Process Control Systems Industry Conference

RiskMAP: Translating ICS Risk Assessments Into Corporate Terms

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

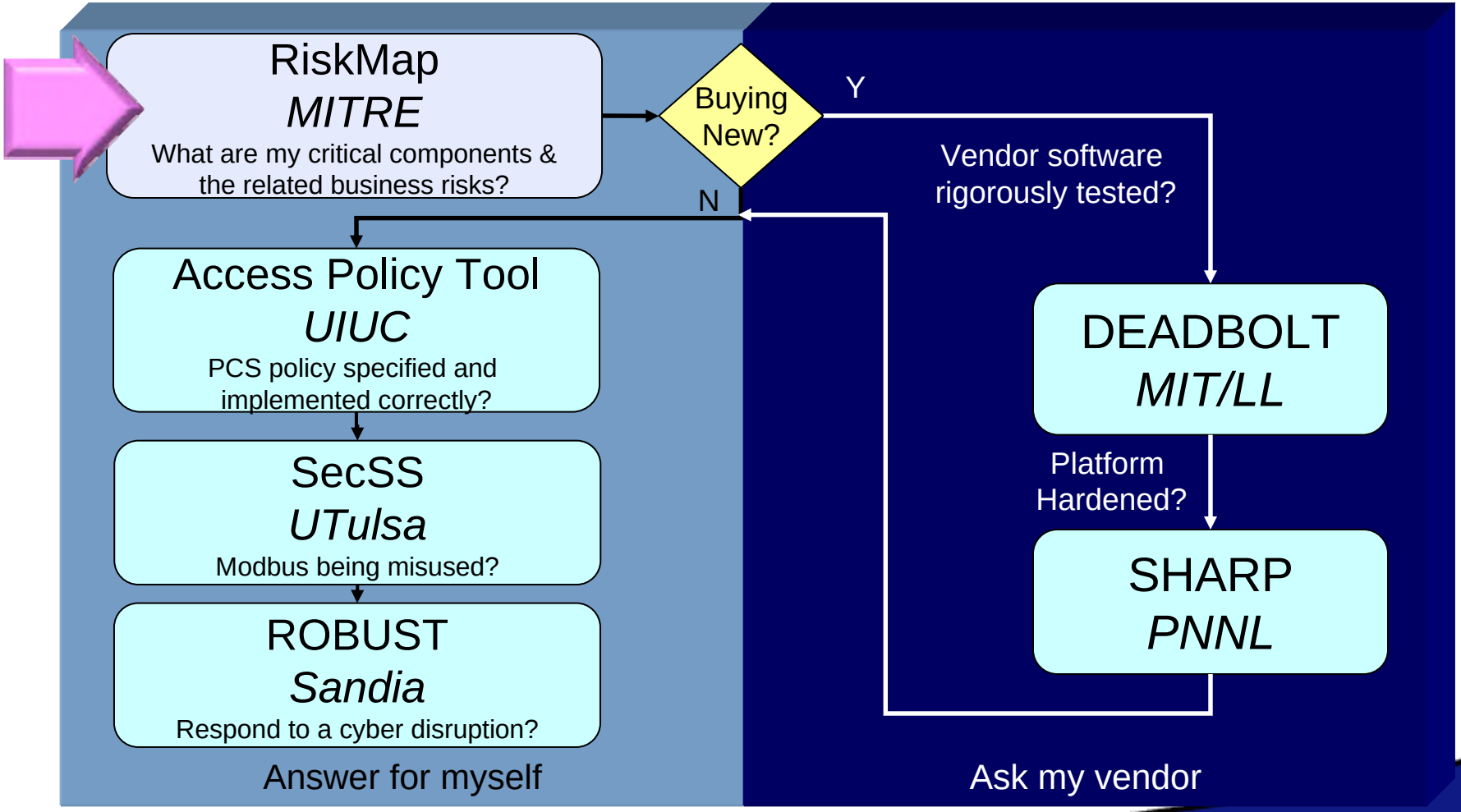
August 28, 2008

MITRE I3P

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.

