Situation Awareness for Cyber Defense

June 20-22, 2006

Leslie D. Cumiford, PhD, PE
Knowledge Discovery and Extraction
Defense Systems and Assessments
Sandia National Laboratories
ldcumif@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Overview

- Situation awareness (SA)
- Cyber defense domain
- Addressing of complexity
- Cyber situation awareness
- Reduction of complexity
- Conclusions

Situation Awareness (SA)

The ability to rapidly and effectively address incoming stimuli with appropriate responses.

- **Awareness of current environment**
- **Ability to assess and impact environment**
- **Ability to accomplish goals**
- **Reasoning about time**
- **Selective attention for crowded environments**

Cyber Defense Domain

- Characteristics in common with domains of terrorism analysis, infrastructure protection, and IED defense
- Complex, interacting issues are ill-defined, ambiguous, and evolving
- Patterns of communication and association across interfaces
- Level of system complexity and timeframe of relevance are important choices

(Hayden 2006)

Cyber Agents for Defensive Operations

Defend:

- **Self**
- **Related information systems**
- **Control systems for physical systems**
- **Human force or operation**
- **Allied forces or systems**
- **A combination of the above**

Cyber Defense Domain Complexity

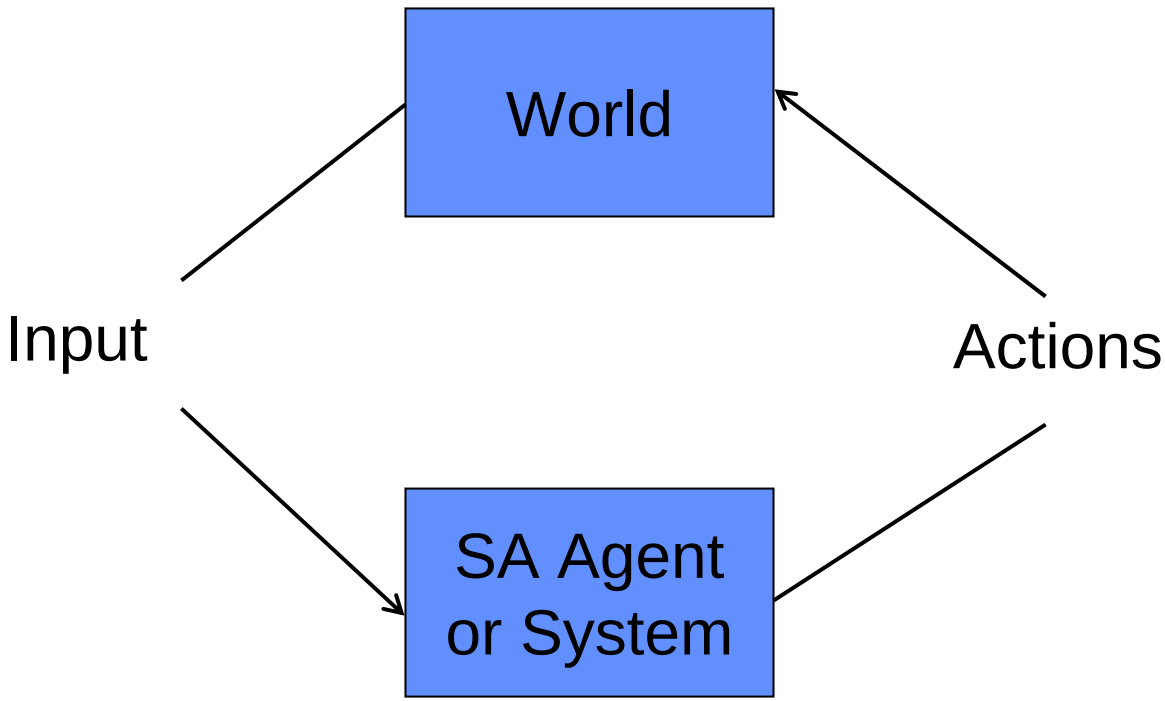
Cyber SA: need discernment and spontaneity

- **Two dimensions: digital and physical defense**
- **Tasks, to be dynamically conducted over time:**
  - **Assess and track enemy's cyber capabilities**
  - **Predict and defend against attacks**
  - **Assess and track own defense capabilities**
  - **Coordinate with allied operations**
  - **Note influence of environmental factors (e.g., hardware failures)**
  - **Maintain tempo faster than that of hostile attacking systems**
  - **Battle damage assessment of self and friendly systems**

