34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

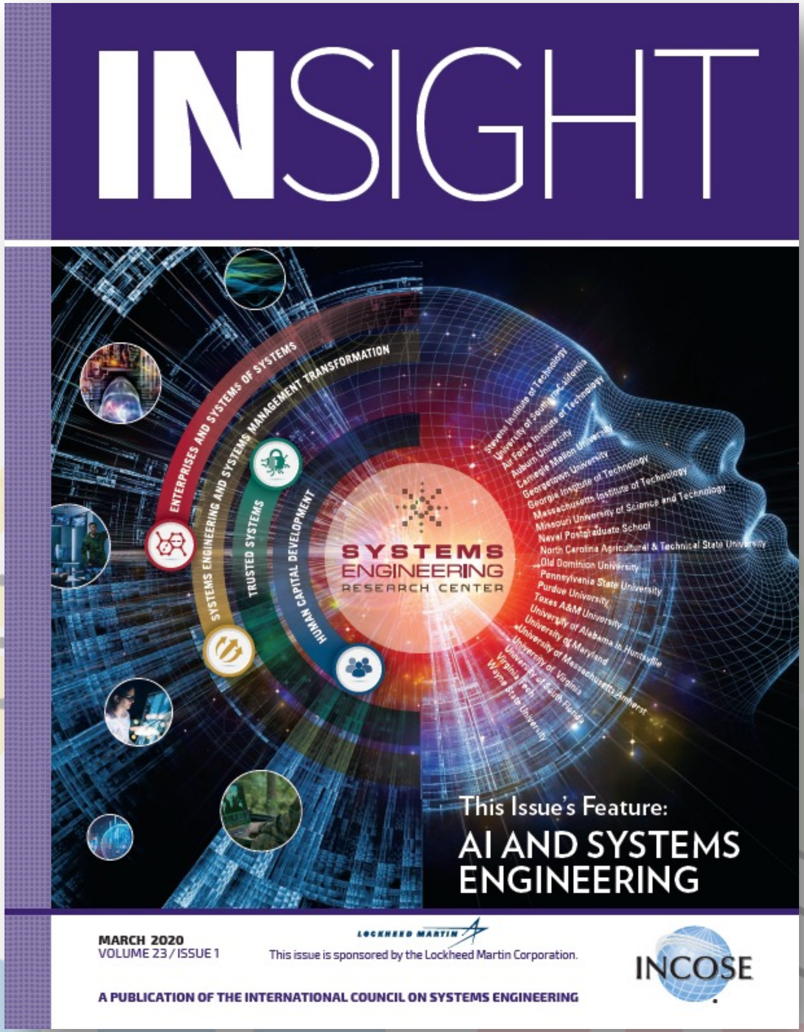
Tom McDermott

The Updated SERC AI and Autonomy Roadmap

SYSTEMS ENGINEERING RESEARCH CENTER

AIRC ACQUISITION INNOVATION RESEARCH CENTER

Initial SERC AI & Autonomy Roadmap


INSIGHT
SYSTEMS ENGINEERING RESEARCH CENTER
ENTERPRISES AND SYSTEMS OF SYSTEMS
SYSTEMS ENGINEERING AND SYSTEMS MANAGEMENT TRANSFORMATION
TRUSTED SYSTEMS
HUMAN CAPITAL DEVELOPMENT

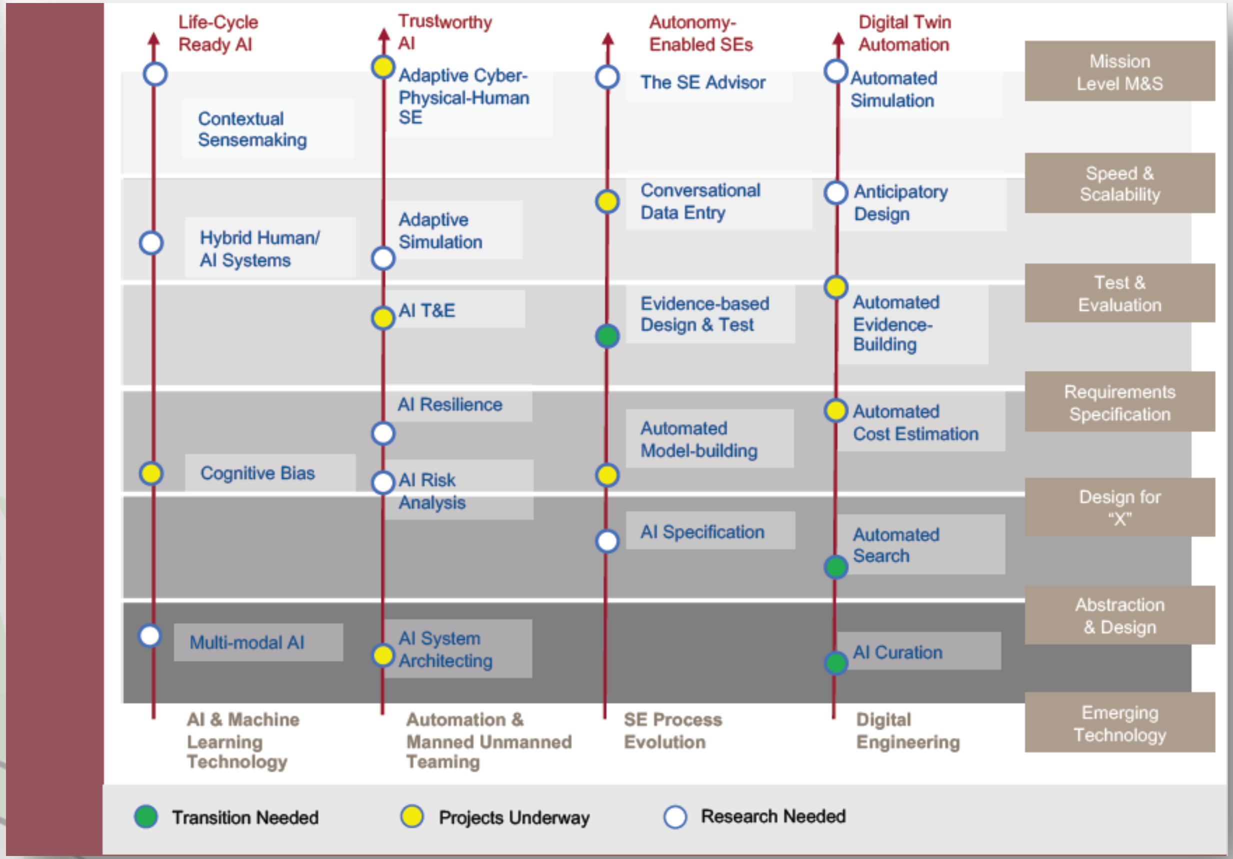
This Issue's Feature:
AI AND SYSTEMS ENGINEERING

MARCH 2020
VOLUME 23 / ISSUE 1

LOCKHEED MARTIN
This issue is sponsored by the Lockheed Martin Corporation.

INCOSE

A PUBLICATION OF THE INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING



Life-Cycle Ready AI: Contextual Sensemaking; Hybrid Human/AI Systems; Cognitive Bias; Multi-modal AI — AI & Machine Learning Technology

Trustworthy AI: Adaptive Cyber-Physical-Human SE; Adaptive Simulation; AI T&E; AI Resilience; AI Risk Analysis; AI System Architecting — Automation & Manned Unmanned Teaming

Autonomy-Enabled SEs: The SE Advisor; Conversational Data Entry; Evidence-based Design & Test; Automated Model-building; AI Specification — SE Process Evolution

Digital Twin Automation: Automated Simulation; Anticipatory Design; Automated Evidence-Building; Automated Cost Estimation; Automated Search; AI Curation — Digital Engineering

Mission Level M&S

Speed & Scalability

Test & Evaluation

Requirements Specification

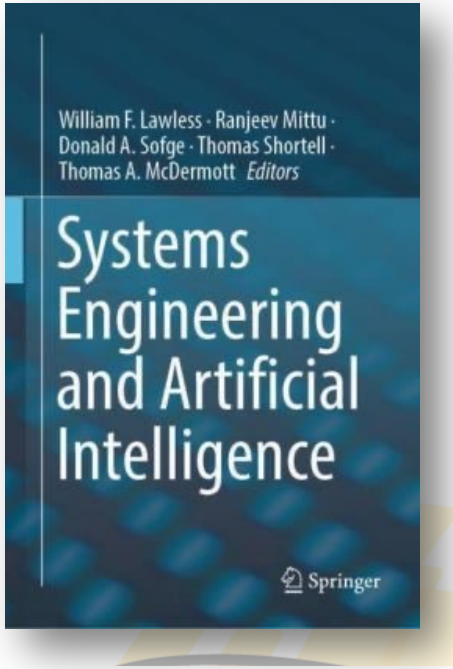
Design for "X"

