

## EXECUTIVE SUMMARY

CSX is a leading supplier of rail-based freight transportation in North America, specifically in the Eastern half of the United States. CSX moves a wide variety of commodities ranging from agriculture products to Machinery. The specific network that we've chosen within CSX is the movement of Ethanol via CSX's Ethanol expressway (EthX™). The importance of this network lies within the actual commodity being transported which is ethanol. Ethanol is a volatile, flammable, colorless liquid which has uses ranging from Ingredients in thermometers, solvents, spirits and the largest single use being fuel for different types of engines and rocket motors. Over 69% of the world's supply of ethanol comes from Brazil and different supply depots within the United States.

EthX™ is CSX's Express Ethanol Delivery Service. The express delivery service provides an efficient and cost-effective way to deliver ethanol east of the Mississippi. The importance of Ethanol along with CSX's impressive network for transporting it were the driving factors that helped us choose this network for our project. Figure 1 is a detailed graphical representation of our EthX™ network.

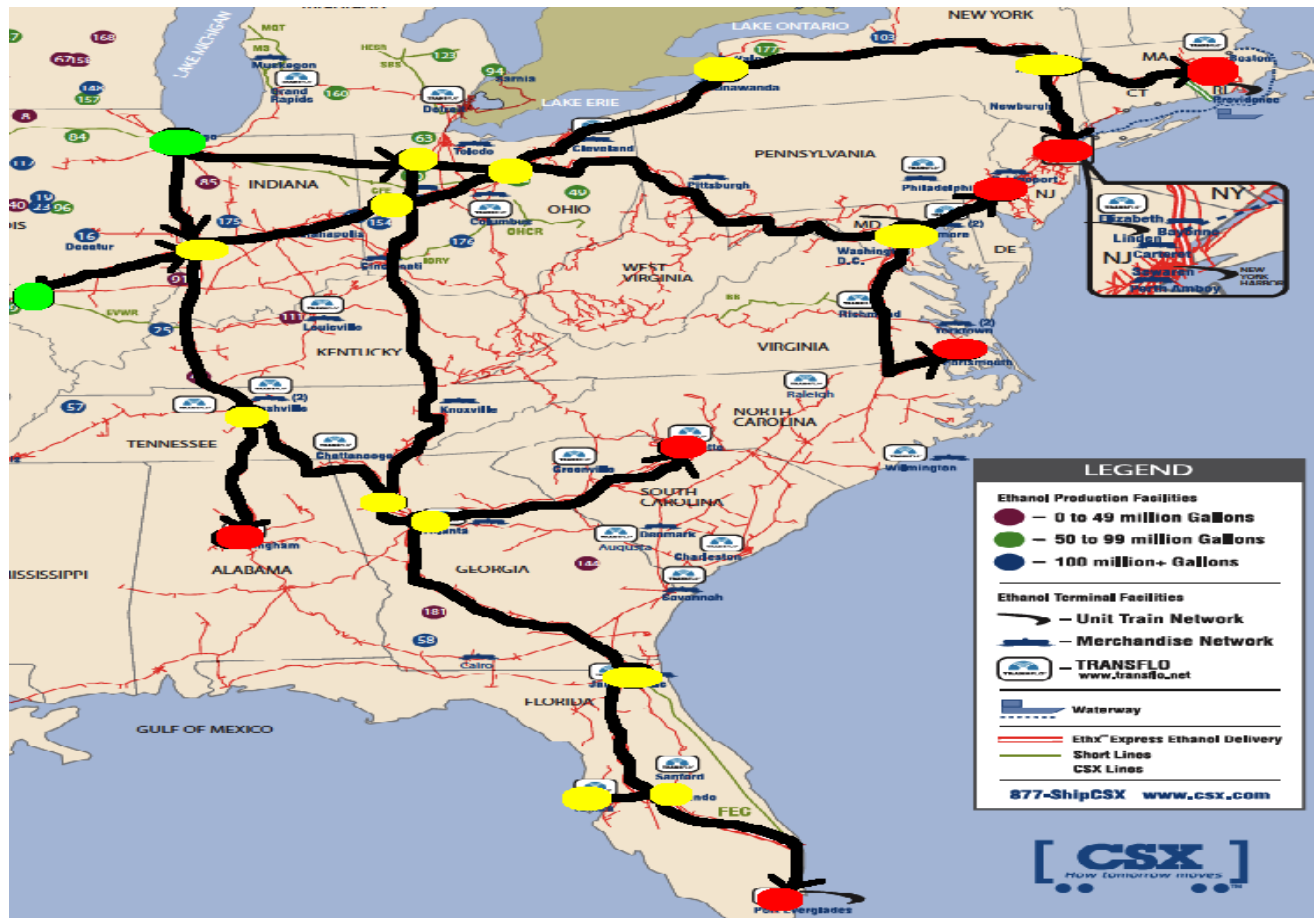


Figure 1: The graphical representation contains nodes which serve as major processing plants and intersecting cities that serve as main routes within the network. The nodes are color coordinated with "supply depots", "offload destinations", and major route intersections filled with the colors green, red, and yellow respectively.

A major vulnerability of our network is a terrorist attack. An attack or a threat of this nature, along with any government response, may adversely affect CSX’s financial condition. This risk could cause significant business interruption and result in increased costs and liabilities thus resulting in decreased revenues. With this type of risk in place, we decided to model several different scenarios that involve threats of terrorist attacks on different arcs in the network and actual attacks on the arcs.

