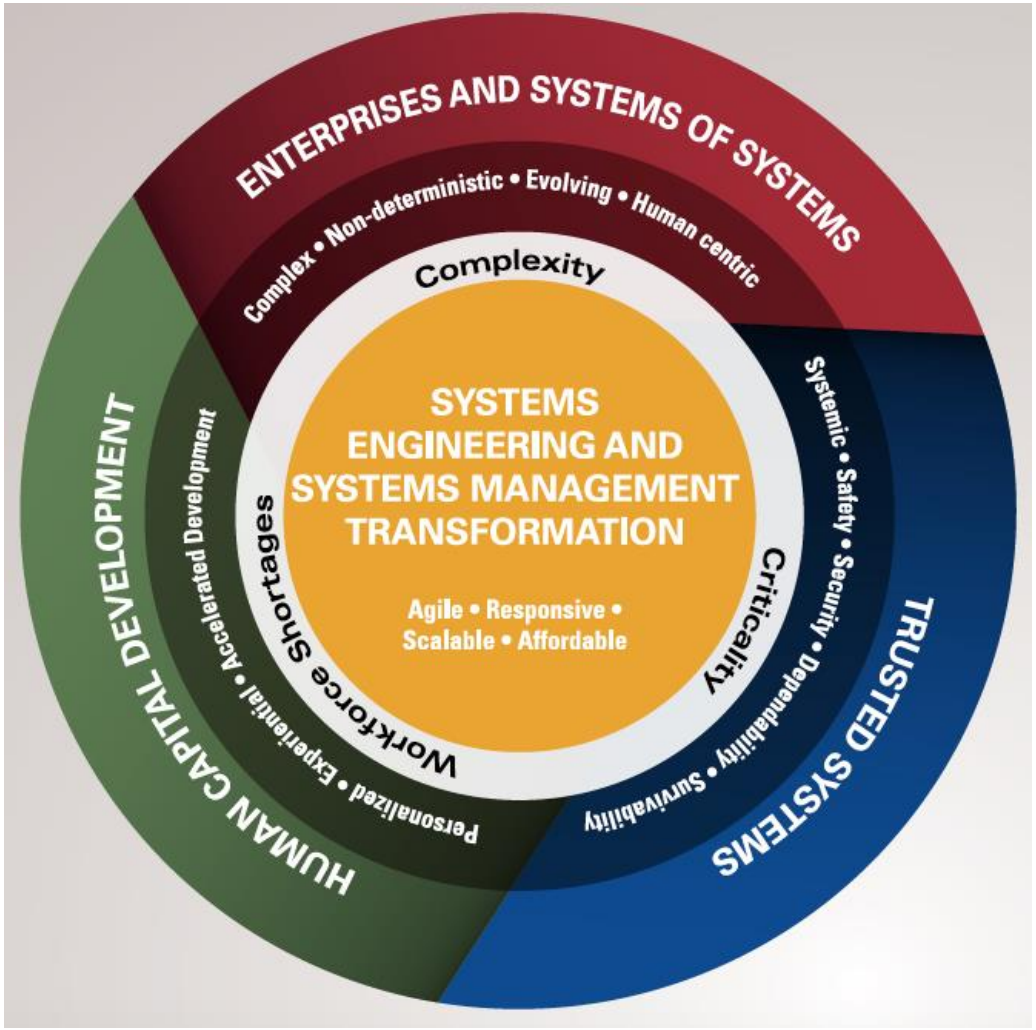
A Framework to Guide AI/ML and Autonomy Research in Systems Engineering

22nd Annual NDIA Systems and Mission Engineering Conference

Tom McDermott, Deputy Executive Director, SERC
Stevens Institute of Technology – October 24, 2019

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract H98230-08-D-0171. The SERC is a federally funded University Affiliated Research Center (UARC) managed by Stevens Institute of Technology consisting of a collaborative network of over 20 universities. More information is available at www.SERCuarc.org

SERC Research Thematic Areas



Enterprises and SoS

- *Enterprise and System of Systems Modeling and Analysis*
- *Mission Engineering*

Trusted Systems

- *Systemic Security*
- *Systemic Assurance*

Human Capital Development

- *Evolving Body of Knowledge*
- *Experience Acceleration*
- *SE and Technical Leadership*
- *Emerging/Critical Areas*

SE & Systems Mgmt Transformation

- *SE for Velocity and Agility*
- ***Digital Engineering***
- ***SE Methods for AI and Autonomous Systems***