Abstraction & Design

Emerging Technology

● Transition Needed ● Projects Underway ○ Research Needed

Second SERC AI & Autonomy Roadmap



William F. Lawless · Ranjeev Mittu · Donald A. Sofge · Thomas Shortell · Thomas A. McDermott *Editors*

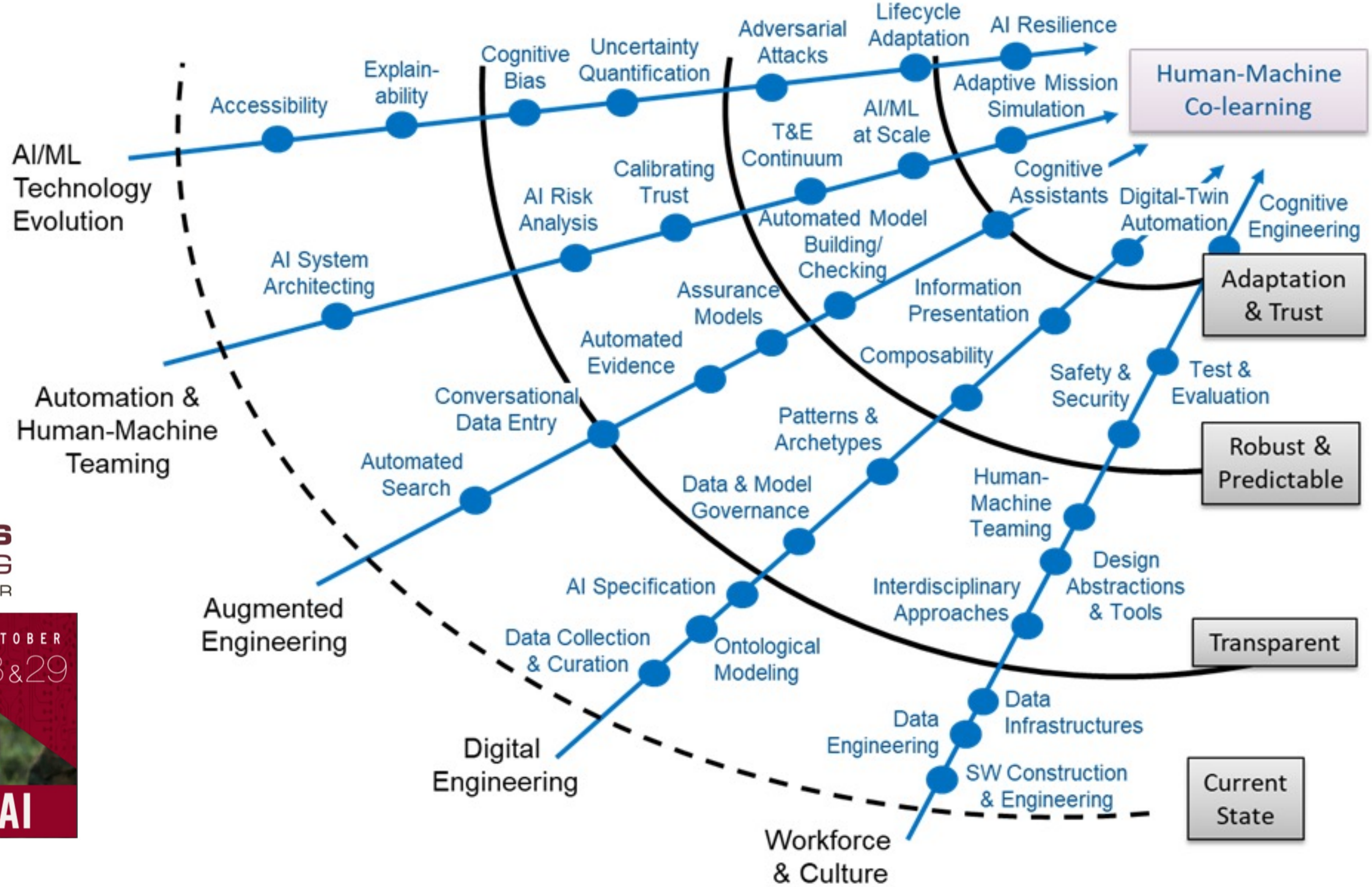
Systems Engineering and Artificial Intelligence

