}
```

```
4704010310036, 11: 0.1316305661612524, 12: 0.059826976878661335, 13: 0.26072754885717686, 14: 0.26072754885717686, 15: 0.059826976878661335}
```

## Flow Network characterization:

```
Figure 9.3

Adjacency Matrix C:
[[0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0]
 [0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
 [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]]
Degree of Node 0 = 1
Degree of Node 1 = 1
Degree of Node 2 = 1
```

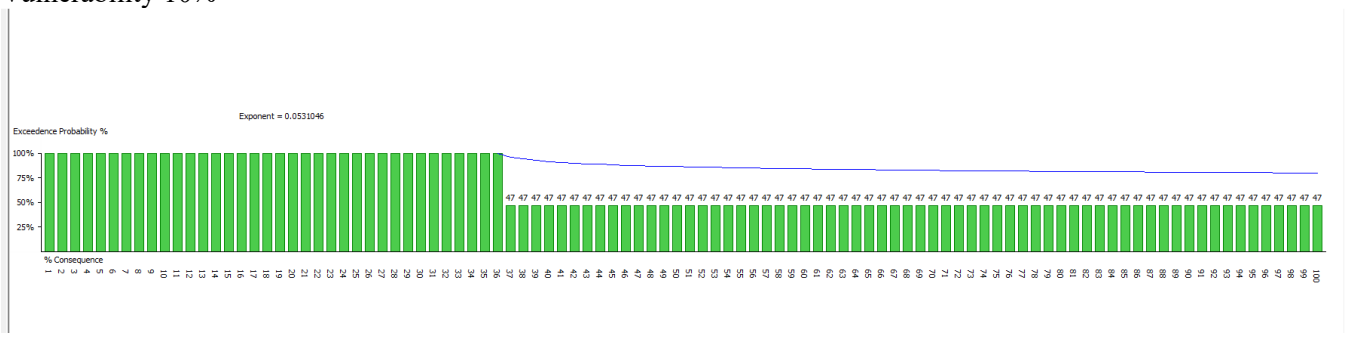
```
Degree of Node 0 = 1
Degree of Node 1 = 1
Degree of Node 2 = 1
Degree of Node 3 = 1
Degree of Node 4 = 3
Degree of Node 5 = 1
Degree of Node 6 = 1
Degree of Node 7 = 1
Degree of Node 8 = 1
Degree of Node 9 = 2
Degree of Node 10 = 0
Degree of Node 11 = 2
Degree of Node 12 = 0
Degree of Node 13 = 0
Degree of Node 14 = 0
Degree of Node 15 = 0
NetworkDegree =  3

Number of Nodes =  16

Number of Links Undirected =  7
```

```
Number of Links Undirected =  7

Link Robustness =  0.33333333333333337

Links that can be removed =  2


Eigenvalues of connection matrix C=
[0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.]

Spectral radius of connection matrix C=
0.0

Node Robustness =  0

Nodes that can be removed = 0

Blocking Nodes = 16
```

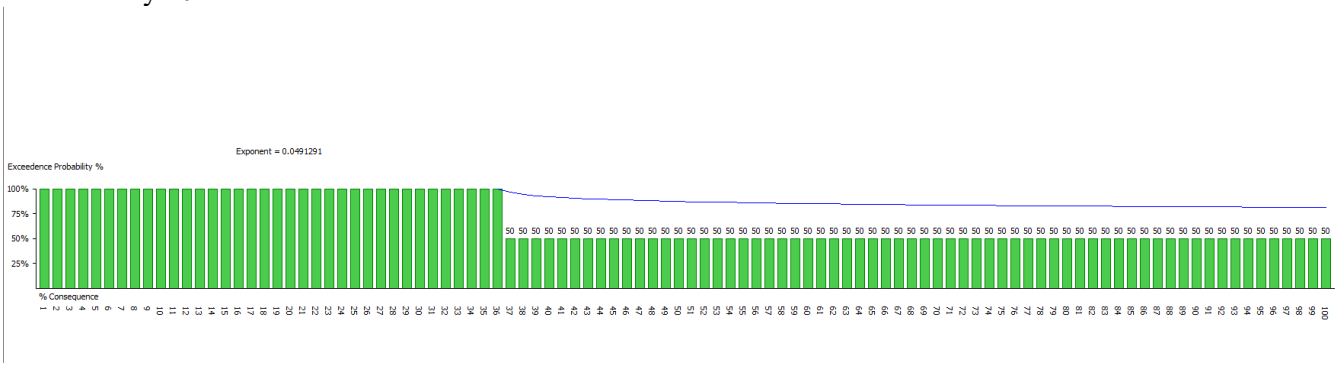
```
Eigenvalues of connection matrix C=
[0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.]

Spectral radius of connection matrix C=
0.0

Node Robustness =  0

Nodes that can be removed = 0

Blocking Nodes = 16


Degree Centrality of connection matrix C=
{0: 0.06666666666666667, 1: 0.13333333333333333, 2: 0.13333333333333333, 3: 0.13333333333333333, 4: 0.26666666666666666, 5: 0.13333333333333