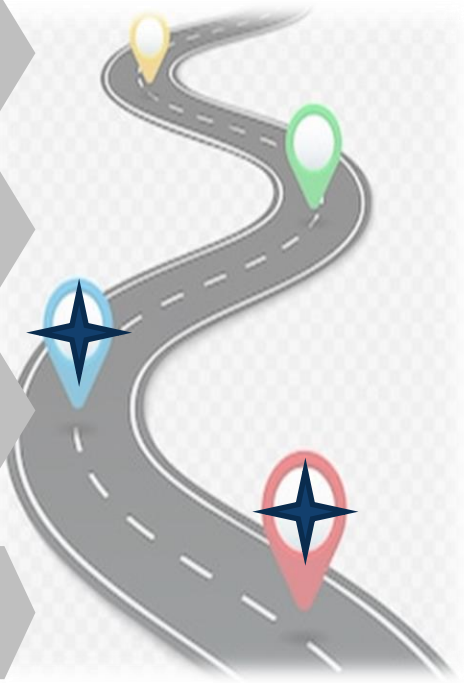
SERC Research Areas and Missions

Mission Engineering

	TRUSTED SYSTEMS	ENTERPRISES AND SYSTEMS OF SYSTEMS	SYSTEMS ENGINEERING AND MANAGEMENT TRANSFORMATION	HUMAN CAPITAL DEVELOPMENT
V	**VELOCITY** Developing and sustaining capabilities that support emergent and evolving mission objectives (deter and defeat emergent and evolving adversarial threats and exploit opportunities, affordably and with increased efficiency)			
S	**SECURITY** Designing and sustaining the demonstrable ability to safeguard critical technologies and mission capabilities in the face of dynamic (cyber) adversaries			
A	**AI & AUTONOMY** Developing and supporting system engineering MPTs to understand, exploit and accelerate the use of AI and autonomy in critical capabilities			

Digital Engineering

SERC Technical Plan Roadmaps



SYSTEMS ENGINEERING RESEARCH CENTER

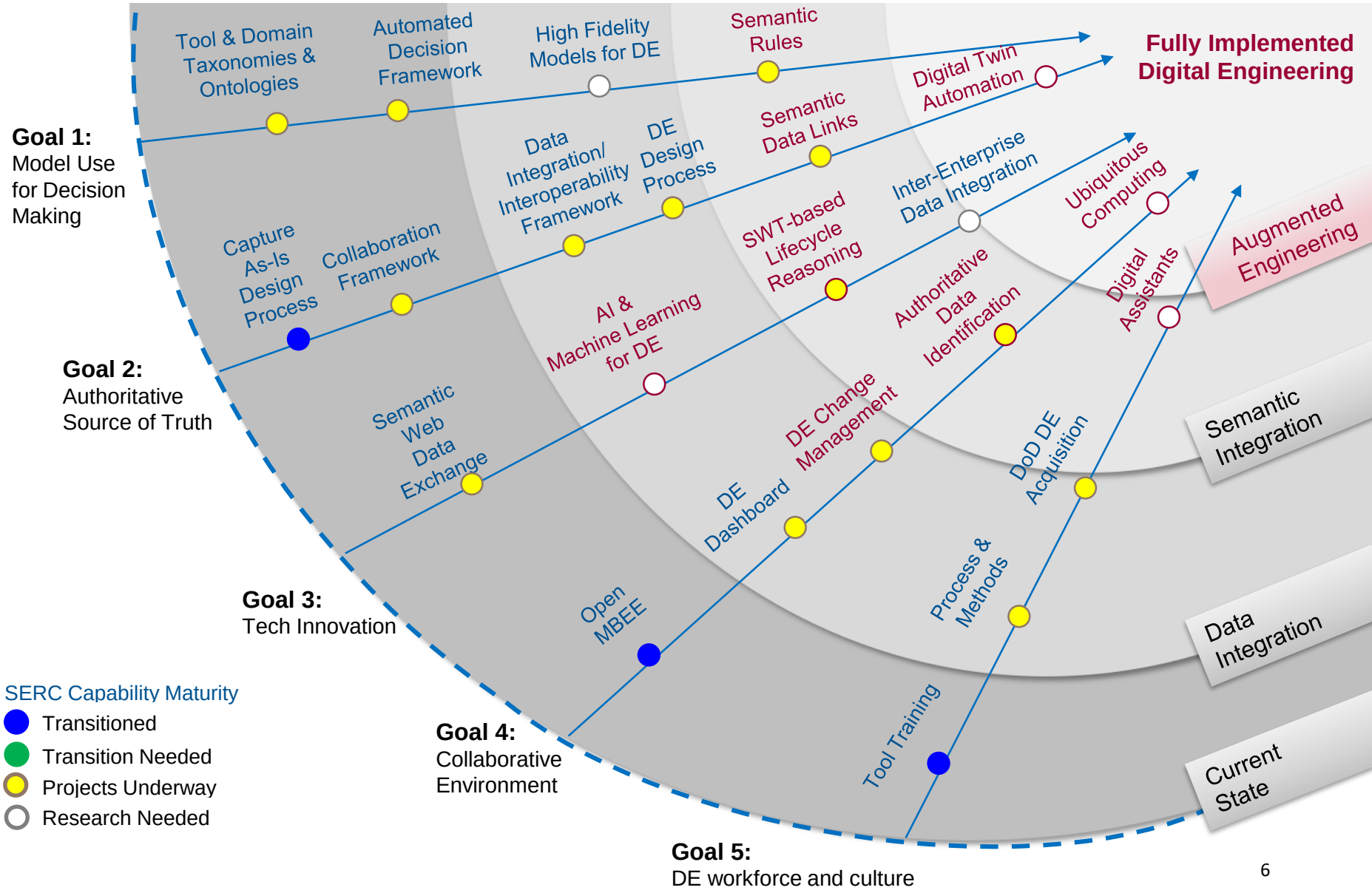
Which of These Digital Innovations will Transform the Engineering Disciplines?

