AI and Systems Engineering: A MITRE Perspective

Peter Schwartz, PhD

October 28, 2020

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Social Media – Promise vs. Reality

Promise

- Increased connection to friends and family
- Democratization of information

Reality

- Inability to agree on what is true
- Inability to react to important issues
- Deterioration of the social fabric

See thesocialdilemma.com

MITRE

Social Media – A Failure of AI and SE

Incentives are misaligned

- Users want free services
- Social media companies make money through targeted advertising
- AI is the perfect tool for targeted advertising
- Users are more predictable if they are subdivided and politically polarized

System-level issues have been ignored

- What are the side effects?
- What are the ethical concerns?
- What are the unintended consequences?
- Can what is good for the company also be good for users and society?

Agenda

AI Maturity Model

Systems Engineering for AI

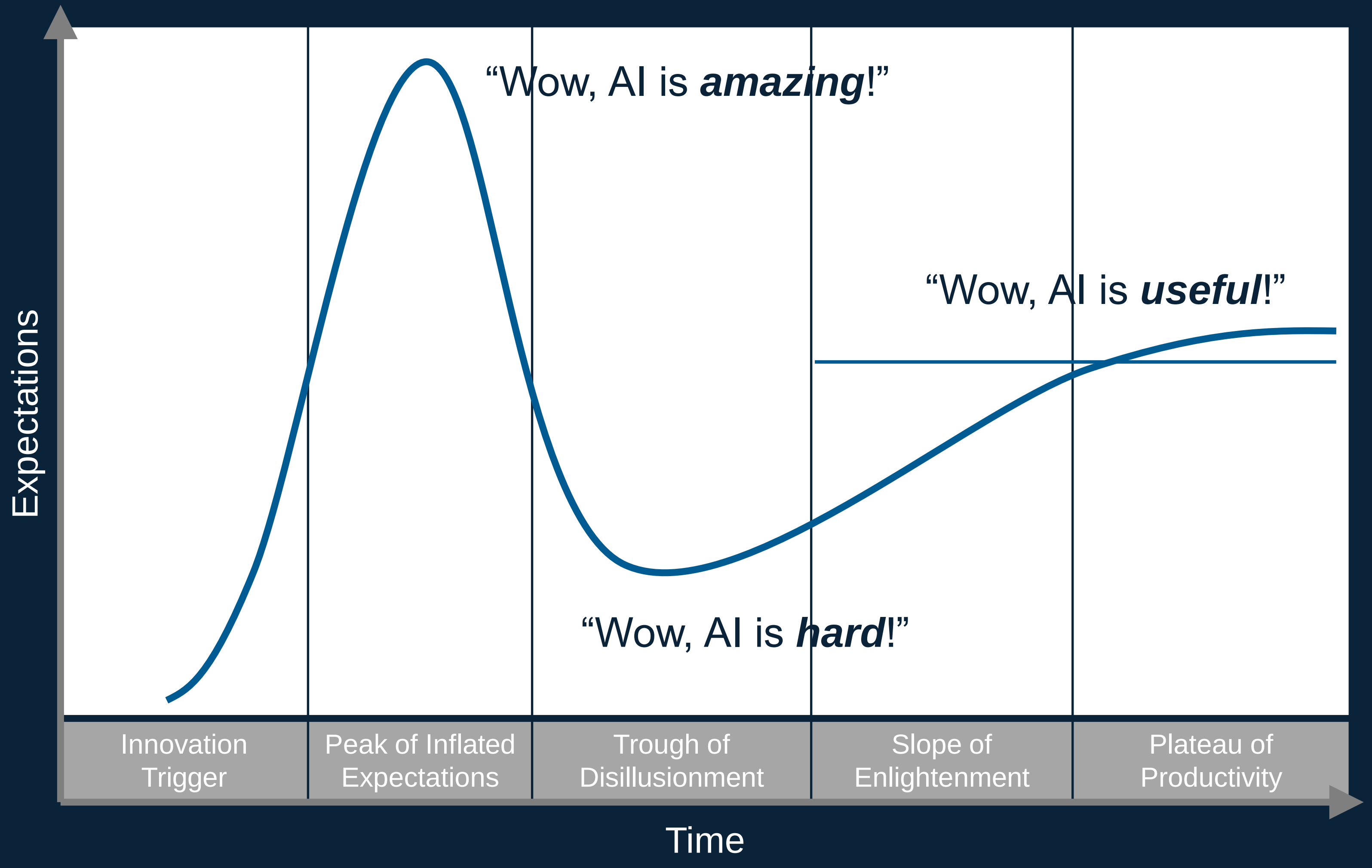
- Workforce Development
- Innovation
- Solution Monitoring
- Trust

