RESEARCH ROADMAPS 2019-2020

SYSTEMS ENGINEERING RESEARCH CENTER

ROADMAP CONTRIBUTORS

SERC LEADERSHIP

Dr. Dinesh Verma

Mr. Thomas McDermott, Jr.

Ms. Kara Pepe

Stevens Institute of Technology

SERC RESEARCH COUNCIL

Dr. Mark Blackburn

Stevens Institute of Technology

Dr. Barry W. Boehm

University of Southern California

Dr. Paul D. Collopy

University of Alabama in Huntsville

Dr. John M. Colombi

Air Force Institute of Technology

Dr. Olivier de Weck

Massachusetts Institute of Technology

Dr. Daniel A. DeLaurentis

Purdue University

Dr. Barry Horowitz

University of Virginia

Dr. William B. Rouse

Georgetown University

Dr. Valerie Sitterle

Georgia Tech Research Institute (GTRI)

Dr. Jon Wade

Stevens Institute of Technology

ADDITIONAL CONTRIBUTORS

Dr. Peter Beling

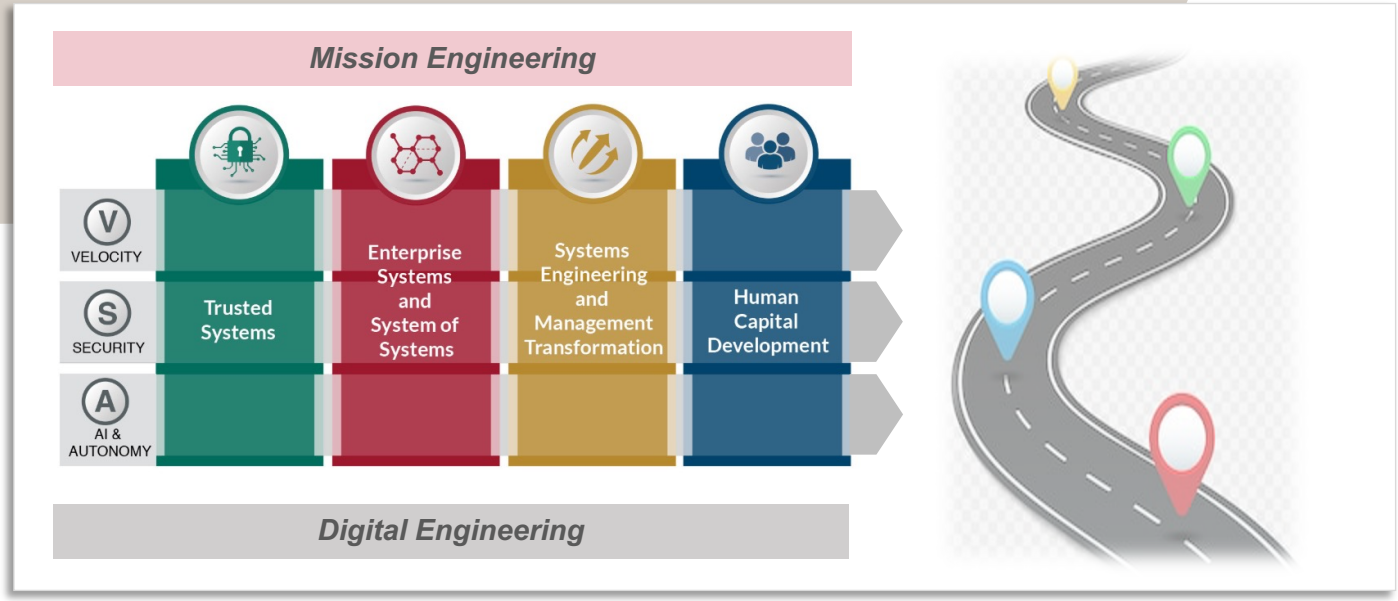
University of Virginia

Dr. Mary Bone

Stevens Institute of Technology

ABOUT THE ROADMAPS

The SERC research strategy aligns three mission areas which are supported by four Research Areas: *Enterprises and Systems of Systems* (ESOS), *Trusted Systems* (TS), *Systems Engineering and Systems Management Transformation* (SEMT) and *Human Capital Development* (HCD). The mission areas that the SERC is addressing are:



Velocity: Developing and sustaining timely capabilities that support emergent and evolving mission objectives (deter and defeat emergent and evolving adversarial threats and exploit opportunities, affordably and with increased efficiency).

Security: Designing and sustaining the demonstrable ability to safeguard critical technologies and mission capabilities in the face of dynamic (cyber) adversaries.

Artificial Intelligence (AI) and Autonomy: Developing and supporting system engineering MPTs to understand, exploit and accelerate the use of AI and autonomy in critical capabilities.

