Adaptive Risk Management for Networked Critical Infrastructure

Mihaela Ulieru
Canada Research Chair in
Adaptive Information Infrastructures for the e-Society

OVERVIEW

- 1. Preambule: Next Generation Cyberinfrastructure
- 2. Networked embedded control systems
- 3. eNetworks as backbone for critical infrastructure
- 4. Network self-organization to improve resilience
- 5. Adaptive risk management
- 6. Applications: Beyond e-Magination!

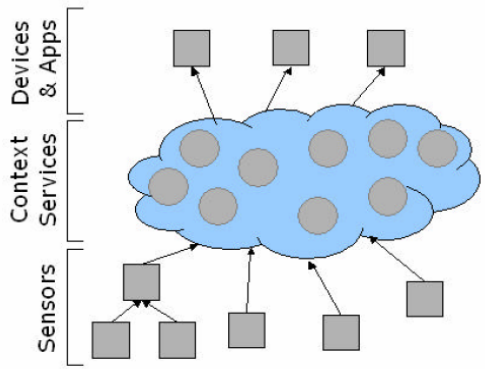
Next genaration Cyberinfrastructure

- Vast intelligence network capable of learning to connect distributed sensory input to distributed actions in the real world, **integrated so as to maximize the performance of the global system**

Networked Embedded Control Systems

eNetworks

Figure 1. An infrastructure for context-awareness can provide a middleware laye between sensors on one side and devices and applications on the other. Th middleware layer presents a uniform layer of abstraction, making it easie update individual pieces independently of each other.



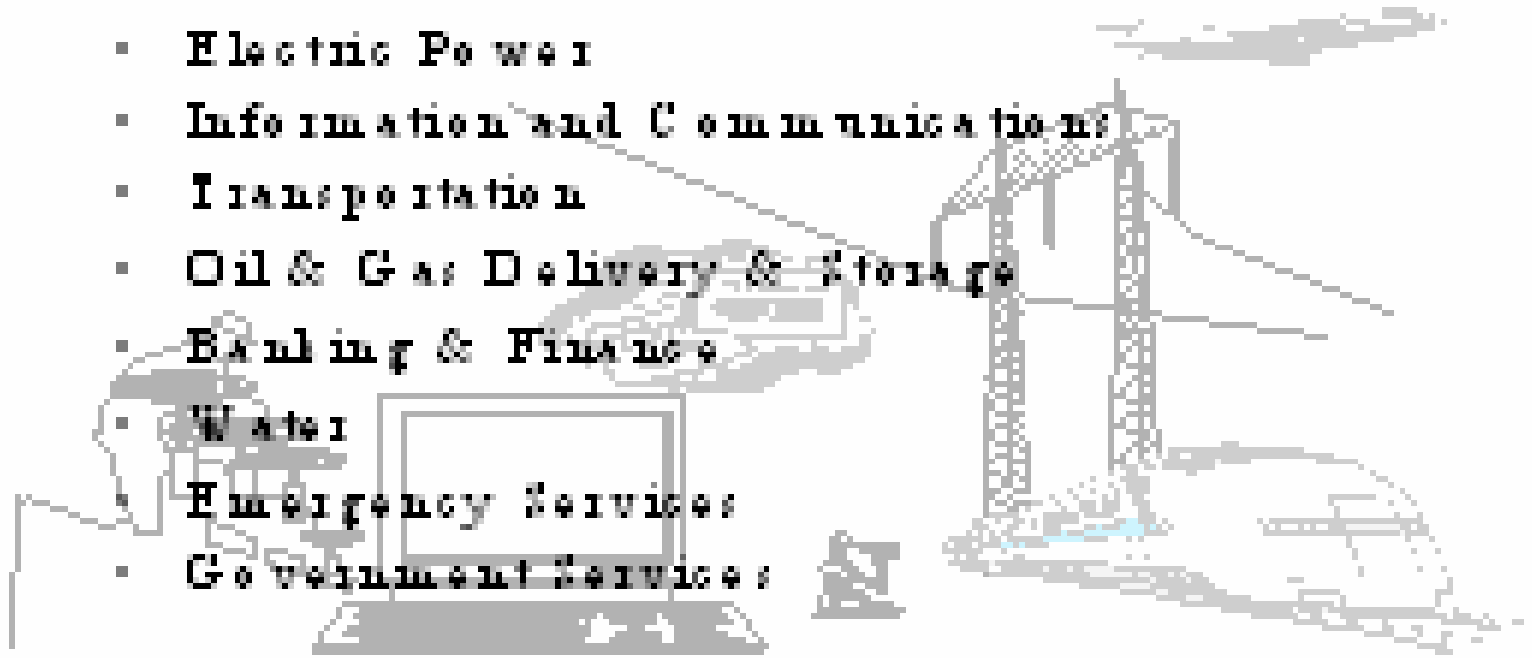
Cyber-Physical Systems: Systems enabled by **e-Networks**

- **Integration** and **networking** of systems across all scales to create intelligent environments of self-organizing artifacts applicable in several areas, from e-Manufacturing, e-Health, e-Commerce…
- **Cyberinfrastructure** - artificial nervous system for the entire economy, providing **optimal** integrated management of large critical infrastructures ranging from electric power and water to environment and finances with seamless market interface

Networked Critical Infrastructure

Critical Infrastructures

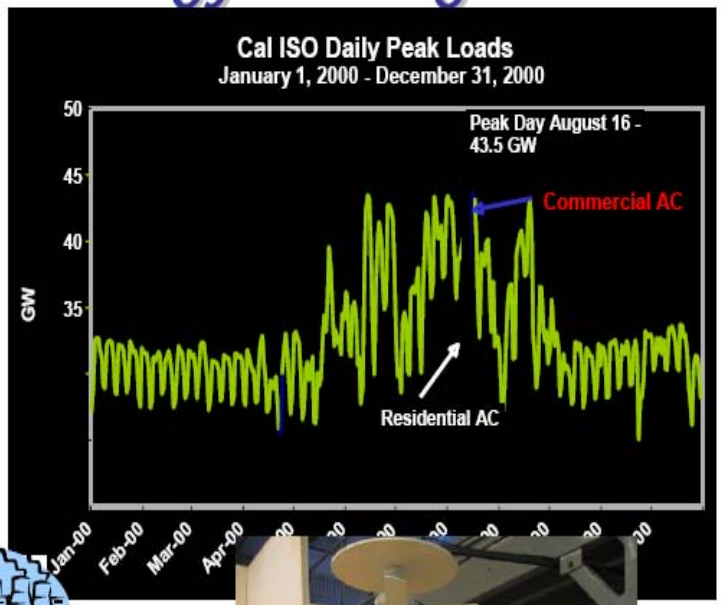
- Electric Power
- Information and Communications
- Transportation
- Oil & Gas Delivery & Storage
- Banking & Finance
- Water
- Emergency Services
- Government Services

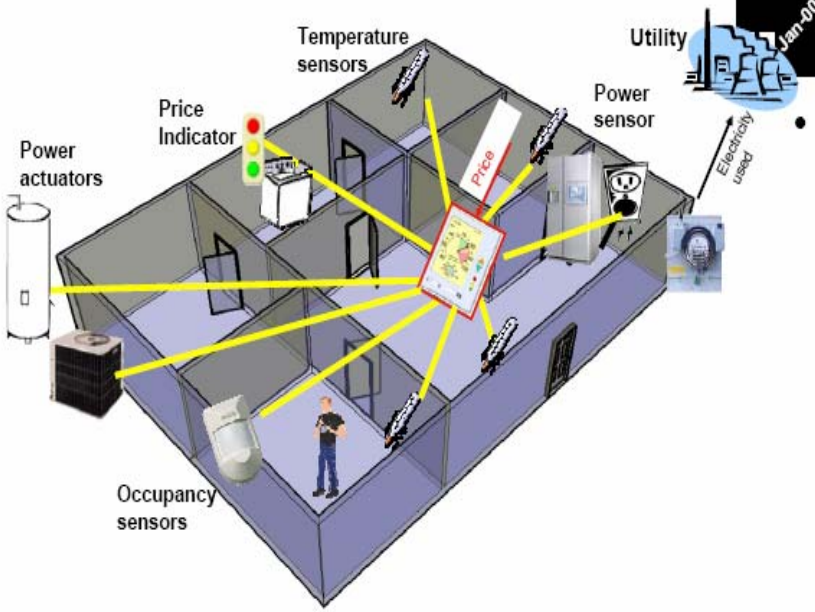


Demand Response and Energy Management

Make energy prices dependent upon time-of-use

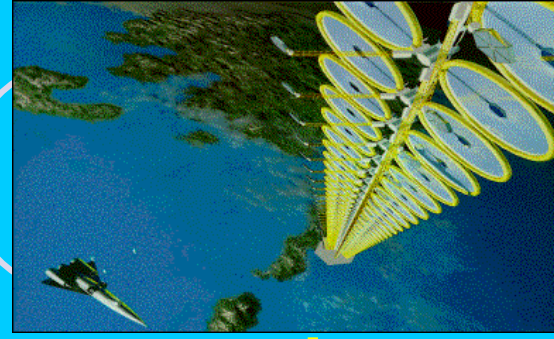
- Advanced thermostats operate on required level of comfort, energy cost, weather forecast and distributed measurements to offload peak times
- Appliances energy and cost aware





In collaboration with CEC

ResearchQuestion

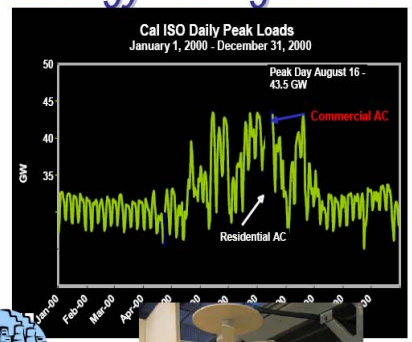


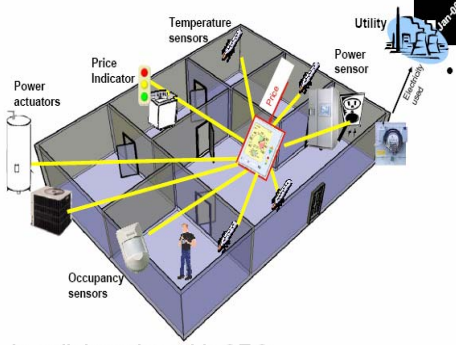
- How can we control complex systems and processes (such as energy production, distribution and consumption) using the eNetwork?

Demand Response and Energy Management

Make energy prices dependent upon time-of-use

- Advanced thermostats operate on required level of comfort, energy cost, weather forecast and distributed measurements to offload peak times
- Appliances energy and cost aware

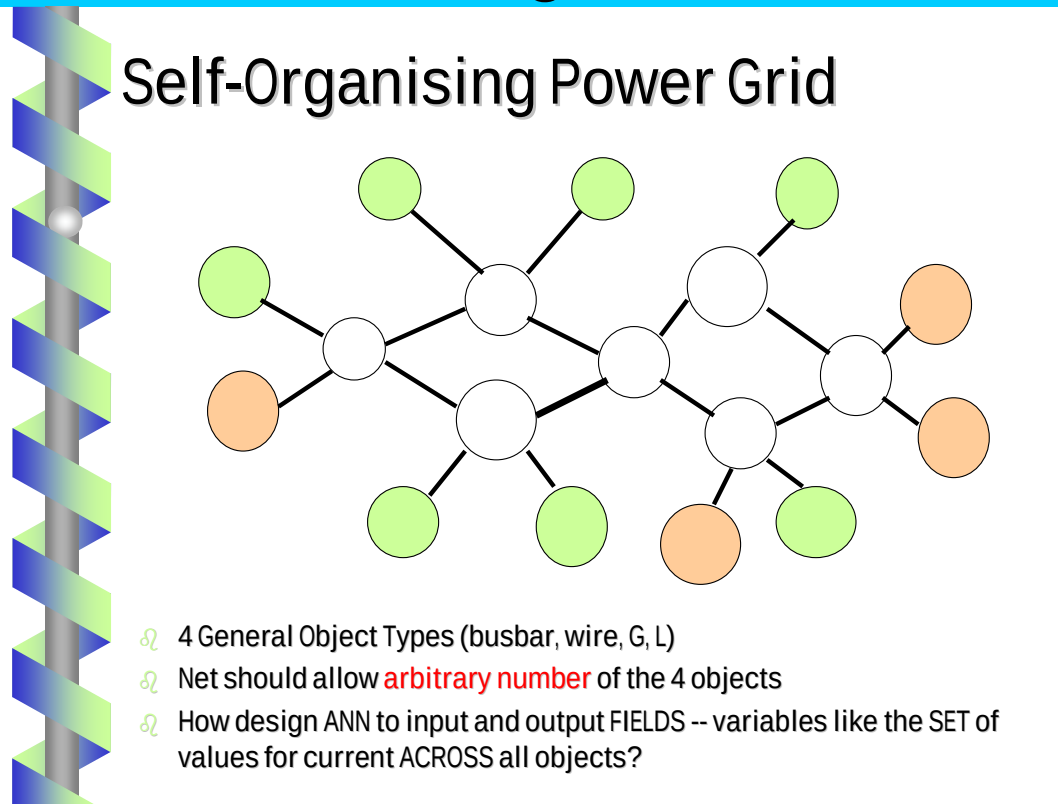




In collaboration with CEC

- Requires development of more advanced general-purpose algorithms for tasks such as **adaptive, intelligent sensing, pattern recognition and management of complex systems** for the overall architecture of a new Cyberinfrastructure to manage complex physical infrastructures such as electric power, communications, intelligent environments, etc

eNetework



eNetworks - backbone for CRITICAL INFRASTRUCTURE

- A vast new flow of information from distributed sensors all over the world can be communicated and merged with other information, and combined with high-performance computing and intelligence, in order to provide more useful guidance and imagery to humans, and to control vast new arrays of actuators which manage physical flows from fire detection/prevention to factory equipment.