AI for Systems Engineering

Conclusions

The Need for an AI Maturity Model

Gartner Hype Curve



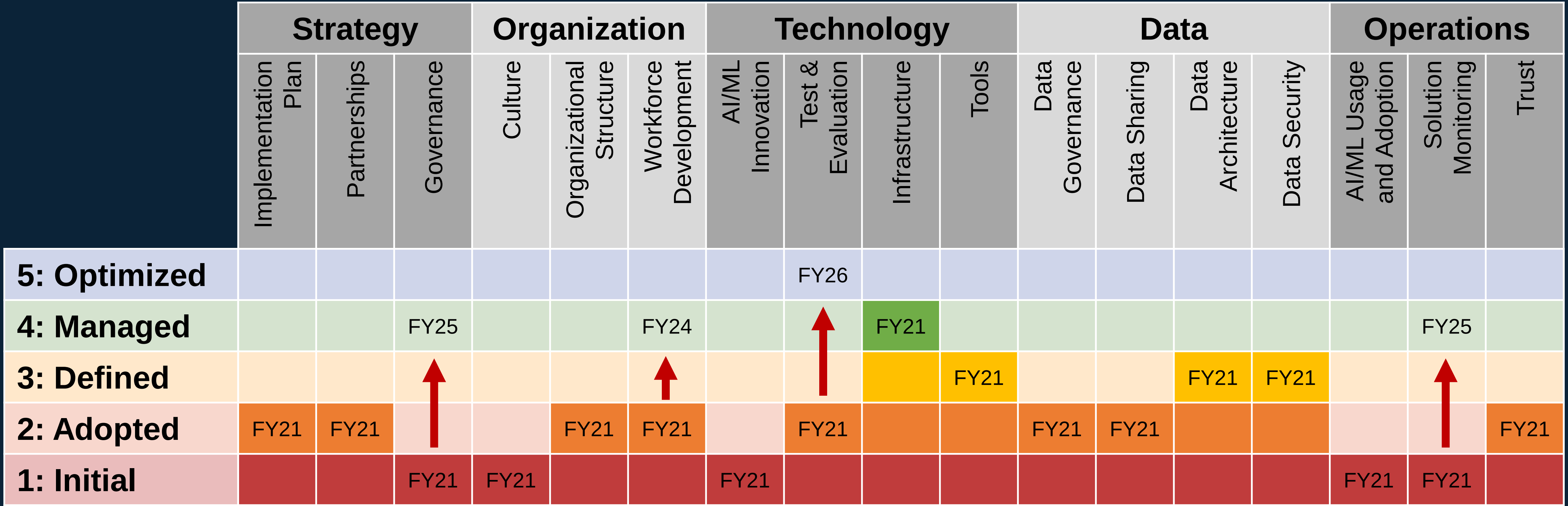
“…AI could free up ***30 percent*** of the government workforce’s time…”
- [Deloitte]

“Through 2022, ***only 20%*** of analytic insights will deliver business outcomes.”
- [Gartner]

“…our data shows that ***only 8%*** of firms engage in core practices that support widespread [AI] adoption.”
- *[Harvard Business Review]*

MITRE

MITRE AI Maturity Model



	Strategy			Organization			Technology				Data				Operations		
	Implementation Plan	Partnerships	Governance	Culture	Organizational Structure	Workforce Development	AI/ML Innovation	Test & Evaluation	Infrastructure	Tools	Data Governance	Data Sharing	Data Architecture	Data Security	AI/ML Usage and Adoption	Solution Monitoring	Trust
5: Optimized								FY26									
4: Managed			FY25			FY24			FY21							FY25	
3: Defined										FY21			FY21	FY21			
2: Adopted	FY21	FY21			FY21	FY21		FY21			FY21	FY21					FY21
1: Initial			FY21	FY21			FY21								FY21	FY21	

