

Co-Active Emergence for Human-Automation Cyber Security Awareness

Marco Carvalho, Ph.D.
**Florida Institute for Human and
Machine Cognition**

Boise, ID – August 10, 2011

Acknowledgments

Cyber Situation Awareness

- Jeff Bradshaw
- Larry Bunch
- Tom Eskridge
- Paul Feltovitch

Cyber Lab

- Carlos Perez
- Adrian Granados
- Marco Arguedas
- Massimiliano Marcon

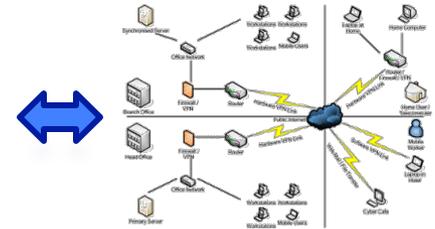
Cyber Security and Critical Infrastructure Protection

- Complex Infrastructures
 - Multiple interacting systems
 - Often under different administrative control
 - Very large number of heterogeneous sensors and data streams
 - Multiple operating time-scales for different components and subsystems
 - Time-critical / Mission-critical
- Users generally track specific metrics at any given time.
- Difficult to model and predict
- Require some level of automated monitoring and control

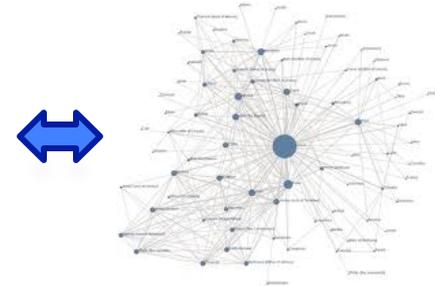


Automation in Complex System Monitoring

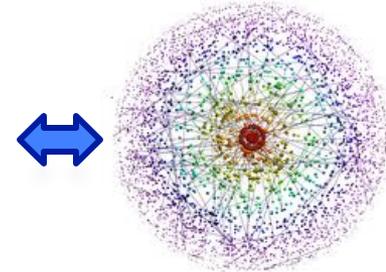
- Small scale systems were first monitored directly by users.
 - User has a mental model of the system
 - Single administrative domain
- Increasing scale and complexity requires some level of automation
 - High-tempo events
 - Large number of nodes
 - Large number of events
 - Complex very complex model
- Human becomes increasingly detached from the system
- Control/Defense becomes brittle and hard to understand/control



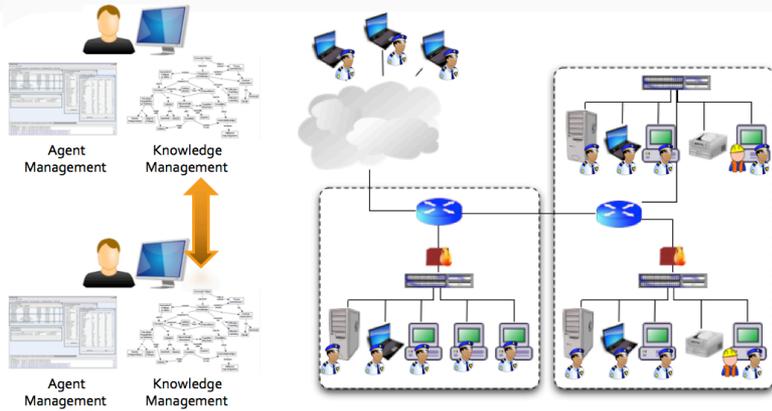
Automation



Automation



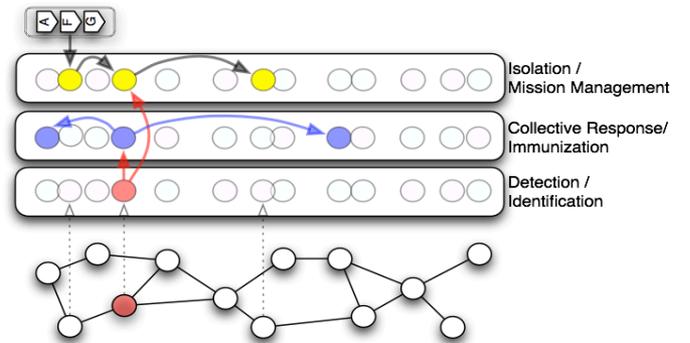
Enterprise Security



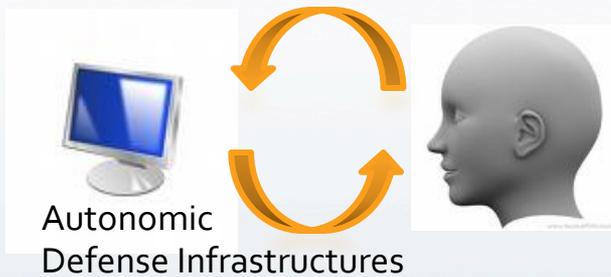
Intelligent Traffic Management and Critical Infrastructure Protection