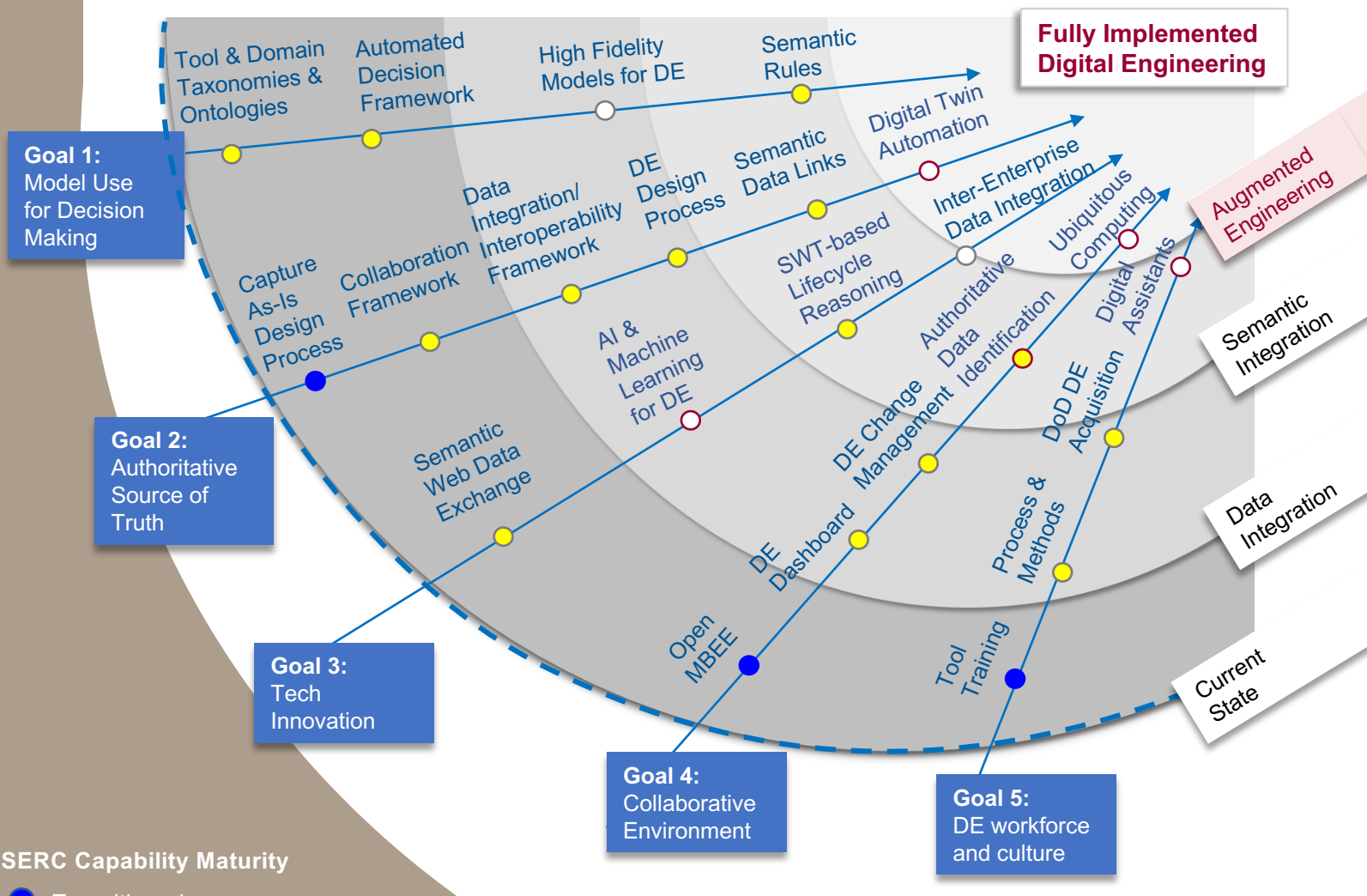
These are enabled by **Digital Engineering**: the transformation of the Systems Engineering discipline from document based methods and artifacts to linked digital data and models.

The missions and research areas are guided by the SERC Technical Plan, which outlines a 5-year vision for each of the four research areas. In this summary you will find four roadmaps providing more detail on the crosscutting mission areas. These were developed as a collaborative effort by our SERC Research Council over a 5-month effort in 2019. Each roadmap has a set of verticals leading to a visionary outcome or set of outcomes, and a set of capabilities we believe are needed to meet those long term outcomes. The capabilities are color coded by our assessment of the current capability. Following each roadmap are bullet form descriptive summaries of each capability.

The listed capabilities reflect not only SERC research, but other areas of research either known to be active or prioritized by our sponsors and the systems engineering community in general and our sponsors. It is our hope by sharing this work we will guide not only SERC research but also the transformation of the systems engineering discipline in general.

Research Roadmap: Digital Engineering For Systems Engineering

Digital Engineering forms the basis for all three of the SERC crosscutting missions and resulting research roadmaps. We are leading a systems engineering transformation process that is based on the use of data (an Authoritative Source of Truth) and collaboration using models (Collaborative Integrated Modeling Environments). The Digital Engineering research roadmap aligns with the five goals of our DoD sponsor's strategy: (1) Model Use for Decision Making; (2) the Authoritative Source of Truth (AST); (3) Technological Innovation; (4) Collaborative Environments; and (5) Workforce and Cultural evolution. The progression in Digital Engineering is expected to begin with data integration in the AST followed by the semantic integration of models. We expect to soon see advances in Augmented Intelligence – the use of models and "big data", that bring automation to engineering processes and system quality and certification. In our Digital Engineering roadmap you see growing maturity through the many research activities underway (yellow items on the roadmap progression).



