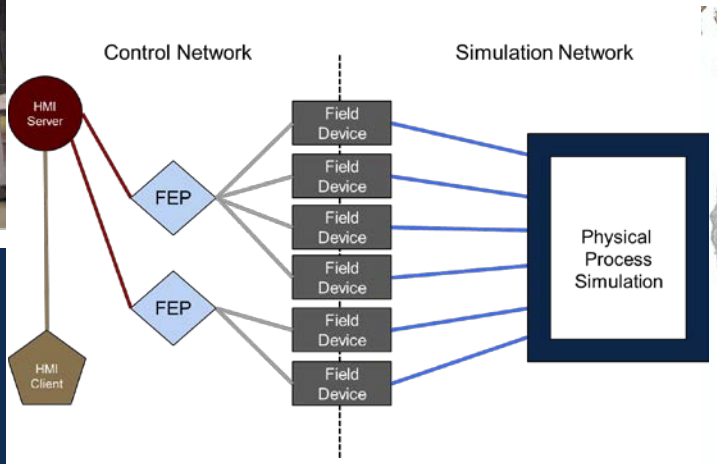
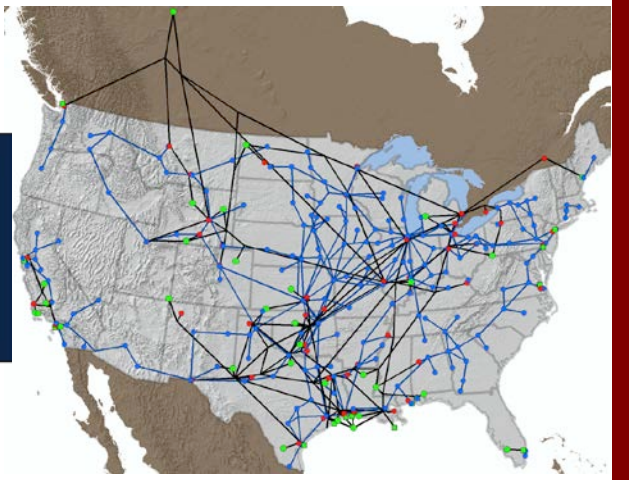
Refinery Control Systems in National Transportation Fuels Modeling

Andjelka Kelic, Derek H. Hart
Michael L. Wilson, Thomas F. Corbet

Photos: US Chemical Safety Board, BP America Refinery Explosion Final Report





SCEPTRE Control System Model

National Transportation Fuels Model

Sandia National Laboratories

Exceptional service in the national interest

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2015-

The National Infrastructure Simulation and Analysis Center is a joint program between Los Alamos National Laboratory and Sandia National Laboratories funded by the Department of Homeland Security Office of Cyber and Infrastructure Analysis..