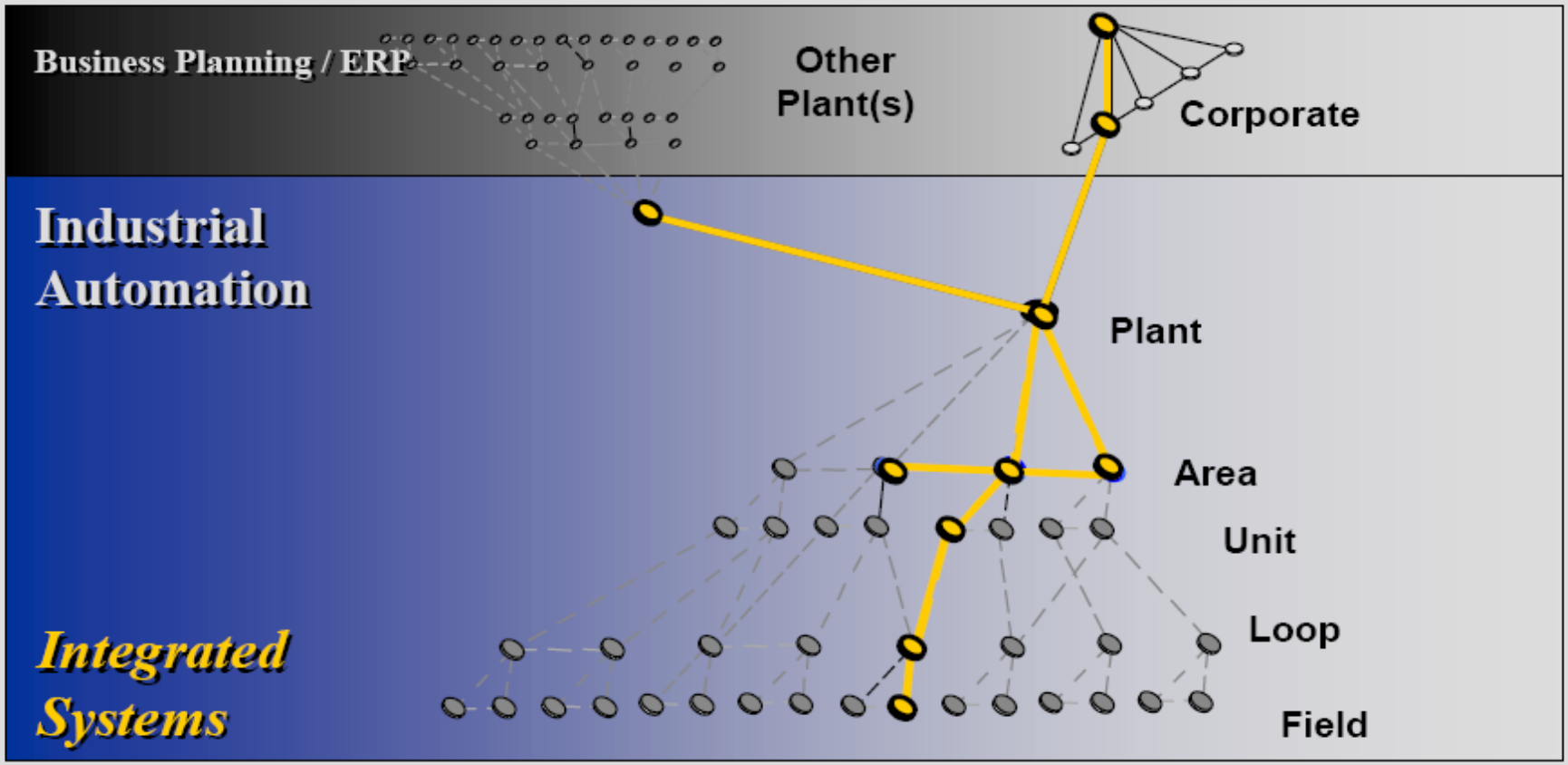
Network Optimization Theory (old)

- Capacitated network flow model (removing a fixed number of nodes)
- Minimum cost flow model (interdiction reduces capacity and increases cost flow along an arc)
- Shortest path model – optimal set of arcs to be monitored so as to cost-effectively detect an evader

A New Science of Networks

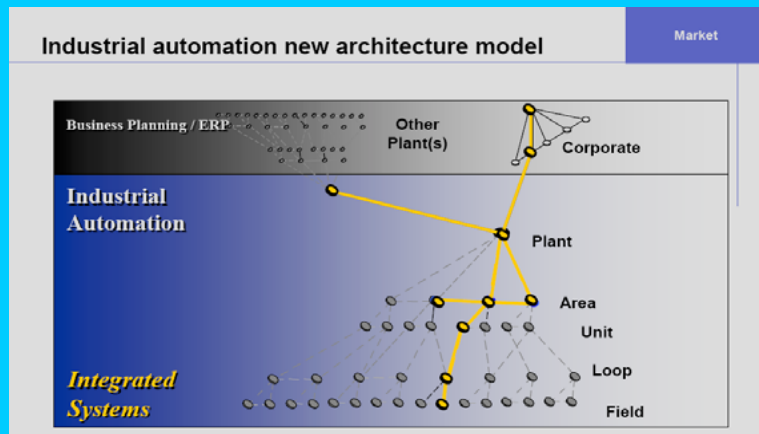
Market

Industrial automation new architecture model

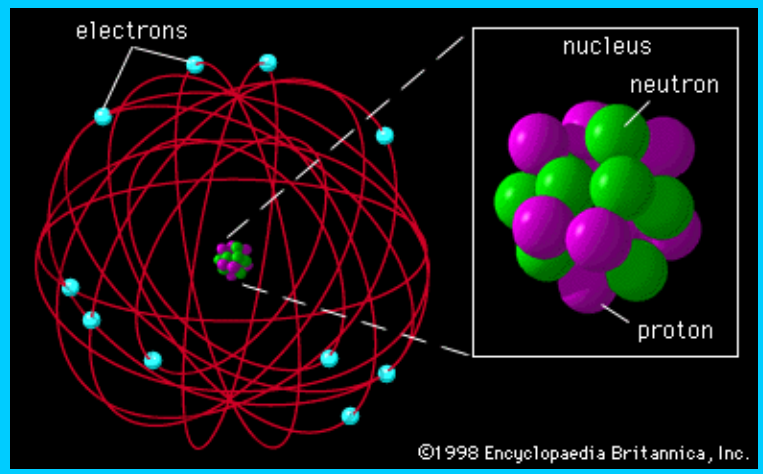


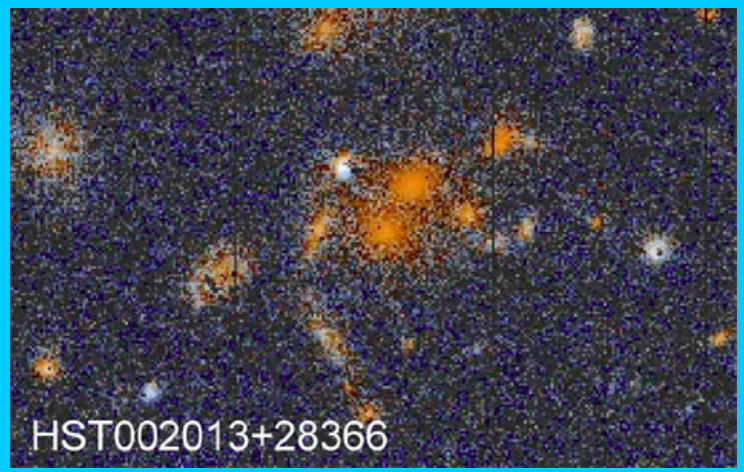
How do complex networks self-organize? (Albert-Laszlo Barabasi)

- UNIVERSAL LAWS:
- - Power Law Distribution (**a few hubs with lots of links, very many nodes with few links**) governs the transition from disorder to order
- - **Preferential attachment** to the ‘fittest’ nodes
- The ‘order’ exhibits an intrinsic holonic structure



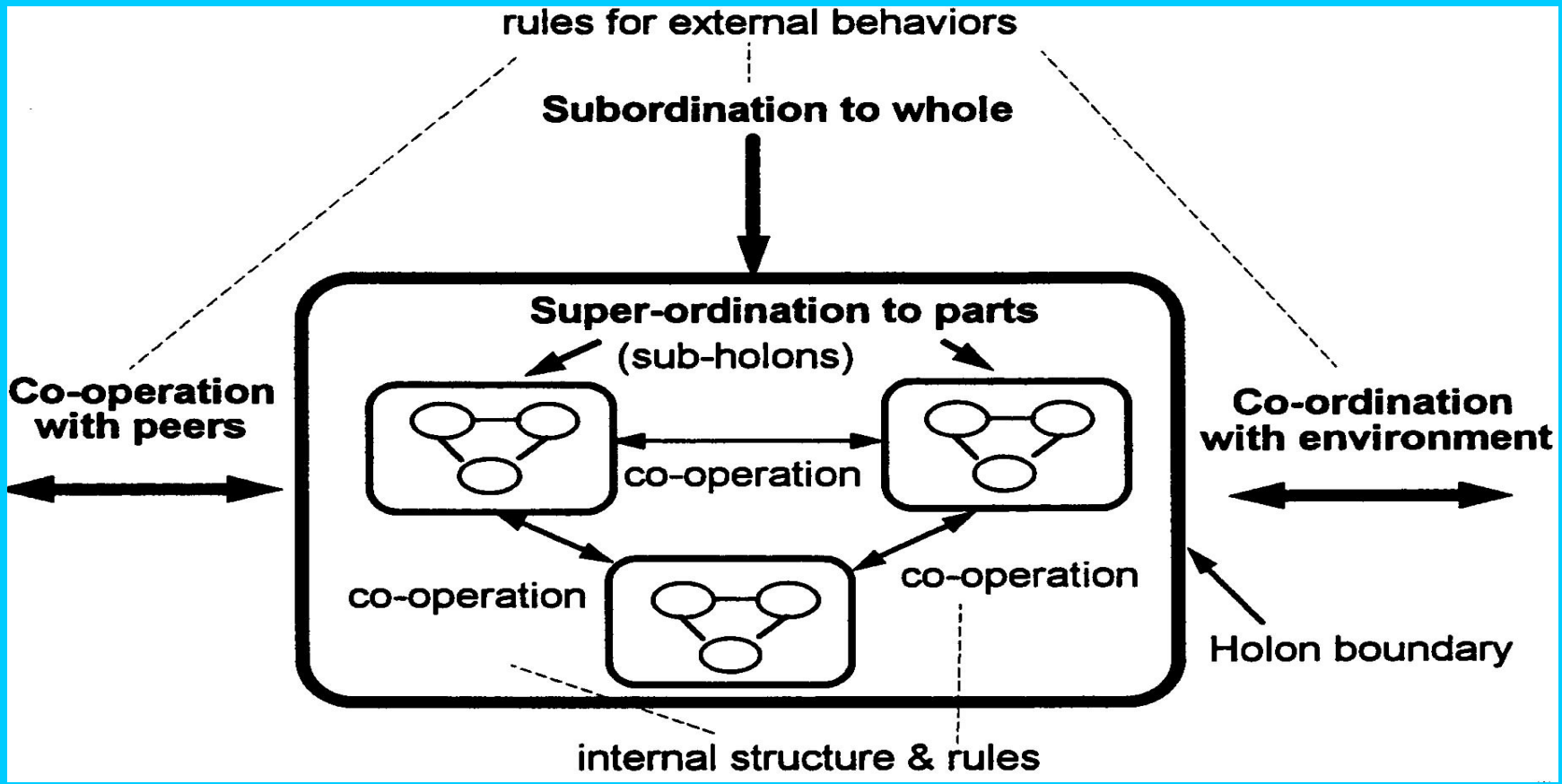
HOW THE UNIVERSE WORKS





HOLARCHY OF HOLONS:

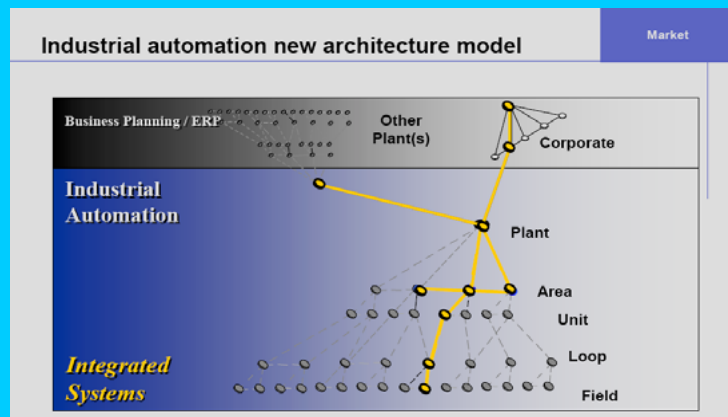
MULTIRESOLUTION



Self-regulatory Networks

- Autocataliticity in dynamic systems – **order emerges from disorder according to power law distributions**
- (Sub)systems (cells, nodes in a network) cluster around the ‘fittest’ systems/nodes
- This governs also the behavior of growing dynamic networks such as

Cyberspace



Generic Research Question

- How to enable visualization, analysis and adaptive reconfiguration of complex systems due to emergent behavior or environmental changes, so as to develop reliable, agile, self-aware networked infrastructures capable to anticipate and annihilate eventual threats before they occur, for domain specific applications.

APPROACH – converging streams

a. Network self-organization to preserve/ increase resilience

- Multi-agent, self-healing, and reconfiguration methodologies integrated into a framework in which services are able to organize themselves in a resilient system without requiring any manual intervention.
- Such resilient network services will be able to reconfigure the network to minimize system vulnerability by performing short-term adaptations to the environment as well as long-term evolution of new self-* functionalities.

WWRF's vision of Ubiquitous Computing

- Personal networks
- Immediate environment
- Instant partners
- Radio access
- Interconnectivity
- Cyberworld

Self-Organizing Artifacts

- A setup where different devices, with different fabrications and functionalities, and moving in and out of different configurations, can communicate and integrate information to produce novel functionalities that the devices by themselves could not achieve.

Self-organizing Technological Artefacts

- They are able to communicate and perform **desirable tasks** with minimal human intervention

SELF-ORGANIZING APPLIANCES

Emerging Purpose

- The purpose should not be explicitly designed, programmed, or controlled.
- The components should interact freely with each other and with the environment, mutually adapting to reach an intrinsically “preferable” or “fit” configuration (attractor), thus defining an ***emergent purpose*** for the system

Emergence of Life

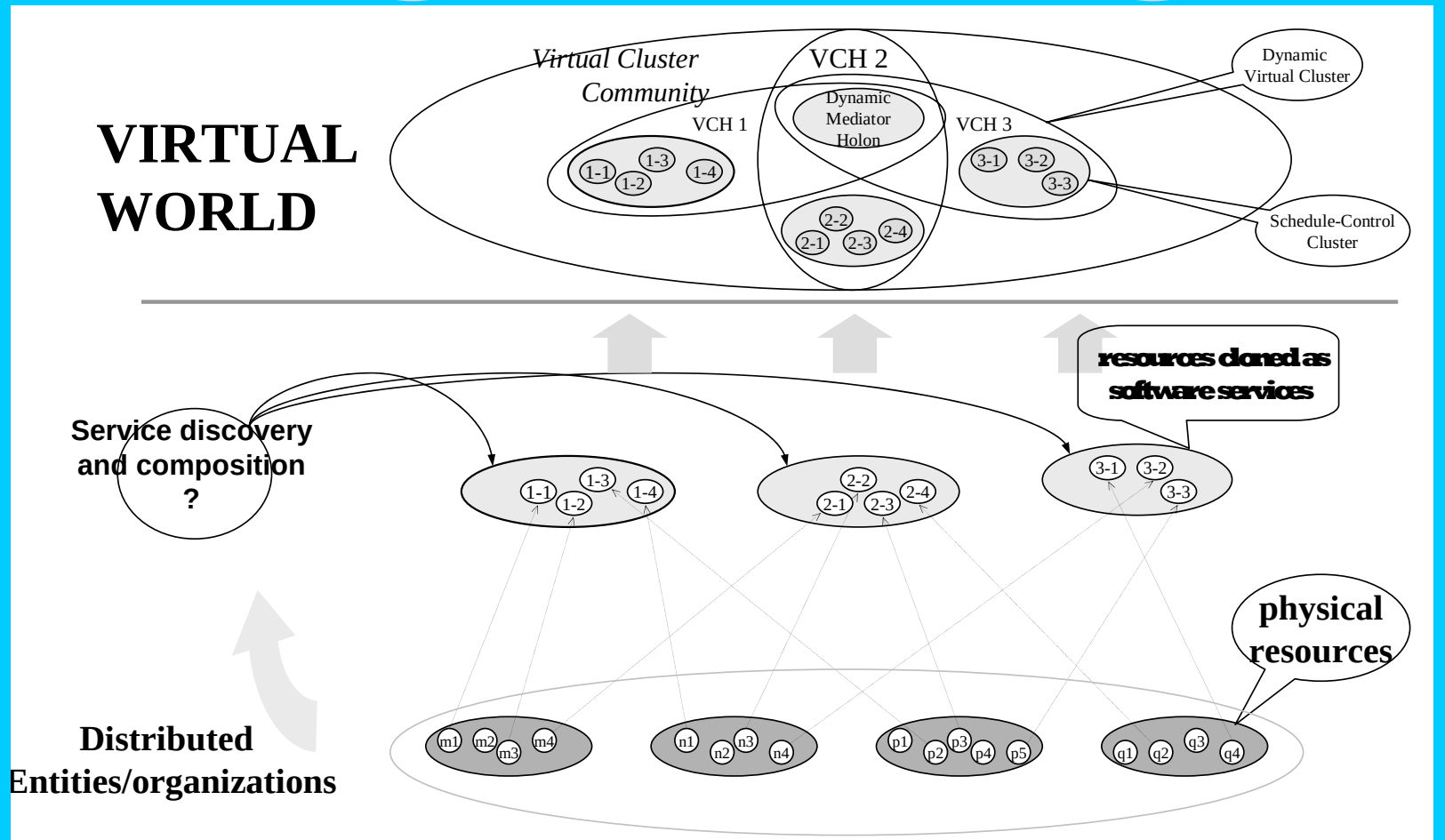
- Stuart Kauffman (cellular biology) [At Home in the Universe] – ‘Life ***emerged*** through collective autocatalitic processes fueled by self-organization and natural selection’.
- The Phenomenon of Emergence involves:
- **Self-organization** of the dynamical systems to enable evolution
- **Selection** - through interaction with other systems

Modeling Emergence in Cyberspace

MULTI-AGENT SYSTEMS

- **Self-Organization** (ENTROPY)
- **Evolution (selection pressure)**
- **Adaptive Cyberspace**

PARALLEL UNIVERSE OF INFORMATION



What we learned from Nature: Stigmergy

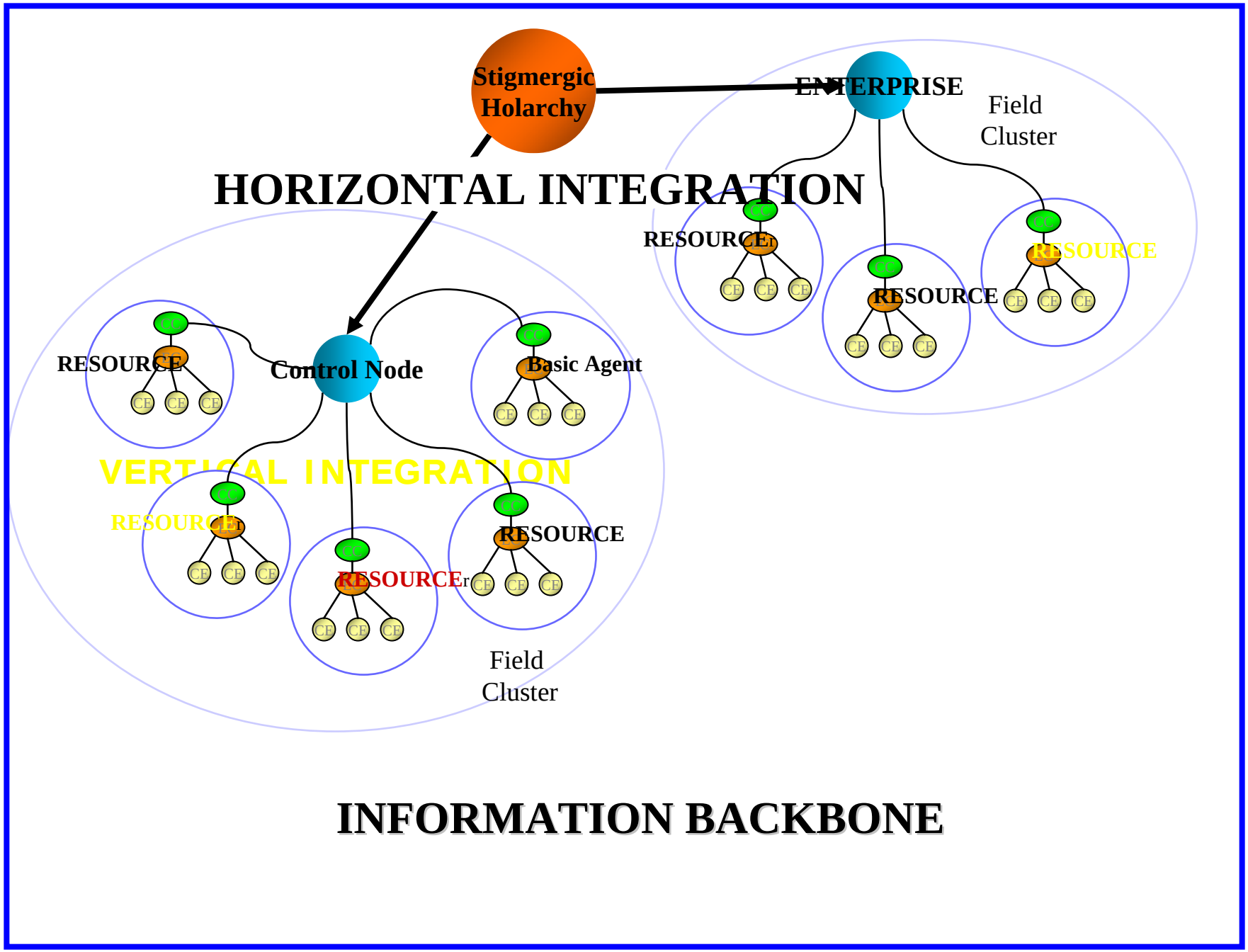
- Stigmergy appears to be an important mechanism that assists a system to structure itself through the collective behaviour of individuals within the system's environment.
- An individual could move through the environment, gathering or emitting information, but it can also interact with the environment. Both actions could be considered stigmergy.

Stigmergic Collaboration

- “from the Greek words stigma ‘sign’ and ergon ‘action,’ and captures the notion that an agent’s actions leave signs in the environment, signs that it and other agents sense and that determine their subsequent actions.” [Bonabeau 1999]
- **We use stigmergic collaboration to tune the degree of holonic self-organization**

Holonic Stigmergy (Stefan Grobbelaar)

- “We introduce the concept of holonic stigmergy as a mechanism for tuning the emergence of optimal organizational structures in networks and illustrate how it works on a power network energy saving example”.