- **5G mobility** – enhanced bandwidth and connectivity mobile services
- **Collaborative telepresence** – Highly realistic, haptics enabled video conferences
- **AI and ML** – Artificial Intelligence and Machine Learning
- **Immersive Realities** – Human, Augmented, and/or Virtual Reality technology integration
- **Blockchain** – Blockchain derived technologies to manage workflows
- **Cloud Evolution** – Evolving cloud computing architectures
- **NL/Chatbots/social robots** – true human realistic natural language interfaces
- **IoT** – Internet of Things sensors and architectures
- **Low-code SW** – Domain specific design languages/visual composition design methods
- **DevSecOps** – Secure Continuous development and deployment environments
- **Quantum computing** – Evolving non-binary computing architectures
- **Advanced Manufacturing** – Rapid programming/realization of hardware design
- **DNA-based Data Storage** – High speed, ultra-high capacity storage devices
- **Digital Identities** – Computer (not human) determines identity verification

* SERC Project WRT-1001 presented to the Digital Engineering Working Group 08/2019

SYSTEMS ENGINEERING RESEARCH CENTER

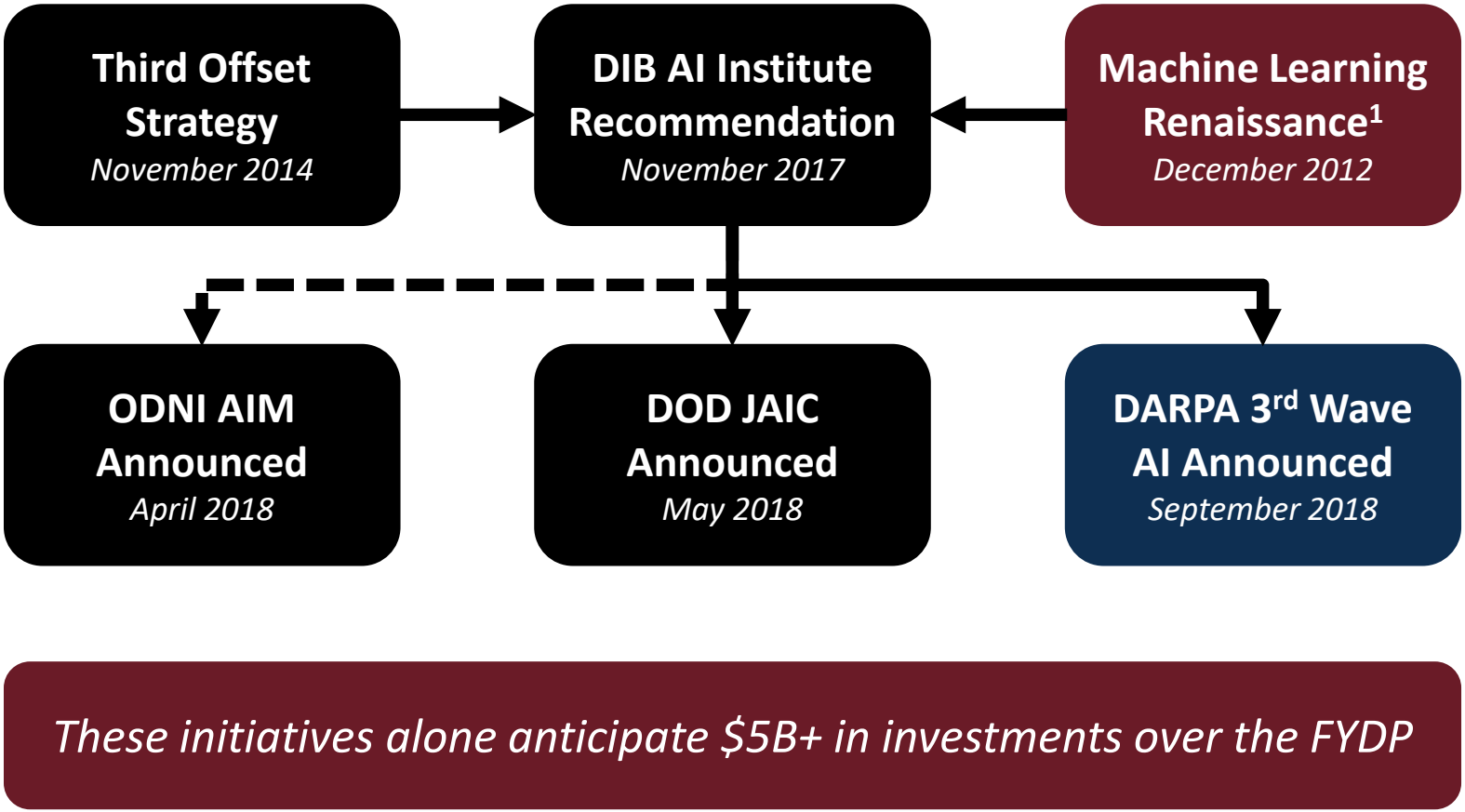
Research Roadmap: Digital Engineering for Systems Engineering