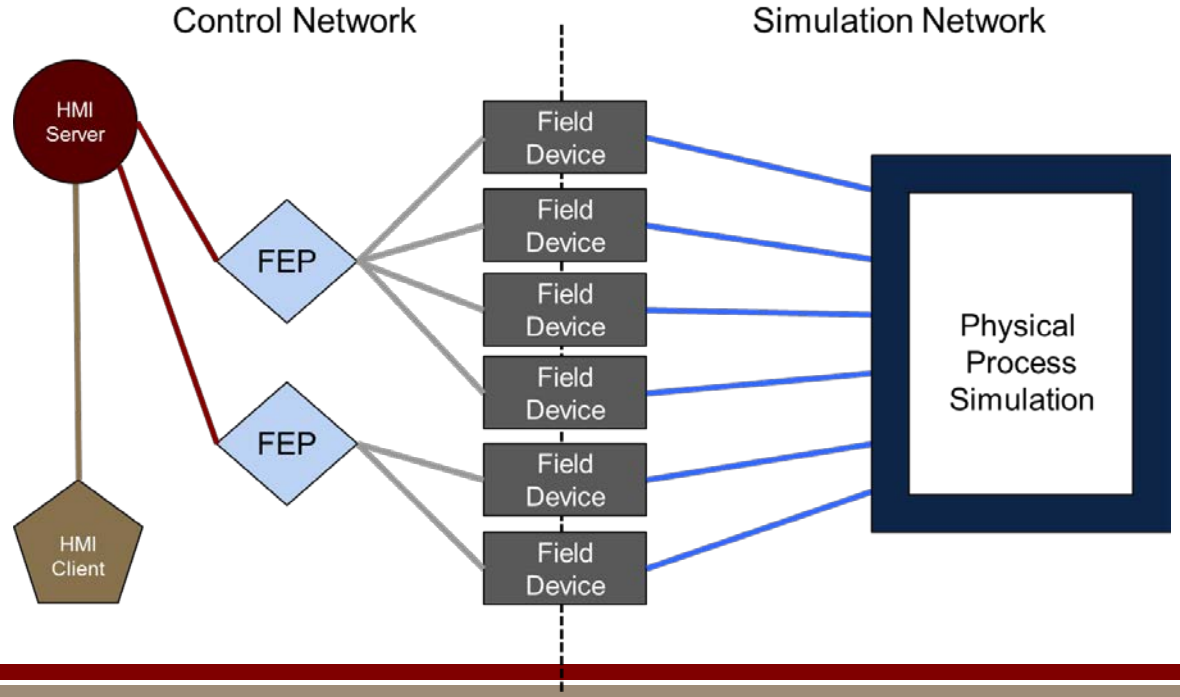
Goal

- Model cyber-physical impacts on transportation fuels network
- Combine control system modeling tools (SCEPTRE) with national infrastructure models (National Transportation Fuels Model – NTFM)
- Determine important areas for future work

SCEPTRE Control System Modeling

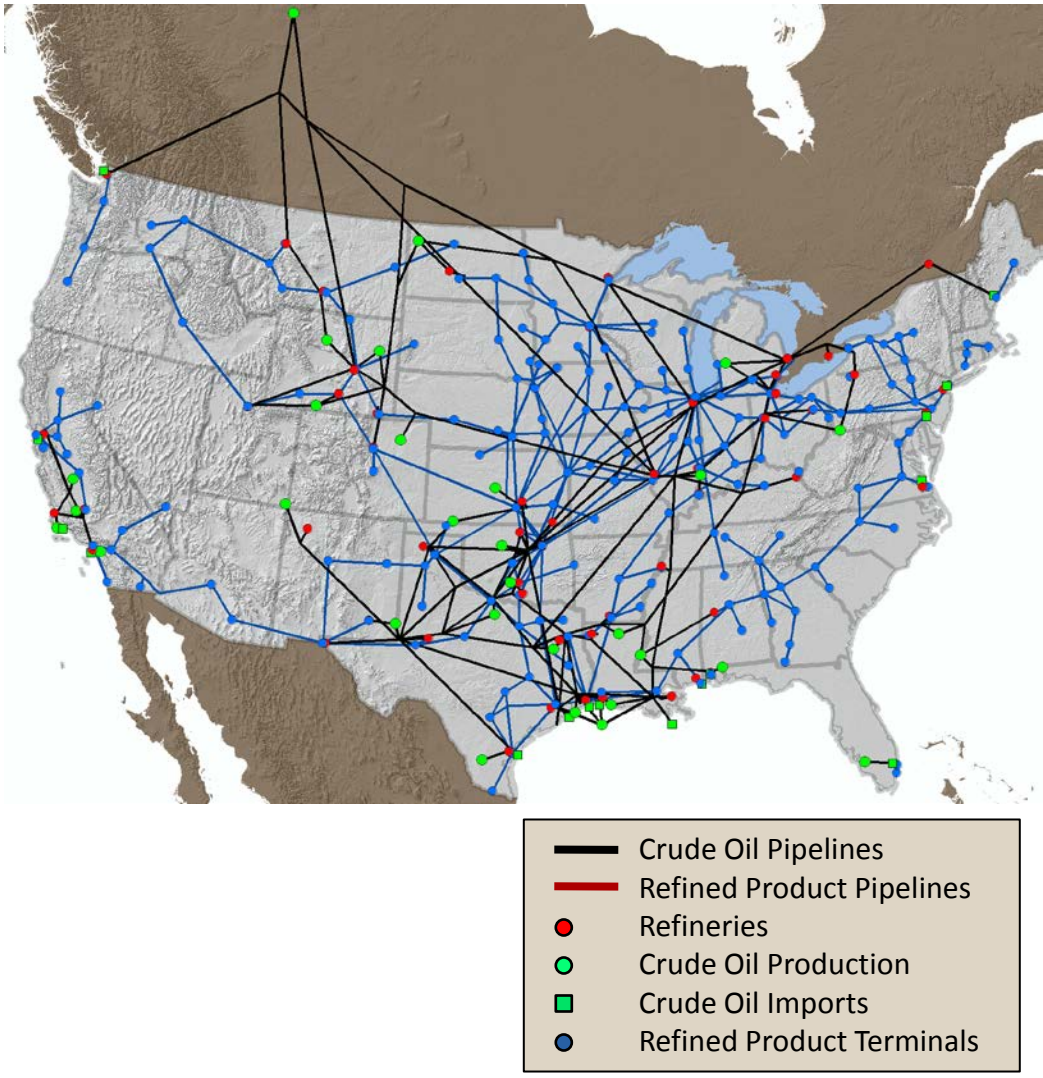
Sandia National Laboratories

- SCEPTRE combines control system devices and physical process simulations in an integrated system that represents realistic responses in the physical process as events occur
- Control system devices communicate and interact via actual SCADA protocols
  - Can put hardware in the loop and monitor communications using standard network tools (Splunk, Wireshark, etc)