AI Governance Plan

AI Workforce Development Plan

AI Test & Evaluation Plan

AI Solution Monitoring Plan

MITRE

Organization: Workforce Development

Challenges

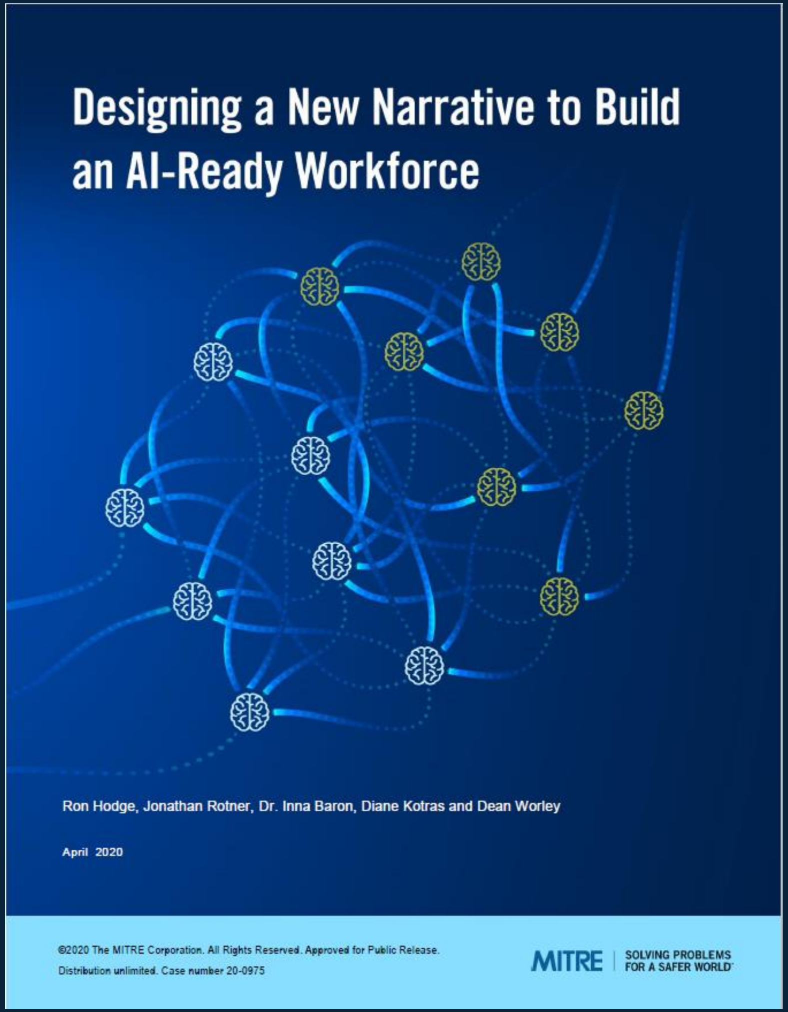
Questions

- How can the DoD keep pace with technological acceleration in AI?
- How does the DoD address the cultural gap between it and the modern workforce?

Issues

- The DoD lacks in-house AI skills and can’t compete with industry for talent
- Industry owns the technical baseline but doesn’t partner w/ the DoD like it used to

The time is ripe for a change in narrative



Designing a New Narrative to Build an AI-Ready Workforce

Ron Hodge, Jonathan Rotner, Dr. Inna Baron, Diane Kotras and Dean Worley

April 2020

©2020 The MITRE Corporation. All Rights Reserved. Approved for Public Release.
Distribution unlimited. Case number 20-0975

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

See www.mitre.org/publications/technical-papers/designing-a-new-narrative-to-build-an-ai-ready-workforce

Organization: Workforce Development

Approach

Cultivate a public AI workforce that *wants* to engage with the DoD.