Springer

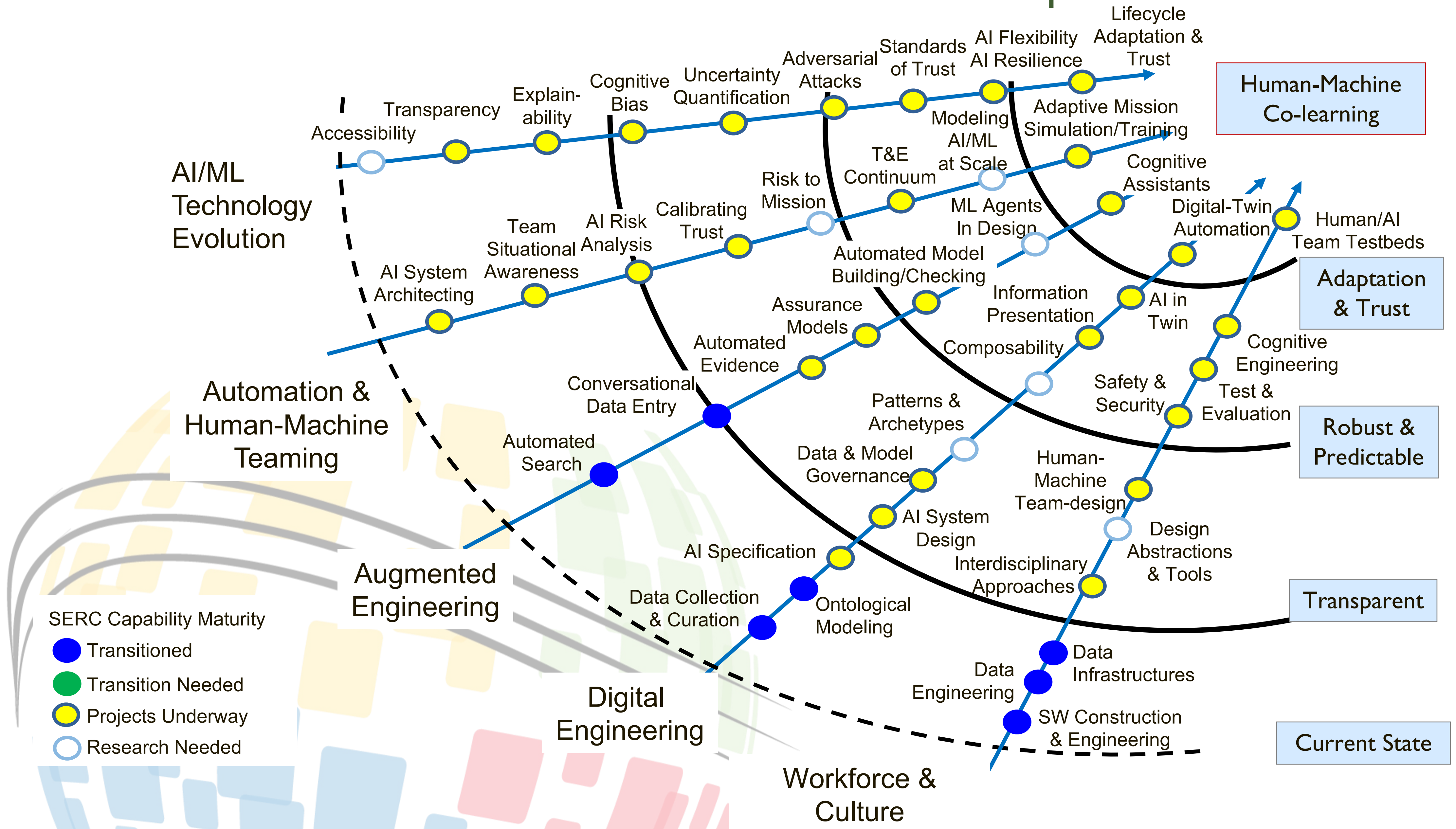
SYSTEMS ENGINEERING RESEARCH CENTER

OCTOBER 28 & 29

RESEARCH WORKSHOP: AI *for* SE & SE *for* AI



2024 SERC SE4AI/AI4SE Research Roadmap



AI/ML Technology Evolution

Accessibility

Transparency

Explainability

Cognitive Bias

Uncertainty Quantification

Adversarial Attacks

Standards of Trust

AI Flexibility AI Resilience

Lifecycle Adaptation & Trust

AI System Architecting

Team Situational Awareness

AI Risk Analysis

Calibrating Trust

Risk to Mission

T&E Continuum

Modeling AI/ML at Scale

Adaptive Mission Simulation/Training

Automation & Human-Machine Teaming

Automated Search

Conversational Data Entry

Automated Evidence

Assurance Models

Automated Model Building/Checking

ML Agents In Design

Cognitive Assistants

Augmented Engineering

Digital Engineering

Data Collection & Curation

Ontological Modeling

AI Specification

AI System Design

Data & Model Governance

Patterns & Archetypes

Composability

Information Presentation

AI in Twin

Digital-Twin Automation

Workforce & Culture

SW Construction & Engineering

Data Engineering

Data Infrastructures

Interdisciplinary Approaches

Design Abstractions & Tools

Human-Machine Team-design

Safety & Security

Test & Evaluation

Cognitive Engineering

Human/AI Team Testbeds

Human-Machine Co-learning

Adaptation & Trust

Robust & Predictable

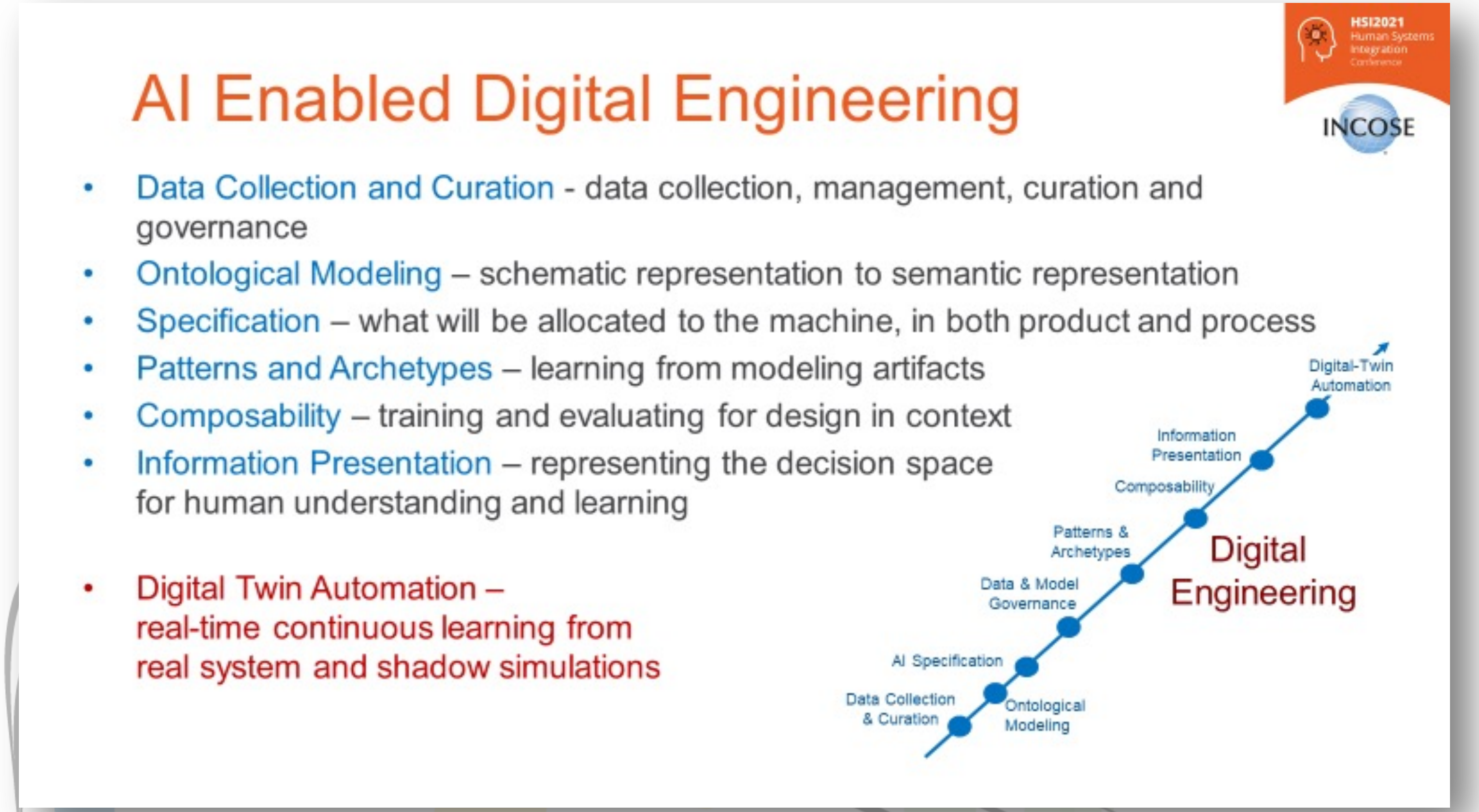
Transparent

Current State

SERC Capability Maturity

- ● Transitioned
- ● Transition Needed
- ● Projects Underway
- ○ Research Needed

Digital Engineering Transformation



AI Enabled Digital Engineering

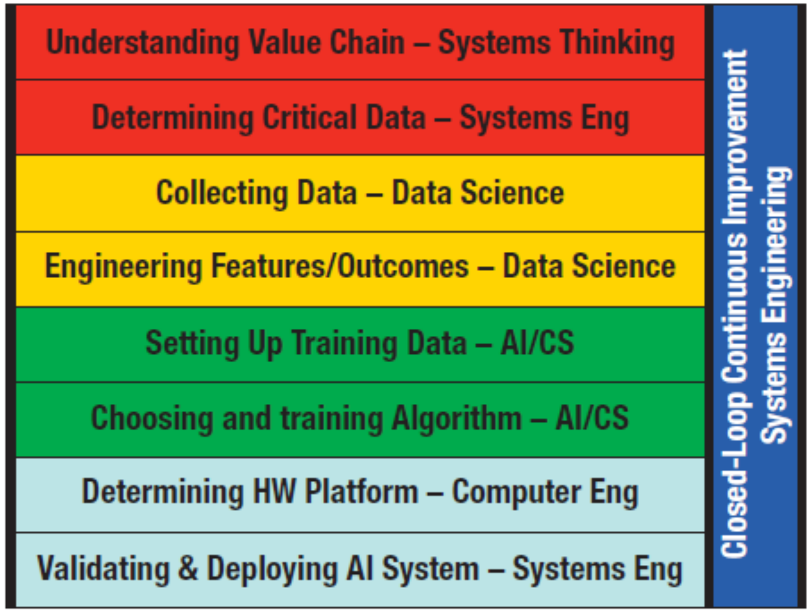
- Data Collection and Curation - data collection, management, curation and governance
- Ontological Modeling – schematic representation to semantic representation
- Specification – what will be allocated to the machine, in both product and process
- Patterns and Archetypes – learning from modeling artifacts
- Composability – training and evaluating for design in context
- Information Presentation – representing the decision space for human understanding and learning

- Digital Twin Automation – real-time continuous learning from real system and shadow simulations

- Convergence of Data Science and Systems Engineering Disciplines
- Models become central to defining complex systems of systems
- Results in Product plus Virtual Twins of Product
- Human-Machine interfaces and Visualization of complex interrelationships

Start with Workforce and Culture

- Digital Engineering Competencies
- Integrating AI/ML experts with Domain experts, all disciplines
- Evolving tools to align with design and disciplinary abstractions =>
- Human Systems Engineering: no longer a specialty discipline



Understanding Value Chain – Systems Thinking

Determining Critical Data – Systems Eng

Collecting Data – Data Science

Engineering Features/Outcomes – Data Science

Setting Up Training Data – AI/CS

Choosing and training Algorithm – AI/CS

Determining HW Platform – Computer Eng

Validating & Deploying AI System – Systems Eng

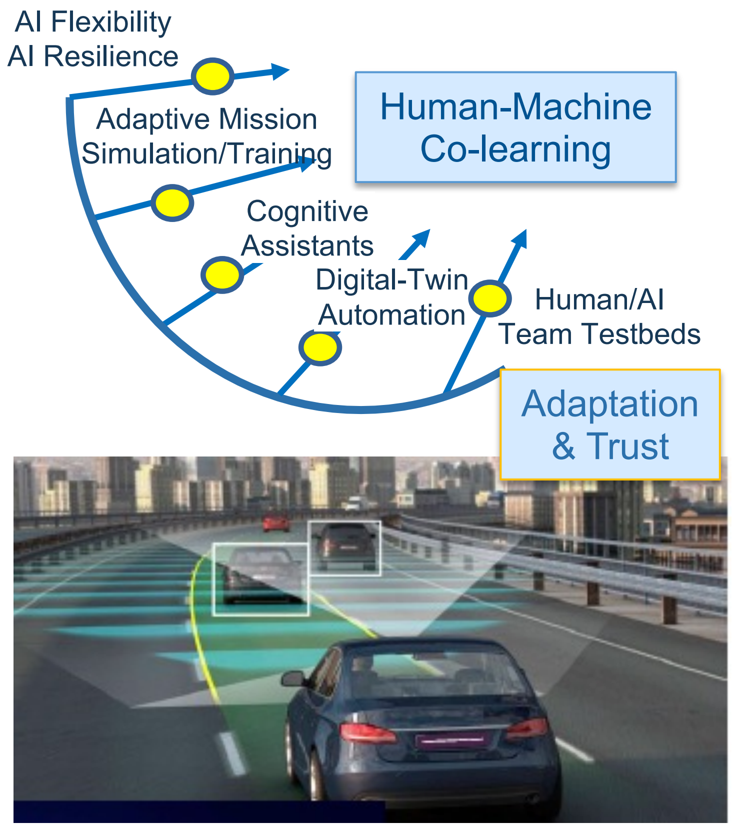
Closed-Loop Continuous Improvement Systems Engineering

Wade, J., Buenfil, J. and Collopy, P. (2020), A Systems Engineering Approach for Artificial Intelligence: Inspired by the VLSI Revolution of Mead & Conway. INSIGHT, 23: 41-47.