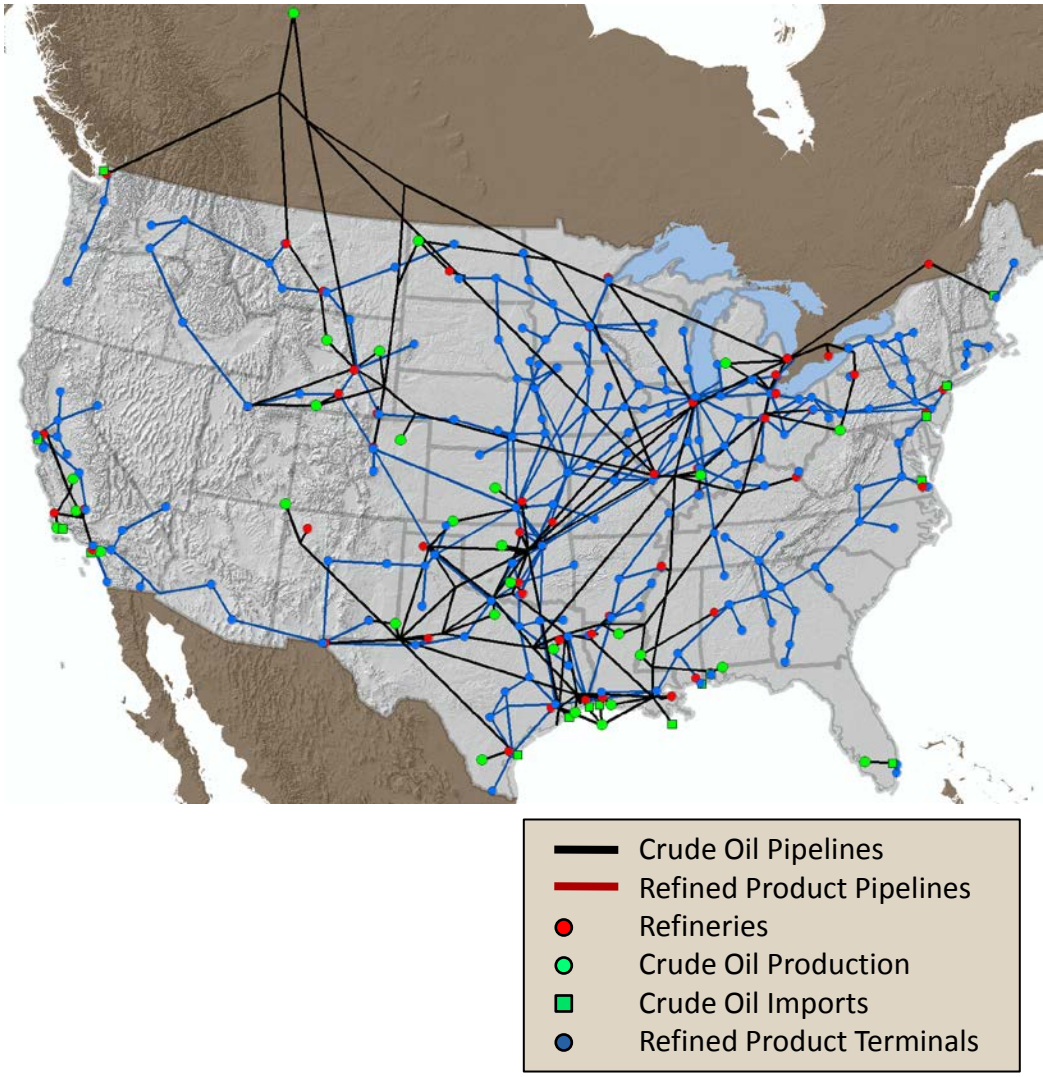
National Transportation Fuels Model

- Network-based model of the U.S. transportation fuel infrastructure
  - Algorithms, databases, and a GIS-based interface to simulate commodity flows
  - Includes crude production, refining nodes, pipeline linkages, terminals, and ports
- Constrained by connectivity and capacities