Change the narrative to change the outcome

- Acknowledge and accept the DoD's history
- Share examples of efforts that reflect values of audience
- Relate long-standing practices of responsible tech deployment
- Use established and new ways to target your audience

Rethink how to attract and retain capable people

- Use financial and other incentives and expand existing pipelines (like ROTC)
- Raise AI literacy for the entire workforce, not just coders
- Expand opportunities for partnering with start-ups

Technology: Innovation

Challenges

Questions

- How much can AI-enabled systems improve mission outcomes?
- How will operational procedures and timelines change?
- Could there be adoption and trust issues that mitigate impact?
- Should the AI-enabled system provide recommendations or make autonomous decisions?

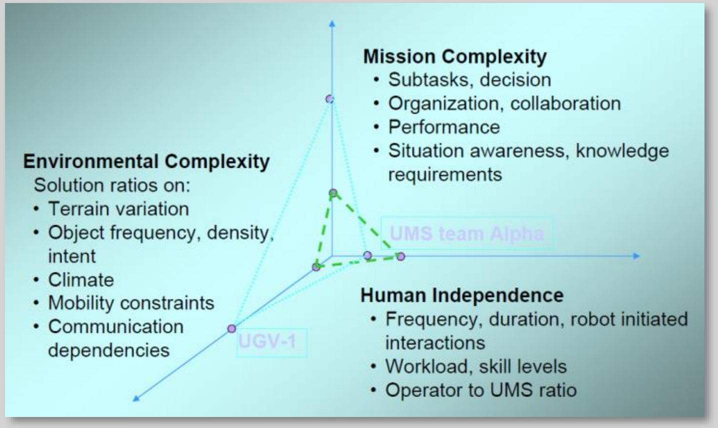
Issues

- Proliferation of concepts for AI-enabling systems
    - Especially involving autonomous systems
- Need for mission-level simulations to support analysis of AI-enabled systems and their impact
    - But current battle simulations typically don’t represent the effects of AI-enabled system concepts out-of-the-box

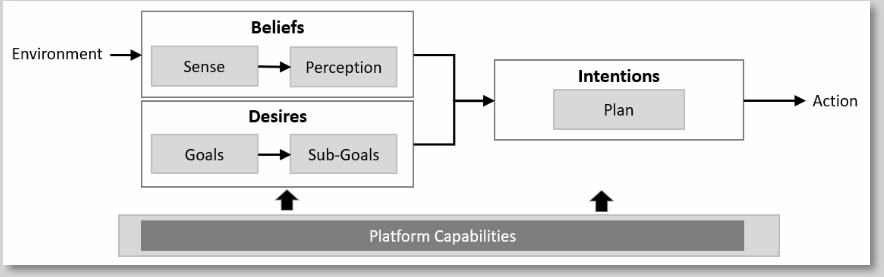
Generating guiding principles, and enhancing our simulations, to be able to evaluate emerging AI-enabled system concepts.

Technology: Innovation

Approach



Autonomy Levels Framework for Unmanned Systems, NIST, 2008.



Consider using Conceptual Frameworks

- **Helps create transparent, formalism-guided models**
- **In particular, consider the BDI conceptual framework in unmanned systems context**

Understand the relationship between AI and Autonomous Systems

- Modeling the human controlled ↔ autonomous behavior continuum

Research Intelligent Systems Modeling best practices

- Approaches: mathematical simplifications, graphical approaches, conceptual frameworks, cognitive architectures, and hybrids of these
- Use Conceptual Frameworks for modeling most AI-enabled system behaviors
  - Provide formal, guided approach for range of AI-enabled behaviors
- Use Beliefs, Desires, and Intentions (BDI)*** framework in particular
  - Explainability and transparency
  - Abundance of open source literature, and models to start from

Define key simulation capability tenets for AI-enabled systems

- Domain Strength
- Modeling Flexibility
- Model Transparency
- Fidelity Matching
- External Interfacing

Map candidate simulations to tenets; recommend enhancement paths

*** Rao, A.S., Georgeff, M.P., (1995). BDI Agents: From Theory to Practice, in: Proceedings of the First International Conference on Multiagent Systems, Edited by L. Gasser and V. Lesser. San Francisco, CA, pp. 312–319.

