

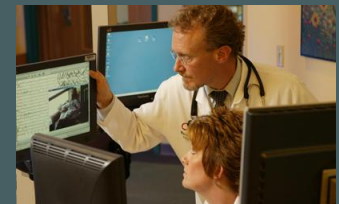
The Risk-to-Mission Assessment Process (RiskMAP)

Jim Watters, jwatters@mitre.org
Peter Kertzner, kertzner@mitre.org
Adam Hahn, ahahn@mitre.org
Deb Bodeau, dbodeau@mitre.org

The MITRE Corporation

API Pipeline Conference & Cybernetics Symposium
April 10, 2008

This material is based upon work supported by the U.S. Dept. of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.



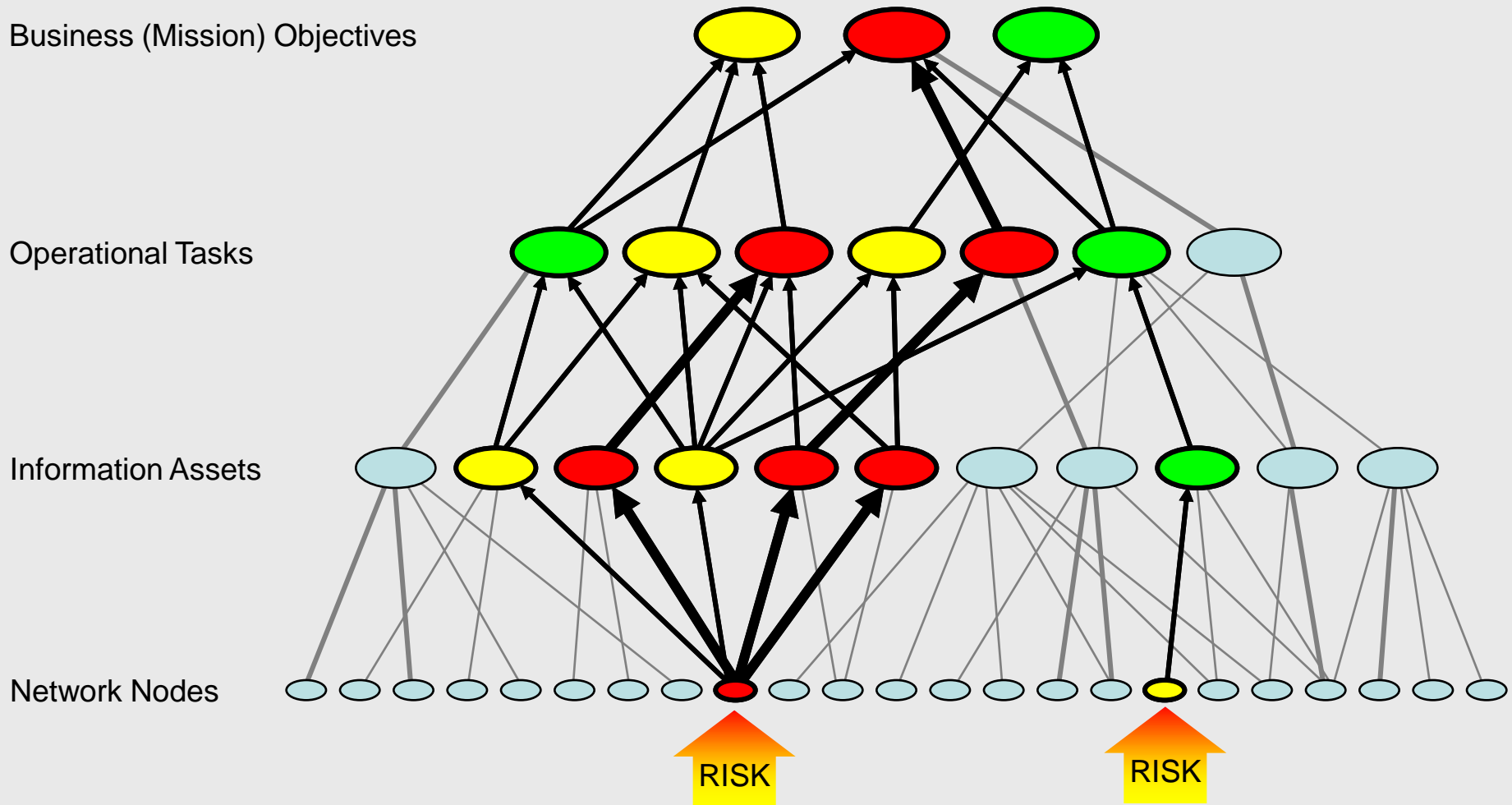
The Need

- As PCS networks are integrated with corporate business networks, the need for inherently secure PCS networks increases
 - Technical security risk analysis is key to improving the security of the system throughout its life cycle
- Network risk analyses are typically done by technologists, while risk mitigation decisions are made by managers
 - Managers must view technical security risks in the larger context of business risks
- **Needed**: A process for assessing PCS network risk *and translating the results* into terms meaningful to corporate-level managers

