Analytics for Cybersecurity of Cyber-Physical Systems

Relevance for Business and Industry

Nazli Choucri
Professor of Political Science, PI
nchoucri@mit.edu

Stuart E. Madnick
Professor, Sloan School of Management
smadnick@mit.edu

Gaurav Agarwal
MIT Alum,
MS SDM 2010
gauravag@mit.edu

Complexity of Policy

Burdens of Cybersecurity Guidelines

Policy guidelines are transmitted in text form:

- Text creates barriers to understanding & implementation.
- Contains critical information not available just by reading.
- Impedes effective & efficient response.

Managing Complexity

Analytics & Methods to:

- Transform policy texts into strategic assets.
- Create suite of models & analytical for customized applications.
- Identify vulnerabilities, risks & impacts levels.
- Prioritize protection targets & define specific actions.

What Value to Enterprise?

Enhance Enterprise Cyber Risks Management

- Customize tools for different type of support
- Provide suite of methods to identify, evaluate, manage, & monitor risks.
  - Internal control system.
  - Compliance management system.
  - Risk early warning system.

Illustrating Views of Systems & Guidelines

National Airspace System Architecture-Simplified

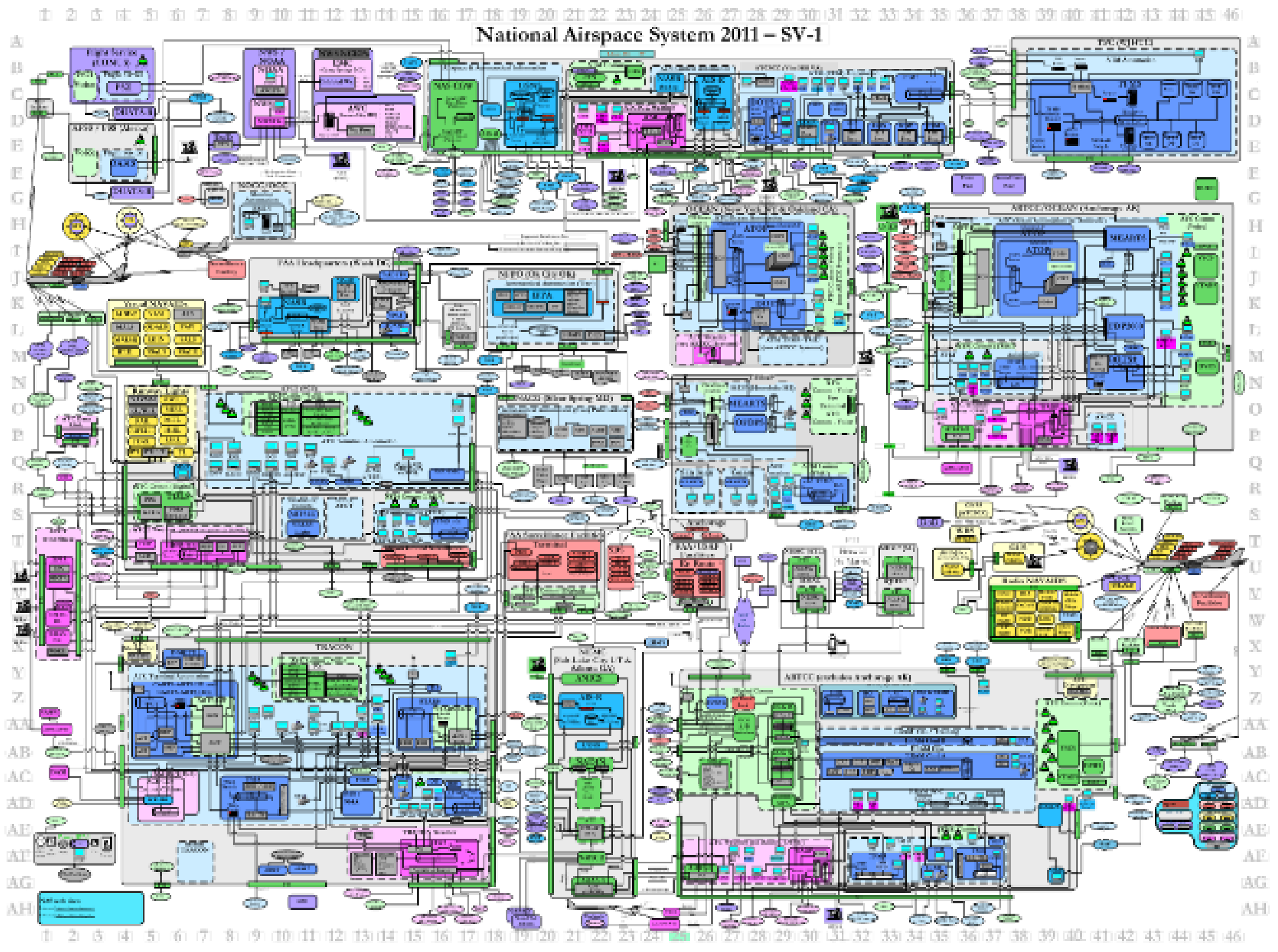


Image Source: Mike Hritz, Acting Chief Architect of National Airspace Systems, FAA NEXTGEN , "Complexity In the Next Generation: FAA National Airspace System" in AIAA Complex Aerospace Systems Exchange, 11 - 13 September 2012, Pasadena, California