Betweenness Centrality of connection matrix C=
{0: 0.0, 1: 0.13333333333333336, 2: 0.24761904761904763, 3: 0.34285714285714286, 4: 0.6000000000000001, 5: 0.5333333333333334, 6: 0.5142857
```

The following fractal dimension q values were observed for flow network:

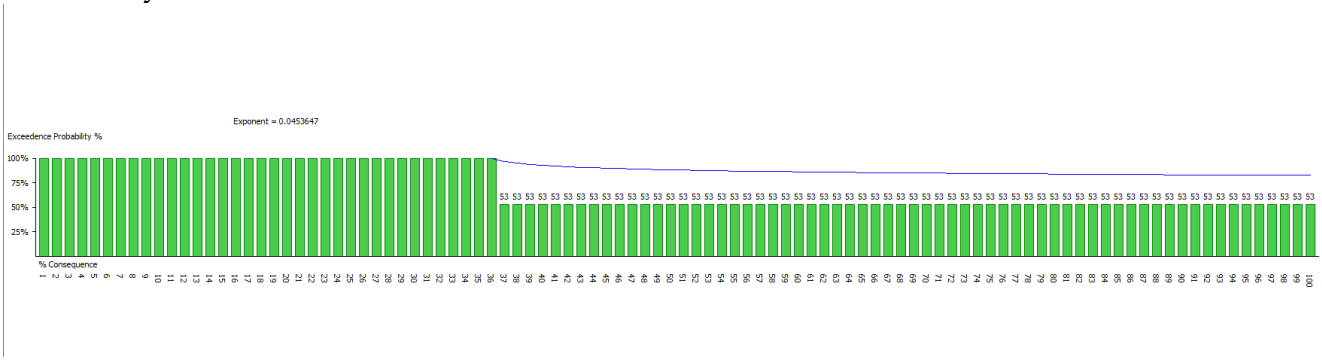
Vulnerability 10%



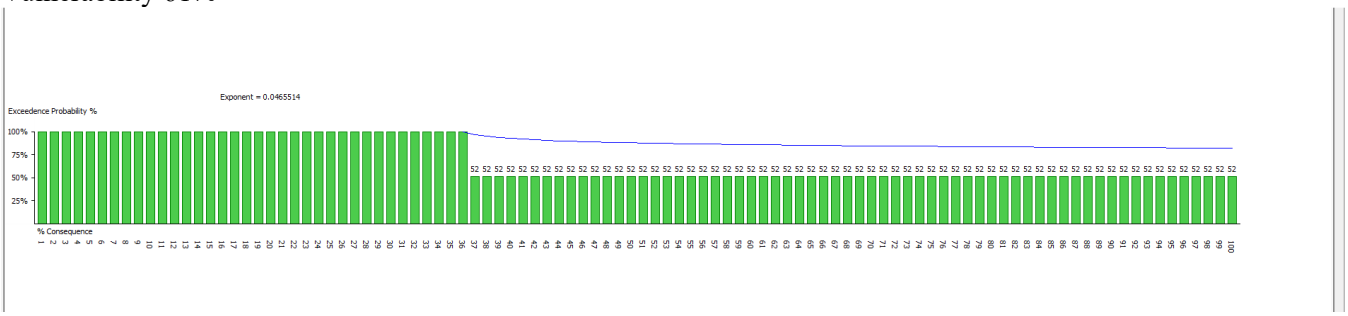

Vulnerability 20%



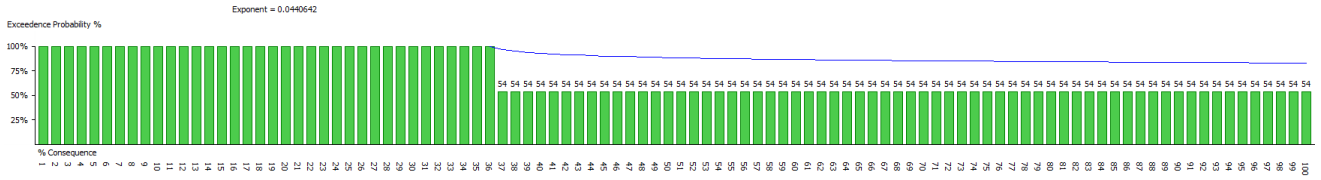

Vulnerability 52%



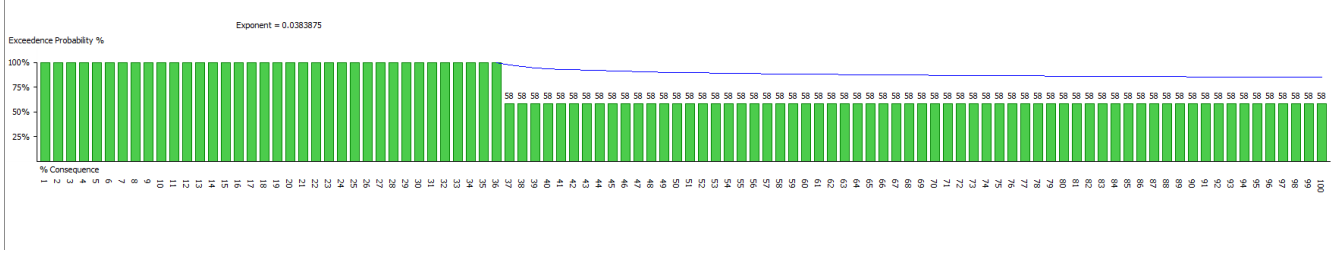

Vulnerability 61%




Vulnerability 73%

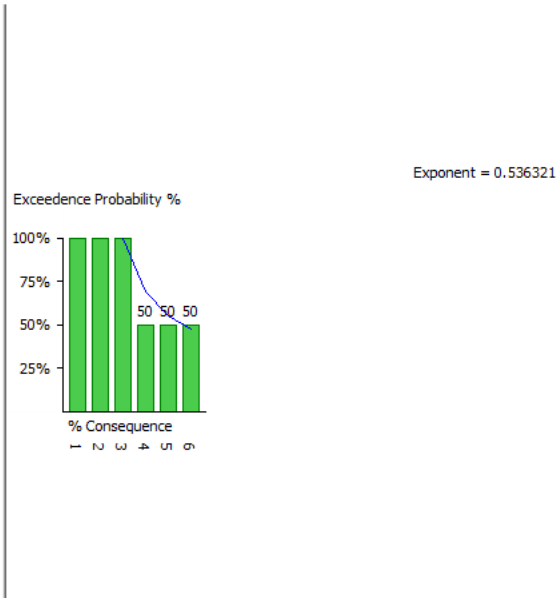



Vulnerability 80%

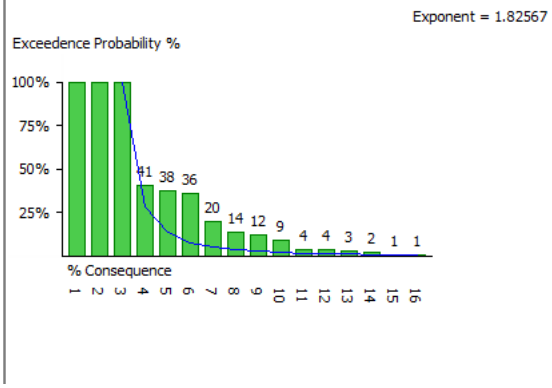



The following fractal dimension q values were observed for Cascade network:

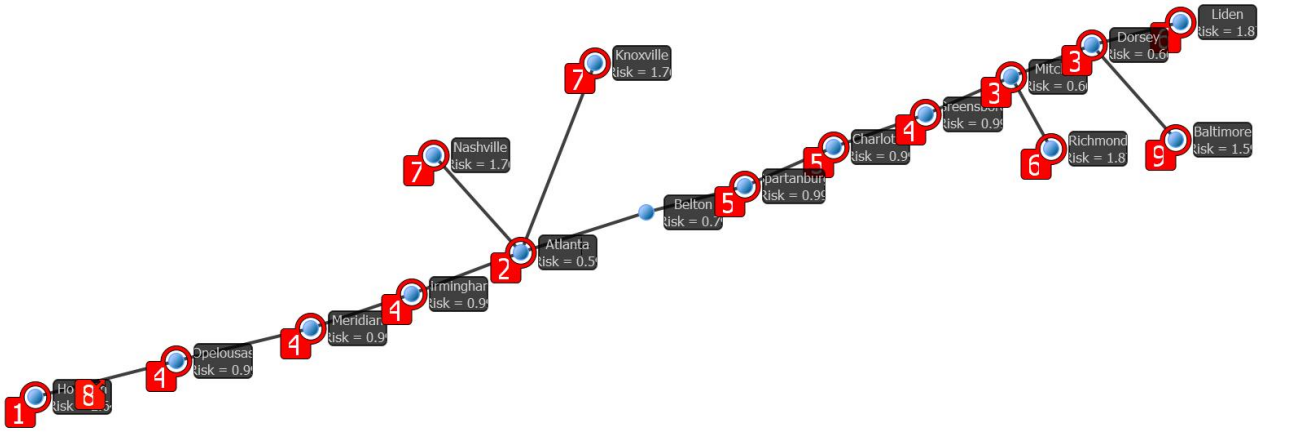
Vulnerability 90%



Vulnerability 20%




**Cascade Network:**



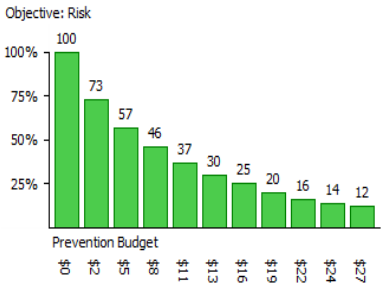
Data Table

| | Name | Threat (%) | Vulnerability (%) | Consequence $(millions) | Prevention Cost $(millions) | **Response Cost $(millions)** | Risk Initial $(millions) | Risk Reduced $(millions) |
|---|---|---|---|---|---|---|---|---|
| 1 | Houston | 100.00 | 30.00 | 11.15 | 1.20 | 0.60 | 3.35 | 2.64 |
| 2 | Meridian | 100.00 | 30.00 | 7.80 | 0.90 | 0.45 | 2.34 | 0.99 |
| 3 | Birmingham | 100.00 | 30.00 | 7.80 | 0.90 | 0.45 | 2.34 | 0.99 |
| 4 | Atlanta | 100.00 | 30.00 | 10.04 | 1.08 | 0.54 | 3.01 | 0.59 |
| 5 | Belton | 100.00 | 30.00 | 7.00 | 0.72 | 0.36 | 2.10 | 0.79 |
| 6 | Charlotte | 100.00 | 30.00 | 7.50 | 0.90 | 0.45 | 2.25 | 0.99 |
| 7 | Spartanburg | 100.00 | 30.00 | 7.50 | 0.90 | 0.45 | 2.25 | 0.99 |
| 8 | Greensboro | 100.00 | 30.00 | 7.80 | 0.90 | 0.45 | 2.34 | 0.99 |
| 9 | Nashville | 100.00 | 30.00 | 6.50 | 0.80 | 0.45 | 1.95 | 1.76 |
| 10 | Knoxville | 100.00 | 30.00 | 6.50 | 0.80 | 0.40 | 1.95 | 1.76 |
| 11 | Meri-Birm | 100.00 | 72.00 | 7.80 | 0.90 | 0.45 | 5.62 | 1.33 |
| 12 | Birm-Atlan | 100.00 | 95.00 | 8.00 | 1.00 | 0.50 | 7.60 | 1.34 |
| **13** | Atla-Belt | 100.00 | 95.00 | 8.00 | 1.00 | 0.50 | 7.60 | 1.34 |
| 14 | Atl-Nash | 100.00 | 68.00 | 6.50 | 0.80 | 0.40 | 4.42 | 1.21 |
| 15 | Atl-Knox | 100.00 | 68.00 | 6.50 | 0.80 | 0.40 | 4.42 | 1.21 |
| 16 | Belt-Spart | 100.00 | 72.00 | 7.00 | 0.85 | 0.42 | 5.04 | 1.26 |
| 17 | Spart-Charlo | 100.00 | 72.00 | 7.50 | 0.90 | 0.45 | 5.40 | 1.33 |