Cyber Situation Awareness

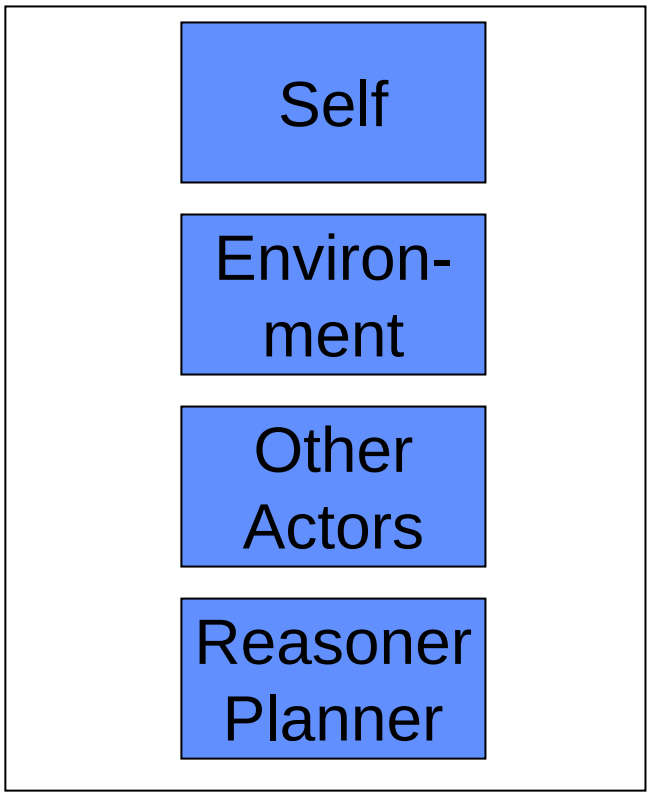
- Process incoming data
  - Asynchronous
  - Disparate in composition and source
  - High in volume
- Abstract low-level details into higher-level models
- Capture and reason about past, present, and future states
- Bootstrap to evolve models
- Track progress to goals

Simple SA Feedback Loop

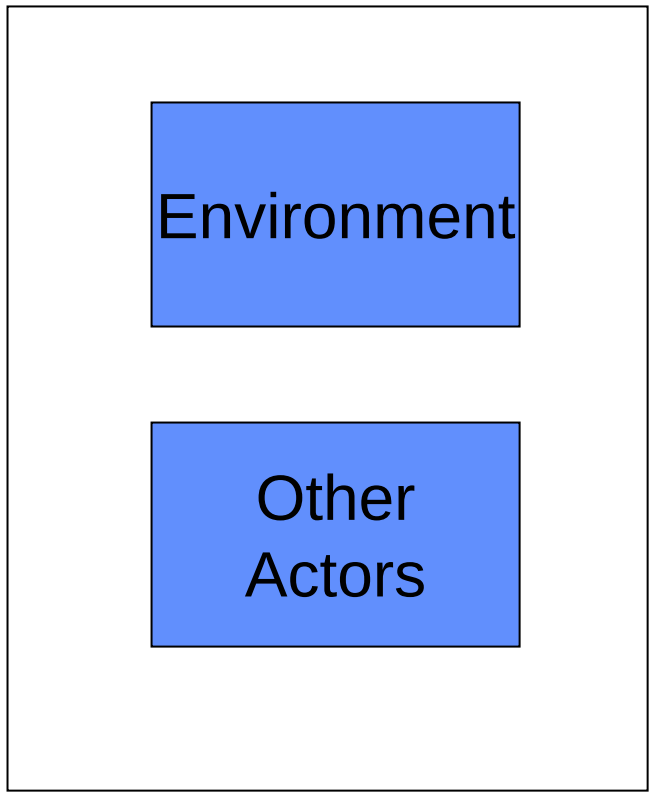


Situation Awareness Models

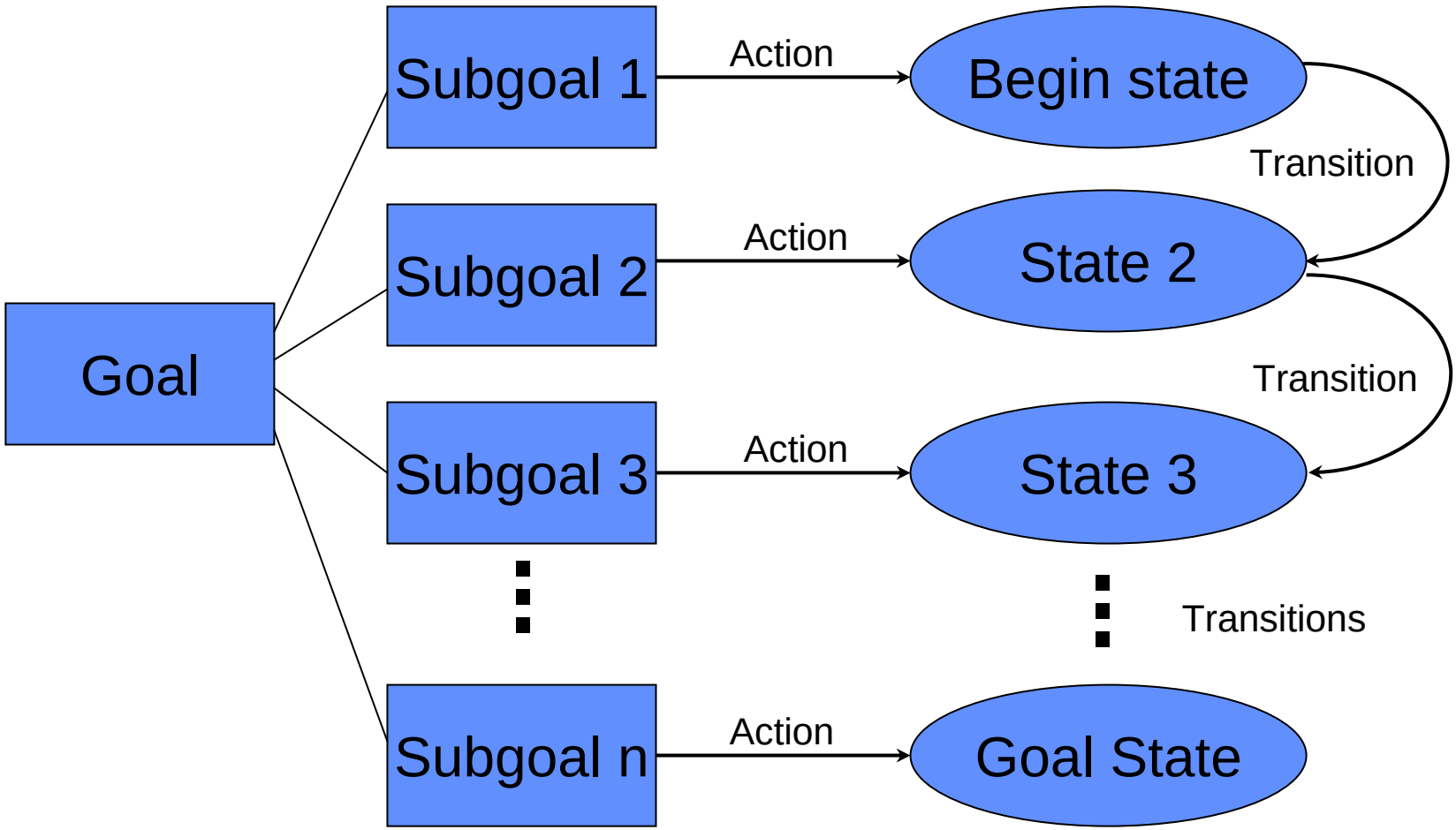
SA Agent or System



World



Incremental Goal Satisfaction

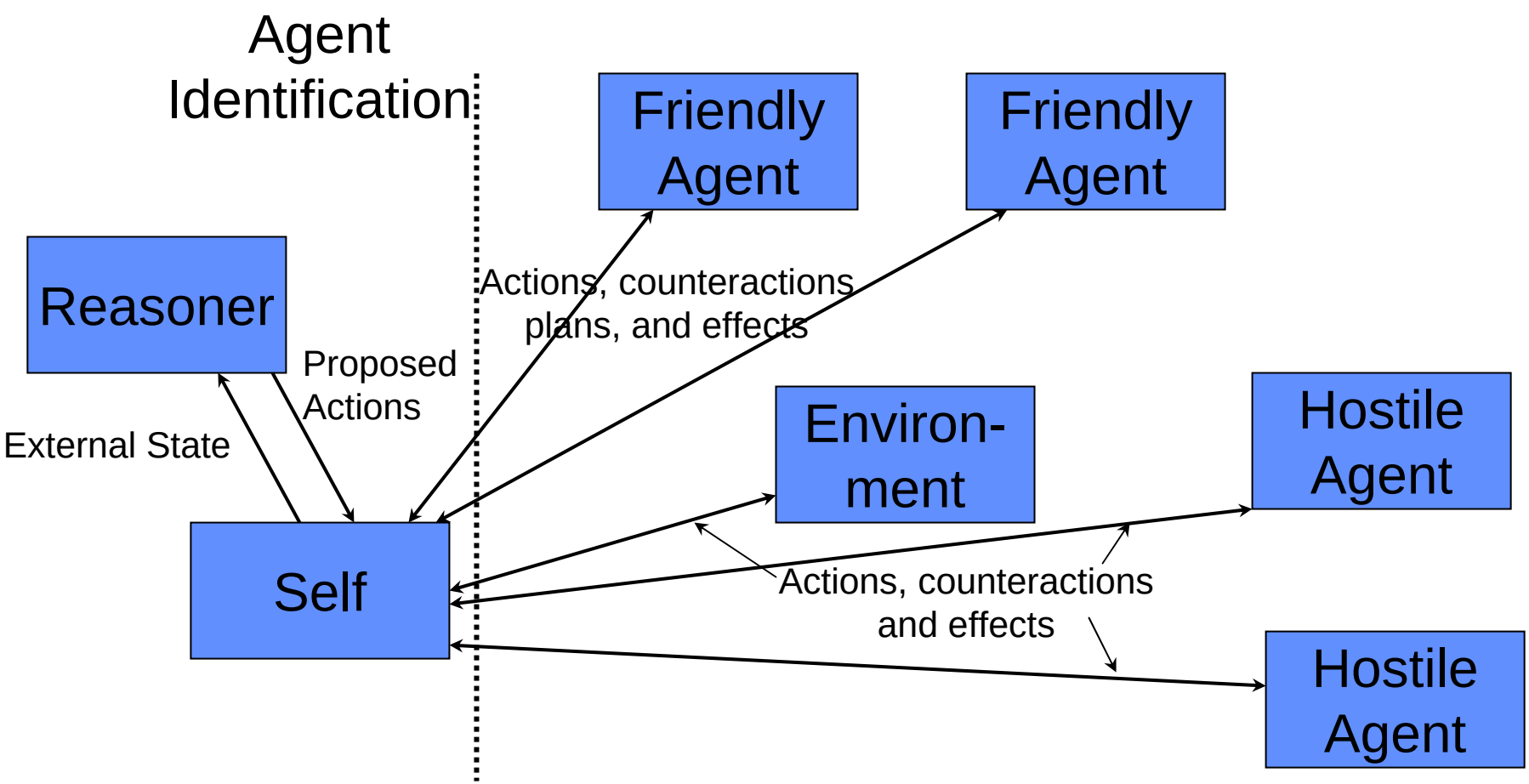


Sandia National Laboratories

Higher-Level SA Capability

- Explicit temporal reasoning (modal logic)
  - To see deadlines, coincident events, etc.
- Domain may require spatial or other specialized reasoning
- Truth maintenance
  - To sync reality with models
- Selective attention
  - To reduce information overload in crowded environments
- Learning
  - To benefit from past experience

More Complex SA Feedback Loop

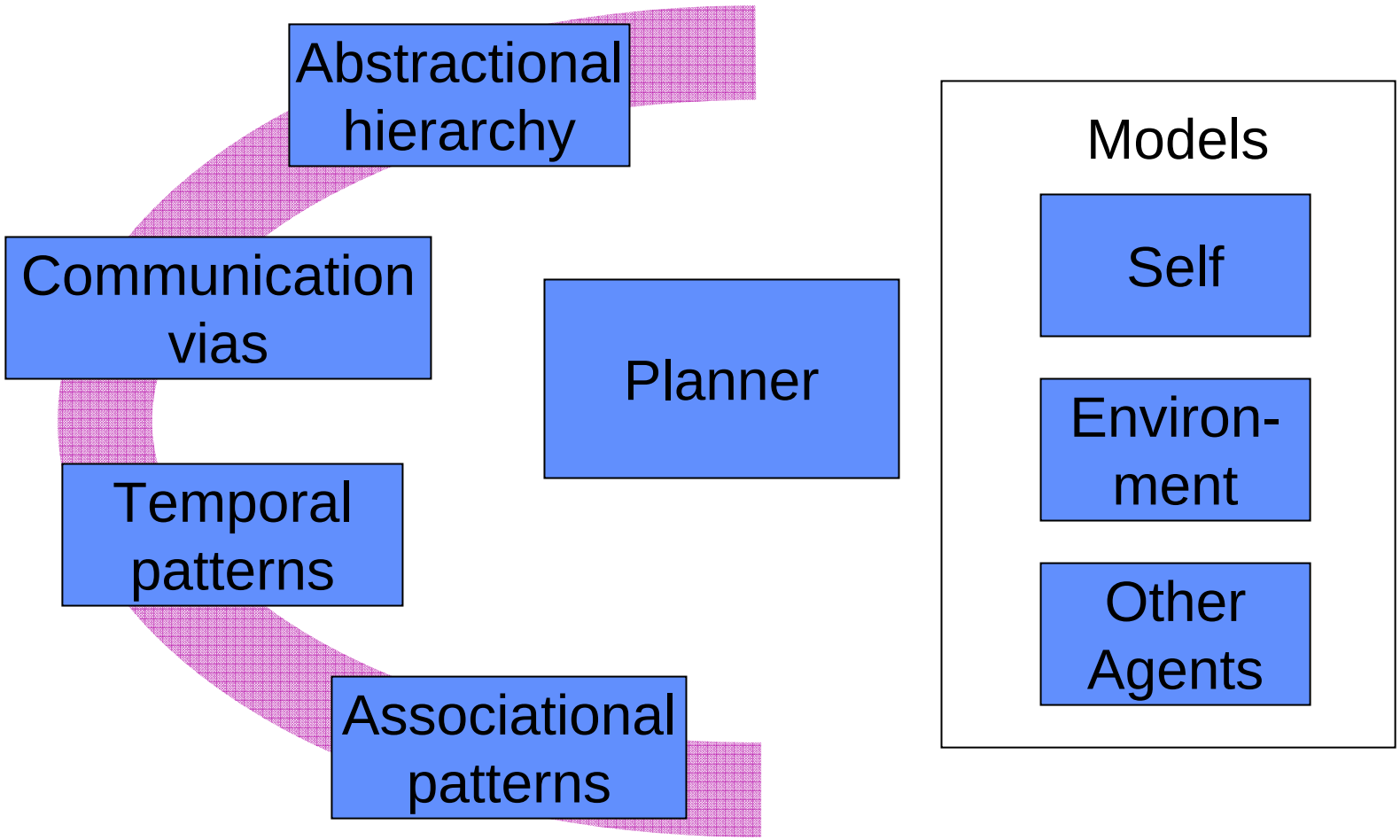


Sandia National Laboratories

Cyber SA Agent: Handling Other Actors

- **Benevolent other actors**
  - **communication and coordination associated with team SA**
- **Malevolent other actors**
  - **game theory with antagonistic players**
- **Domain may include both**
  - **Authentication of communication sources and identity of other actors**
    - **Avoid spoofing**
    - **Identify source of attack**

Situation Awareness Reasoning



Sandia National Laboratories

Reduction of Complexity

Lessons from brain research (Hawkins 2004)

- Different kinds of data from our senses are made into common patterns for cortex processing
- Patterns are stored in memory as temporal sequences by the cortex
- Auto-associative recall
- Invariant representations

Conclusion for cyber SA: Focus on transformation of incoming patterns more fruitful than matching of complexity in system structure to that of the domain

Conclusions

- Understand the complexity of the cyber defense domain
- Mirroring the complexity in the cyber SA system is not necessarily the answer
- Focus on patterns and memory
- Judiciously balance dichotomies in the design:
  - Prediction vs novel events
  - Control vs assessment
  - Benevolent vs malevolent other actors
  - Specialized vs generalized patterns
  - Complex vs simple