Stigmergic Holarchy
ENTERPRISE
Field Cluster
HORIZONTAL INTEGRATION
RESOURCE
RESOURCE
RESOURCE
RESOURCE
Control Node
Basic Agent
VERTICAL INTEGRATION
RESOURCE
RESOURCE
RESOURCE
Field Cluster
INFORMATION BACKBONE

Holarchy

Holon – Part whole, a nodal point in a hierarchy describing the dependency between self-complete entities and other dependent parts.

Holarchy – Hierarchy of holons cooperate to achieve a goal. It defines rules for cooperation and limits the holons' autonomy.

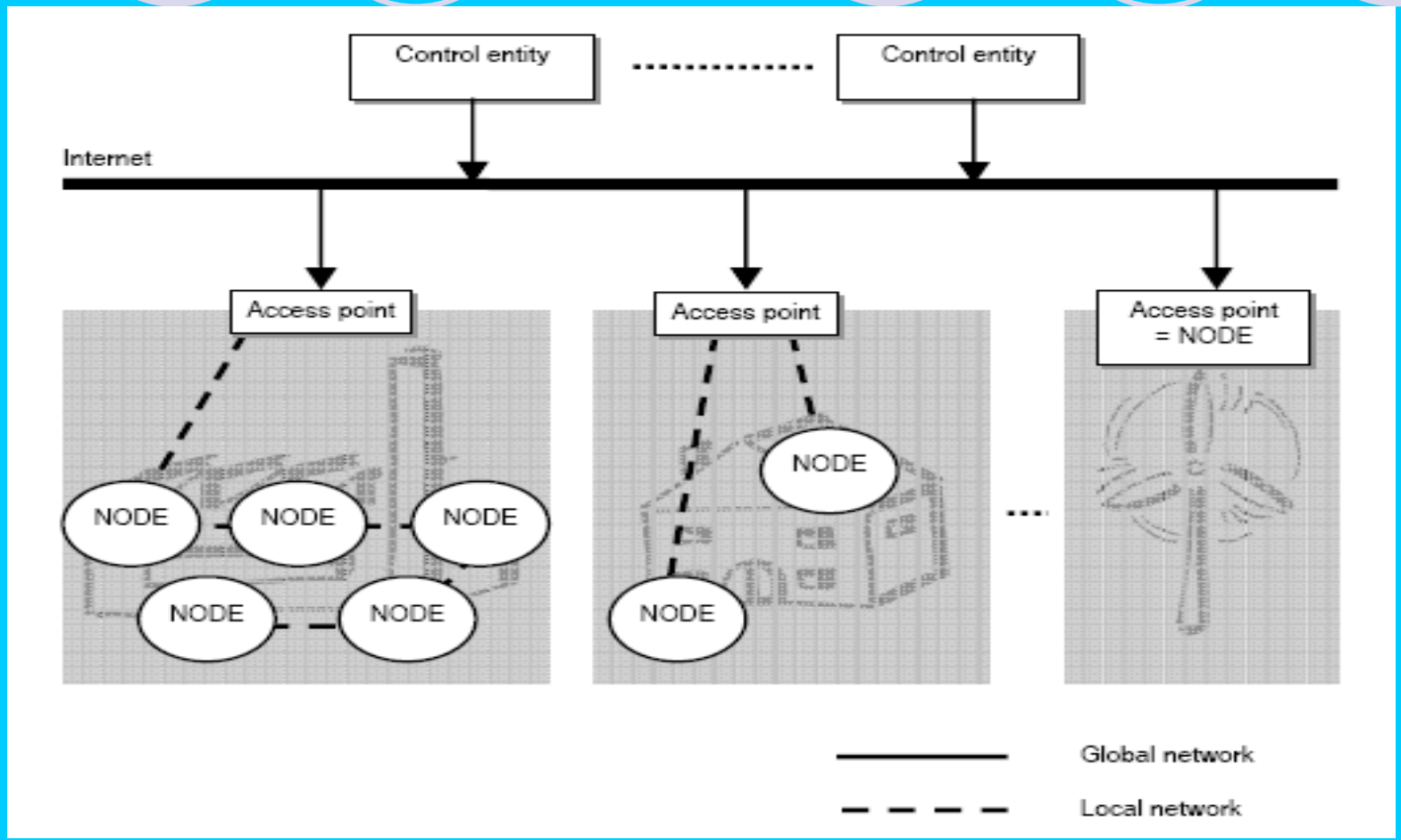
Groupings of parts which share a similar context.

We define an imposed goal and it's associated high priority as a goal which *limits* a holon's autonomy

Balancing Reactive and Goal-Oriented Behavior

- We want our holons to be reactive, responding to changing conditions in an appropriate (timely) fashion
- We want our holons to systematically work towards long-term goals
- These two considerations can be at odds with one another
- **Designing an agent that can balance the two remains an open research problem**

Application Scenario



Stigmergy

Method of communication whereby individual parts modify their environment.

Parts not necessarily dependent on each other

A grouping may emerge, knowingly or unknowingly

Similar intended goals

We define an intended goal and it's associated high priority as a goal which *increases* a holon's autonomy

Context

Information used to characterize the state of a holon, specifically its goals and priorities and how these relate to the goals and priorities of others

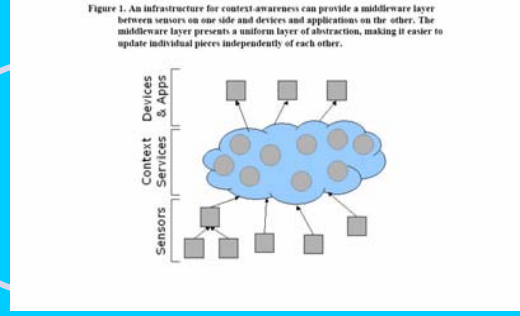
Holonic stigmergy describes a system of holons which belong to a holarchy and have stigmergic properties

- System created around user needs
- Needs translate to context
- Context is user goals and priorities

Definitions

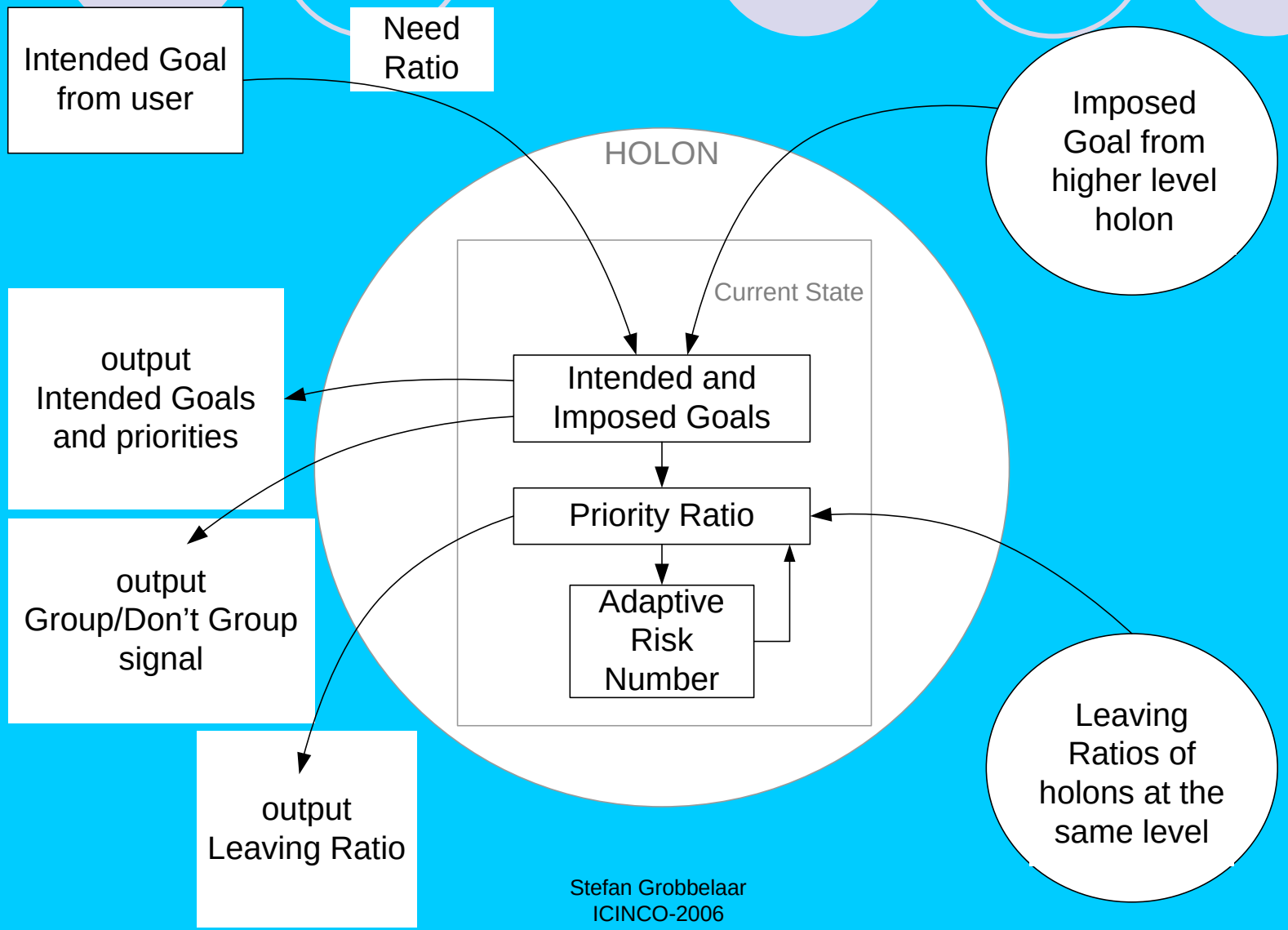
- **Need Ratio:** need for grouping (never 0, otherwise network collapses) / need to follow intended goal
- **Priority Ratio:** The ratio(s) of Intended goal priority(s)/Imposed goal priority(s)
- **Leaving Ratio:** The priority ratio of a holon at a time of leaving the holarchy.
- **Adaptive Risk Number**: A risk of leaving percentage, comparing the priority ratio of the holon to the leaving ratios of holons in the surrounding area.

Operational Integration



Observations (Inputs)	Signals (Outputs)
- Intended goals from user	- Intended goals (as information to surrounding holons and imposed goals to holons at a lower level)
- Intended goals of surrounding holons	- Group/don't group signal
- Imposed goals of higher level holons	- Leaving ratios and priority ratios of the holon
- Leaving ratios and priority ratios of surrounding holons	

Context Model



TUNING THE SYSTEM: Intended vs. Imposed Goals - Balancing holonics and stigmergy

To adjust the model towards stigmergy or holarchy – adjust need ratio to give priority to either intended or imposed goals

More power (greater influence) to the intended goal of a holon at a level will make lower holons more hierarchic.