Approved for Public Release; Distribution Unlimited. MITRE Nos. 08-1243 and 06-0760.Copyright © 2008 by the Trustees of Dartmouth College. The I3P Logo is a trademark of Dartmouth College. All information contained in this document may not be reproduced without permission by the I3P.

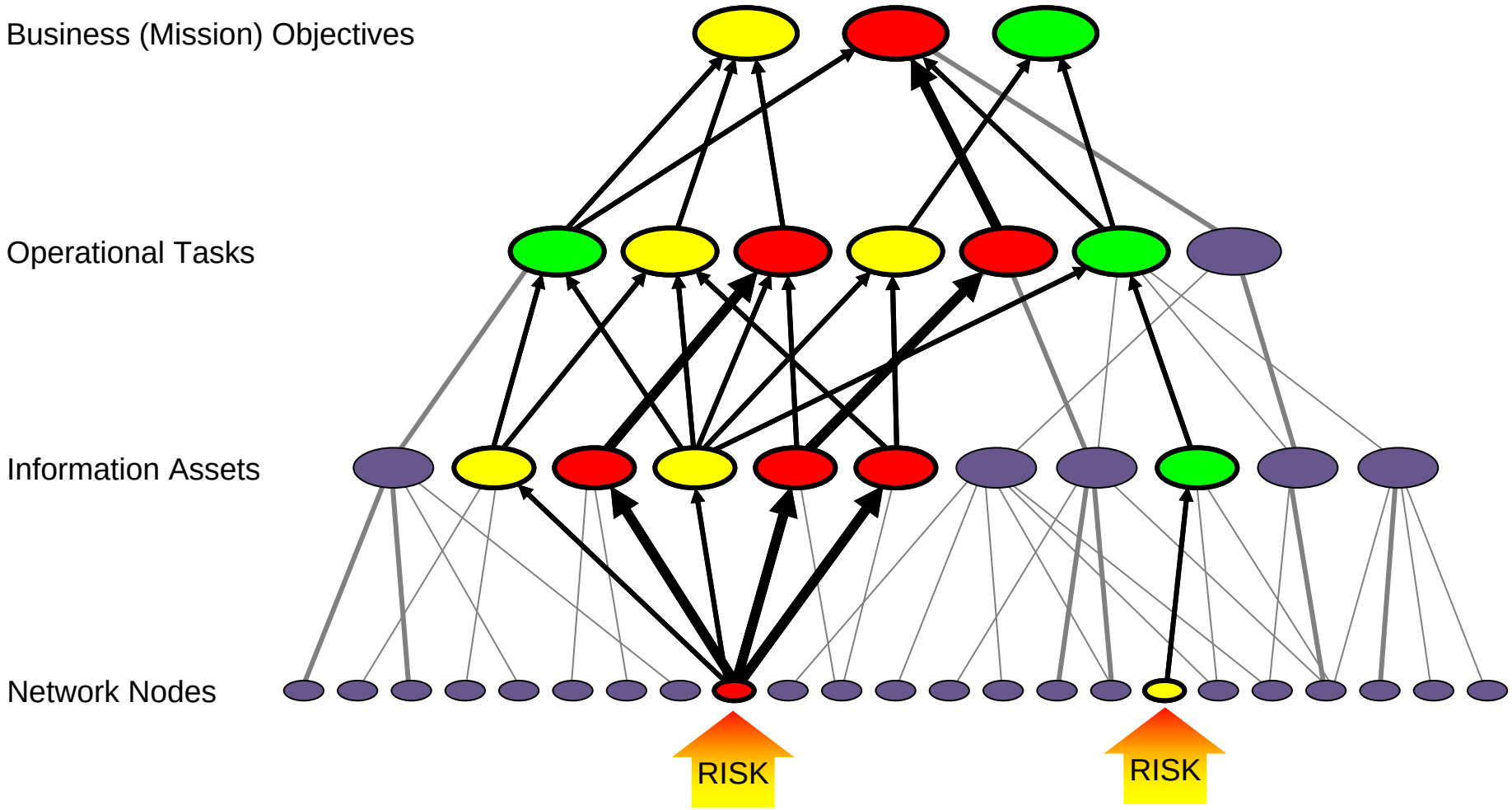
RiskMAP is One of Several I3P Tools Aimed at Answering Tough Security Questions



