SE for AI: The Use of AI, and Systems Engineering Processes, in and for Testing of AI Based Systems

Dr. Craig Arndt

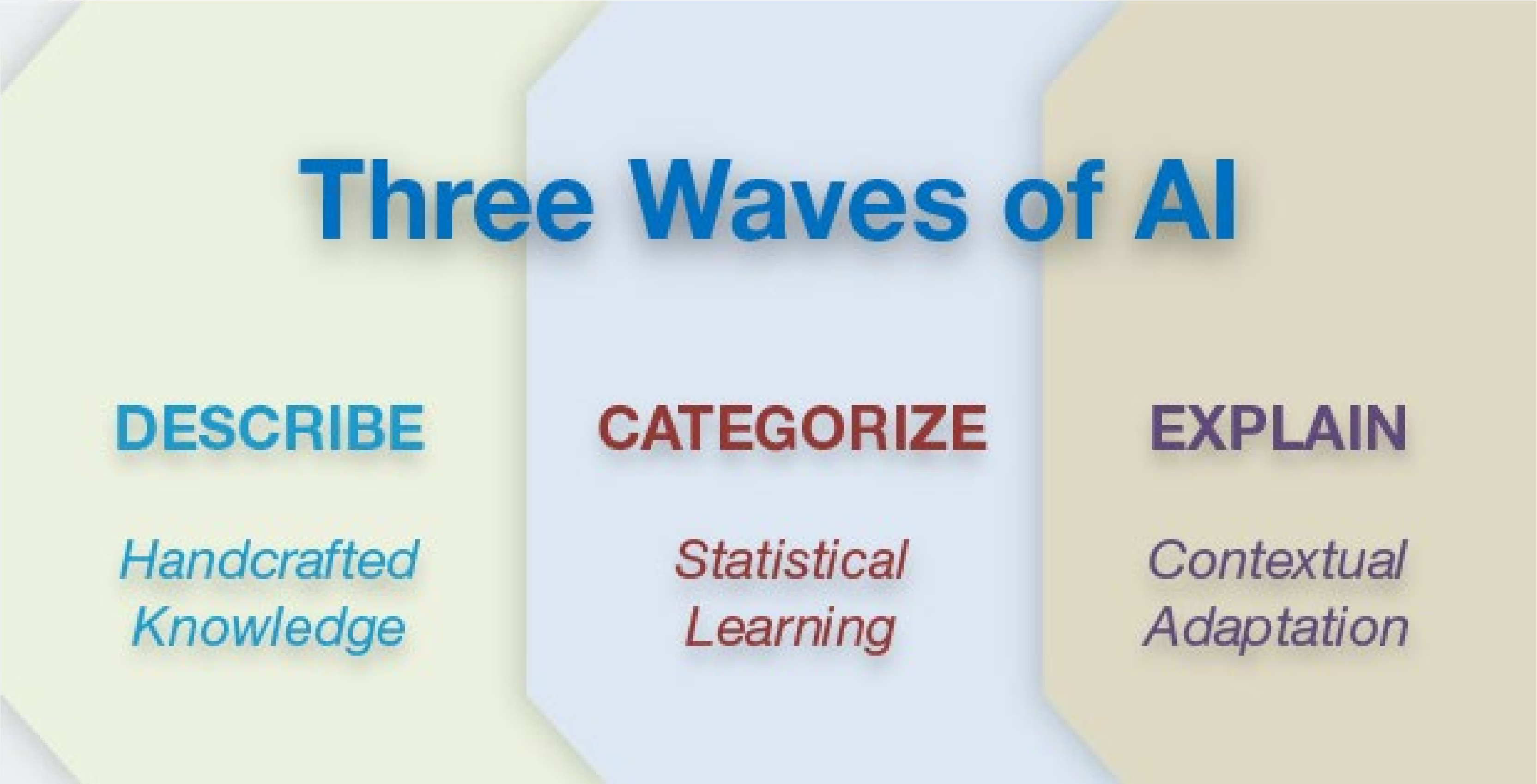
Dr. Awele Anyanhun

Agenda

- What problem are we trying to solve
- Challenges
- Requirements
- Test methods
- Model-based Systems Engineering
- Metrics
- Use Cases
- Example
- Summary
- Path forward

The advanced testing of complex system is dependent on the integration of Threat (IC), Acquisition, and Testing Models

