Intent Driven Adversarial Modeling

June 14, 2005

Lynn Lehman
llehman@securboration.com

Duane A. Gilmour
duane.gilmour@rl.af.mil

Lee Krause
lkrause@securboration.com

Dr. Eugene Santos
eugene@cse.uconn.edu

Dr. Qunhua Zhao
qzhao@engr.uconn.edu

Agenda

- Adversary Modeling
- Increased Demands on the Planning Paradigm
- Emergent Adversarial Modeling
- The EAMS Intent Driven Approach
- EAMS “Proof of Concept” Demonstration
- EAMS Expansion
- Acknowledgements

Adversary Modeling

- The increase in limited conflict warfare has created new challenges in mission planning and simulation.
- New approaches to warfare planning, such as effects based operations and predictive battlespace awareness, have also increased the need for improved simulations.
- Current adversarial simulation requires continual assessment of friendly courses of action and is currently “human assessment capability” limited.
- In the post-cold war era of limited conflict and unconventional adversary response, simulations based on attrition principles do not yield realistic or useable results.
- Modern elements of military intelligence and decision making require predictions of adversary force actions and reactions to provide a complete and realistic viewpoint.

Increased Demands on the Planning Paradigm

- **Traditionally, Blue COAs are wargamed against the "most likely / dangerous" adversary COAs** *(as a pre-scripted sequence of events independent of Blue actions)*
- **Important to create and exercise realistic adversary responses as part of simulation for mission planning**
- **Non-conventional adversaries seldom have capabilities that rival U.S. forces adversarial intent and response become more important**
- **In the post-cold war era of limited conflict and unconventional adversary response, attrition- based simulations do not yield realistic results.**
- **Assessment / re-assessment of friendly courses of action is currently limited by human capability**
- **Need to model dynamic adversary behaviors that integrate with various intelligence and mission data sources (Modernized Integrated Database (MIDB), Air Operations Database (AODB), IPB Products, etc.**
- **The Emergent Adversarial Modeling System (EAMS) addresses operational patterns, behaviors, and doctrines of present-day adversaries (terrorist cells, local insurgents, guerillas, and armed thugs) as well as more conventional force elements.**

Emergent Adversarial Behavior

What is the concept of Emergent Adversarial Behavior

- **Emergent behavior refers to intelligent dynamic adversarial actions generated at the operational level in response to the execution of the friendly force within the simulation**
- **Red Force reacts to Blue Force actions (from their perspective**
  - **Monitor and understand battle-space *observables* and how they relate to *adversary* intent**
  - **Form a mission or missions (*reacting*) based on the *observables***
- **Red Force intent drives their actions**
  - **Missions differ based on differing intent**
- **Predictive adversary modeling is one of the key requirements for EBO, where the adversary is addressed as a system.**

Emergent Adversarial Modeling

- EAMS demonstrates alterations of Red force behavior in response to observed Blue force actions.
- Blue force actions are addressed from the perspective of the Red force (i.e. what does Red think or believe that Blue is doing)
- The adversary force reacts, and also learns from and adapts to Blue force actions
- Adversarial behavior emerges during the interactions/encounters between Red force and Blue force
- Plans and strategies, which result in courses of action (COAs), are evaluated to determine the necessary steps to meet the overall strategic objectives.
- COA analysis, also defined as wargaming, is the process of performing "what if" analysis of actions and reactions designed to visualize the flow of the battle and evaluate each friendly COA
- The uncertainty of the adversarial decision process makes it necessary to evaluate friendly COAs against a range of adversary COAs.

The EAMS Intent Driven Approach

- **Soft factors are those factors that influence adversarial intent in their decision making process, which include social, cultural, religious, political, economic and psychological issues.**
- **A significant amount of uncertainty is associated with any emergent adversarial actions**
- **Goals/Foci**: A prioritized (by probability) list of short and long term goals representing adversary intents, objectives or foci. The goal component captures ***what*** the adversary is doing.
- **Rationale Network**: A probabilistic network representing the influences of the adversary's beliefs, both about themselves and their opposition, on their goals and on high level actions associated with those goals. The rationale component infers ***why*** the adversary is behaving in a certain fashion.
- **Actions Network**: A probabilistic network representing the detailed relationships between adversary goals and possible actions to realize those goals. The action component captures ***how*** an adversary might act.