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
- **<u>Needed</u>: A process for assessing PCS network risk *and translating the results* into terms meaningful to corporate-level managers**

Our Approach: Find the Dependency Paths

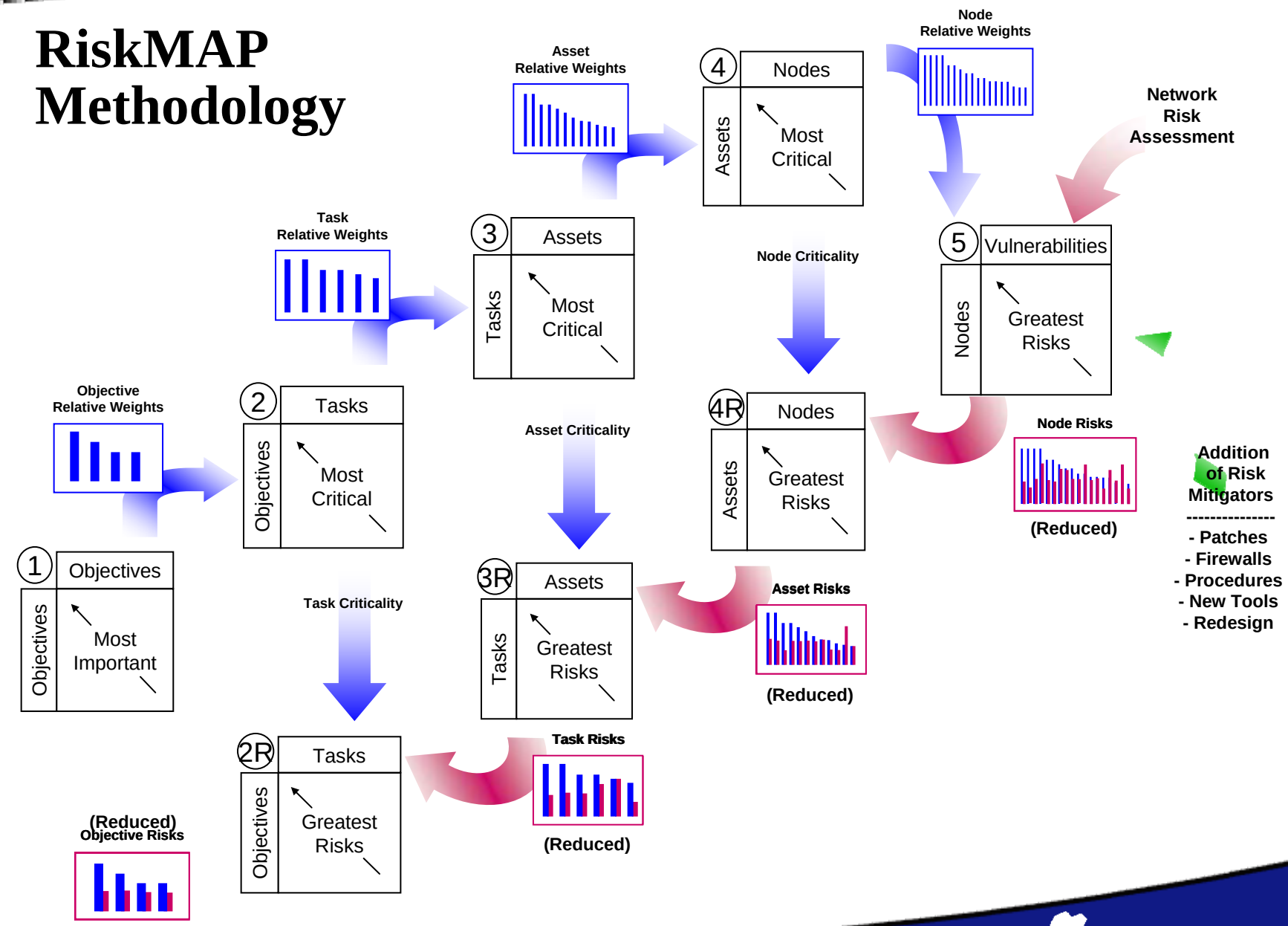


Risk Follows Dependency Paths

Our Approach (Continued)