- Threat models, safety, security, resilience, and other ‘iliities
- Evolving test and evaluation competency
- Training the Users to appropriately interact with AI’s

HUMAN-MACHINE CO-LEARNING

- Adaptive Cyber-Physical-Human Systems – digital twins: modeling of cyber-physical systems as influenced by humans, in testbeds…
  - Adaptive Mission Simulation/Training – Simulation and training that supports non-static objectives (pick-up games)
  - AI Flexibility & Resilience – AI systems that self-adapt to changing operational boundaries while maintaining rigorous safety and security and policy constraints



AI Flexibility
AI Resilience

Adaptive Mission
Simulation/Training

Human-Machine
Co-learning

Cognitive
Assistants

Digital-Twin
Automation

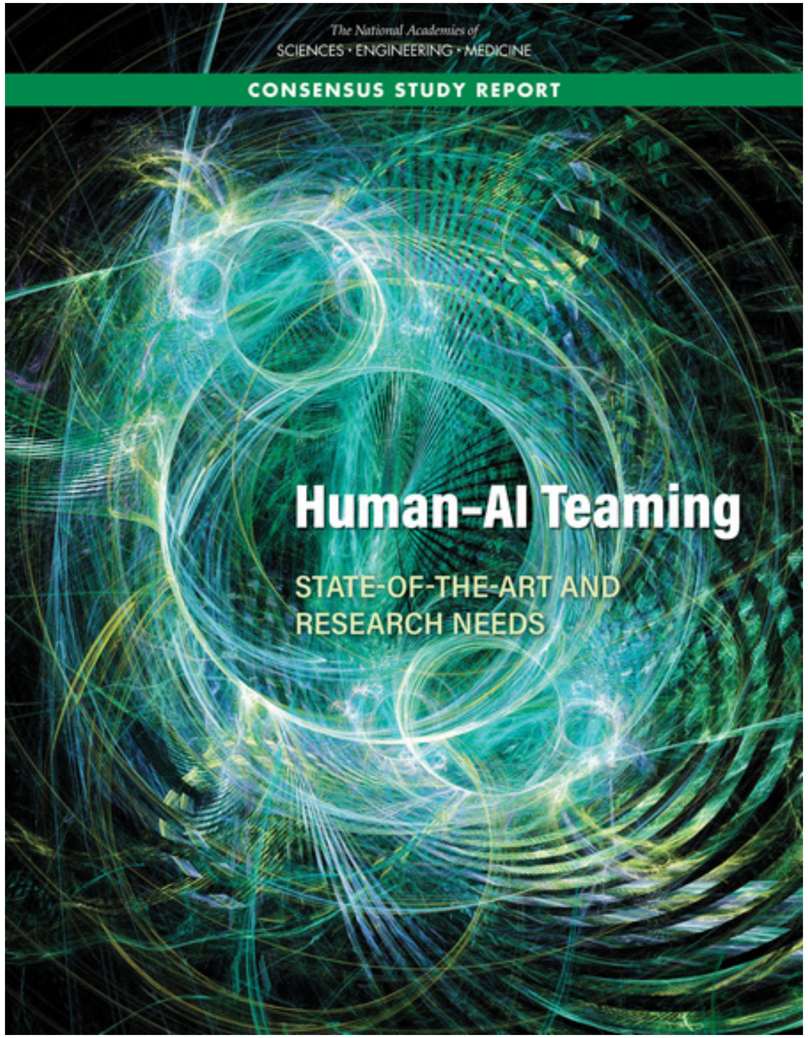
Human/AI
Team Testbeds

Adaptation
& Trust

SE/HSI Objectives

Significant value in considering the human and AI as a team

- Long-term, distributed, and agile human-AI teams through improved team assembly, goal alignment, communication, coordination, social intelligence, and the development of a new human-AI language – **AI System Architecting**
- Methods for improving human situational awareness of AI systems
- Improved AI system transparency and explainability
- **Interaction mechanisms and strategies within the human-AI team**
- Advance understanding of how broader sociotechnical factors affect trust in human-AI teams
- Better understand the interdependencies between human and AI decision-making biases
- What, when, why, and how to best train human-AI teams
- **Advances in HSI processes and measures**



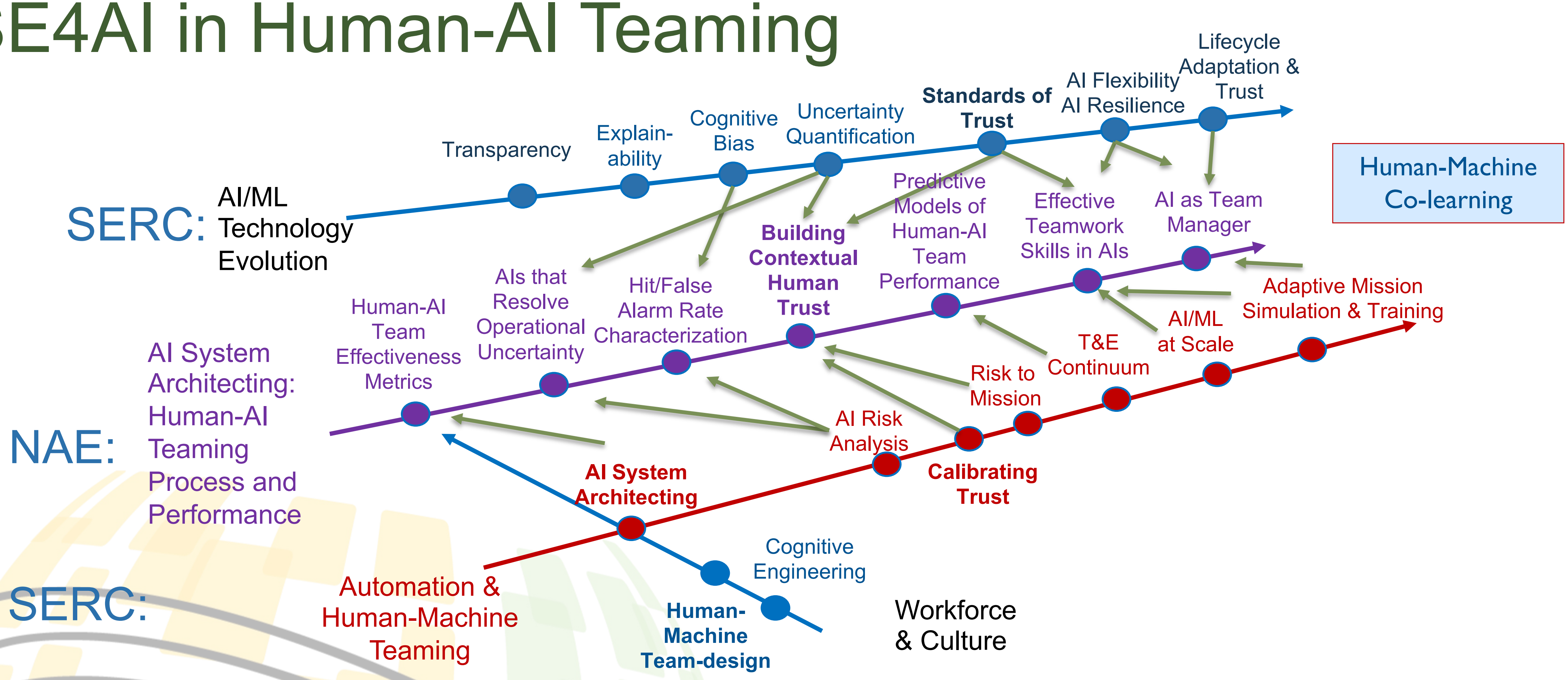
The National Academies of
SCIENCES · ENGINEERING · MEDICINE