Bio-Inspired Tactical Infrastructure Protection

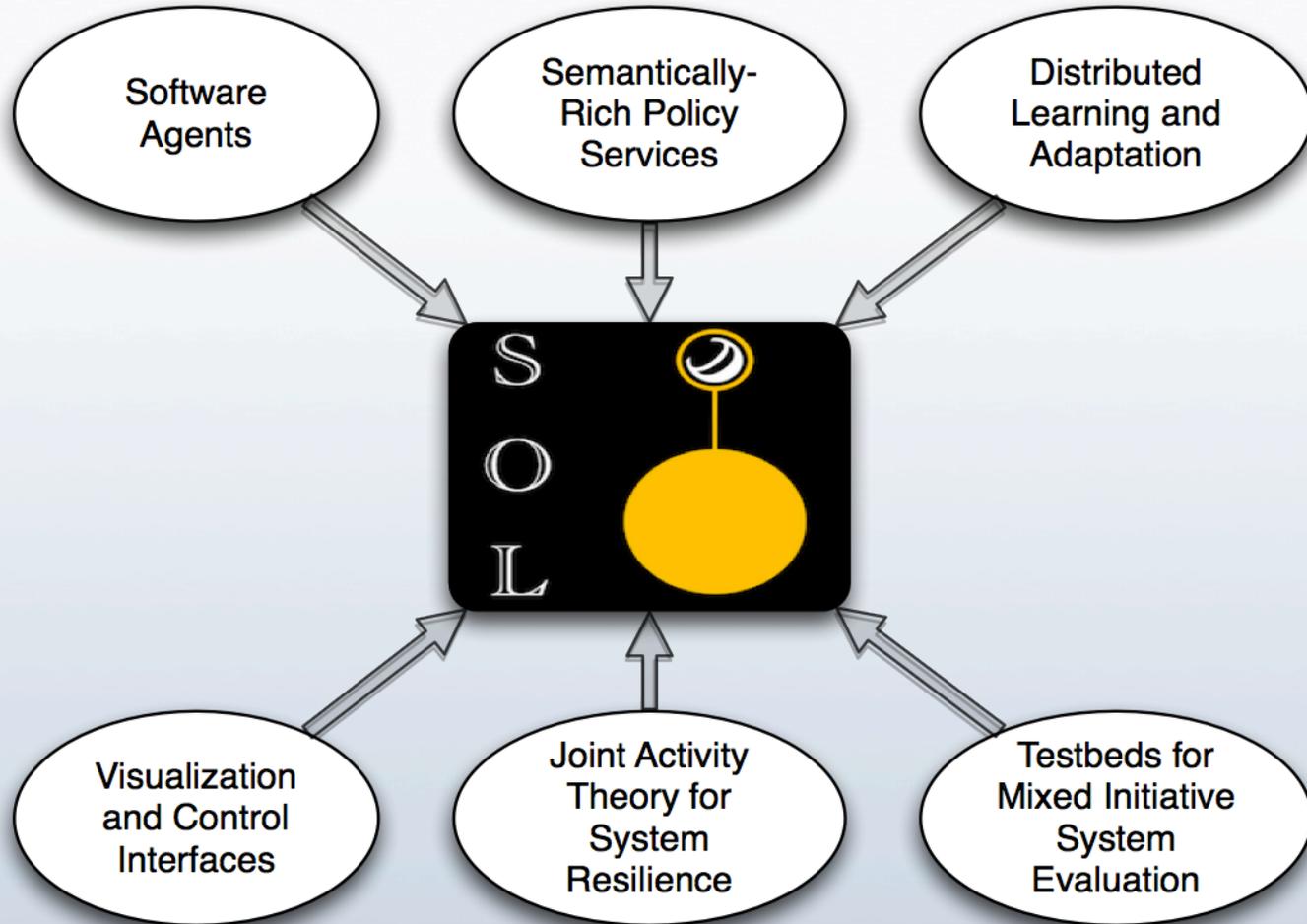


Defense Infrastructures Incorporating Principles of Human-Automation Teamwork



- Design security infrastructures to **enhance** human capabilities and performance on **monitoring, diagnostics and control** of complex and critical systems.
- Design new **defense infrastructures** with significant **automation** but which are capable of **sophisticated joint activity** with people