DARPA, Perspective on AI



AI systems stresses our ability to test in a meaningful manner

UNCLASSIFIED

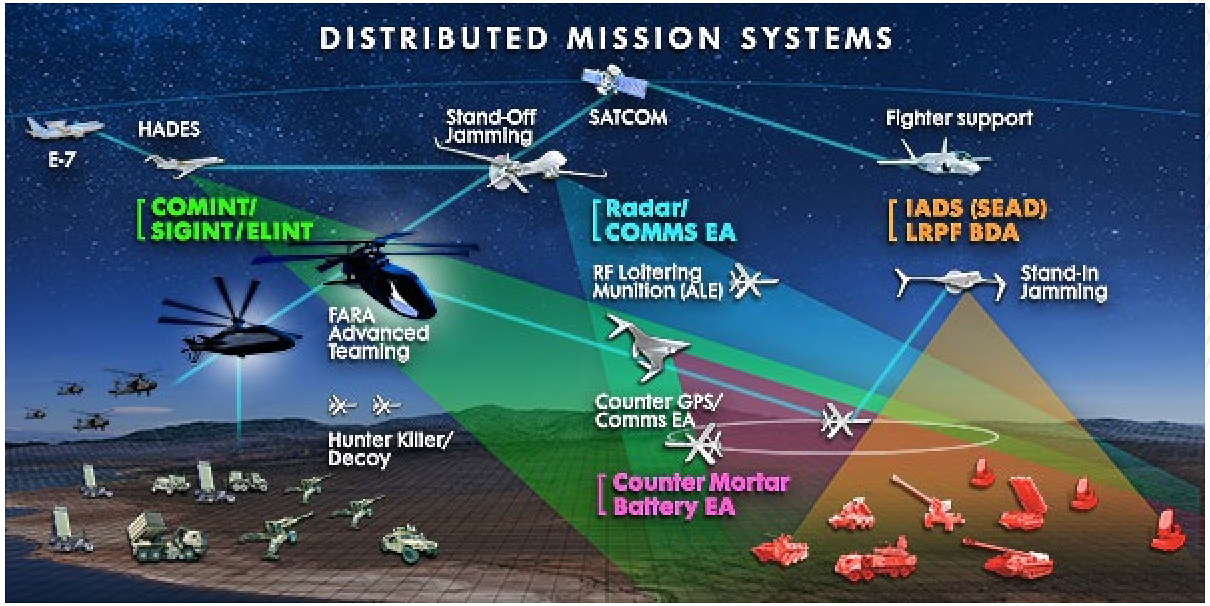
Georgia Tech Research Institute

The Current State of the Art in AI

- Statistical Learning based AI is being used extensively in the DoD on tactical and decision support applications.

- Embedded Electronic Warfare and Automated Target Recognition systems are currently challenging our ability to effectually test systems performance.

- High performance AI systems can fail in unpredictable and dramatic ways.