SERC Capability Maturity

- Transitioned
- Transition Needed
- Projects Underway
- Research Needed

Goal 1: Formalize the development, integration, and use of models to inform enterprise and program decision-making.

Tool & Domain Taxonomies & Ontologies

- We look to interoperability through ontologies in the future – graph databases for linked data are becoming more prominent; taxonomies provide the starting point for building ontologies, ultimately enabling AI-based reasoning

Automated Decision Framework

- The combination of Ontologies, SysML (descriptive models), and analytics provide a framework for decision making related to alternative analysis across any type of decision, characterized by an objective hierarchy (basis for decision)

High Fidelity Models for DE

- Having the appropriate fidelity model is important for addressing the needed information; our research includes looking at different optimization architectures, and another research challenge it moving back to the parametric space after moving to higher fidelity models

Semantic Rules

- Based on knowledge representations such as ontologies, provides the basis for reasoning (AI) about completeness and consistency

Goal 2: Provide an enduring, authoritative source of truth (AST).

Capture As-Is Design Process Collaboration Framework

- Provides a means for new operational paradigm for gov. insight and oversight as well as more seamless collaboration between industry
- Challenges include Data Rights, IP, security

Data Integration/Interoperability Framework

- A means to analyze data/information across domains, disciplines, and from mission to systems, and downwards to components across the lifecycle

DE Design Process

- Future state as initially reflected by some examples demonstrating the art-of-the-possible by doing "everything" in models, simulations, data, etc. including subsuming processes enabled by an AST

Semantic Data Links

- Semantics such as the use of ontologies provides the basis for more meaningful interrelationships of information, and provides the basis for apply AI

Digital Twin Automation

- This is the "end game" – fully dynamic (automation)

Goal 3: Incorporate technological innovation to improve the engineering practice.

Semantic Web Technology Data Exchange

- Ontology-based and associated SWT infrastructure to enable Data/Information exchange with increasingly more semantics

AI & Machine Learning

- SWT for Ontologies-based Knowledge Representation to enable reasoning about Mission and Systems Engineering to enable Augmented Intelligence: Human + Machines
- Need high performance computing and other technologies

SWT-based Lifecycle Reasoning

- Enabled reasoning across the domains throughout DE lifecycle, including Bayesian analyses

Inter-Enterprise Data Integration

- Data/information seamlessly updated/exchanged continuously in "real-time" cutting across the entire enterprise (technical, manufacturing, cost, risk)

Goal 4: Establish a supporting infrastructure and environments to perform activities, collaborate, and communicate across stakeholders.

OpenMBEE: exemplar to demonstrate model management, DocGen & Views

DE Dashboard – communication on continuous flow of data

- Visualization of multi-parametric and multi-objective information to support decision making
- Personalized based on stakeholder needs

DE Change Management

- Extending change management to consider model management, which is much more "object-based" also aligned to competencies and roles of stakeholders

Authoritative Data Identification

- Automating how to find the "authoritative data" – assisted by AI/ML – understanding what the user is looking for

Ubiquitous Computing

- We won't even think about the underlying computation or where it is stored
- Challenge is managing the access/security

Goal 5: Transform the culture and workforce to adopt and support digital engineering across the lifecycle.

Tool Training

- Challenge is having relevant examples to learning the tools (see methods)

Process & Methods

- Focus more on the methods that characterize the information that must be captured and the associated process that provides guidance in capturing the relevant information to build right system and build the system right (V&V)
- Will be enabled by reason-based AI, that should be aligned with ontologies for relevant domains and applications