NISTIR- 7628 Smart Grid Conceptual Model

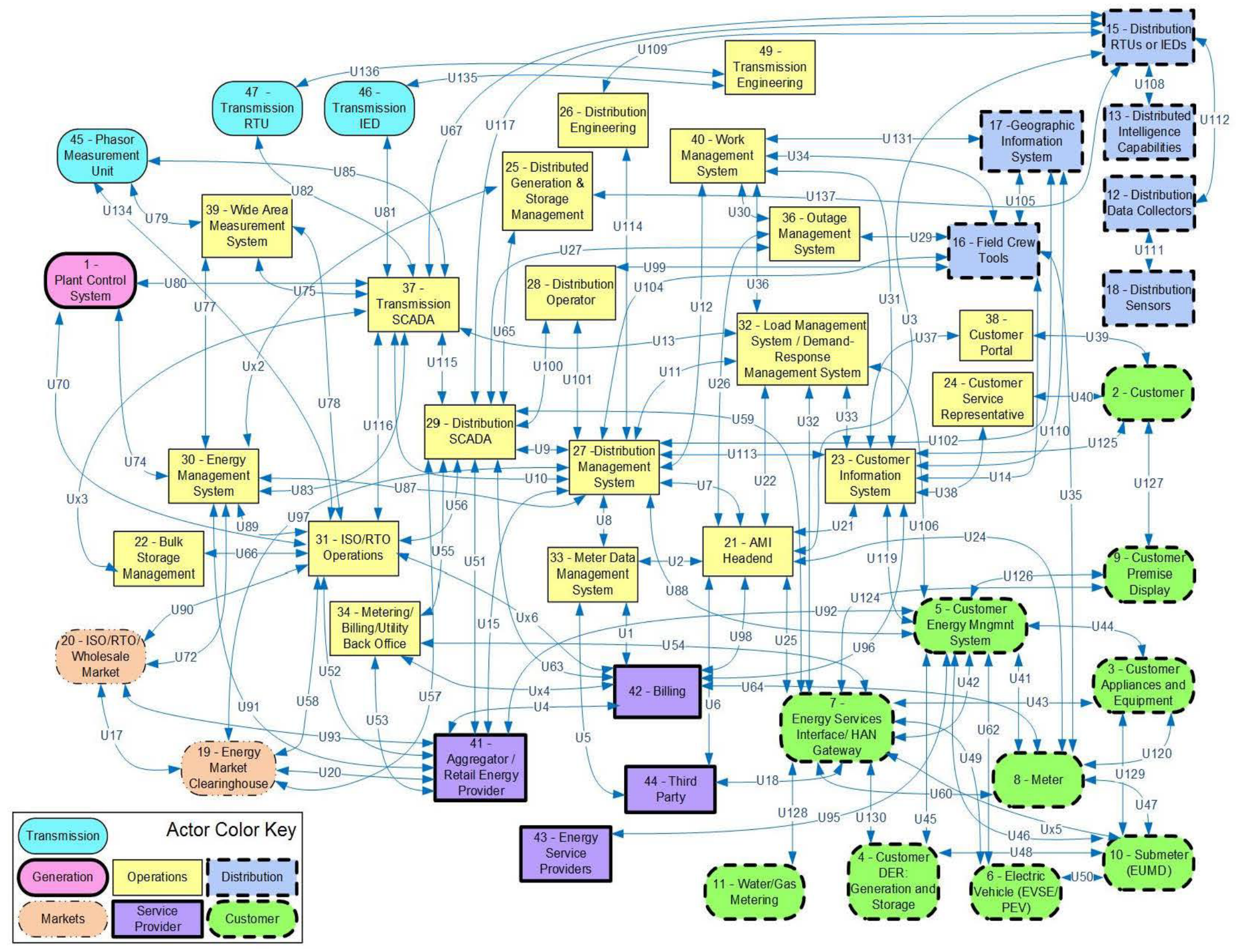