The EAMS Intent Driven Approach

- **Adversary axioms (X)** – represent the underlying beliefs of the adversary about themselves (vs. beliefs about Blue forces). Axioms typically serve as inputs or explanations to the other RVs, such as adversary goals.
- **Adversary beliefs (B)** – represent the adversary's beliefs regarding Blue forces (e.g., an adversary may believe that U.S. forces will not destroy religious sites or shrines).
- **Adversary goals (G)** – represent the goals or desired end-states of the adversary (e.g., preserving launchers, damage world opinion of U.S. action, defeat U.S. foreign policy, etc.).
- **Adversary actions (A)** – represent the actions of the adversary that can typically be observed by Blue forces.

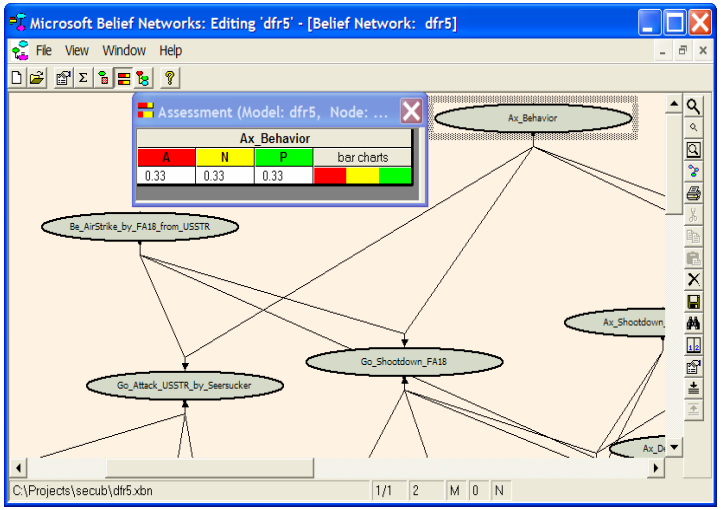
The EAMS Intent Driven Approach

- EAMS takes inputs from multiple sources:
  - Evidence/observables from battlefield, recon, sensor arrays, etc.
  - Projected Red COAs from the adversarial specification represented by an instance in the EAMS Ontology.
  - Analyst inputs from the Intelligence Situation Processor (ISP) component of EAMS, critical to merging and working with human analysts.

Behavior and Affects

Ax_Behavior represents a soft factor of red (commander).

Three states:
Aggressive,
Neutral,
Passive



Assessment (Model: dfr5, Node: Go_Shootdown_FA18)

Parent Node(s)			Go_Shootdown_FA18		
Ax_ShootDown_FA18	Be_AirStrike_by_FA18_from_USSTR	Ax_Behavior	Yes	No	bar charts
Yes	Yes	A	0.766	0.234	
		N	0.649	0.351	
		P	0.433	0.567	
	No	A	0.649	0.351	
		N	0.474	0.526	
		P	0.316	0.684	
No	Yes	A	0.474	0.526	
		N	0.211	0.789	
		P	0.141	0.859	
	No	A	0.374	0.626	
		N	0.061	0.939	
		P	0.041	0.959	

Assume the probability for the neutral states (N) is p_n,
The Probability for aggressive states (A) is: $p_n + 0.33 * (1.0 - p_n)$
The Probability for passive states (P) is: $(1- 0.33) * p_n$

Generate BKFs based on Ontology/KB

- Generate the Beliefs
  - Beliefs: what red believes that blue is going to do
  - Identify possible pairs of blue units/assets attacking red units/assets
  - Generate a Belief for each pair
    - Search through previous cases
    - Identify new Beliefs where the pair is not covered previously and match to closest historical frequency data
- Generate the Axioms
  - Axioms: what red believes about themselves
  - Identify red units/assets
  - Generate axioms for:
    - Status: for example, the operation condition of a airport
    - Effectiveness: Probability of hitting of the target with the asset, etc.