Our Approach

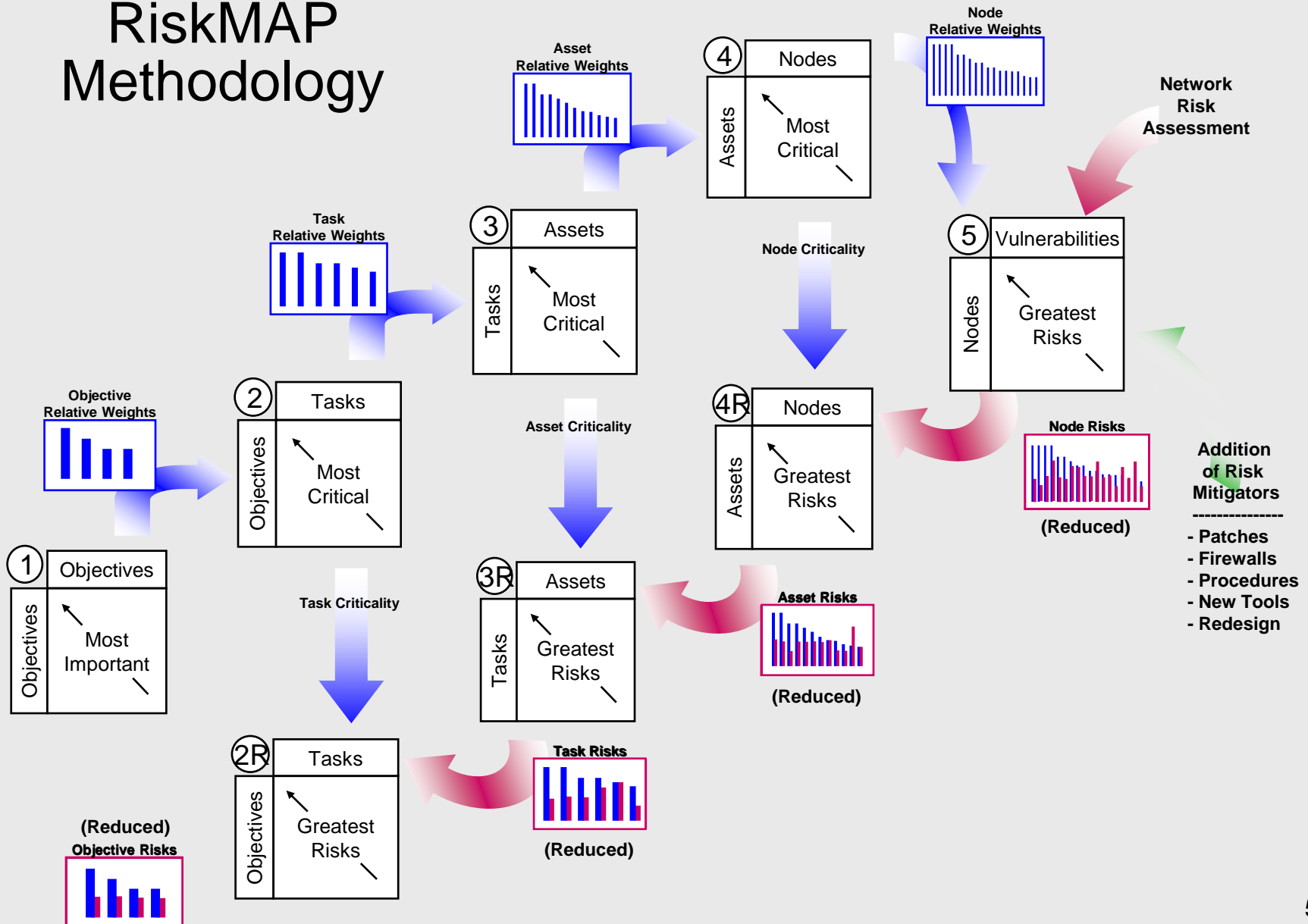
- Apply the Risk-to-Mission Assessment Process (RiskMAP) developed in Support of DHS-Funded I3P PCS Security project
 - Model key features of an organization, from the *Business (Mission) Objectives* to the *Operational Tasks* and *Information Assets* needed to achieve them, to the *Network Nodes* that store, send and make the information available
 - Builds on MITRE work from mid-1990's on DoD risk assessments
 - Draw upon Analytical Hierarchy Process (AHP) and Quality Function Deployment (QFD) methods
 - Capture priorities among corporate mission objectives and operational tasks, and identify the most critical information assets and network nodes
 - Use this model to map risks at the Network level up to the Business (Mission) Objective level, providing executives with solid, credible support for risk mitigation decisions

