Network Reliability and Resilience

Mark S. Daskin
Dept. of IE/MS
Northwestern University
Reliability and Resilience

- Reliability
  - Low probability of failure

- Resilience
  - Consequences of failure are designed to be small
  - Return to normal function is rapid
Outline

- Framework for network resilience
- Industry perspectives
- Examples of research at NU
- Directions for future work and collaboration
Sources of Supply Chain or Network Unreliability

- Natural disasters
- Weather
- Congestion of facilities
- Business failures
- Economics, Energy, Environment
- Labor disruptions
- Terrorist actions

We live in an uncertain world.
<table>
<thead>
<tr>
<th>Severity</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>
Reliability/Resilience Taxonomy: Duration is also important

Frequency – how often does something fail

Severity – what fraction of network capability is lost
– what is the cost?

Duration – how long is it disabled
Threats and countermeasures

- Intellectual property
- Government regulation
- Environmental concerns
- Demand uncertainty
- Terrorist attacks
- Supplier reliability
- Supplier yield
- Labor disruptions
- Weather
- Natural disasters
- Energy availability
- New entrants products
- R&D/new prod.
- R&D/options
- Market res.
- Forecasting
- Fortification
- Purchase options
- Inv./options
- Contracts/flex.
- Multi-sourcing
- Regulation/other
- Lobbying
- Firm
Threats and countermeasures

Supplier reliability

Multi-sourcing

Firm

Inventory

Supplier yield

Fortification/Intelligence/Detection

Terrorism

Yield – high frequency, short duration, low consequence, unpredictable

Supplier reliability – lower frequency, longer duration, moderate consequence, may be targeted

Terrorism – very low frequency, long duration, high consequence, targeted
Threats and countermeasures

Weather delay

Overbooking
- high frequency, few flights impacted, low consequence, somewhat unpredictable

Weather delay
- lower frequency, longer duration, moderate to high network consequences, may be foreseen

Terrorism
- very low frequency, very long duration, high consequence, targeted at vulnerable facilities

Inducements

Fortification

Recovery plans

Airline

Overbooking

Terrorism
Event planning is a cycle
Pre-event planning

- **Prevent** events
- **Defend** against events (harden facilities)
- **Design** systems to be resilient with respect to failures
- **Prevent** overbooking via improved forecasting
- **Defend** against terrorism via screening
- **Design** routes and networks to be robust w.r.t. weather delays
- **Prevent** shortages thru better forecasting
- **Defend** against shortages via safety stock
- **Design** products for substitutability; networks with multiple suppliers
During event

- Detect events
- Diagnose event
- Prescribe action
- Communicate action
- Coordinate response
- Control response

- Detect weather problems early
- Diagnose severity of disruption due to weather
- Prescribe response (reroute aircraft, call in backup crews)
- Communicate with passengers
- Coordinate with other airlines and hotels
- Control entire response

- Detect shortages by monitoring key suppliers
- Diagnose shortage severity (total, partial)
- Prescribe actions (draw on safety stock, invoke contracts)
- Communicate plans with plants, suppliers, and customers
- Coordinate response across system
- Control production
Post event

- Recovery actions
- Redesign system for better response
- Reconstruct system

- Recovery actions to reposition aircraft and crews
- Redesign network, routes, aircraft assignments, response system
- Reconstruct may not be applicable in weather case except in the extreme

- Recovery actions to get production back and marketing to recover market share
- Redesign supply chain to mitigate future shortages (improve forecasting, safety stock, multi-source)
- Reconstruct supply chain and replenish safety stocks
Key observations

- **Network effects** make pre-event, during event and post-event difficult

- **Solutions must encompass**
  - Detection and Diagnosis
  - Communication and Coordination
  - Recovery and Redesign
Questions for Industry

➢ How do you think about resilience?
➢ How do you ensure resilience?
➢ How do you monitor your network(s)?
➢ What is the impact of a network failure?
➢ How do you contain/recover from failures?
➢ What “unmet needs” do you have?