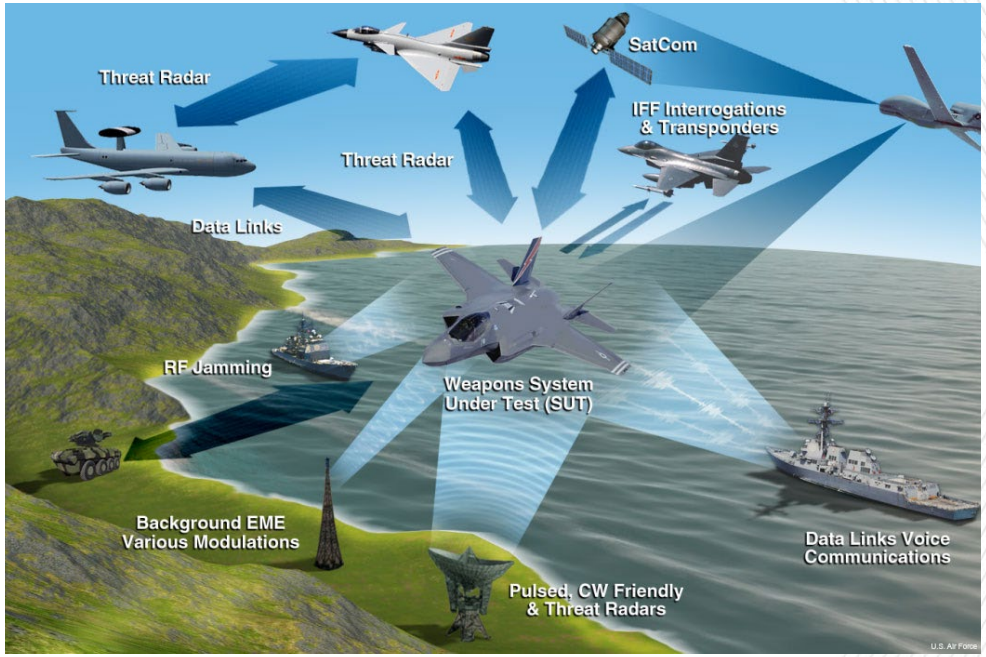
Georgia Tech Research Institute

UNCLASSIFIED

What Problem are we Trying to Solve?

- Existing Systems Engineering methods are not designed to test systems after deployment

- Testing AI based systems have requirements that are outside of the standard methods for systems engineering based on performance outside of delivered baselines.



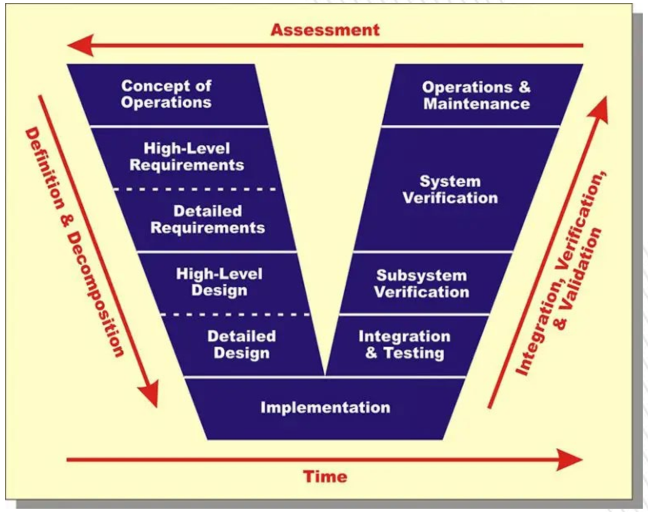
UNCLASSIFIED

Challenges

- Understanding future performance and system behavior.
- Developing effective testing of unknown future systems configurations.
- Measuring the effectiveness of future testing on unknown configurations of systems under development

Systems Engineering Methods

- Challenge: Currently implemented systems engineering methods do not allow for the development of testing for systems not defined early in the lifecycle.
- Opportunity: Change two major aspects of test. The first is change the objective of testing from validating fixed requirements to test to predict future performance of the system. The second is to create the ability and method for early testing of future unspecified configurations.
- Need: Develop new model based approaches to test in systems based on more than one future.



UNCLASSIFIED

Georgia Tech Research Institute

Requirements

- Challenge: Currently systems, including AI embedded systems, do not allow for requirements that are not deterministic

- Opportunity: Create new use cases for AI and modular program requirements (system specifications) that facilitate multiple requirements based on variable configurations linked to future threats and operating environments, and supporting early testing of these different configurations.

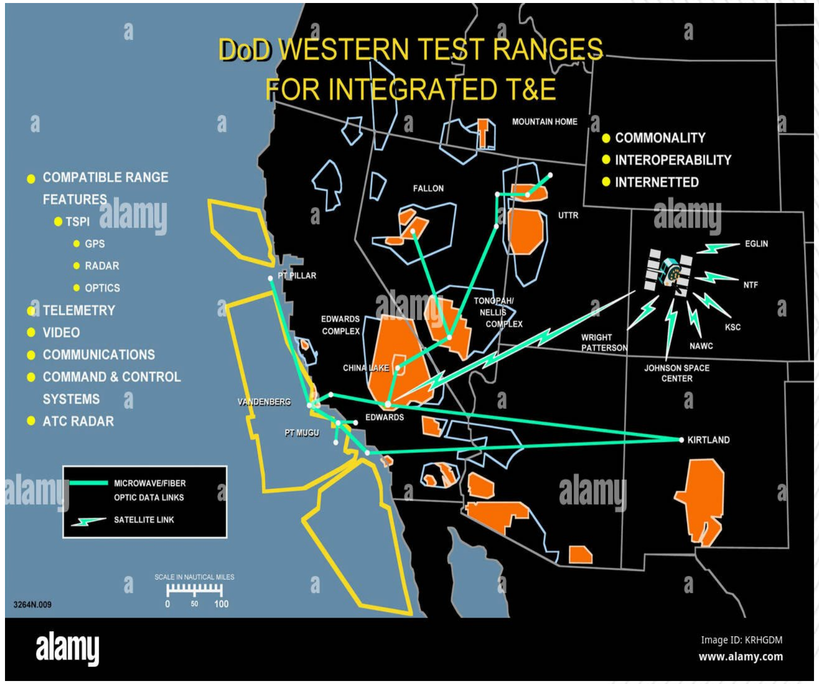
- Need: Requirements that fully represent the links to test, and tests of future systems that may or may not be implemented over time.

