# AI4SE and SE4AI

TechOps Track – Presentation

Ali K. Raz, George Mason University

Tom McDermott, Systems Engineering Research Center (SERC)

Outline

- **Introduction to AI Systems Working Group**
  - AI Systems WG Charter
  - Current activities and on-going projects
  - Framing the SE and AI Discussion

- **A Deeper Dive into SE4AI**
  - The need for SE4AI
  - Examples of Recent Research in SE4AI

- **A Deeper Dive into AI4SE**
  - AI4SE Opportunities
  - Examples of Recent Research in AI4SE
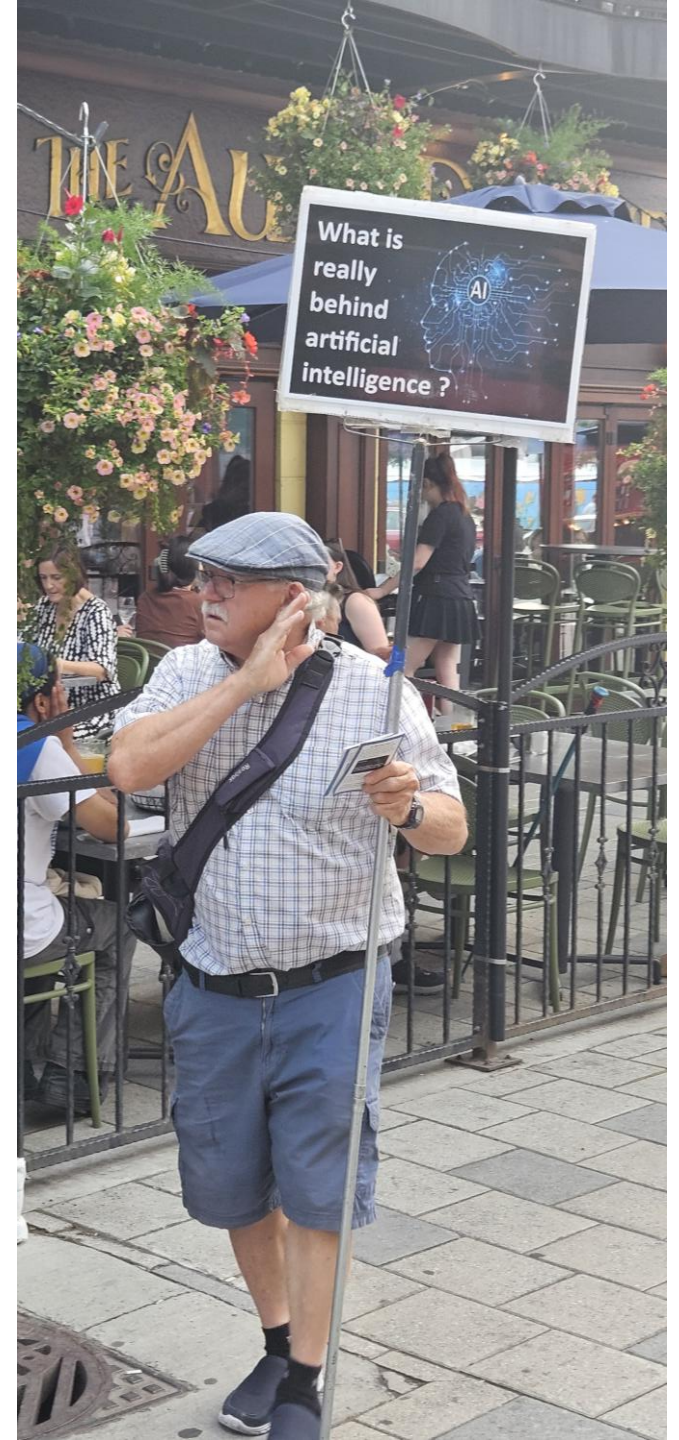
AI Systems Working Group

- **Purpose:**
  - Explore AI Relevance to Systems Engineering and Systems Engineers
  - Develop educational materials for introducing AI to SE community
  - Create INCOSE products covering the spectrum of SE4AI and AI4SE

SE4AI
Exploration and Application of Systems Engineering Principles for benefit of Artificial Intelligence Systems

AI4SE
Exploration and Application of Artificial Intelligence Developments for benefit of System Engineering

Who's Who in AI Systems WG

Chair

Dr. Ali Raz (CSEP) is an Assistant Professor of Systems Engineering and an Assistant Director of Intelligent Systems and Integration at George Mason University C4I and Cyber Center. He holds a BSc and MSc in Electrical Engineering from Iowa State University and a doctorate in Aeronautics and Astronautics from Purdue University.

Co-Chair

Dr. Ramakrishnan "Ramki" Raman (ESEP, INCOSE Fellow) is Senior Chief Engineer at Eaton. He received B.Tech and MS degrees from IIT Madras, and PhD from IIIT-Bangalore. He is a certified Six Sigma Black Belt and is Fellow of INCOSE and Fellow of ISSE.

Past Chair

Dr. Barclay R. Brown (ESEP) is Senior Fellow – AI Research at Collins Aerospace, a division of Raytheon Technologies. He is a certified Expert Systems Engineering Professional (ESEP), certified Systems Engineering Quality Manager, and CIO of INCOSE for 2021-2023. He is the author of Engineering Intelligent Systems book.

What are we working on (and have worked on) ?

- **Multiple Tutorials & Teach-Through sessions (IS and IW)**
  - IS 2021, IW 2022, IS 2023, IW 2023
  - IW 2025: A mini-tutorial on AI and SE

- **AI article in SEBoK [released 2021]**
  - https://sebokwiki.org/wiki/Artificial_Intelligence

- **AI Systems Primer**
  - Development complete
  - Awaiting external reviews
  - Expected to be released by the end of this year

- **SE Emerging Area article for Systems Engineers guide to Large Language Models**
  - SEBoK next release
  - Lead Author: Dr. Barclay Brown
  - Scheduled for next SEBoK release

What else are we working on?

- INCOSE Systems Engineering Journal Special Issue on AI and Systems Engineering
  - Call For Papers: https://incose.onlinelibrary.wiley.com/hub/journal/15206858/call-for-papers/si-2024-000807
  - Submissions Closed

- Multiple high quality paper already under the journal review process

- One of the first SE journal issue on AI
  - Addresses both SE4AI and AI4SE

Framing AI & SE Discussion (1)

## Role for Systems Engineers in AI space

AI4SE   and   **SE4AI**

Focuses on **application of AI in support of systems engineering processes**, enabling enhanced decision-making, optimization, and efficient effort allocation.