DE Research – Enabler for other Strategies

- Mature AI/ML applications for SE based on knowledge representation using ontological representations for mission and systems engineering developed in ongoing research
- Model-Based System Assurance, maturing knowledge-driven safety/dependability/security processes, methods, and tools
- Digital Engineering as an enabler for Velocity and Agility
  - —Employing MBSE to manage system architecture for DevOps
  - —Core enabler to Lifecycle Ready AI
- Digital Engineering to transform Test and Evaluation
  - —Application of MBSE formalisms and methods to T&E activities
  - —Development of T&E methodologies for machine learning and automation

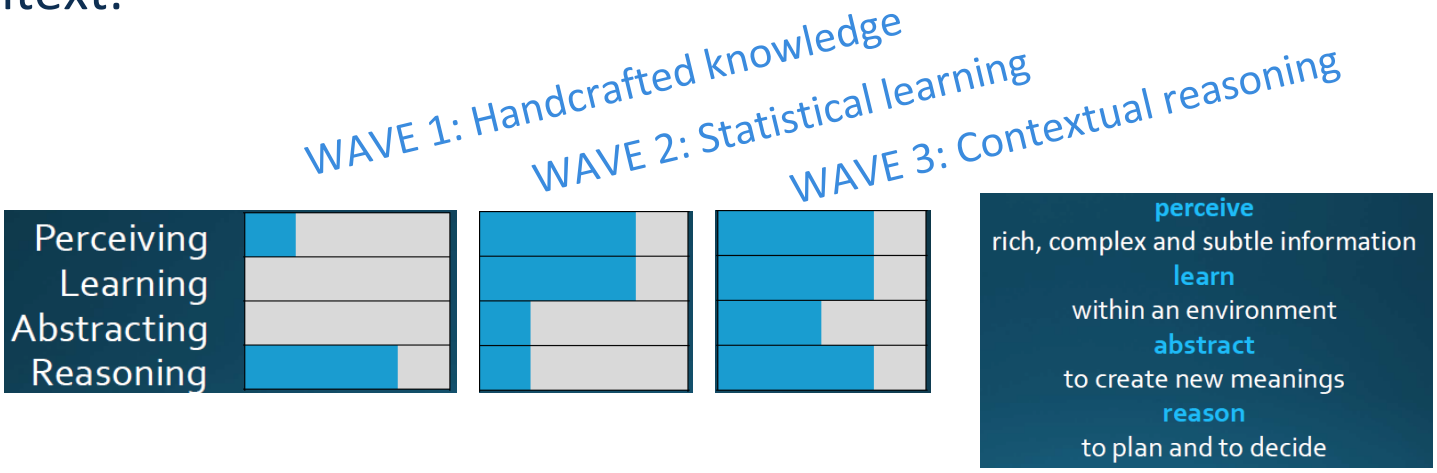
AI Eats the World…
(while Engineering goes Digital)