| 18 | Charlo - Greens | 100.00 | 72.00 | 7.50 | 0.90 | 0.45 | 5.40 | 1.33 |
| 19 | Mitchell | 100.00 | 30.00 | 7.80 | 0.90 | 0.45 | 2.34 | 0.66 |
| 20 | Richmond | 100.00 | 30.00 | 7.00 | 0.85 | 0.42 | 2.10 | 1.87 |
| 21 | Gren-Mitc | 100.00 | 83.00 | 7.50 | 0.90 | 0.45 | 6.22 | 1.26 |
| 22 | Baltimore | 100.00 | 30.00 | 6.50 | 0.72 | 0.36 | 1.95 | 1.59 |
| 23 | Dorsey | 100.00 | 30.00 | 7.80 | 0.90 | 0.45 | 2.34 | 0.66 |
| 24 | Mitch-Dors | 100.00 | 80.00 | 7.80 | 0.90 | 0.45 | 6.24 | 1.28 |
| 25 | Opelousas | 100.00 | 30.00 | 7.80 | 0.90 | 0.45 | 2.34 | 0.99 |

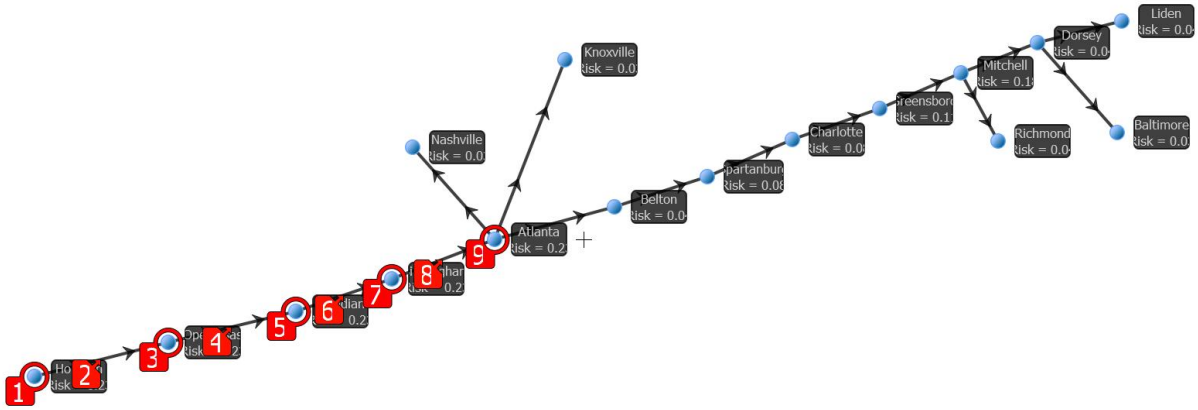
Data Table

| | Risk Reduced $(millions) | Flow Consequence $(millions) | Prevention Allocation $(millions) | Response Allocation $(millions) | Attack Allocation $(millions) | Vulnerability Reduced (%) |
|---|---|---|---|---|---|---|
| 1 | 2.64 | | 0.16 | 0.00 | 0.00 | 23.70 |
| 2 | 0.99 | | 0.43 | 0.00 | 0.00 | 12.71 |
| 3 | 0.99 | | 0.43 | 0.00 | 0.00 | 12.71 |
| 4 | 0.59 | | 0.98 | 0.00 | 0.00 | 5.92 |
| **5** | 0.79 | | 0.39 | 0.00 | 0.00 | 11.33 |
| 6 | 0.99 | | 0.41 | 0.00 | 0.00 | 13.22 |
| 7 | 0.99 | | 0.41 | 0.00 | 0.00 | 13.22 |
| 8 | 0.99 | | 0.43 | 0.00 | 0.00 | 12.71 |
| 9 | 1.76 | | 0.05 | 0.00 | 0.00 | 27.11 |
| 10 | 1.76 | | 0.05 | 0.00 | 0.00 | 27.11 |
| 11 | 1.33 | | 0.49 | 0.00 | 0.00 | 17.07 |
| 12 | 1.34 | | 0.59 | 0.00 | 0.00 | 16.75 |
| 13 | 1.34 | | 0.59 | 0.00 | 0.00 | 16.75 |
| 14 | 1.21 | | 0.40 | 0.00 | 0.00 | 18.61 |
| 15 | 1.21 | | 0.40 | 0.00 | 0.00 | 18.61 |
| 16 | 1.26 | | 0.44 | 0.00 | 0.00 | 17.97 |
| 17 | 1.33 | | 0.47 | 0.00 | 0.00 | 17.75 |
| 18 | 1.33 | | 0.47 | 0.00 | 0.00 | 17.75 |
| 19 | 0.66 | | 0.64 | 0.00 | 0.00 | 8.47 |
| 20 | 1.87 | | 0.05 | 0.00 | 0.00 | 26.74 |
| 21 | 1.26 | | 0.51 | 0.00 | 0.00 | 16.86 |
| 22 | 1.59 | | 0.08 | 0.00 | 0.00 | 24.40 |
| 23 | 0.66 | | 0.64 | 0.00 | 0.00 | 8.47 |
| 24 | 1.28 | | 0.51 | 0.00 | 0.00 | 16.42 |
| 25 | 0.99 | | 0.43 | 0.00 | 0.00 | 12.71 |

| | ons) | Attack Allocation $(millions) | Vulnerability Reduced (%) | Consequence Reduced $(millions) | Calculated Threat (%) | Weight | Weight x Objective | Degrees | Rank |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | 0.00 | 23.70 | 11.15 | 100.00 | 0.250 | 0.661 | 1 | 1 |
| 2 | | 0.00 | 12.71 | 7.80 | 100.00 | 0.500 | 0.496 | 2 | 4 |
| 3 | | 0.00 | 12.71 | 7.80 | 100.00 | 0.500 | 0.496 | 2 | 4 |