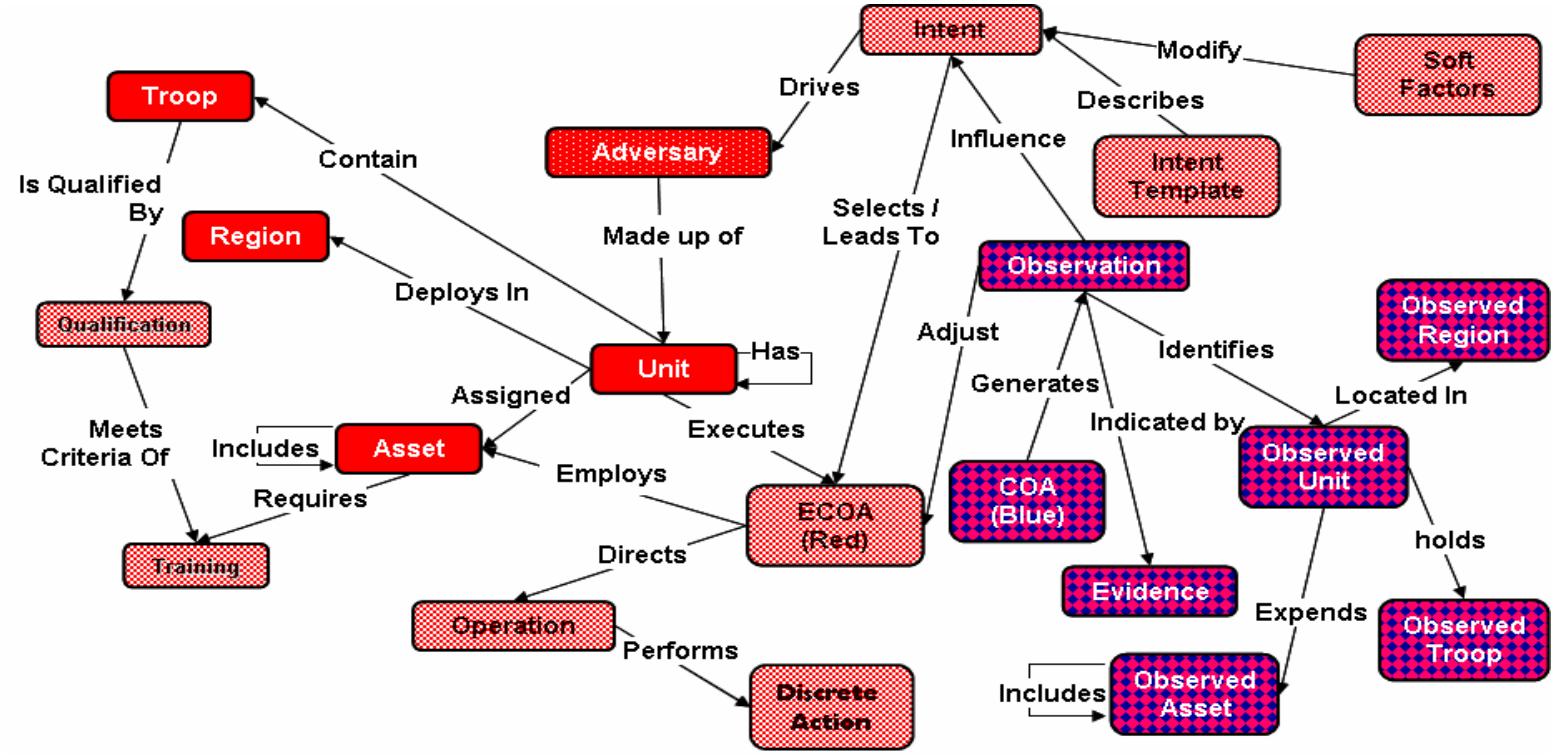
Generate BKFs (cont..)

- Generate the Beliefs and Axioms Based on
  - What are the doctrines defined in the ontology
  - What red/blue has: units/assets
  - What red believes the units/assets can do
  - Frequency data from history (database)
  - Examples:
    - No surrender (Ax_Surrender, yes = 0.01, no = 0.99)
    - Has 12 seersuckers (Ax_Has_Seersucker_12)
    - Seersucker has a single-shot hit probability of 70%, but blue can block it with 85% chance (Ax_Hit_Target_by_Seersucker_1, yes = 0.105, no = 0.895)