[1] Krizhevsky, Sutskever, Hinton, "ImageNet Classification with Deep Convolutional Neural Networks", NIPS 2012

Fundamental Research in AI and ML Technology – needed for use in design

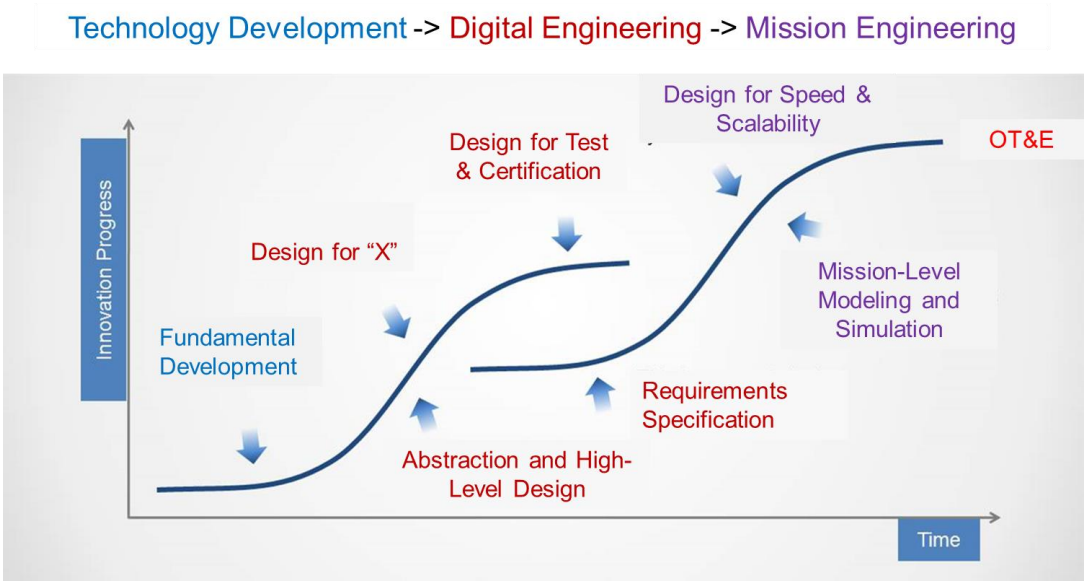
- Multi-Modal AI – holistic analysis of multi-modal data with the aim to produce actionable intelligence for decisions
- Cognitive Bias – intentionally or unintentionally misleading decision-making in AI systems
- Contextual Adaptation and Sensemaking – AI that perceives and learns context:



- Design principles for AI – confident exploration of design space for learning-enabled systems