| 4 | | 0.00 | 5.92 | 10.04 | 100.00 | 1.000 | 0.595 | 4 | 2 |
| 5 | | 0.00 | 11.33 | 7.00 | 100.00 | 0.500 | 0.396 | 2 | 10 |
| 6 | | 0.00 | 13.22 | 7.50 | 100.00 | 0.500 | 0.496 | 2 | 5 |
| 7 | | 0.00 | 13.22 | 7.50 | 100.00 | 0.500 | 0.496 | 2 | 5 |
| 8 | | 0.00 | 12.71 | 7.80 | 100.00 | 0.500 | 0.496 | 2 | 4 |
| 9 | | 0.00 | 27.11 | 6.50 | 100.00 | 0.250 | 0.441 | 1 | 7 |
| 10 | | 0.00 | 27.11 | 6.50 | 100.00 | 0.250 | 0.441 | 1 | 7 |
| 11 | | 0.00 | 17.07 | 7.80 | 100.00 | 0.250 | 0.333 | 1 | 12 |
| 12 | | 0.00 | 16.75 | 8.00 | 100.00 | 0.250 | 0.335 | 1 | 11 |
| 13 | | 0.00 | 16.75 | 8.00 | 100.00 | 0.250 | 0.335 | 1 | 11 |
| 14 | | 0.00 | 18.61 | 6.50 | 100.00 | 0.250 | 0.302 | 1 | 18 |
| 15 | | 0.00 | 18.61 | 6.50 | 100.00 | 0.250 | 0.302 | 1 | 18 |
| 16 | | 0.00 | 17.97 | 7.00 | 100.00 | 0.250 | 0.314 | 1 | 17 |
| 17 | | 0.00 | 17.75 | 7.50 | 100.00 | 0.250 | 0.333 | 1 | 13 |
| 18 | | 0.00 | 17.75 | 7.50 | 100.00 | 0.250 | 0.333 | 1 | 13 |
| 19 | | 0.00 | 8.47 | 7.80 | 100.00 | 0.750 | 0.496 | 3 | 3 |
| 20 | | 0.00 | 26.74 | 7.00 | 100.00 | 0.250 | 0.468 | 1 | 6 |
| 21 | | 0.00 | 16.86 | 7.50 | 100.00 | 0.250 | 0.316 | 1 | 16 |
| 22 | | 0.00 | 24.40 | 6.50 | 100.00 | 0.250 | 0.396 | 1 | 9 |
| 23 | | 0.00 | 8.47 | 7.80 | 100.00 | 0.750 | 0.496 | 3 | 3 |
| 24 | | 0.00 | 16.42 | 7.80 | 100.00 | 0.250 | 0.320 | 1 | 15 |
| 25 | | 0.00 | 12.71 | 7.80 | 100.00 | 0.500 | 0.496 | 2 | 4 |




## Flow Network:




| | Name | Threat (%) | **Vulnerability (%)** | Consequence $(millions) | Prevention Cost $(millions) | Response |
|---|---|---|---|---|---|---|
| 1 | Houston | 100.00 | 90.00 | 5.00 | 1.50 | 0.75 |
| 2 | Meridian | 100.00 | 80 | 4.50 | 1.50 | 0.75 |
| 3 | Birmingham | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 4 | Atlanta | 100.00 | 85.00 | 5.00 | 1.50 | 0.75 |
| 5 | Belton | 100.00 | 75.00 | 4.50 | 1.25 | 0.63 |
| 6 | Charlotte | 100.00 | 75.00 | 4.50 | 1.25 | 0.63 |
| 7 | Spartanburg | 100.00 | 77.00 | 4.50 | 1.25 | 0.63 |
| 8 | Greensboro | 100.00 | 76.00 | 4.50 | 1.25 | 0.63 |
| 9 | Nashville | 100.00 | 70.00 | 4.00 | 0.75 | 0.38 |
| 10 | Knoxville | 100.00 | 70.00 | 4.00 | 0.75 | 0.38 |
| 11 | Liden | 100.00 | 75.00 | 4.00 | 1.25 | 0.63 |
| 12 | Meri-Birm | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 13 | Birm-Atlan | 100.00 | 80.00 | 4.75 | 1.25 | 0.63 |
