Establishment of the European ICT Security Risk Management Initiative (SRMI)

ENISA Risk Management Workshop

October 13, 2006, Rome, Italy

Eyal Adar
Chairman of the SRMI
CEO of White Cyber Knight
Eyal@WhiteCyberKnight.com
http://www.WhiteCyberKnight.com

SecurIST

White Cyber Knight
WCK

Introducing Eyal Adar

Eyal Adar is a leading experts in the areas of Risk Management, CIP (Critical Infrastructure Protection) and IT Security

- Involvement in leading Research Activities by the European Commission:
  - The ***ACIP*** Project (Assessment of Critical Infrastructure Protection); this project yielded a roadmap for the development and application of methodologies and tools for CIP related activities
  - A member of the advisory board for the ***CI2RCO*** project (the European Commission's project on Critical Information Infrastructure Research Co-ordination), aimed at coordinating European CIP research
  - A member of the advisory board for the ***IRRIIS*** project (Integrated Risk Reduction of Information-based Infrastructure Systems), aimed at analyzing dependencies between critical infrastructures
  - A Founding Editor of the ***European CIIP Newsletter***
- Founder and Chairman of *iTcon Ltd.* (1995), an information security consulting firm, specializing in enterprise security architecture, in Israel and in Europe
- Founder and CEO of *White Cyber Knight* (2006), a start-up company developing a comprehensive IT Risk Management software, for large and medium-sized organizations

Building a Trustworthy Service-centric Information Society

ESFORS Software and Service Development, Security & Dependability Workshop

- Trustworthy, scalable services across any medium & domain
- Trusted cross-domain Collaborations & Interactions
- Trusted Computing Infrastructures
- Situational & Context Awareness; Self-Awareness
- Risk assessment & Risk Management
- Engineering Secure and Dependable complex SW & Service systems
- Empowering Users: User-friendly Privacy & Trust Services
- Metrics, Certification, Standards
- …

ESFORS NESSI

From: "*Setting the Scene and PF7 Update*" by **Jacques Bus**, presented at the ESFORS workshop in Paris, September 2006

Information Society Technologies
Funded by EC contract FP6-027599

Security Risk Management Initiative

- The *SRMI* is a European Commission's ICT Security and Dependability Task Force initiative