CONSENSUS STUDY REPORT

Human-AI Teaming

STATE-OF-THE-ART AND RESEARCH NEEDS

SE4AI in Human-AI Teaming



SERC: AI/ML Technology Evolution

Transparency

Explain-ability

Cognitive Bias

Uncertainty Quantification

Standards of Trust

AI Flexibility AI Resilience

Lifecycle Adaptation & Trust

Human-Machine Co-learning

NAE: AI System Architecting: Human-AI Teaming Process and Performance

Human-AI Team Effectiveness Metrics

AIs that Resolve Operational Uncertainty

Hit/False Alarm Rate Characterization

Building Contextual Human Trust

Predictive Models of Human-AI Team Performance

Effective Teamwork Skills in AIs

AI as Team Manager

SERC: Automation & Human-Machine Teaming

AI System Architecting

AI Risk Analysis

Calibrating Trust

Risk to Mission

T&E Continuum

AI/ML at Scale

Adaptive Mission Simulation & Training

Cognitive Engineering

Human-Machine Team-design

Workforce & Culture

Human-Machine Team Design –>

AI System Architecting –>

Building Contextual Human Trust –>

Standards of Trust

New Areas of Emphasis in SE4AI Research

- Holistic view of the system of systems
- Measurement of “ilities” (e.g., flexibility, resilience, trust)
- Architecting / Human-system integration
- Product platforms / evolvability of systems of systems
- Lifecycle risk analysis
- Linking “Design for X” “T&E” and lifecycle value.
- Understanding human behavior as part of the system
- Emergent system behavior

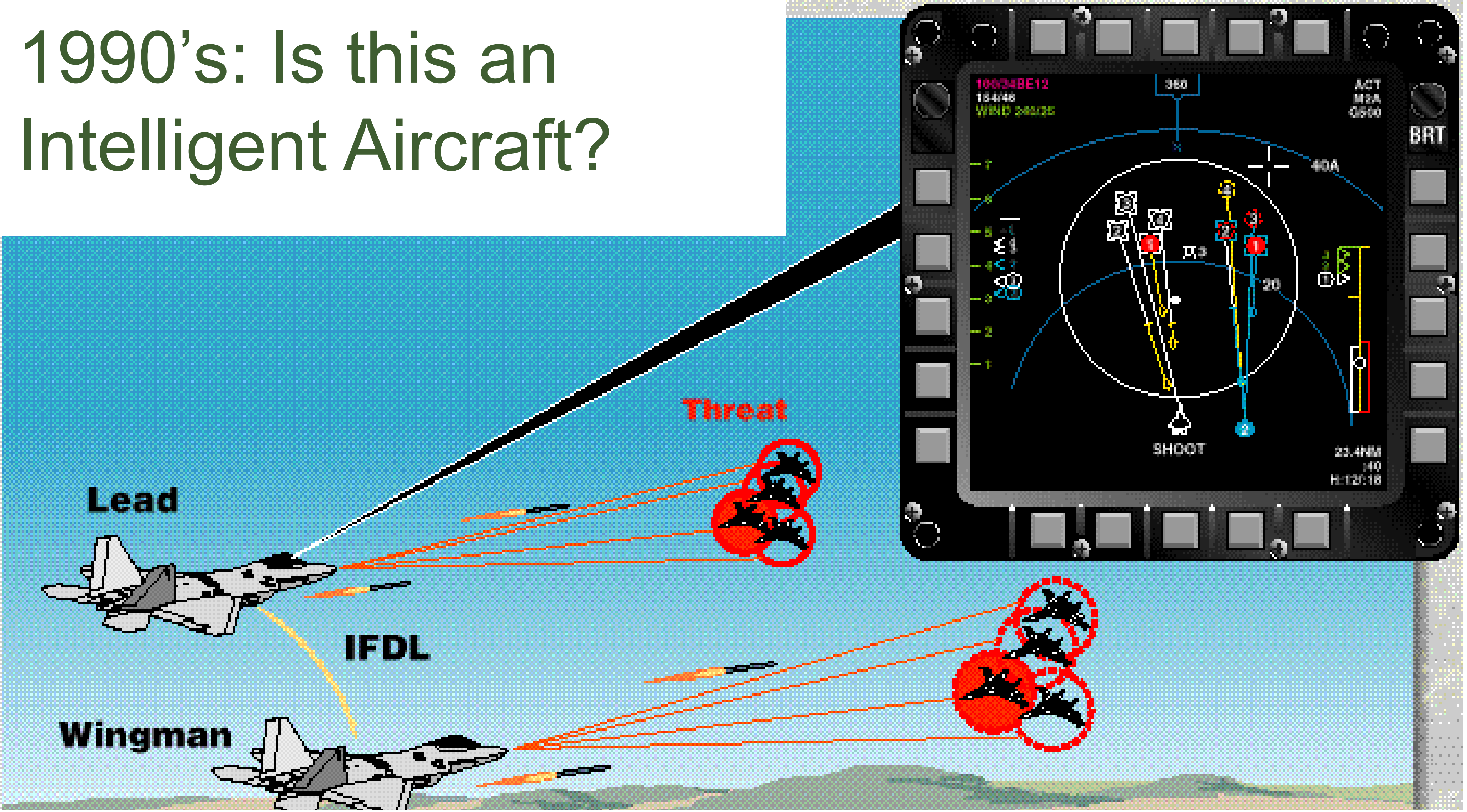
Building user Trust by understanding the Human AI system

Architecting AI Systems for long-term trust: Linking task & function allocation, test and risk analysis and need for **systems** testbeds

T&E as a Continuum: what to test and how to interpret for AI Systems of varying complexity and embeddedness

AI Resilience: Strategies to mitigate disruptions / ensure acceptable behaviors and recoveries when failures occur

1990’s: Is this an Intelligent Aircraft?



The sensor fusion loop detects threat aircraft, tracks location and movement, identifies the type, calculates an optimal engagement, even tells the pilot when to shoot. The pilot must initiate the shot. This all happens beyond the visual range of the pilot. How does the pilot trust the information provided by the sensor fusion in this critical situation?

What makes you trust (or not trust) “the AI”?

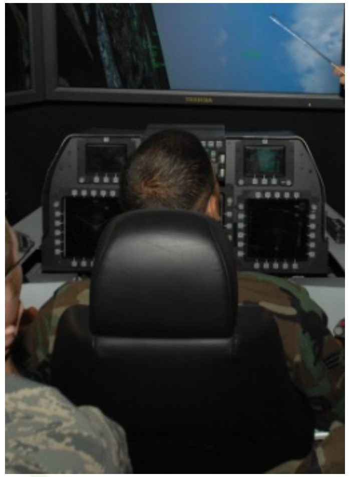
Developer

[1]

Accuracy:

If you’re a computer scientist you want to see the math of this specific algorithm or at least a visualization of the prediction.

Domain Expert



[2]

Agrees with me:

If you’re a pilot flying in an engagement using your display image, you might want to see the system agree with you often enough.

End User

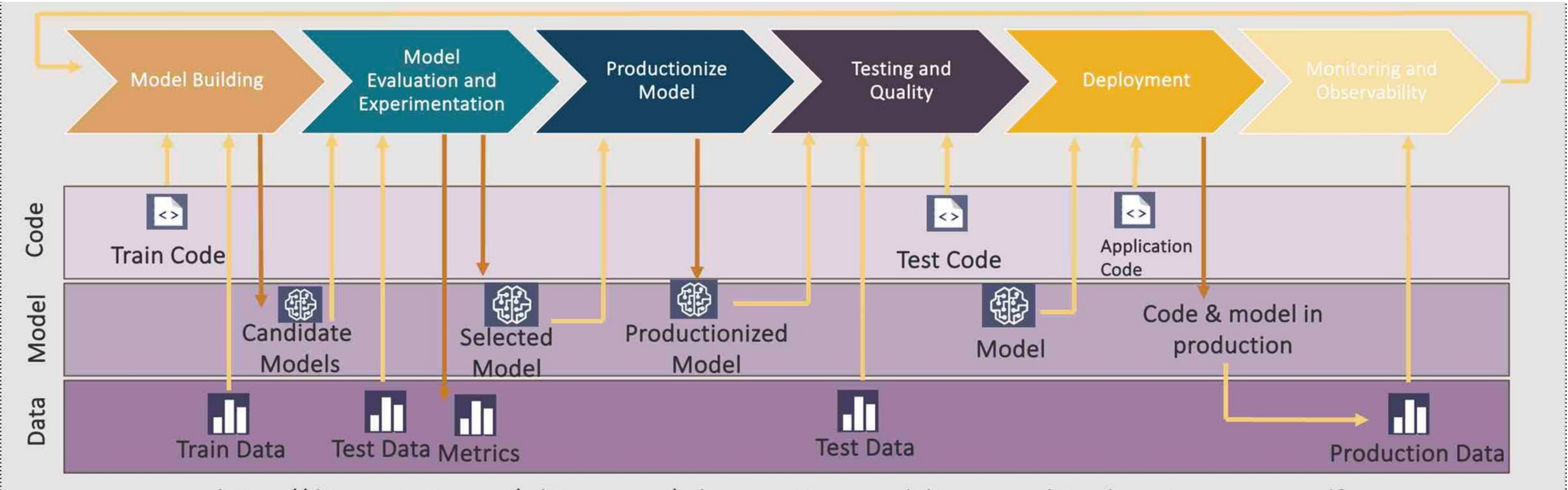
[3]

Trusted 3rd Party:

If you’re an operational evaluator, you might want to certify it’s safety…and for commanders, not have created any international incidents!