| 14 | Atla-Belt | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 15 | Atl-Nash | 100.00 | 80.00 | 4.00 | 0.75 | 0.38 |
| 16 | Atl-Knox | 100.00 | 80.00 | 4.00 | 0.75 | 0.38 |
| 17 | Belt-Spart | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 18 | Spart-Charlo | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 19 | Charlo - Greens | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 20 | Mitchell | 100.00 | 78.00 | 4.50 | 1.50 | 0.75 |
| 21 | Richmond | 100.00 | 75.00 | 4.50 | 1.25 | 0.63 |
| 22 | Gren-Mitc | 100.00 | 80.00 | 4.75 | 1.25 | 0.63 |
| 23 | Baltimore | 100.00 | 70.00 | 4.00 | 0.75 | 0.38 |
| 24 | Dorsey | 100.00 | 78.00 | 4.50 | 1.50 | 0.75 |
| 25 | Mitch-Dors | 100.00 | 80.00 | 4.50 | 1.50 | 0.75 |

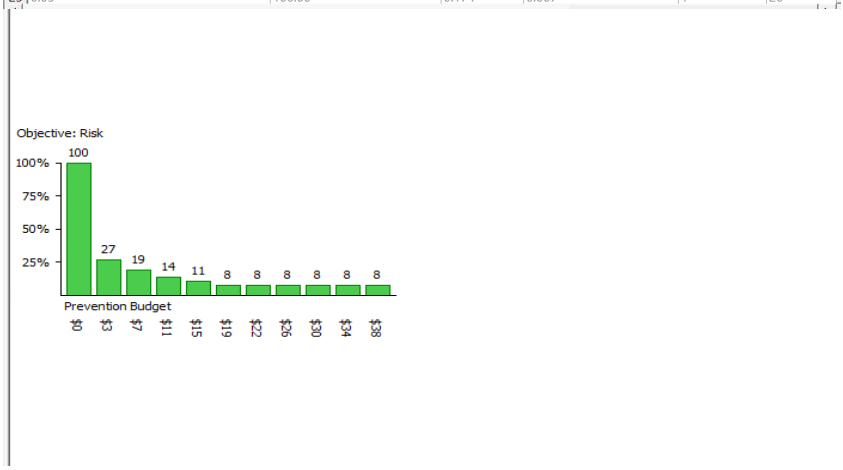
| | Name | Threat (%) | Vulnerability (%) | Consequence $(millions) | Prevention Cost $(millions) | Response |
|---|---|---|---|---|---|---|
| 7 | Spartanburg | 100.00 | 77.00 | 4.50 | 1.25 | 0.63 |
| 8 | Greensboro | 100.00 | 76.00 | 4.50 | 1.25 | 0.63 |
| 9 | Nashville | 100.00 | 70.00 | 4.00 | 0.75 | 0.38 |
| 10 | Knoxville | 100.00 | 70.00 | 4.00 | 0.75 | 0.38 |
| 11 | Liden | 100.00 | 75.00 | 4.00 | 1.25 | 0.63 |
| 12 | Meri-Birm | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 13 | Birm-Atlan | 100.00 | 80.00 | 4.75 | 1.25 | 0.63 |
| 14 | Atla-Belt | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 15 | Atl-Nash | 100.00 | 80.00 | 4.00 | 0.75 | 0.38 |
| 16 | Atl-Knox | 100.00 | 80.00 | 4.00 | 0.75 | 0.38 |
| 17 | Belt-Spart | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 18 | Spart-Charlo | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 19 | Charlo - Greens | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 20 | Mitchell | 100.00 | 78.00 | 4.50 | 1.50 | 0.75 |
| 21 | Richmond | 100.00 | 75.00 | 4.50 | 1.25 | 0.63 |
| 22 | Gren-Mitc | 100.00 | 80.00 | 4.75 | 1.25 | 0.63 |
| 23 | Baltimore | 100.00 | 70.00 | 4.00 | 0.75 | 0.38 |
| 24 | Dorsey | 100.00 | 78.00 | 4.50 | 1.50 | 0.75 |
| 25 | Mitch-Dors | 100.00 | 80.00 | 4.50 | 1.50 | 0.75 |
| 26 | Opelousas | 100.00 | 80.00 | 4.50 | 1.50 | 0.75 |
| 27 | Hous-Ope | 100.00 | 80.00 | 5.00 | 1.50 | 0.75 |
| 28 | Ope-Meri | 100.00 | 80.00 | 4.50 | 1.50 | 0.75 |
| 29 | Dor-Li | 100.00 | 80.00 | 4.00 | 1.25 | 0.63 |
| 30 | Mitch-Richm | 100.00 | 80.00 | 4.50 | 1.25 | 0.63 |