DoD DE Acquisition

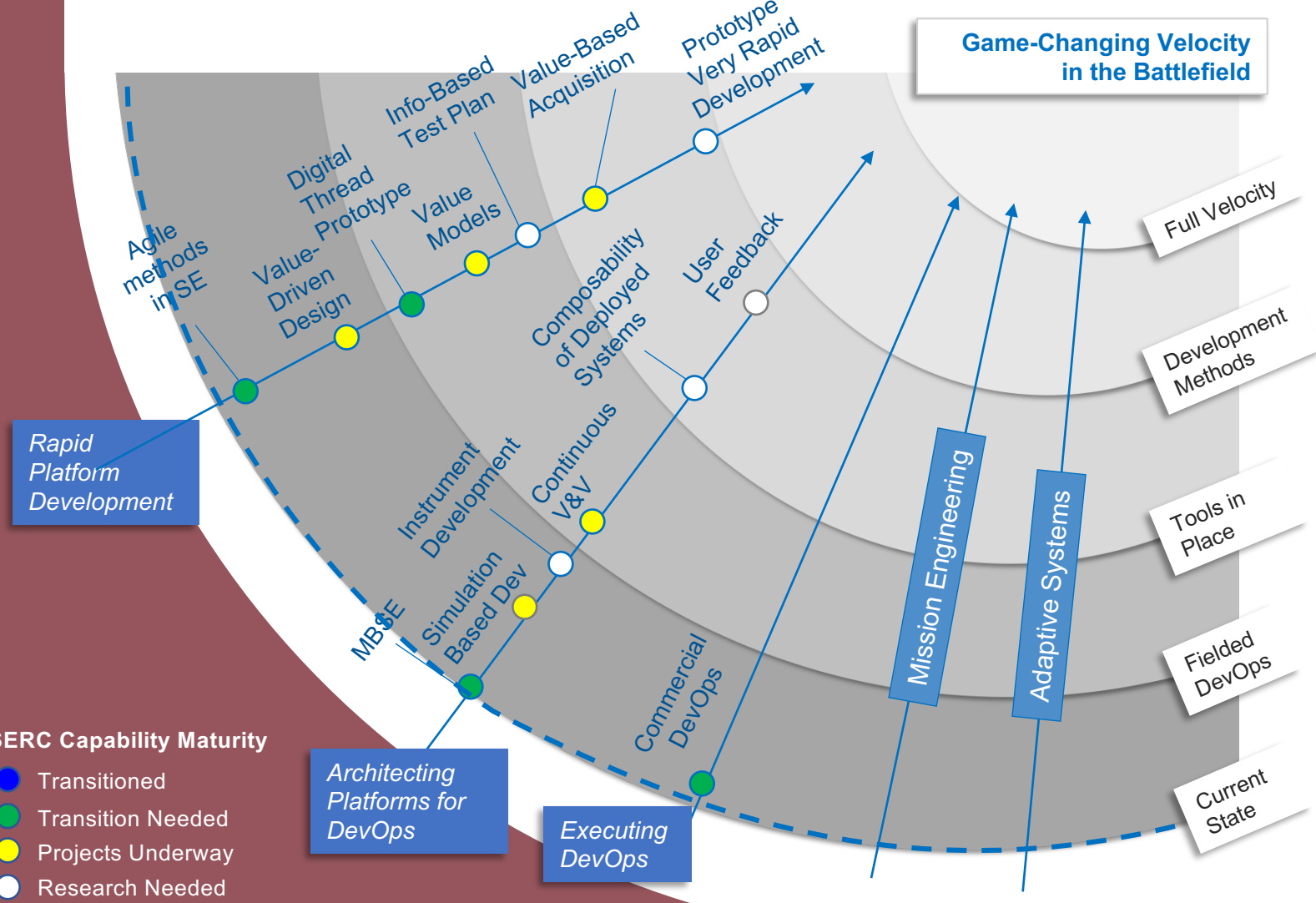
- The new environments, including AST, with change processes and needed DE competencies, as well as influence
- New policies that aligns with the new operational model and information that is required during RFPs
- Transformation of CDRLs to reviews "in the model" in the AST