AI/SE Research Framework

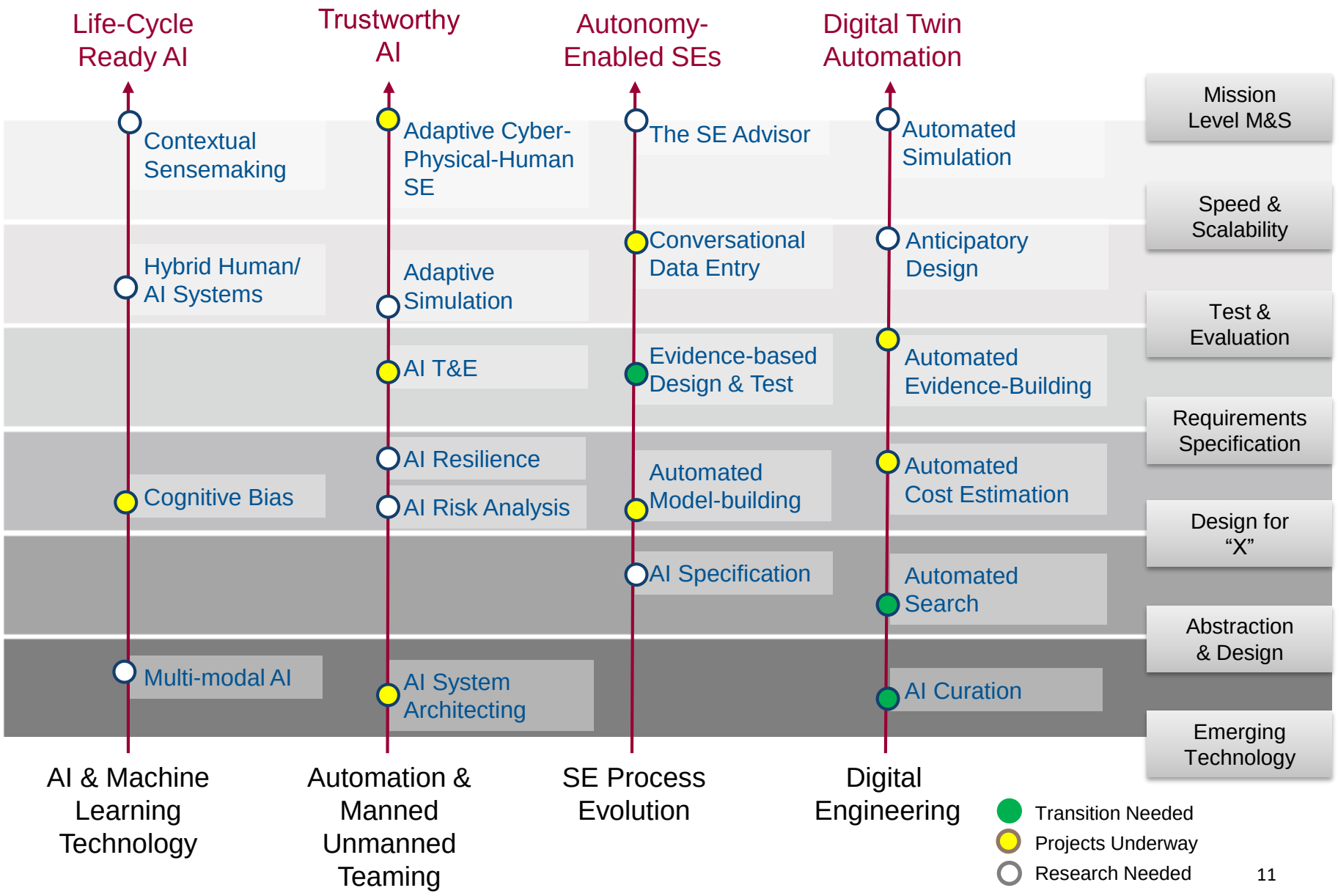
- AI/ML and Autonomy encompass a broad range of methods, processes, tools, and technologies
- There is not yet a clear vision for a roadmap linking AI/ML, Autonomy, and SE – but we can categorize research areas in an evolutionary framework
- Major "verticals":
  - —AI/ML Technology
  - —Automation & Teaming
  - —SE Process Evolution
  - —Digital Engineering



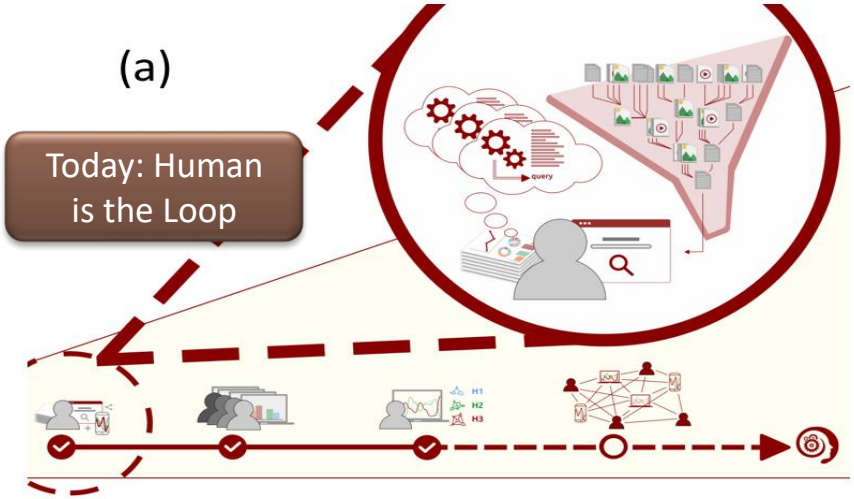
The "Double S" curve of Tech innovation provides an effective categorization of SE Research contributions to emerging technology