| 31 | Dor-Bal | 100.00 | 80.00 | 4.00 | 0.75 | 0.38 |

| | Response Cost $(millions) | Risk Initial $(millions) | Risk Reduced $(millions) | Flow Consequence $(millions) | Pr |
|---|---|---|---|---|---|
| 1 | 0.75 | 4.50 | 0.23 | 4.50 | 1.50 |
| 2 | 0.75 | 3.60 | 0.23 | 4.50 | 1.50 |
| 3 | 0.63 | 3.60 | 0.23 | 4.50 | 1.25 |
| 4 | 0.75 | 4.25 | 0.23 | 4.50 | 1.50 |
| 5 | 0.63 | 3.38 | 0.04 | 0.00 | 0.00 |
| 6 | 0.63 | 3.38 | 0.08 | 1.62 | 1.23 |
| 7 | 0.63 | 3.46 | 0.08 | 1.62 | 1.25 |
| 8 | 0.63 | 3.42 | 0.11 | 1.62 | 1.12 |
| 9 | 0.38 | 2.80 | 0.03 | 0.00 | 0.00 |
| 10 | 0.38 | 2.80 | 0.03 | 0.00 | 0.00 |
| 11 | 0.63 | 3.00 | 0.04 | 0.00 | 0.00 |
| 12 | 0.63 | 3.60 | 0.23 | 4.50 | 1.25 |
| 13 | 0.63 | 3.60 | 0.23 | 4.50 | 1.25 |
| 14 | 0.63 | 0.00 | 0.04 | 0.00 | 0.00 |
| 15 | 0.38 | 0.00 | 0.04 | 0.00 | 0.00 |
| 16 | 0.38 | 0.00 | 0.04 | 0.00 | 0.00 |
| 17 | 0.63 | 1.30 | 0.08 | 1.62 | 1.25 |
| 18 | 0.63 | 1.30 | 0.08 | 1.62 | 1.25 |
| 19 | 0.63 | 1.30 | 0.09 | 1.62 | 1.19 |
| 20 | 0.75 | 3.51 | 0.18 | 1.62 | 1.06 |
| 21 | 0.63 | 3.38 | 0.04 | 0.00 | 0.00 |
| 22 | 0.63 | 1.30 | 0.12 | 1.62 | 1.06 |
| 23 | 0.38 | 2.80 | 0.03 | 0.00 | 0.00 |
| 24 | 0.75 | 3.51 | 0.04 | 0.00 | 0.00 |
| 25 | 0.75 | 0.00 | 0.04 | 0.00 | 0.00 |

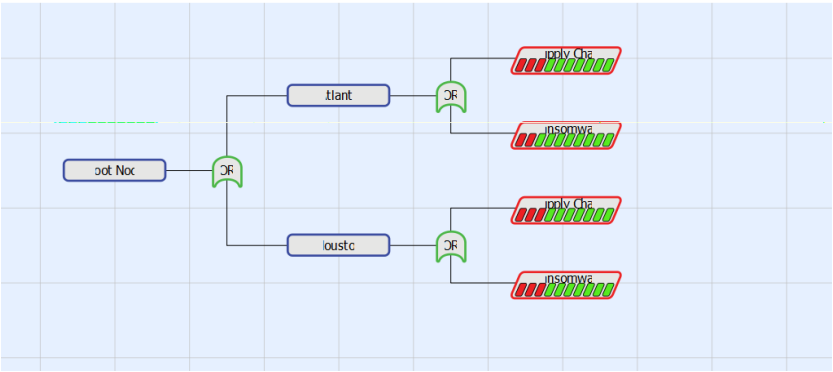
| | Response Allocation $(millions) | Attack Allocation $(millions) | Vulnerability Reduced (%) | Consequence Reduced $(r |
|---|---|---|---|---|
| 1 | 0.00 | 0.00 | 5.00 | 4.50 |
| 2 | 0.00 | 0.00 | 5.00 | 4.50 |
| 3 | 0.00 | 0.00 | 5.00 | 4.50 |
| 4 | 0.00 | 0.00 | 5.00 | 4.50 |
| 5 | 0.00 | 0.00 | 75.00 | 0.05 |
| 6 | 0.00 | 0.00 | 5.23 | 1.62 |
| 7 | 0.00 | 0.00 | 5.00 | 1.62 |
| 8 | 0.00 | 0.00 | 6.70 | 1.62 |
| 9 | 0.00 | 0.00 | 70.00 | 0.05 |
| 10 | 0.00 | 0.00 | 70.00 | 0.05 |
| 11 | 0.00 | 0.00 | 75.00 | 0.05 |
| 12 | 0.00 | 0.00 | 5.00 | 4.50 |
| 13 | 0.00 | 0.00 | 5.00 | 4.50 |
| 14 | 0.00 | 0.00 | 80.00 | 0.05 |
| 15 | 0.00 | 0.00 | 80.00 | 0.05 |
| **16** | 0.00 | 0.00 | 80.00 | 0.05 |
| 17 | 0.00 | 0.00 | 5.00 | 1.62 |
| 18 | 0.00 | 0.00 | 5.00 | 1.62 |
| 19 | 0.00 | 0.00 | 5.75 | 1.62 |
| 20 | 0.00 | 0.00 | 11.14 | 1.62 |
| 21 | 0.00 | 0.00 | 75.00 | 0.05 |
| 22 | 0.00 | 0.00 | 7.67 | 1.62 |
| 23 | 0.00 | 0.00 | 70.00 | 0.05 |
| 24 | 0.00 | 0.00 | 78.00 | 0.05 |
| 25 | 0.00 | 0.00 | 80.00 | 0.05 |