MITRE

Operations & Maintenance: Solution Monitoring

Challenges

Questions

- How can we ensure that a model continues to perform as expected after it is deployed?
- Can we detect a drop in performance and react to it?
- Can we anticipate a drop in performance and prevent it?
- How can we certify a model with quantifiable, reliable guarantees of expected performance?
- How can we accomplish all this efficiently?

Issues

- Source and target are distributed differently
- Target is unknown in advance or changes over time
- If users notice drop in performance, they lose trust
- If users don't notice drop in performance, errors propagate

← Source (training data)

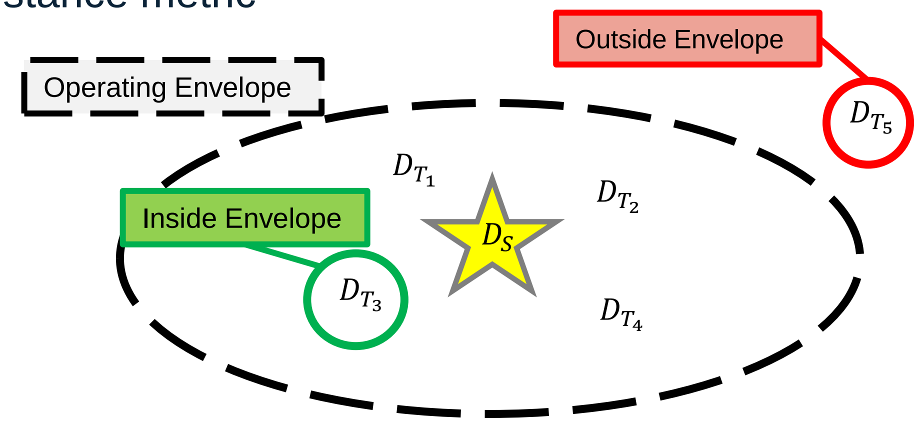
Target → (operational data)

AI/ML will need performance guarantees to be dependable in mission- and safety-critical systems, but performance depends on the data.

Operations & Maintenance: Solution Monitoring

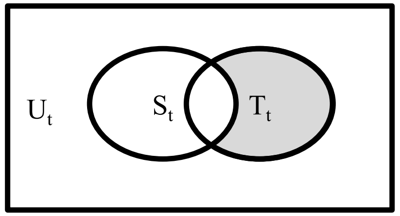
Approach

A. Distance metric



B. Coverage metric

Source
- Military plane in field
- Military plane in daylight



Target
- Military plane in field in daylight

This approach is based on work from the University of Virginia, Old Dominion University, and Virginia Tech. Look for their talk later in this workshop.

Define operating envelopes of models

A. Measure distance between source and target data distributions

B. Use metadata to measure proportion of target data covered by source data

Incorporate operating envelopes into an efficient, automated process to ensure certification

1. Search model zoo for model with sufficient predicted performance based on metrics
2. Create ensemble of models from model zoo with sufficient predicted performance
3. Fine-tune model with more target data
4. Identify unlabeled data to collect based on metrics
5. Identify labeled data to collect based on metrics