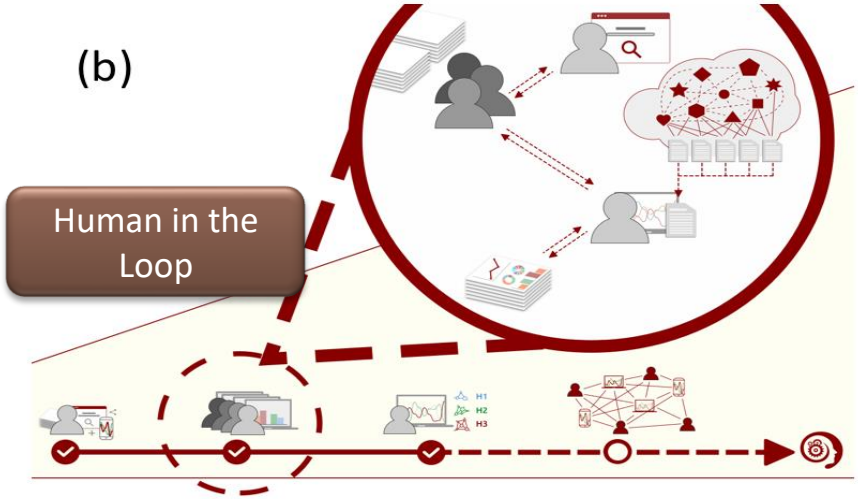
SYSTEMS ENGINEERING RESEARCH CENTER

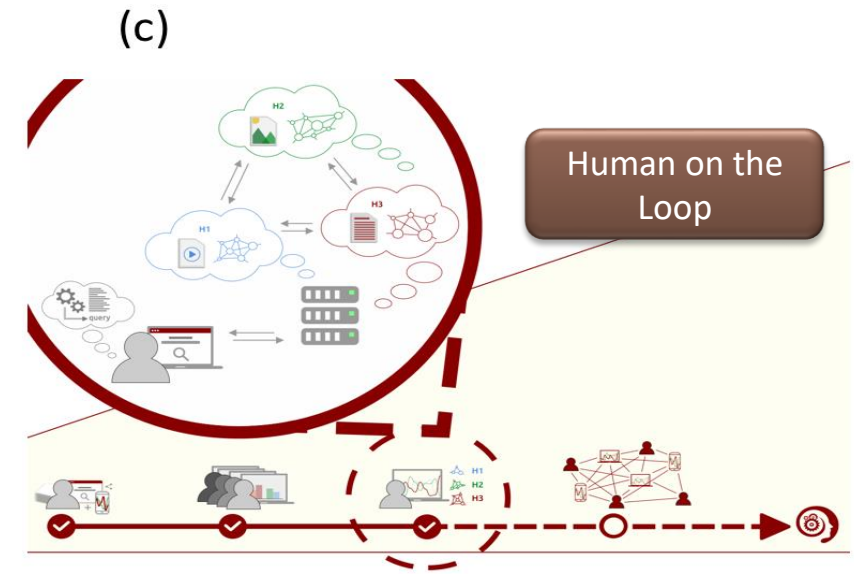
SERC AI/Autonomy/SE Research Classification Framework



Hybrid Systems for Sensemaking: Evolution of AI for SE



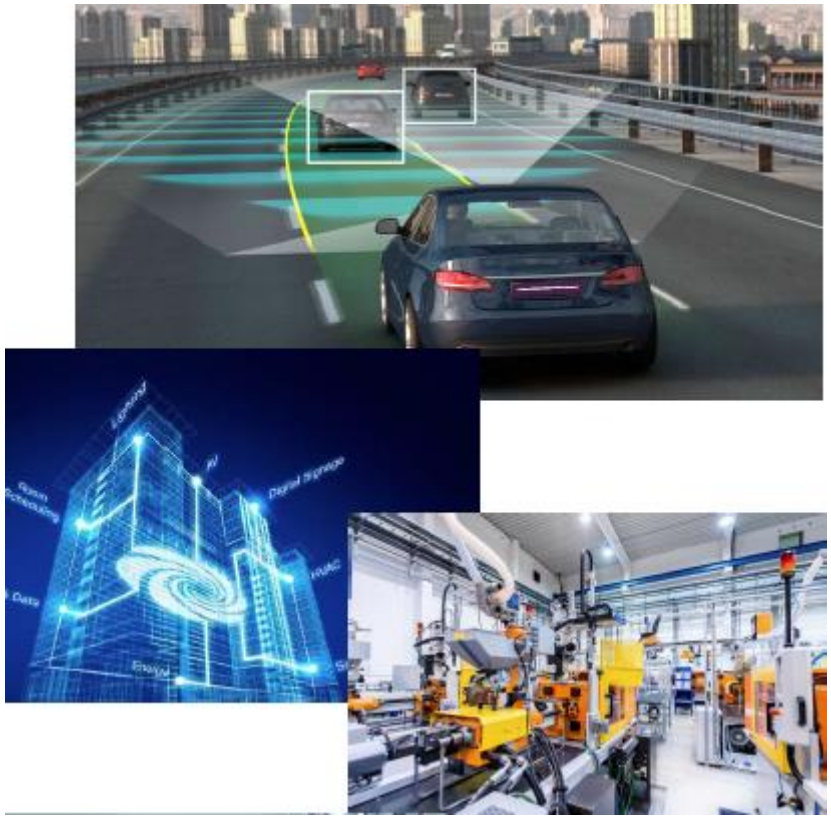




As human leaves loop, lifecycle issues and contextual learning become more and more important