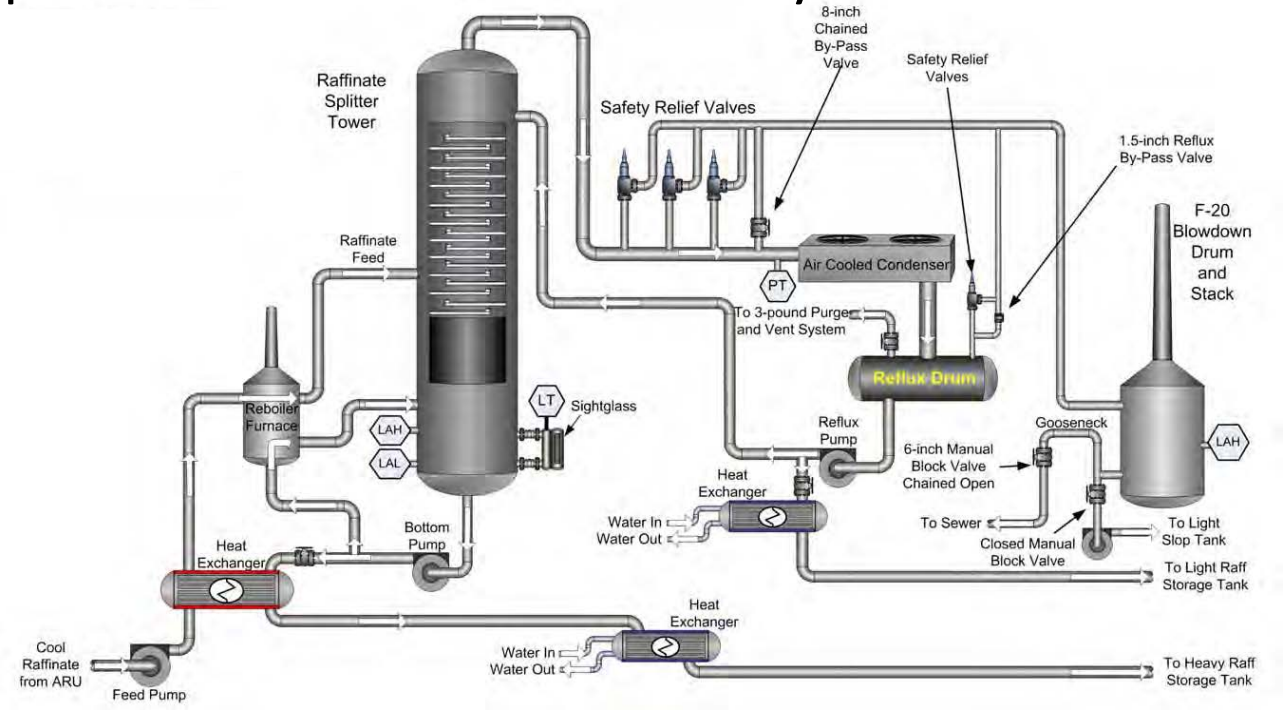
National Transportation Fuels Model

- Transportation fuels availability during disruptions to the fuel supply network
- Adapts to disruptions by:
  - Rerouting of shipments.
  - Drawdown of inventories.
  - Use of surge capacity in transportation, refining, and imports to mitigate fuel shortage



The Challenge

- Find a real-world event to replicate and explore transportation fuels impact
- Refineries are the points in the system with the most control
- No known cyber attack related incidents at refineries
- Replicate an event with control system-related failures



Graphic: US Chemical Safety Board, BP America Refinery Explosion Final Report, 2007.

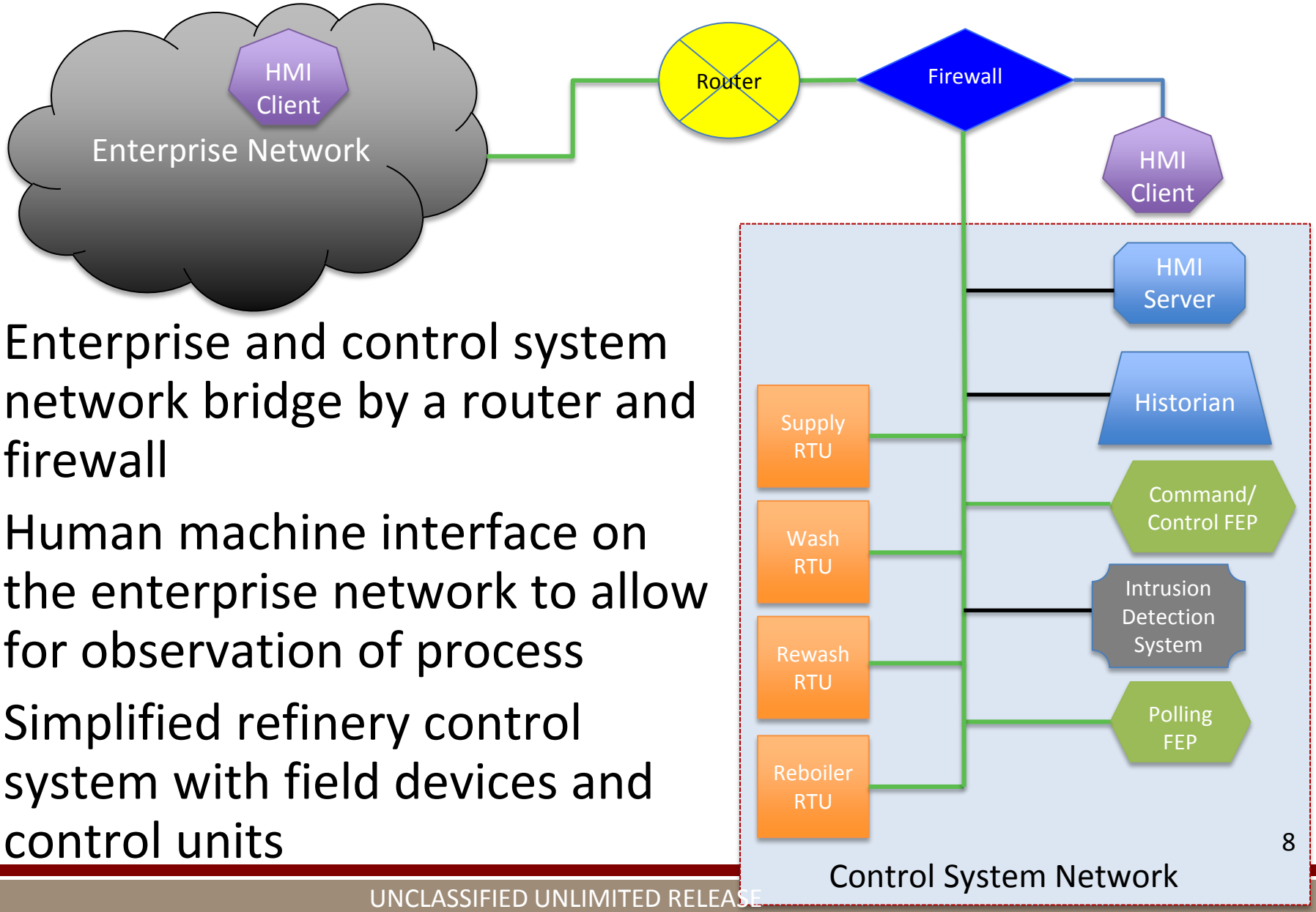
The Scenario: 2005 Texas City BP America Refinery Explosion*