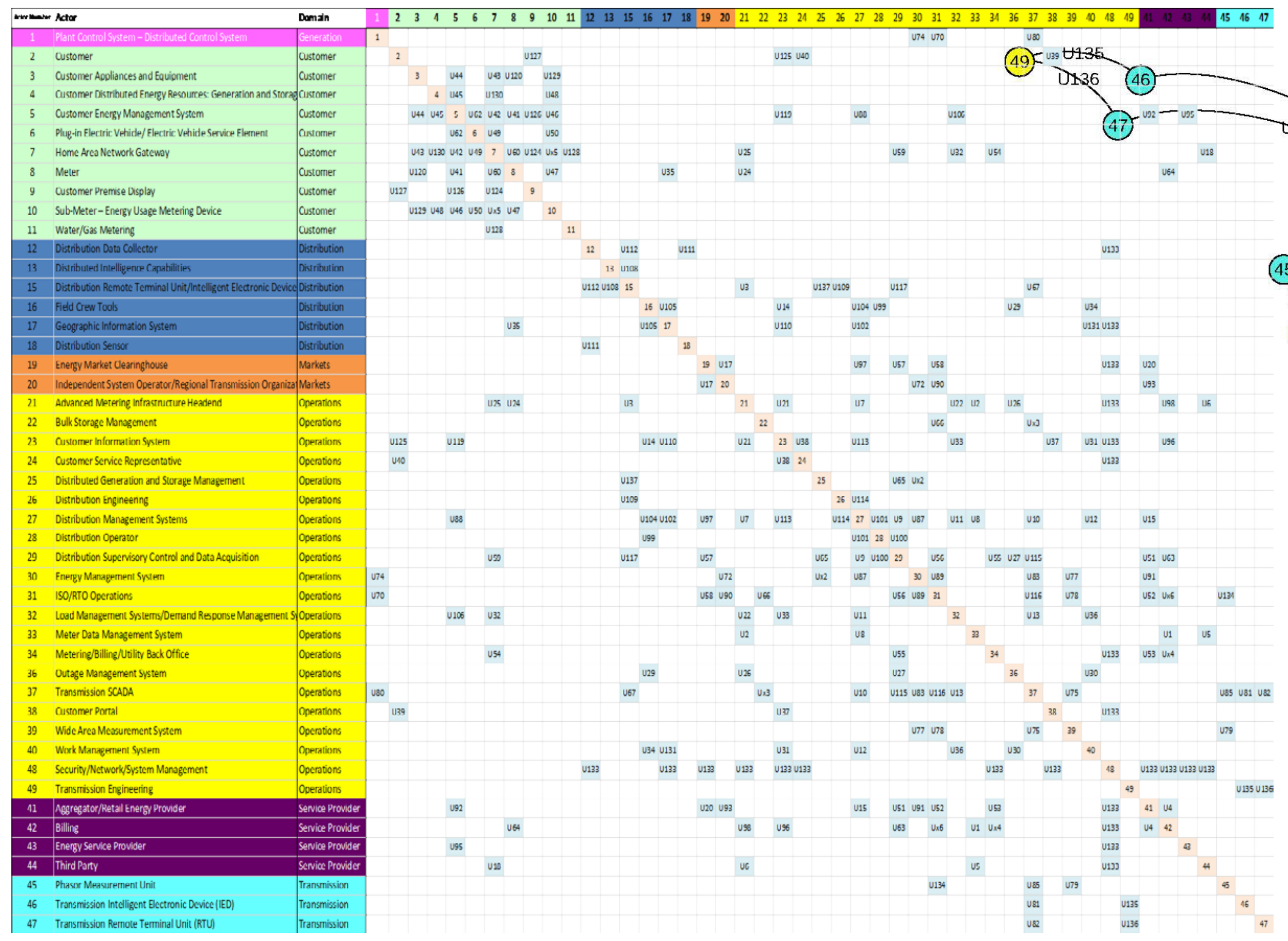