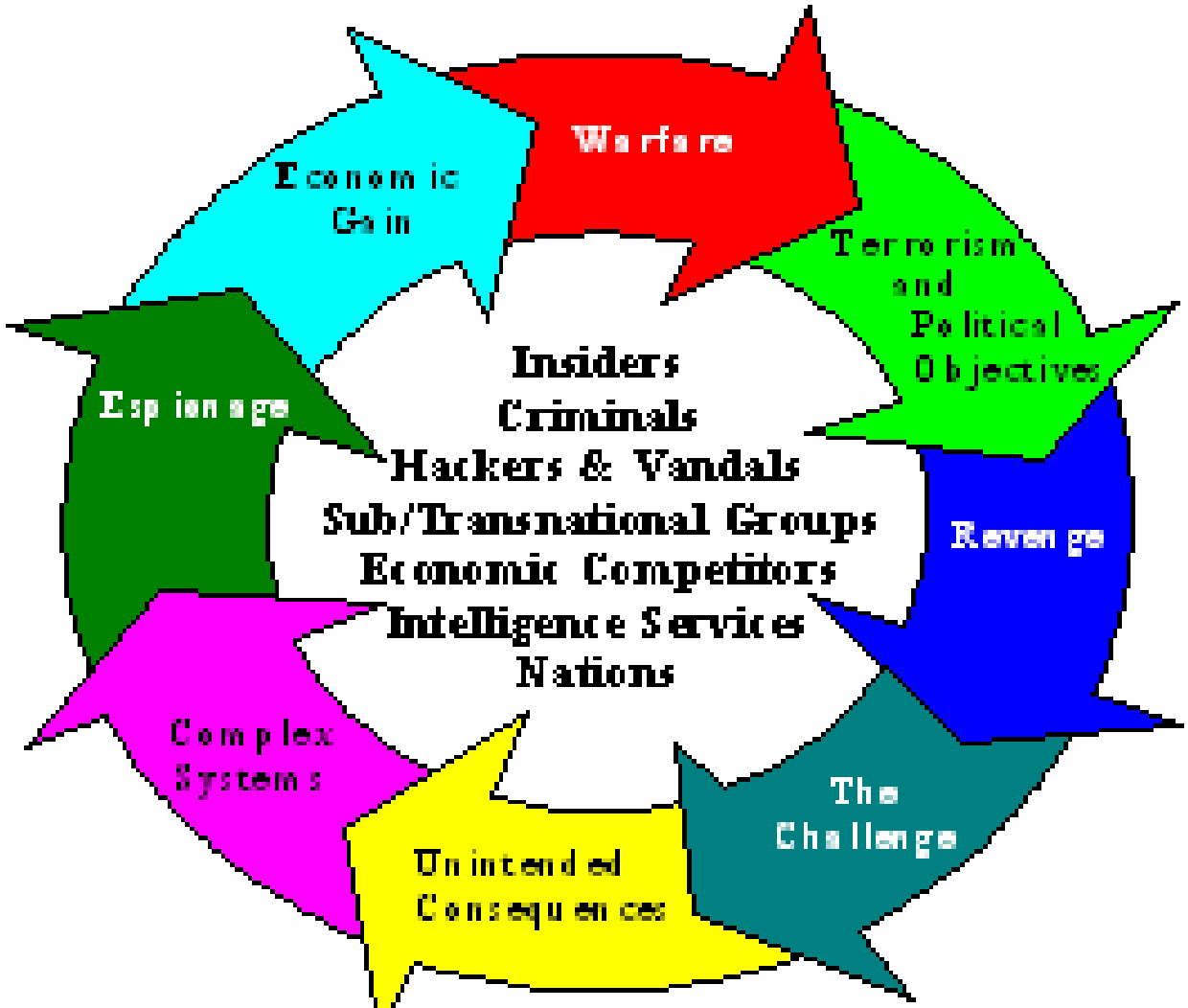
Holons at a specific level and above will become more stigmergent

By adjusting the influence (power) to the intended goals of holons at a level, we are able to vertically shift the holonic/stigmergent balance.

b. The security challenge

- eNetworks - the monitoring and control engine for the system status and means to reduce vulnerabilities of all other critical infrastructures
- Generic methodologies of design for resilience of critical infrastructures in which the eNetwork middleware will continuously self-organize to adapt the resilience of the infrastructure accordingly as vulnerabilities and threats emerge.

Threat Sources



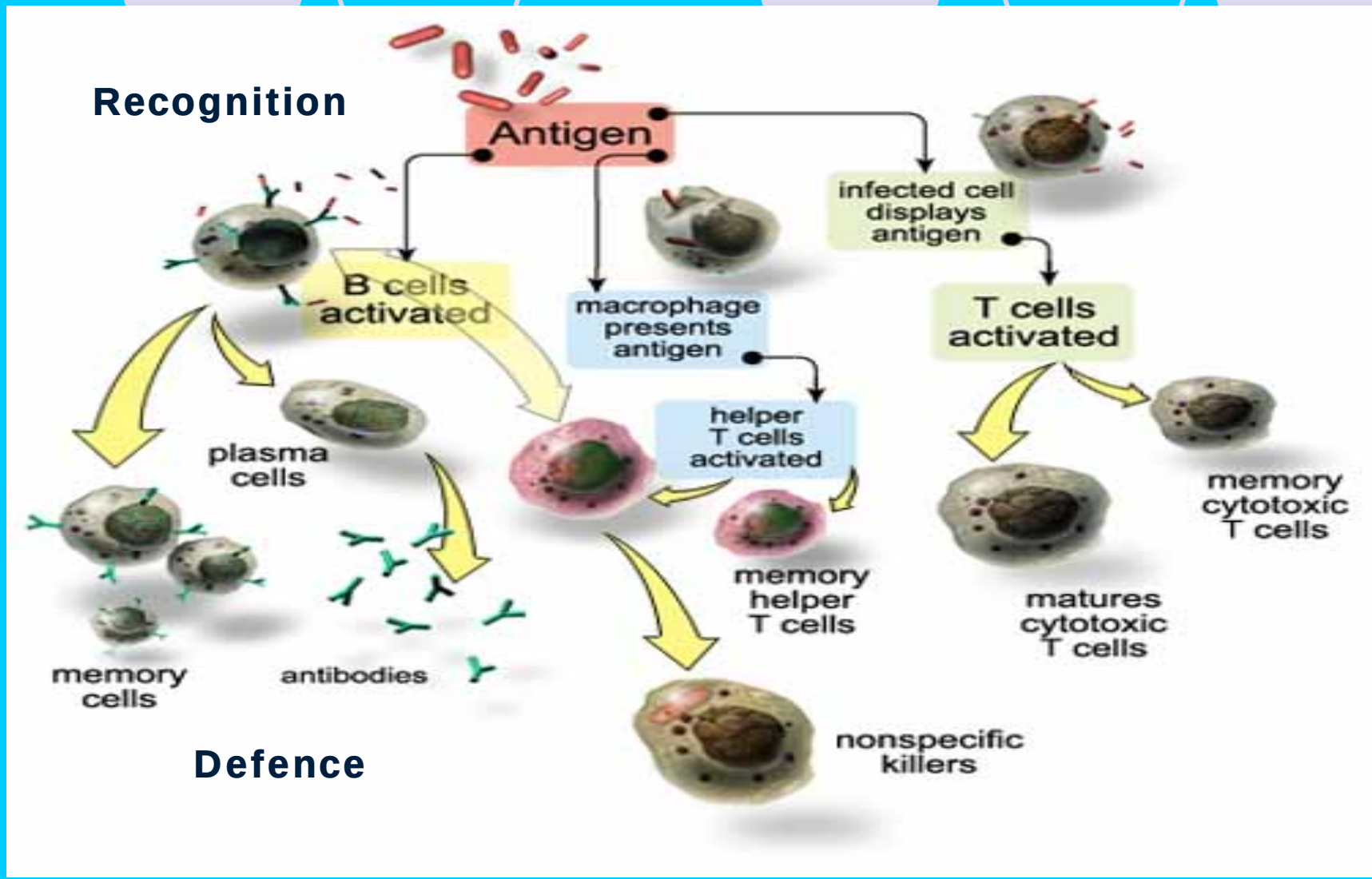
Network Safeguarding

- Determine the frail links and nodes with respect to a given type of threat and add resources (e.g. sensors) to detect and thwart threats
- ? Where do we place the sensors (**At critical hubs**)
- Security-aware design of supply networks – capture the effect of safeguarding constraint on parameters and network cost

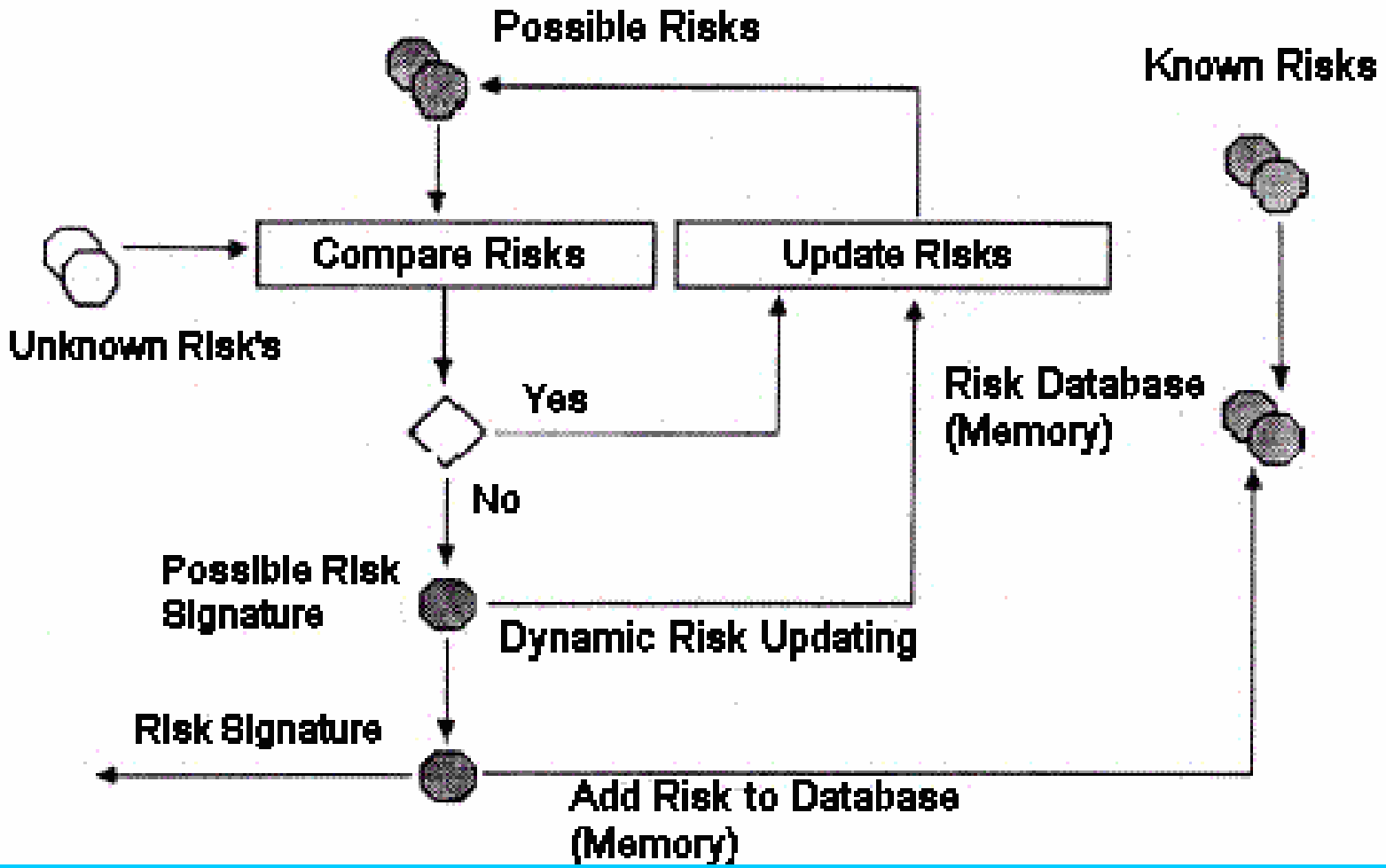
Risk Mitigation via eNetworks

- CFI – funded Lab: Develop strategies for proactive network self-awareness by extracting risk metrics from multidimensional, multifaceted risk models continuously adapted through monitoring and vulnerability assessment as well as situational awareness strategies.
- **Inject ‘anticipation’ into the network**

Human Immune Response System



Artificial Immune Response System (Cyberorganism)