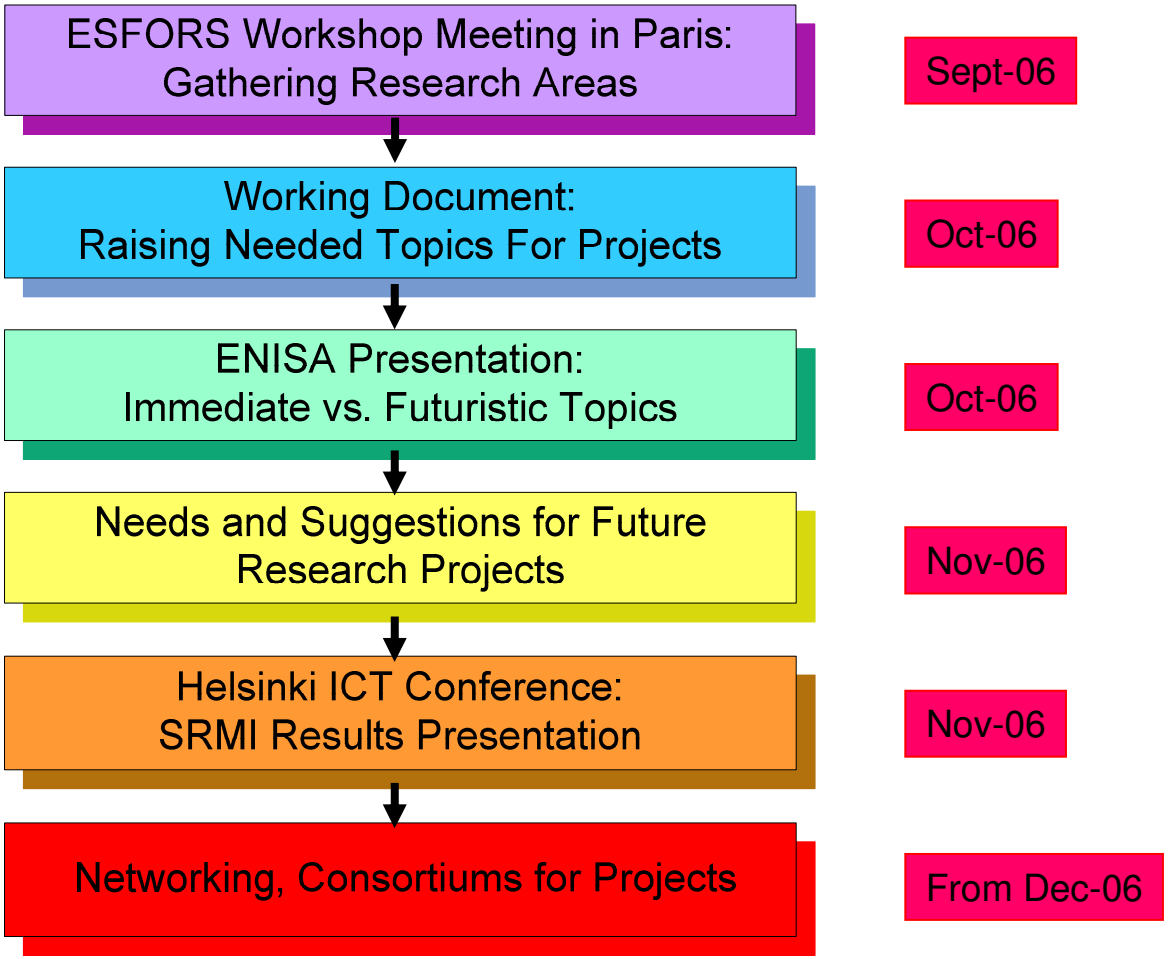
  http://www.securitytaskforce.org/

- The SRMI's goals:
  - Assisting the EC to characterize key Risk Management research topics
  - Helping in the creation of an umbrella for consortiums and projects under the Seventh Program

Consortium Members

- Michael Ruigidel, ENST
- Uwe Beyer, Fraunhofer
- Simin Teherani, Linkopongs
- Alan Stanley, ISF
- Aljosa Pasic, Atos Origin
- Volkmar lotz, SAP
- Pascal Bisson, Thales
- Dominico Salvati, Credit Suisse and ETH
- Andreas Wuchner, Novartis
- Louis Marinos, Enisa
- Jim Clarke, Waterford (Core Team),
- Bernhard Haemerlli, HAT, (Core Team)
- Eyal Adar, WCK, (Chairman)