Testing Methods

- Challenge: AI system configurations are tested based on existing designs before they are fielded. These configurations do not represent future configurations after future updates.

- Opportunity: Expanding early testing based on future threat data and the configurations of systems.

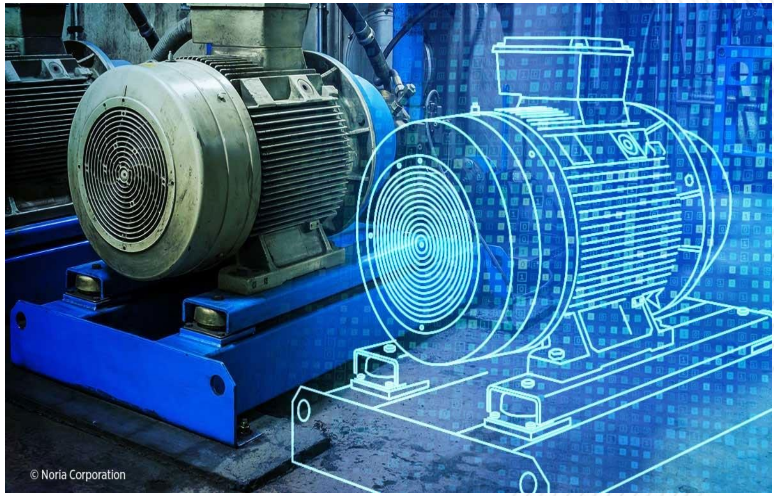
- Need: Enhanced testing methods which include
  1. Integration of IC future threat information into design and testing
  2. Simulated future threat environments
  3. Simulated training data
  4. Simulation-based AI driven systems and test configurations.



Georgia Tech Research Institute

Modeling and Simulation

- Simulation is key to the development of testing of future configurations in response to a range of possible threat environments.
- The models of the future threat environment can then be used to generate synthetic training data for the AI systems and also for the threat systems models needed to develop test cases.
- Most statistical learning based AI systems (neural networks) can be reverse engineered. The resulting systems used with predictive AI algorithms create the different versions of the future system
- Different version of Digital Twins of the system can then be tested in simulations of future threat environments.



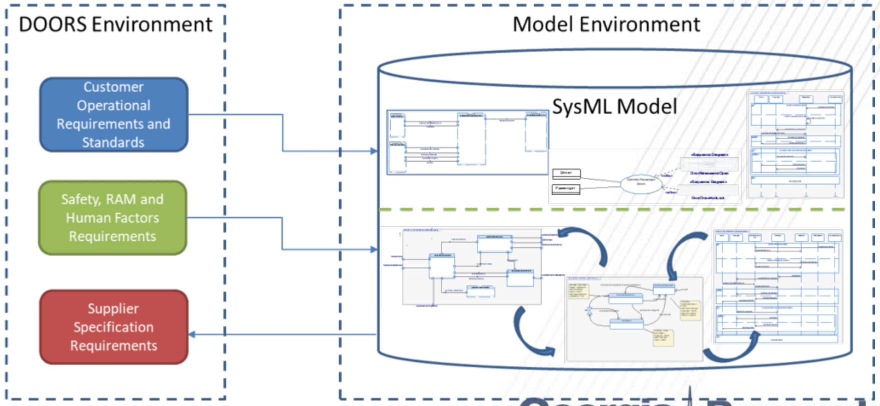
UNCLASSIFIED
Georgia Tech Research Institute

Model-based Systems Engineering

- Challenge: MBSE allows for the movement of data across system boundaries. To support AI testing we need to also move data across time.