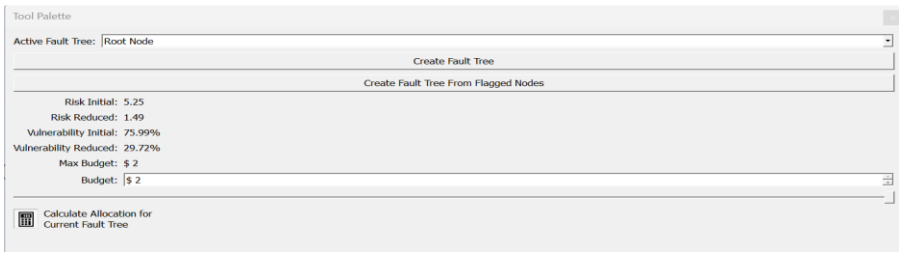
| | Vulnerability Reduced (%) | Consequence Reduced $(millions) | Calculated Threat (%) | Weight | Weight x Objecti |
|---|---|---|---|---|---|
| 1 | 5.00 | 4.50 | 100.00 | 1.000 | 0.225 |
| 2 | 5.00 | 4.50 | 100.00 | 0.826 | 0.186 |
| 3 | 5.00 | 4.50 | 100.00 | 0.739 | 0.166 |
| 4 | 5.00 | 4.50 | 100.00 | 0.652 | 0.147 |
| 5 | 75.00 | 0.05 | 100.00 | 0.565 | 0.021 |
| 6 | 5.23 | 1.62 | 100.00 | 0.391 | 0.033 |
| 7 | 5.00 | 1.62 | 100.00 | 0.478 | 0.039 |
| 8 | 6.70 | 1.62 | 100.00 | 0.304 | 0.033 |
| 9 | 70.00 | 0.05 | 100.00 | 0.043 | 0.002 |
| 10 | 70.00 | 0.05 | 100.00 | 0.043 | 0.002 |
| 11 | 75.00 | 0.05 | 100.00 | 0.043 | 0.002 |
| 12 | 5.00 | 4.50 | 100.00 | 0.783 | 0.176 |
| 13 | 5.00 | 4.50 | 100.00 | 0.696 | 0.157 |
| 14 | 80.00 | 0.05 | 100.00 | 0.609 | 0.024 |
| 15 | 80.00 | 0.05 | 100.00 | 0.087 | 0.003 |
| **16** | 80.00 | 0.05 | 100.00 | 0.087 | 0.003 |
| 17 | 5.00 | 1.62 | 100.00 | 0.522 | 0.042 |
| 18 | 5.00 | 1.62 | 100.00 | 0.435 | 0.035 |
| 19 | 5.75 | 1.62 | 100.00 | 0.348 | 0.032 |
| 20 | 11.14 | 1.62 | 100.00 | 0.217 | 0.039 |
| 21 | 75.00 | 0.05 | 100.00 | 0.043 | 0.002 |
| 22 | 7.67 | 1.62 | 100.00 | 0.261 | 0.032 |
| 23 | 70.00 | 0.05 | 100.00 | 0.043 | 0.002 |
| 24 | 78.00 | 0.05 | 100.00 | 0.130 | 0.005 |
| 25 | 80.00 | 0.05 | 100.00 | 0.174 | 0.007 |

| | Consequence Reduced $(millions) | Calculated Threat (%) | Weight | Weight x Objective | Degrees | Rank |
|---|---|---|---|---|---|---|
| 1 | 4.50 | 100.00 | 1.000 | 0.225 | 1 | 1 |
| 2 | 4.50 | 100.00 | 0.826 | 0.186 | 2 | 5 |
| 3 | 4.50 | 100.00 | 0.739 | 0.166 | 2 | 7 |
| 4 | 4.50 | 100.00 | 0.652 | 0.147 | 4 | 9 |
| 5 | 0.05 | 100.00 | 0.565 | 0.021 | 2 | 19 |
| 6 | 1.62 | 100.00 | 0.391 | 0.033 | 2 | 14 |
| 7 | 1.62 | 100.00 | 0.478 | 0.039 | 2 | 12 |
| 8 | 1.62 | 100.00 | 0.304 | 0.033 | 2 | 15 |
| 9 | 0.05 | 100.00 | 0.043 | 0.002 | 1 | 24 |
| 10 | 0.05 | 100.00 | 0.043 | 0.002 | 1 | 24 |
| 11 | 0.05 | 100.00 | 0.043 | 0.002 | 1 | 23 |
| 12 | 4.50 | 100.00 | 0.783 | 0.176 | 1 | 6 |
| 13 | 4.50 | 100.00 | 0.696 | 0.157 | 1 | 8 |
| 14 | 0.05 | 100.00 | 0.609 | 0.024 | 1 | 18 |
| 15 | 0.05 | 100.00 | 0.087 | 0.003 | 1 | 22 |
| 16 | 0.05 | 100.00 | 0.087 | 0.003 | 1 | 22 |
| 17 | 1.62 | 100.00 | 0.522 | 0.042 | 1 | 10 |
| 18 | 1.62 | 100.00 | 0.435 | 0.035 | 1 | 13 |