ARM Lab

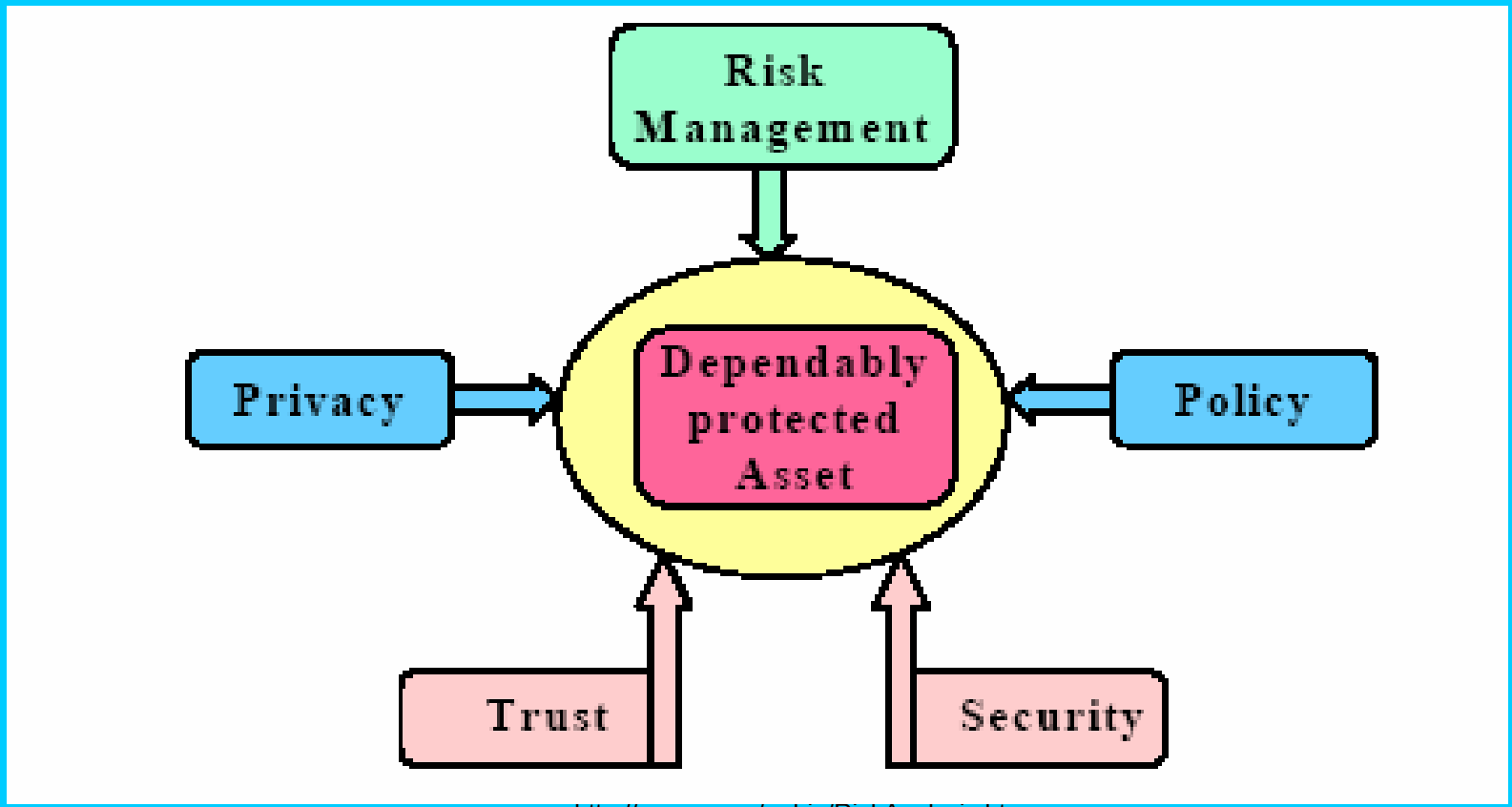
- System vulnerability concepts, indices and algorithms that incorporate complex interactive dynamics integrated in a methodology to develop networked intelligent surveillance systems for security of critical infrastructures which will fuel innovative ways to use eNetworks as infrastructure for public notification systems, evacuation and rescue operation as well as terrorist attack tracking and pandemic mitigation approaches, while identifying strategies and tools to support emergency managers during critical events;
- Intelligent adaptive methods allowing control and protective devices to adapt to changing system conditions;
- System restoration strategies based on reconfiguration needs.

Risk Management Approach to Security

- **Risk management is at the core of security and trust**
- **Risk analysis** - the process of evaluating system vulnerabilities and the threats facing it
- Risk analysis involves ability to **trust** our judgement as well as the reliability and **security** or predictability of the environment in which the analysis is performed.
- We must also be able to **trust** that our **privacy** is not at risk.

CIP Framework

http://www2.nr.no/coras/



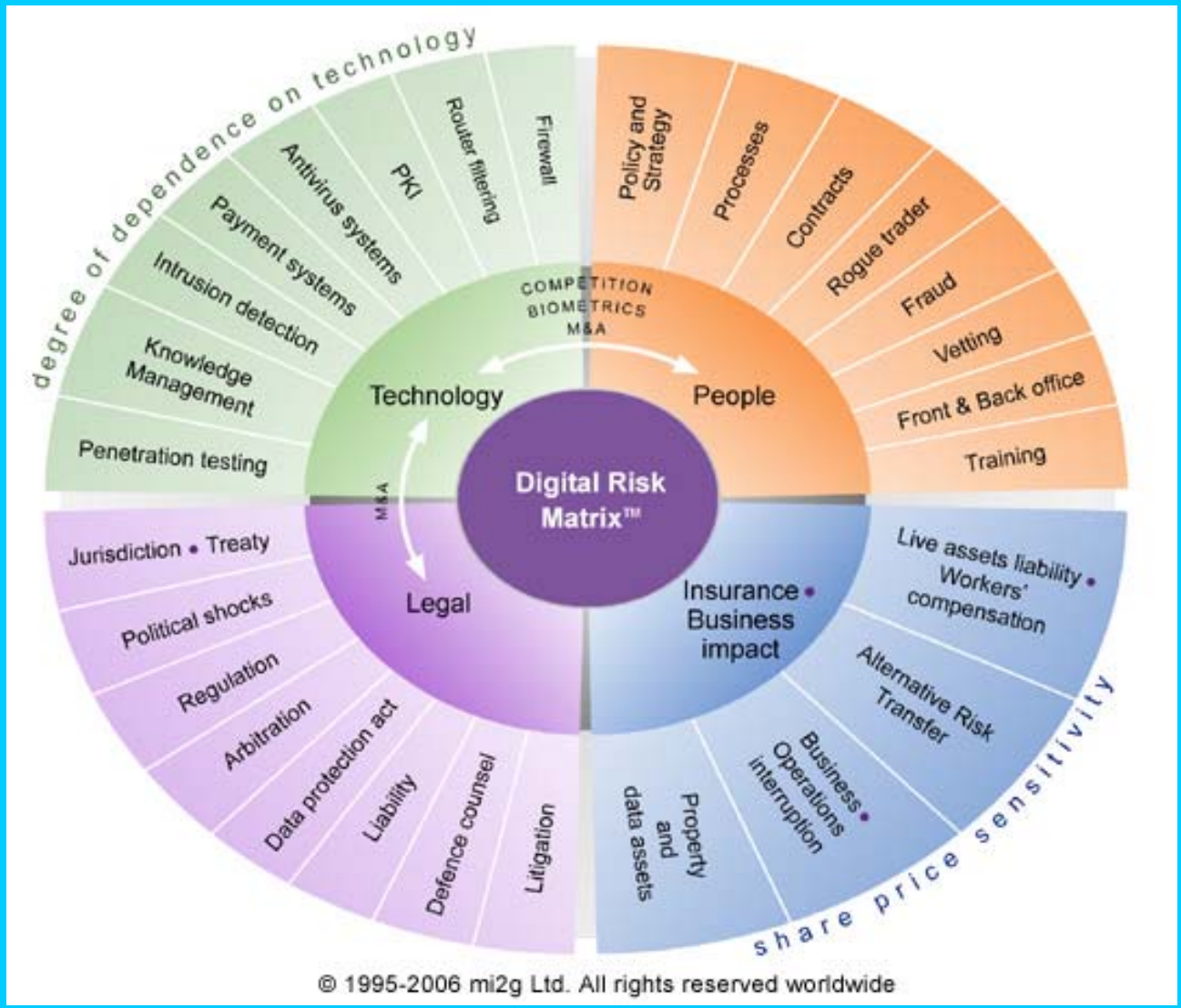
http://www.nr.no/~abie/RiskAnalysis.htm

Changing Risk Profile

- Business Risk
  =
  Threat +
  Vulnerability +
  Consequences
- Change with IT dependence:
  - Emerging sources of threat
  - Emerging and unforeseen vulnerabilities
  - Consequences: Incidental disruptions/outages becoming substantive management issues

- Risk analysis aids in developing a security strategy and provides the basis for establishing a cost-effective security program that minimizes the effects of risk.