The model used in our analysis is a “Min Cost, Max Flow” which represents the transportation of ethanol amongst the nodes. Each node has a capacity which corresponds to the amount of cars that can be sent from that node. Each arc has a value associated with it which corresponds to the cost per day to move one car amongst the arc. The first step in the modeling process involves running the model with no threats or attacks. The output of this run gives the optimal flow of ethanol throughout our network at the minimal cost while adhering to the capacity constraint on each node. Next we implement interdictions in on our network. There are two types of interdictions; the first being a “terrorist threat” and the second being an actual “terrorist attack”. A threat causes a delay of 12 hours but does not render this arc inoperable. The “12 hour” delay is a penalty added to the overall cost to traverse the affected arc. The exact calculation for the delay penalty is  $((\sum c_{ij})/m) * 1.5 = 4232$ . The value 1.5 includes the day already assigned to traverse the arc, plus the additional 12 hours. This delay time represents the time required for an explosive ordinance disposal team to inspect the track and ensure it’s safe for use. A terrorist attack is an actual attack which renders the affected arc inoperable (delay=nC). The GAMS interface provides optimal routes for all three of the scenarios given the start (green) and end (red) nodes with the associated supply and demands. Figure2 below illustrates how our network performs when imposing threats and attacks.

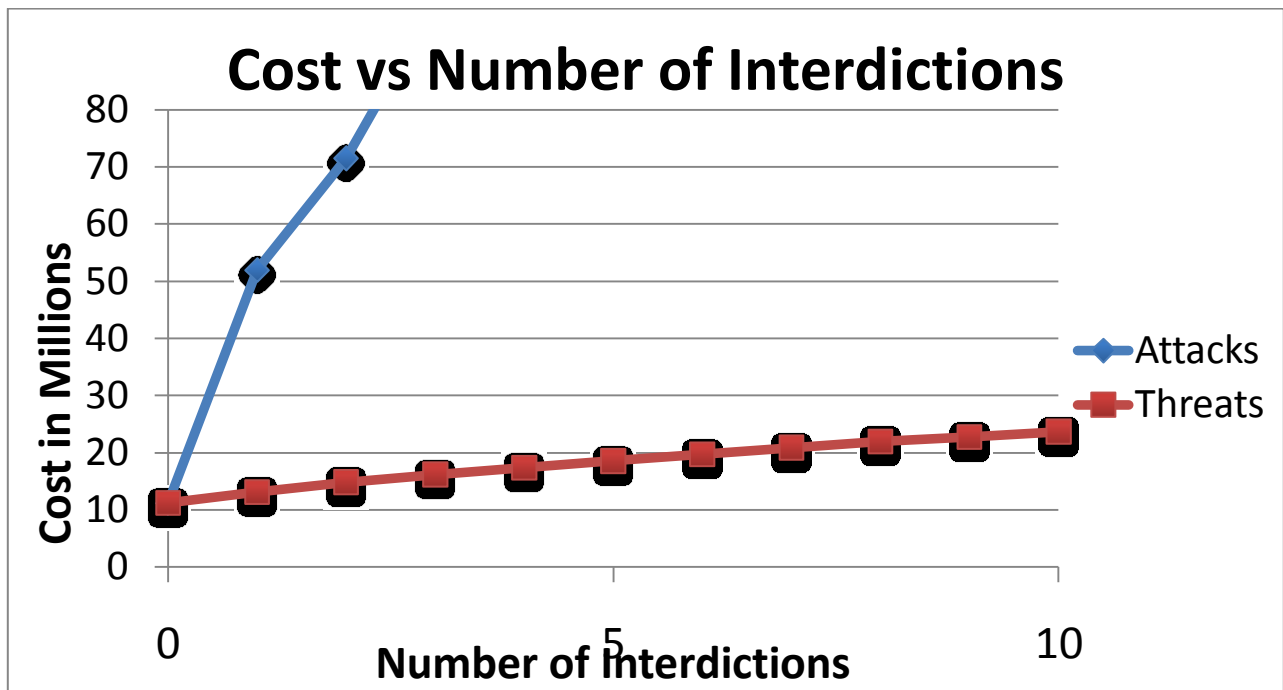


Figure 2: This shows a linear relationship of the cost to ship ethanol the most efficient way when threats are imposed on the network. When attacks are implemented, there is a vast increase in cost and heads to an infinite cost once it reaches 3 attacks. This is due to the fact that there is an infeasible solution at 3 or more attacks on the network.

From figure 2 we can see that our model allows the supply and demand requirements with the capacity constraints to be achievable with a cost of roughly \$10M. When threat-type interdictions are implemented in the network, all the demand is still achievable whereas with attack-type interdictions, demand met significantly decreases with each attack. At three or more attacks, there is no flow on the network (i.e. no demand met).

The results from the attack-type interdiction show the great vulnerability and lack of robustness on our network. In order to mitigate these problem spots and make the network more robust there are a few contingency plans that can be implemented. First thing would be to add additional supply nodes to the network and/or increase the amount of routes from current supply nodes. This will not only increase the amount of options to push flow throughout the network, but will also allow an increase in supply, therefore accommodating an increase in total demand. A second recommendation to improve the network would be to increase capacities, especially at critical nodes which serve as potential choke points. This will also increase overall flow throughout the network. Lastly, we recommend deriving a contingency plan to utilize alternative means to transport ethanol at various nodes to meet other demand requirements. These alternative means such as water/shipping routes or truck transportation would enable demand to continue to be met despite interdictions on the network which directly affect a particular demand node.