Digital Assistants

- Trusting AI guidance in engineering and decision making

Research Roadmap: Velocity

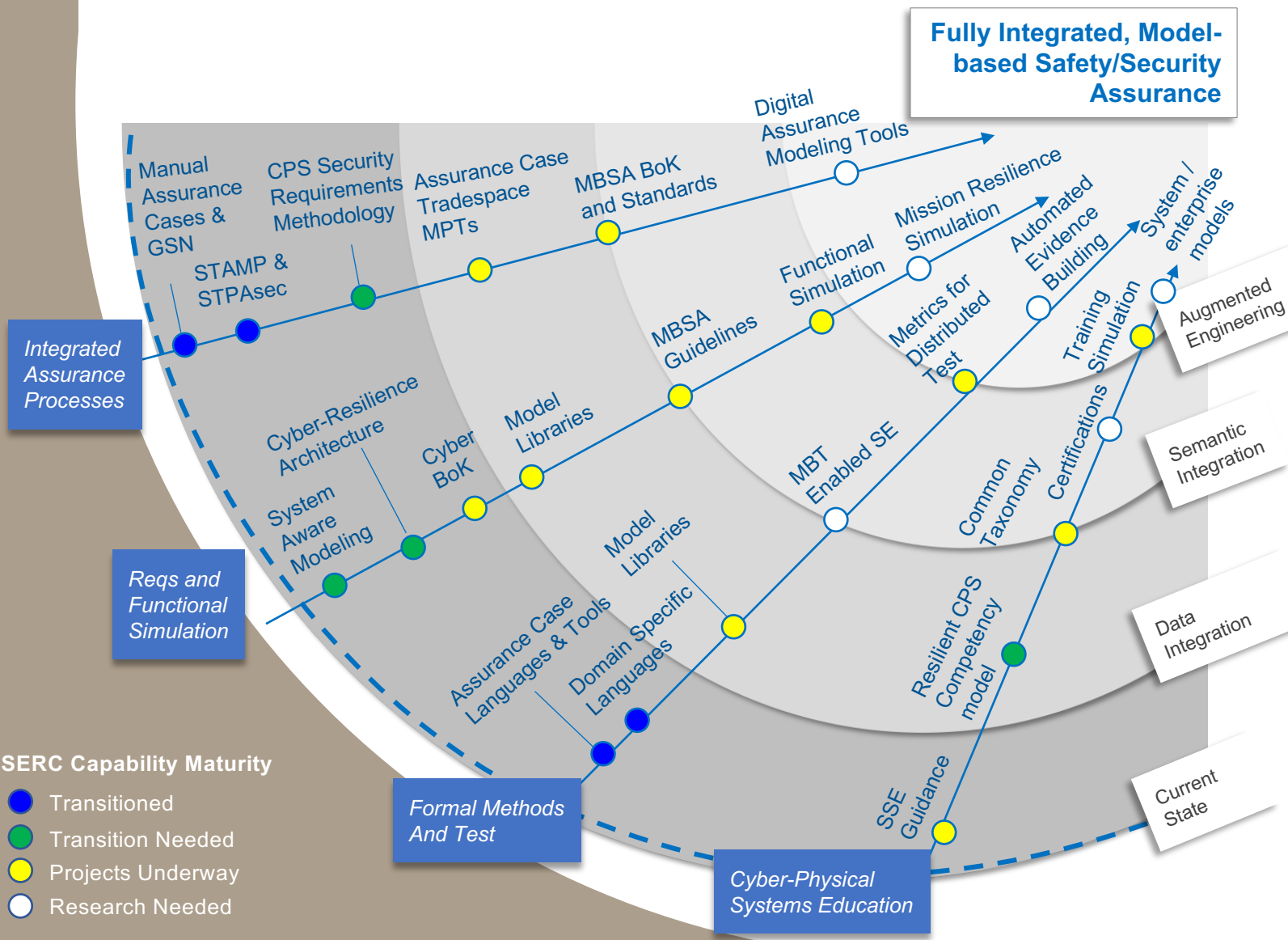
Velocity and agility are critical characteristics of future systems, both for the system that is being deployed and the system that is developing and maintaining the deployed system. With the fusion of development in operations, DevOps, the delineation between these is disappearing. A research roadmap for Velocity is perhaps the most difficult to articulate as it is rooted in current organizational implementation of these practices and methodologies. One might ask, where is the needed research? With our defense and other government sponsors, velocity centers on three goals: (1) architecting systems for continuous development and deployment, (2) leading an agile transition across large government and contractor systems, and (3) the role of Collaborative Integrated Modeling Environments as an enabler. Overall our vision is to enable the transformation of systems engineering from sequential, document-driven, highly constrained practices toward much faster, flexible mission and enterprise-oriented approaches enabled by advances in modeling, simulation, data-driven analysis and artificial intelligence. The research verticals in this area strive for application into two areas: improved mission engineering processes and creation of more adaptive systems. Research areas include rapid development of systems as platforms, architecting these platforms for DevOps enabled systems and environments, and execution of DevOps practices in our sponsor organization. This mission area will always be led by execution, but research is needed in the areas of value-driven design, decision processes, composable systems and platforms, and development environments supporting these characteristics.



- **Agile Methods in SE**: agile development is widely used in software. Corollaries to software agile development processes have been researched and constructed for systems engineering in many domains. The current challenge is to assist DoD acquisition organizations as they transform to agile systems engineering.
- **Commercial DevOps**: existing commercial environments, such as Amazon or Tesla, continuously roll new designs out into the field. DoD systems are moving toward DevOps. The SERC can support this transition with knowledge and manpower.
- **Composability of Deployed Systems**: a key to velocity is to build effective systems from existing elements rather than developing all-new systems. However, often the existing elements are not designed to interface together. The research is to develop methods to architect new systems so that they can be deeply integrated in the field, primarily sharing DevOps software control.
- **Continuous V&V**: continuous development will require treating verification and validation as parallel processes to system development, beginning in the search for materiel solution. At every step, V&V should be answering the question, "Why do we believe this system will be successful to warfighters in the field?" The search for a validation argument will lead to a continuously evolving review and testing strategy.
- **Digital Thread Prototype**: digital engineering is becoming well understood, but putting the methods into practice is a challenge. In the Software Engineering Transformation project, SERC researchers are working hand-in-hand with acquisition professionals to exercise a complete set of digital engineering methods and transform the acquisition culture.
- **Info-Based Test Plan**: SERC research is needed to develop methods, processes and tools that test planners can use to balance the information that will be delivered by an engineering test with the cost of executing the test. Value of Information theory provides a solid basis for this research, but the theory must be implemented in the context of the DoD testing culture. Expected results are more detailed testing in specific areas combined with widespread elimination of tests that cannot justify the cost and schedule they consume.
- **Instrument Development**: determine architectural rules and standard processes that provide instrumentation on new systems, particularly platforms, that can support new capabilities, yet to be designed, that will be introduced through DevOps software change alone.
- **Prototype Very Rapid Development**: pull together the MPTs intended to accelerate system development and exercise them in a realistic scenario. An important step in the SERC plan is to identify the best-qualified company or companies for realizing the best balance across speed, performance, cost and risk for the needed range of systems.
- **Simulation Based Dev**: very early in conceptual design, build a high fidelity simulation of the system in the field. Update the simulated system continuously as design and test proceed, and monitor the field performance in the simulation.
- **User Feedback**: the continuous development and delivery strategy is dependent on user feedback mechanisms that are designed directly into systems. DevOps MPTs should treat direct user feedback as system requirements.
- **Value-Based Acquisition**: a contracting method where the contract incentivizes industry to develop optimal systems, balancing time, cost, risk, performance and –ilities. The basic logic of VBA is being developed in NSF-sponsored research, but SERC research is necessary to make these methods practical and transition them to the acquisition community.
- **Value Models**: mathematical representations of the value proposition for a system that can be used as an objective for optimal design. Value-models have been developed throughout DoD since the mid-1990s, but a reliable process for generating the models needs to be developed and transitioned to practice.
- **Value-Driven Design**: a distributed optimal design approach that drives design trade decision-making down to the lowest possible organizational level when the most data is available to assure the success of the design. Some elements of Value-Driven Design have been prototyped at DARPA, and VDD processes are widely used in Europe, particularly by Airbus and Rolls-Royce. However, the methods need to be tailored for DoD acquisition. Transition to VDD will require SERC support of acquisition cultural transformation.