Focuses on **leveraging systems engineering principles to develop AIES that are safe,** robust, and efficient, while extending them in response to the nature of AI enabled systems.
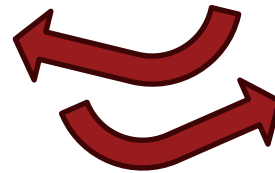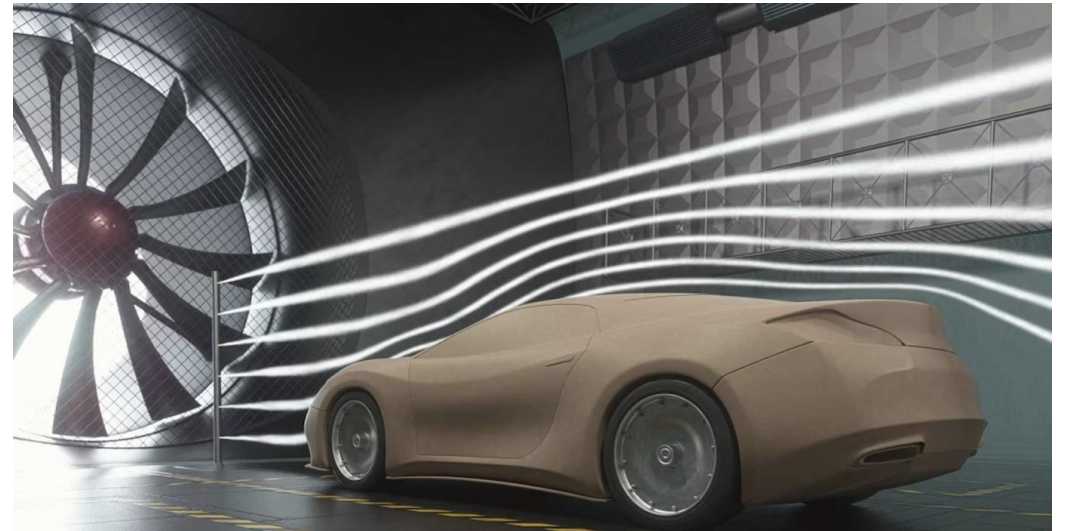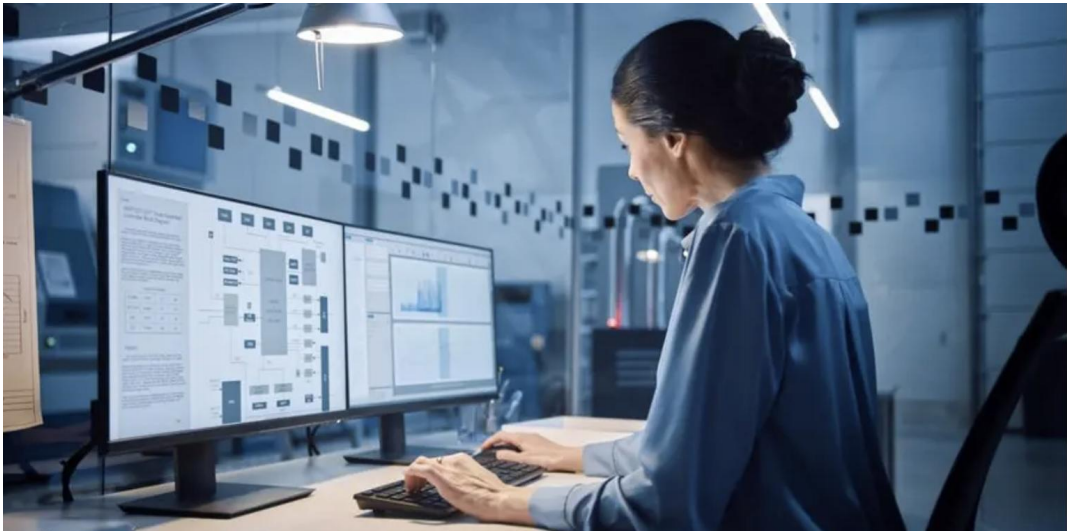
SE4AI applies to AI4SE too, but types of AI tools tend to be different

… and AI4SE might change what SEs do too.

Framing AI & SE Discussion (2)

Generative AI → **AI4SE** and **SE4AI** ← Trust in AI

How should AI fit into the system engineer's workflow?   How will AI(s) in the system, change core SE functions.
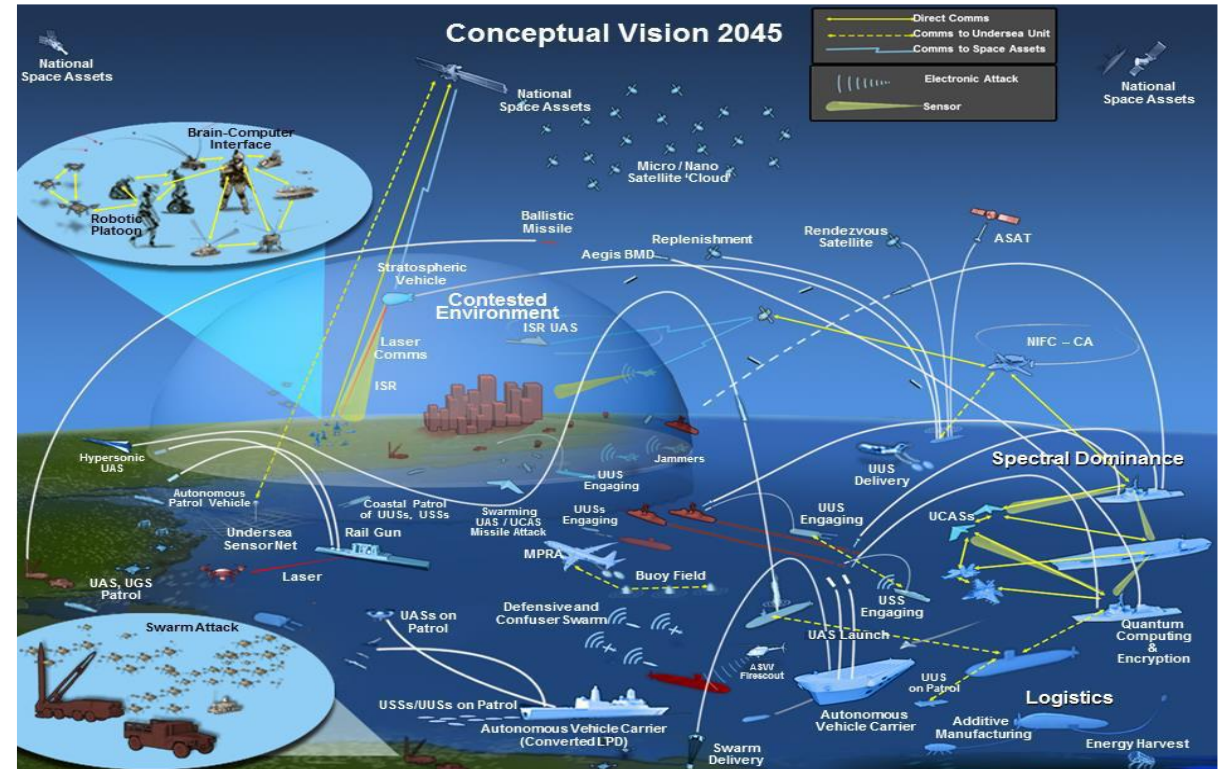
A Deeper Dive into SE4AI

(Raz)

Why do we need SE to ensure safe/robust/trustworthy AIES?
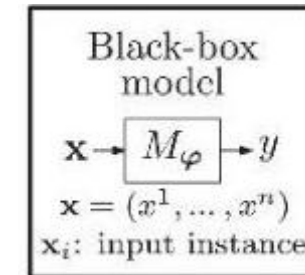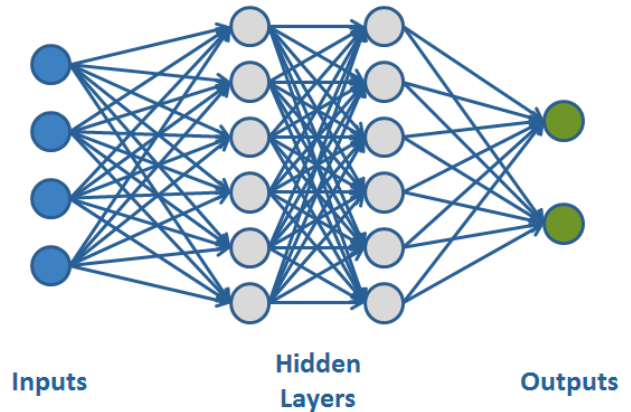