The SRMI's Work Process



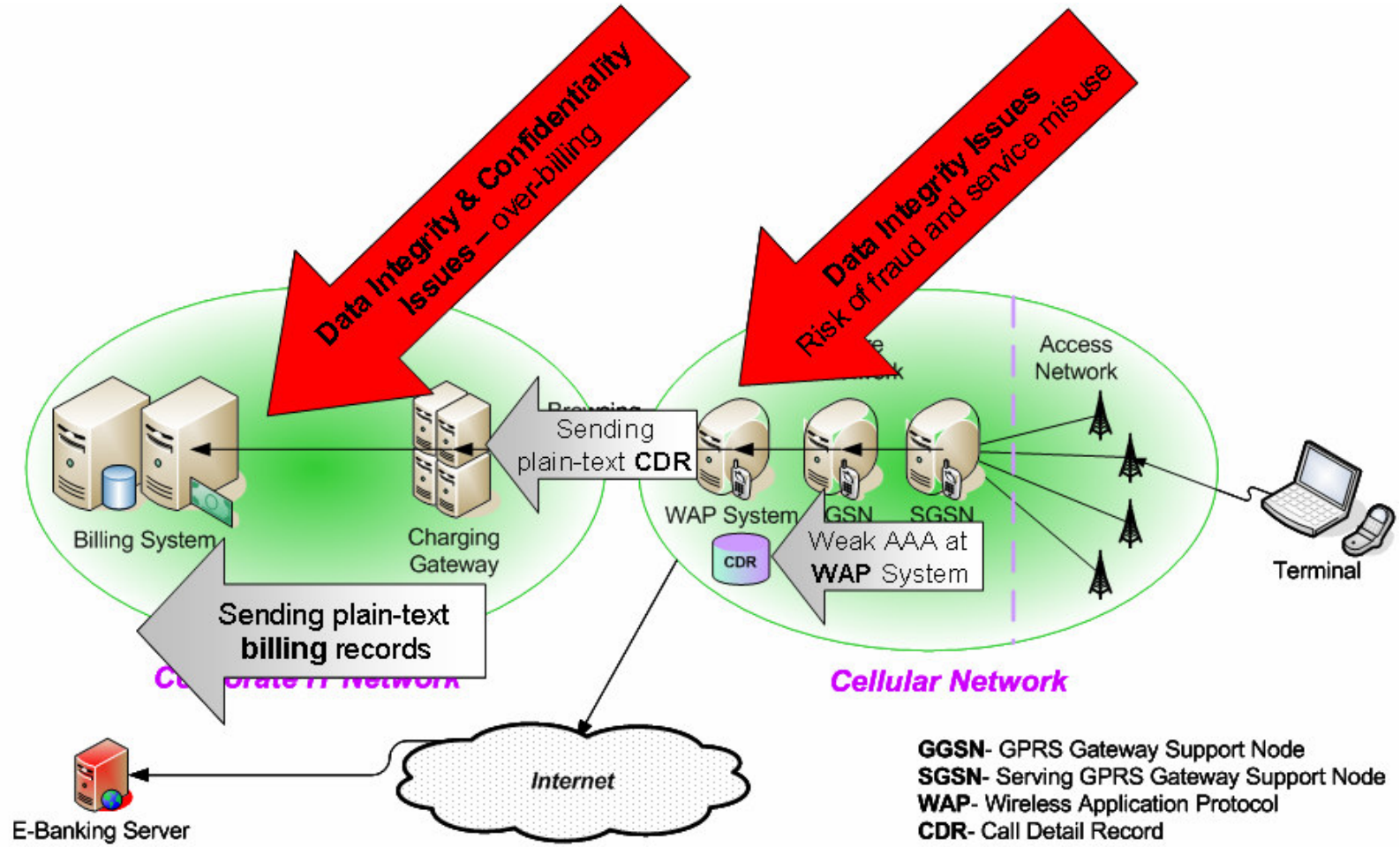
SRMI Research Areas I

- **Taxonomy and Terminology**
  - Examples:
    - Defined agreed terminology
    - For example Measure vs. Metrics
    - Integrative approach
- **Scenarios**
  - Example:
    - banking are using non-banking partners to deliver services, based on SOA and different security policies and the risks and responsibilities are not cleared
  - European research can address this challenge in an effective and an efficient way across different sectors