Sandia National Laboratories

- On March 23, 2005 the BP America Refinery in Texas City exploded, killing 15 and injuring 180
- This was not a cyber attack related event
- Control system indicators malfunctions
- Alarms failed to trigger
- Operators responded to alarms they saw, ultimately resulting in the explosion
- We create a simplified version of this event that uses the control system to overheat the reboiler without operator knowledge

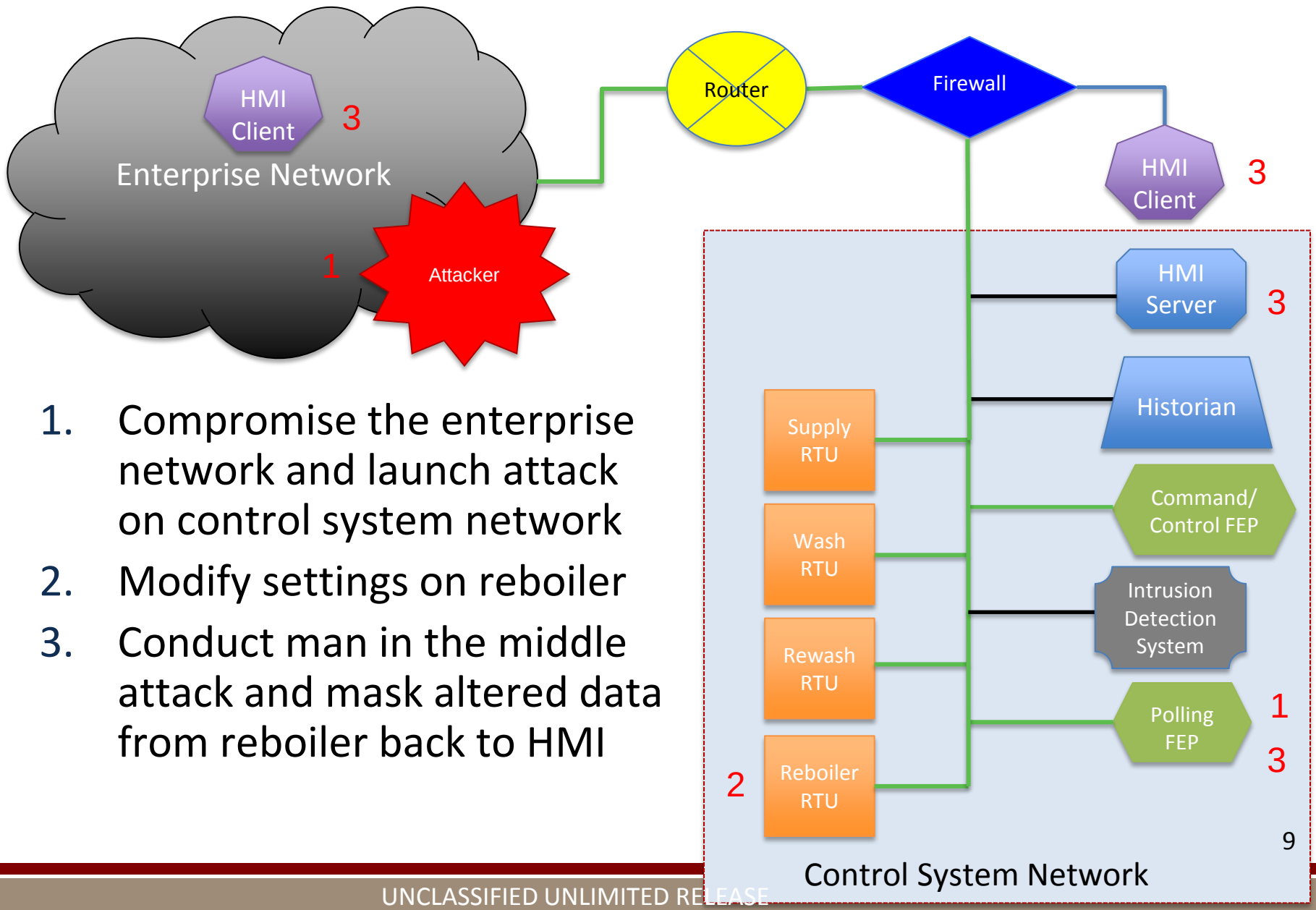
*US Chemical Safety Board, BP America Refinery Explosion Final Report, 2007.