Research Roadmap: Security

The SERC Security roadmap focuses on critical engineered systems such as cyber-physical systems, embedded systems, and weapon systems. These are often highly assured systems. The roadmap recognizes attributes such as security and resilience as critical system properties, and assurance as a process that yields an evidentiary case that a system is trustworthy with respect to the properties its stakeholders legitimately rely upon. Ongoing SERC security research focuses on three areas: (1) prevent, detect, and mitigate security vulnerabilities; (2) design, model, and conduct analysis of trustworthiness (i.e., safe and secure aspects) of complex cyber-physical system capabilities and behaviors; and (3) develop models, processes, and tools to assure the trustworthiness of system behaviors/ performance envelopes increasingly driven by machine learning, autonomous capabilities, and manned-unmanned teaming. Research is underway in four areas: Integrated Assurance Processes, which address the system design space in a way that integrates security/safety/reliability and advances practices across all three disciplines; Requirements and Functional Simulation, which focuses on early stage design practices and security patterns (build the right system); Formal Methods and Test, which hopes to advance research in proof driven validation and evidence (build the system right); and Cyber Physical Systems Education, addressing the current shortfall of security related education in engineering programs.



Integrated Assurance Processes

- **Manual Assurance Cases:** traditional assurance case design using goal-structured notation or similar arguments, there has been limited adoption of assurance cases for cybersecurity. The SERC is developing a standardized approach.
- **STAMP and STPASec:** move from causal chain based assurance to control loop analyses. This process from MIT has matured and has been the basis of SERC security engineering work.
- **CPS Security Requirements Methodology**: systematic process for behavioral analysis of security threats to CPS and risk assessment leading to the desired architectural design decisions. SERC has led the research in this area and is ready for transition.
- **Assurance Case Tradespace Tools**: quantifiable measures of safety/security assurance, via economic studies and criticality models, to examine and formally trade development from a safety and security view.
- **MBSA Body of Knowledge and Standards**: develop and disseminate agreed on practices for combined safety/security assurance.
- **Digital Assurance Modeling Tools**: rigorous use cases and environment for modeling assurance and trades.

Requirements and Functional Simulation

- **System Aware Modeling**: MBSA approach to capture and model combined system, threat, and countermeasure behaviors. SERC projects are looking at aspects of systems modeling.
- **Cyber Resilience Architecture**: development and demonstration of cyber-physical system architecture patterns that support behavioral models of cyber threats and assurance cases. This has been prototyped in System Aware security as an add-on device.
- **Cyber Body of Knowledge**: comprehensive BoK of cyber threats and countermeasures in the CPS domain, and visualization tools. Work continuing on SERC Security Engineering projects.
- **MBSA Guidelines**: guides and standards for MBSE and model quality to support functional assurance.
- **Model Libraries**: reusable libraries of system, threat, and countermeasure functional components and patterns. Needed as complexity of the analysis increases.
- **Functional Simulation**: MPTs that support simulation of system functions to evaluate threat/countermeasure effectiveness, and visualization tools.
- **Mission Resilience Simulation**: MPTs that support simulation of missions and operations in cyber-threat environments linked to quantifiable measures.

Formal Methods and Test

- **Assurance Case formalisms and tools**: standard and domain specific assurance case languages linked to design tools. DARPA HACMS and CASE programs prototyped an assurance case language that has seen limited use.
- **Domain Specific Languages:** modeling of CPS architectures and characteristics to support automated design and code generation. DARPA HACMS and CASE programs demonstrated the use of AADL as a domain specific language for formality in embedded computing systems.
- **Model Libraries:** reuse and aggregation of component models to support design and test buildup.
- **Metrics for distributed test:** measurement models and AI/ML based prediction of coverage for distributed testing.
- **Automated evidence building** – automation of test and certification processes via models and QA.
- **MBT Enabled SE**: user friendly MBT tools.