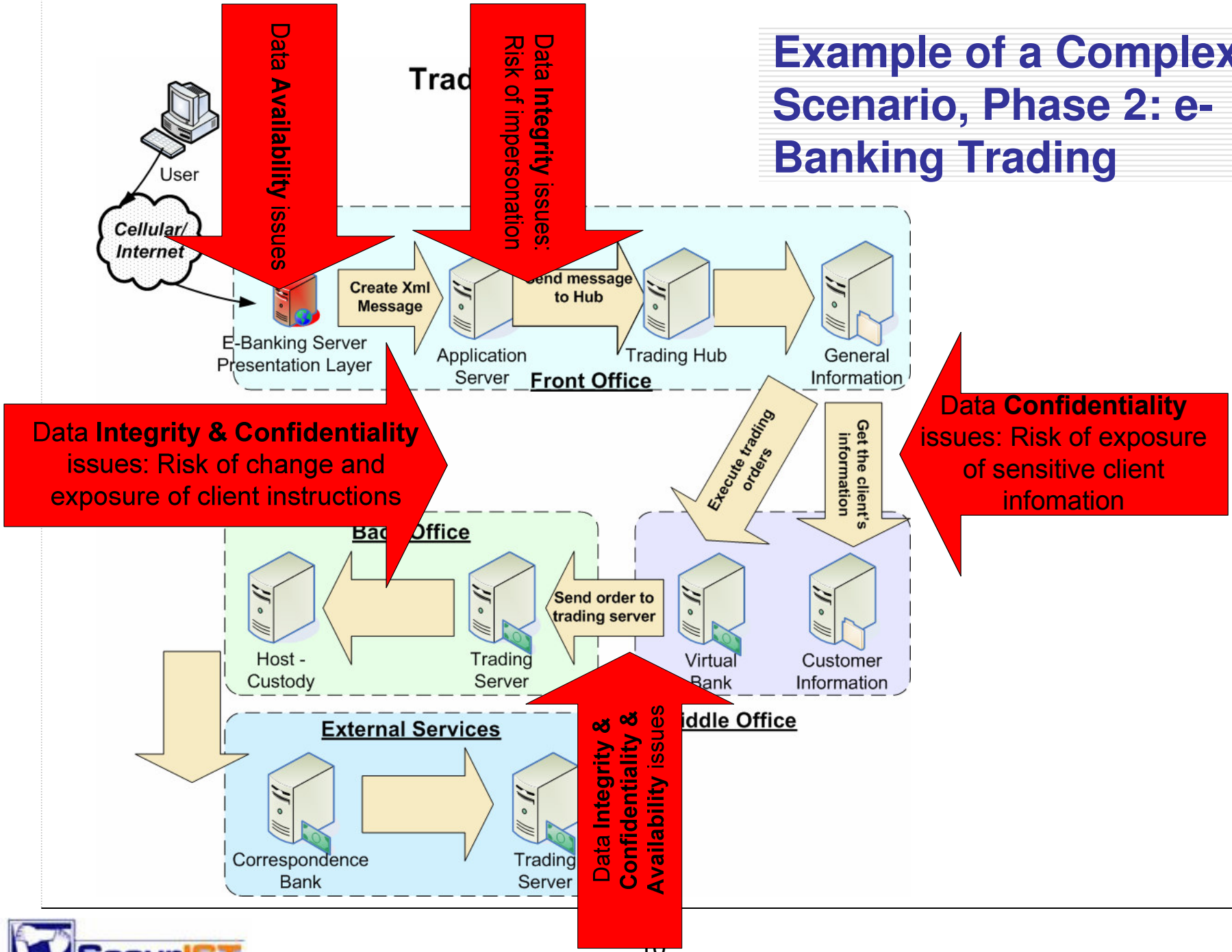
SRMI Research Areas II

- **Threats**
  - Examples:
    - Identification, measure (statistics), complex scenarios, motivation Identification, Integrating threat and incident management, anonymity of threats information
    - Finding methods and tools to identify new threats of complex systems, behavior of it systems (Attack scenarios and trees)
    - Likelihood and Impact of threats
    - Metrology (finding the right variables)
    - Develop understanding of threats, escalation and propagation
    - Intentional vs. unintentional threats