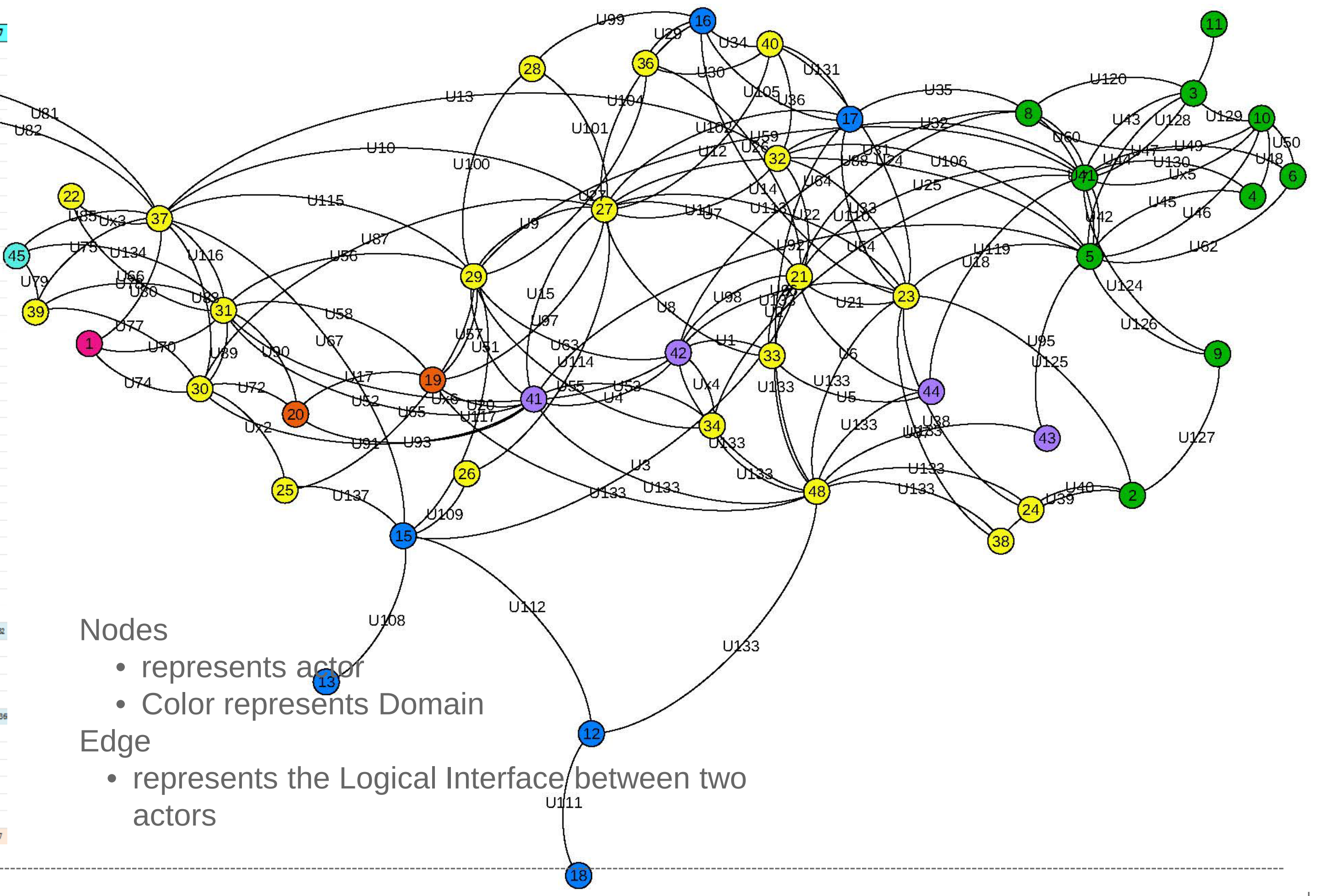
Image Source: NIST. "I, September, 2014; **doi:** NIST.IR.7628r1, p16. *Guidelines for Smart Grid Cybersecurity-Volume 1,*" NISTIR 7628 Revision

MIT Analytics for Transparency of System & Guidelines

Design Structure Matrix of NIST Model



Network View of DSM



Nodes
- represents actor
- Color represents Domain

Edge
- represents the Logical Interface between two actors

From Transparency to Business Decisions: Aviation Case Study

Airport -- an *energy service interface* -- Critical for Aviation System

- Airport at center of e-Landscape.
- Smart grid at center of power system.
- NIST provides for Cybersecurity of Smart Grid.