Increasing Cost

Operations & Maintenance: Trust

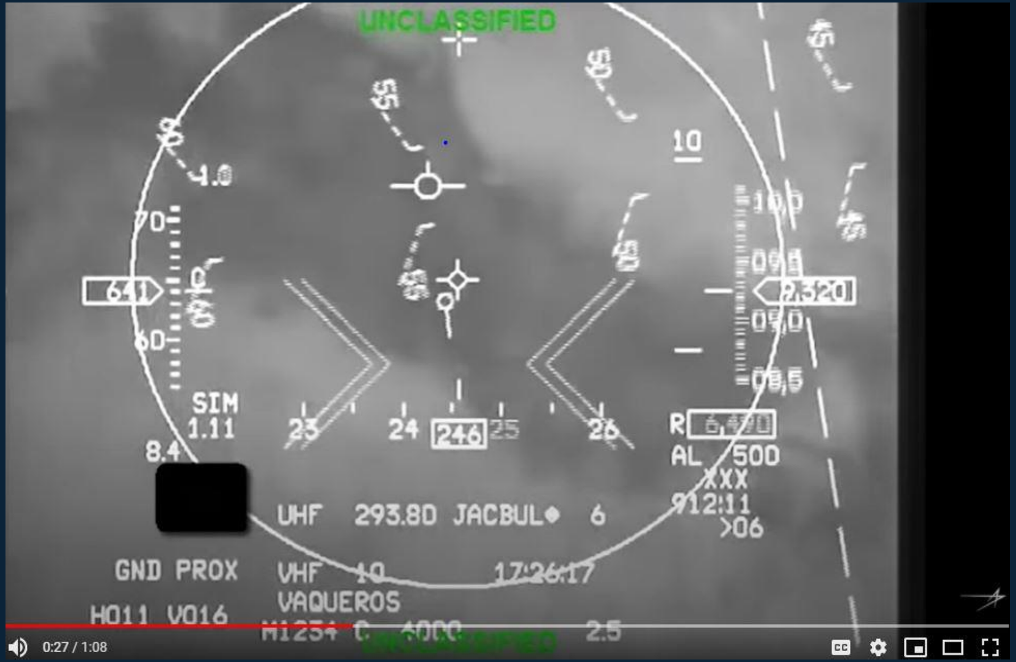
Challenges

Questions

- <u>Partnership</u>: How can we design technologies to be adaptive partners that augment human work in a game-changing way? [realize 3rd Offset]
- <u>Adoption</u>: How can we position the new technologies to not only be adopted, but to succeed with impact?
- <u>Trust</u>: How can we ensure appropriate trust in technologies used in time-sensitive, high stakes, ambiguous situations?

Issues

- Technologies developed without user engagement to understand ‘why AI’ and ‘what AI functionality is needed’
- Technology adds time and work; does not solve user’s needs
- Investment wasted; technology turned off



Automated Ground Collision Avoidance System (Auto-GCAS)
See www.youtube.com/watch?v=bF6VN1e7LMg

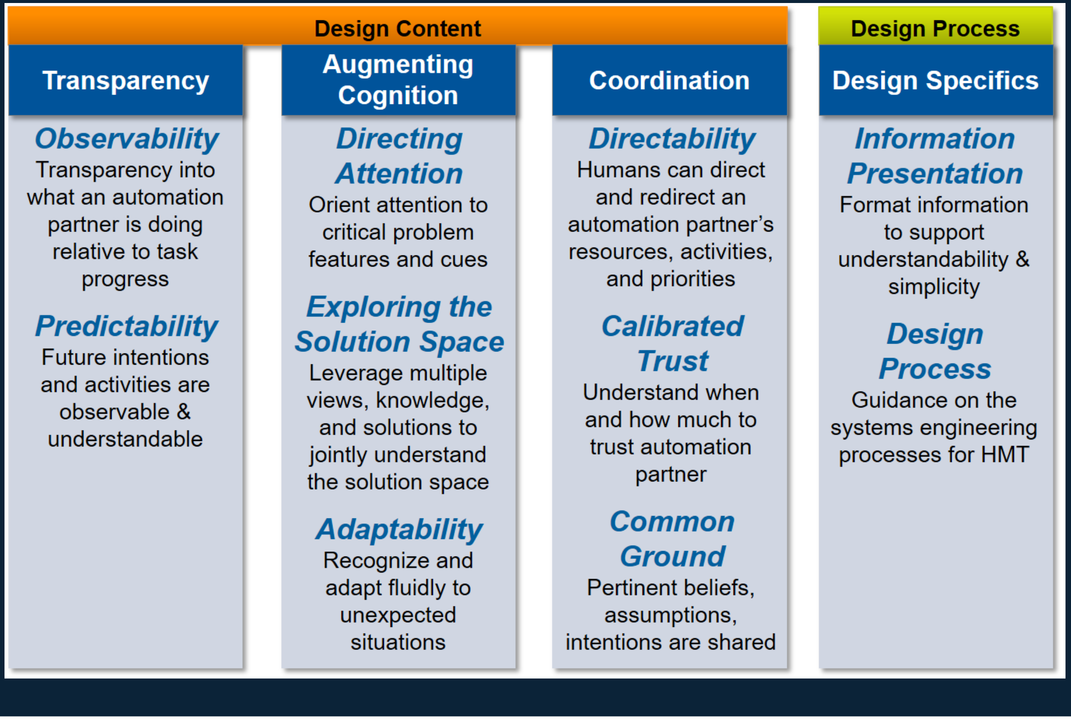
HMT is defined as adaptive, bi-directional team interaction among humans and machines that augments human capabilities for improved mission outcomes.