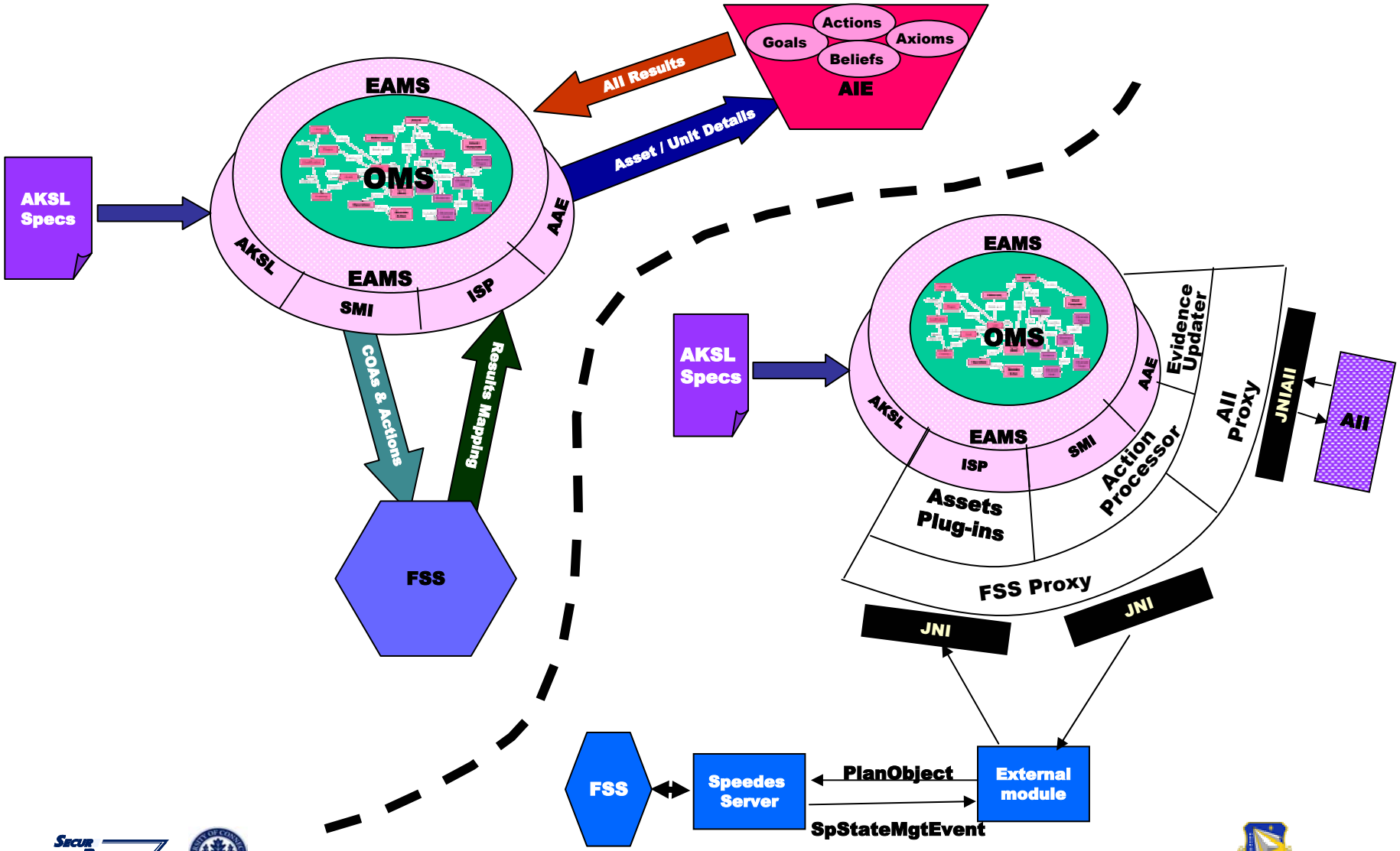
Proof of Concept Demo

- Demonstrated fluid (dynamic) adversarial response based upon observations of Blue Force actions
- Utilized Securboration's Scenario Generation Service (SGen) to support COA generation (Red and Blue Force COAs possible)
- Demonstrated (on limited basis) a structured adversary specification
- Deny Force Scenario running on the Force Structure Simulation
  - Demonstrated alternate Red Force responses
  - Supported actions driven by adversary's intent