| 19 | 1.62 | 100.00 | 0.348 | 0.032 | 1 | 16 |
| 20 | 1.62 | 100.00 | 0.217 | 0.039 | 3 | 11 |
| 21 | 0.05 | 100.00 | 0.043 | 0.002 | 1 | 23 |
| 22 | 1.62 | 100.00 | 0.261 | 0.032 | 1 | 17 |
| 23 | 0.05 | 100.00 | 0.043 | 0.002 | 1 | 24 |
| 24 | 0.05 | 100.00 | 0.130 | 0.005 | 3 | 21 |
| 25 | 0.05 | 100.00 | 0.174 | 0.007 | 1 | 20 |




## Cascade Network Fault Tree:



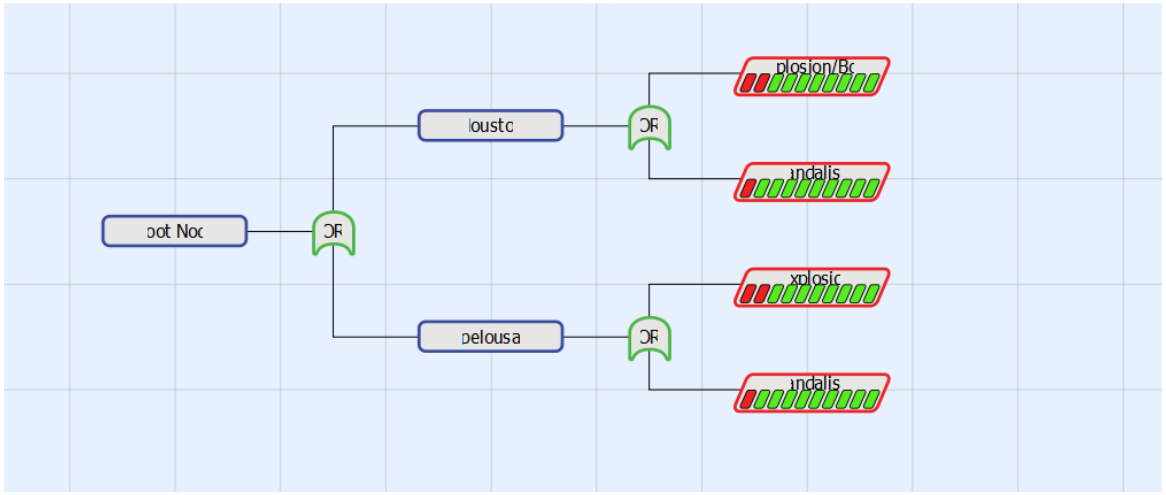



Data Table

| | Name | Threat (%) | Vulnerability (%) | Elimination Cost $(millions) | Consequence $(millions) | Risk Initial | Allocation $(millions) | Vulnerability Reduced (%) | Risk Reduced |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Supply Chain | 100.00 | 30.00 | 0.75 | 4.79 | 1.44 | 0.54 | 8.16 | 0.39 |
| 2 | Ransomware | 100.00 | 30.00 | 0.90 | 4.84 | 1.45 | 0.57 | 9.69 | 0.47 |
| 3 | Supply Chain | 100.00 | 30.00 | 0.65 | 3.92 | 1.18 | 0.45 | 8.64 | 0.34 |
| 4 | Ransomware | 100.00 | 30.00 | 0.55 | 3.96 | 1.19 | 0.44 | 7.24 | 0.29 |

| | /ulnerability (%) | Elimination Cost $(millions) | Consequence $(millions) | Risk Initial | Allocation $(millions) | Vulnerability Reduced (%) | Risk Reduced | Path |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0.75 | 4.79 | 1.44 | 0.54 | 8.16 | 0.39 | Root Node.Houston.Supply Chain |
| 2 | 0 | 0.90 | 4.84 | 1.45 | 0.57 | 9.69 | 0.47 | Root Node.Houston.Ransomware |
| 3 | 0 | 0.65 | 3.92 | 1.18 | 0.45 | 8.64 | 0.34 | Root Node.Atlanta.Supply Chain |
| 4 | 0 | 0.55 | 3.96 | 1.19 | 0.44 | 7.24 | 0.29 | Root Node.Atlanta.Ransomware |

## Flow Network Fault Tree:




Data Table

| | Name | Threat (%) | Vulnerability (%) | Elimination Cost $(millions) | Consequence $(millions) | Risk Initial |
|---|---|---|---|---|---|---|
| 1 | Explosion/Bomb | 100.00 | 35.00 | 1.00 | 5.00 | 1.75 |
| 2 | Vandalism | 100.00 | 50.00 | 0.75 | 4.50 | 2.25 |
| 3 | Explosion | 100.00 | 30.00 | 0.80 | 4.70 | 1.41 |
| 4 | Vandalism | 100.00 | 45.00 | 0.70 | 3.80 | 1.71 |

Data Table

| | Risk Initial | Allocation $(millions) | Vulnerability Reduced (%) | Risk Reduced | Path |
|---|---|---|---|---|---|
| 1 | 1.75 | 0.86 | 6.59 | 0.33 | Root Node.Houston.Explosion/Bomb |
| 2 | 2.25 | 0.75 | 5.00 | 0.23 | Root Node.Houston.Vandalism |
| 3 | 1.41 | 0.71 | 6.13 | 0.29 | Root Node.Opelousas .Explosion |
| 4 | 1.71 | 0.68 | 5.28 | 0.20 | Root Node.Opelousas .Vandalism |