Automation and Manned/Unmanned Teaming

- Adaptive Cyber-Physical-Human Systems – modeling of cyber-physical systems as influenced by humans, from requirements analysis to design
- Adaptive Simulation – Computer based simulation and training that supports non-static objectives (pick-up games)
- **Trustworthy AI – AI systems that self-adapt while maintaining rigorous safety and security and policy constraints**



Systems Engineering Process Evolution

- AI abstraction – library tools and methods that abstract AI algorithms and modules to general engineering
- AI Specification – a requirements specification and management process for adaptation and learning in systems (blending agile, devops, etc.)
- Evidence-based design and test – formal methods and processes that move from explicit verification of composition to evidence building
- Conversational data entry: human-computer interaction processes to convert natural language and other media to formal models
- The SE Advisor – a conversational system that automates many mundane data exploration and engineering calculation tasks
- **Autonomy enabled SEs – we become masters at deploying "autonomy as a design variable"**

Image: https://internetofbusiness.com/ai-will-augment-and-diversify-human-thinking-says-tata-communications/

Excerpt from the DoD AI Strategy

1. **Objective: Scaling AI's impact across DoD through a common foundation that enables decentralized development and experimentation.**
   - Ensure interoperability is considered early in the design lifecycle. This will help mitigate the risk of creating AI tools that are powerful for narrow applications but fail in joint settings. In addition, USD(R&E) will help mature the DoD's AI Engineering discipline. This includes developing the systems engineering, sustainment and assessment methods, processes, and tools to deploy AI-embedded capabilities.

AI Enabled Digital Engineering

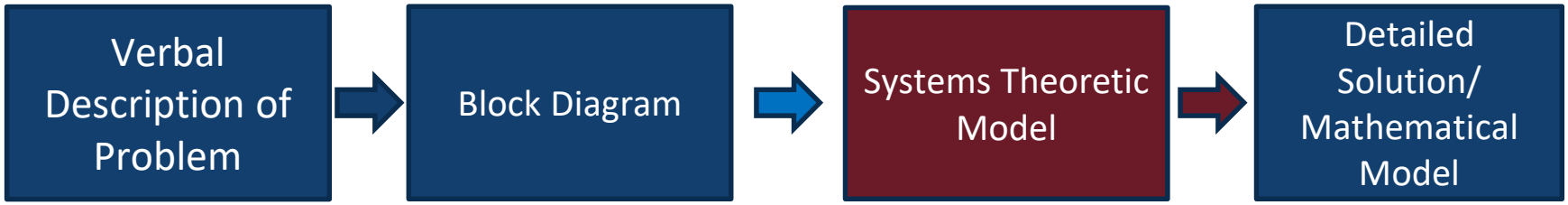
- AI Curation - data management and curation to support evolving application of AI capabilities
- Automated search, model-building, and cost estimation – application of ML to historical data and relationships
- Automated evidence building – automation of certification processes via models and Quality Assurance data
- Anticipatory design – anticipating system emergence (failures, etc.) from design & operational data
- Automated Simulation – use of simulation to train and evaluate ML, evolution of GANs
- **Digital Twin Automation – real-time continuous learning from real system and shadow simulations**

  — From zero history to unlimited history?

Image: https://survicate.com/customer-feedback/ai-in-marketing/

Building Theoretical Foundations for Lifecycle AI

- **Systems theory** provides an approach for modeling lifecycle challenges faced by AI systems in a framework naturally rooted in systems design and analysis
- Mathematical superstructure for learning that allows learning algorithms to be formally studied in the context of the systems within which they operate
- Models of random processes undergone by systems can lead to principled design and operational decision-making



Summary: Key AI/Autonomy Research Goals

- **AI for SE:** AI/ML to support the practice of SE
  - —Support scale in digital model construction
  - —Create confidence in design space exploration
- **SE for AI:** SE approaches to systems with AI/ML capabilities
  - —Principles of learning-based systems design
  - —Models of life cycle evolution, Model curation methods
- **Lifecycle Ready AI:**
  - —AI-related agility: new SE methods and tools that anticipate adaptation
  - —Technical and management policies that assure lifecycle-ready AI
- **Systems Validation of AI:**
  - —Early visibility for deployment, validation of post-deployment changes
  - —System level testbeds – to study systems, not just data & algorithms

Questions and Discussion