CPS Education

- **Common Taxonomy**: the community lacks a lexicon/taxonomy to adequately describe the cyber-physical system security domain. Develop a formal taxonomy to link the computing and military cybersecurity domains.
- **Competency Model:** extend existing IT focused frameworks with the goal to address engineering competencies, specializations, and roles.
- **System Security Engineering (SSE) guidance**: specific guides are needed for the CPS domain.
- **Educational simulations**: cyberspace-realistic virtual reality simulation for a relevant systems (aircraft, missile, Trucks, power plants, etc.) in an unclassified domain.
- **Certifications**: formal security certifications for engineering professionals.
- **System/enterprise models**: collect and model the pathology of CPS security decisions to inform both engineering assumptions in practice and inform use cases for education and training.

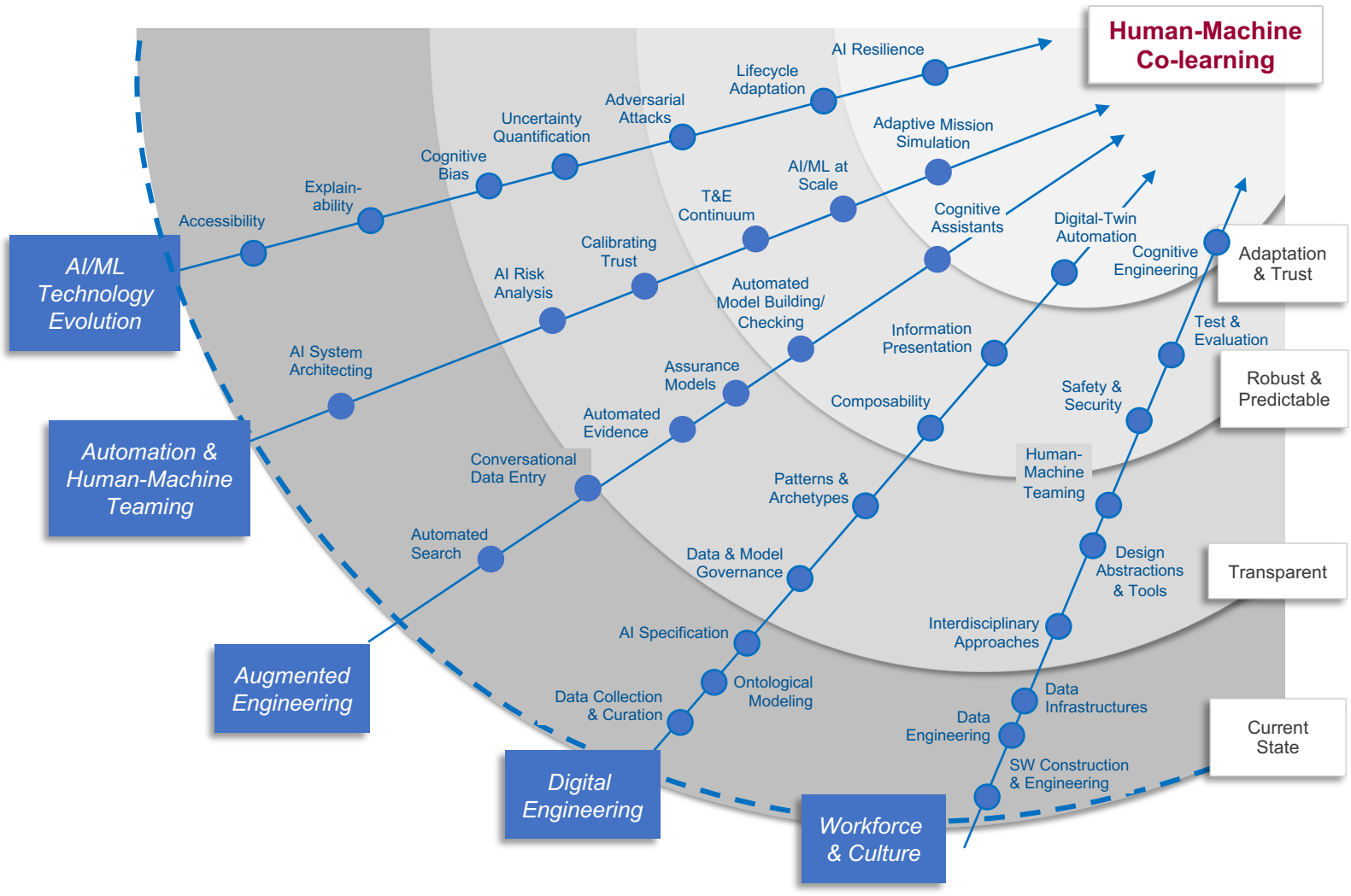
Research Roadmap: AI/Autonomy Framework

The envisioned long-term outcome of the SERC AI and Automation roadmap is "Human-Machine Co-learning." This outcome captures a future where both humans and machines will adapt their behavior over time by learning from each other or alongside each other. More importantly for systems engineering, this is a lifecycle model that is not envisioned and supported by most of the current-day systems engineering practices.