Six Key Research Thrusts

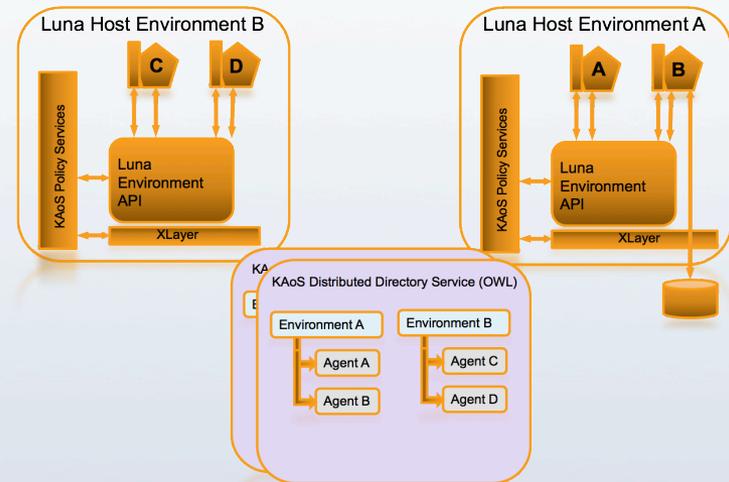


Key Research Thrusts: Software Agents

Luna Conceptual Architecture

The Luna Agent System

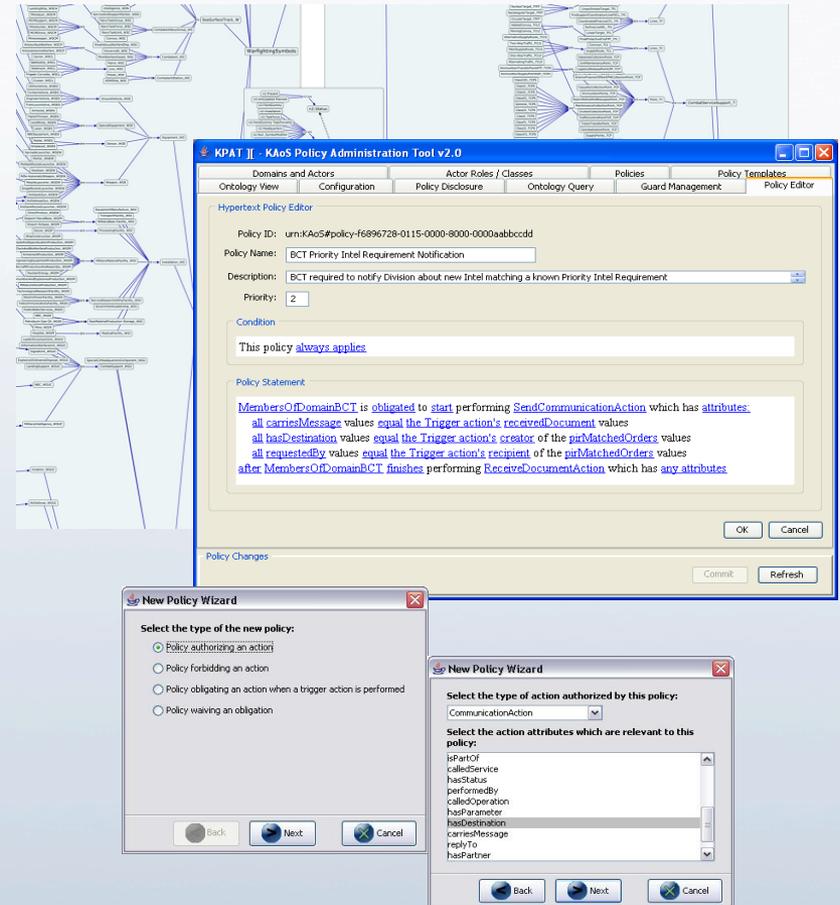
- Lightweight and Efficient
- Comprehensive Policy-Governed Operation
- Controlled Hosting Environment
- Agent Persistence
- State Mobility
- Dynamic Load-Balancing
- Adaptive Resource Utilization for Scalability
- Resource Awareness and Control
- Flexible Agent Messaging
- Full Semantic Representation
- Automatic Generation of OWL Ontologies
- Easy to Learn, Use, and Maintain
- Robust Implementation



Key Research Thrusts: Semantically-Rich Policies

Benefits

- The application of policy to regulate agent and system behavior makes interaction as natural and effective as possible, while providing assurance that security and other important operational concerns are fully respected.



Key Research Thrusts: Testbed for Mixed-Initiative Research

Benefits

- Data sources and data management infrastructure are securely housed as part of IHMC-Ocala's Cyber Security testbed facility, and supports distributed evaluation and experimentation to IHMC-Pensacola and potentially other sites.