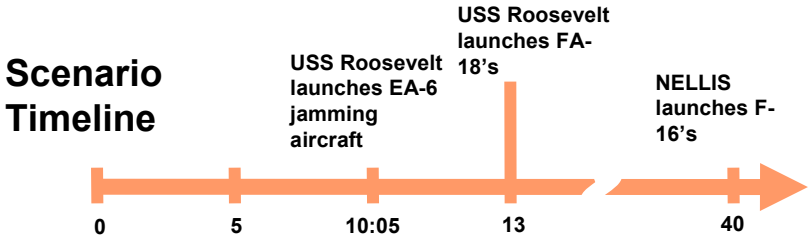
EAMS Ontology

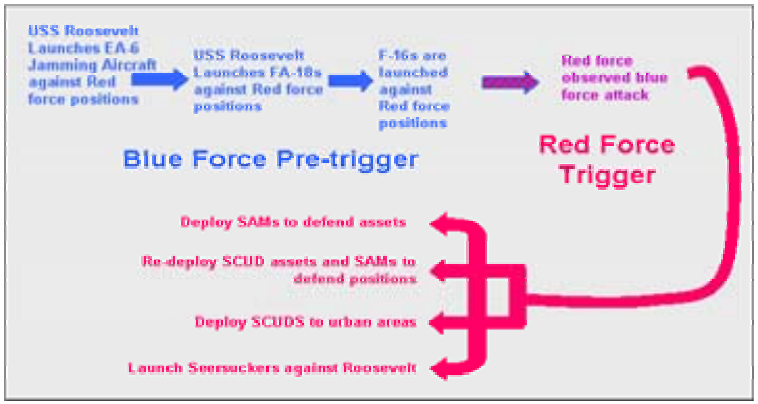


POC Architecture and Implementation



Deny Force Scenario





Demo Scenario 1

Significant Observable Events

- Meadows Detects Enemy
- Meadows Experiences Destruction
- Twenty Nine Palms Detects Enemy

Commander Intent - Aggressive

- Defend Initial Attack
  - Move GOA's into Meadows from Pendleton
- React To Destruction
  - Launch SeerSucker at USSTR from Vandenberg
- Continue To Defend
  - Move GOA's into Twenty Nine Palms from Pendleton

Demo Scenario 2

Significant Observable Events

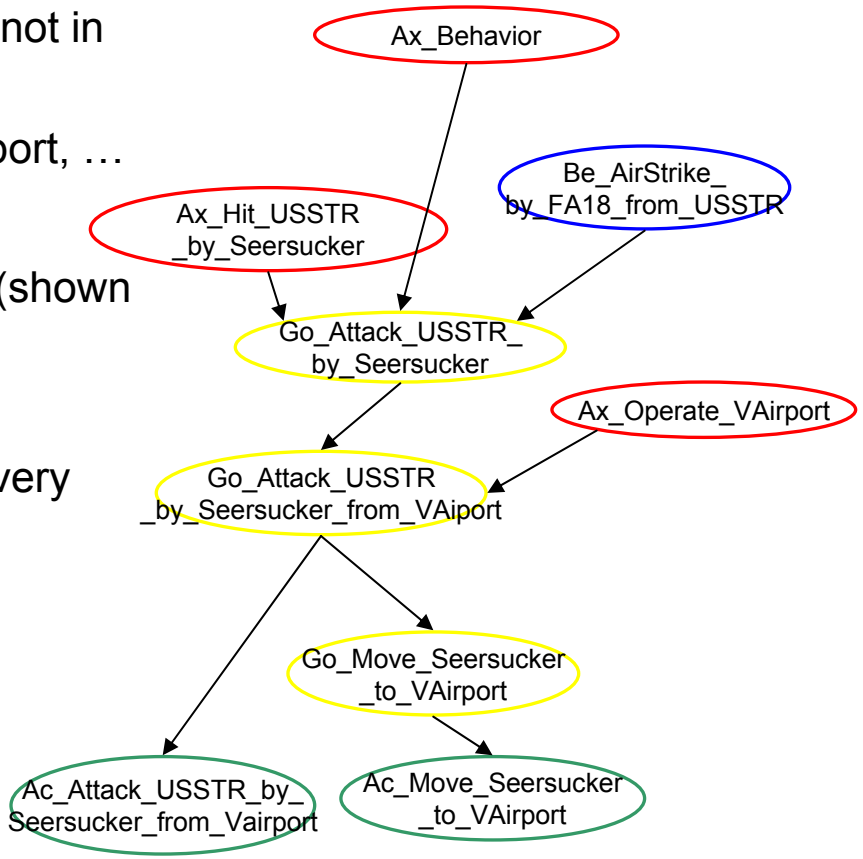
- Meadows Detects Enemy
- Meadows Experiences Destruction
- Twenty Nine Palms Detects Enemy

Commander Intent - Passive

- Defend Initial Attack
  - Move GOA's into Meadows from Pendleton
- Continue To Defend
  - Move GOA's into Twenty Nine Palms from Pendleton
- Defend With Authority
  - Operate All SA-2's