AI SYSTEMS ARCHITECTING: THE AI/ML PIPELINE TODAY

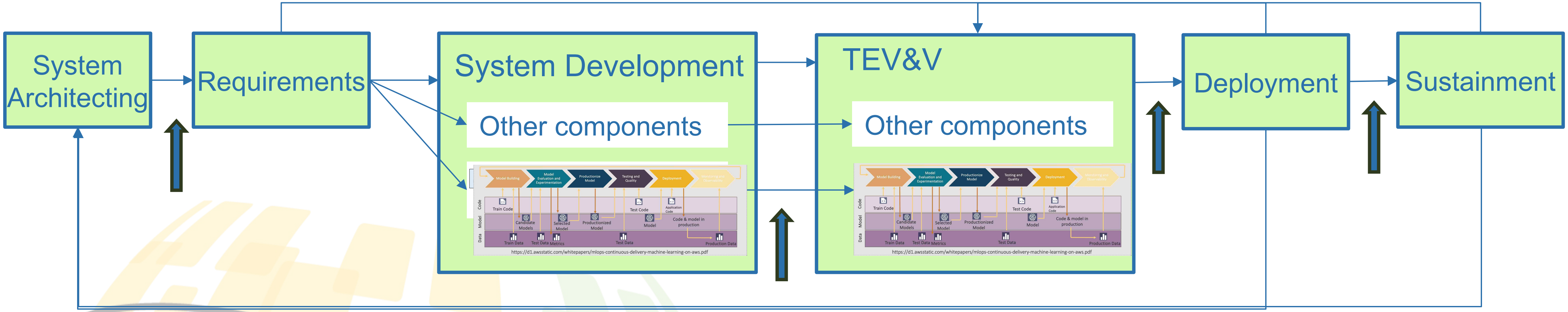
Typical representation of AI/ML pipeline:



https://d1.awsstatic.com/whitepapers/mlops-continuous-delivery-machine-learning-on-aws.pdf

… but this is still focused on the AI model as the system.

For Systems Engineers, AI is part of a “system”



System Architecting

Requirements

System Development

Other components

TEV&V

Other components

Deployment

Sustainment

https://d1.awsstatic.com/whitepapers/mlops-continuous-delivery-machine-learning-on-aws.pdf

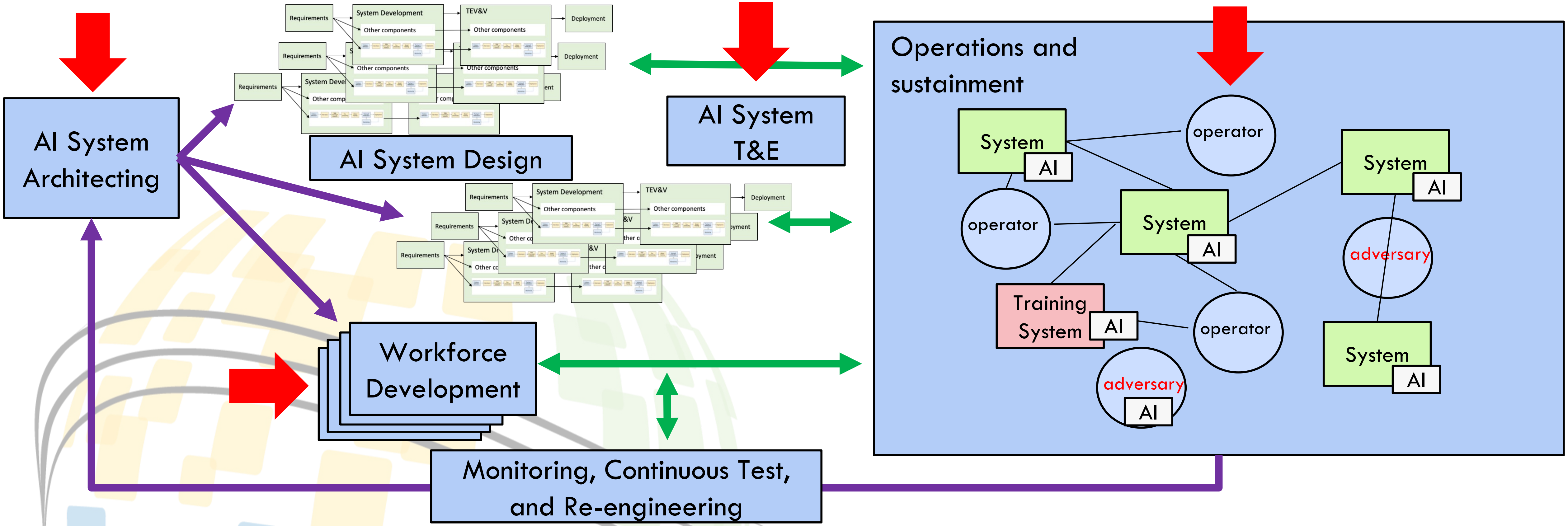
https://d1.awsstatic.com/whitepapers/mlops-continuous-delivery-machine-learning-on-aws.pdf

Emphasizes tradeoffs in performance and risk

Recognizes that system might need to work in unplanned ways over its lifecycle and that behavior (and failures) must be acceptable

The real world operates in a socio-technical systems architecture

Involving complex interactions among humans and systems that were not always intended to work together in a constantly changing environment.



AI System Architecting

AI System Design

AI System T&E

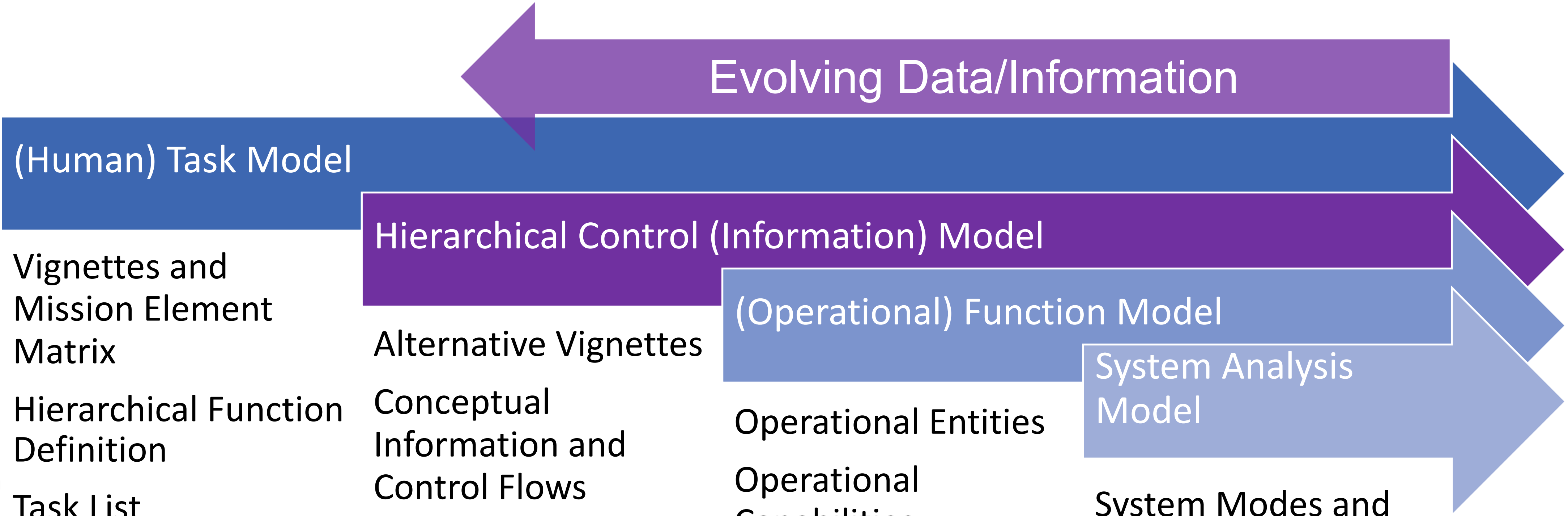
Workforce Development

Monitoring, Continuous Test, and Re-engineering

Operations and sustainment

AI in system context; Building user trust; Architecting for long-term trust; T&E as a continuum