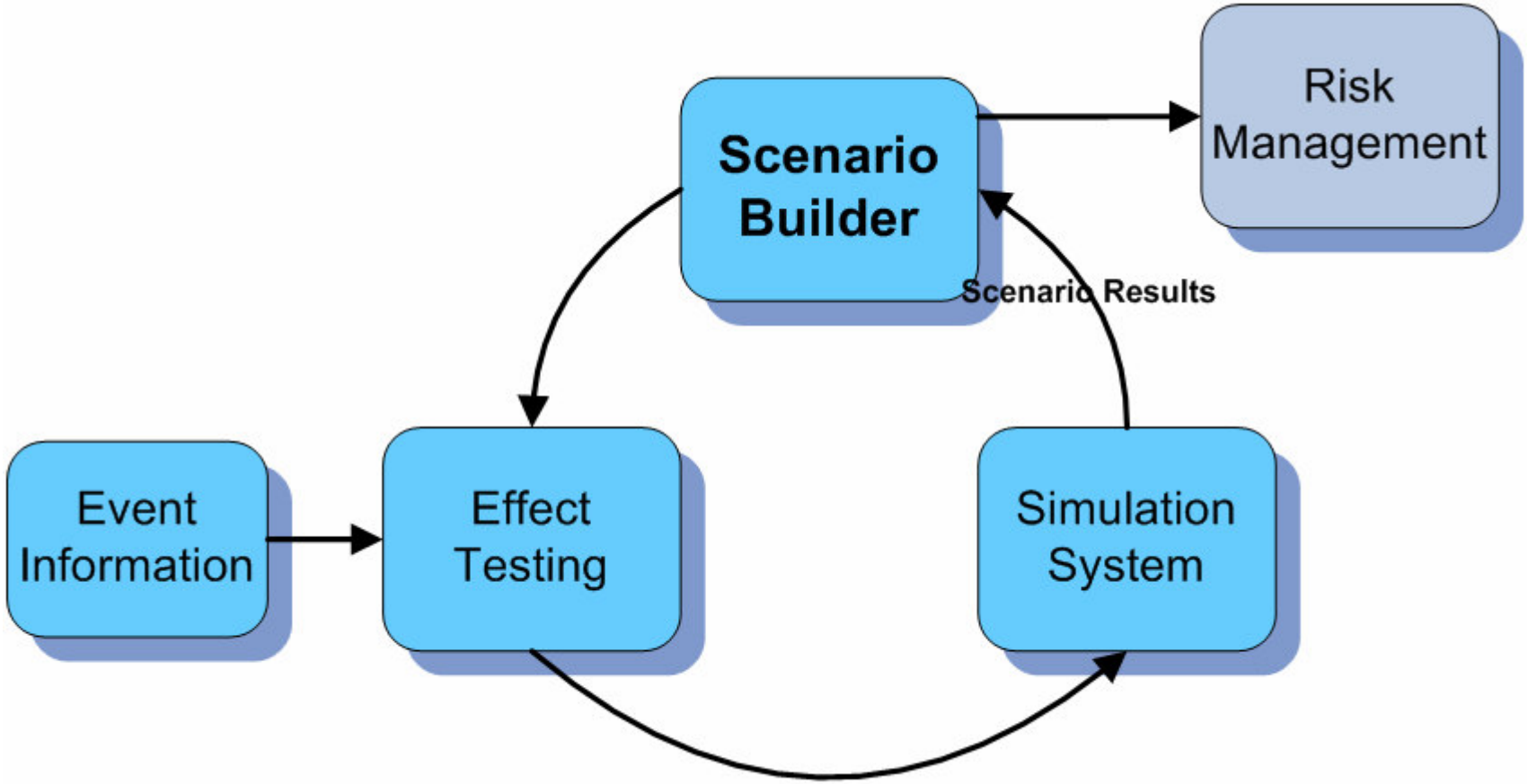
Example of A Complex Scenario, Phase 1: Cellular Browsing into an e-Banking Server



Example of a Complex Scenario, Phase 2: e-Banking Trading



Example for a Research Project – A Scenario Builder for Complex Systems



SRMI Research Areas III

- **Vulnerabilities**
  - Examples:
    - Meta language for automated tools
    - Threats to Vulnerabilities correlation
- **Risks**
  - Examples:
    - Risks ownership in complex environment
    - Organizational and process model to audit and control risk and impacts, and decision process