MITRE

Operations & Maintenance: Trust

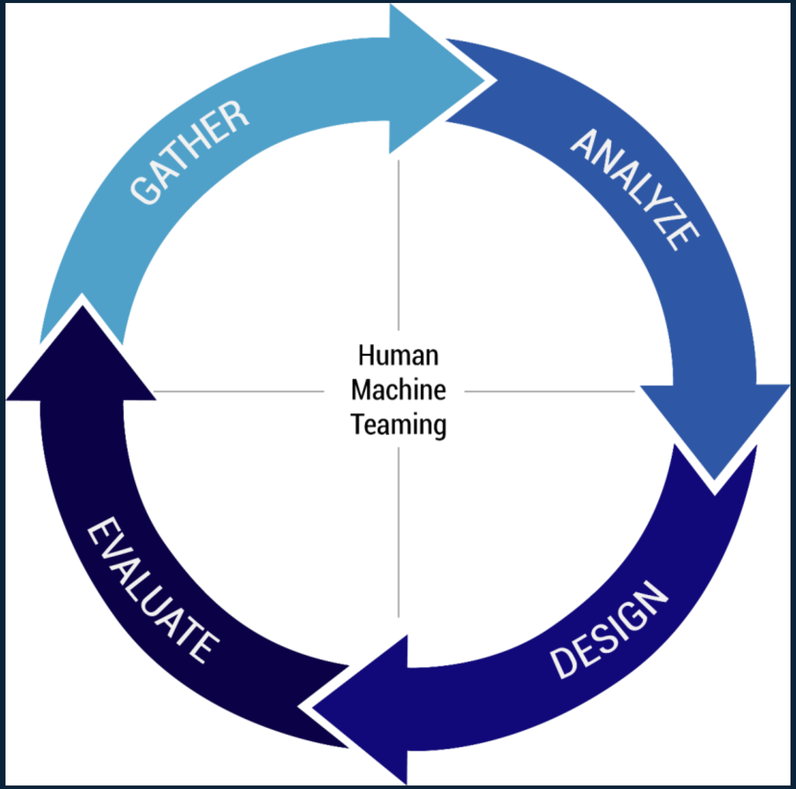
Approach

Apply Framework of
Research-Driven Principles



Design Content			Design Process
Transparency	Augmenting Cognition	Coordination	Design Specifics
Observability Transparency into what an automation partner is doing relative to task progress ***Predictability*** Future intentions and activities are observable & understandable	***Directing Attention*** Orient attention to critical problem features and cues ***Exploring the Solution Space*** Leverage multiple views, knowledge, and solutions to jointly understand the solution space ***Adaptability*** Recognize and adapt fluidly to unexpected situations	***Directability*** Humans can direct and redirect an automation partner's resources, activities, and priorities ***Calibrated Trust*** Understand when and how much to trust automation partner ***Common Ground*** Pertinent beliefs, assumptions, intentions are shared	***Information Presentation*** Format information to support understandability & simplicity ***Design Process*** Guidance on the systems engineering processes for HMT