SCEPTRE Control System Network



1. Enterprise and control system network bridge by a router and firewall
2. Human machine interface on the enterprise network to allow for observation of process
3. Simplified refinery control system with field devices and control units

Replicating the Scenario in SCEPTRE



1. Compromise the enterprise network and launch attack on control system network
2. Modify settings on reboiler
3. Conduct man in the middle attack and mask altered data from reboiler back to HMI

Applying the Results in NTFM: Three Scenarios

Sandia National Laboratories

1. Disruption of all ConocoPhillips refineries (10 refineries).
2. Disruption of all Valero refineries (10 refineries).

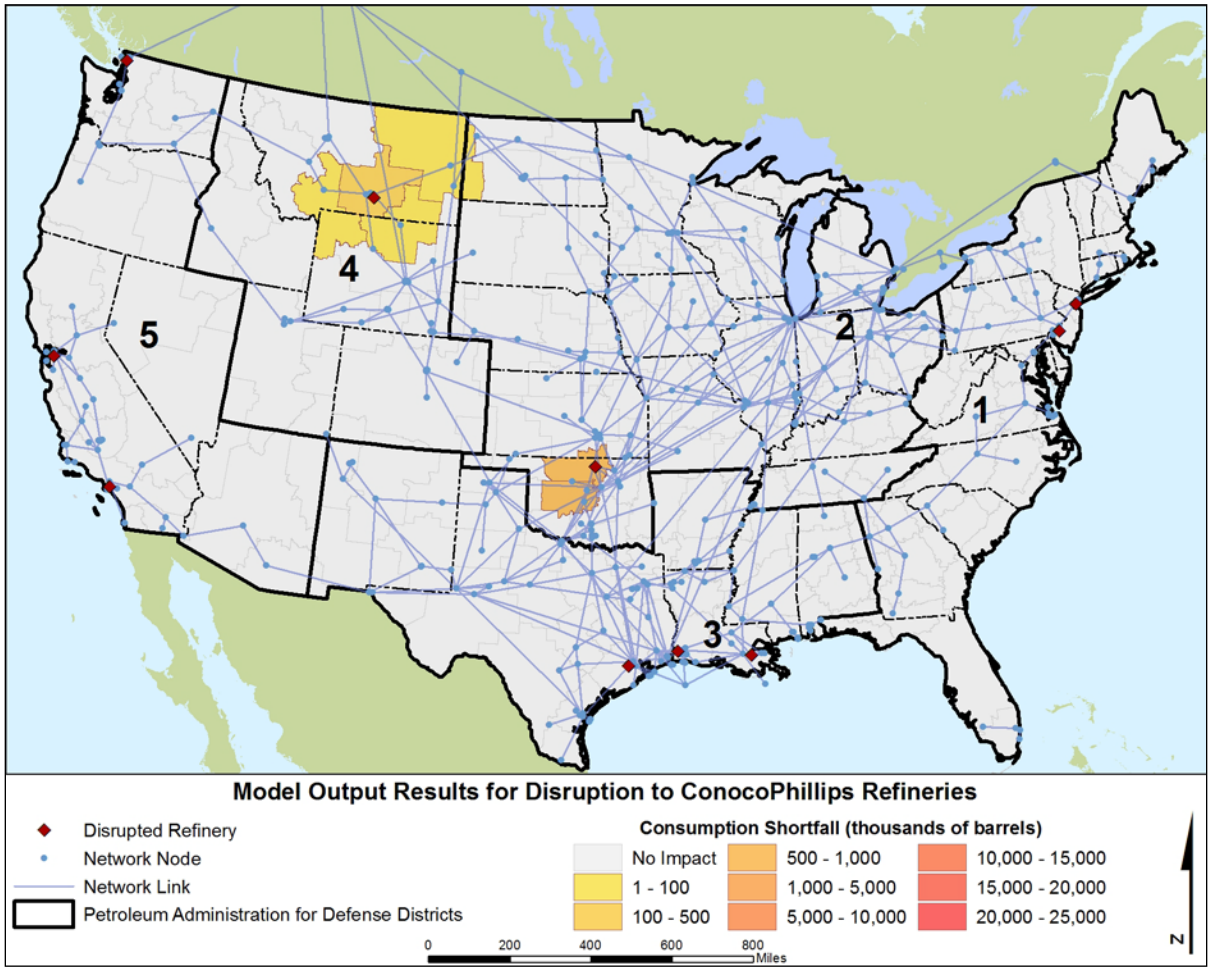
These disruptions assume common corporate ownership means common control system implementations and vulnerabilities