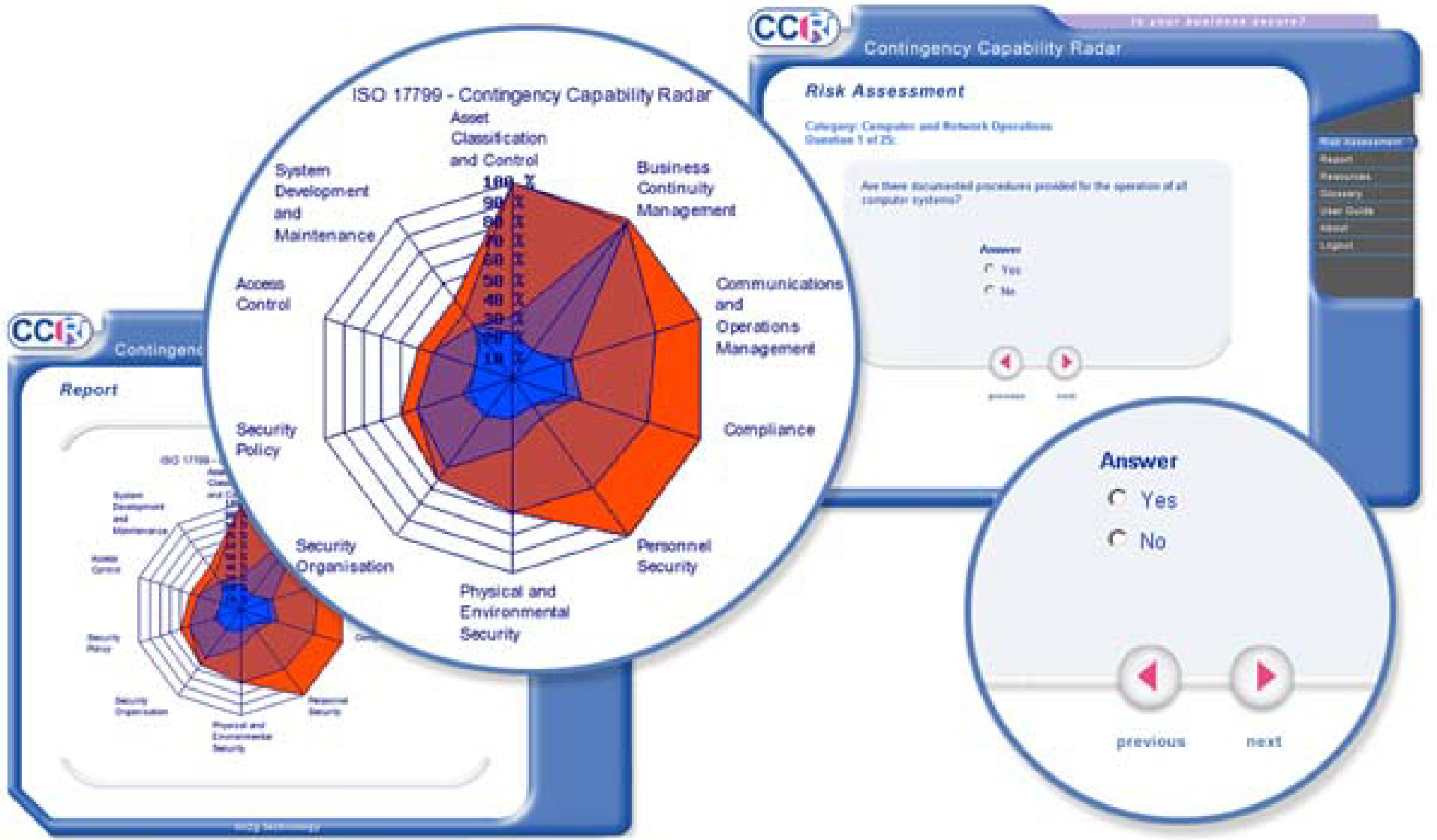
Integrated Approach to Security



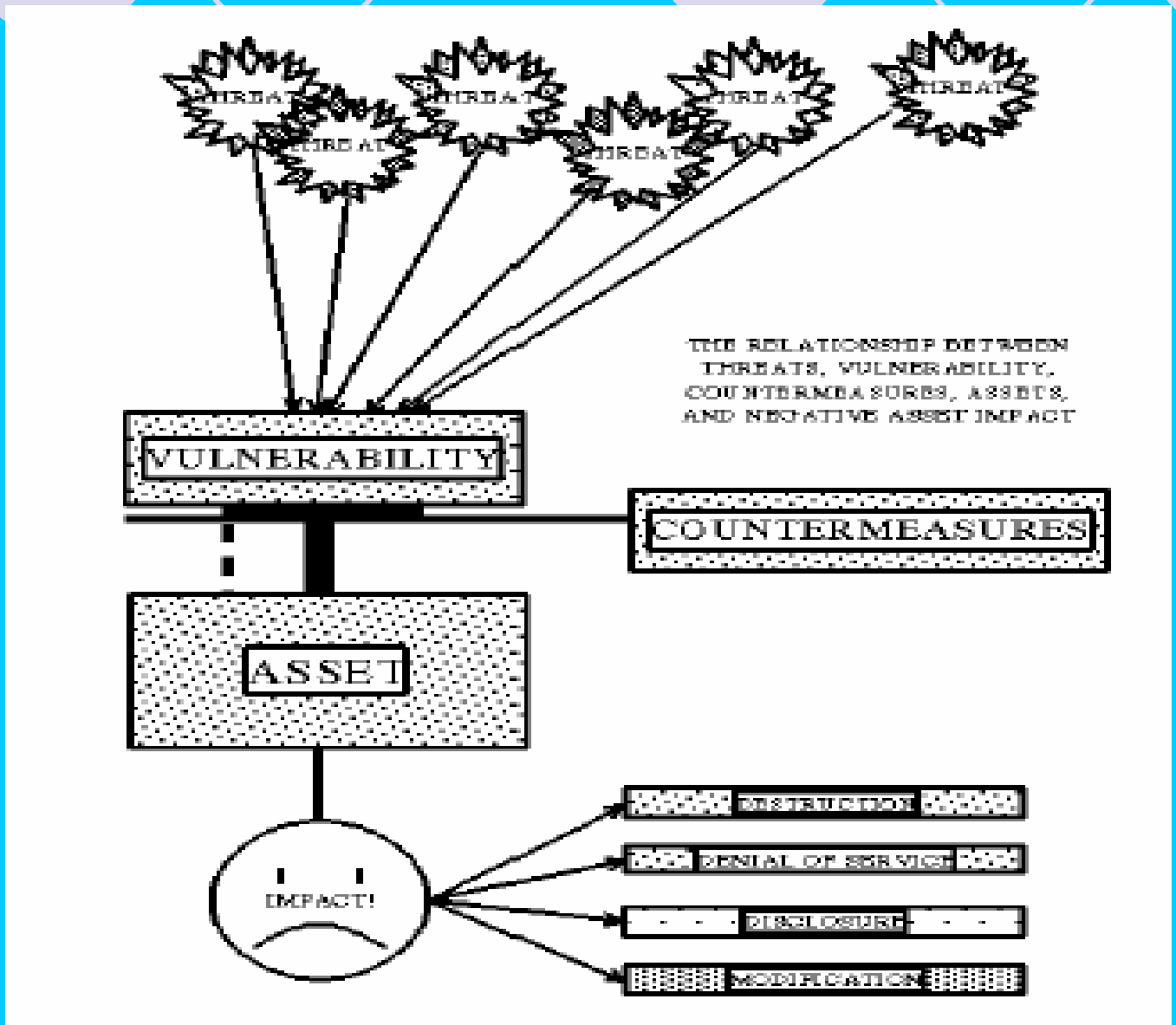
Security Risk Analysis

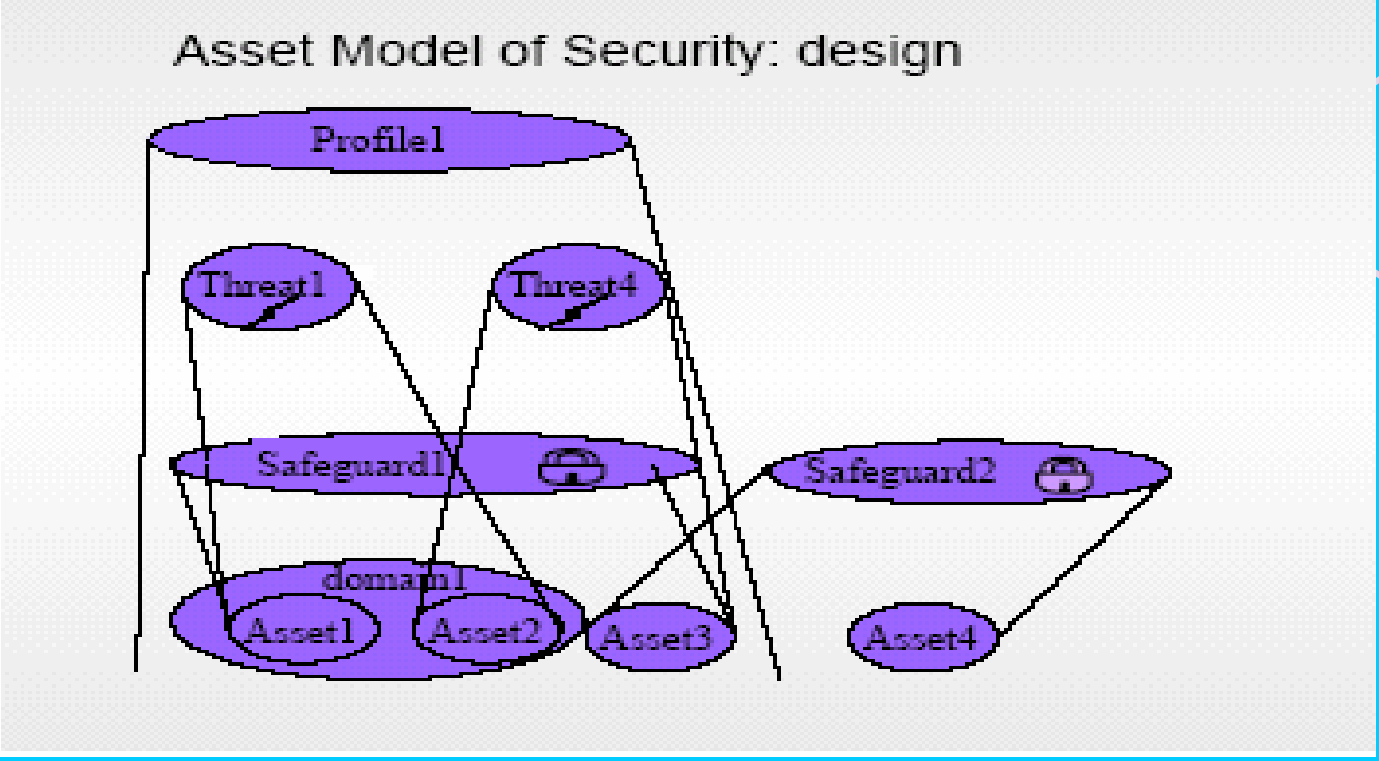
- Should indicate
- (1) the current level of risk (Risk metrics),
- (2) the likely consequences, and
- (3) what to do about it if the residual risk is too high.

Risk Metrics



Security Risk Analysis





- All risk analysis methodologies enable system users to compare possible losses to their agency with the cost of countermeasures (a.k.a. safeguards or controls) designed to protect against those losses.

Risk Analysis Terminology

- **Asset** - Anything with value and in need of protection.
- **Threat** - An action or potential action with the propensity to cause damage.
- **Vulnerability** - A condition of weakness. *If there were no vulnerabilities, there wouldbe no concern for threat activity.*
- **Countermeasure** - Any device or action with the ability to reduce vulnerability.
- **Expected Loss** - The anticipated negative impact to assets due to threat manifestation.
- **Impact** - Losses as a result of threat activity are normally expressed in one or more**Risk Analysis Terminology**
- **Impact areas** Four areas are commonly used; Destruction, Denial of Service, Disclosure, and Modification.

Security Risk Analysis

- Examination of the **interrelationships** between assets, threats, vulnerabilities, and countermeasures to determine the **current** level of risk.
- **Residual risk:** the level of risk that remains after consideration of all in-place countermeasures, vulnerability levels, and related threats**.**
- Ultimately, it is the residual risk that must be accepted [as is] or reduced to a point where it can be accepted.

Risk Assessment

- Identifies plausible threats, vulnerabilities, and potential consequences.
- Process that identifies the probable consequences or risks associated with the vulnerabilities and provides the basis for establishing a cost-effective security program.

Risk Management

- The process of implementing and maintaining countermeasures that reduce the effects of risk to an acceptable level.

- Consists of the spectrum of decisions made and actions taken to prevent, mitigate, or manage adverse consequences if potential threats become reality and exploit identified vulnerabilities.

Risk Assessment

- Includes the following steps:
- • Identifying core service processes
- • Identifying **critical assets** (including supporting information technology systems) that support those core processes
- • Identifying the potential threats to and vulnerabilities of those critical assets

Risk Analysis

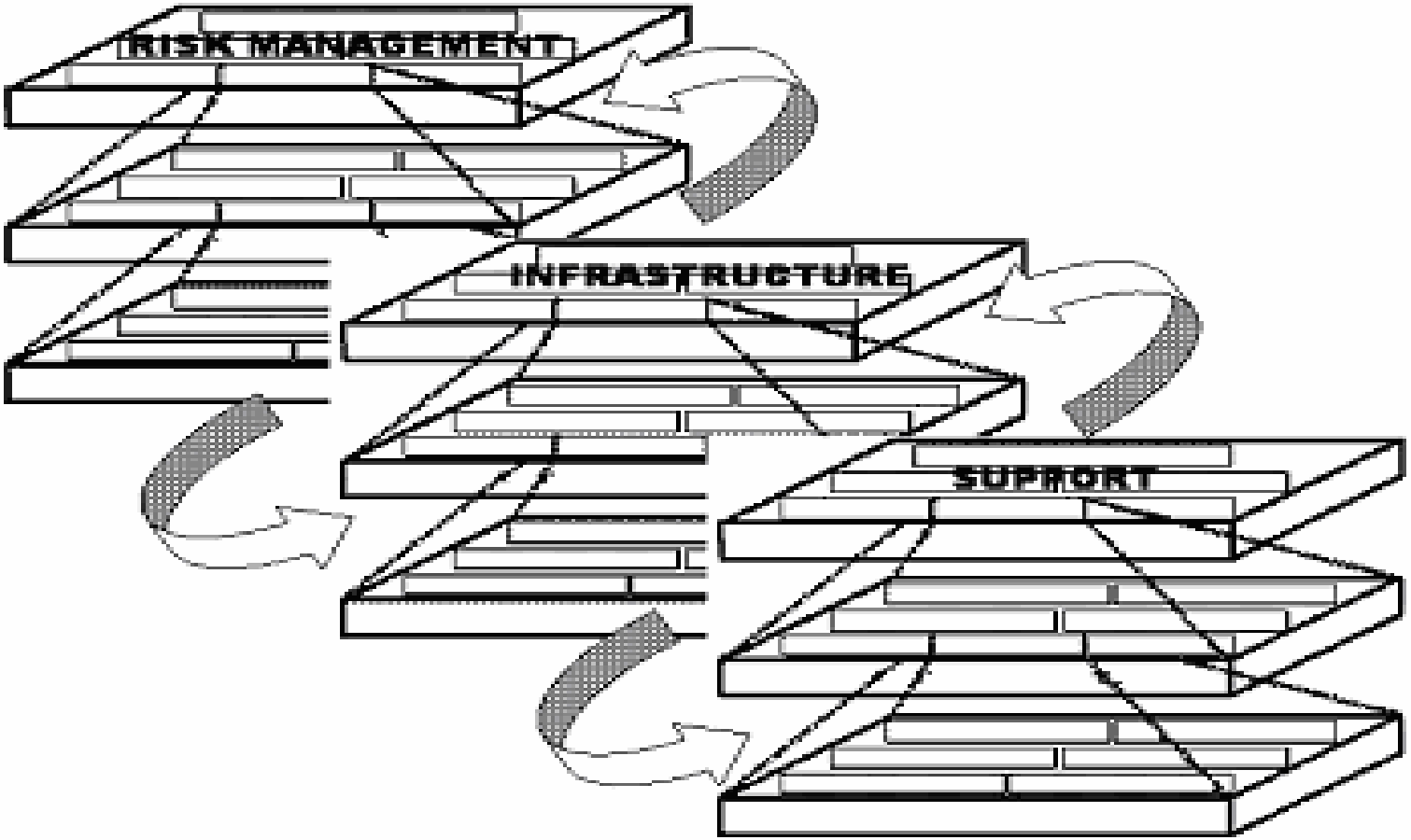
Identifies the existing security controls, calculates vulnerabilities, and evaluates the effect of threats on each area of vulnerability.