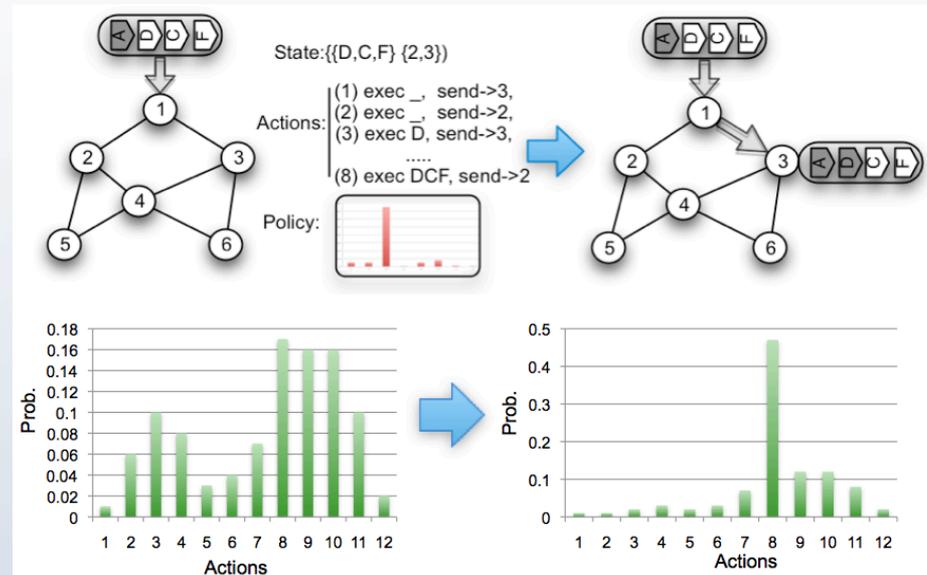
Cyber Defense Laboratory facilities at
IHMC-Ocala



Key Research Thrusts: Learning and Adaptation

Benefits

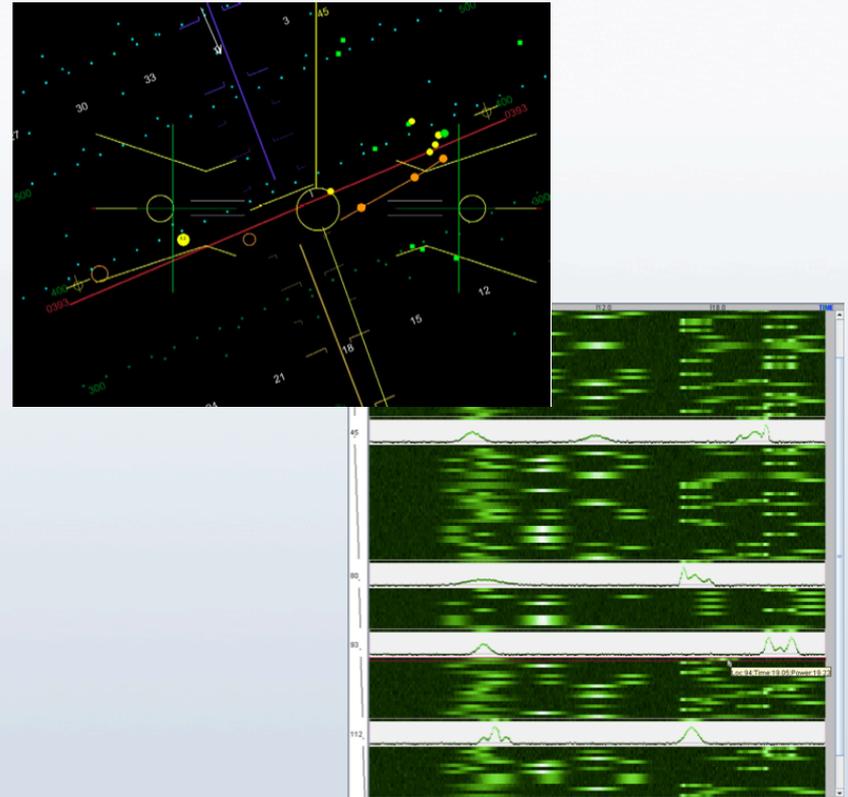
- Distributed policy learning and adaptation provides a key capability for the realization multi-agent software systems that keep the human in the loop, and in control, while allowing for automatic or semi-automatic adaptation.



Key Research Thrusts: Visualization

Benefits

- The techniques used to present data will enable operators to discover anomalies and key data relationships.
- Innovative processing techniques allow visualizations to answer a number of different questions while accessing underlying data only once.
- Visual display of group problem solving behavior promotes greater team efficiency.



Thank you!

Marco Carvalho
Research Scientist
mcarvalho@ihmc.us
(850) 202-4446

Institute for Human and Machine Cognition
15 SE Osceola Ave.
Ocala, FL.

www.ihmc.us