Our Approach: Find the Dependency Paths

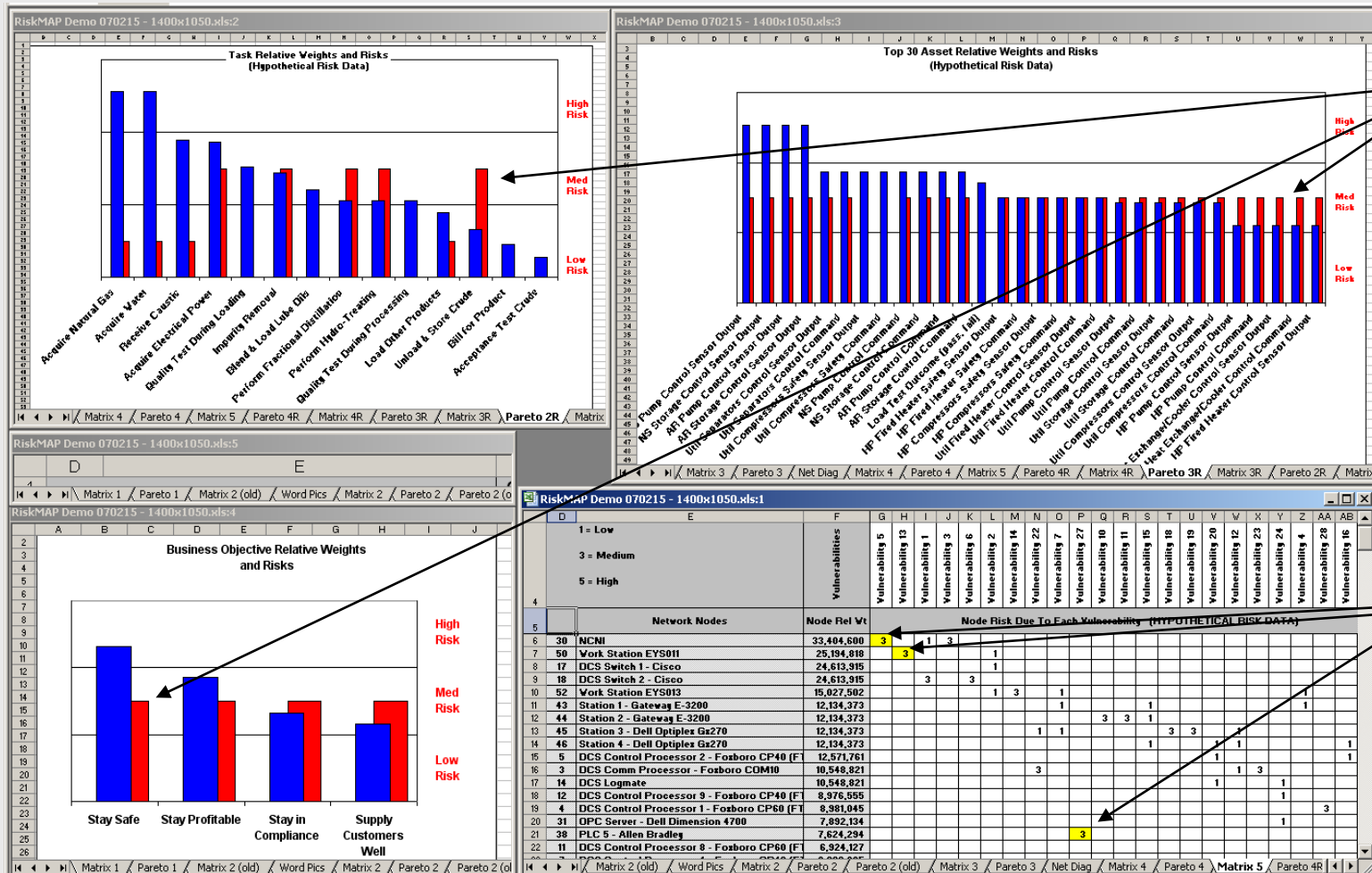


Risk Follows Dependency Paths

RiskMAP Methodology



Dashboard View – After Mitigation



Screen Shot of RiskMAP prototype

Status and Future Research

- RiskMAP Methodology:
 - Adapt from DoD methods
 - Add Calibrated Weighting Scales
 - Add treatment of CONFIDENTIALITY
 - Perform sensitivity analysis of QFD
- Data Templates:
 - Small Refinery (with Ergon Refining, Inc.)
 - Large Refinery (with a major energy firm)
 - Pipeline Operation (seeking a collaborator)
 - Other Sector (Water, Power, Telecommunications)

Technology Transition

- License Agreement signed with Matrikon, Inc. on 10 Oct 07
 - Produce commercial tool based on RiskMAP technology
 - Exclusive license to sell to the following:
 - Power Generation Facilities (Coal, Hydroelectric, Nuclear)
 - Power Transmission & Distribution
 - Chemical Plants
 - Oil & Gas Refineries
 - Non-exclusive in other sectors
- Fluid Innovation (Austin, TX) serves as intermediary
 - Licensing available for other sectors
 - Info at www.fluidinnovation.com

What Can You Do?

- Today:
 - Start thinking about your own enterprise in terms of business objectives, supporting tasks, information assets, and associated network nodes.
 - What are your dependencies at each level?
 - What would you put into a RiskMAP model?
- For Additional Practical Information:
 - Forthcoming Matrikon tool - rick.kaun@matrikon.com
 - Licensing opportunities - andrew.allemann@fluidinnovation.com
- For Additional Research Information:
 - RiskMAP methodology - www.thei3p.org/publications
 - Collaborating on a data template - jwatters@mitre.org