- Procedure attempts to strike an ***economic balance*** between the impact of risks and the cost of security solutions intended to manage them

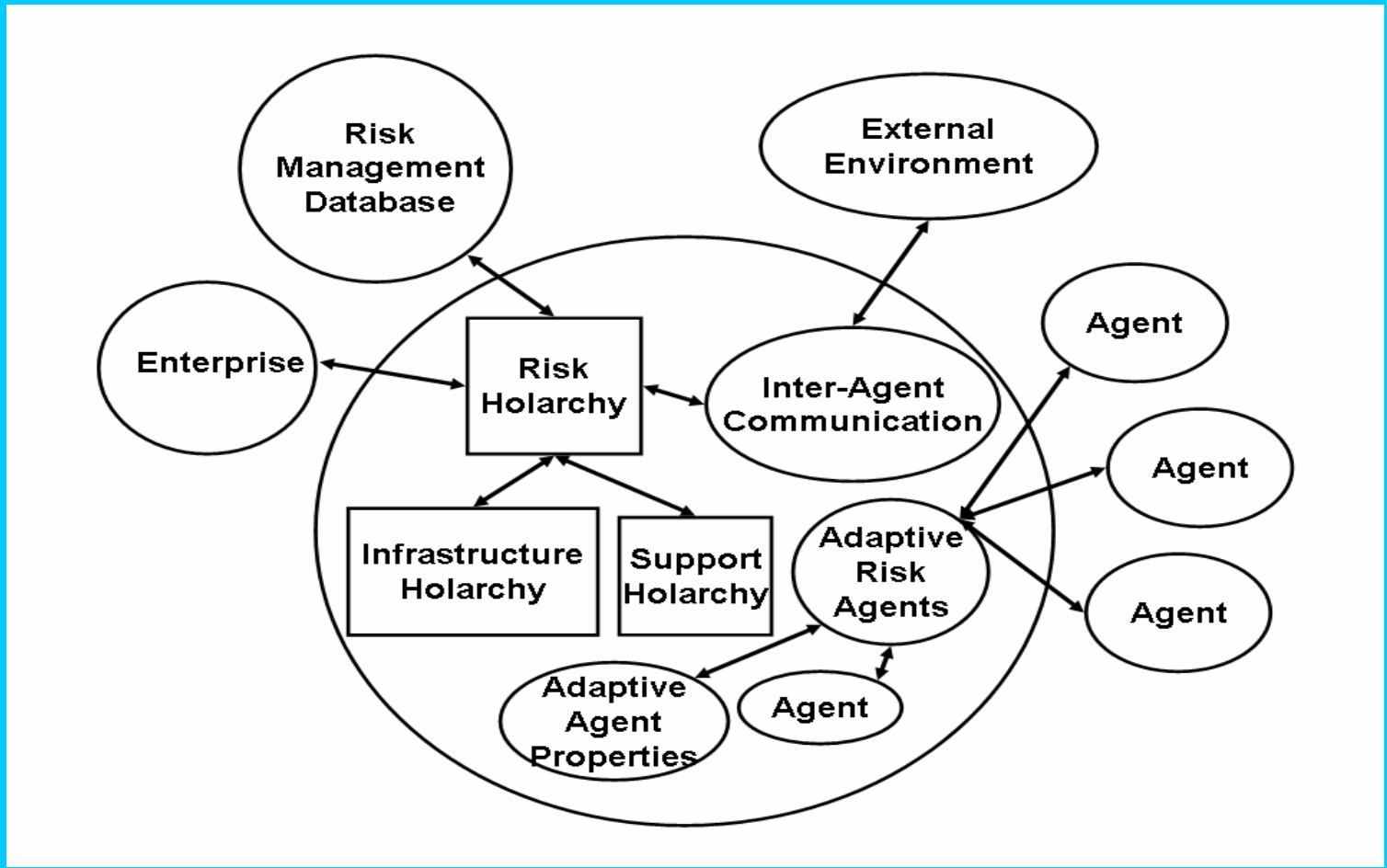
KEY FACTORS

- To be useful, a risk analysis methodology should produce a quantitative statement of the impact of a risk or the effect of specific security problems. The **three key elements** in risk analysis are;
- (1) A statement of impact or the cost of a specific difficulty if it happens,
- (2) A measure of the effectiveness of in-place countermeasures, and
- (3) A series of recommendations to correct or minimize identified problems.

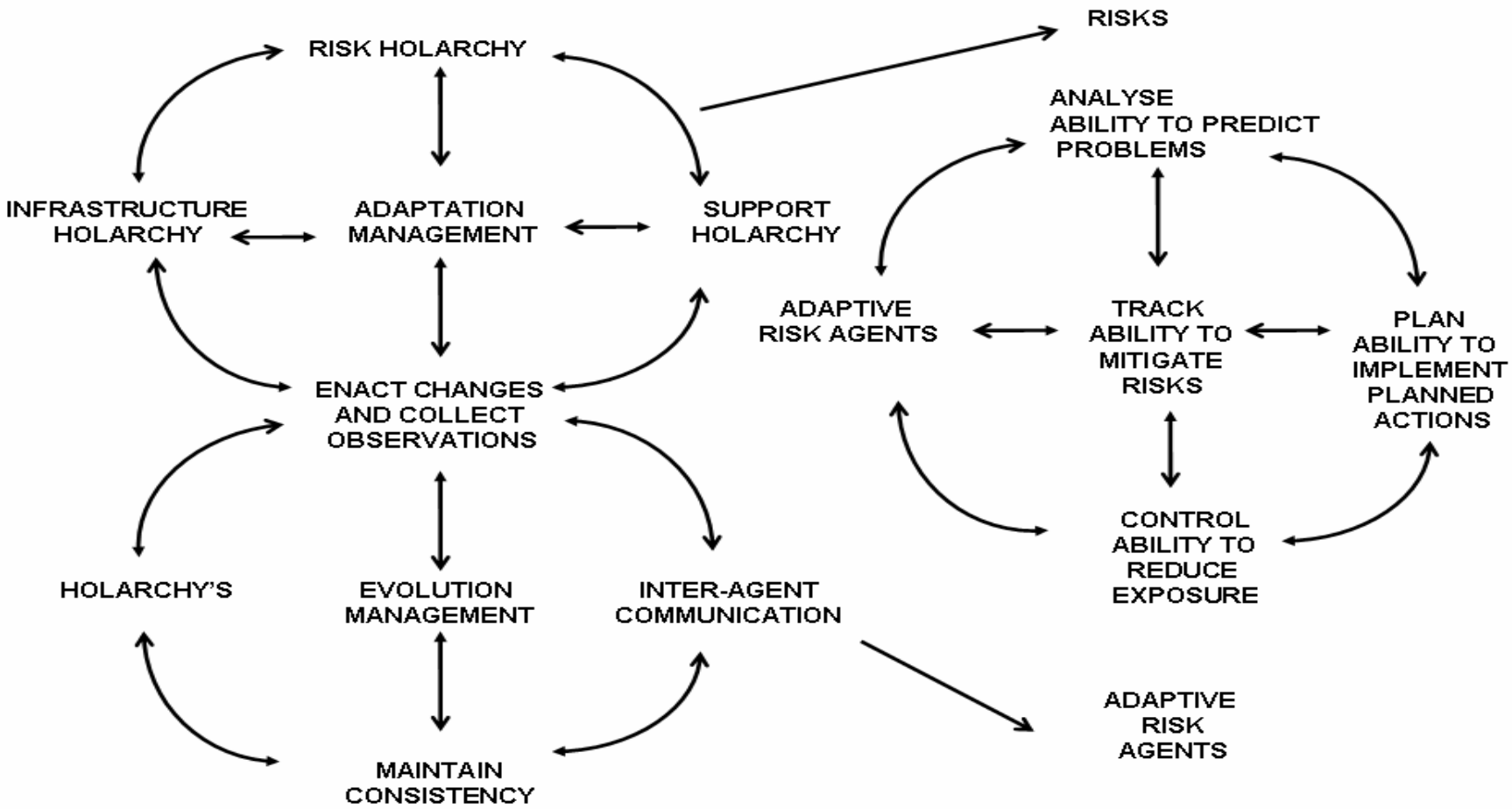
ARMS Framework



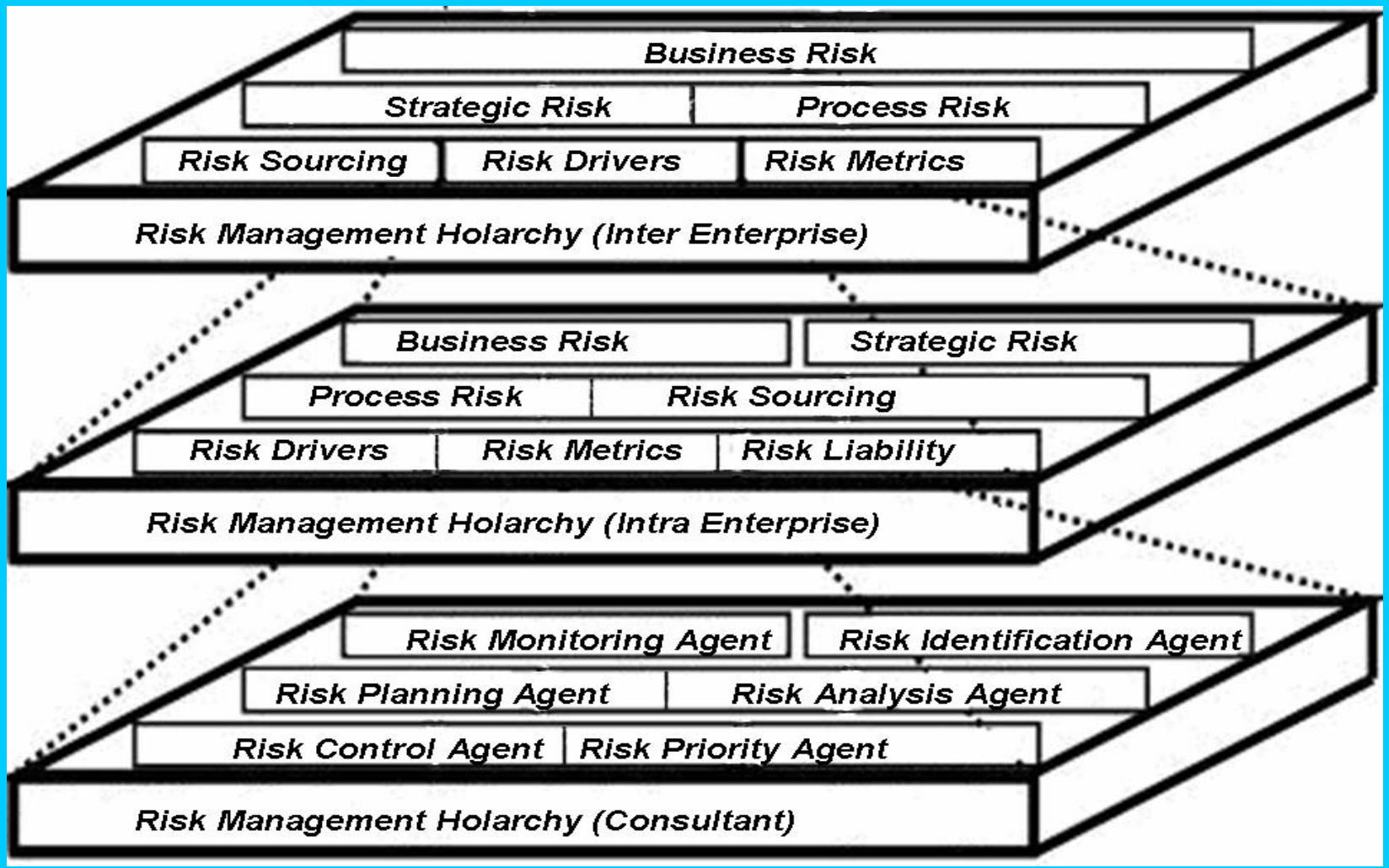
Functional Ecomap of ARMS



Functional View of ARMS



Risk Holarchy



CONCLUSIONS

- **A generic methodology to build resilient networked infrastructures encompassing an adaptive risk management mechanism of self defense (including potential to annihilate malicious attackers).**
- **Applications ranging from terrorist network annihilation to drug design for cancer cure, interception and defense against biochemical attacks; pandemic mitigation; modeling sustainability and resilience via environmental monitoring**

APPLICATIONS

- blackout-free electricity generation and distribution; terrorist network interception and annihilation [Vidyasagar, 2005]; interception of and defence against biochemical attacks (e.g. using dedicated sensor networks capable of long range detection of various agents; buildings equipped with safety mechanisms, for example, automatically shutting off air conditioning if a biochemical attack is detected); hazard free transportation (automotive networks for aerospace and avionics); disaster response and pandemic mitigation (public notification systems, evacuation and rescue operations coordination)

IMPACT

- **forecasting long term sustainability and resilience of life on our planet** – e.g., by identifying and modeling interdependencies between climate change, economic (natural resource) scarcity, ecological and environmental influences, including the potential to design eNetworks to monitor such changes to anticipate their trends and impact on mankind's future; **monitoring the evolution of global interdependent economies and markets** – e.g. , by detecting intentional risk through network analysis of global capital flows.