- **Apply the Risk-to-Mission Assessment Process (RiskMAP) developed during the previous 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
    - 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

RiskMAP Methodology



Brief Demonstration

User Remarks (1 of 3)

- **Provided by Steve Elwart – Ergon Refining, Inc.**
  - Director of Systems Engineering
  - Chairman, NPRA Cyber-Security Subcommittee
  - Member, Energy Sector Control Systems Working Group (ESCSWG)
    - Working on the Interactive Energy Roadmap (***ieRoadmap***)
  - Unable to attend due to late-breaking schedule change for major system upgrade

User Remarks (2 of 3)

- **Ergon's Cost of Using RiskMAP**
  - Executive* time expended = 42 hrs
    - Project kickoff and approval
    - Capture Objectives, Tasks, and weights
    - Review interim results

      * - Refinery Management (non-IT)
  - Staff time expended = 56 hrs
    - Capture Assets, Nodes, and weights
    - Update detailed network diagram
    - Validate model information

User Remarks (3 of 3)

- **Ergon's Observations from using RiskMAP:**
  - Going through the process was of value to all concerned
    - Fixing vulnerabilities began the same day as the results were known
  - Results seem to accurately reflect the risks at the Ergon Refining plant
    - Borne out by subsequent instance of municipal water loss
  - Any process as sizable as this needs to have management support
    - Ergon Refining, Inc. management provided support and involvement

Other Methods and/or Tools

- **Numerous methods and/or tools have been observed and considered during the development of RiskMAP, including:**

  - @Risk
  - AMP
  - API-NPRA
  - CARVER
  - COBRA
  - CORA
  - CRAMM
  - CS2SAT
  - Enterprise Risk Register
  - IA CAT
  - MAAP
  - MORDA
  - OCTAVE
  - RAMCAP
  - RAM-D (et al)
  - RAPSA
  - RiskNav
  - RiskOptimizer
  - RiskWatch
  - RRAT
  - SCAP
  - SEMS
  - Skybox
  - VSAT

More Details

What's Unique About RiskMAP?

- **Many risk assessment methods and tools are available, some of which address *linkage to mission***
  - Those addressing linkage to mission seem to exhibit one or more common characteristics:
    - Asset criticality is tied to "importance to the organization" rather than to a specific business (mission) objective
    - The user identifies the important assets that come to mind, but can omit assets whose mission criticality is subtle but significant
  - The result is an assessment that is:
    - Too abstract in its mission-linkage argument, or
    - Potentially misleading as to its level of completeness
- **RiskMAP addresses both shortcomings**
  - Node-level risks are linked directly to Business (Mission) Objectives
  - Mission-decomposition approach discovers all critical assets

Status and Future Research

- **Data Templates:**
  - ☑ Small Refinery (with Ergon Refining, Inc.)
  - ☑ Large Refinery (with a major energy firm)
  - IN WORK ❑ Other Sector (Water, Power, Telecommunications)
- **RiskMAP Methodology:**
  - ☑ Adapt from DoD work
  - ☑ Add Calibrated Weighting Scales
  - IN WORK ❑ Add treatment of CONFIDENTIALITY
  - ❑ Perform sensitivity analysis of QFD

Why Confidentiality?