System behavior is not **only** about the algorithm…

… or even one human working with one cognitive assistant…

… it's an embedded socio-technical systems problem, which is an extension of SE practices

The Need for Systems Engineering of AI

- Deep Neural Networks (DNNs) are most common form of AI/ML Implementation

  ✓ State-of-the-art implementation for AI/ML algorithms *(Supervised, Unsupervised, Reinforcement Learning, Natural Language Processing etc.)*

  ✓ Well-established performance outcomes in a variety of applications
    (Intuitive and non-intuitive outcomes)

  ✓ Strong focus on algorithmic development, computational efficiency, and implementation

 ✓ Selective demonstration of test cases, mostly based on training data partitioning in training and validation sets

- Common Challenges for DNNs

  ❑ Trained DNNs are essentially backboxes to the designers and users

  ❑ Limited characterization of performance bounds due to variations and uncertainties; limited Monte Carlo simulations and user selected variations

  ❑ Limited explanation of black-box decision-making logic

  ❑ Limited evaluation of acceptable and unacceptable performance regions

Inputs   **Hidden Layers**   **Outputs**

Black-box model

$$\mathbf{x} \rightarrow \boxed{M_\varphi} \rightarrow y$$
$$\mathbf{x} = (x^1, \ldots, x^n)$$
$$\mathbf{x}_i: \text{input instance}$$

Systems Engineering Perspective Example SE Questions to Ask

❑ What is the impact of variations in input data and environment?

❑ How does the input (i.e., observed state) influence DNNs decision making?

❑ Does training data considers edge cases?

❑ How does the DNNs respond to modeled (i.e., included in training) and unmodeled uncertainties?

❑ How does the DNN interact with other system components and external systems?

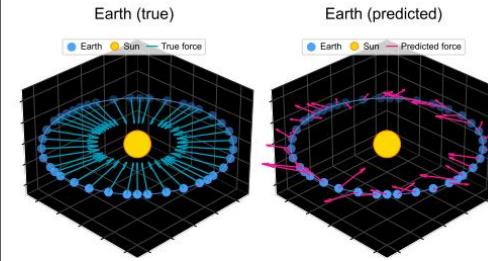# WHEN AI IS ONLY ARTIFICIALLY INTELLIGENT!
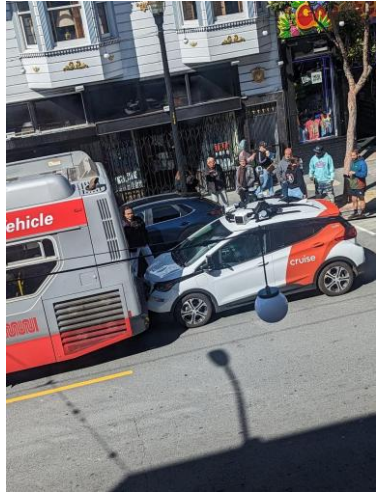
ChatGPT hallucinates court cases

Amazon AI-enabled recruitment tool only recommended men

Zillow wrote down millions, slashed workforce due to algorithmic home-buying disaster

Air Canada pays damages for chatbot lies

Uncovering Understanding of Foundation Models... Predicting Planetary Motion**

"…foundation models trained on orbital trajectories consistently fail to apply Newtonian mechanics when adapted to new physics tasks."

UNSOLVED PROBLEMS IN ML SAFETY*

Robustness — Create models that are resilient to adversaries, unusual situations, and Black Swan events.

Monitoring — Detect malicious use, monitor predictions, and discover unexpected model functionality.

Alignment — Build models that represent and safely optimize hard-to-specify human values.

Systemic Safety — Use ML to address broader risks to how ML systems are handled, such as cyberattacks.

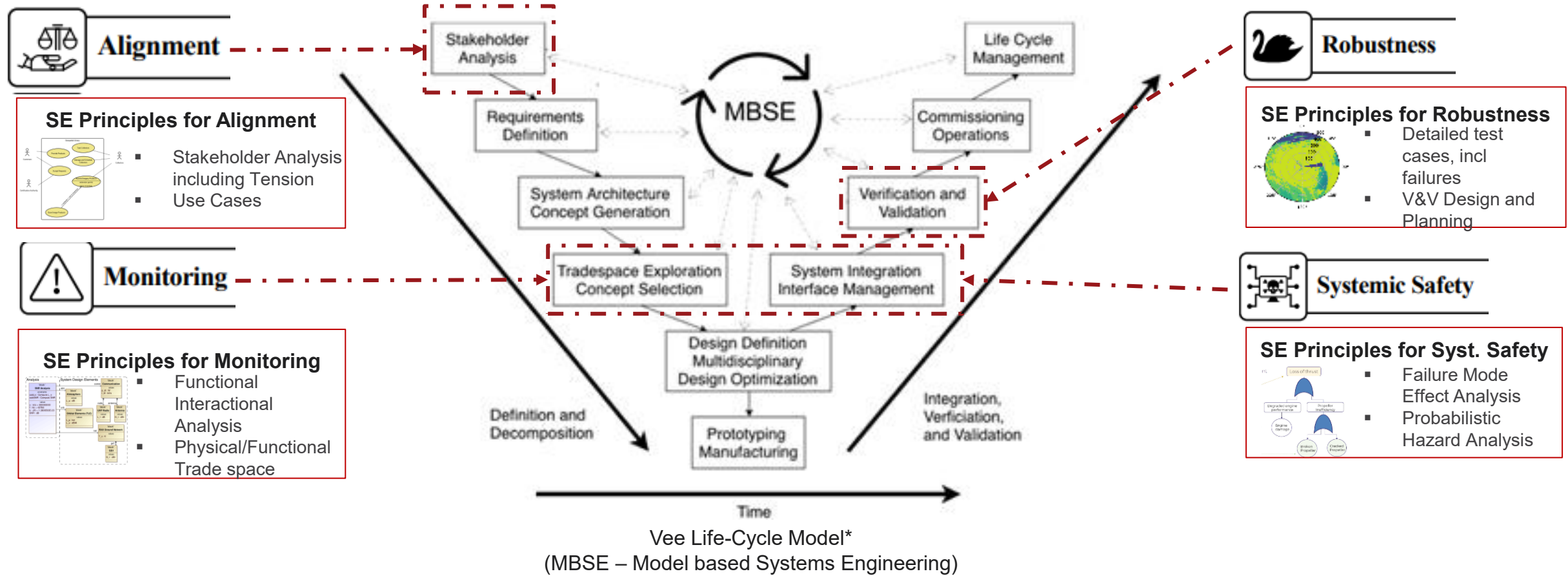https://www.cio.com/article/190888/5-famous-analytics-and-ai-disasters.html
*Hendrycks, Dan, Nicholas Carlini, John Schulman, and Jacob Steinhardt. "Unsolved problems in ml safety." *arXiv preprint arXiv:2109.13916* (2021)
**Vafa, K., Chang, P. G., Rambachan, A., & Mullainathan, S. (2025). What Has a Foundation Model Found? Using Inductive Bias to Probe for World Models. *arXiv preprint arXiv:2507.06952*.