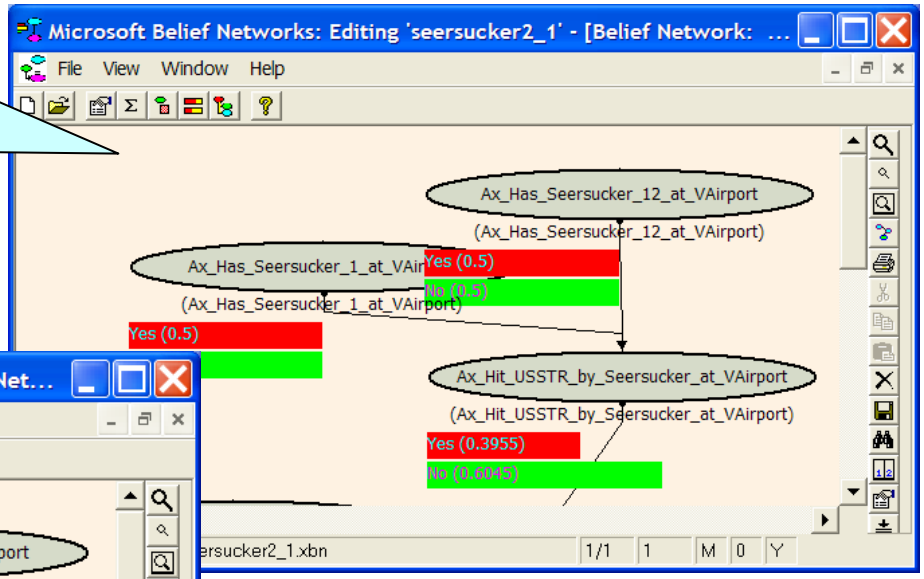
An example of BKF generation

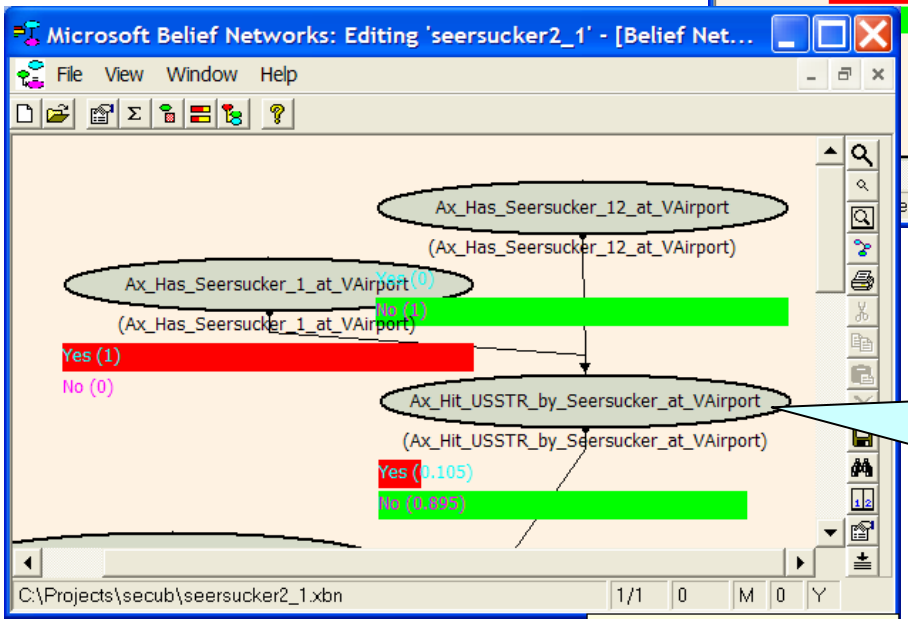
- According to the scenarios, there is a goal to attack USS TR with sunburn, which is a new asset not in the working network.
  - Assets include: USS TR, sunburn, VAirport, …
- Search in the library retrieves one fragment (shown next)
  - Include, USS TR, VAirport, seersucker.
  - Also the goals, axioms, and beliefs are very similar



Represent numbers of assets in BN

Red possibly has 1 or 12 seersuckers from 2 different reports. Hit
p(yes = 0.3955, no =0.6045)