Engage in Cyclical SE Process:
Gather, Analyze, Design, and Evaluate



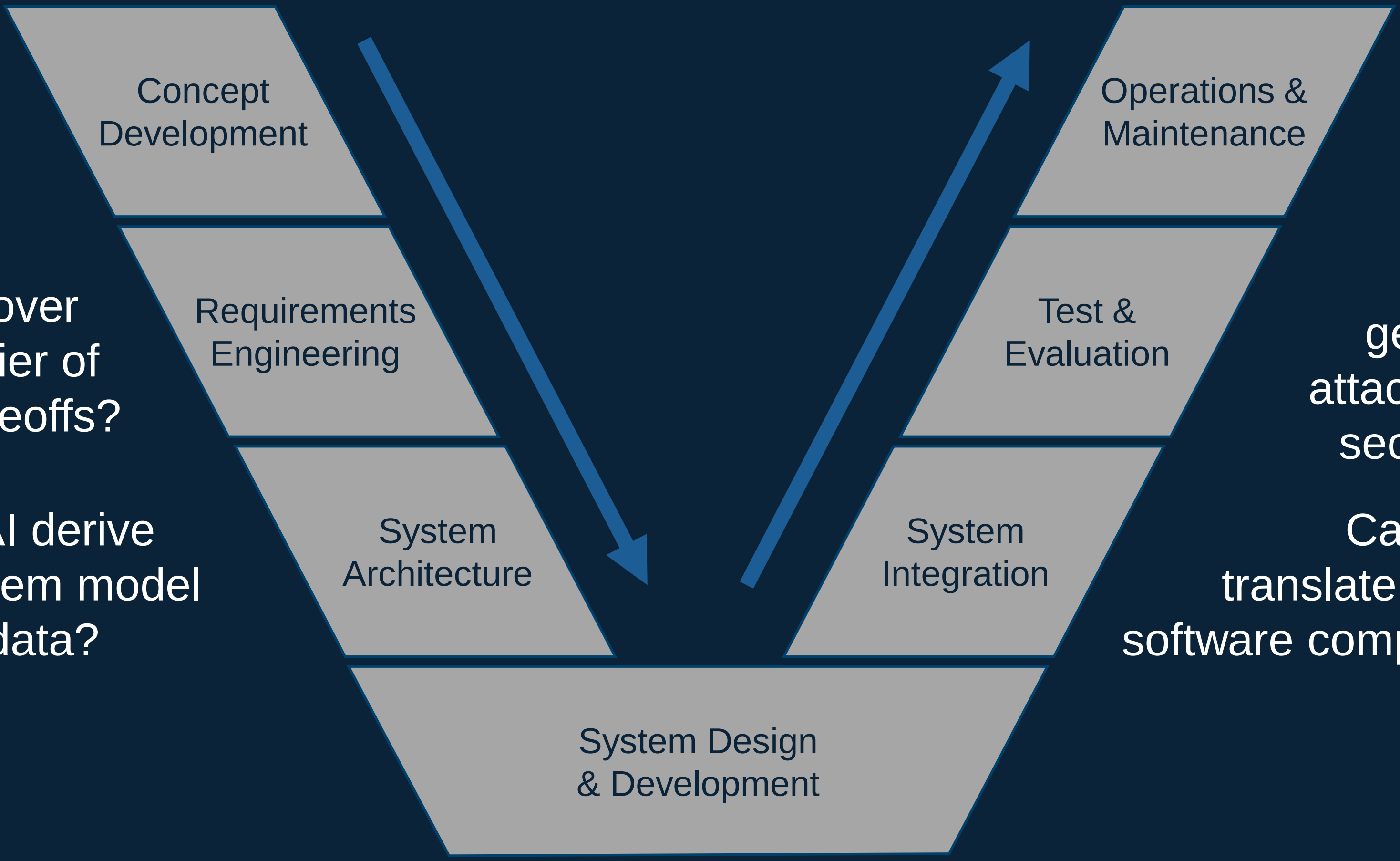
See www.mitre.org/publications/technical-papers/human-machine-teaming-systems-engineering-guide

AI4SE – Opportunities

Can AI discover optimal behaviors for new system concepts in M&S?

Can AI discover Pareto frontier of optimal tradeoffs?

Can AI derive a system model from data?



Can AI identify thresholds when models should be updated?

Can AI help generate cyber attacks to support security testing?

Can AI help translate between software components?

Can AI optimize the overall system design?

Conclusions

MITRE's AI Maturity Model can serve to organize SE4AI

There are many examples of ongoing work in SE4AI across MITRE

There are opportunities for AI4SE, but not as much ongoing work to my knowledge

There is still much to do!

- How can SE help the reality of AI live up to the promise?
- How can AI help increase the efficiency of SE?

How can we combine AI and SE to tackle today's biggest challenges?

Questions?

Peter Schwartz, PhD

pschwartz@mitre.org

in www.linkedin.com/in/peterjschwartzphd/

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™