SYSTEMS ENGINEERING CALL FOR AI/ML

- Examine, develop, and build AI with the SE principles, concepts, and tools
  - **SE life-cycle stages place particular emphasis on the unsolved problems for AI/ML at the outset**

Vee Life-Cycle Model*
(MBSE – Model based Systems Engineering)

Raz, Ali K., et al. "Explainable AI and counterfactuals for test and evaluation of intelligent engineered systems." *INCOSE International Symposium*. Vol. 33. No. 1. 2023.
de Weck, O. L. Vee-Model. MIT OCW. https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-842-fundamentals-of-systems-engineering-fall-2015/lecture-notes/MIT16_842F15_Ses1SE_Ovr_vw.pdf.

EXAMPLES OF RECENT SE4AI RESEARCH (1)

Systems Engineering based Test and Evaluation of Reinforcement Learning

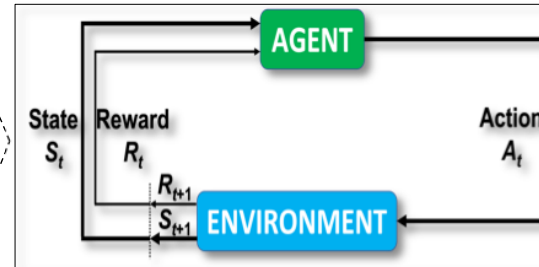### Robustness Testing

Purpose:
Sensitivity analysis of variations in action space, enviorment, and state observation
Methodology:
Design of Experiments and Statistical Analysis
Value:
Performance bounds and characterization of uncertanities

Compare to Known Solutions

Purpose:
Evaluate RL performance to known and accepted solutions
Methodology:
Problem space dependent; closed form mathematical solutions.
Value:
Validate RL performance and robustness testing results

Explainable AI (XAI)

Purpose:
Determine influential features of trained RL decision-making logic
Methodology:
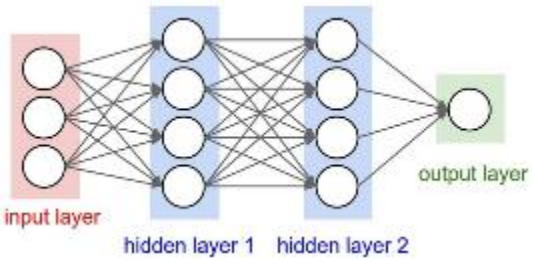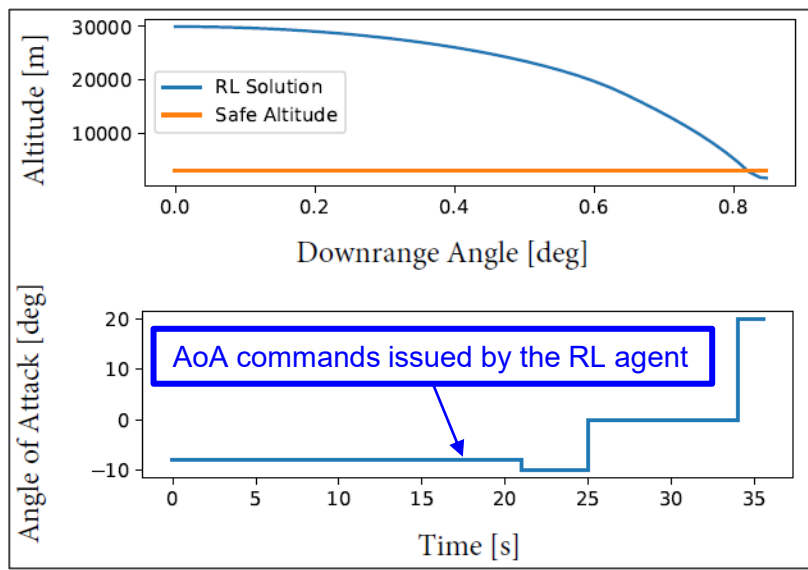Post-hoc XAI method: Shapely Additive Explanations
Value:
Explain which state vector values contribute to RL decision and why sensitivities are present in robustness test

Raz, Ali K., et al. "Explainable AI and Robustness-Based Test and Evaluation of Reinforcement Learning." *IEEE Transactions on Aerospace and Electronic Systems* 60.5 (2024): 6110-6123.

Reinforcement Learning Testing and Explainability

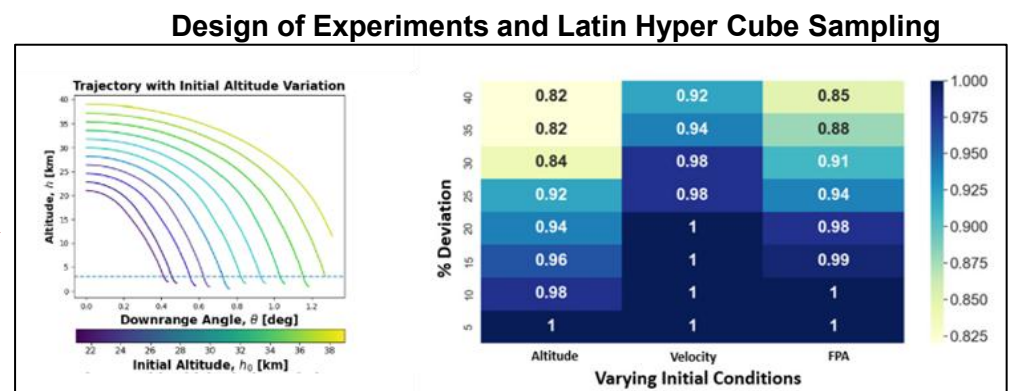Solving Flight Control Problem through Reinforcement Learning

- RL provides Angle of Attack commands to guide a vehicle to a pre-determined safe altitude (30km to 3km)
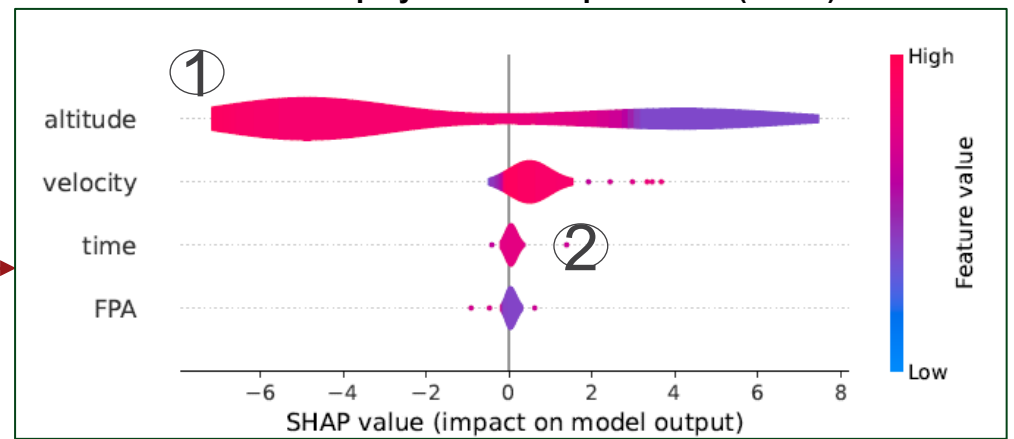

Robustness Testing of RL

Design of Experiments and Latin Hyper Cube Sampling

100% success for 5% tolerance in altitude

RL Agent: Deep Neural Network

Explainability of RL

Shapley Additive Explanations (SHAP)

① *Higher altitude values oppose a change in AoA whereas lower altitudes support it*

② *Higher velocity values positively influence change in AoA*

RL performs well but the user cannot tell under what conditions it works and what it has learned?