- Opportunity: By using MBSE as the framework we can insert technology including AI based predictive analysis to predict training sets and performance of future embedded AI systems.

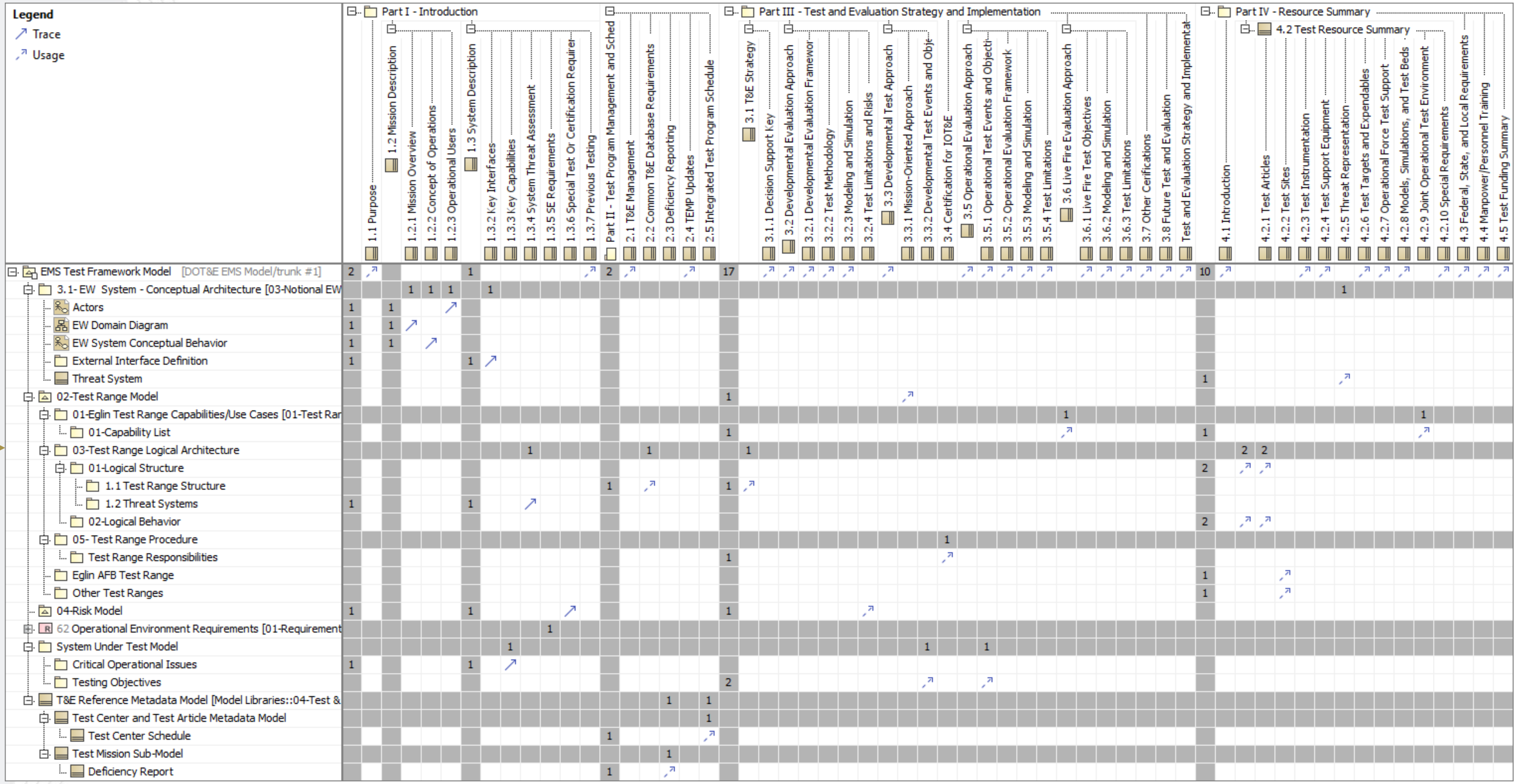
- Need: In order to facilitate the ability to move data across both tasks and different parts of the lifecycle we need to integrate models across threat modeling, development and test.