- **Currently, RiskMAP addresses Integrity and Availability issues**
  - Topmost issues identified by Oil & Gas owner-operators.
- **Confidentiality issues lurk behind the scenes for current users**
  - PCS equipment settings, lab results, operational data represent significant intellectual property
- **Future use of RiskMAP could be in sectors where Confidentiality is of equal or greater importance**
  - E.g., Medical, Law Enforcement, Defense or Financial sectors

More Details

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 Research Information:
  - RiskMAP methodology - *www.thei3p.org/publications*

Backup Charts

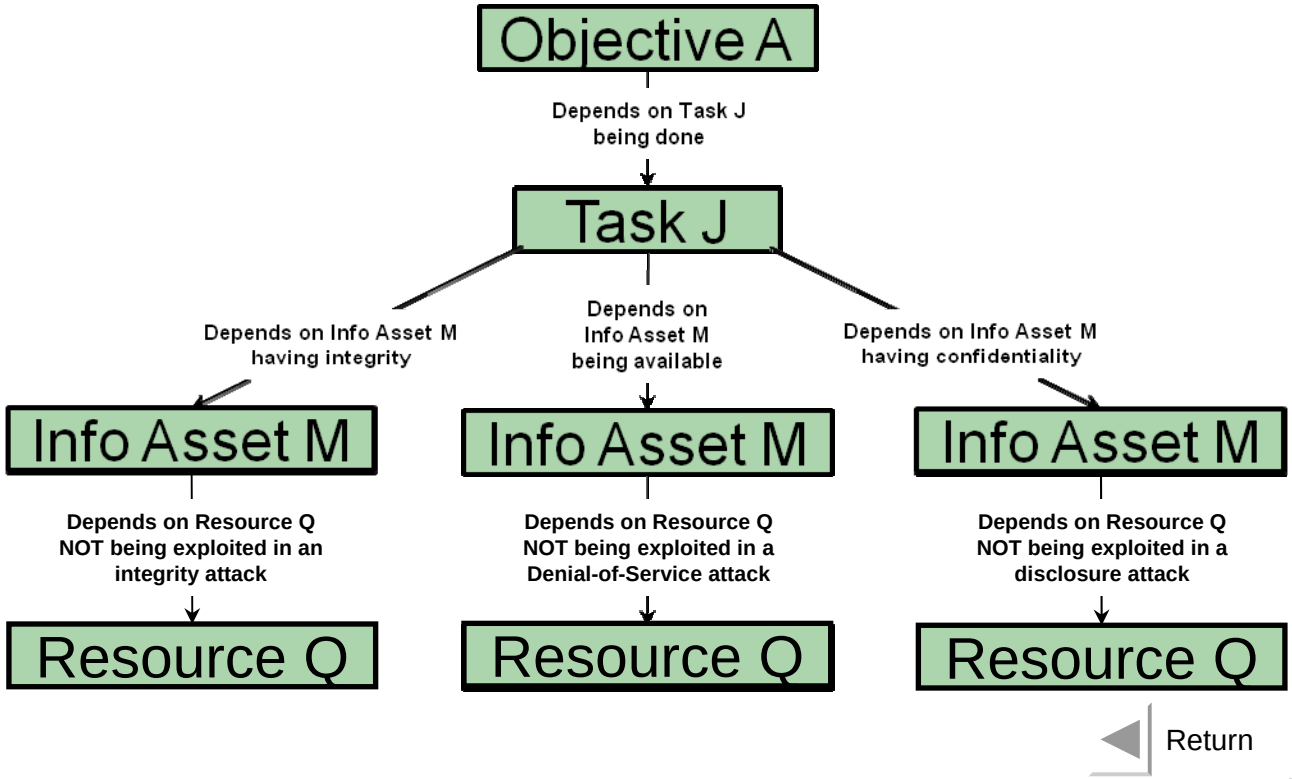
Extending the RiskMAP Model: Overview

- Refine the set of business objectives
- Define clusters of tasks related to confidentiality, integrity, and availability of information
- Map those tasks to business objectives
- Refine the definition of information asset
- Generalize “node” to “resource”
- Refine the assessment process to accommodate the dimensions of confidentiality, integrity, and availability
- Refine the “word pictures” to align with FIPS PUB 199 impact definitions