Expanded SE modeling flow



Evolving Data/Information

(Human) Task Model

Hierarchical Control (Information) Model

(Operational) Function Model

System Analysis Model

Vignettes and Mission Element Matrix

Hierarchical Function Definition

Task List

Mission/System Narratives

Alternative Vignettes

Conceptual Information and Control Flows

Operational and System Decomposition

Operational Entities

Operational Capabilities

Operational Activities

Operational Activity Flows

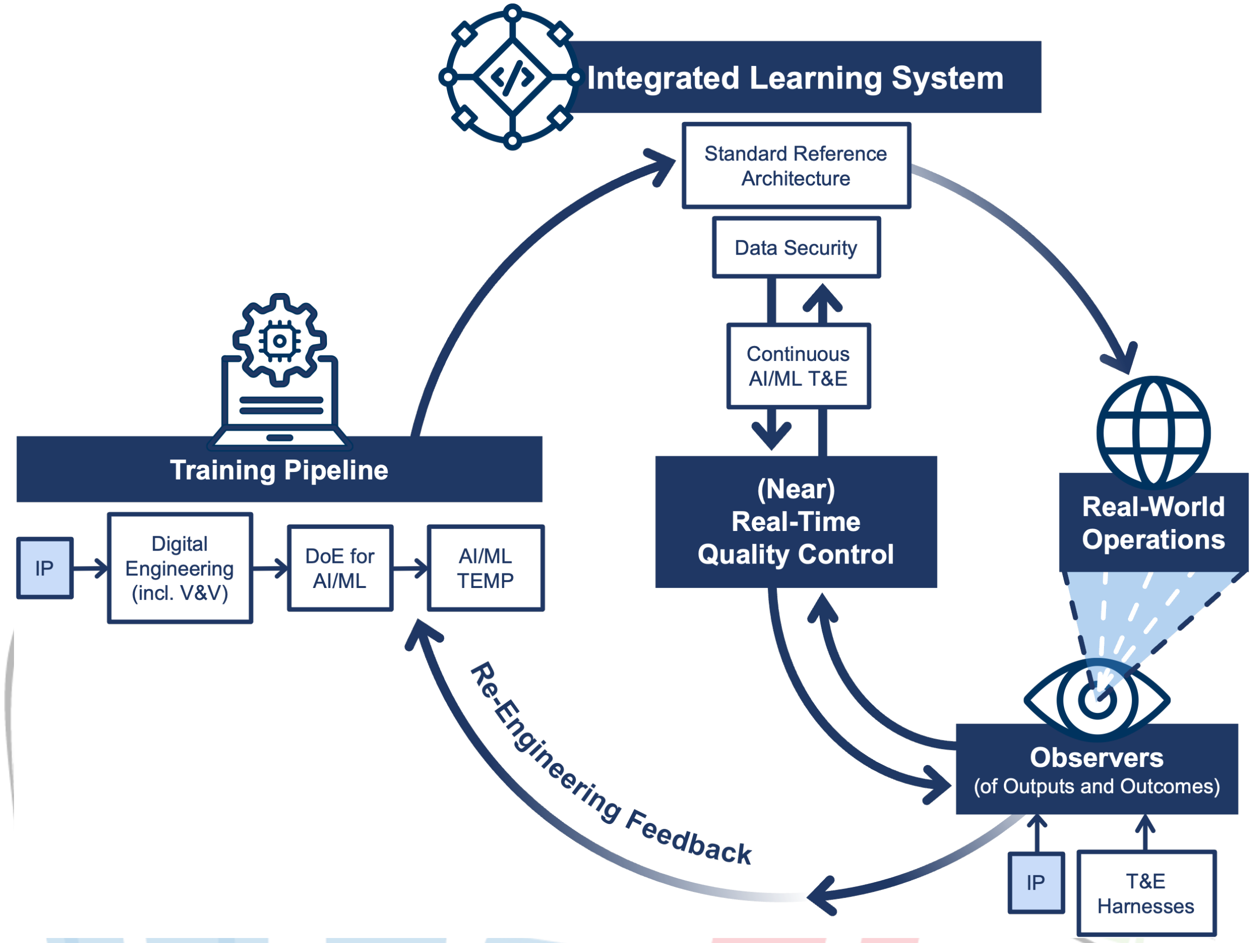
System Modes and States

System Capabilities

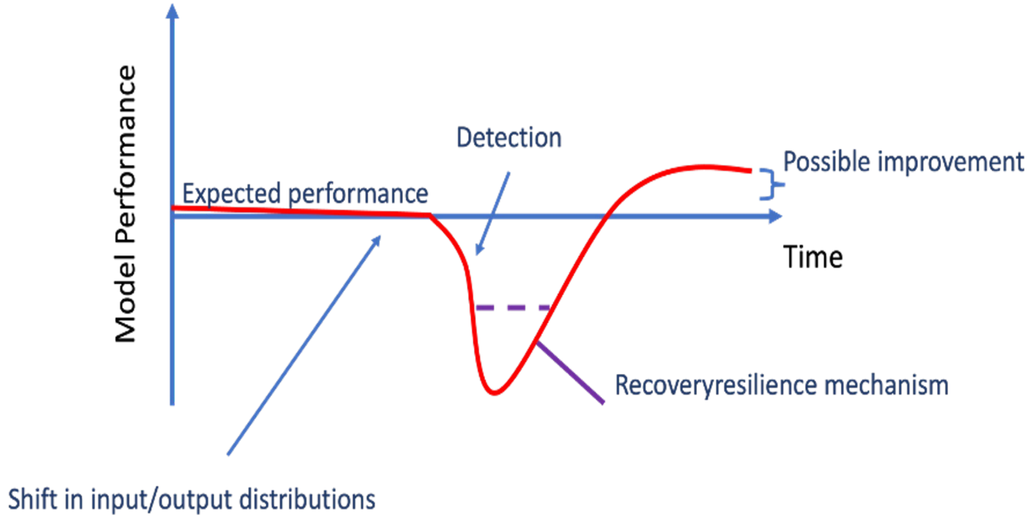
System Functions and Activities

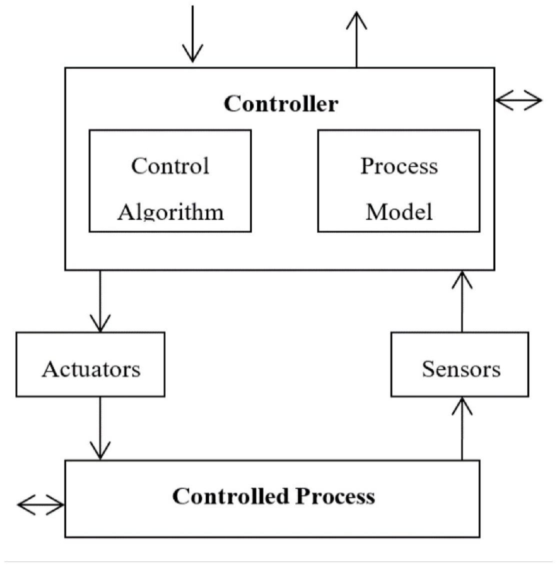
Requirements

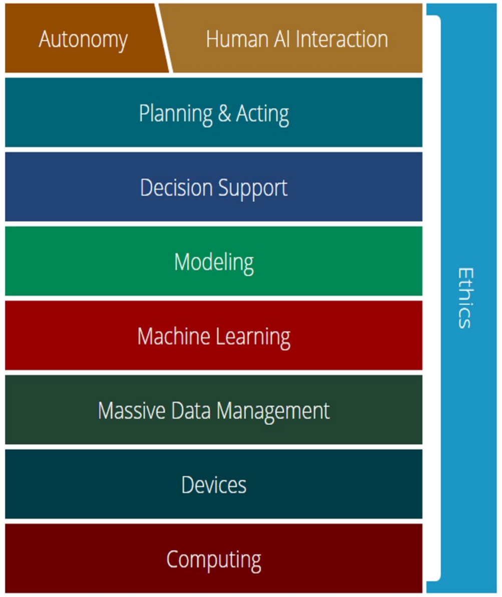
FRAMEWORK FOR AI RESILIENCE THROUGH EVALUATION OF SYSTEMS AND TECHNOLOGY (FAIREST)



Integrated Learning System
Standard Reference Architecture
Data Security
Continuous AI/ML T&E
Training Pipeline
IP
Digital Engineering (incl. V&V)
DoE for AI/ML
AI/ML TEMP
(Near) Real-Time Quality Control
Real-World Operations
Observers (of Outputs and Outcomes)
IP
T&E Harnesses
Re-Engineering Feedback