Raz, Ali K., et al. "Explainable AI and Robustness-Based Test and Evaluation of Reinforcement Learning." *IEEE Transactions on Aerospace and Electronic Systems* 60.5 (2024): 6110-6123.

Examples of Recent SE4AI Research (2)

Integrating Autonomy in System of Systems: Towards a System of Autonomous Systems
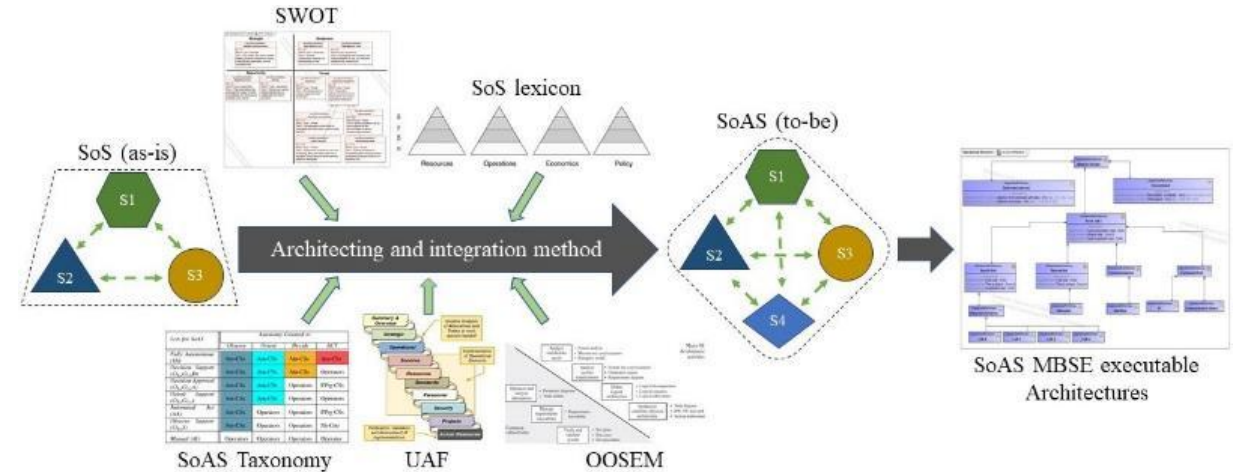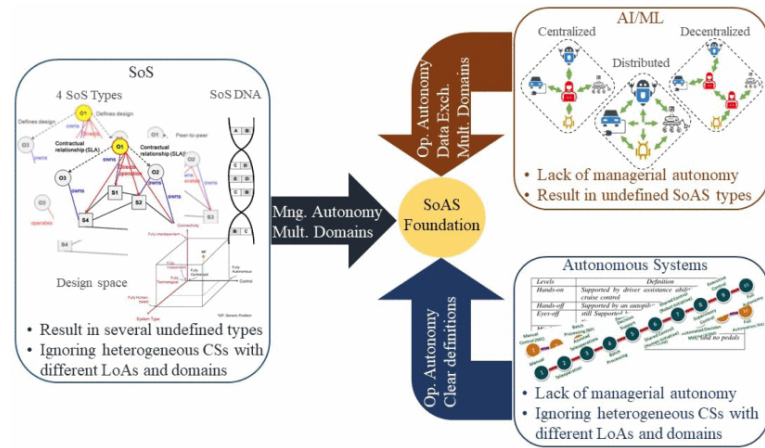
Currently building MBSE frameworks for Architecture, Integration, Test, and Evaluation of System of Autnomous Systems:

Key Research Questions:

1) How to identify the right **Level of Autonomy** in System of Autnomous Systems?

2) How to characterize **emergent behaviors** with different Level of Autnomoy?
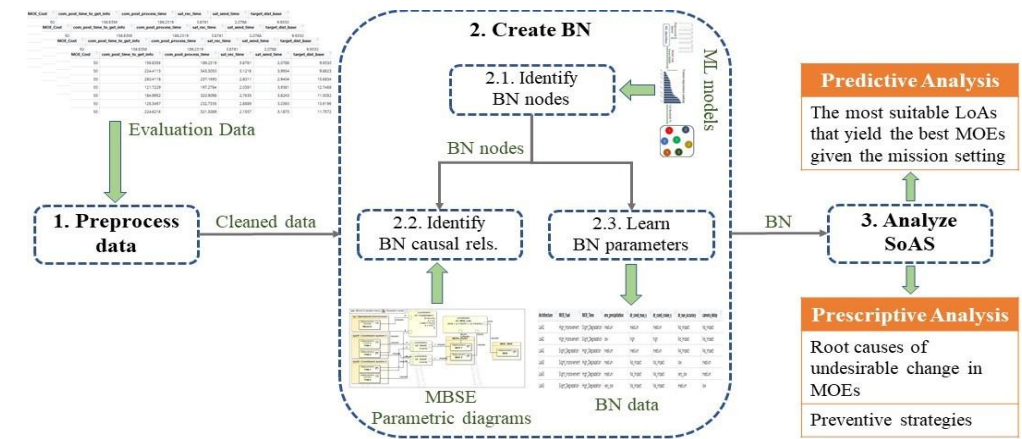
Torkjazi, M., & **Raz, A. K**. (2024b). Model-Based Systems Engineering (MBSE) Methodology for Integrating Autonomy into a System of Systems Using the Unified Architecture Framework. *INCOSE International Symposium*, 34, 1051–1070. https://doi.org/10.1002/iis2.13195

Torkjazi, M., & **Raz, A. K**. (2024c). Predictive and Prescriptive Analyses of Autonomy Integration into the System of Systems. In A. Salado, R. Valerdi, R. Steiner, & L. Head (Eds.), *The Proceedings of the 2024 Conference on Systems Engineering Research* (pp. 213–228). https://doi.org/10.1007/978-3-031-62554-1_14

SERC Topics in SE4AI

SE4AI

Modeling AI as part of a complex SoS

Systematic review of SoS emphasizes need for new analytical tools to assess integration of different tools at different levels of autonomy in SoAS context.