Return

Our Approach

- **Extend the current RiskMAP tool to capture Confidentiality-based dependencies**
  - Utilize the same basic structure – just add parallel analysis paths



Details – *Other Methods/Tools (1 of 3)*

Method/Tool	Source
@Risk	@Risk developed by Palisade Corporation, Ithaca, NY. www.palisade.com
AMP	Assessment Management Platform (AMP) developed by SPI Dynamics, Atlanta, GA. www.spidynamics.com
API-NPRA	Security Vulnerability Assessment (SVA) methodology developed by API-NPRA. www.api.org or www.npra.org
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability (CARVER) developed for the Food industry. www.ngfa.org/pdfs/Carver_Shock_Primer.pdf
CobiT	CobiT developed by the IT Governance Institute (ITGI) www.itgi.org
COBRA	COBRA developed by C&A Systems Security, Ltd. www.riskworld.net
CORA	Cost-of-Risk Analysis (CORA) developed by International Security Technology, Inc., NY. www.ist-usa.com/aboutcora.htm
CORAS	CORAS developed by the Institute if Computer Science http://www2.nr.no
CRAMM	UK Government's Risk Analysis and Management Method (CRAMM) developed by Siemens, UK. www.cramm.com
CS2SAT	Control System Cyber Security Self-Assessment Tool (CS2SAT) developed by Idaho National Laboratory (INL) for DHS www.isa.org/asci/CS2SAT

Return to List

Details – *Other Methods/Tools (2 of 3)*

Method/Tool	Source
Enterprise Risk Register	Enterprise Risk Register developed by Incom PTY LTD, Roseville, Australia. www.incom.com.au
IA CAT	Info Assurance Compliance Assessment Tool (IA CAT) developed by MITRE team led by Daryl Hild.
MAAP	Mission Assurance Analysis Protocol (MAAP) developed by CMU. www.sei.cmu.edu/pub/documents/05.reports/pdf/05tn032.pdf
MORDA	Mission-Oriented Risk and Design Analysis (MORDA) developed by Innovative Decisions, Inc., Vienna, VA. www.innovativedecisions.com
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) developed by CMU. octave-info@sei.cmu.edu
RAMCAP	Risk Analysis And Management For Critical Asset Protection (RAMCAP) developed by ASME Innovative Technologies Institute for DHS. www.asme-iti.org/RAMCAP
RAM-D (et al)	Risk Assessment Methodologies (RAMs) developed by Sandia National Labs. Www.sandia.goc/ram
RAPSA	Risk Analysis and Probabilistic Survivability Assessment (RAPSA) developed by the University of Idaho for NIST. {ctaylor, krings, jimaf}@cs.uidaho.edu