3. Disruption of the ten highest-impact refineries.

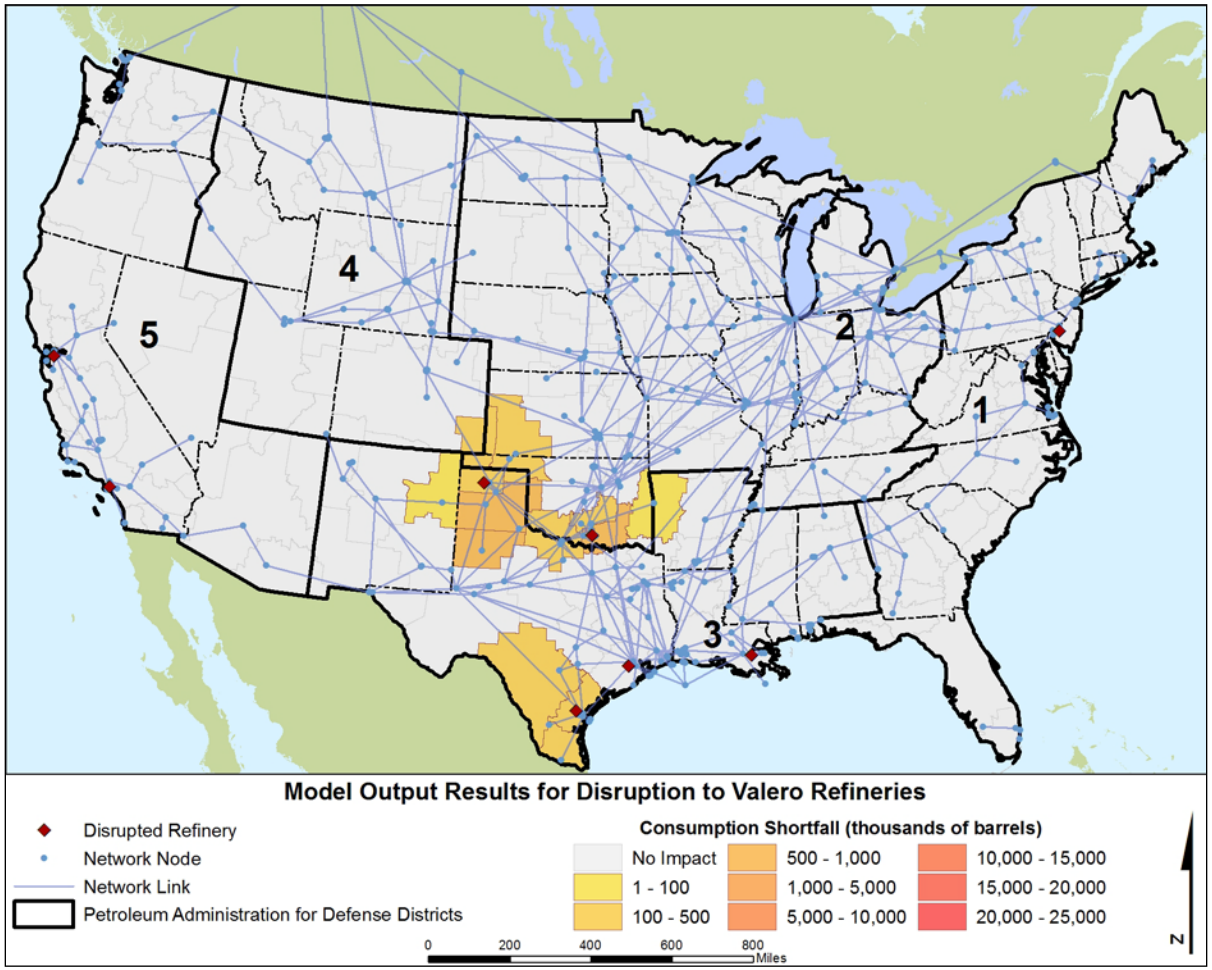
This disruption assumes common control system components due to limited vendor space