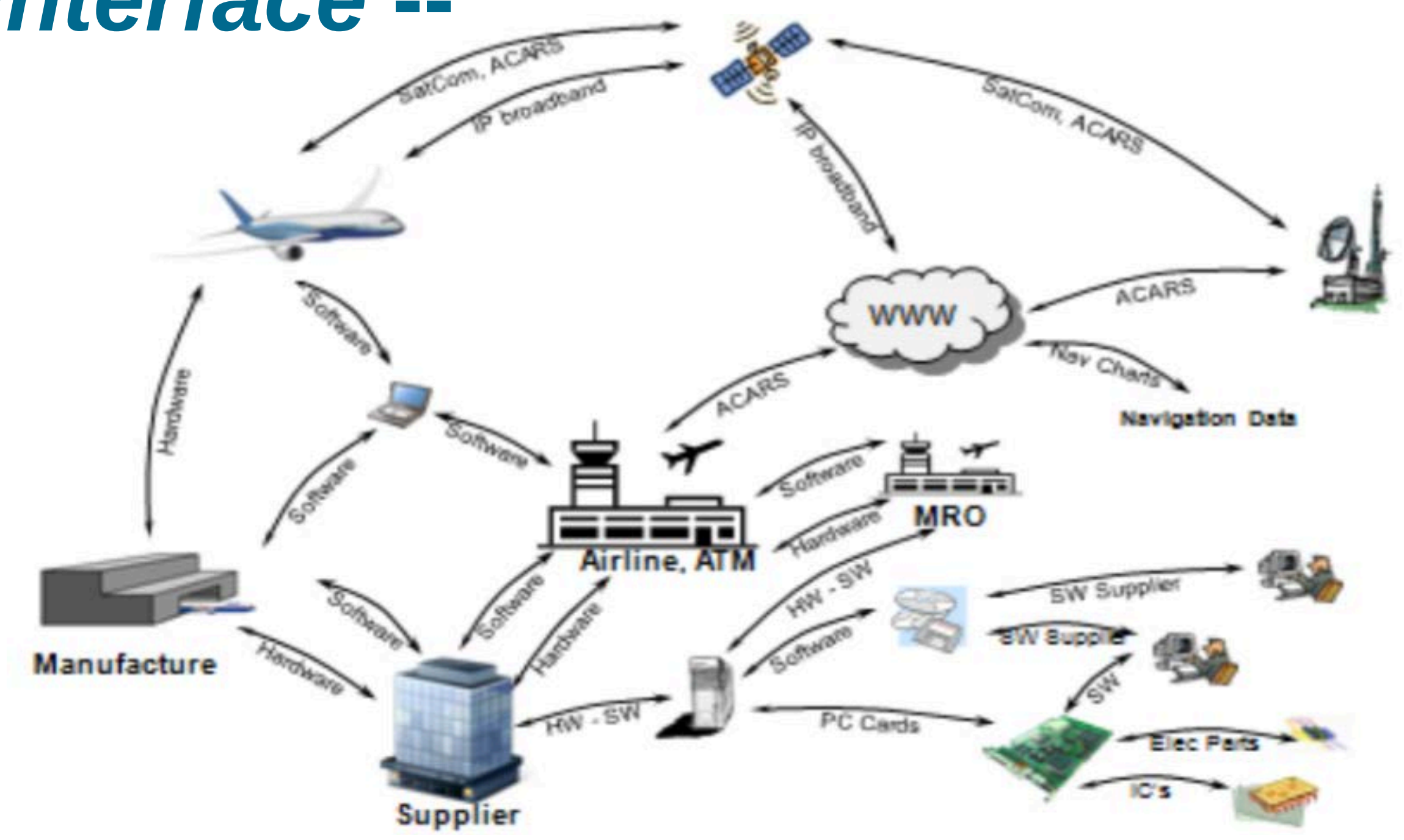


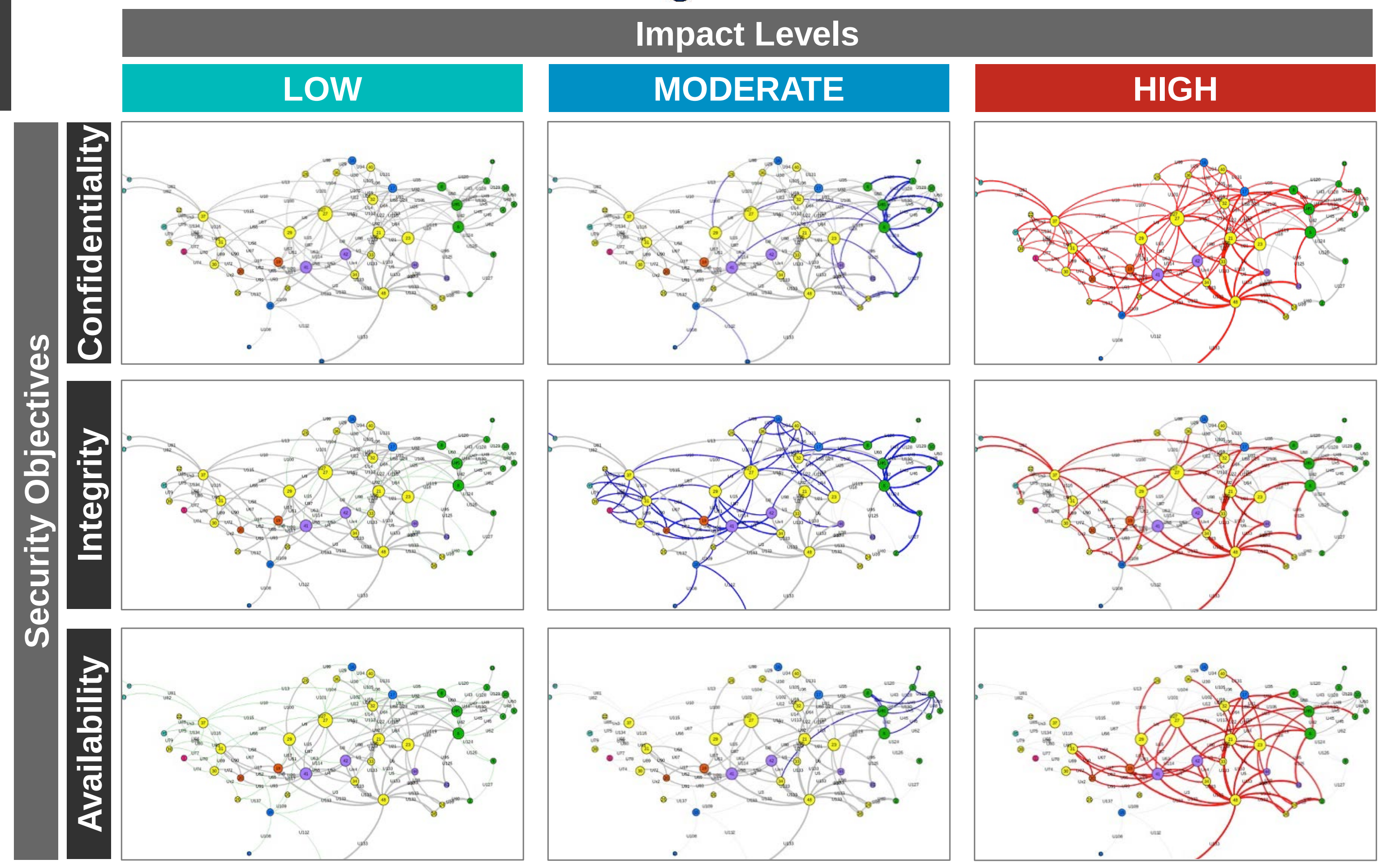
Image source: AIAA, "The Connectivity Challenge: Protecting Critical Assets in a Networked World; A Framework for Aviation Cybersecurity", An AIAA Decision Paper, August 2013.

We can now identify critical nodes for system security

In this case:

- Energy Service Interface (Airport) (7).
- Distribution SCADA (29).
- Demand Response Management System (32).
- Advanced Metering Infrastructure Headend (21).

And impact for three security objectives



Massachusetts Institute of Technology

• Based on Analytics for Cyber-Physical System Cybersecurity: Policy-Governed Secure Collaboration • SoS Lablet Kickoff and Quarterly Meeting, March 13-14, 2018
• see https://www.nsa.gov/what-we-do/research/science-of-security/ for details. • **© 2018 Massachusetts Institute of Technology. All rights reserved.**

April 04, 2018