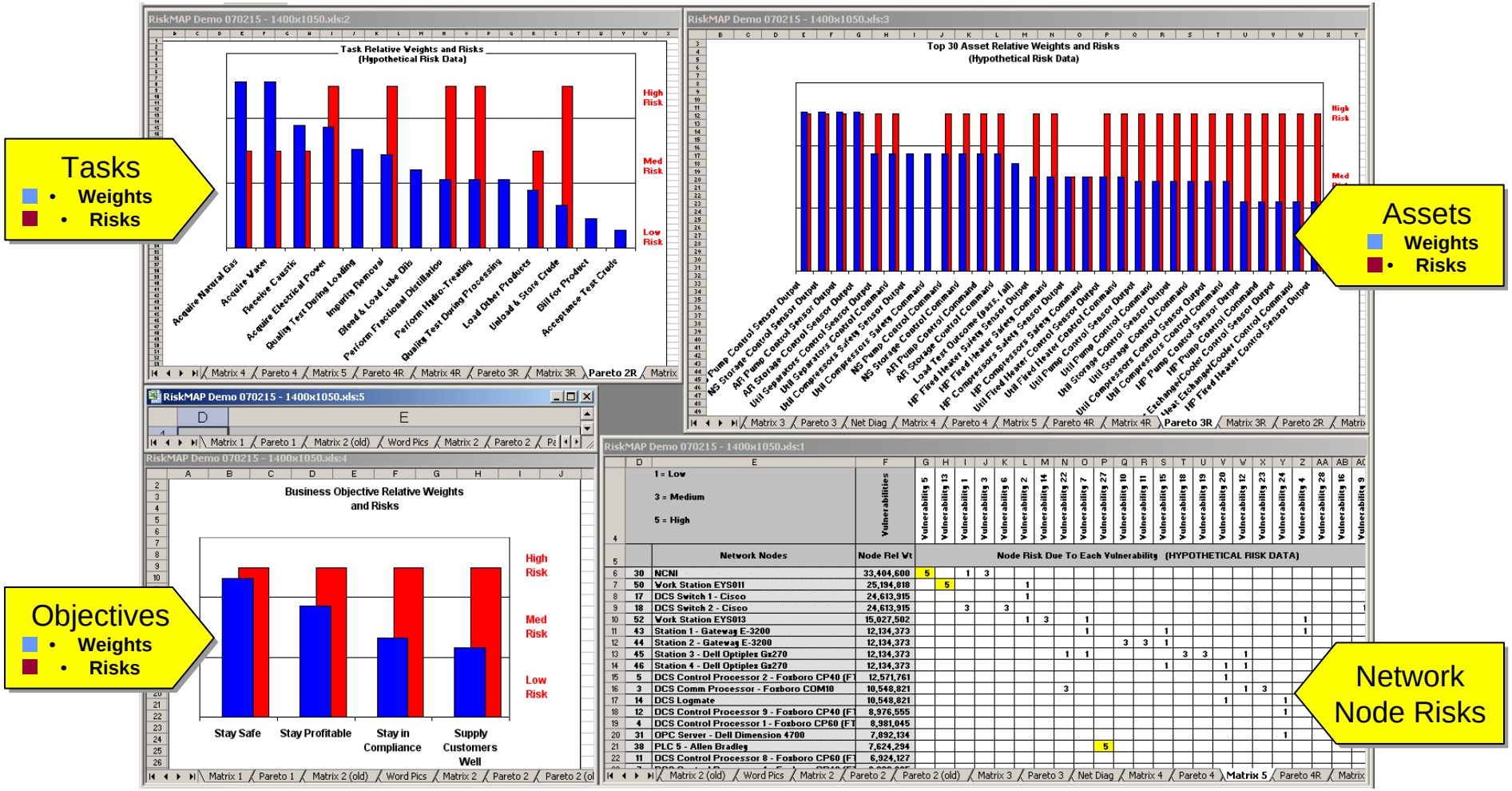
Return to List

Details – *Other Methods/Tools (3 of 3)*

Method/Tool	Source
RiskNav	RiskNav developed by MITRE. www.mitre.org/work/sepo/toolkits/risk/ToolsTechniques/RiskNav.html
RiskOptimizer	RiskOptimizer developed by Palisade Corporation, Ithaca, NY. www.palisade.com/riskoptimizer
RiskWatch	RiskWatch developed by RiskWatch Headquarters, Annapolis MD. www.riskwatch.com
RRAT	Risk Reduction Analysis Tool (RRAT) developed by Idaho National Laboratory for US-CERT CSSC. www.inl.gov
SCAP	Security Content Automation Protocol (SCAP) developed by NIST. http://nvd.nist.gov/scap.cfm
SEMS	Security and Emergency Management System (SEMS) developed by SEMS Technologies, LLC www.semstechnologies.com
Skybox	Skybox developed by Skybox Security Inc. www.skyboxsecurity.com
VSAT	Vulnerability Self Assessment Tool (VSAT™) released by the Association of Metropolitan Sewerage Agencies (AMSA). Available at VSATusers.net.