Georgia Tech Research Institute

TEMP Content Areas- Mapping of TEMP content areas to a test-integrated framework. (U)

Test-Integrated Framework

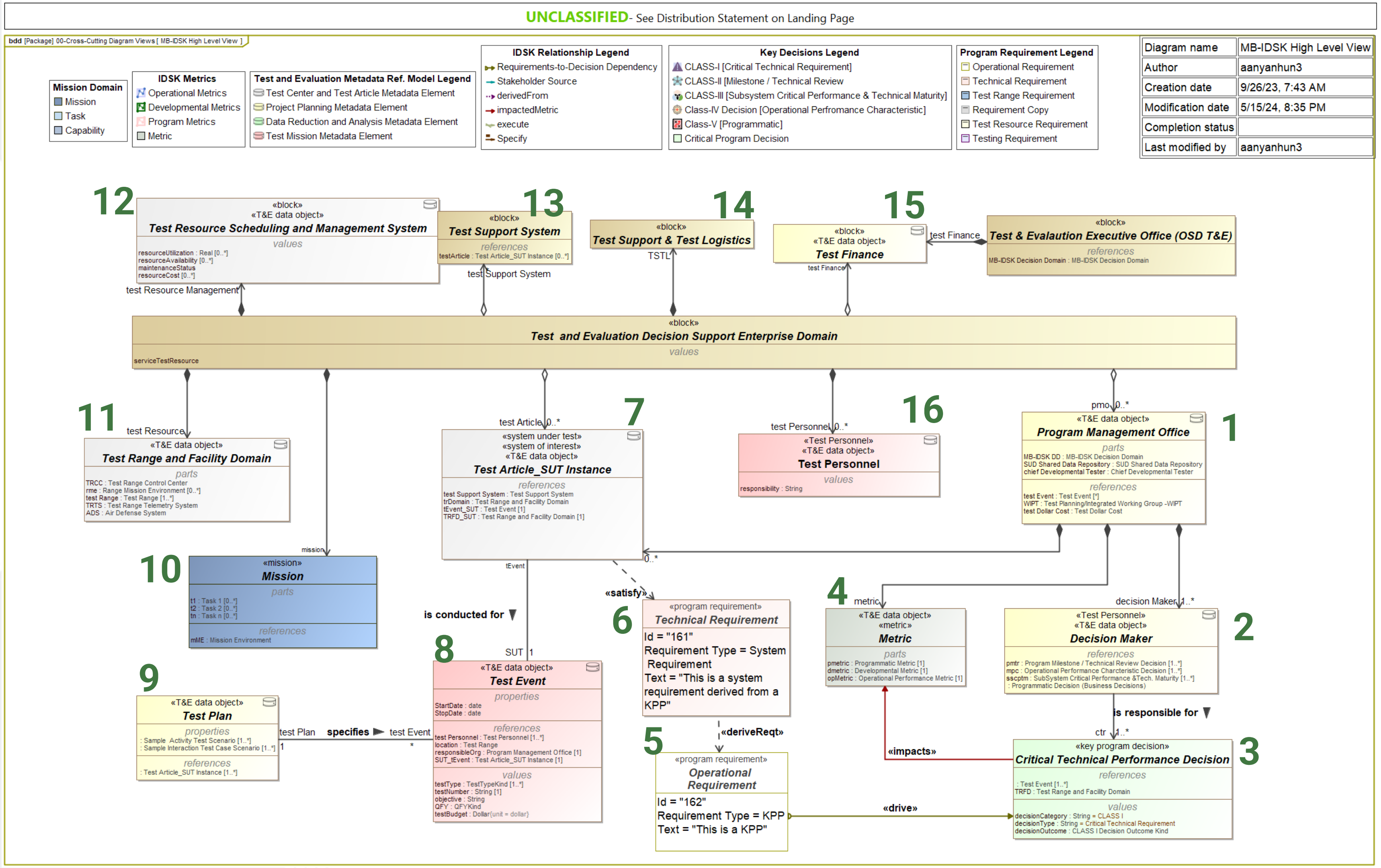


TEMP Content Areas

UNCALSSIFIED

Georgia Tech Research Institute

Top-level IDSK view portraying only key IDSK elements.(U)



UNCALSSIFIED

IDSK Elements:

1. Program Office
2. Decision Authority
3. Decision
4. Metrics
5. Operational Requirement
6. Technical Requirement
7. Test Article
8. Test Event
9. Test Plan
10. Mission
11. Test facility
12. Test Resource & Sch System
13. Test Support System
14. Test Support Logistics
15. Test Finance
16. Test Personnel

Metrics

- Challenge: Current testing metrics are based on designing test around validation of performance to a specific requirement.
- Opportunity: To change the way we look at test from verifying performance to predicting future performance of the system.
- Need: Develop knowledge-based metrics that support an understanding of our level of knowledge of the system.

Future metrics models for modeling of Knowledge of acquisition

- **For specific decisions at milestones we look at the**

$$K_{S\,D\,N} = \sum_{1}^{N} \Delta\,(K_{D\,N\,meastured} - K_{D\,N\,expected})$$

$K_{S\,D\,N}$ is the knowledge of the system at a given decision point (D) cross a range of different aspects of the system (N)

$(K_{D\,N\,meastured} - K_{D\,N\,expected})$ is the difference between the knowledge of the system that we have at a given decision point and the level knowledge that is needed (expected) in order to make the decision

- **In order to evaluate the value of specific tests, or sets of tests to support decisions.**

$$\Delta K_S = \sum_{1}^{N\,test} K_{S\,Ntest}\, P_N R_N$$

R_N is the set of requirements 1-N
P_N are the different performance factors 1-N for the tests

- **Then we describe risk as**

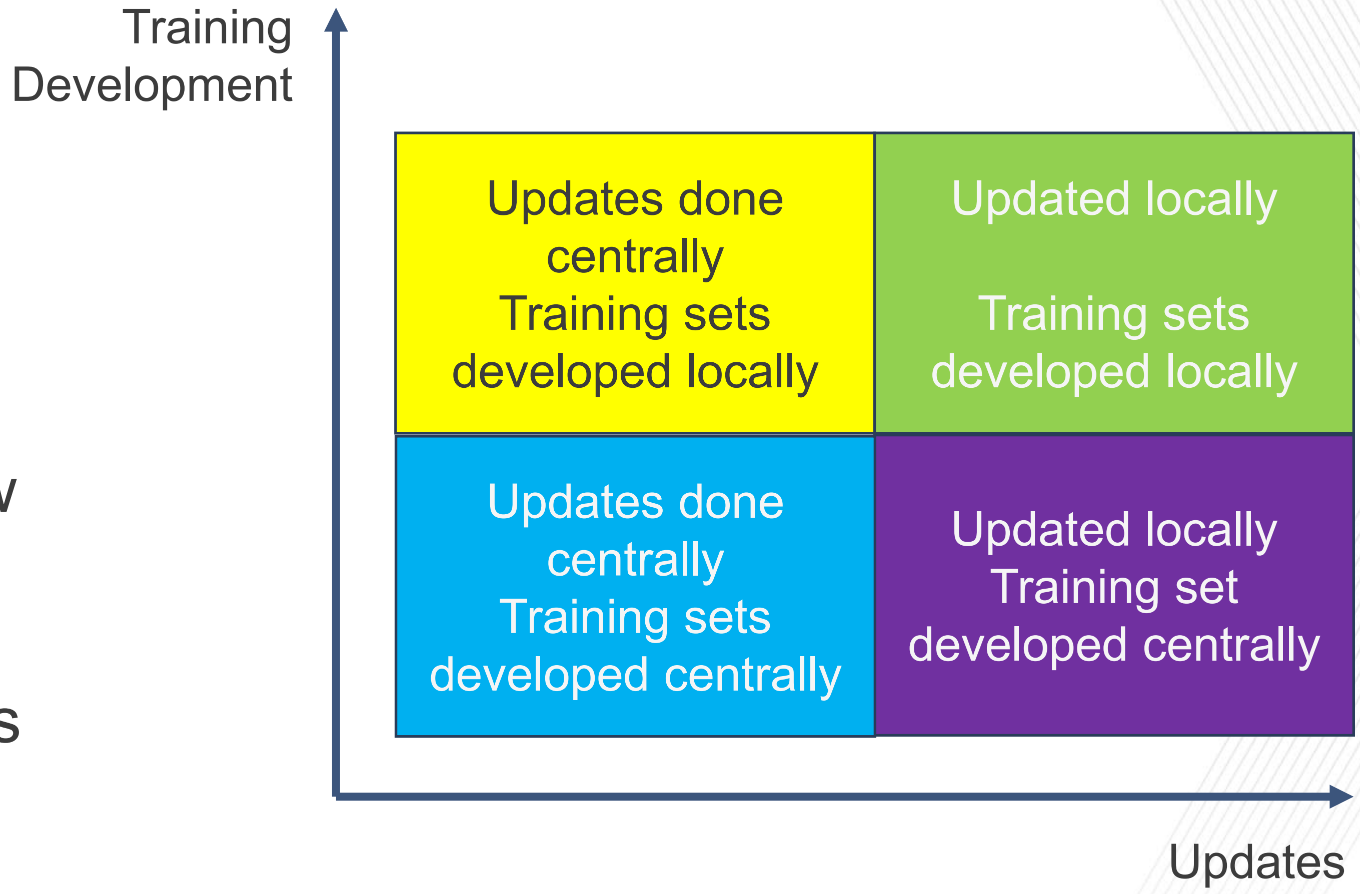
$$Min\ Risk = Max \sum_{1}^{N} K_{S\,R\,N}$$