(Raz)

AI "-ilities" relevant to SE measurement

Extending core concepts like resilience and flexibility to AIES, including systems theoretic perspectives.(Cody/Beling)   Evolving algorithm-based measures like explainability/ interpretability and social concepts of trust to AIES. (Broniatowski/Szajnfarber)

T&E as a continuum + testbeds

Key questions around what to test, when, and how to interpret tests along the continuum. Examining model aggregation and analogs. (Panchal) AI Test harness aimed at better testing and better training for T&E of AIES (Freeman et al).
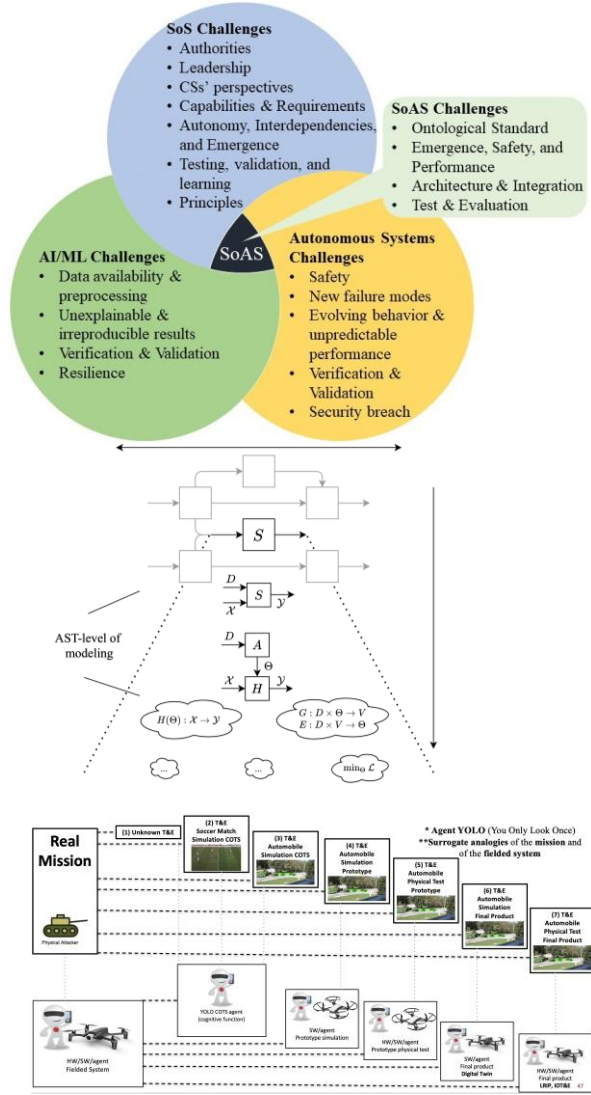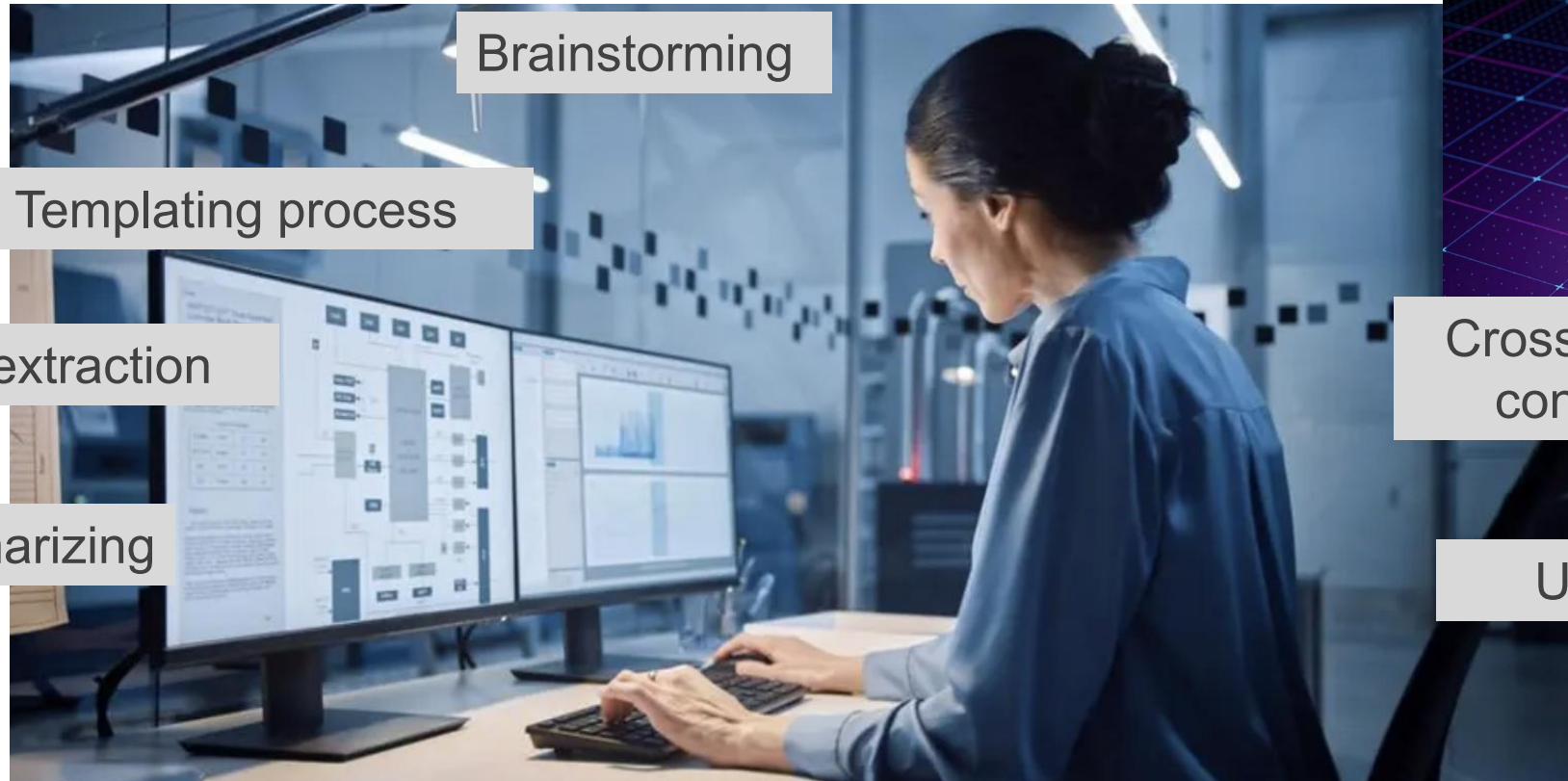
A Deeper Dive into AI4SE

(McDermott)

Like everyone else: many projects prototyping functions and exploring what can be done.
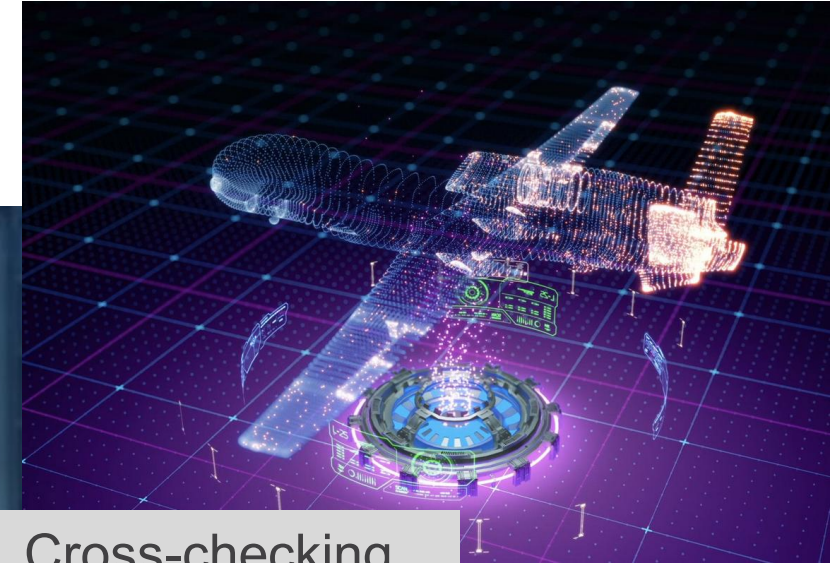