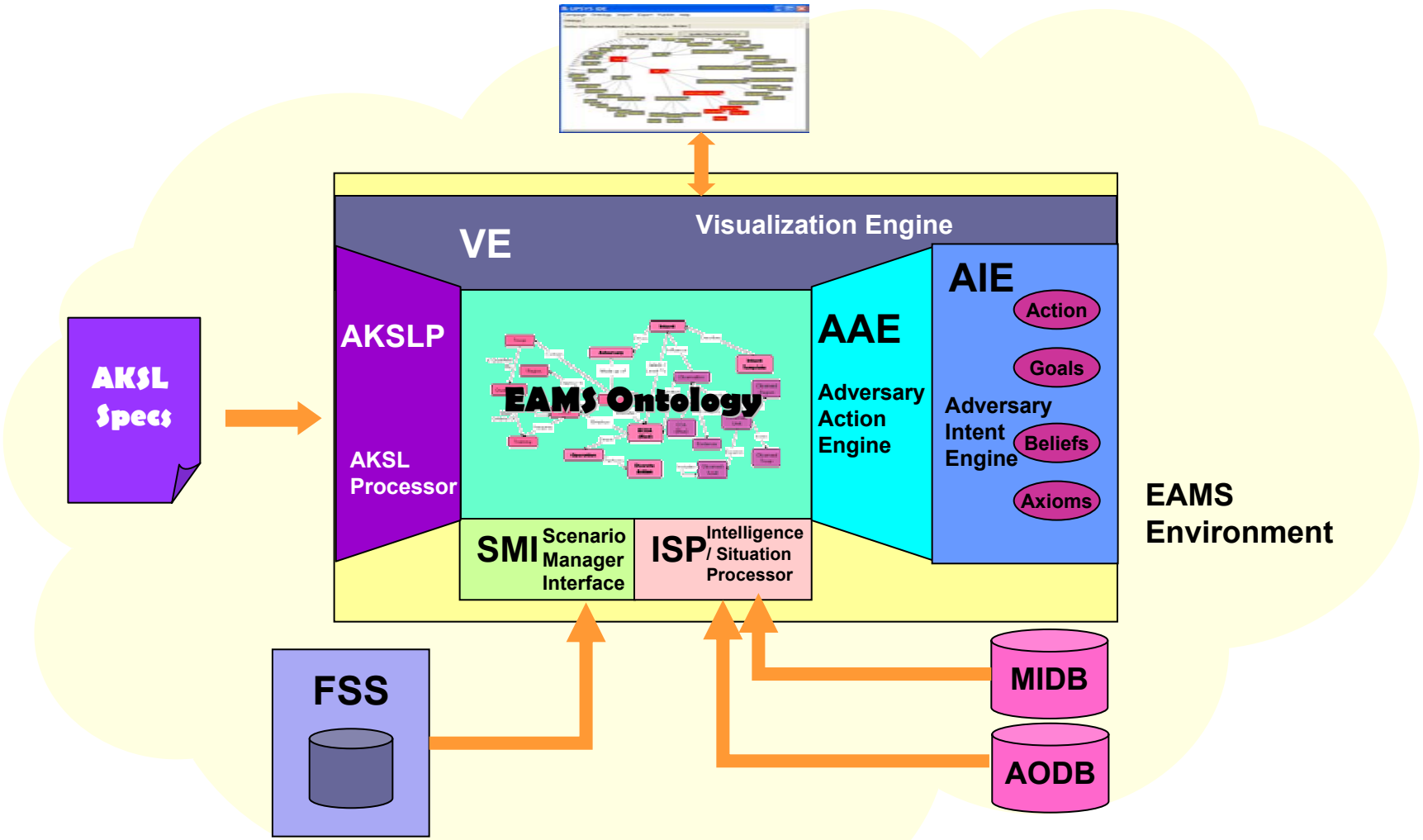


Now confirmed, they only have 1 seersucker.
Hit
p(yes = 0.105, no =0.895)

EAMS Phase I

- Completed a robust EAMS Ontology Framework
  - Provides Support for Adversary Parameterization
  - Supports “build-up” or enhancement of adversary capabilities
- Established EAMS Components Interaction Framework
- Completed Proof-of-Concept Demonstration
  - Emergent behavior (red forces action to blue force observables)
    - Ability to develop COA based on observables
  - Intent driven adversary
  - Observables that drive the scenario are captured in EAMS
  - Ability to recreate complete scenarios for future analysis

Prototype Architecture Phase II



Architecture Components

- EAMS Ontology (EO)
  - OWL based ontology
  - Describes data and semantic relationships between information necessary to support simulation of adversarial behavior.
- Adversarial Intent Engine (AIE)
  - Formerly All
  - Will generate alternative adversarial intent with probability assessments of those corresponding courses of action.
- Adversarial Knowledge Specification Language (AKSL)
  - Used to define adversaries and their capabilities from a series of lower level descriptions and general constraints.
  - Will offer descriptions of adversarial data and semantic relationships.

Architecture Components cont..

- AKSL Processor (AKSLP)
  - Interpreter to process AKSL
  - Will establish adversarial specification within a specific ontology instance
- Intelligence / Situation Processor (ISP)
  - Will convert situational information for incorporation into the EAMS Ontology instance.
  - Bulk will populate observations of battlefield situation from a Red force perspective (i.e. Observations by the Red force of operations being conducted by the Blue force.)
  - Can be used to provide real (observed) and hypothetical ("what-if") observations from multiple data sources.
  - Will support creation of "pop-up" adversaries or adversaries that appear suddenly in a battle scenario.

Architecture Components cont..

- Scenario Manager Interface (SMI)
  - Will support a two-way interface between EAMS and the SGen Scenario Manager.
  - EAMS will communicate with simulation tools via the SGen Scenario Manager.
- Adversary Action Engine (AAE)
  - Component will form the basic adversarial constructs from observables and serve as the primary interface to the AIE.
  - Will extract the EO instance of the current adversary and develop Red Force or adversary COAs
- Visualization Engine (VE)
  - Component provides interface capabilities for analysts to view various result sets.
  - Will employ hyperbolic view capabilities from Securboration's UPSYS program.

Key Concepts Validated in Phase I

- Adversarial modeling with a system focus on Emergent behavior
- Selectable adversary intent
- Ability to maintain current status of observables in the SMI
- Demonstrated the relationships between observables, axioms, beliefs to support the generation of candidate actions and goals
- Logging of interaction to support play back analysis
- Algorithm/method for generating BKFs from Ontology/KB
- Base probabilities of red capabilities change as red units/assets change
- Systematic mechanism for parameterization / alteration of Red behavior based on soft factors

Contact and Additional Info

For additional Information contact

Lee Krause

Securboration Inc

321.591.9836

lkrause@securboration.com

Acknowledgements

The research described in this paper was funded under a Small Business Innovative Research (SBIR) grant from the Air Force Research Laboratory in Rome, NY. The Phase I award, entitled Campaign Level Adversarial Modeling System (Contract Number FA8750-04-C-0118) was completed in January of 2005. The research is currently progressing under a Phase II grant.

- Santos E. Jr., A Cognitive Architecture for Adversary Intent Inferencing: Knowledge Structure and Computation, Proceedings of the SPIE 17th Annual International Symposium on Aerospace/Defense Sensing and Controls: AeroSense 2003, Orlando, FL, 2003.
- Santos E. Jr. and Negri A., Constructing Adversarial Models for Threat Intent Prediction and Inferencing,Proceedings of the SPIE Defense & Security Symposium, Vol. 5423, Orlando, FL 2004.
- Fayette D.F, 2001, Effects-Based Operations: Application of New Concepts, Tactics, and Software Tools Support the Air Force Vision for Effects-Based Operations, AFRL Technology Horizons, Available at:
- http://www.afrlhorizons.com/Briefs/June01/IF00015.html.
- Surman J., Hillman R. and Santos E. Jr., 2003, Adversarial Inferencing for Generating Dynamic Adversary Behavior, Proceedings of the SPIE 17th Annual International Symposium on Aerospace/Defense Sensing and Controls: AeroSense 2003, Orlando, FL. 2003.
- Grabo C.M., 2002, Anticipating Surprise: Analysis for Strategic Warning. (ed) Goldman J., Center for Strategic Intelligence Research, Joint Military Intelligence College.
- Gilmour D., Hanna J., Koziarz W., McKeever W. and Walter M., 2005, High-Performance Computing for Command and Control Real-Time Decision Support, AFRL Technology Horizons, Available at:
- http://www.afrlhorizons.com/Briefs/Feb05/IF0407.html.
- Koziarz, Walter A., Krause, Lee S., Lehman, Lynn A., "Automated Scenario Generation," SPIE 17th Annual International Symposium on AeroSense Enabling Technologies for Simulation Science, Cambridge, MA, April 21-25, 2003
- McQueary B., Krause. L., Santos E. Jr., Wang H., and Zhao Q., 2004, Modeling, Analysis and Visualization of Uncertainty in the Battlespace, 16th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2004).
- Whittaker G.M., 2000, Asymmetric Wargaming: Toward A Game Theoretic Perspective.