



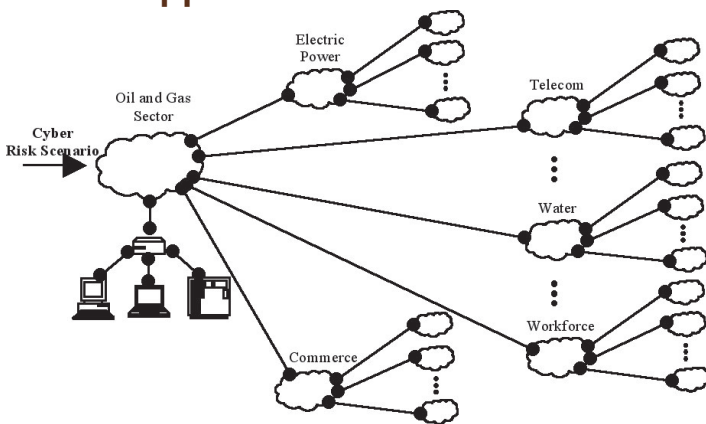
Inoperability Input-Output Model (IIM)

Overview of the IIM

The **Inoperability Input-Output Model (IIM)** is an analytical framework to quantify and address the risks from the intra- and inter-connectedness of economic and infrastructure sectors in the United States. Critical infrastructures (e.g. transportation, telecommunications, energy, or banking) are highly complex and interconnected, and they have become increasingly dependent on networked information systems for efficient operations and timely delivery of products and services. These interconnections allow flow of information, shared security, and physical flows of commodities, among others.

The IIM uses data from the U.S. Department of Commerce to assess the economic interdependencies of sectors and to estimate sector disruptions as a result of direct and indirect effects. Disruptions can be demand or supply shocks due to willful attacks, accidental events, or natural disasters.

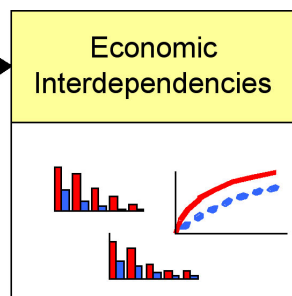
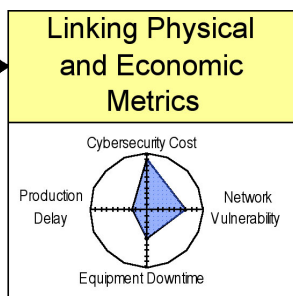
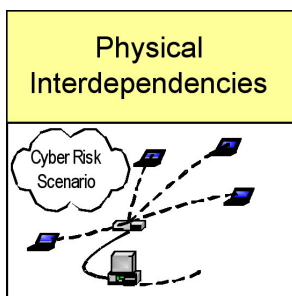
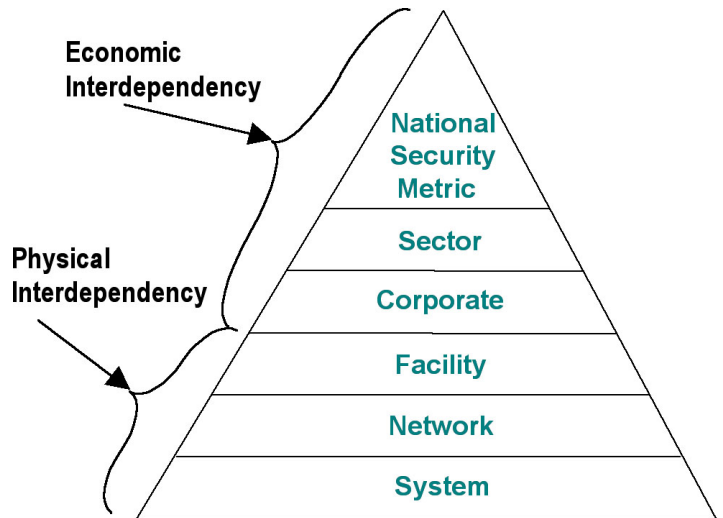
Sector Ripple Effects



As shown, the effects from a single sector's disruption (e.g. Oil and Gas) will ripple throughout the economy. "Downstream" sectors are affected, which can then affect further interconnected sectors, and so on. These higher order risks are captured in the IIM, and a metrics-based approach is useful for integrating this knowledge into business and risk management decisions.

Framework for Linking Hierarchies of Cyber Security Metrics

Security metrics play an important role in the operation of the IIM. These security metrics span a range of decision making hierarchies. For simplicity, security metrics can be grouped into two broad categories:



This framework presents a hierarchical view of how physical and economic systems interact. The bottom half of the pyramid represents plant-level process control system (PCS) security metrics, which is the foundation for SCADA security. The top half of the pyramid represents the industry/regional/national-level economic metrics, which is a necessary viewpoint for understanding how the sector as a whole integrates into the larger picture of national security.