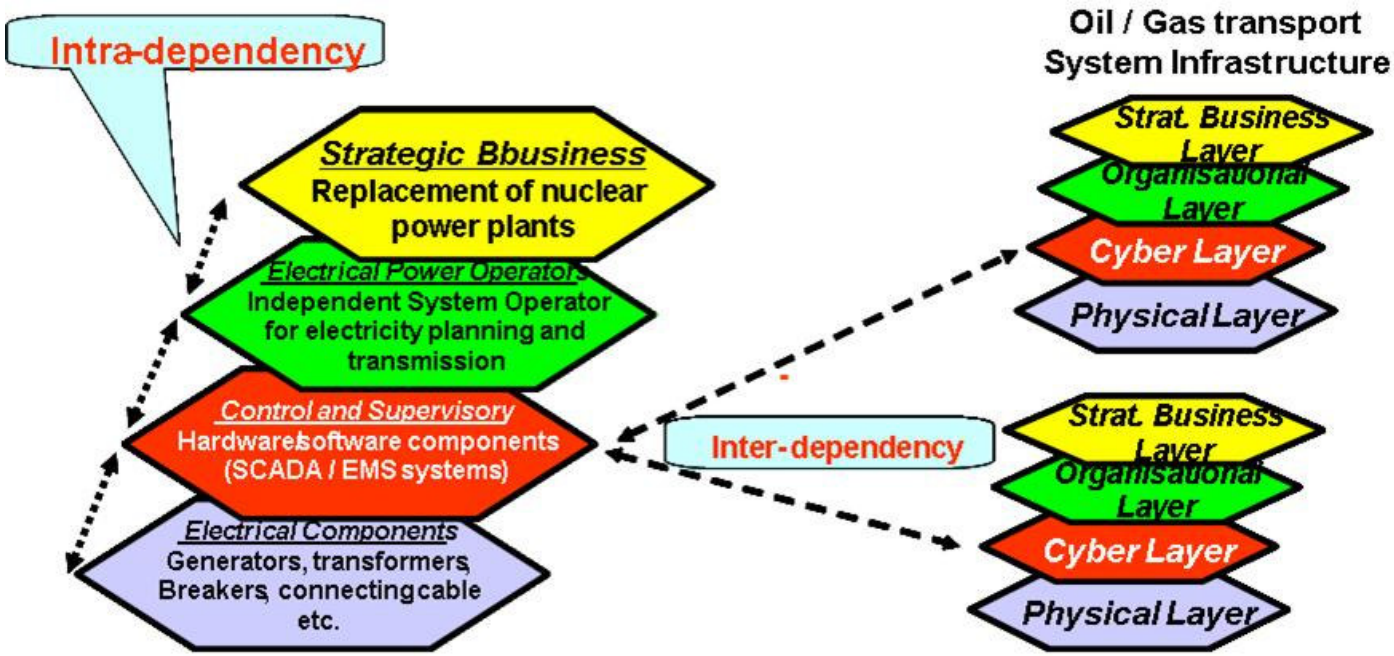
SRMI Research Areas IV

- **Metrics**
  - Examples:
    - Needed security level, technical requirements, SLA
    - Quantitative variables to quantify RM aspects
- **Cross Border Aspects**
  - Examples:
    - Identify gaps between countries and organizations
    - Reaching mutual recognition