100 day outages accounting for disruption, investigation, and remediation

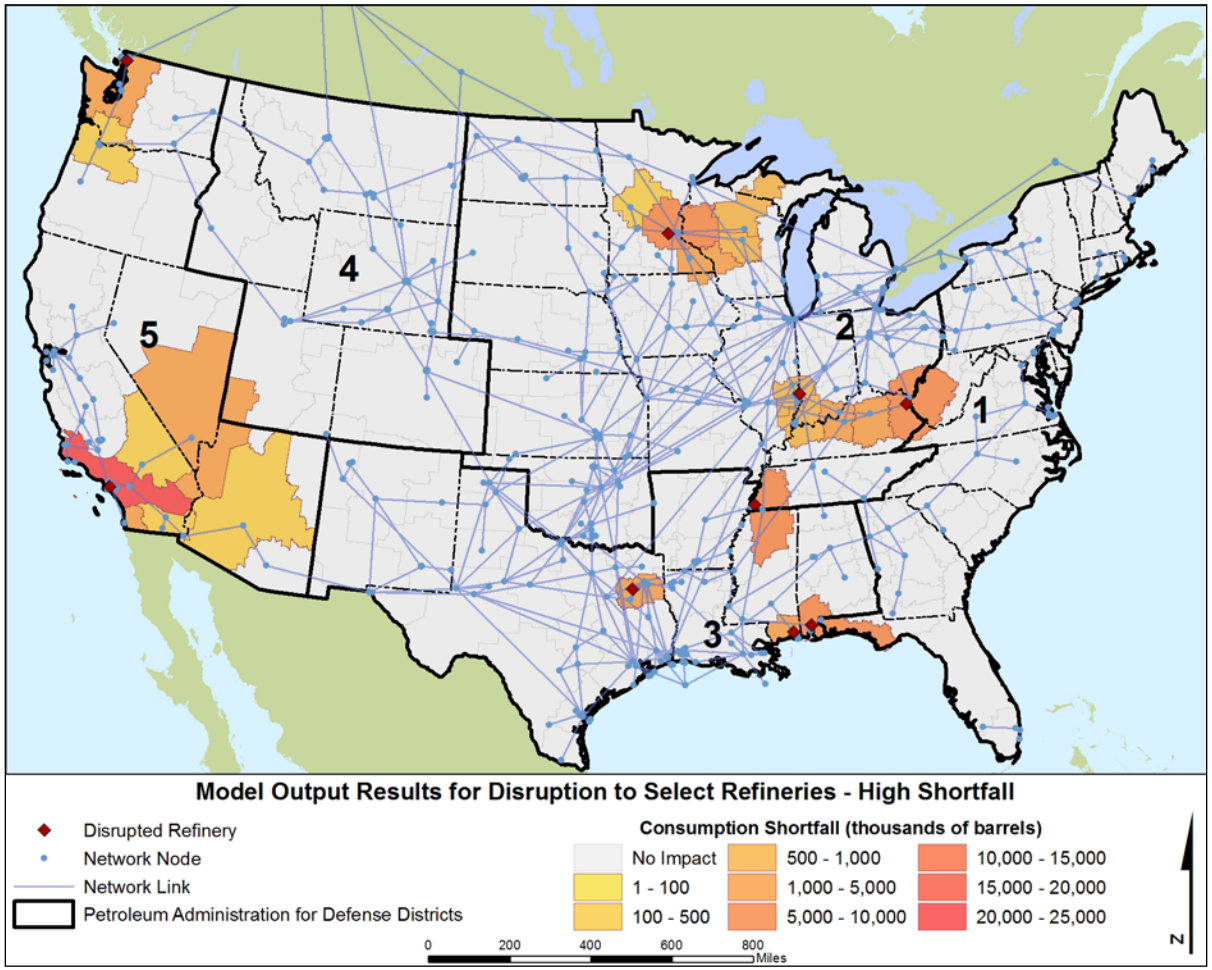
ConocoPhillips Refinery Disruption



Valero Refinery Disruption



Highest Impact Refinery Disruption



Conclusions

- Three scenarios analyzed show that there can be a wide range of impacts for a disruption of ten refineries.
- The amount of demand that is unmet depends very much on the sizes and locations of the refineries
- The assumptions about the commonality of vulnerabilities matter

Future Direction

- Better understanding of control system vendors and penetration rates
- Better understanding of how refinery ownership ties to implementation and refresh rates of control components
- Better understanding of how tightly controlled a process is to add granularity
  - Processes for which control is required versus just for efficiency
  - How much can you control with the control system?
  - How much does this vary across refineries?