Researcher Contact Information



Joost Santos (UVA)
 jrs8e@virginia.edu
 (434) 924-3283

Other team members include:
Bayard Gennert
 bvg4n@virginia.edu

About the University of Virginia

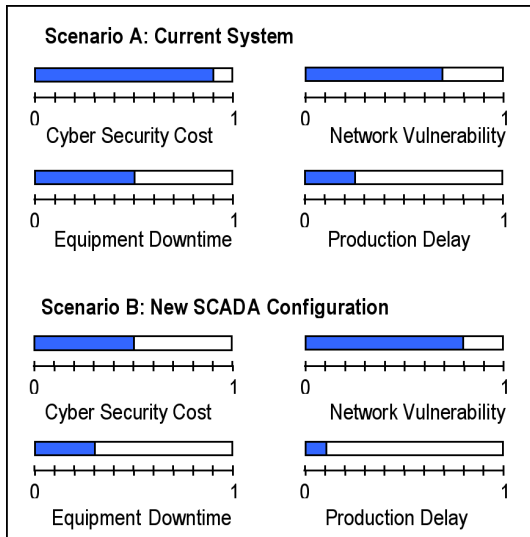
Founded by Thomas Jefferson in 1819, the University of Virginia sustains the ideal of developing, through education, leaders who are well-prepared to help shape the future of the nation. A public university, with its main campus in Charlottesville, the university's offers 50 bachelor's degrees in 47 fields, 85 master's degrees in 67 fields, and 59 doctoral degrees in 58 fields.

This work was supported under Award number 2003-TX-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

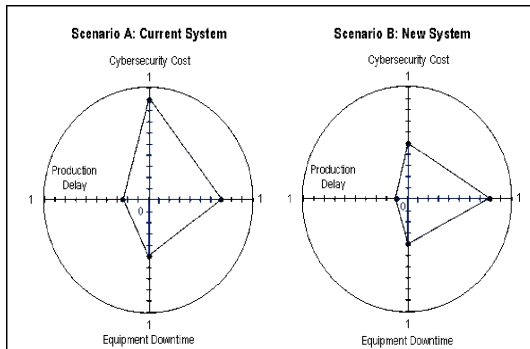
SCADA systems are composed of thousands of components and control subsystems, which may be vulnerable to malicious cyber attacks. To secure process control systems, it is imperative to quantify all categories of risks and to implement the risk management policy options accordingly so PCS can be hardened for potential disruptions, and the consequences of such disruptions be minimized.

Integrating Multiple Metrics

Risk scenarios can be generated, and the resulting effects can be evaluated using multiple metrics. The example shown below represents the expected changes in four cost and risk measures from implementing a new SCADA configuration.



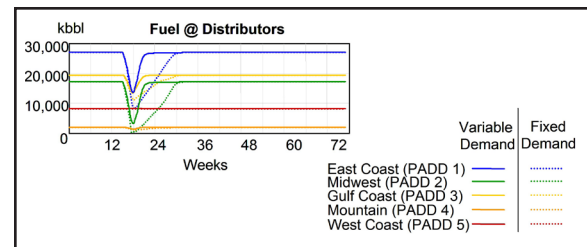
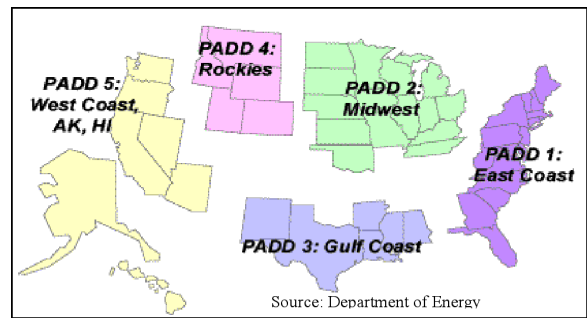
These results can be aggregated to generate an overall criticality rating. Radar charts (below) are useful methods for displaying multiple perspectives simultaneously.



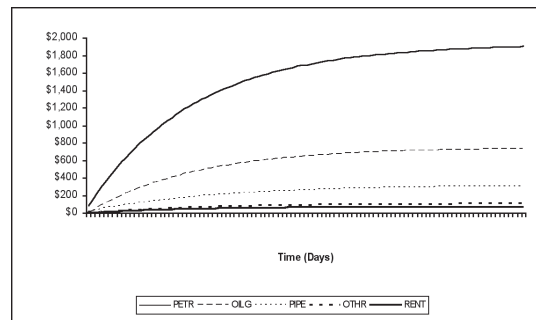
The process components with highest-risk ratings can then be prioritized for focused risk management. These specific scenarios at the PCS, network, or plant level can then be translated into disruption inputs for the IIM. The result will be an estimation of cumulative disruption effects in both financial loss and business inoperability across the region and nation.

Relating Simulation Models with the IIM: Case Study

In a case study, the IIM considered a cyber-enabled attack scenario that would cause Gulf of Mexico crude oil terminals to become inaccessible to tankers for five weeks. The first figure shows the U.S. Petroleum Administration for Defense Districts (PADD). Incorporating results from the Sandia Stock and Flow Model for Gulf Coast Disruption, the next two figures show the impact of the disruption on fuel distribution in each PADD and the cumulative economic losses in several industry sectors.



Sample Results for PADD 3: Economic Losses



PETR Petroleum and coal products manufacturing
 OILG Oil and gas extraction
 PIPE Pipeline transportation
 OTHR Other services
 RENT Rental and leasing services and lessors of intangible assets

Summary

- A framework is presented for integrating analyses of systems as viewed from different hierarchies and modeling perspectives.
- The framework aims to link the analysis of plant-level disruptions to the IIM for estimating the ripple effects across sectors and regions.
- Visualization tools such as radar charts can aid in converting different security metrics into an integrated metric that can be entered into the IIM.
- A case study was conducted to analyze a cyber attack scenario that causes a crude oil supply disruption in the Gulf Coast region.