SRMI Research Areas V

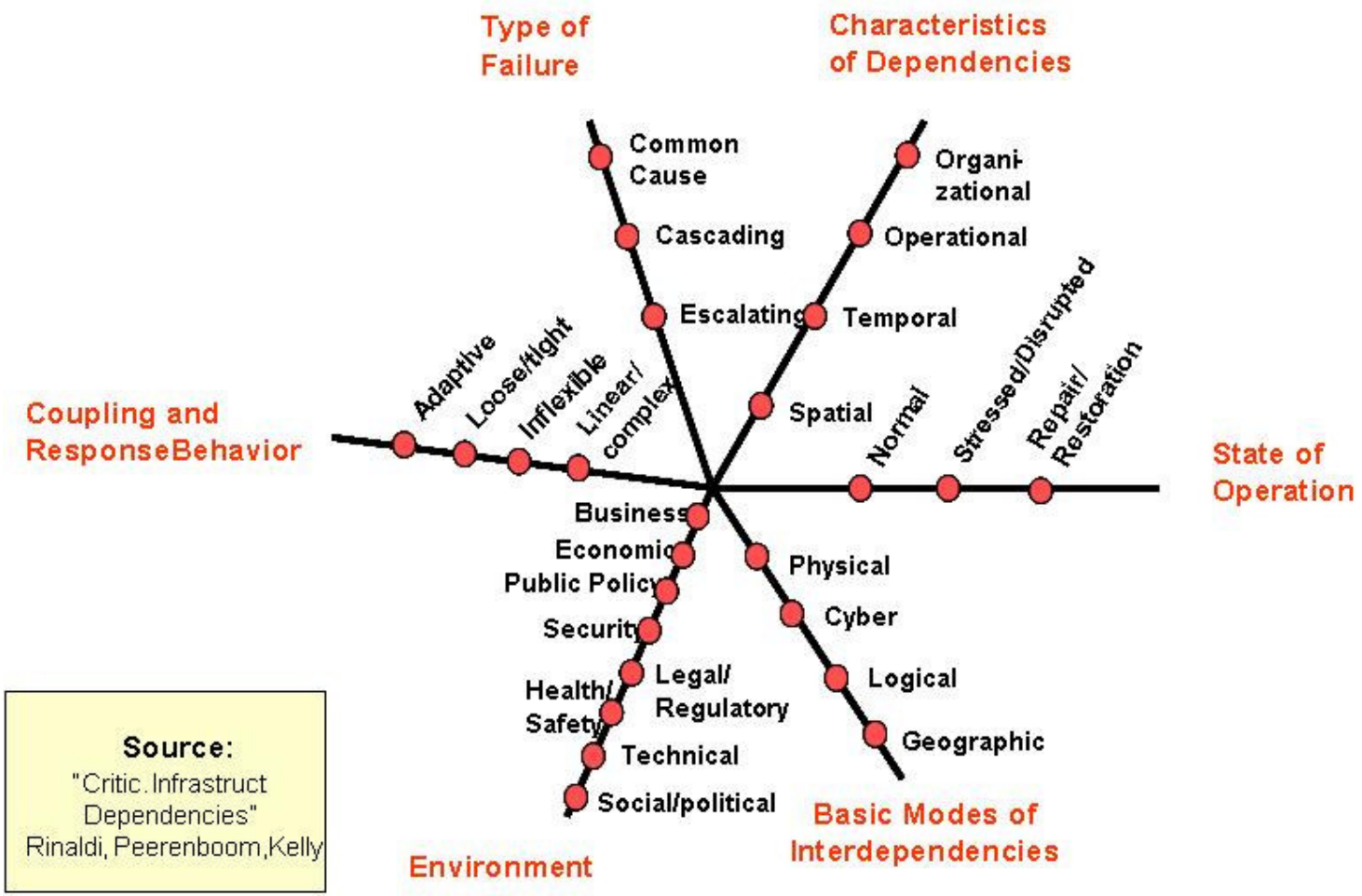
- **Policies**
  - Example:
    - Defined the needed future policies, dynamic and adaptive policies, converting policies to reality, policies implementation verification tools
- **Assessment**
  - Examples:
    - Futuristic assessment models
    - CIP (Critical Infrastructure Protection) dependencies
    - CIP Multidimensional Impact Vector
    - Dependencies between Governance and technical security