Brainstorming

Templating process

Fact extraction

Summarizing

Cross-checking, consistency

Un-"fixating"

Common Themes in AI4SE

NLP/LLMs and ML/AI are good at:
- Deductive coding of unstructured text, including translating among concepts
- Scaling repetitive tasks, making it possible to pay attention to many more variables
- Identifying patterns within datasets
- Supporting interactive dashboards and data visualization more broadly
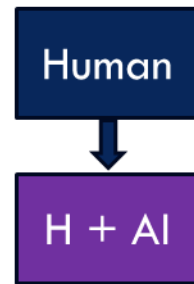
They're getting better at:
- Synthesis tasks
- Generating artifacts, depending on the level of structure and correctness needed

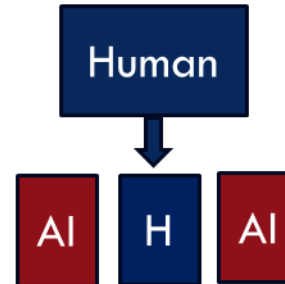These apply across a wide range of tasks across defense acquisition…

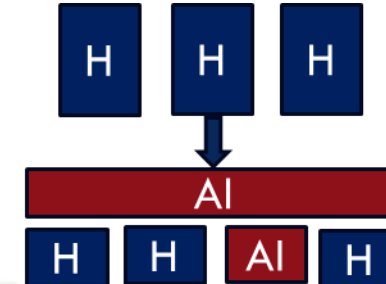… but, most tasks that humans do require some of each lists + judgement and prioritization
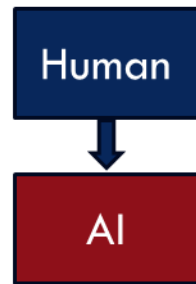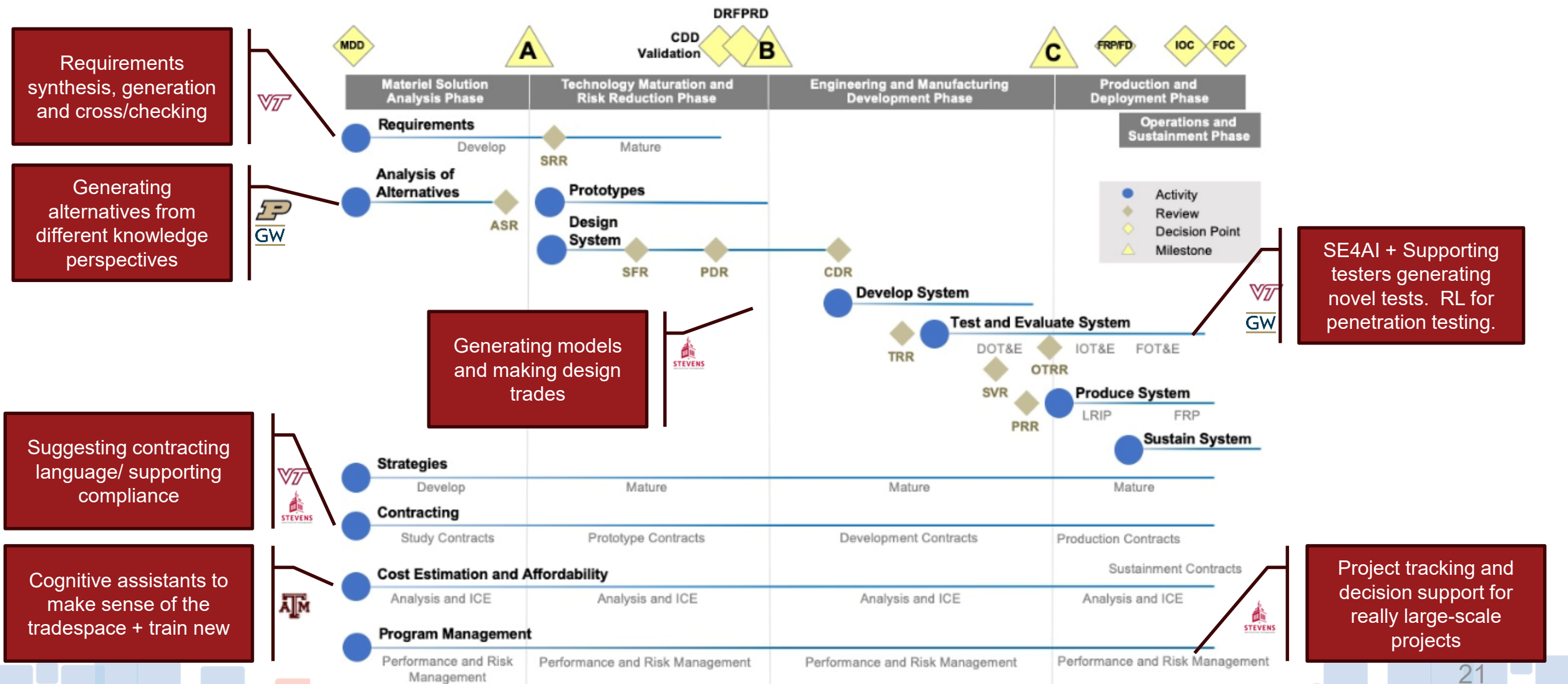

Replacement   Augmentation   Task Remapping   Task "System" Remapping
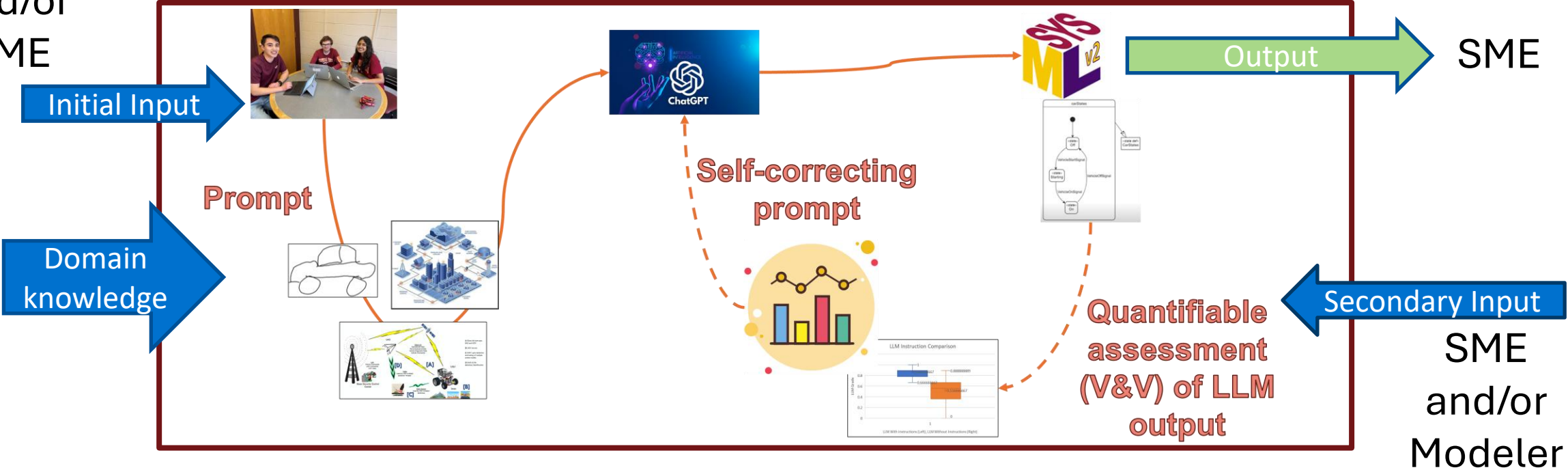
GW

Where CAN AI Support/Augment Humans Decision-Making NOW?