Return to List

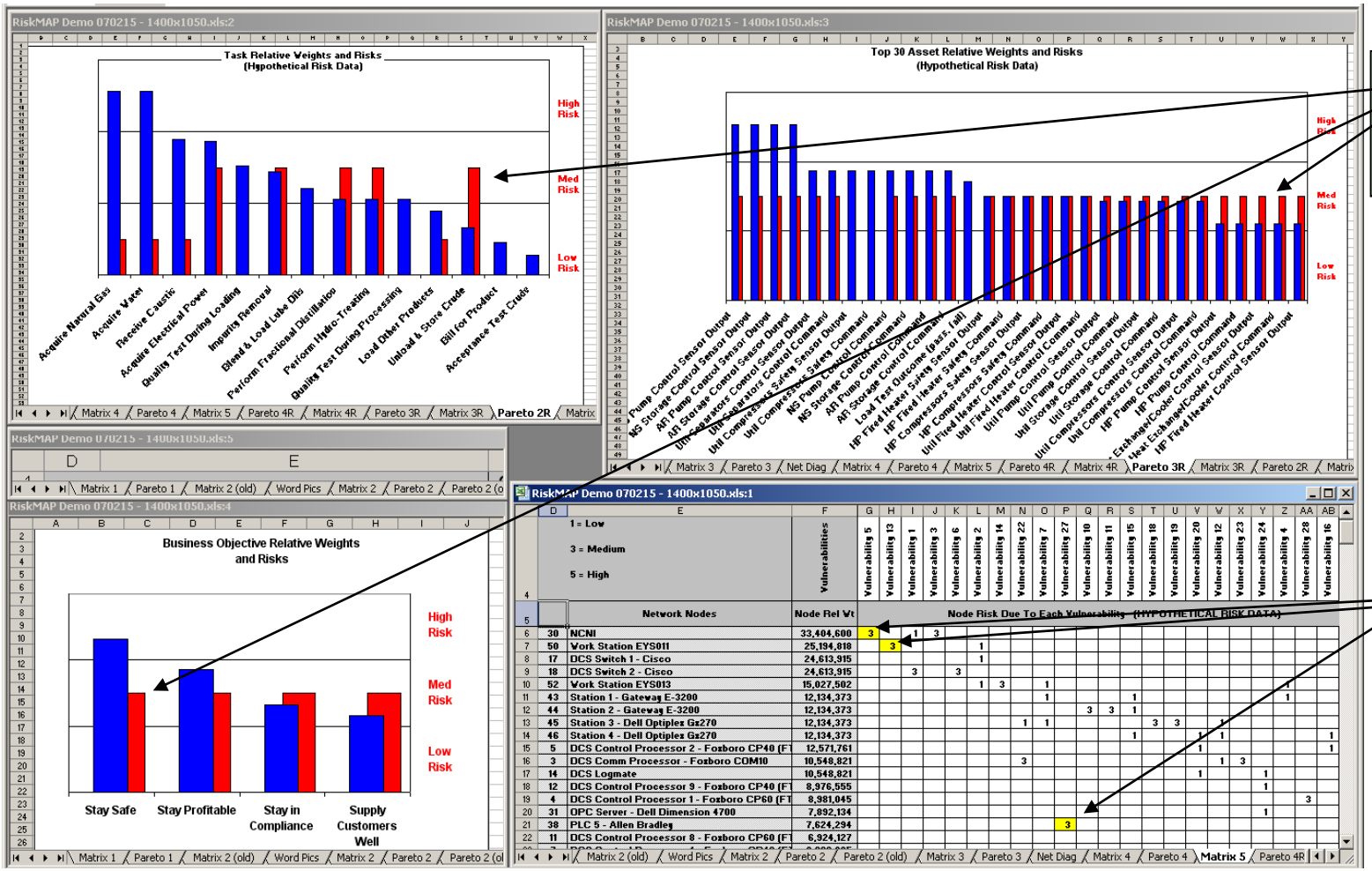
Dashboard View – Before Mitigation



Screen Shot of RiskMAP prototype

Process Control Systems Industry Conference

Dashboard View – After Mitigation



Reduced Risks Based on Modeled Dependencies

Addition of Risk Mitigators

Screen Shot of RiskMAP prototype

Process Control Systems Industry Conference