CIP Dependencies Assessment



Source: ACIP Project, D6.2

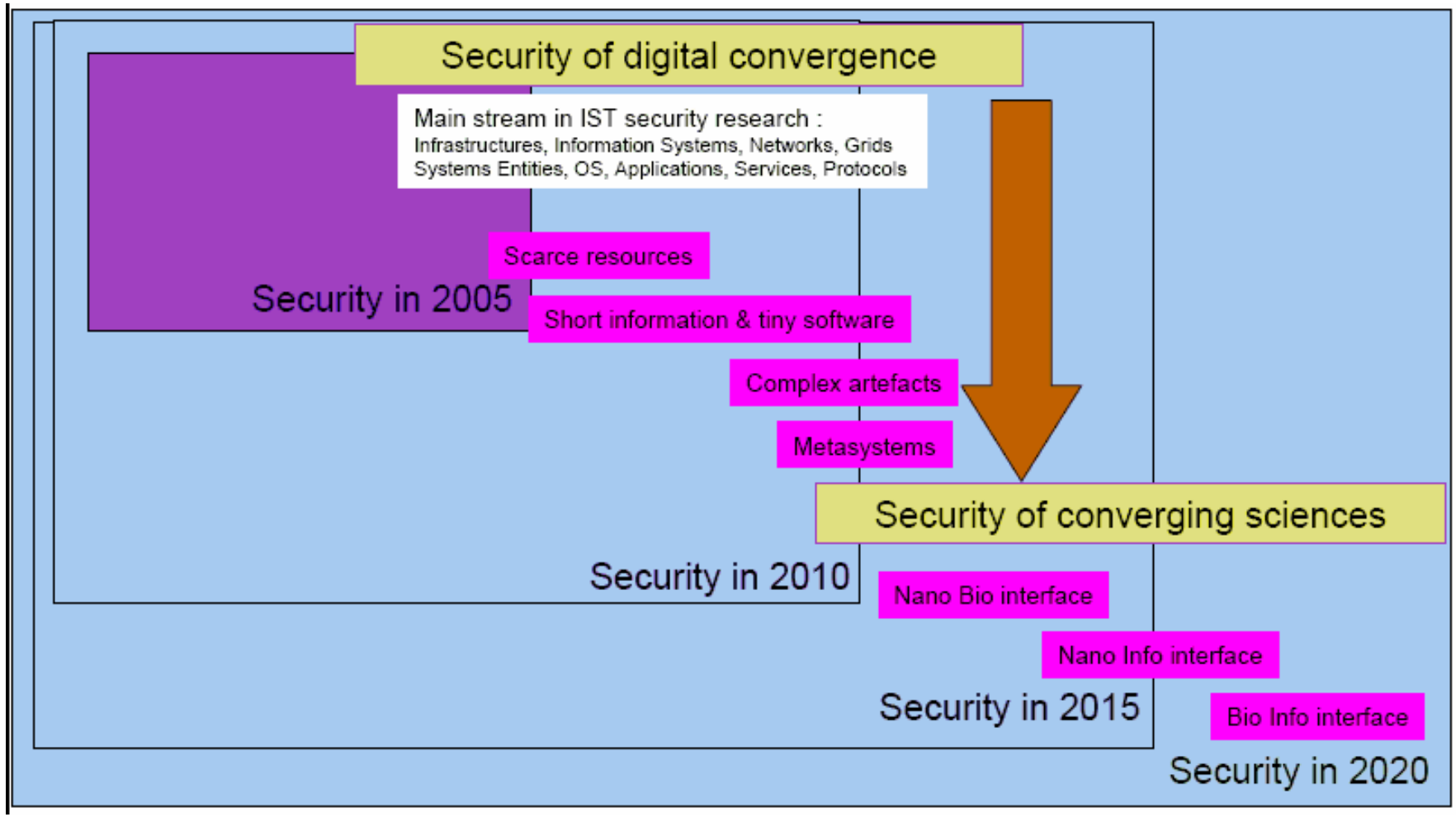
CIP Multi-Dimensional Impact Vectors



SRMI Research Areas VI

- **RM Models for New Technologies**
  - Examples:
    - SOA, Grid, Tiny physical Objects (RFID, Smart dust, etc…)
    - Typical RM aspects for each technology
    - Dynamic automatic Mapping of methods and controls

RM Models for New Technologies
(Michel Riguidel, Enst Paris, ESFORS Workshop, 2006)



SRMI Research Areas VII

- **Safeguard Selection**
  - Example:
    - Correlating threats and vulnerabilities to safeguards, Effective safeguard selection
- **Cost**
  - Examples:
    - Cost benefit analysis
    - Economics of cost, identifying costs and integrating it in RM
    - "What if" scenarios and simulations (cost related)
    - ROSI, cost of not doing

- **Business**
  - Examples:
    - Business Impact Analysis
    - Identification of business needs: protection level, assets, processes

SRMI Research Areas VIII

- **Compliance**
  - Example:
    - Compliance risk management,
      Compliance consolidation and cost-effectiveness
- **SME's, Citizens**
  - Example:
    - Cost-effective RM solutions for SME's
- **Sectors Templates**
  - Example:
    - CIIP: Health, Financial, Government, Energy, etc…

Thank You!