(Traditional) Lifecycle View of Major Capability Acquisition

Requirements synthesis, generation and cross/checking

Generating alternatives from different knowledge perspectives

Generating models and making design trades

SE4AI + Supporting testers generating novel tests. RL for penetration testing.

Suggesting contracting language/ supporting compliance

Cognitive assistants to make sense of the tradespace + train new

Project tracking and decision support for really large-scale projects

Milestones and phases shown: MDD, A, CDD Validation, DRFPRD, B, C, FRP/FD, IOC, FOC

Phases: Materiel Solution Analysis Phase, Technology Maturation and Risk Reduction Phase, Engineering and Manufacturing Development Phase, Production and Deployment Phase, Operations and Sustainment Phase

Legend:
- Activity
- Review
- Decision Point
- Milestone

July 30, 2025

21

Slide Credit: Dr. Zoe Szajnfarber, SERC Chief Scientist; Used with SERC Permission

Architecture Generator

Modeler and/or SME

Initial Input

Domain knowledge

Prompt

Self-correcting prompt

Quantifiable assessment (V&V) of LLM output

Output → SME

Secondary Input

SME and/or Modeler

Thrusts
1. Text to text
2. Text/image to SysMLv2 code
3. SysML image/code to text
4. SysML V1 to V2
5. Systems engineering expertise

Ex1: LLM Support of Core SE Tasks: Architecture Generator

Efficiency, Accessibility, and Reproducibility

Artifact Generation
- Requirements documents, ICDs, ConCops, etc.

SysML Translation and Model Manipulation
- SysMLv1 to SysMLv2, Text-to-SysML, etc.

Model Interpretation
- Explain structural/behavioral models to non-expert stakeholders

Knowledge Transfer
- Bridge communication between system modelers and SMEs

Concept Development
- Act as brainstorming partner using chain-of-thought prompts
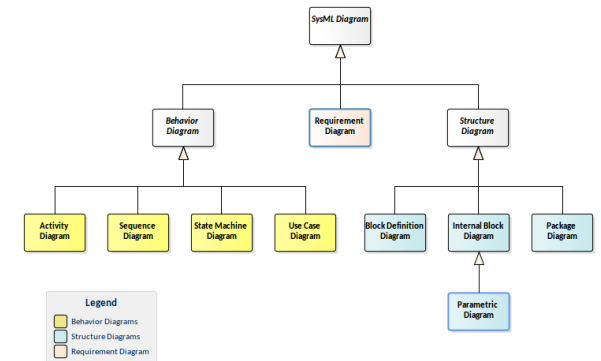
Automation of Repetitive SE Tasks
- Generating traceability matrices from requirements to design elements, etc.

SysMLv2
- **Generation, manipulation, translation, etc.**

Other Examples

AI4SE

AI to support information processing

J-books summarization: reasonable extraction of facts from ~20page chunks; useful Q&A interface. Some preprocessing helpful. (Buettner)

AI to support SE content generation

Generating SE artifacts (operational context statement): Capable of generating expert-like artifacts with relatively small training sets, but _how_ you prompt matters (Topcu/Wach)

Architecture of Human AI Collaboration

Studied LLMs as part of a design team: focused on how the designers used GPT-4 as part of their design process; which activities worked/didn't. (Szajnfarber/Pless)

AI4RE Project

- **Purpose**:
  - Joint study group between Requirements Working Group and AI Systems Working Group to study the interplay and integration between Requirements Engineering and AI

- **Scope**:
  - Understanding current maturity & future potential of AI4RE, with a position paper on AI4RE
  - Roadmap, AI4RE adoption guidance, AI4RE practice maturity scorecard
  - Revisions to applicable existing Requirements Working Group work product(s), incorporating AI4RE, and Proposal for updates to applicable sections in SEBOK

Exponentially increasing complexity of systems, spanning multiple disciplines

Rapid advancements in AI Technologies

Increasing drive & demand for agility and automation in engineering workflows

Growing volume of requirements data and the need for traceability

- Assist in Requirement Elicitation & Analysis..??
- Assist in Requirements Consistency & Quality Checking..??
- Aid in managing Requirements Volatility and Evolution..??

Continue the Discussion…..

Join the AI Systems Working Group

- Go to http://profile.incose.org and check the box for AI Working Group

ARTIFICIAL INTELLIGENCE SYSTEMS
VISIT OUR WORKING GROUP HOMEPAGE
AI

- Checkout AIWG Homepage:
www.incose.org/ai

AI4SE & SE4AI RESEARCH APPLICATION WORKSHOP

Sep 17 – Sep 18, 2025
Washington, D.C.

SYSTEMS ENGINEERING RESEARCH CENTER

The AI4SE & SE4AI Research and Application Workshop is an annual two-day gathering of systems engineers and AI experts.

Annual Conference on Systems Engineering Research (CSER)

CSER 2026

Theme: Intelligent Digital Twin-enabled Systems Engineering for 21st Century Sociotechnical Systems

April 6th to 9th 2026, Arlington, VA, USA

Honorary Co-Chairs		General Co-Chairs		Panels Chair	Sponsor Chair
Dr Azad Madni	Dr Dinesh Verma	Dr John Shortle	Dr. Ali Raz	Marilee Wheaton	Dr. Lance Sherry

Research Paper Topics

- Generative AI
- Human-AI Teaming
- Transdisciplinary Systems Engineering
- Model Based Systems Engineering
- Software-Defined Vehicles
- Adaptive Cyber-Physical Human Systems
- Systems and SoS Integration
- System Architecture and Complexity
- Trade-space Visualization and Analysis

- Digital Engineering and Digital Twinning
- Sociotechnical Systems Engineering
- Systems Thinking and Complexity Management
- Interactive Storytelling in Systems Engineering
- XR in Systems Engineering
- Smart Manufacturing
- New Topics in Systems Engineering Education
- Cybersecurity Systems Engineering
- Agent-Based Simulation

Application Areas

- Autonomous Vehicles
- Defense Systems and System-of-Systems
- Space and Aerospace Systems
- Global Supply Chains
- Healthcare Delivery
- Homeland Security
- Smart Manufacturing
- Medical Devices
- Sustainable Energy
- Transportation Systems
- Urban Systems and Infrastructure

Stay Tuned For

- Keynote Speakers
- Conference Workshops
- SEANET Workshop for Doctoral Students
- Executive Leadership Panel

Technical Program Chairs

Dr. Matthew Amissah   Dr. Abbas Zaidi

GEORGE MASON UNIVERSITY   INCOSE   SYSTEMS ENGINEERING RESEARCH CENTER