$K_{S\,R\,N}$ is the knowledge of the system associated with specific risks.

Use Cases

- There are four major use cases for the implementation of statistical learning AI systems.

- The use cases are based on how the new data for training is collected and training is done, and where and when the updates to the functional software is made.

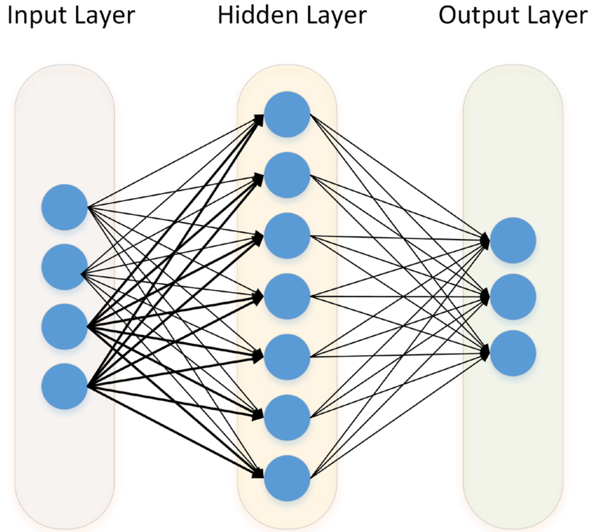


UNCLASSIFIED

Georgia Tech Research Institute

Example: Automatic Targeting System (ATR) Statistical learning (Trained Neural Network)

- A major example of Statistical learning system.
- The ATR is based on a trained Neural Net image processing system
- Future network configurations will be based on new threats introduced into the environment.
- The future threats, and environment will be documented by the IC community
- The system will be updated to target the new threats based on new training data based on images of the threat in the environment (Tanks in the woods).
- By pulling the digital thread from the future threat assessment through the design of the system using new training data based on the new threat, test cases for future configurations of the system can be developed.



UNCLASSIFIED

Example

Base Line Design

Future threats

Modeling and simulation

Training data

New Targeting systems

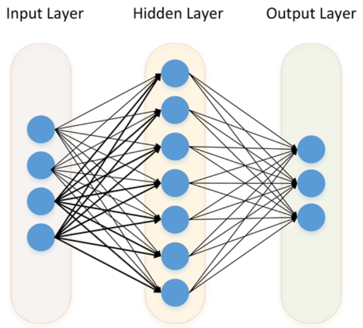
Test cases

Possible new Designs

Threat

Environment

Network



Georgia Tech Research Institute

Summary

- The testing of AI-based systems is a real and growing challenge.
- Testing of unknown future configurations of AI based systems require new methods to reduce risk.
- Introducing Model based design, threat analysis and testing will allow for greater visibility and flexibility to test future configurations.
- New Metrics of Knowledge gained in testing will be needed to manage the testing of future systems.
- Predictive modeling using other AI systems will allow for testing of future configurations based on multiple predicted training data sets.
- Model Based Systems Engineering will support incremental testing of different future systems.

Path forward

- Implement MBSE tools across the Lifecycle
  - IC Future Threat systems
  - Acquisition Systems
  - Test planning and execution (TEMP)
- Embed AI predictive models into test planning
- Develop next generation Acquisition Knowledge metrics
- Demonstrate the value of early testing of future configurations of AI embedded systems
  - Faster development
  - Higher confidence in utility of systems once deployed
  - Knowledge of future performance, guiding early design