To achieve this end state, one might consider there is a need for both the AI and SE disciplines to pass through a set of "waves" or eras. The first of these includes sets of technologies and approaches that make the decisions produced by AI systems more transparent to the human developers and users. The second wave is to produce systems that learn but are also appropriately robust and predictable in the type of critical applications normal to SE. The third wave involves systems that actually adapt and learn dynamically from their environments.

The vectors of this notional roadmap span five categories. The first of these vectors recognizes that the technological implementation of AI systems will evolve and will need to evolve in directions relevant to SE. Most of these can be related to the development of transparency and trust in technology. The second vector recognizes that the purpose of AI in systems is generally to provide automation of human tasks and decisions.

The third vector recognizes that AI technologies will gradually be used more and more to augment the work of engineering and the fourth vector recognizes that the current digital engineering transformation will be enabler for that. *A short description of each node of the first four vectors is included on the next page.* The final vector recognizes a transformation will need to be accomplished in the SE workforce, with significantly more integration of software and human behavioral sciences at the forefront



UPDATED 2021

AI & Machine Learning Technology

- **Accessibility:** AI algorithms and methods become more available in tools that can be used by multiple disciplines
- **Explainability:** Developing sets of machine learning techniques that produce more explainable models, while maintaining a high level of learning performance (prediction accuracy); and enable human users to understand, appropriately trust, and effectively manage the resulting automation
- **Cognitive Bias**: Reducing errors induced in sampled data or algorithms that cause the expected results of the system to be inappropriate for use
- **Uncertainty Quantification**: Representing the uncertainty of AI predictions as well as the sources of uncertainty
- **Adversarial Attacks:** Use of adversarial samples to fool machine learning algorithms; defensive techniques for detection/classification of adversarial samples
- **Lifecycle Adaptation:** Evolution of AI performance over the lifecycle of a system as the system changes/evolves
- **AI Resilience:** Operational resilience of the system and its users incorporating AI, particularly involving the characteristics of ML systems

Automation and Human-Machine Teaming

- **AI System Architecting:** Building appropriate data and live and virtual system architectures to support learning and adaptation, and more agile change processes
- **AI Risk Analysis:** Methods, processes, and tools need to connect system risk analysis results with AI software modules related to those risks
- **Calibrating Trust:** AI systems that self-adapt while maintaining rigorous safety, security, and policy constraints
- **T&E Continuum:** Methods for addressing AI-related system test and evaluation addressing these systems' ability to adapt and learn from changing deployment contexts
- **AI/ML at Scale:** Appreciation for the dependence of an AI's outputs on its inputs; scale in AI-based systems will increasingly lead to more general intelligence and an inability to relegate AI to a particular subsystem or component
- **Adaptive Mission Simulation:** Computer-based simulation and training supporting non-static objectives and/or goals (games, course of action analysis) necessary to provide contextual learning environments for these systems

Augmented Engineering

- **Automated Search:** Applying ML to historical data and relationships in the engineering domains
- **Conversational Data Entry**: Human/computer interaction processes to convert natural language and other media to formal models
- **Automated Evidence**: Automation of certification and accreditation processes via models and automation of quality assurance data
- **Assurance Models:** Automation of evidence- based models for assuring correctness and completeness of system requirements and design
- **Automated Model Building/ Checking:** Automated construction of models from features in semantic data, used in both creation of new models and correctness of developed models
- **Cognitive Assistants:** Conversational systems automating many mundane data entry, exploration, and engineering calculation tasks, and many workflows

Digital Engineering

- **Data Collection & Curation:** Specific activities to build infrastructure and collect and manage data needed for engineering and programmatic activities in system development and support
- **Ontological Modeling:** Knowledge representation of engineering and programmatic data providing interoperability through standard and domain specific ontologies
- **AI Specification:** System-level and formal specifications for AI behaviors supporting verification activities
- **Data & Model Governance:** Lifecycle management, control, preservation and enhancement of models and associated data to ensure value for current and future use, as well as repurposing beyond initial purpose and context
- **Patterns & Archetypes:** Widely used modeling constructs that separate design from implementation, supporting better reuse and composition
- **Composability:** Rapid development and integration of design using higher level abstracted components and patterns, across multiple disciplines
- **Information Presentation:** Visualization approaches and interfaces supporting human-machine real-time collaborative information sharing via multiple media
- **Digital Twin Automation:** Fully dynamic virtual system copies built from the same models as the real systems running in parallel to physical systems and updating from the same data feeds as their real counterparts

ABOUT SERC

A University-Affiliated Research Center (UARC) of the US Department of Defense, leverages the research and expertise of faculty, staff, and student researchers from more than 20 collaborating universities throughout the United States. SERC is unprecedented in the depth and breadth of its reach, leadership, and citizenship in Systems Engineering.

FOR MORE INFORMATION

Mr. Thomas McDermott, Jr.
Deputy Director, SERC
tmcdermo@stevens.edu