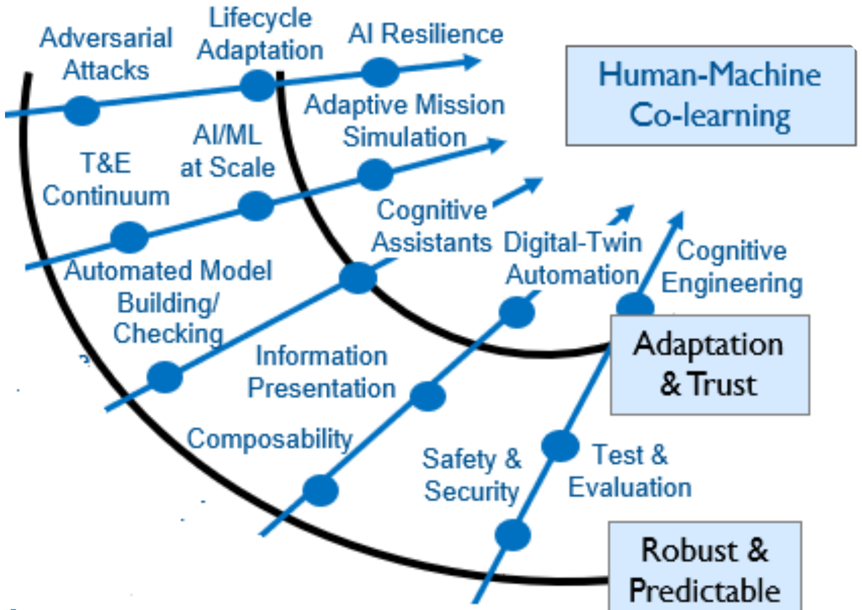






Challenges for Test & Evaluation of AI

- Testing & Evaluation is a continuum
  - Information accumulates over time across varying operating envelopes
  - does not end until the system retires
- All AI areas need testbeds
- Operational relevance is essential
- Data Management is foundational
- AI systems require a probabilistic risk-based approach
- Previous test metrics apply, but may have different interpretations
  - Task & mission level performance, course of action, non-functional requirements
- An expanded definition of external context is necessary
- The T&E workforce and culture must evolve

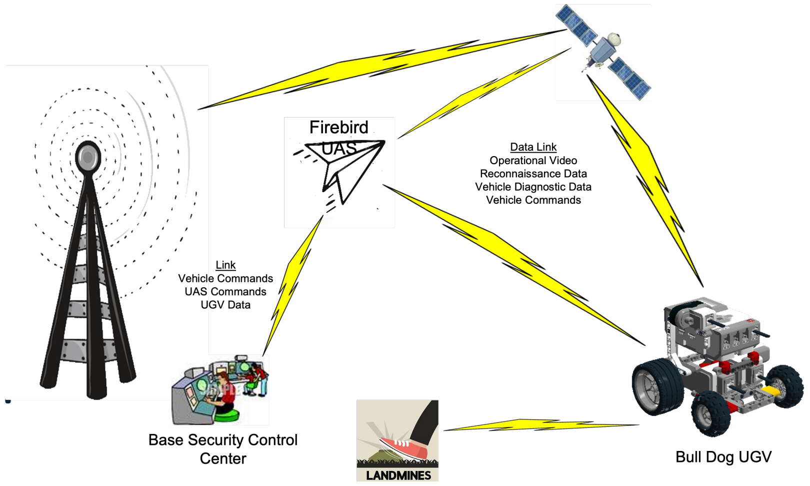


Freeman, L. (2020), Test and Evaluation for Artificial Intelligence. INSIGHT, 23: 27-30.

TRUSTED ARTIFICIAL INTELLIGENCE SYSTEMS ENGINEERING CHALLENGE

- Teams engage in
  - Assured design of AI and autonomy into notional system
  - Risk-based monitoring and management of operational use of AI capabilities.

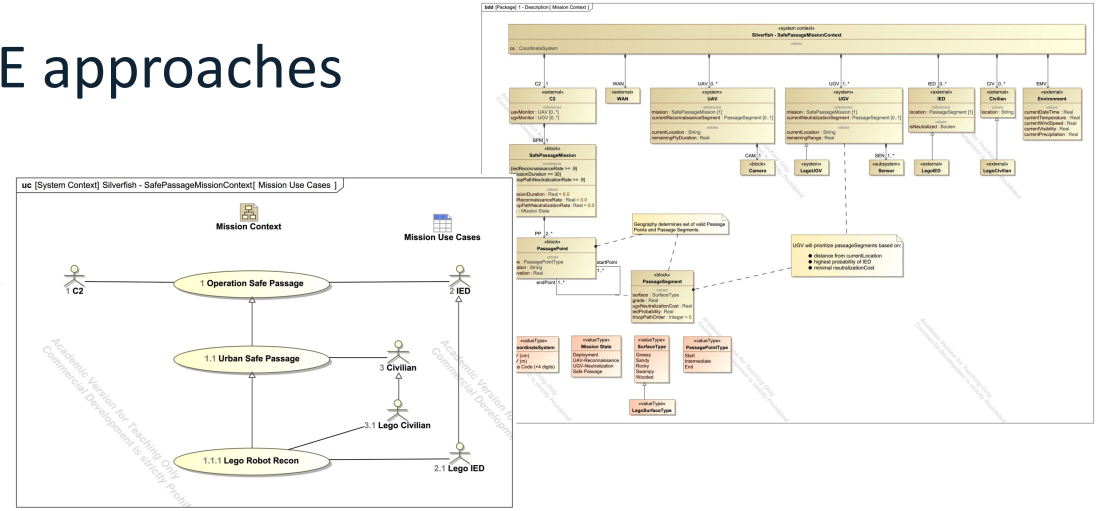
- Semester-long Stages:
  1. Explore performance of AI models over variety of operational scenarios.
  2. Design of the decision system; human-machine teaming, resilience.
  3. Operational simulation of mission scenarios.



- Teams judged on quantitative performance & SE approaches used to design and operate the system.

- Open to all SERC universities + HBCUs and MSIs

- Prizes! Sponsored by DEVCOM


uc [System Context] Silverfish - SafePassageMissionContext[Mission Use Cases]
Mission Context
Mission Use Cases
1 C2
1 Operation Safe Passage
2 IED
1.1 Urban Safe Passage
3 Civilian
3.1 Lego Civilian
1.1.1 Lego Robot Recon
2.1 Lego IED
bdd [Package] 1 - Description [Mission Context]
«system context» Silverfish - SafePassageMissionContext
cs : CoordinateSystem
«external» C2
uavMonitor : UAV [0..*]
ugvMonitor : UGV [0..*]
«external» WAN
«system» UAV
mission : SafePassageMission [1]
currentReconnaissanceSegment : PassageSegment [0..1]
currentLocation : String
remainingFlyDuration : Real
«system» UGV
mission : SafePassageMission [1]
currentNeutralizationSegment : PassageSegment [0..1]
currentLocation : String
remainingRange : Real
«external» IED
location : PassageSegment [1]
isNeutralized : Boolen
«external» Civilian
location : String
«external» Environment
currentDateTime : Real
currentTemperature : Real
currentWindSpeed : Real
currentVisibility : Real
currentPrecipitation : Real
«block» SafePassageMission
{iedReconnaissanceRate >= .9}
{missionDuration <= 30}
{troopPathNeutralizationRate >= .9}
«block» Camera
«system» LegoUGV
«subsystem» Sensor
«external» LegoIED
«external» LegoCivilian
«block» PassagePoint
«block» PassageSegment
surface : SurfaceType
grade : Real
ugvNeutralizationCost : Real
iedProbability : Real
troopPathOrder : Integer = 0
Geography determines set of valid Passage Points and Passage Segments.
UGV will prioritize passageSegments based on:
distance from currentLocation
highest probability of IED
minimal neutralizationCost

SERC 5TH ANNUAL AI4SE & SE4AI WORKSHOP

AI4SE & SE4AI

RESEARCH AND APPLICATION WORKSHOP
SEPTEMBER 27-28, 2023

SYSTEMS ENGINEERING RESEARCH CENTER
U.S. ARMY
DEVCOM
AI
UNCLASSIFIED
DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

2023 SUMMARY REPORT

AI4SE & SE4AI

RESEARCH AND APPLICATION WORKSHOP

SEPTEMBER 17-18, 2024 | Arlington, VA

The conference theme, “Safer AI-Enabled Complex Systems: Responsible Deployment of AI through Systems Engineering,” aims to foster discussions and insights on how systems engineering can support the development of robust and ethical AI systems, and how AI tools can in turn transform the practice of systems engineering.

https://sercuarc.org/event/ai4se-se4ai-workshop-2024/#dates

34th Annual **INCOSE**
international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS